Blockchain and The Value of Operational Transparency

Jiri Chod, Nikolaos Trichakis, Gerry Tsoukalas

Henry Aspegren, Mark Weber*

February 22, 2019

Abstract

In this paper, we develop a new theory that shows signaling a firm's fundamental quality (e.g., its operational capabilities) to lenders through inventory transactions to be more efficient—it leads to less costly operational distortions—than signaling through loan requests, and we characterize how the efficiency gains depend on firm operational characteristics such as operating costs, market size, inventory salvage value and failure probability.

Signaling through inventory being only tenable when inventory transactions are verifiable at low enough cost, we then turn our attention to how this verifiability can be achieved in practice and argue that blockchain technology has the potential to enable it more efficiently than traditional monitoring mechanisms. To exemplify, we introduce `b_verify`, an open-source software/hardware blockchain system we developed to demonstrate how this technology can be implemented in agricultural supply chains, in a cost effective way.

Our paper identifies an important benefit of blockchain adoption—by opening a window of transparency into a firm's operations, blockchain technology furnishes the ability to secure favorable financing terms at lower signaling costs. Furthermore, our analysis of the preferred signaling mode sheds light on what types of firms or supply chains would stand to benefit the most from this use of blockchain technology.

*Chod (chodj@bc.edu): Carroll School of Management, Boston College; Trichakis (ntrichakis@mit.edu): MIT Operations Research Center and Sloan School of Management; Tsoukalas (gtsouk@wharton.upenn.edu): The Wharton School, University of Pennsylvania; Aspegren (henry.aspegren@sc.tsinghua.edu.cn): MIT Media Lab & Tsinghua University; Weber (mark.weber@ibm.com): IBM Research & MIT-IBM Watson Artificial Intelligence Lab.

1 Introduction

Firms seeking the capital needed to efficiently run their operations are often impeded by the vexing problem of information asymmetry. Unable to readily ascertain their fundamental operational capabilities and gauge their risk, prospective lenders frequently command prohibitively high financing rates, which lead to operational distortions. Information asymmetry can be especially problematic for small and medium-sized enterprises (SMEs) and startups, which are likely to be engaged in innovative operations and lack track record and reputation, particularly in developing economies plagued by trust and fraud issues. To overcome this problem, extant literature argues that firms can credibly signal private information to their lenders by distorting loan requests. For instance, a cash-strapped entrepreneur with an innovative prototype can try to signal good demand prospects by requesting a larger loan, accepting restrictive covenants, or shortening loan maturities.

In this paper, we first develop a new theory that shows signaling a firm's fundamental quality (e.g., its operational capabilities) to lenders through inventory transactions to be more efficient—it leads to less costly operational distortions—than signaling through loan requests. Of course, verifiability of a firm's individual inventory transactions involves monitoring costs, which can have a fixed or variable component or both. We characterize conditions under which the benefits of inventory signaling justify these costs. In particular, our theory predicts that inventory signaling (resp. cash signaling) is *strictly* preferable under high (resp. low) inventory perishability, inventory illiquidity, creditworthiness, operating costs, or small (resp. large) market size.

The paper's second goal is to argue that blockchain technology has the potential to lower monitoring costs and provide inventory transaction verifiability more efficiently than traditional monitoring mechanisms. To this end, we introduce `b_verify`, an open-source software/hardware blockchain system we developed to demonstrate how this technology can be implemented in supply chains, in a way that is accessible to SMEs in developing economies. Taken together, our paper identifies an important benefit of blockchain adoption—by opening a window of transparency into a firm's operations, blockchain technology furnishes the ability to secure favorable financing terms at lower signaling costs.

Signaling operational capabilities: cash vs. inventory

In the presence of information asymmetry between firms and their lenders regarding firms' creditworthiness, high-quality firms have an incentive to signal their operational capabilities to obtain more favorable credit terms, whereas low quality firms have incentive to imitate. Among the many potential signaling mechanisms to lenders that have been studied, the majority involve distorting loan terms (Ross 1977, Besanko and Thakor 1987, Milde and Riley 1988). Indeed, signaling through loan requests, which we refer to here as *cash signaling*, is the *de facto* mechanism as lenders observe loan requests directly without incurring monitoring costs.

Firms can also signal their quality by distorting an actual physical investment, e.g., an inventory transaction. What we refer to as *inventory signaling* has been studied primarily in the context of signaling to equity investors, who observe delayed and audited financial reports (Bebchuk and Stole 1993, Lai, Xiao and Yang 2012, Lai and Xiao 2018), and suppliers (Cachon and Lariviere 2001, Özer and Wei 2006, Chod, Trichakis and Tsoukalas 2018). Because lenders such as banks generally do not costlessly (and perfectly) observe inventory transactions, this setting has received far less attention.

Although both these signaling mechanisms are well established in their own separate literature streams, we are not aware of any work that would pit them against each other. Our work bridges this gap by identifying and resolving the tradeoffs firms face when given a choice between these two mechanisms, and deriving conditions on firm operational parameters under which inventory signaling is more efficient. To this end, we take the perspective of a firm that orders inventory of an input good and transforms it into output in the face of uncertain downstream demand. The firm can be one of two types, either high or low quality, which determines its credit risk and constitutes its private information. To finance the input order transaction, the firm requests a loan from a perfectly competitive lender, which sets credit terms according to its belief regarding the firm's quality. When input order transactions are verifiable (at some monitoring cost) by the lender, the lender forms its belief based on the order quantity, and an inventory signaling game emerges. Otherwise, the lender has to form its belief based on the loan request, in which case a cash signaling game arises. Under cash signaling, high-quality firms may be able to separate by inflating their loan requests to the level that low-quality firms are not willing to imitate. Under inventory signaling, separation involves inflating inventory orders rather than loan amounts.

Which of the two mechanisms enables firms to transmit information about their quality more efficiently is not obvious. In particular, our analysis brings to light the following tradeoff: On the one hand, overborrowing by one dollar is generally less costly than overordering by one dollar worth of potentially illiquid inventory. On the other hand, the lower "unit cost" of cash signaling requires that high-quality firms distort their actions by a larger amount in order to separate. Thus, setting the monitoring costs aside, the tradeoff between cash signaling and inventory signaling is a tradeoff between a lower unit cost of overborrowing and a smaller distortion required when overordering.

We resolve the ensuing tradeoff in two steps. First, in the absence of monitoring costs, we show that inventory signaling is generally preferable and characterize the conditions under which this preference is strict. Loosely speaking, this suggests that increased operational transparency (inventory transparency in this case) makes it harder for low-quality firms to imitate and makes "cheap talk" outcomes less possible. Second, in the presence of monitoring costs, we characterize the conditions under which cash signaling strictly dominates inventory signaling and vice versa. More specifically, our theory predicts that (i) inventory perishability, (ii) inventory illiquidity, (iii) firm's creditworthiness, (iv) smaller firm market's size, (v) lower monitoring costs, and (vi) higher operating costs all favor inventory signaling, and, therefore, blockchain adoption.

To the best of our knowledge, our paper is the first to establish the advantage of inventory signaling over cash signaling. Interestingly, this result has evaded even the literature on trade credit financing, which is most pertinent because unlike a bank, a trade creditor observes the inventory transaction automatically. That is, in this paper's nomenclature, trade credit (bank financing) involves inventory (cash) signaling. Our analysis thus implies that signaling to trade creditors is generally more efficient than signaling to banks, which provides a rationale for trade credit financing under information asymmetry regarding borrowers' creditworthiness. The existing papers that rationalize trade credit based on information asymmetry regarding borrowers' creditworthiness (e.g., Biais and Gollier 1997, Jain 2001) assume that suppliers have *a priori* some exogenous informational advantage over banks, for example, due to operating in the same industry. In contrast, our model does not ascribe any *a priori* informational advantage to any party—it begins with a level information playing field, and identifies an advantage of supplier financing that emerges endogenously from the very nature of the transaction and the operational transparency it provides. A more thorough discussion of our contribution to the literature is included in Section 2.

Enabling inventory transaction verifiability through Blockchain

The proposed benefit of inventory signaling is only tenable when firms' individual inventory transactions are verifiable by lenders at low enough costs, which then raises the question of how this can be achieved in practice. We argue that blockchain technology could provide such operational transparency in a more efficient way relative to traditional monitoring mechanisms.

Banks do not generally observe inventory transactions and, if they do (e.g., through letter of credit issuance or asset-based lending) such monitoring is costly and imperfect (Stiglitz and Weiss 1981, Diamond 1991, Burkart and Ellingsen 2004, Fabbri and Menichini 2016). For example, financing through a letter of credit, whereby the bank pays directly the supplier upon the shipment of goods, involves intermediaries and a significant paper trail, and can be costly, time consuming, and subject to fraud.[1] Similarly, an inventory-based loan requires intermediaries to issue and audit warehouse receipts, which is again costly and prone to fraud (Trichakis, Tsoukalas and Moloney 2015).[2]

Trade credit financing, discussed above, is one setting where inventory transparency arises naturally thanks to the dual role of suppliers as creditors. The use of supplier financing, however, has limits as suppliers tend to face a considerably higher cost of capital than banks (Chod 2016). Furthermore, suppliers are often capital constrained themselves, and to extend credit, they usually borrow from banks, i.e., they act as intermediaries.

Blockchain technology has the potential to mitigate many of these issues. Blockchains are cryptographically secure, distributed ledgers whose main technological feature has been the ability to provide verifiability of *digital goods transactions*.[3] The advantages of the technology are relatively well known—at least as they relate to storing records of digital transactions—including 1) strong security (unhackable systems); 2) dis-intermediation, e.g., the ability to provide trust in the absence of a trusted party;[4] 3) record immutability, which provides a permanent chain of audit and reduces fraud opportunities; 4) automation, so that tasks such as making loan payments can be automated (Babich and Hilary 2018). In brief, these features can be leveraged to address many of the aforementioned shortcomings including the paper trail inefficiencies, the need for costly intermediaries, and issues of fraud.

There are, however, some potential obstacles that may limit the technology's relevance to supply chain implementation, or may yet make it expensive to deploy. First, it is not obvious to what extent and how exactly blockchains can be successfully ported to provide verifiability of *physical goods transactions*, such as procuring inventory. In particular, physical transactions involve a certain amount of human intervention and, therefore, are more susceptible to mistakes or deliberate misrepresentation, which could completely negate the main purpose of blockchain adoption in providing transparency.

[1] According to the FBI, "Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped" (https://www.fbi.gov/scams-and-safety/common-fraud-schemes/letter-of-credit-fraud).

[2] Perhaps the most infamous example of falsifying warehouse receipts in asset-based lending is the De Angelis salad oil swindle, which nearly crippled the New York Stock Exchange (Taylor Nov 23, 2013).

[3] Blockchains were originally designed to solve the infamous double spending problem for digital currency, i.e., to ensure that a digital asset transmitted from one party to another has not already been spent elsewhere.

[4] In the Bitcoin blockchain, for instance, the task of recording transactions is assigned to individual miners who compete through a proof of work mechanism at every round, to append blocks to the existing chain, in exchange for compensation (composed of transaction fees, and new currency issuance).

Second, even if transaction verifiability can be successfully ported, it is not clear whether blockchain can be deployed in a way that keeps implementation and operating costs low enough to make it relevant to SMEs in developing economies. To this point, there are substantial differences to consider between *private* and *public* blockchain implementations, each having their own advantages and disadvantages in the context of supply chains. On the one hand, private blockchains have some desirable properties in terms of privacy but 1) are usually not fully decentralized and do not fully eliminate intermediation, 2) have difficulties scaling to achieve adequate security guarantees, and 3) have (relatively speaking) large infrastructure costs. On the other hand, public blockchains, such as the one backing the Bitcoin network, do not suffer from these issues, but they do lack some of the desired properties that are important to supply chains, such as identification of verified parties, privacy of data, and transaction costs that are controlled in-network.

To demonstrate how these technological and cost issues can be overcome in practice, we developed an open-source software/hardware blockchain system termed `b_verify`, for a use case in agricultural supply chains in developing economies. At a high level, the system is designed to leverage the cost-saving and infrastructure benefits of public blockchains, while taking advantage of several clever innovations that mitigate some of the aforementioned privacy, identification and transaction cost issues. (More details about the system, its relevance to SMEs, and its key innovations are included in Section 6.) In summary, `b_verify` is purposed to provide verification of warehousing transactions. Warehouses often play a central role in agricultural supply chains, being frequented by suppliers who deposit inventory, buyers who procure inputs, and banks who utilize warehousing receipts and transactions to process loans (Trichakis, Tsoukalas and Moloney 2015). Installing blockchain at this nexus of stakeholder interaction provides all parties, including the bank, with a 360° view of transactions occurring in the supply chain, along with a cryptographic proof that the records are authentic and that no record has been omitted. According to our theory, this in turn should enable high-quality firms to use inventory as a credible signaling device and thereby unlock access to favorable financing terms with smaller operational distortions.

2 Related Literature

Signaling Models *Signaling through loan requests* has been well studied in the finance literature, going back to Ross (1977) who shows that high-quality firms, concerned with short-term valuation, can signal to investors by requesting larger loans. In Besanko and Thakor (1987), lenders screen borrowers using a credit policy consisting of interest rate, loan amount, collateral, and the credit granting probability, and high-quality firms signal by borrowing more in equilibrium than they would under full information. Milde and Riley (1988) model a game, in which banks screen borrowers by offering higher loans at higher interest rate, and depending on project characteristics, high-quality borrowers may signal by choosing larger or smaller loans in equilibrium. Duan and Yoon (1993) show that when borrowers choose between spot market borrowing and a loan commitment, high-quality borrowers signal by using larger loan commitments.

Signaling through inventory has been studied primarily in the operations management literature in the context of signaling to suppliers and signaling to equity investors. Inventory signaling to suppliers is the subject of Cachon and Lariviere (2001) and Özer and Wei (2006), both of whom examine how a privately informed manufacturer can credibly share demand forecast with a supplier, which then uses this forecast to build capacity. Taking the perspective of the manufacturer and that of the supplier, respectively, Cachon and Lariviere (2001) and Özer and Wei (2006) show that the manufacturer can signal by overordering. Chod, Trichakis and Tsoukalas (2018) study supplier diversification in a model that features inventory signaling to suppliers who are also trade creditors.

The literature on inventory signaling to equity investors draws upon Bebchuk and Stole (1993), who show that when firms are concerned with the short-term valuation and investors observe the investment level, firms can signal high productivity by overinvesting. Building on the same premise but in the supply chain context, Lai, Xiao and Yang (2012) show that inventory overinvestment due to signaling can be prevented using a menu of buyback contracts; Lai and Xiao (2018) find that the first-best inventory decisions can be also achieved in equilibrium when the manager's short-termism is endogenous; and Schmidt et al. (2015) focus on characterizing pooling equilibria.

Our paper contributes to the above literatures by contrasting signaling with loan requests and signaling with inventory, and by establishing the conditions under which the latter dominates. By studying the effect of inventory transaction observability in the context of lending, our paper is intimately related and contributes to the literature on supplier financing.

Supplier Financing The literature on supplier financing is vast and we only review papers here that are closest to ours. Burkart and Ellingsen (2004) show that observability of the input transaction by the supplier reduces the borrower's diversion opportunities. Considering multiple inputs, Fabbri and Menichini (2016) and Chod (2016) show that transaction observability also reduces the asset substitution problem. Although these papers focus on moral hazard, our work focuses on information asymmetry, where it affords new insights. In particular, the insights in these papers are less relevant in settings in which opportunistic behavior can be alleviated through other means, such as debt covenants, strong legal institutions, and so forth (Iancu, Trichakis and Tsoukalas 2016). Our theory holds irrespective of buyer opportunism.

Closer to our work, within information asymmetry models, Burkart and Ellingsen state that "*there is no obvious distinction between lending cash and lending inputs*" (p. 571). Our work demonstrates that such a distinction does exist: it characterizes the conditions under which an input transaction (inventory signaling) transmits private information about the borrower quality more efficiently than a cash transaction (cash signaling). So doing, our work contributes to this literature by providing a novel explanation for the use of supplier financing under information asymmetry.

The explanation offered by our model is distinct from, and possibly more robust than, existing explanations that rationalize supplier financing based on the assumption that suppliers have an *a priori* informational advantage over banks (Emery 1984, Biais and Gollier 1997, Jain 2001). Albeit certainly the case in some instances, it is unlikely that financial institutions specialized in developing lending relationships and assessing creditworthiness are systematically disadvantaged relative to suppliers. Our proposed explanation is immune to this criticism because our model assumes a level playing field between banks and suppliers, and identifies a monitoring advantage of supplier financing that emerges endogenously from the very nature of the transaction and the operational transparency it provides. Our theory, although robust to the foregoing criticisms, admits its own limitation, namely, that it is relevant only in the presence of information asymmetry between buyers (borrowers) and lenders regarding the former's creditworthiness.

Blockchain Literature Most existing literature on blockchains is in computer science, starting with the original white paper by Nakamoto (2008). Several papers examine the economics of mining and optimal design of blockchain systems, e.g., Biais et al. (2017), Huberman, Leshno and Moallemi (2017), Budish (2018), and references therein. Given that blockchain technology is very new and still being actively developed, the management literature on the topic is scarce. Babich and Hilary (2018) provide a qualitative discussion of the technology's potential to improve production and distribution networks and implications for operations management researchers. To the best of our knowledge, ours is the first research paper to explore both practical and theoretical implications of blockchains for supply chain finance and operations management.

A few recent papers, however, have started exploring the impact of blockchain in other areas. For instance, Yermack (2017) examines implications of blockchains for corporate governance, arguing that the transparency of ownership offered by blockchains may upend the balance of power in traditional governance structures. Catalini and Gans (2017) study how blockchain technology could shape innovation by reducing transaction verifiability costs and bypassing intermediaries. Chod and Lyandres (2018) and Gan, Netessine and Tsoukalas (2019) study financing of entrepreneurial ventures by issuing crypto-tokens (ICOs) on existing blockchain platforms. Falk and Tsoukalas (2019) study crowdsourcing, and more specifically, token-weighted voting, for blockchain-based systems, such as token-curated registries (TCRs). Halaburda (2018) provides a comprehensive analysis of blockchain economics.

We contribute to this literature by examining how the existing blockchain technology and, in particular, the transaction verifiability it provides, can be used by firms to transmit information about their inherent quality. Although the literature has recognized the benefits of blockchain-enabled verifiability of *asset ownership* (Biais et al. 2017), we are not aware of any papers that would connect transactional verifiability afforded by blockchain to transparency regarding the firm fundamental *quality*. As we show in this the paper, the leap from one to the other is possible, but can be very subtle.

Other relevant literatures Our paper is related to the operations literature on information sharing and signaling which spans different areas, including signaling operational capabilities in supply chain finance (Tang, Yang and Wu 2018), signaling quality in experimentation and innovation settings (Bimpikis, Drakopoulos and Ehsani 2017, Acemoglu, Drakopoulos and Ozdaglar 2017), signaling content accuracy in social networks (Candogan and Drakopoulos 2017), signaling to crowdfunding contributors (Chakraborty and Swinney 2017), screening firm production capabilities (Chick, Hasija and Nasiry 2016), and many others. Because the key innovation of the blockchain technology that we focus on is that it enables information sharing when transacting parties do not trust each other, our work also contributes to the literature on trust in supply chains (Özer, Zheng and Ren 2014).

More broadly, our paper is related to research at the interface of operations and finance. Early papers include Babich and Sobel (2004), Buzacott and Zhang (2004), Xu and Birge (2004), and Ding, Dong and Kouvelis (2007), who study how financial considerations affect a firm's operations. Closer to our setting, Boyabatlı and Toktay (2011) consider the impact of capital market imperfections on firm technology choice, though they do not consider information asymmetry, which is our main focus. A review of this literature is provided by Kouvelis (2012).

Our work, and particularly our `b_verify` system inspired from use cases in agricultural supply chains in Latin America, contributes to a fairly recent but growing literature studying operations management issues in agriculture industries. For example, Boyabatlı, Kleindorfer and Koontz (2011) study procurement, processing, and production decisions in beef supply chains. At a higher level, Akkaya, Bimpikis and Lee (2016) explore the role of Government intervention in promoting sustainable practices in agriculture, and investigate the effectiveness of a number of policy instruments, such as taxes taxes and subsidies, at spurring adoption and welfare. Serhatli, Calmon and Yucesan (2017) examine inventory/productions decisions in the context of corn seed manufacturing. Calmon, Hasija and Sudhir (2017) discuss the problem of a retailer that sources perishable goods from small farmers, whose quality depends on some non-contractible effort that the farmer exerts. Our work adds to this literature by examining how novel blockchain technology can be implemented in central storage warehouses for perishable produce to alleviate information asymmetry issues in developing economy agriculture supply chains.

3 Model

Consider a firm that can be one of two types: low-quality or high-quality, denoted by subscripts L and H, with probability $1-h$ and h, respectively. The two types differ in their operational capabilities, which manifest in different demand curves the firms face in the output market. Firm of type i, or simply firm i, sells its output at price $\tilde{\alpha}_i - x$, where x is the quantity sold and $\tilde{\alpha}_i$ is a demand shock or price intercept that follows a two-point distribution

$$\tilde{\alpha}_i := \begin{cases} \alpha_i \text{ with probability } 1-b_i, \\ 0 \text{ with probability } b_i, \end{cases} \qquad i \in \{L, H\},$$

where $\alpha_H > \alpha_L$ and $b_H < b_L$. When $\tilde{\alpha}_i = \alpha_i$ ($\tilde{\alpha}_i = 0$), we say that firm i's product is a success (failure). If the product is a success, the firm generates sales revenue $(\alpha_i - x)\,x$; if the product is a failure, it generates no revenue and we assume that the unsold output has no residual value. Thus, a high-quality firm has a higher probability of success and faces a larger market size conditional on success.[5] A firm's type constitutes its private information.

Before the firm finds out whether its product is a success or a failure, it purchases Q units of an input, referred to as "inventory" at a unit cost c. Subsequently, but still before success/failure is revealed, the firm transforms x units of this input into output, and brings this output to the market. Any linear internally funded cost of production can be subsumed by the demand curve intercept α_i, which can thus be also interpreted as an (inverse) measure of the firm's operating costs. Inventory units not processed spoil and have zero salvage value.

Inventory is financed entirely by credit, which is priced competitively, i.e., the lender charges

[5]The reason we assume that a higher probability of success is associated with a larger market size is that both are likely to result from superior management or operations capabilities.

fair interest at which it expects to break even.[6,7] For example, when the lender provides credit D and expects no repayment in the bankruptcy state whose probability it believes to be b, and full repayment otherwise, it charges interest r given by

$$(1-b)(D+r) = D \iff r = D\frac{b}{1-b}. \tag{1}$$

One can easily see that firm i goes bankrupt if its product is a failure.

We assume that the production lead time is longer than the grace period granted to the firm by the input supplier. In other words, the firm needs to secure input financing before it completes production and, as a result, cannot use output (whether it is ultimately observable by the lender or not) as a signaling device vis-à-vis the lender. We also assume that firms are not allowed to pay dividends unless they repay lenders, they cannot repay early, and they deposit all excess cash at the risk-free rate, which is normalized to zero. The equity value of a firm of type i that purchases Q units of input, transforms x units of this input into output, and faces interest r, equal to

$$V_i(Q,x,r) := (1-b_i)((\alpha_i - x)x - cQ - r), \quad i \in \{L, H\}.$$

Firms make decisions so as to maximize their equity value.

We make a technical assumption that the difference between the failure probabilities of the two types is large enough so that

$$\frac{b_L}{1-b_L}(\alpha_L - c) > \frac{b_H}{1-b_H}(\alpha_H - c). \tag{2}$$

This condition ensures that if high and low types request the same loan amount under full information, the low type is charged a higher interest. This condition is necessary to rule out the unlikely, but theoretically conceivable scenario in which the lender charges the low type a more favorable interest, knowing that given its smaller market size, the low type will put at risk (by investing into inventory) a smaller fraction of the amount borrowed. Most important, this condition provides the high (low) type with the incentive to signal (imitate).

4 Analysis

Our analysis proceeds as follows. We first consider a benchmark "full information" case, wherein the lender knows the firm's true type. We then consider the asymmetric information case under two

[6]Fairly priced credit is a standard assumption in the finance literature (see e.g., Biais and Gollier 1997 and Burkart and Ellingsen 2004).

[7]We normalize the lender's cost of capital to zero without a loss of generality.

alternative scenarios that differ with respect to the firm's operational transparency *vis-à-vis* the lender. Section 4.2 deals with the cash signaling game that ensues absent operational transparency, i.e., when the lender does not observe the firm's inventory order before setting the credit terms. Under the assumption of zero monitoring costs, Section 4.3 deals with the inventory signaling game that arises in the presence of operational transparency, i.e., when the lender does observe the firm's inventory order before setting the credit terms. Then, in Section 4.4, we pit the two signaling games against each other, and characterize the equilibrium choice of signaling mechanism. Section 4.5 provides a sensitivity analysis. The assumption of zero monitoring costs is relaxed in Section 4.6, wherein we characterize the conditions under which cash signaling is strictly preferred and vice versa. In our analysis of signaling games, we focus on pure-strategy perfect Bayesian Nash equilibria (PBE).

Note that, in this section, we use blockchain simply as a running example of a monitoring mechanism that can provide operational transparency to lenders; our analysis remains applicable to all other alternative mechanisms we discussed in the Introduction. (We use blockchain as our running example because, as we argue in Section 6, it has the potential to provide operational transparency at a lower cost relative to conventional alternatives.) Accordingly, we denote the equilibrium outcomes of the cash and inventory signaling games using subscripts $\varnothing$ and Ƀ, respectively, where Ƀ is a mnemonic for blockchain-enabled operational transparency.

4.1 Full Information

Suppose for now that the lender knows the firm's true type. Under full information, the lender can always infer the firm's inventory order from the loan amount. Furthermore, absent any signaling incentives, the firm has no reason to borrow more than it will spend on inventory, or to order more inventory than it will process into output, i.e., $D = c\,Q$ and $x = Q$.

When financing Q units of inventory, firm of type i faces interest $c\,Q\frac{b_i}{1-b_i}$ according to (1). Consequently, its optimal inventory decision is

$$Q_i^{\text{fb}} := \arg\max_{Q\geq 0} V_i\left(Q, Q, c\,Q\frac{b_i}{1-b_i}\right), \quad i \in \{L, H\}. \tag{3}$$

It is easy to show that the optimal solution to (3) is $Q_i^{\text{fb}} = \frac{1}{2}\left(\alpha_i - \frac{c}{1-b_i}\right)$, the corresponding optimal loan amount is $D_i^{\text{fb}} = c\,Q_i^{\text{fb}}$, and the resulting equity value is $V_i^{\text{fb}} = \left(Q_i^{\text{fb}}\right)^2(1-b_i)$.

The inventory level that maximizes the value of equity in (3) also maximizes total value of equity and debt, i.e.,

$$Q_i^{\text{fb}} = \arg\max_{Q\geq 0}\left[-c\,Q + (1-b_i)(\alpha_i - Q)\,Q\right], \quad i \in \{L, H\}.$$

Therefore, we refer to Q_i^{fb} as the first-best inventory order and to D_i^{fb} as the first-best loan amount of firm i. Because the first-best order quantity increases with demand curve intercept α_i, and decreases with bankruptcy probability b_i, the high type chooses a larger order quantity than the low type, i.e., $Q_H^{\text{fb}} \geq Q_L^{\text{fb}}$.

The rest of the analysis focuses on the more interesting case in which lenders do not know *a priori* the firm type. Instead, their prior is that any given firm is of type H with probability h. We first analyze the benchmark scenario, in which firms borrow in the absence of blockchain-enabled inventory monitoring.

4.2 Cash Signaling: Borrowing in the Absence of Blockchain

Recall that in the absence of blockchain, the lender cannot observe the firm's inventory order before pricing the loan. It can only observe the loan amount requested D, based on which it forms its belief about the firm's type, $\beta_\varnothing(D) \in \{L, H\}$. We follow Spence (1973) in assuming that this belief follows a threshold structure:

$$\beta_\varnothing(D) := \begin{cases} H & \text{if } D \geq d, \\ L & \text{o/w.} \end{cases} \tag{4}$$

The lender believes that a firm is of the high type if, and only if, it requests a loan amount $D \geq d$ for some (endogenously determined) threshold $d > 0$. Associating a larger loan request with the high type is reasonable because the first-best loan amount of the high type is above that of the low type.[8] The interest the lender sets is then a function of the loan amount, i.e., $r_\varnothing = r_\varnothing(D)$.

The firm faces a three-stage decision problem. In the first stage, it chooses the loan amount D. The lender issues the loan and sets the interest based on its belief $\beta_\varnothing(D)$ regarding the firm type. In the second stage, the firm chooses the amount of inventory Q to purchase, subject to the loan obtained covering the purchasing cost, $D \geq cQ$. In the third stage, the firm decides how much of the purchased inventory to process, x. We solve the firm's problem by backward induction.

Because the lender does not observe the order quantity, the firm cannot use inventory to signal and, therefore, has no incentive to buy more inventory than it will eventually process. Therefore, the third-stage production decision simplifies into $x = Q$. However, the lender observes the loan amount, which thus becomes a signaling device. As a result, the firm may overborrow, i.e., borrow more than its first best—or even more than it will eventually invest in inventory—to signal its type.

[8] As we show in Section 4.7, assuming a threshold-type belief structure is without any loss of generality because starting with an arbitrary belief structure leads to the same *least-cost* separating equilibrium.

Having obtained a loan D at interest $r_{\varnothing}(D)$, the firm of type i purchases inventory

$$Q_i(D) := \arg \max_{0 \le Q \le D/c} V_i\left(Q, Q, r_{\varnothing}(D)\right), \quad i \in \{L, H\}.$$

It can be shown that the optimal inventory order is

$$Q_i\left(D\right) = \frac{1}{c} \min\left\{D, \overline{D}_i\right\}, \quad i \in \{L, H\}, \tag{5}$$

where $\overline{D}_i := \frac{c}{2}\left(\alpha_i - c\right)$ is the "investment cap," above which it is not economical to invest cash into inventory, i.e., any borrowing above the investment cap sits idle.

Because the firm has no other investment or diversion opportunities, the lender rationally anticipates that any amount borrowed above the investment cap will not be put at risk. Therefore, it charges interest based only on the amount that it expects to be invested in inventory, $c\, Q_{\beta_{\varnothing}(D)}(D)$, in accordance with its belief $\beta_{\varnothing}(D)$. The fair interest is then given by

$$r_{\varnothing}\left(D\right) = \begin{cases} c\, Q_H\left(D\right) \dfrac{b_H}{1 - b_H} & \text{if } D \ge d, \\ c\, Q_L\left(D\right) \dfrac{b_L}{1 - b_L} & \text{o/w.} \end{cases} \tag{6}$$

In the first stage, the firm requests a loan amount D so as to maximize the value of equity

$$V_{i\varnothing}\left(D\right) := V_i\left(Q_i\left(D\right), Q_i\left(D\right), r_{\varnothing}\left(D\right)\right), \quad i \in \{L, H\}.$$

A separating equilibrium (SE) is characterized by the optimal loan amounts $\{D_L^{\text{se}}; D_H^{\text{se}}\}$ and a consistent belief structure given by (4) that satisfies the following necessary and sufficient conditions:

$$\max_{D<d} V_{H\varnothing}\left(D\right) \le \max_{D \ge d} V_{H\varnothing}\left(D\right), \quad \text{and} \tag{7}$$

$$\max_{D<d} V_{L\varnothing}\left(D\right) \ge \max_{D \ge d} V_{L\varnothing}\left(D\right). \tag{8}$$

Condition (7) ensures that the high-quality firm borrows an amount at or above the threshold d, whereas condition (8) ensures that the low-quality firm borrows below d. Because these conditions may lead to multiple SE's, we adopt the Cho and Kreps (1987) intuitive criterion refinement which eliminates any Pareto-dominated equilibria. We refer to any equilibria that survive as least-cost separating equilibria (LCSE).

Intuitively, at the least-cost SE the high type borrows either the minimum amount of money necessary to separate from the low type, or his first best, whatever is larger. The minimum loan amount that the high type needs to borrow to separate from the low type is the maximum loan amount that the low type is willing to borrow to imitate the high type. This amount determines the least-cost equilibrium belief threshold d, and it is such that the low type is indifferent between ordering d while being perceived as high type, and ordering his first best while being perceived as low type. Before stating the equilibrium results, it is useful to define two thresholds. Let

$$\begin{aligned} b^{\text{se}} &:= \frac{2(1-b_L)b_L\alpha_L - c\left(2b_L - b_L^2\right)}{2(1-b_L)^2\alpha_H + 2(1-b_L)b_L\alpha_L - c\left(2 + b_L^2 - 2b_L\right)}, \quad \text{and} \\ b^{\varnothing} &:= \frac{2(1-b_L)b_L\alpha_L - c\left(2b_L - b_L^2\right)}{2(1-b_L)\alpha_L - c\left(2 + b_L^2 - 2b_L\right)}. \end{aligned}$$

It is straightforward to show that $b^{\varnothing} > b^{\text{se}}$.

Proposition 1. Absent blockchain-enabled operational transparency, if $b_H > b^{\text{se}}$, there exists a unique LCSE, which is given by loan amounts $D_L^{\text{se}} = D_L^{\text{fb}}$ and $D_H^{\text{se}} = \max\left(D_H^{\text{fb}}, d\right)$ where

$$d = \begin{cases} \frac{c}{2}\left(\alpha_L - \frac{c}{1-b_H} + \sqrt{\left(\alpha_L - \frac{c}{1-b_H}\right)^2 - 4\left(Q_L^{\text{fb}}\right)^2}\right) & \text{if } b_H \geq b^{\varnothing}, \\ \frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right)\frac{1-b_H}{1-b_L}\frac{b_L}{b_H} & \text{o/w.} \end{cases} \tag{9}$$

If $b_H \leq b^{\text{se}}$, no separating equilibrium exists.

When a SE exists, the low type follows its first best, whereas for the high type there are two scenarios. When $d \leq D_H^{\text{fb}}$, the low type is not willing to borrow up to the high type's first best, and so the high type can borrow its first-best D_H^{fb} without being imitated. The second and more salient scenario takes place when $d > D_H^{\text{fb}}$, i.e., the low type is willing to mimic the high type's first best. In this case, the high type needs to overborrow up to d to separate itself. This ultimately distorts its inventory investment as well in the sense that $Q_H(d) > Q_H^{\text{fb}}$.[9]

The existence and form of the separating equilibrium depends critically on the bankruptcy probability of the high type, b_H, which determines the strength of low type's incentives to imitate.

1. If $b_H \geq b^{\varnothing}$, the high type's bankruptcy probability is relatively high, which limits the low type's willingness to imitate. Specifically, the low type is not willing to borrow beyond its investment cap in order to imitate, i.e., $d \leq \overline{D}_L$.

2. If $b^{\text{se}} \leq b_H < b^{\varnothing}$, the advantage of being perceived as the high type is significant enough for the low type to be willing to borrow beyond its investment cap in order to imitate, i.e., $d > \overline{D}_L$.

3. If $b_H \leq b^{\text{se}}$, the high type's bankruptcy probability is so low, that in order to be perceived as the high type, the low type is willing to borrow up to the *high type's* investment cap $\overline{D}_H$.

[9]Whereas the LCSE loan amounts are always unique, the belief threshold is unique only in this second scenario. When both firms choose first best, any belief threshold in $[d, D_H^{\text{fb}}]$ is consistent with their equilibrium actions.

Thus, the high type cannot separate by borrowing less than $\overline{D}_H$. Recall that any borrowing beyond $\overline{D}_H$ would not be invested in inventory by either type. Without further distorting a firm's operations and thereby increasing its signaling cost, borrowing beyond this point would be a cheap talk. Therefore, borrowing beyond $\overline{D}_H$ does not allow the high type to separate either. As a result, no separating equilibrium can exist in this case.

4.3 Inventory Signaling: Borrowing in the Presence of Blockchain

We assume for now that the use of blockchain technology comes at no monitoring cost, and then relax this assumption in Section 4.6. Because blockchain allows lenders to observe and verify firms' inventory orders, firms can use inventory as a signaling device. Let $\beta_{\mathrm{B}}(Q) \in \{L, H\}$ be the belief regarding the firm type that the lender forms upon observing an order quantity Q. We borrow again from Spence (1973) in assuming that the lender's belief has a threshold structure, i.e.,

$$\beta_{\mathrm{B}}(Q) := \begin{cases} H & \text{if } Q \geq q, \\ L & \text{o/w.} \end{cases} \tag{10}$$

Thus, if a firm orders inventory Q above some (endogenous) threshold q, the lender believes the firm to be of the high type. Otherwise, it believes that the firm is of the low type. This is reasonable given that the high type has a higher first-best order quantity, i.e., $Q_H^{\mathrm{fb}} > Q_L^{\mathrm{fb}}$.

Because the lender forms its belief based on the actual order quantity rather than the loan request, the firm has no incentive to borrow more than what it invests in inventory. The firm's decision problem thus simplifies into a two-stage optimization. In the first stage, it decides the order quantity Q or, equivalently, the loan amount $D = c\,Q$. The lender provides the loan and charges interest

$$r_{\mathrm{B}}\left(Q\right) := \begin{cases} c\,Q\,\dfrac{b_H}{1-b_H} & \text{if } Q \geq q, \\ c\,Q\,\dfrac{b_L}{1-b_L} & \text{o/w,} \end{cases} \tag{11}$$

according to (1) and (10). In the second stage, the firm decides how much of the purchased inventory Q to transform into output x. We solve the two-stage problem via backward induction.

Because the firm may have incentive to overorder in the first stage to signal that it is of the high type, it may end up with more inventory than it will be willing to process into output in the second stage. Therefore, we can no longer take for granted that $x = Q$. Instead, we need to allow the firm to choose its output level optimally. Given an inventory amount Q and facing interest $r_{\mathrm{B}}(Q)$, the firm of type i chooses output

$$x_i\left(Q\right) := \arg\max_{x \leq Q} V_i\left(Q, x, r_{\mathrm{B}}(Q)\right), \quad i \in \{L, H\}.$$

Because the sales revenue starts decreasing in output at $\overline{Q}_i := \frac{1}{2}\alpha_i$, the firm will never produce beyond this "production cap," even if it means not using the entire inventory. In other words, the firm's optimal output is given by

$$x_i(Q) = \min\{Q, \overline{Q}_i\}, \quad i \in \{L, H\}. \tag{12}$$

In the first stage, the firm selects the order quantity Q to maximize the value of equity

$$V_{i\mathrm{B}}(Q) := V_i(Q, x_i(Q), r_{\mathrm{B}}(Q)), \quad i \in \{L, H\}.$$

A separating equilibrium is characterized by the low type's and the high type's optimal order quantities $\{Q_L^{\mathrm{se}}; Q_H^{\mathrm{se}}\}$ and a consistent belief structure given by (10) that satisfies the following necessary and sufficient conditions:

$$\max_{Q<q} V_{H\mathrm{B}}(Q) \leq \max_{Q\geq q} V_{H\mathrm{B}}(Q), \quad \text{and} \tag{13}$$

$$\max_{Q<q} V_{L\mathrm{B}}(Q) \geq \max_{Q\geq q} V_{L\mathrm{B}}(Q). \tag{14}$$

Condition (13) ensures that a high-quality firm orders a quantity at or above the threshold q. Condition (14) ensures that a low-quality firm orders a quantity below this threshold.

Similar to d, the LCSE belief threshold q is given by the low type's indifference point. In this case, it is the maximum amount of inventory that the low type is willing to order so as to imitate the high type. Before characterizing the SE, it is useful to define a threshold bankruptcy probability

$$b^{\mathrm{B}} := \frac{2(1-b_L)\, b_L \alpha_L - c}{2(1-b_L)\,\alpha_L - c}.$$

Proposition 2. In the presence of blockchain-enabled operational transparency, there always exists a unique LCSE, which is given by order quantities $Q_L^{\mathrm{se}} = Q_L^{\mathrm{fb}}$ and $Q_H^{\mathrm{se}} = \max\left(Q_H^{\mathrm{fb}}, q\right)$ where

$$q = \begin{cases} \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_H} + \sqrt{\left(\alpha_L - \frac{c}{1-b_H}\right)^2 - 4\left(Q_L^{\mathrm{fb}}\right)^2}\right) & \text{if } b_H \geq b^{\mathrm{B}}, \\ \frac{1}{2}\left(\alpha_L - \frac{1}{2}\frac{c}{1-b_L}\right)\frac{1-b_H}{1-b_L} & \text{o/w.} \end{cases} \tag{15}$$

In the LCSE, the low type always orders its first best Q_L^{fb}, being unable to imitate the high type. For the high type, there are two possible scenarios depending on the low type's willingness to overorder. If the low type is not willing to imitate the high type's first best, i.e., $q \leq Q_H^{\mathrm{fb}}$, the high type can order its first best. The second scenario is more interesting. If the low type is willing to imitate the high type's first best, i.e., $q > Q_H^{\mathrm{fb}}$, the high type has to inflate its order up to q units to avoid imitation.[10]

[10]Whereas the LCSE quantities $\{Q_L^{\mathrm{se}}, Q_H^{\mathrm{se}},\}$ are always unique, the equilibrium belief threshold is unique only in this second scenario. When both firms order first best, any belief threshold in $[q, Q_H^{\mathrm{fb}}]$ is an equilibrium belief structure.

The functional form of the belief threshold q in (15) depends on the high type's bankruptcy probability, which affects the low type's incentive to imitate.

1. If $b_H \geq b^{\text{Ƀ}}$, the high type's bankruptcy probability is considerable, so the advantage of being perceived as a high type is not sufficient to justify for the low type to order above its production cap in an attempt to imitate, i.e., $q \leq \overline{Q}_L$.

2. If $b_H < b^{\text{Ƀ}}$, the reward from imitating the high type is so significant that the low type is willing to order beyond its own production cap in order to imitate, i.e., $q > \overline{Q}_L$.

Finally, note that a SE always exists with blockchain. Because increasing inventory of illiquid and perishable goods beyond a firm's first best is always costly, overordering inventory, unlike overborrowing cash, is never cheap talk. Furthermore, because such overordering always is costlier for the low type, which derives less value from each unit of inventory, separation is always possible.

In the next section, we examine the firm's choice whether or not to adopt blockchain technology.

4.4 Comparison of Signaling Modes: Equilibrium Adoption of Blockchain

Suppose that in addition to making the operations and financing decisions that we have examined thus far, firms need to decide whether or not to adopt blockchain. In this case, the set of potential separating equilibria comprises four possible classes: Ƀ-∅, Ƀ-Ƀ, ∅-∅, and ∅-Ƀ, where the left (right) entry represents the low (high) type's technology choice. For example, Ƀ-∅ means that in equilibrium the low type uses blockchain whereas the high type does not.

We continue to assume that each lender holds a threshold belief structure, where q and d denote the equilibrium order quantity and loan amount thresholds, respectively. The necessary and sufficient conditions characterizing a separating equilibrium in this case are

$$\begin{aligned}
\max\left\{\max_{D<d} V_{H\varnothing}(D), \max_{Q<q} V_{H\text{Ƀ}}(Q)\right\} &\leq \max\left\{\max_{D\geq d} V_{H\varnothing}(D), \max_{Q\geq q} V_{H\text{Ƀ}}(Q)\right\}, \\
\max\left\{\max_{D<d} V_{L\varnothing}(D), \max_{Q<q} V_{L\text{Ƀ}}(Q)\right\} &\geq \max\left\{\max_{D\geq d} V_{L\varnothing}(D), \max_{Q\geq q} V_{L\text{Ƀ}}(Q)\right\}.
\end{aligned}$$

These conditions in some sense combine conditions (13)-(14) and (7)-(8) from our previous analysis. The first inequality ensures that in any SE, the high type chooses to signal high – with blockchain or without – by ordering or borrowing above the corresponding belief threshold. The second inequality ensures that the low type chooses to order or borrow below the corresponding belief threshold. Both firms' actions are thus consistent with their lenders' beliefs in equilibrium.

Note that in any SE, the low type chooses its first best financing/inventory. Because its operations/financing decisions are not distorted by signaling, the low type is indifferent between using and not using blockchain, i.e., for any SE of class Ƀ-Ƀ (Ƀ-∅), there is an equivalent equilibrium of class ∅-Ƀ (∅-∅), in which both types make the same inventory/financing decisions. Because in practice, the use of blockchain comes at a cost, in what follows we restrict our attention to SE in which the low type does not use blockchain.

Proposition 3. (1) A separating equilibrium always exists.
(a) If $b_H \leq b^{\text{se}}$, all separating equilibria belong to class $\varnothing - \text{Ƀ}$. Among these, there exists a unique LCSE, which is given by $D_L^{\text{se}} = D_L^{\text{fb}}$ and $Q_H^{\text{se}} = \max\left(Q_H^{\text{fb}}, q\right)$, with $d = \infty$ and

$$q = \begin{cases} \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_H} + \sqrt{\left(\alpha_L - \frac{c}{1-b_H}\right)^2 - 4\left(Q_L^{\text{fb}}\right)^2}\right) & \text{if } b_H \geq b^{\text{Ƀ}}, \\ \frac{1}{2}\left(\alpha_L - \frac{1}{2}\frac{c}{1-b_L}\right)\frac{1-b_H}{1-b_L} & \text{o/w.} \end{cases} \tag{16}$$

(b) Otherwise, there are additional separating equilibria, which belong to class $\varnothing - \varnothing$. Among these, there exists a unique LCSE, which is given by $D_L^{\text{se}} = D_L^{\text{fb}}$ and $D_H^{\text{se}} = \max\left(D_H^{\text{fb}}, d\right)$, with $q = \infty$ and

$$d = \begin{cases} \frac{c}{2}\left(\alpha_L - \frac{c}{1-b_H} + \sqrt{\left(\alpha_L - \frac{c}{1-b_H}\right)^2 - 4\left(Q_L^{\text{fb}}\right)^2}\right) & \text{if } b_H \geq b^{\varnothing}, \\ \frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right)\frac{1-b_H}{1-b_L}\frac{b_L}{b_H} & \text{o/w.} \end{cases} \tag{17}$$

(2) No pooling equilibria survive the intuitive criterion.

Depending on the high type's failure probability b_H, one of two scenarios arises:

(a) If $b_H \leq b^{\text{se}}$, the high type cannot separate itself without using blockchain because borrowing large amounts of cash without being able to show how it was spent is cheap talk. If this is the case, the high type has no choice but to use blockchain in order to separate itself. The low type follows its first best without the use of blockchain. Thus, all separating equilibria fall into the ∅-Ƀ class, and the least-cost among them has a structure analogous to the LCSE characterized in Section 4.3.

(b) If $b_H > b^{\text{se}}$, the high type is able to separate even without blockchain and, therefore, additional separating equilibria emerge in the ∅-∅ class. The least-cost among them is identical to the LCSE described in Section 4.2. In other words, there are two candidates for the LCSE of the full game: one of class ∅-∅, in which the high type does not adopt blockchain, and one of class ∅-Ƀ, in which it does. Which of these two equilibria leads to lower signaling costs and thus emerges as the LCSE is what we examine next.

We formally define the signaling costs for any given SE as the difference between the high type's equity value under the first best and under that SE.[11] The high type's equity value under

[11] Recall that in any SE, the low type follows its first best and it is the high type that bears all signaling costs.

the $\varnothing$-Ƀ and $\varnothing$-$\varnothing$ equilibria identified in Proposition 3 is $V^{\text{se}}_{H\text{Ƀ}} := V_{H\text{Ƀ}}\left(Q^{\text{se}}_H\right)$ and $V^{\text{se}}_{H\varnothing} := V_{H\varnothing}\left(D^{\text{se}}_H\right)$, respectively. Therefore, the signaling costs under equilibrium of class $\varnothing$-j are

$$\mathcal{C}_j := V^{\text{fb}}_H - V^{\text{se}}_{Hj}, \quad j \in \{\text{Ƀ}, \varnothing\}.$$

When both technology modes allow the high-quality firm to separate, using blockchain is preferable and the LCSE is of class $\varnothing$-Ƀ if, and only if, $\mathcal{C}_{\text{Ƀ}} \le \mathcal{C}_\varnothing$.

Whether the last inequality holds true or not depends on the cost of overborrowing cash relative to the cost of overordering inventory, as well as on the total amount by which the high type needs to overborrow or overorder in order to separate itself. Overborrowing by one dollar is generally cheaper than overordering by one dollar worth of inventory because the former affords the option not to convert the cash into goods. Consequently, the low type is willing to overborrow more than it is willing to overorder in order to imitate. As a result, signaling with cash generally requires a *larger distortion* by the high type than signaling with inventory. In particular, when both signaling mechanisms allow separation, we have

$$d > cq \quad \text{if} \quad b^{\text{se}} < b_H < b^{\varnothing}, \text{ and} \tag{18}$$

$$d = cq \quad \text{if} \quad b_H \ge b^{\varnothing}. \tag{19}$$

Interestingly, when $b_H \ge b^{\varnothing}$, the low type is not willing to overborrow beyond its investment cap and the aforementioned option is "out of the money." In this case, overborrowing cash is equally costly to the low type as overordering inventory, and both signaling games result in the same equilibrium distortion.

To sum up, in order to separate itself without the use of blockchain, the high type needs to overborrow by the same or a larger amount than it has to overorder with blockchain. At the same time, overordering a unit of inventory is equally or more costly than overborrowing the equivalent amount of cash. Which of the two effects dominates determines whether blockchain adoption increases or decreases the total signaling cost and, therefore, whether or not it emerges as the LCSE. Before resolving the tradeoff, we define a critical value $b^{\text{cr}} := \min\{b^0, b^{\varnothing}\}$, where b^0 is the smaller of the two roots in b_H of the following equation:

$$\frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right)\frac{1-b_H}{1-b_L}\frac{b_L}{b_H} = D^{\text{fb}}_H. \tag{20}$$

It can be shown that $b^{\text{se}} < b^{\text{cr}}$, and we have the following result, which answers the key questions as to when, and why, a high-quality firm prefers to use the blockchain technology.

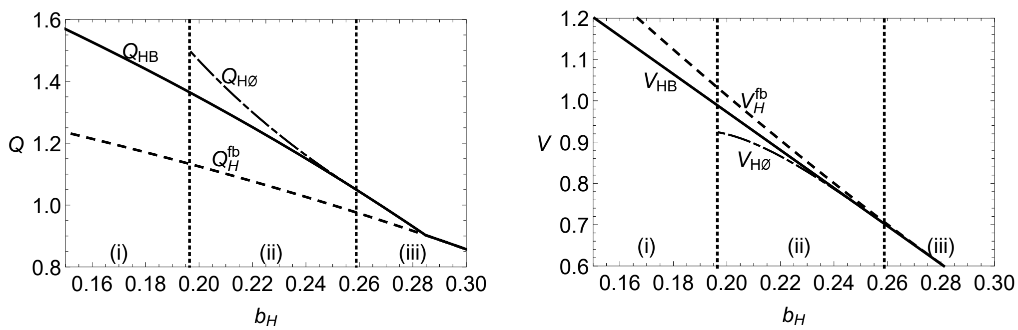
Theorem 1. Preference for the use of blockchain depends on the failure probability b_H as follows:

(i) If $0 \le b_H \le b^{\mathrm{se}}$, the high-quality firm prefers to use blockchain because in its absence it cannot separate itself from the low type.

(ii) If $b^{\mathrm{se}} < b_H < b^{\mathrm{cr}}$, the high-quality firm prefers to use blockchain because it allows separation from the low type at a lower cost, i.e., $\mathcal{C}_{\mathrm{B}} < \mathcal{C}_{\varnothing}$.

(iii) If $b^{\mathrm{cr}} \le b_H$, the high-quality firm is indifferent regarding the use of blockchain, i.e., $\mathcal{C}_{\mathrm{B}} = \mathcal{C}_{\varnothing}$.

These three regimes are illustrated in Figure 1. Whether the high type can separate and, if so, at what cost, depends, among others, on how strongly the low type is willing to imitate. The low type's incentive to imitate then depends on the benefit of being perceived as the high type, which in turn depends on the high type's failure probability, b_H.



(a) Order quantities. (b) Firm values.

Figure 1: First-best outcomes (dashed line); outcomes without blockchain (dot-dashed line); outcomes with blockchain (solid line) for the high type under $a_L = 5.1, a_H = 6, c = 3, b_L = 0.4$.

(i) When b_H is small, the low type is so eager to imitate that, in a cash signaling game, it is willing to overborrow all the way up to the high type's investment cap. This makes it impossible for the high type to separate because borrowing beyond this cap is a cheap talk. In contrast, overordering illiquid inventory is never a cheap talk and inventory signaling thus always allows separation. Therefore, the benefit of blockchain adoption for a firm of "very high" quality is that it makes separation possible.

(ii) When b_H is moderate, both inventory signaling and cash signaling allow the high type to separate. However, because the low type finds it costlier to overorder inventory than to overborrow an equivalent amount of cash, the high type is able to separate with a relatively smaller inventory distortion. Importantly, unlike the low type, the high type finds it always optimal to invest all cash in inventory, and is therefore indifferent between overborrowing cash and overordering the equivalent amount of inventory. As a result, the high type always prefers a smaller inventory distortion to a larger credit distortion. To put it differently, the high type prefers signaling with inventory because it has a comparative advantage in monetizing inventory. The benefit of blockchain adoption for a firm of "moderately high" quality is thus a smaller signaling cost.

(iii) When b_H is large, both inventory and cash signaling allow the high type to separate at the same signaling costs. In this regime, the low type's incentive to imitate is so low, that in a cash signaling game, it is not willing to borrow more than it is willing to invest in inventory. Overborrowing cash and overordering inventory is thus equally costly even for the low type, and there is no difference between cash signaling and inventory signaling. Thus, a firm of "somewhat high" quality does not benefit from blockchain adoption in the context of signaling to lenders.

In more informal terms, the main message of Theorem 1 can be summed up as follows.

Main result. *The transaction verifiability afforded by blockchain technology enables firms to convey private information about operational capabilities to lenders more efficiently.*

Perhaps somewhat counterintuitively, preference for one signaling mechanism or the other cannot be explained by the mere observation that overordering is costlier than overborrowing. To shed more light on this point, let us consider a generic signaling game in which two signaling mechanisms are available, and one incurs higher unit distortion costs than the other.

Example 1. A firm of type $i \in \{H, L\}$ generates revenue 2 if identified as H, and 1 otherwise. Type i can signal either by taking action $A \geq 0$ at a cost $a_i \times A$, or by taking action $B \geq 0$ at a cost $b_i \times B$, where cost parameters (a_H, a_L, b_H, b_L) are nonnegative and bounded. Signaling through action A is costlier, that is $a_i > b_i$, $\forall i$. Signaling is costlier for the low type, that is $a_H < a_L$ and $b_H < b_L$.[12]

To explore whether either of the two actions—the cheaper or the costlier—tends to be preferred in equilibrium, consider sampling cost parameter values uniformly at random from their feasible sets. Let $\mathbb{A}$ (resp. $\mathbb{B}$) be the set of cost parameter values for which the strictly preferred separating mechanism is signaling through action A (resp. B). Then, the frequency at which action A (resp. B) is preferred is proportional to the "volume" of the set $\mathbb{A}$ (resp. $\mathbb{B}$), which we can quantify using the Lebesgue measure, denoted here with μ.

Lemma 1. In Example 1, the cheaper action B is preferred more often, in particular with frequency

$$\frac{\mu(\mathbb{B})}{\mu(\mathbb{A}) + \mu(\mathbb{B})} = \frac{3}{4}.$$

According to Lemma 1, 75% of the time it is the cheaper action B, and 25% of the time the costlier action A, that is preferred in equilibrium in this generic signaling game.

[12]The assumption of signaling costs being linear and higher for the low type follows Spence (1973).

What the above example illustrates is that the observation of one signaling action being costlier fails to determine on its own whether or not that action is preferred in equilibrium. To develop more intuition about this, let us revert back to our model. The high type's total signaling cost, $\mathcal{C}_j$, in the two signaling games, $j \in \{\text{Ƀ}, \varnothing\}$, can be, loosely speaking, expressed as follows.

Cash signaling

low unit cost of imitating $\Rightarrow$ requires a larger distortion to separate $\Rightarrow$

$$\mathcal{C}_\varnothing = \text{large distortion} \times \text{low unit cost of signaling.}$$

Inventory signaling

high unit cost of imitating $\Rightarrow$ requires a smaller distortion to separate $\Rightarrow$

$$\mathcal{C}_{\text{Ƀ}} = \text{small distortion} \times \text{high unit cost of signaling.}$$

Therefore, to deduce whether inventory or cash signaling is preferable, the high type needs to consider the tradeoff between its own higher (resp. lower) unit signaling costs and a smaller (resp. larger) distortion resulting from the low type's higher (resp. lower) unit signaling costs under inventory (resp. cash) signaling. An important driver of how this tradeoff is resolved is the relation between the cost premia of inventory signaling for the two types.

To provide more intuition about why inventory signaling weakly dominates cash signaling, consider first the per dollar unit signaling costs. To ease exposition, let $c = 1$ without loss of generality, so that a unit of inventory costs one dollar. Figure 2 characterizes how the unit cost of overordering, $S_{i\text{Ƀ}}(Q) := -\frac{d}{dQ}V_{i\text{Ƀ}}(Q)$, relates to that of overborrowing, $S_{i\varnothing}(D) := -\frac{d}{dD}V_{i\varnothing}(D)$, for type i, in different regions, which are labeled following Theorem 1. In region (iii), the distortion is low enough so that both types invest the entire borrowing into inventory and, thus, overborrowing and overordering are equally costly for both types. In region (ii), the distortion is moderate yet exceeds the low type's investment cap, $\overline{D}_L$, and therefore the low type no longer invests the entire borrowing into inventory, which makes its overborrowing unit cost lower than its overordering unit cost. In region (i), the distortion is high enough to exceed even the high type's investment cap, $\overline{D}_H$, and any additional overborrowing becomes cheap talk, i.e., costless for both types.

To separate, the high type overorders (overborrows) up to the low type's respective indifference point, which we denoted by $c\,q$ (d). If the indifference points are "low" (region (iii)), the low type is willing to overorder or overborrow up to the same amount, because the two actions are equally costly. Facing equal distortions and equal unit costs, the high type is indifferent between the two signaling modes. If the indifference points are "moderate" (region (ii)), the low type faces lower overborrowing costs and is therefore willing to overborrow by a larger amount. Facing a larger

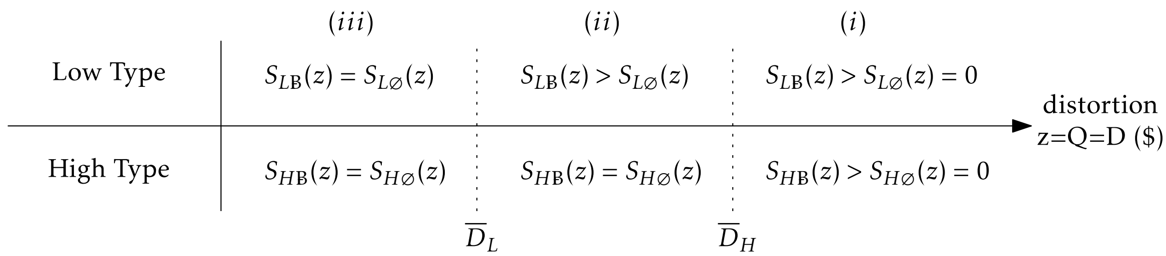


Figure 2: The relationship between per dollar overborrowing and overordering costs for the two types as a function of the distortion, whereby c is normalized to 1.

overborrowing distortion and equal unit costs, the high type then strictly prefers to overorder. Finally, if the indifference points are "high" (region (i)), overborrowing becomes costless and can no longer provide separation, so the high type can only separate by overordering.

Another salient point of our analysis is that *strict* preference for inventory signaling, which could ultimately drive blockchain adoption, relies on the high type, i.e., the less risky firm, to also have a comparative advantage in processing inventory, i.e., $\alpha_H > \alpha_L$. This becomes most apparent if we consider a situation in which $\alpha_L > \alpha_H$, i.e., the riskier firm can process inventory more profitably, conditional on success. In this case, signaling by overordering inventory not only loses its edge, but it becomes impossible, as formalized in the next proposition.

Proposition 4. When $\alpha_H < \alpha_L$ with all other elements of our model remaining intact, no separating equilibrium exists under inventory signaling.

This result further highlights the fact that superiority of inventory signaling is not universal, and it does not follow automatically from overordering being a stronger commitment than overborrowing. Surely enough, it is possible that in this setting, a SE exists where the high type signals by underordering.[13] Even if this is the case, however, there is no difference between inventory signaling and cash signaling. The reason is that whenever a firm borrows below the first best, the lender knows that the firm will spend the entire borrowing on inventory, and operational transparency thus becomes irrelevant.

This result has important implications for blockchain adoption. The advantage of operational transparency established as our main result exists only when the less risky firm can process inventory more profitably conditional on success. As we remarked earlier, this could be the case when a higher probability of success as well as a larger market size or a lower production cost (both of which correspond to a larger α_H) result from superior management or operations capabilities. However,

[13]Such an equilibrium would also require an alternative belief structure whereby the lender associates a low order with the high type.

the reverse could be also true. For example, the low type could have a more efficient technology, but one that is more prone to failure, or it could face a potentially larger, but more uncertain demand. In such cases, the low type would earn a higher net revenue on each unit produced conditional on success, resulting in $\alpha_L > \alpha_H$. According to Proposition 4, the advantage of inventory signaling and preference for blockchain adoption in all these cases fade. In what follows, we revert back to our base-case model with $\alpha_H > \alpha_L$.

4.5 Sensitivity Analysis

In this section, we discuss how the characteristics of a high-quality firm affect its preference for the signaling mode and thus for blockchain adoption.

Failure probability b_H

It follows directly from Theorem 1 that as the high type's failure probability increases, its preference for blockchain adoption fades. Intuitively, as the high type becomes less creditworthy, the low type's incentive to imitate weakens, and it becomes easier for the high type to separate even absent operational transparency.

Demand curve intercept α_H

Recall that a larger α_H can capture a larger market size as well as lower operating cost of the high type. To understand the effect of α_H, we can reformulate Theorem 1 so as to link the equilibrium outcome to the value of this parameter. To that end, we define two thresholds:

$$\alpha^{\text{se}} := \frac{2(1-b_L)\,b_L\alpha_L(1-b_H) + c\left(2+b_L^2-2b_L\right)b_H - c\left(2b_L-b_L^2\right)}{2b_H(1-b_L)^2}, \text{ and} \tag{21}$$

$$\alpha^{\text{cr}} := \left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right)\frac{1-b_H}{1-b_L}\frac{b_L}{b_H} + \frac{c}{1-b_H}. \tag{22}$$

It is straightforward to show that $\alpha^{\text{se}} < \alpha^{\text{cr}}$. Noting that threshold $b^{\varnothing}$ is independent of α_H, we can write the following corollary to Theorem 1.

Corollary 1. If $b_H \geq b^{\varnothing}$, the high-quality firm is indifferent regarding the use of blockchain, i.e., $\mathcal{C}_{\text{B}} = \mathcal{C}_{\varnothing}$, for any α_H. Otherwise, preference for the use of blockchain depends on α_H as follows:

(i) If $\alpha_H \leq \alpha^{\text{se}}$, the high-quality firm prefers to use blockchain because in its absence it cannot separate itself from the low type.

(ii) If $\alpha^{\text{se}} < \alpha_H < \alpha^{\text{cr}}$, the high-quality firm prefers to use blockchain because it allows separation from the low type at a lower cost, i.e., $\mathcal{C}_{\text{B}} < \mathcal{C}_{\varnothing}$.

(iii) If $\alpha_H \geq \alpha^{\text{cr}}$, the high-quality firm is indifferent regarding the use of blockchain, i.e., $\mathcal{C}_{\text{B}} = \mathcal{C}_{\varnothing}$.

According to the corollary, the high-type's preference for blockchain is negatively related to α_H. As α_H becomes larger, i.e., as the high type's market size increases or its operating costs decrease, its first-best input order as well as loan request increase. Thus, it becomes more difficult for the low type to imitate, which makes it easier for the high type to separate even absent operational transparency.

Salvage value

Finally, recall our assumption that input inventory is perishable or illiquid (e.g., due to its customization) and thus has no salvage value. In the next corollary, we consider the other extreme case, in which the input goods can be resold for the full procurement cost.

Corollary 2. If the input inventory can be salvaged without a loss, there is no difference between cash signaling and inventory signaling and, therefore, preference for the use of blockchain vanishes.

If the firm can resell input inventory and recover its full procurement cost, buying inventory is cheap talk and operational transparency makes no difference from a signaling perspective.

4.6 Cost of Operational Transparency

In practice, operational transparency comes at some monitoring cost, which can be both fixed and/or proportional to the transaction quantity. Committing transactions to a blockchain ledger, for example, typically incurs fixed transaction costs. In addition, not every lender may be willing to use the technology, which may force the firm to borrow from a boutique lender who requires a higher return on capital and thus offers less competitive rates. Traditional means of achieving operational transparency are also costly. For example, the use of trade credit means borrowing from a supplier who is likely to face a higher cost of capital than a bank. Issuing a letter of credit typically incurs a fixed cost and a percentage fee.

We now relax the assumption of zero monitoring costs. To this end, suppose that there is a fixed cost Φ per transaction, as well as a variable cost ϕ per dollar of inventory financed. When either of the two costs is high enough, inventory signaling is not a viable option regardless of firm characteristics. To focus on the more interesting scenario, in which the choice between the two signaling modes is more subtle and depends on firm parameters, we impose upper bounds on Φ and ϕ. Namely, we assume

$$\Phi < (1-b_H)\left(r(\overline{D}_H) - \frac{b_H+\phi}{1-b_H}\overline{D}_H\right) \text{ and} \tag{23}$$

$$\Phi < \frac{1-b_H}{4}\left(\alpha_H - \frac{c(1+\phi)}{1-b_H}\right)^2 - \frac{1-b_H}{4}\left(\alpha_H - \frac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)^2, \tag{24}$$

where $r(\ )$ is the fair interest charged by a lender who cannot distinguish between the two types in the absence of blockchain, and it is given in (91). Note that when $\phi = \Phi = 0$, condition (23) simplifies into our initial assumption (2), whereas condition (24) is satisfied trivially. In general, both conditions are satisfied when ϕ and Φ are not too high. Technically speaking, these two conditions rule out pooling equilibria by making inventory signaling a preferable alternative in case cash signaling does not allow separation.[14]

The next proposition characterizes preference for blockchain adoption in the presence of monitoring costs.

Proposition 5. When blockchain technology is costly, preference for adoption depends on the failure probability b_H as follows:

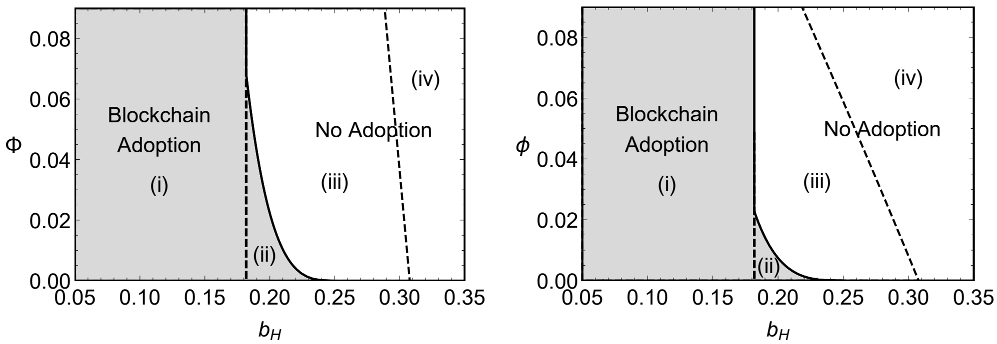
(i) If $0 \leq b_H \leq b^{\text{se}}$, the high-quality firm strictly prefers inventory signaling, and thus strictly prefers to use blockchain.

(ii) If $b^{\text{se}} < b_H < b^{\text{cr}}$, the high-quality firm strictly prefers inventory signaling, and thus strictly prefers to use blockchain, if, and only if, the fixed and variable costs, Φ and ϕ, are sufficiently low.

(iii) If $b^{\text{cr}} \leq b_H$, the high-quality firm strictly prefers cash signaling, and thus strictly prefers not to use blockchain.

When b_H is low, the high type prefers to use blockchain because cash signaling does not allow separation. When b_H is high, the high type strictly prefers not to adopt blockchain because cash signaling is net cheaper. When b_H is moderate, there is a benefit to inventory signaling, but cash signaling is possible and, therefore, the high type prefers to use blockchain as long as it is not too costly.

[14] More precisely, condition (23) ensures that for any given loan amount $D \in [\overline{D}_L, \overline{D}_H]$ the high-quality firm's payoff when identified as a high type with blockchain exceeds its payoff under pooling without blockchain. Condition (24) ensures that the high-quality firm's first-best payoff with blockchain exceeds its best possible payoff under pooling when borrowing $D \in [0, \overline{D}_L]$ without blockchain.



(a) Fixed costs (Φ) (b) Variable costs (ϕ)

Figure 3: Adoption of blockchain technology as a function of costs. Parameters: $\alpha_H = 6, \alpha_L = 5, c = 3, b_L = 0.4, h = 0.25$.

This is illustrated in Figure 3, which depicts the high type's preference for blockchain adoption as a function of its failure probability b_H and the cost of using blockchain: fixed cost Φ in panel (a) and variable cost ϕ in panel (b). Each panel shows the three regimes (i)-(iii) described by Proposition 5. When b_H is low (high), the high type prefers to adopt (not to adopt) regardless of the cost because cash signaling does not allow separation (inventory signaling has no benefit). When b_H is moderate, the high type prefers to adopt as long as the cost is not too high. Finally, region (iv) corresponds to the parameter values, which violate our assumptions (23)–(24), or assumption (2) if $\phi = \Phi = 0$, in which case the high type prefers not to signal, let alone to adopt blockchain.

4.7 General Belief Structure

Up to now, we assumed that suppliers' beliefs about their buyers' types were threshold-based. Next, we show that even if one starts with a general belief structure, all of our results remain intact. Suppose that in the cash lending game, a lender, upon observing a loan request D, forms a belief

$$\beta_\varnothing(D) := \begin{cases} H & \text{if } D \in \mathcal{H}_\varnothing, \\ L & \text{o/w}, \end{cases} \tag{25}$$

where $\mathcal{H}_\varnothing \subset \mathbb{R}$ is an arbitrary set, to which we shall refer as belief set. An analogous belief structure is also adopted for the inventory signaling game. All other elements of our model remain the same.

Proposition 6. The LCSE existence, uniqueness, and actions of both types remain the same under a general belief structure.

The intuition is as follows. For equilibrium to be *least-cost*, the high-type needs to signal with the *minimal* distortion possible, which is determined uniquely by how far the low type is willing to go imitating. To make sure that the low type does not imitate, any action below this critical point needs to be associated with "low" belief, whether we impose a threshold belief structure or not. At the same time, the belief associated with actions above this critical point is irrelevant because neither type will choose it, even if it means being perceived "high." Thus, imposing a threshold belief structure that requires the belief to be "low" ("high") below (above) the critical point, has no effect on the equilibrium outcome.

5 Insights and Predictions

Opening a small window of transparency into a firm's operations, in particular, its input transactions, could go a long way to alleviate the difficulty of financing operations, which is a systemic problem for SMEs, that is all the more severe in developing economies. As we demonstrate in the next section, blockchain technology could provide an efficient way to accomplish this by furnishing input transaction verifiability in supply chains in a way that is accessible to SMEs. The potential benefits are vast and global in scale. Although the SME sector represents the backbone of many of the world economies, accounts for over half of jobs and over a third of GDP worldwide, the World Bank estimates that its global financing shortfall tops $2.6 trillion (Alibhai, Bell and Conner 2017). Notably, the emergence of trading platforms, such as Amazon and Alibaba, has provided one possible solution to the SMEs' struggles: being able to observe virtually all business transactions of participants, these platforms have very recently started to provide cheap loans through their financing arms—Amazon Lending and Ant Financial. Unfortunately, these benefits are confined to members of such closed systems. The use of publicly available blockchain platforms, in contrast, has the potential to redefine global supply chain operations by democratizing operational transparency.

By comparing signaling costs in the presence and absence of blockchain, our analysis also provides a way to quantify the benefits that this technology affords to potential adopters. These benefits can then be weighed against the practical costs of adoption, so that firms can make a more informed strategic decision about implementation.

Our analysis also sheds light onto what types of supply chains would profit the most from blockchain adoption and what specific benefits this would provide.

Prediction 1. Propensity to adopt blockchain is positively related to the firm's creditworthiness.

This prediction follows from Proposition 3, according to which only high-quality firms adopt blockchain in equilibrium, and Theorem 1, according to which preference for adoption increases with the firm's success probability. Note that our model assumes that a firm's creditworthiness (success probability) is not observable to outsiders. Therefore, to test this prediction, one would need to measure creditworthiness by the ex-post default rate while controlling for risk factors observable ex ante, such as firm age, size, profitability, leverage, etc.

Prediction 2. Propensity to adopt blockchain by a high-quality firm is (a) negatively related to the firm's market size, and (b) positively related to the firm's operating costs.

The result follows from Corollary 1, according to which the high-type's preference for blockchain adoption is negatively related to α_H, which can relate to the firm's market size as well as its operating costs. Importantly, this negative relation is true only conditional on the firm being of a high type. Thus, we expect the relation to hold empirically only within a sample of relatively creditworthy firms.

Prediction 3. Propensity to adopt blockchain is (a) positively related to perishability of the firm's inputs, and (b) negatively related to liquidity of the firm's inputs.

As stipulated in Corollary 2, the benefit of operational transparency disappears if input inventory can be converted to cash without a loss. In general, as the salvage value of inventory increases, overordering becomes a weaker signal, and the benefit of operational transparency afforded by blockchain fades. Therefore, the blockchain benefits are expected to be greater when the firm sources perishable or illiquid (e.g., unique or customized) inputs.

Prediction 4. Propensity to adopt blockchain is positively related to the degree of information asymmetry that the firm is subject to.

This prediction follows directly from the fact that the benefit of blockchain identified in our model exists only in the presence of information asymmetry between borrowers and lenders (compare the results in Sections 4.1 and 4.4). Therefore, we expect the technology to be more prevalent in supply chains that are innovation-intensive, dominated by smaller, privately-owned firms, and/or in which output is more differentiated across firms.

Prediction 5. Blockchain adoption decreases the cost of debt financing and operational distortions for high-quality firms.

This prediction follows from Theorem 1, according to which blockchain adoption allows high-quality firms to signal their quality to lenders in some cases, and it reduces signaling cost in others. In other words, blockchain enables high-quality firms to obtain external funds at the cost that reflects their true default risk, which would be either impossible or would require larger operational distortions otherwise. The second part of the prediction follows from the fact that blockchain adoption reduces excess ordering.

6 Porting Blockchain to Supply Chains: The b_verify System

The proposed benefit of inventory signaling is only tenable when firms' individual inventory transactions are verifiable by lenders at low enough costs. Our discussion in the introduction highlighted that blockchain represents a promising technology that could provide operational transparency more effectively than existing mechanisms. At the same time, it became clear that potential obstacles also exist that could limit its relevance to supply chain implementation and could increase operational costs. How exactly these obstacles could be overcome in practice is an important and non-trivial question. To make some headway, we launched a comprehensive project resulting in the development of a blockchain system termed `b_verify`, for an intended use case in agricultural supply chains. The system was developed by an interdisciplinary team of experts in computer science, engineering and business, in collaboration with the MIT Media Lab Digital Currency Initiative (DCI) and with the support of Inter-American Development Bank (IDB). In this section, we give an overview of the system, discussing several of its innovative features and illustrating how they could help alleviate the aforementioned adoption obstacles.

Overview

We designed `b_verify` to be a low-cost open-source software/hardware system, whose main objective is to enable a network of firms and their lenders, to securely record and verify physical transactions on an immutable distributed ledger, in the absence of mutual trust. To make the technology accessible to SMEs and startups in developing economies, implementation and operating costs are kept low via a "hybrid" design approach, whereby the system leverages some of the existing low-cost advantages of permissionless public blockchains (infrastructure, security, immutability), while also implementing novel solutions to preserve other desirable properties often associated with more expensive private blockchain implementations, such as permissioning and privacy.

In particular, `b_verify` stores transaction data on the public Bitcoin ledger. Importantly, the transactions are processed by a low-cost disposable and "un-trusted" server, that uses a cryptographic data structure to allow for public commitments to the ledger. The first core innovation here is that server and data processing protocols leverage the security guarantees provided by the Bitcoin blockchain—specifically non-equivocation[15]—to create a partially ordered, timestamped

[15] Equivocation is a concept from Computer Science that refers to a situation in which an entity is able to make inconsistent statements to different parties. For example, the server could simply leave out or hide a record of a transaction from a specific entity. Put another way, non-equivocation requires that all parties see the same set of

record of transactions that can be verified by interested parties.

Barring the technical details, which are left for Appendix A, the end result is a protocol in which a user's device can present a cryptographic proof that a set of records is complete and authentic. The second core innovation is that the protocol requires only a short "signature" or "hash-key" of the transaction data to be committed to the public ledger, therefore lowering bandwidth-related costs, while providing privacy. That is, parties need to verify only a subset of the ledger that pertains to a specific user or type of asset. We provide more details further below.

Agriculture Warehouse Implementation

To showcase the features of the system, we will focus on a particular use case: that of warehouse receipts in agricultural supply chains. The choice of the use case was informed by our collaborations and field visits with the Mexican and Ukrainian governments, which have identified this area as a priority where the technology has the potential to make meaningful and immediate impact. Furthermore, as discussed in the introduction, warehouses often play a central role in supply chains (Trichakis, Tsoukalas and Moloney 2015), and, therefore, installing `b_verify` at this nexus of stakeholder interaction affords multiple benefits. Specifically, `b_verify` is capable of recording multiple transactions, including in- and outshipments of goods, pledging goods as collateral for secured loans, and transferring collateral ownership to lenders upon default. Critically, `b_verify` can provide to an outside entity, such as a lender, access to a complete record of a firm's transactions with the warehouse, along with a cryptographic proof that these records are authentic and that no record has been omitted.

Figures 4 and 5 provide a schematic overview that exemplifies a warehouse implementation. In Figure 4, a farmer deposits or withdraws produce from a warehouse. The produce is weighed by a warehouse employee, optionally, using a digital IoT scale. Using the `b_verify` protocol, the farmer, the warehouse employee, and the IoT digital scale, all sign the transaction using their private keys, to the globally distributed Bitcoin blockchain, an event represented by box 1 in the figure. The `b_verify` protocol verifies the consistency of all the information submitted by the different public keys and if successful, registers the transaction. The transaction is then permanently and immutably registered on the blockchain. The transaction could then be subsequently costlessly and immediately accessed by an affiliated bank system, e.g., for loan underwriting purposes, an event represented by the dotted line in Figure 5. Loan issuance could then also be signed to the blockchain, an event represented by box 2 in Figure 5.

records. This means that the server cannot "lie" to one party without having to "lie" to everyone.

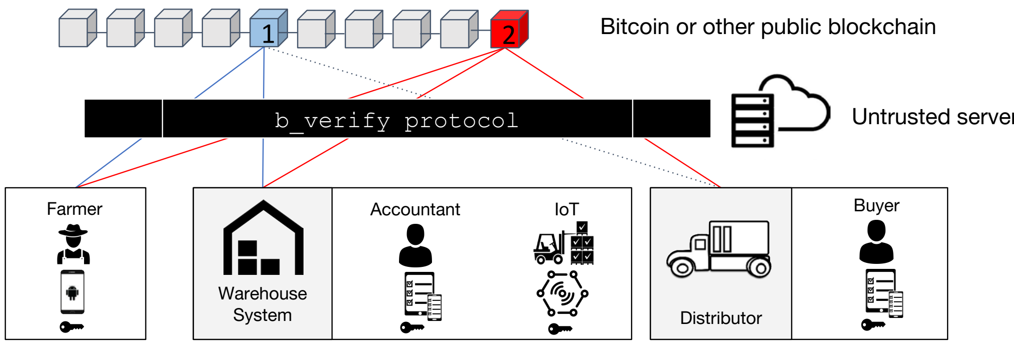


Figure 4: Deposit and sale of goods. A farmer and warehouse system use `b_verify` to sign a transaction to the globally distributed Bitcoin blockchain. Legend: Box labeled 1: Deposit goods (owner and warehouse sign commitment to a public blockchain). Box labeled 2: Transfer ownership (buyer authenticates, owner and warehouse updates commitment).

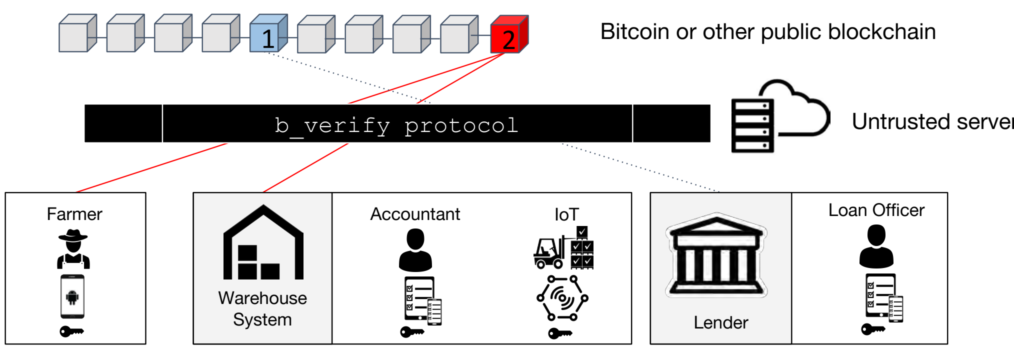


Figure 5: Using `b_verify`, a bank can verify previous data entries and sign new transactions (e.g., loan terms) with the farmer. Legend: Box labeled 1: Bank authenticates record via blockchain query Lien is placed on pledged assets (owner and warehouse update commitment). Box labeled 2: Opportunities for "smart contract" enforcement of terms.

Technical Innovations & Features

We discuss below several key innovative features of the system that were made to overcome the barriers to entry for SMEs wanting to adopt blockchain technology for operational transparency.

Verification of physical transactions. As mentioned, Blockchain technology was originally developed in the context of the Bitcoin currency, involving merely digital transactions. Its main technological feature has been its ability to provide individual transaction verifiability. How exactly this technology has to be adapted to provide verifiability of physical goods transactions, such as procuring inventory, is currently an open question that is actively being pursued by practitioners (e.g., see IBM TrustChain 2017).

In providing verifiability, there could be many differentiating factors between digital and physical goods transactions. In our view, the paramount factor, which `b_verify` addresses, is that operational transactions in supply chains involve a certain amount of human intervention or manual entries and, therefore, are more susceptible to mistakes or deliberate misrepresentation. In an agricultural supply chain, for example, transactions involving commodities usually require warehouse employees to weigh physical goods to verify the quantity traded. In addition, lab employees use various tools, including advanced electronic devices, to assess quality variables such as moisture, oil levels, and protein content. In this process, an employee could mishandle (by accident or not) the incoming inventory shipment and misrepresent the quantity received or its quality. These types of issues undermine verifiability and could negate any of the potential advantages of implementing the technology in the first place.

To mitigate this issue, `b_verify` solicits independent attestations from multiple clients before permanently committing a transaction to the blockchain. Clients, who could be people or Internet-connected devices, cryptographically sign and attest to the details of the transaction. In the warehousing implementation, for instance, the IoT digital scale has a direct feed to the `b_verify` system, and the transaction is committed only if the information input to the server by all three parties (warehouse employee, depositor and the digital device) is consistent. Importantly, as we mentioned earlier, the cloud server need not be trusted because public key cryptography and authenticated data structures ensure the server cannot manipulate data, whether by its own accord or via external cyber attack on the server. Once the system verifies the consistency of all the attestations, it encrypts the data and commits it to the public bitcoin blockchain where it is immutably stored to provide a permanent audit chain.[16] These two factors, multiplicity of attestations and

[16] The immutability property is only as strong as the public blockchain in question. We have used the bitcoin

immutability, arguably may not always suffice to fully alleviate fraudulent behavior, but they do mitigate it compared to the status quo.

Privacy and permissioning. Two key issues that arise when public ledgers are used to store private data, are 1) to be able to identify the parties involved and 2) to ensure that the stored data is encrypted in such a way that only permissioned parties are able to recover it. To deal with the first issue, `b_verify` requires a public key infrastructure to identify participants and verify their signatures. Regarding the second issue, it is important to recognize that blockchains require data to be shared among a set of participants. In the context of a supply chain this could represent a problem because firms have a strong incentive to guard proprietary data and prevent it from falling into the hands of competitors. In the agriculture sector that `b_verify` targets transaction records are often required by law to be public so this need not always be an issue. More generally this problem can be addressed at a technological level by using encryption to selectively hide or obfuscate data, or by committing to the ledger only a "hash signature" of the information—something that `b_verify` accomplishes using so-called Merkle Prefix Trie data structures (see Appendix A). Privacy is a major concern in practice and is currently an area of active research and development.

Hardware requirements. The main hardware requirements of the `b_verify` system are fairly limited, in that the application itself can be launched from a basic smartphone and/or a tablet, and only a basic server is required to do the data processing and encryption, before it is committed to the public ledger. In particular, neither of these devices is required to have state of the art storage or processing capabilities. Recognizing that SMEs often have limited hardware computing resources, we designed `b_verify` so that it can accommodate "thin clients" that are not required to download the entire Bitcoin blockchain to participate,[17] providing an easy "plug-and-play" experience for users to facilitate adoption on the ground. To this end, we are also building a `b_verify` pilot kit tailored to the agricultural warehouse use cases outlined above. The pilot kit has a modular design and consists of a physical box of cell phones, tablets, and computers, all with preloaded software packages servicing the `b_verify` protocol, as well as reference implementation in English, Spanish, and other languages. The only other pieces of hardware required relate to the digital IoT devices, such as the digital scale, but such devices can be skipped (at the cost of increased probability of

blockchain because it is one of the most robust blockchains in terms of proven immutability properties.

[17]This is important because it means that clients can fully participate without having to download the entire Bitcoin blockchain that is currently (as of June 2018) over 163 gigabytes long. This is crucial requirement to provide support for users who only have access to a cell-phone

fraud), and in many instances, such devices happen to already be in place.

Implementation and Operating Costs. On the one hand, one of the advantages of utilizing a public ledger to store data, such as the one provided by the Bitcoin blockchain, is that there are virtually no infrastructure implementation costs, as discussed in the previous paragraph. The immutability of the data is then ensured by the Proof of Work system that Bitcoin already has in place. In other words, `b_verify` "piggy backs" on the infrastructure already in place, and the security guarantees that it provides. On the other hand, transacting on the public ledger involves transaction costs. For the bitcoin ledger, these costs are generally low, typically, less than $1 per transaction as of June 2018. However, historically, these costs have experienced volatility at times when the network is over congested, reaching for instance around $50 per transaction, at their worst point. We expect such issues to become less problematic going forward as new technological innovations such as "proof of stake," "sharding" and side-chains (such as the lightning network) go live and increase network throughput. Nonetheless, to mitigate this potential issue, the `b_verify` system was designed to be robust to different ledgers, so that it can be ported to alternative public ledgers with lower transaction costs if needed, with relatively few modifications.

References

Acemoglu, D, Kimon Drakopoulos, and A Ozdaglar. 2017. "Information obfuscation in a game of strategic experimentation." *Working Paper.*

Akkaya, Duygu, Kostas Bimpikis, and Hau Lee. 2016. "Agricultural supply chains under government interventions." Working Paper 3 (3).

Alibhai, S, S Bell, and G Conner. 2017. "What's Happening in the Missing Middle? Lessons from financing SMEs." *World Bank.*

Babich, V, and G Hilary. 2018. "What Operations Management Researchers Should Know About Blockchain Technology." Georgetown University Working Paper.

Babich, V, and MJ Sobel. 2004. "Pre-IPO Operational and Financial Decisions." *Management Science*, 50(7): 935–948.

Bebchuk, LA, and LA Stole. 1993. "Do short term objectives lead to under or overinvestment in long term projects?" *Journal of Finance*, 48(2): 719–730.

Besanko, D, and AV Thakor. 1987. "Competitive equilibrium in the credit market under asymmetric information." *Journal of Economic Theory*, 42(1): 167 – 182.

Biais, B, and C Gollier. 1997. "Trade credit and credit rationing." *Review of Financial Studies*, 10(4): 903–937.

Biais, B, C Bisiere, M Bouvard, and C Casamatta. 2017. "The Blockchain Folk Theorem." *Toulouse School of Economics, TSE-817 Working Paper.*

Bimpikis, K, Kimon Drakopoulos, and S Ehsani. 2017. "Disclosing Information in Strategic Experimentation." *Working Paper.*

Boyabatlı, Onur, and L Beril Toktay. 2011. "Stochastic capacity investment and flexible vs. dedicated technology choice in imperfect capital markets." *Management Science*, 57(12): 2163–2179.

Boyabatlı, Onur, Paul R Kleindorfer, and Stephen R Koontz. 2011. "Integrating long-term and short-term contracting in beef supply chains." *Management Science*, 57(10): 1771–1787.

Budish, E. 2018. "The Economic Limits of Bitcoin and the Blockchain." Working Paper.

Burkart, M, and T Ellingsen. 2004. "In-kind finance: A theory of trade credit." *American Economic Review*, 94(3): 569–590.

Buzacott, AJ, and QR Zhang. 2004. "Inventory management with asset-based financing." *Management Science*, 50(9): 1274–1292.

Cachon, G, and M Lariviere. 2001. "Contracting to assure supply: How to share demand forecasts in a supply chain." *Management Science*, 47(5): 629–646.

Calmon, Andre P, Sameer Hasija, and K Sudhir. 2017. "Increasing the Quality of Agricultural Produce in Developing Countries." *Working Paper.*

Candogan, Ozan, and Kimon Drakopoulos. 2017. "Optimal Signaling of Content Accuracy: Engagement vs. Misinformation." *Working Paper.*

Catalini, C, and JS Gans. 2017. "Some simple economics of the blockchain." *MIT Sloan Research Paper No. 5191-16.*

Chakraborty, Soudipta, and Robert Swinney. 2017. "Signaling to the Crowd: Private Quality Information and Rewards-Based Crowdfunding." *Working Paper.*

Chick, Stephen E, Sameer Hasija, and Javad Nasiry. 2016. "Information elicitation and influenza vaccine production." *Operations Research*, 65(1): 75–96.

Chod, J. 2016. "Inventory, Risk Shifting, and Trade Credit." *Management Science.*

Chod, J, and E Lyandres. 2018. "A Theory of ICOs: Diversification, Agency, and Information Asymmetry." Boston College Working Paper.

Chod, J, N Trichakis, and G Tsoukalas. 2018. "Supplier diversification under buyer risk." *Management Science forthcoming.*

Cho, IK, and M Kreps. 1987. "Signaling games and stable equilibria." *Quarterly Journal of Economics*, 102(2): 179–221.

Diamond, DW. 1991. "Monitoring and reputation: The choice between bank loans and directly placed debt." *Journal of political Economy*, 99(4): 689–721.

Ding, Qing, Lingxiu Dong, and Panos Kouvelis. 2007. "On the integration of production and financial hedging decisions in global markets." *Operations Research*, 55(3): 470–489.

Duan, J-C, and SH Yoon. 1993. "Loan commitments, investment decisions and the signalling equilibrium." *Journal of Banking & Finance*, 17(4): 645 – 661.

Emery, GW. 1984. "A pure financial explanation for trade credit." *Quarterly Journal of Economics*, 19(3): 271–285.

Fabbri, D, and AMC Menichini. 2016. "The commitment problem of secured lending." *Journal of Financial Economics*, , (120): 561–584.

Falk, B, and G Tsoukalas. 2019. "Token-Weighted Crowdsourcing." *Working Paper.*

Gan, R, S Netessine, and G Tsoukalas. 2019. "Inventory, Speculation and ICOs." *Working Paper.*

Halaburda, H. 2018. "Blockchain Revolution without the Blockchain." New York University Working Paper.

Huberman, G, JD Leshno, and CC Moallemi. 2017. "Monopoly without a monopolist: An Economic Analysis of Bitcoin Payment System." *Columbia Business School Working Paper.*

Iancu, DA, N Trichakis, and G Tsoukalas. 2016. "Is operating flexibility harmful under debt?" *Management Science.*

IBM TrustChain. 2017. "Consortium of Jewelry Industry Leaders Announce TrustChain, First Global Blockchain Initiative to Bring Full Transparency to Consumers." http://newsroom.ibm.com/announcements?item=122899.

Jain, N. 2001. "Monitoring costs and trade credit." *Quarterly Review of Economics and Finance*, 41: 89–110.

Kouvelis, P. 2012. *Handbook of Integrated Risk Management in Global Supply Chains.* New York:Wiley.

Lai, G, and W Xiao. 2018. "Inventory Decisions and Signals of Demand Uncertainty to Investors." *Manufacturing & Service Operations Management*, 20(1): 113—-129.

Lai, G, W Xiao, and J Yang. 2012. "Supply chain performance under market valuation: An operational approach to restore efficiency." *Management Science*, 57(2): 332–346.

Milde, Hellmuth, and John G. Riley. 1988. "Signaling in Credit Markets." *The Quarterly Journal of Economics*, 103(1): 101–129.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Working Paper.*

Özer, Özalp, and Wei Wei. 2006. "Strategic commitments for an optimal capacity decision under asymmetric forecast information." *Management Science*, 52(8): 1238–1257.

Özer, Özalp, Yanchong Zheng, and Yufei Ren. 2014. "Trust, trustworthiness, and information sharing in supply chains bridging China and the United States." *Management Science*, 60(10): 2435–2460.

Ross, Stephen A. 1977. "The Determination of Financial Structure: The Incentive-Signalling Approach." *The Bell Journal of Economics*, 8(1): 23–40.

Schmidt, W, V Gaur, R Lai, and A Raman. 2015. "Signaling to partially informed investors in the newsvendor model." *Prod. Oper. Manag.*, 24(3): 383–401.

Serhatli, Utku, Andre P Calmon, and Enver Yucesan. 2017. "Optimal Supply Planning for Commercial Seeds." *Working Paper.*

Spence, M. 1973. "Job Market Signaling." *Quarterly Journal of Economics*, 87(3): 355–374.

Stiglitz, JE, and A Weiss. 1981. "Credit Rationing in Market with Imperfect Information." *American Economic Review*, 71(3): 393–410.

Tang, Christopher S., S. Alex Yang, and Jing Wu. 2018. "Sourcing from suppliers with financial constraints and performance risk." *Manufacturing & Service Operations Management*, 20(1): 70–84.

Taylor, Bryan. Nov 23, 2013. "How The Salad Oil Swindle Of 1963 Nearly Crippled The NYSE." *Business Insider.*

Trichakis, N, G Tsoukalas, and E Moloney. 2015. "Credem: Banking on Cheese." *Harvard Business School Case 615-046.*

Xu, X, and JR Birge. 2004. "Joint production and financing decisions: Modeling and analysis." Working Paper.

Yermack, D. 2017. "Corporate governance and blockchains." *Review of Finance Forthcoming.*

Appendix

A Additional Technical Specifications for the `b_verify` System

Securing Receipts via Merkle Trees. In `b_verify` a warehouse receipt is a digital document that can be issued, transferred or redeemed. To perform these operations all parties involved (e.g. the warehouse & depositor) must consent by digitally signing ownership changes. Note that the use of digital signatures alone does not guarantee everyone will see the same owner for each receipt. For example a nefarious participant could transfer a receipt he owns and then try to redeem or loan the old receipt. To prevent this from happening the receipts in `b_verify` have associated cryptographic proofs which use commitments to the Bitcoin blockchain to guarantee that everyone will agree on who currently owns a receipt. `b_verify` constructs these proofs efficiently through the use of a central server, shown in Figure 6. However unlike in a typical client-server model, `b_verify` does not require clients to trust the server. Instead participants use cryptographic proofs to carefully update and verify receipt ownership.

Figure 7 illustrates this process. Receipt ownership is tracked using a forest of Merkle trees. Each user's "account" at a given warehouse is mapped to a Merkle tree that contains the receipts issued by the warehouse that are currently owned by the user. This set changes over time as individual receipts are issued, transferred or redeemed. Any updates to this tree require both the warehouse and the user to sign. The central server is only required to manage the roots (a 32-byte cryptographic digest) of each Merkle tree. It maintains a mapping from the account to the root using a data structure called a Merkle Prefix Trie (MPT). The server commits to this mapping by "witnessing" it to Bitcoin through broadcast of a Bitcoin transaction. Whenever the ownership record changes, some subset of the Merkle trees will change, resulting in new roots. The server will then update its data structures to reflect the changes and witness the new commitment to Bitcoin. Since clients do not trust the server, they require proofs from the server to ensure that the mapping was updated correctly. In `b_verify` the server can perform many updates simultaneously in a single transaction on the Bitcoin ledger to increase throughput and amortize transaction costs.

Users in `b_verify` participate by downloading a mobile "wallet" application. This application periodically syncs with the Bitcoin network and the central server. Hidden from the user, the application maintains the user's receipts along with the associated cryptographic proof. As the server broadcasts new commitments, the mobile application updates the proofs as needed. The proof of ownership of a receipt can then be sent to and verified by anyone using the `b_verify`

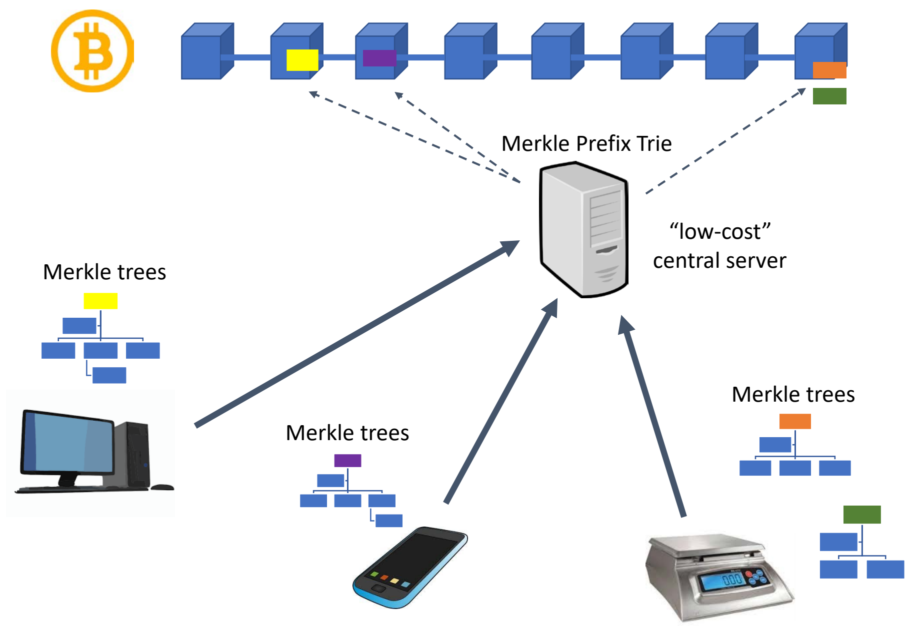


Figure 6: A basic low-cost "untrusted" server is used to pool transactions and encrypt the data before it is sent to the Bitcoin blockchain.

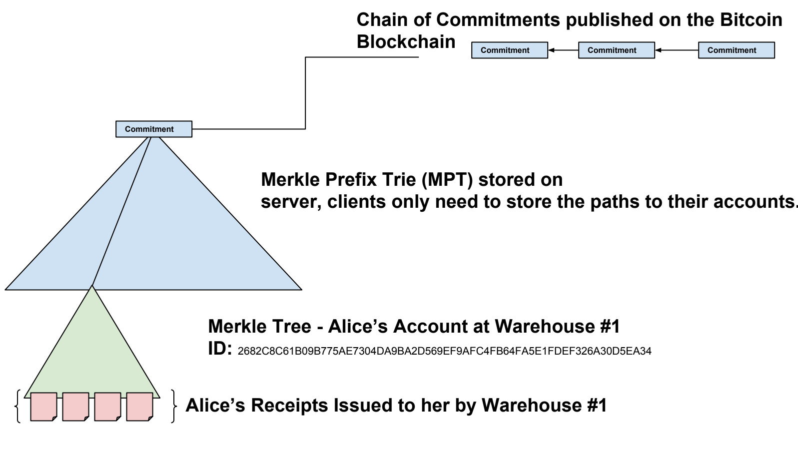


Figure 7: The `b_verify` Merkle Prefix Trie (MPT) structure

A path to a client's account in the server MPT.
This is stored by the client and is used in proofs.
The account ID is: 2682C8C61B09B775AE7304DA9BA2D569EF9AFC4FB64FA5E1FDEF326A30D5EA34
The value of the ADS Root is: 2682C8C61B09B775AE7304DA9BA2D569EF9AFC4FB64FA5E1FDEF326A30D5EA34


```
<MPTDictionaryPartial
+ <InteriorNode>
+0 <InteriorNode>
+00 <InteriorNode>
+000 <Stub Hash: 428F31D48A4D1B932BCE5F4A68137E33A984E32E226FD646D8CF311C931A39F6>
+001 <InteriorNode>
+0010 <InteriorNode>
+00100 <InteriorNode>
+001000 <Stub Hash: AB8A74D05434F255E6B61F7CEA411A2FE737F7DA6FED104D9A1D9AAE5FAFF161>
+001001 <InteriorNode>
+0010010 <Stub Hash: BAD14BAB54CE8168ED118211BBA5BD24F2D032CD3F248EBC754F3A25924E6219>
+0010011 <InteriorNode>
+00100110 <InteriorNode>
+001001100 <Stub Hash: D431EAC31AEB1788DCC496B461E79F5711CF5C18F75F53EF7659342926009008>
+001001101 <InteriorNode>
+0010011010 <InteriorNode>
+00100110100 <InteriorNode>
+001001101000 <InteriorNode>
+0010011010000 <InteriorNode>
+00100110100000 <InteriorNode>
+001001101000000 <Stub Hash: 3B2C92E82715BA8217386469FA6F4417E2E64CBB1A8DE4C810C05C07702699F2>
+001001101000001 <DictionaryLeaf K: 2682C8C61B09B775AE7304DA9BA2D569EF9AFC4FB64FA5E1FDEF326A30D5EA34 V:
8A19079CE69D165AAA75C11932DBF4672B48CBDB6647B8ED5A5F40CAACBABE7C Hash:
D80EE2CF0B5A19DC217662EC8F7E67D6D714F95D36DEC1030128B737F8FD0D8F>
+00100110100001 <Stub Hash: 564EEDC0A1E5B0E813111DFB6BC34264A67CDC250346F0C1408116BF9A82FFFB>
+0010011010001 <Stub Hash: B042F92A2AEED4611E113B349B9592EA48FC31C050084130BAD6FF3C5823205D>
+001001101001 <Stub Hash: AC9EC2E1ABE7F2A588FEE21C22A88D4AD8176371DBB717DAC7F1FA180D70C811>
+00100110101 <Stub Hash: 9E00D4F7AB7A039CEAEA3444E26BE9B298C1503AFB86B261F7DE6EFE32796EC7>
+0010011011 <Stub Hash: 4172B6E0EC60BF6D54ED74286AC9A8472849C11909570304785BE3928C21174C>
+00100111 <Stub Hash: A1E6CA902965EA109DA575BA22DCEC9E2C12842DFF5EE40F645691015CF4E49D>
+00101 <Stub Hash: 061C723FDD7812FA5B3A483FA4919A691FE35DF28B868112B7A9B3EE8FD0B74B>
+0011 <Stub Hash: F6B71D241DEEDE801FC6D8FBBBDF6208D1D8B9820BC6077D028EC9380AAC7DE8>
+01 <Stub Hash: 40F682BEB5D1BA09FDC2C6754E77469CC061067E51CB977FB5559716354A0291>
+1 <Stub Hash: A9AE4851C920D0EF04B12E5438A780A4D7F983FD205F15A8D9A5F4C495E67F68>
>
```


Figure 8: Hashed client data stored in the server's Merkle Prefix Trie

protocol and does not require the involvement of the central server. Note that these proofs are only intended to be read and evaluated by computers; to a human the proofs appear to be very long strings of numbers written in hexadecimal, e.g., see Figure 8. In addition to the receipts, the user's wallet application contains the secret keys necessary to transfer or receive new receipts. When a receipt is issued, transferred or redeemed the wallet application ensures that the operation has been performed correctly and then uses these keys to digitally sign updates. The wallet application can then ask for a cryptographic proof from the server.

Issuing a Receipt. If a Warehouse wishes to issue a receipt to Alice (a fictitious user), the Warehouse adds the receipt to Alice's "account" at the warehouse, by inserting the cryptographic hash of the receipt into the Merkle tree representing her account. Alice and the warehouse must then sign the new root of this data structure, reflecting the addition of the receipt. Finally Alice, and the warehouse send the signed updated root to the server, who updates the root in the MPT stored on the server and commits it to Bitcoin. These actions are illustrated in Figure 9.

Once the server has witnessed the commitment to Bitcoin, Alice and the Warehouse can ask the server for the path to the issued receipt. Using this information Alice and the Warehouse can present and share the proof of the issued receipt with others.

Transferring a Receipt. If Alice seeks to transfer a receipt issued to her by Warehouse to Bob (another fictitious user), she removes the receipt from her account Merkle tree and adds it to Bob's account Merkle tree. The addition and removal of the receipt are reflected in the resulting

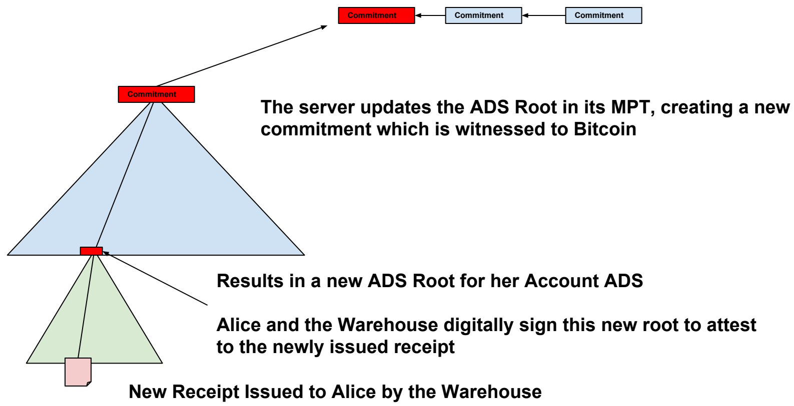


Figure 9: Secure issuance and commitment to the Bitcoin blockchain of warehouse receipts

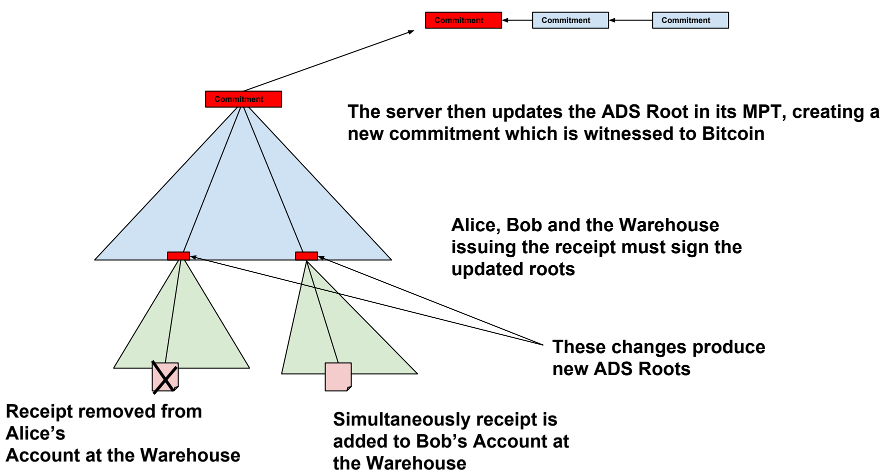


Figure 10: Secure transfer and commitment to the Bitcoin blockchain of a client to client transaction

new Authenticated Data Structures (ADS) roots for the respective data structures. At this point Alice, Bob and the Warehouse must sign the new roots for the transfer to become valid. The server then updates its MPT to reflect this and witnesses the update to Bitcoin. These actions are illustrated in Figure 10.

Once the server has published the commitment to Bitcoin, Alice and Bob can asks for paths to their respective account data structures. Using these paths, both of them can construct proofs for the receipts they own, as well as a proof of provenance for the receipt. Crucially, by broadcasting the new commitment, Alice's previous proof of ownership of the receipt is invalidated. This is critical—she can no longer present a correct proof that she owns the receipt after she has transferred it. Other systems fail to achieve this property without the use of a trusted intermediary.

B Proofs

Proof of Proposition 1: The proof is structured as follows. We fist derive the condition under which bank separating equilibria can exist, by examining three possible cases denoted by A, B and C. We then derive the two functional forms of the low-type's indifference threshold d in subsections (Case 1) and (Case 2). After that, we verify that the equilibrium suggested satisfies condition (8). Finally, we verify that the equilibrium suggested also satisfies condition (7), in subsections (Re Case 1) and (Re Case 2). To ease notation, we drop the subscript $\varnothing$.

Note that since $x = Q$, the firm's equity value is

$$V_i(Q, D, r) = (1 - b_i)((\alpha_i - Q)Q - cQ - r). \tag{26}$$

We first prove that if $b_H \leq b^{\text{se}}$ or, equivalently,

$$\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1 - b_L}\right)\right)\frac{b_L}{1 - b_L} \geq (\alpha_H - c)\frac{b_H}{1 - b_H}, \tag{27}$$

there is no separating equilibrium. In particular, we prove that for any $d \geq 0$, condition (8) is violated, i.e.,

$$\max_{D<d} V_L(D) < \max_{D \geq d} V_L(D). \tag{28}$$

Using (26) and (6), this can be written as

$$\max_{D<d}\left[(1 - b_L)(\alpha_L - Q_L(D) - c)Q_L(D) - cQ_L(D)\frac{b_L}{1 - b_L}\right] <$$
$$\max_{D \geq d}\left[(1 - b_L)\left((\alpha_L - Q_L(D) - c)Q_L(D) - cQ_H(D)\frac{b_H}{1 - b_H}\right)\right]. \tag{29}$$

It is enough to prove the following modification of (29), where the feasibility set in the LHS maximization problem is increased from $D < d$ to $D \leq d$:

$$\max_{D \leq d}\left[(1 - b_L)(\alpha_L - Q_L(D) - c)Q_L(D) - cQ_L(D)\frac{b_L}{1 - b_L}\right]$$
$$< \max_{D \geq d}\left[(1 - b_L)\left((\alpha_L - Q_L(D) - c)Q_L(D) - cQ_H(D)\frac{b_H}{1 - b_H}\right)\right]. \tag{30}$$

To prove (30), we consider three possible intervals for d.

Case A. Suppose $d \leq \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_L}\right)c$. Consider the LHS of (30). Because $D \leq d$, we have $Q_L(D) = \frac{D}{c}$. Thus, the LHS of (30) becomes

$$\max_{D \leq d}\left[(1 - b_L)\left(\alpha_L - \frac{D}{c} - \frac{c}{1 - b_L}\right)\frac{D}{c}\right]. \tag{31}$$

The unconstrained solution to (31) is $\frac{1}{2}\left(\alpha_L - \frac{c}{1-b_L}\right)c \geq d$, so the constrained solution is d, and (31) becomes $(1-b_L)\left(\alpha_L - \frac{d}{c} - \frac{c}{1-b_L}\right)\frac{d}{c}$. Therefore, inequality (30) can be written as

$$\left(\alpha_L - \frac{d}{c} - \frac{c}{1-b_L}\right)\frac{d}{c} < \max_{D \geq d}\left[\left(\alpha_L - Q_L(D) - c\right)Q_L(D) - cQ_H(D)\frac{b_H}{1-b_H}\right]. \tag{32}$$

To prove (32), it is enough to prove

$$\left(\alpha_L - \frac{d}{c} - \frac{c}{1-b_L}\right)\frac{d}{c} < \left(\alpha_L - Q_L(d) - c\right)Q_L(d) - cQ_H(d)\frac{b_H}{1-b_H}. \tag{33}$$

Using $Q_L(d) = \frac{d}{c}$ and $Q_H(d) = \frac{d}{c}$, inequality (33) simplifies into $b_H < b_L$.

Case B. Suppose $D_L^{\text{fb}} = \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_L}\right)c < d \leq \frac{1}{2}(\alpha_H - c)c$. Consider the LHS of (30). Without the constraint $D \leq d$, it is the first-best scenario, which is solved by D_L^{fb} and $Q_L^{\text{fb}} = Q_L\left(D_L^{\text{fb}}\right)$. Since $D_L^{\text{fb}} \leq d$, it is also the constrained solution, and the LHS of (30) becomes $(1-b_L)\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2$. Thus, inequality (30) can be written as

$$\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 < \max_{D \geq d}\left[\left(\alpha_L - Q_L(D) - c\right)Q_L(D) - cQ_H(D)\frac{b_H}{1-b_H}\right]. \tag{34}$$

Let $\overline{D}_H = \frac{1}{2}(\alpha_H - c)c$. Because $\overline{D}_H \geq d$, to prove (34), it is enough to prove

$$\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 < \left(\alpha_L - Q_L\left(\overline{D}_H\right) - c\right)Q_L\left(\overline{D}_H\right) - cQ_H\left(\overline{D}_H\right)\frac{b_H}{1-b_H}. \tag{35}$$

Because $Q_L\left(\overline{D}_H\right) = \frac{1}{2}(\alpha_L - c)$ and $Q_H\left(\overline{D}_H\right) = \frac{1}{2}(\alpha_H - c)$, inequality (35) becomes

$$\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 < \frac{1}{4}(\alpha_L - c)^2 - \frac{1}{2}\frac{b_H}{1-b_H}(\alpha_H - c)c, \tag{36}$$

which can be simplified into (27).

Case C. Suppose $d > \frac{1}{2}(\alpha_H - c)c$. The LHS of (30) is the same as in Case 2 and, thus, inequality (30) simplifies into (34). Hence, it is enough to prove

$$\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 < \left(\alpha_L - Q_L(d) - c\right)Q_L(d) - cQ_H(d)\frac{b_H}{1-b_H}. \tag{37}$$

Because $Q_L(d) = \frac{1}{2}(\alpha_L - c)$ and $Q_H(d) = \frac{1}{2}(\alpha_H - c)$, inequality (37) simplifies into (36), which ultimately simplifies into (27).

Next, we prove that if (27) is violated, $\left\{D_L^{\text{fb}}, \max\left(D_H^{\text{fb}}, d\right)\right\}$ with belief structure (4) and where d satisfies (9) is an SE. We start by finding $d \in (D_L^{\text{fb}}, \overline{D}_H]$ such that the low type is indifferent between borrowing his first-best loan amount D_L^{fb} and borrowing a larger amount d under which he will be perceived as a high type, i.e.,

$$\begin{aligned} V_L\left(D_L^{\text{fb}}\right) &= V_L(d) && (38)\\ \Leftrightarrow \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 &= (\alpha_L - Q_L(d) - c)\, Q_L(d) - cQ_H(d)\frac{b_H}{1-b_H}. && (39) \end{aligned}$$

Because $Q_L(d) = \min\left\{\frac{1}{2}(\alpha_L - c), \frac{d}{c}\right\}$, we distinguish two cases.

Case 1. Suppose $d \le \frac{1}{2}(\alpha_L - c)c$. We have $Q_L(d) = Q_H(d) = \frac{d}{c}$, and eq. (39) becomes

$$d^2 - \left(\alpha_L - \frac{c}{1-b_H}\right) cd + \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 c^2 = 0. \tag{40}$$

It is easy to verify that the smaller of the two roots of (40) is smaller than D_L^{fb}. The larger of the two roots is given by the top expression in (9). Obviously, $d > D_L^{\text{fb}}$ and it is straightforward to show that $d \le \frac{1}{2}(\alpha_L - c)c$ if and only if $b_H \ge b^{\varnothing}$.

Case 2. Suppose $\frac{1}{2}(\alpha_L - c)c < d \le \frac{1}{2}(\alpha_H - c)c$. We have $Q_L(d) = \frac{1}{2}(\alpha_L - c)$ and $Q_H(d) = \frac{d}{c}$, and eq. (39) gives the bottom expression in (9). It is straightforward to show that condition $\frac{1}{2}(\alpha_L - c)c < d$ is equivalent to $b_H < b^{\varnothing}$, whereas condition $d \le \frac{1}{2}(\alpha_H - c)c$ is equivalent to NOT (27).

Thus, we found $d \in (D_L^{\text{fb}}, \overline{D}_H]$ that satisfies (38), and it is given by (9). Next, we verify that this d satisfies conditions (7) and (8), starting with the latter. Given that $D_L^{\text{fb}} < d$, the LHS of (8) is $V_L\left(D_L^{\text{fb}}\right)$. Because d satisfies (38), it is enough to prove that $V_L(D)$ is non-increasing for any $D \ge d$. Using (26) and (6), we have

$$V_L(D) = (1 - b_L)\left((\alpha_L - Q_L(D) - c)\, Q_L(D) - cQ_H(D)\frac{b_H}{1-b_H}\right), \tag{41}$$

where $Q_i(D) = \min\left\{\frac{1}{2}(\alpha_i - c), \frac{D}{c}\right\}$. Thus, $V_L(D)$ is continuous, and it is differentiable almost everywhere. Therefore, to prove that it is non-increasing for $D \ge d$, it is enough to prove that $\frac{d}{dD}V_L(D) \le 0$ at any $D \ge d$ where the derivative exists. It does exist on three intervals. (i) If $D < \frac{1}{2}(\alpha_L - c)c$, then $\frac{d}{dD}V_L(D) = (1 - b_L)\left(\left(\alpha_L - c - c\frac{b_H}{1-b_H}\right)\frac{1}{c} - \frac{2D}{c^2}\right)$. Thus, $\frac{d}{dD}V_L(D) < 0$ iff $D > \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_H}\right)c$, which is clearly true for any $D \ge d$. (ii) If $\frac{1}{2}(\alpha_L - c)c < D < \frac{1}{2}(\alpha_H - c)c$, then $\frac{d}{dD}V_L(D) = -\frac{1-b_L}{1-b_H}b_H < 0$. (iii) If $D > \frac{1}{2}(\alpha_H - c)c$, then $\frac{d}{dD}V_L(D) = 0$. Thus, $V_L(D)$ is non-increasing for any $D \ge d$ and, therefore, condition (8) is satisfied.

Next, we show that d satisfies condition (7). If $d \le D_H^{\text{fb}}$, condition (7) is clearly satisfied because its RHS is the first-best $V_H\left(D_H^{\text{fb}}\right)$. Next, suppose $d > D_H^{\text{fb}}$. For any $D \ge d$, we have

$$V_H(D) = (1 - b_H)\left((\alpha_H - Q_H(D) - c)\, Q_H(D) - cQ_H(D)\frac{b_H}{1-b_H}\right), \tag{42}$$

which is clearly non-increasing for any $D \geq d > D_H^{\text{fb}}$. Therefore, condition (7) is equivalent to

$$\max_{D<d} V_H(D) \leq V_H(d). \tag{43}$$

We prove (43) by showing that $V_H(D) < V_H(d)$ for any $D < d$, considering Case 1 and Case 2 separately.

Re Case 1. Using (42), the fact that $Q_H(d) = \frac{d}{c}$, and (40), we have

$$V_H(d) = (1-b_H)\left((\alpha_H - \alpha_L)\frac{d}{c} + \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2\right). \tag{44}$$

For any $D < d$, we have

$$V_H(D) = (1-b_H)\left((\alpha_H - Q_H(D) - c)\,Q_H(D) - cQ_L(D)\frac{b_L}{1-b_L}\right), \tag{45}$$

where $Q_L(D) = Q_H(D) = \frac{D}{c}$. Therefore, for any $D < d$, the desired inequality $V_H(D) < V_H(d)$ is equivalent to

$$\left(\alpha_H - \frac{c}{1-b_L} - \frac{D}{c}\right)\frac{D}{c} < (\alpha_H - \alpha_L)\frac{d}{c} + \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2. \tag{46}$$

Because $D < d$, inequality (46) must hold if

$$\left(\alpha_L - \frac{c}{1-b_L} - \frac{D}{c}\right)\frac{D}{c} \leq \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2. \tag{47}$$

Inequality (47) is clearly satisfied because its RHS is the maximum of its LHS over any D.

Re Case 2. Using (42) and the fact that $Q_H(d) = \frac{d}{c}$, we have

$$V_H(d) = (1-b_H)\left(\alpha_H - \frac{c}{1-b_H} - \frac{d}{c}\right)\frac{d}{c}. \tag{48}$$

For any $D < d$, we have

$$V_H(D) = (1-b_H)\left((\alpha_H - Q_H(D) - c)\,Q_H(D) - cQ_L(D)\frac{b_L}{1-b_L}\right), \tag{49}$$

where $Q_L(D) = \min\left\{\frac{1}{2}(\alpha_L - c), \frac{D}{c}\right\}$ and $Q_H(D) = \frac{D}{c}$. We prove that $V_H(D) < V_H(d)$ for any $D < d$, in two steps.

Step 1. Suppose that $D \leq \frac{1}{2}(\alpha_L - c)\,c$. Thus, $Q_L(D) = \frac{D}{c}$ and

$$\begin{aligned} V_H(D) &= (1-b_H)\left(\alpha_H - \frac{c}{1-b_L} - \frac{D}{c}\right)\frac{D}{c} && (50)\\ &\leq (1-b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2. && (51)\end{aligned}$$

Because $D_H^{\text{fb}} = \frac{1}{2}\left(\alpha_H - \frac{c}{1-b_H}\right)c < d \leq \frac{1}{2}(\alpha_H - c)\,c$, we have

$$
\begin{aligned}
V_H(d) &\geq V_H\left(\frac{1}{2}(\alpha_H - c)c\right) &(52)\\
&= (1-b_H)\left(\alpha_H - \frac{c}{1-b_H} - \frac{1}{2}(\alpha_H - c)\right)\frac{1}{2}(\alpha_H - c). &(53)
\end{aligned}
$$

Thus, to prove the desired inequality $V_H(D) < V_H(d)$, it is enough to prove

$$
\begin{aligned}
&\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 < \left(\alpha_H - \frac{c}{1-b_H} - \frac{1}{2}(\alpha_H - c)\right)\frac{1}{2}(\alpha_H - c) &(54)\\
\Leftrightarrow &\left(\alpha_H - \frac{c}{2}\left(1 + \frac{1}{1-b_L}\right)\right)b_L > \left(\alpha_H - \frac{c}{2}\left(\frac{2+b_L^2-2b_L}{1-b_L}\right)\right)b_H. &(55)
\end{aligned}
$$

It is easy to verify that inequality (55) follows from the assumption that $b_H < b^{\varnothing}$.

Step 2. Suppose $D > \frac{1}{2}(\alpha_L - c)c$. Thus, $Q_L(D) = \frac{1}{2}(\alpha_L - c)$ and

$$
V_H(D) = (1-b_H)\left(\left(\alpha_H - c - \frac{D}{c}\right)\frac{D}{c} - c\frac{1}{2}(\alpha_L - c)\frac{b_L}{1-b_L}\right). \tag{56}
$$

Therefore, the desired inequality $V_H(D) < V_H(d)$ becomes

$$
\left(\alpha_H - c - \frac{D}{c}\right)\frac{D}{c} - c\frac{1}{2}(\alpha_L - c)\frac{b_L}{1-b_L} < \left(\alpha_H - \frac{c}{1-b_H} - \frac{d}{c}\right)\frac{d}{c}. \tag{57}
$$

Because $D < d \leq \frac{1}{2}(\alpha_H - c)c$, we have

$$
\left(\alpha_H - c - \frac{D}{c}\right)\frac{D}{c} < \left(\alpha_H - c - \frac{d}{c}\right)\frac{d}{c}.
$$

Thus, to prove (57), it is enough to prove

$$
\left(\alpha_H - c - \frac{d}{c}\right)\frac{d}{c} - c\frac{1}{2}(\alpha_L - c)\frac{b_L}{1-b_L} < \left(\alpha_H - \frac{c}{1-b_H} - \frac{d}{c}\right)\frac{d}{c}. \tag{58}
$$

Substituting the bottom expression of (9) for d, inequality (58) simplifies into $b_L > 0$.

Thus, we have shown that d satisfies both equilibrium conditions (7) and (8). This together with the fact $V_H(D)$ is decreasing for $D \geq D_H^{\text{fb}}$ implies that $\left\{D_L^{\text{fb}}, \max\left(D_H^{\text{fb}}, d\right)\right\}$ with belief (4) is an SE.

It remains to prove that this is a least-cost SE. Namely, we need to show that if $d > D_H^{\text{fb}}$, there is no SE in which the high type is better off. Because $V_H(D)$ is decreasing for $D > d > Q_H^{\text{fb}}$, such an equilibrium would have to have a threshold belief $\bar{d} < d$. However, a threshold $\bar{d} < d$ cannot be an equilibrium belief because there exists some $\hat{D} \in \left(\bar{d}, d\right)$ such that $V_L(\hat{D}) > V_L(d) = V_L(D_L^{\text{fb}})$, i.e., the low type could increase his payoff by borrowing $\hat{D}$, and being perceived as the high type. ■

Proof of Proposition 2: The proof is structured as follows: We first solve for the optimal indifference threshold q, and find that it depends on whether all inventory is being used (Case 1) or it is not (Case 2). Next, we prove that this q satisfies the equilibrium conditions (13) and (14). This step requires to go through several subcases detailed below in (Re Case 1) and (Re Case 2).

To ease notation, we drop the subscript Ƀ. Also, let the firm's i equity value given its second-stage optimal production decision, facing interest r be $V_i(Q,r) \equiv V_i(Q, x_i(Q), r)$, that is

$$V_i(Q,r) = \begin{cases} (1-b_i)\left[(\alpha_i - Q)Q - cQ - r\right] & \text{if } Q < \overline{Q}_i, \\ (1-b_i)\left(\overline{Q}_i^2 - cQ - r\right) & \text{if } Q \geq \overline{Q}_i. \end{cases} \tag{59}$$

As a first step, we find $q > Q_L^{\text{fb}}$ such that the low type is indifferent between obtaining his first-best payoff on the one hand, and ordering q so that he is perceived as a high type on the other, i.e.,

$$V_L\left(Q_L^{\text{fb}}\right) = V_L(q). \tag{60}$$

Substituting $Q_L^{\text{fb}} = \frac{1}{2}\left(\alpha_L - \frac{c}{1-b_L}\right) < \frac{1}{2}\alpha_i$ into (59), the LHS of (60) becomes

$$V_L\left(Q_L^{\text{fb}}\right) = (1-b_L)\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2. \tag{61}$$

Using (59) and (11), the RHS of (60) can be written as

$$V_L(q) = \begin{cases} (1-b_L)\left(\left(\alpha_L - q - \frac{c}{1-b_H}\right)q\right) & \text{if } q \leq \frac{1}{2}\alpha_L, \\ (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}q\right) & \text{if } q > \frac{1}{2}\alpha_L. \end{cases} \tag{62}$$

Thus, the solution to (60) in terms of q can take on two different forms.

Case 1. If $q \leq \frac{1}{2}\alpha_L$, eq. (60) becomes

$$q^2 - \left(\alpha_L - \frac{c}{1-b_H}\right)q + \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 = 0. \tag{63}$$

It is straightforward to verify that the smaller root of (63) is smaller than Q_L^{fb}, whereas the larger root is larger than Q_L^{fb}. Thus, q is the larger of the two roots, and it is given by the top expression in (15). Furthermore, condition $q \leq \frac{1}{2}\alpha_L$ can be written as $b_H \geq b^{\text{Ƀ}}$.

Case 2. If $q > \frac{1}{2}\alpha_L$, eq. (60) yields q that is given by the bottom expression in (15), and condition $q > \frac{1}{2}\alpha_L$ can be written as $b_H < b^{\text{Ƀ}}$.

To sum up, we found $q > Q_L^{\text{fb}}$ that satisfies eq. (60), and it is given by (15). Next, we prove that this q satisfies conditions (13) and (14), starting with the latter. Because $Q_L^{\text{fb}} < q$, the LHS of (14) is $V_L(Q_L^{\text{fb}})$. Since $V_L(Q)$ is decreasing in Q for $Q \geq q$, the RHS of (14) is $V_L(q)$. Thus, condition (14) is equivalent to $V_L(Q_L^{\text{fb}}) \geq V_L(q)$. This is satisfied as equality by the definition of q in (60). Second, we show that q satisfies condition (13). If $q \leq Q_H^{\text{fb}}$, condition (13) is clearly satisfied because its

RHS is the first-best $V_H\left(Q_H^{\text{fb}}\right)$. If $q > Q_H^{\text{fb}}$, then $V_H(Q)$ is decreasing in Q for $Q \geq q$ and, therefore, condition (13) is equivalent to

$$\max_{Q<q} V_H(Q) \leq V_H(q). \tag{64}$$

To prove (64), we need to consider Case 1 and Case 2 separately.

Re Case 1. We prove (64) by showing that $V_H(Q) \leq V_H(q)$ for all $Q < q$. Using (59) and the fact that $q \leq \frac{1}{2}\alpha_L < \frac{1}{2}\alpha_H$, for any $Q < q$, the inequality $V_H(Q) \leq V_H(q)$ can be written as

$$\begin{aligned} (1-b_H)\left((\alpha_H - Q)\,Q - Q\frac{c}{1-b_L}\right) &\leq (1-b_H)\left((\alpha_H - q)\,q - q\frac{c}{1-b_H}\right) \\ \Leftrightarrow (1-b_L)(\alpha_H - \alpha_L)\,Q + V_L(Q) &\leq (1-b_L)(\alpha_H - \alpha_L)\,q + V_L(q)\,. \end{aligned} \tag{65}$$

Using (60), inequality (65) becomes

$$(1-b_L)(\alpha_H - \alpha_L)\,Q + V_L(Q) \leq (1-b_L)(\alpha_H - \alpha_L)\,q + V_L(Q_L^{\text{fb}}). \tag{66}$$

For any $Q < q$, we have $V_L(Q) \leq V_L(Q_L^{\text{fb}})$ and, thus, inequality (66) is satisfied.

Re Case 2. When a firm is constrained to choose $Q < q$, it is guaranteed to be perceived as the low type. Therefore, it cannot be optimal for a firm in this situation to buy inventory that will not be used. Thus, at the optimal $Q < q$, the firm is guaranteed to process its entire inventory, and the LHS of (64) can be written as

$$\max_{Q<q} V_H(Q) = \max_{Q<q}\left[(1-b_H)\left((\alpha_H - Q)\,Q - Q\frac{c}{1-b_L}\right)\right]. \tag{67}$$

The solution to (67) is $Q = \frac{1}{2}\left(\alpha_H - \frac{c}{1-b_L}\right) < Q_H^{\text{fb}} < q$. Therefore,

$$\max_{Q<q} V_H(Q) = (1-b_H)\frac{1}{4}\left(\alpha_H - \tfrac{c}{1-b_L}\right)^2,$$

and condition (64) can be written as

$$(1-b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq V_H(q)\,. \tag{68}$$

The RHS of (68) depends on whether it pays off to process the entire inventory q or not, i.e.,

$$V_H(q) = \begin{cases} (1-b_H)\left((\alpha_H - q)\,q - q\frac{c}{1-b_H}\right) & \text{if } q \leq \frac{1}{2}\alpha_H, \\ (1-b_H)\left(\frac{1}{4}\alpha_H^2 - q\frac{c}{1-b_H}\right) & \text{if } q > \frac{1}{2}\alpha_H. \end{cases} \tag{69}$$

Therefore, we need to distinguish two subcases.

First, suppose that $q > \frac{1}{2}\alpha_H$. Using (69) and (15), inequality (68) simplifies into $b_L \geq b_H$, which is true by assumption.

Next, suppose that $q \leq \frac{1}{2}\alpha_H$. Because $V_H(Q)$ is decreasing in Q for $Q \geq q$, we have $V_H\left(\frac{1}{2}\alpha_H\right) \leq V_H(q)$. Thus, to prove (68), it is enough to show

$$(1-b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq V_H\left(\frac{1}{2}\alpha_H\right). \tag{70}$$

Using (69), inequality (70) simplifies into

$$\left(\frac{c}{1-b_L}\right)^2 \leq 2\alpha_H\left(\frac{c}{1-b_L} - \frac{c}{1-b_H}\right). \tag{71}$$

Using (62) and the fact that $q > \frac{1}{2}\alpha_L$, we have

$$\begin{aligned} V_L(q) &= (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}q\right) \\ &< (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}\frac{1}{2}\alpha_L\right). \end{aligned} \tag{72}$$

Combining (72) and (60), we obtain

$$V_L\left(Q_L^{\text{fb}}\right) < (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}\frac{1}{2}\alpha_L\right). \tag{73}$$

Using the fact that $V_L\left(Q_L^{\text{fb}}\right) = (1-b_L)\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2$, inequality (73) implies

$$\left(\frac{c}{1-b_L}\right)^2 < 2\alpha_L\left(\frac{c}{1-b_L} - \frac{c}{1-b_H}\right). \tag{74}$$

Finally, the fact that $b_L > b_H$ together with (74) imply the desired inequality (71).

Thus, we have proved that q satisfies both (13) and (14). This together with the fact $V_H(Q)$ is decreasing for $Q \geq Q_H^{\text{fb}}$ implies that $\left\{Q_L^{\text{fb}}, \max\left(Q_H^{\text{fb}}, q\right)\right\}$ with belief (10) is an SE. It remains to prove that this is a least-cost SE. Namely, we need to show that if $q > Q_H^{\text{fb}}$, there is no SE in which the high type is better off. Because $V_H(Q)$ is decreasing for $Q > q > Q_H^{\text{fb}}$, such an equilibrium would have to have a threshold belief $\bar{q} < q$. However, a threshold $\bar{q} < q$ cannot be an equilibrium belief because there exists some $\hat{Q} \in (\bar{q}, q)$ such that $V_L(\hat{Q}) > V_L(q) = V_L(Q_L^{\text{fb}})$, i.e., the low type could increase his payoff by ordering $\hat{Q}$, and being perceived as the high type. ■

Proof of Proposition 3: We first prove part (1)(a). Because the low type always follows its first best, its payoff is independent of whether it uses blockchain or not. Thus, the strategy profiles of class Ƀ-∅ and Ƀ-Ƀ are equivalent to those of class ∅-∅ and ∅-Ƀ. For conciseness, we focus on ∅-∅ and ∅-Ƀ. When condition (27) holds, strategy profile of class ∅-∅ cannot be an SE either as stipulated in Proposition 1. Thus, the only possible SE is of class ∅-Ƀ. Next, we show that $\left\{D_L^{\text{fb}}, \max\left(q, Q_H^{\text{fb}}\right)\right\}$ with belief thresholds $d = \infty$ and q given by (16), is an SE. The sufficient conditions for an SE of class $\varnothing$-Ƀ with $d = \infty$, are

$$\max_{D} V_{H\varnothing}(D) \leq \max_{Q \geq q} V_{H\text{Ƀ}}(Q), \tag{75}$$

$$\text{and } \max_{D} V_{L\varnothing}(D) \geq \max_{Q} V_{L\text{Ƀ}}(Q). \tag{76}$$

We find $q > Q_L^{\text{fb}}$ such that the low type is indifferent between borrowing his first-best without blockchain and being perceived as the low type, and borrowig/ordering q using blockchain and being perceived as the high type, i.e.,

$$V_{L\varnothing}\left(D_L^{\text{fb}}\right) = V_{L\text{Ƀ}}(q). \tag{77}$$

Because the LHS of (77) is $(1 - b_L)\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2$, whereas the RHS of (77) is given by (62), the solution to (77) in terms of q can take on two different forms.

Case 1. If $q \leq \frac{1}{2}\alpha_L$, eq. (77) becomes

$$q^2 - \left(\alpha_L - \frac{c}{1-b_H}\right) q + \frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2 = 0. \tag{78}$$

It is straightforward to verify that the larger of the two roots of (78) is given by the top expression in (16) and it is is larger than Q_L^{fb}. Furthermore, condition $q \leq \frac{1}{2}\alpha_L$ can be written as $b_H \geq b^{\text{Ƀ}}$.

Case 2. If $q > \frac{1}{2}\alpha_L$,eq. (77) yields q that is given by the bottom expression in (16), and condition $q > \frac{1}{2}\alpha_L$ can be written as $b_H < b^{\text{Ƀ}}$.

To sum up, q given by (16) satisfies eq. (77) and $q > Q_L^{\text{fb}}$. Next, we prove that this q satisfies conditions (75) and (76), starting with the latter. Because $\max_D V_{L\varnothing}(D) = V_{L\varnothing}\left(D_L^{\text{fb}}\right)$, condition (76) holds if

$$V_{L\varnothing}\left(D_L^{\text{fb}}\right) \geq \max_{Q<q} V_{L\text{Ƀ}}(Q), \tag{79}$$

$$\text{and } V_{L\varnothing}\left(D_L^{\text{fb}}\right) \geq \max_{Q \geq q} V_{L\text{Ƀ}}(Q). \tag{80}$$

Inequality (79) is true because its LHS and RHS differ only in that the LHS is the unconstrained maximum. Inequality (80) follows from (77) and the fact that $V_{L\text{Ƀ}}(Q)$ is decreasing in $Q \geq q$.

Condition (75) can be written as

$$(1 - b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq \max_{Q \geq q} V_{H\text{Ƀ}}(Q). \tag{81}$$

If $q \leq Q_H^{\text{fb}}$, the RHS of (81) is $V_{H\text{Ƀ}}\left(Q_H^{\text{fb}}\right) = (1 - b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_H}\right)^2$, and inequality (81) follows from (2). If $q > Q_H^{\text{fb}}$, then $V_{H\text{Ƀ}}(Q)$ is decreasing for $Q \geq q$, and inequality (81) is equivalent to

$$(1 - b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq V_{H\text{Ƀ}}(q). \tag{82}$$

To prove (82), we consider Cases 1 and 2 separately.

Re Case 1. Because $q \leq \frac{1}{2}\alpha_L < \frac{1}{2}\alpha_H$, condition (82) can be written as

$$\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq \left(\alpha_H - q - \frac{c}{1-b_H}\right) q. \tag{83}$$

Using (78), this becomes

$$\left(\alpha_H - \frac{c}{1-b_L}\right)^2 - \left(\alpha_L - \frac{c}{1-b_L}\right)^2 \leq 4\left(\alpha_H - \alpha_L\right) q. \tag{84}$$

Using the fact that $q > Q_H^{\text{fb}} = \frac{1}{2}\left(\alpha_H - \frac{c}{1-b_H}\right)$ and (2), we obtain $q > \frac{1}{2}\left(\alpha_H - \frac{c}{1-b_L}\right)$. Given this last inequality, it is straightforward to show that (84) is true.

Re Case 2. Because the RHS of (82) depends on the range of q as in (69), we need to consider two subcases.

First, suppose that $q > \frac{1}{2}\alpha_H$. The desired inequality (82) becomes

$$\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq \frac{1}{4}\alpha_H^2 - q\frac{c}{1-b_H}. \tag{85}$$

Plugging the bottom expression from (16) for q, inequality (85) becomes simplifies into $b_L \geq b_H$.

Next, suppose that $q \leq \frac{1}{2}\alpha_H$. Because $V_{H\text{B}}(Q)$ is decreasing for $Q \geq q > Q_H^{\text{fb}}$, we have $V_{H\text{B}}\left(\frac{1}{2}(\alpha_H)\right) \leq V_{H\text{B}}(q)$. Thus, to prove (82), it is enough to show that

$$(1-b_H)\frac{1}{4}\left(\alpha_H - \frac{c}{1-b_L}\right)^2 \leq V_{H\text{B}}\left(\frac{1}{2}\alpha_H\right). \tag{86}$$

Using (69), inequality (86) is equivalent to

$$\left(\frac{c}{1-b_L}\right)^2 \leq 2\alpha_H\left(\frac{c}{1-b_L} - \frac{c}{1-b_H}\right). \tag{87}$$

Using (62) and the fact that $q > \frac{1}{2}\alpha_L$, we have

$$\begin{aligned} V_{L\text{B}}(q) &= (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}q\right) \\ &< (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}\frac{1}{2}\alpha_L\right). \end{aligned} \tag{88}$$

Combining (88) and (77), we obtain

$$V_{L\varnothing}\left(D_L^{\text{fb}}\right) < (1-b_L)\left(\frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}\frac{1}{2}\alpha_L\right). \tag{89}$$

Using the fact that $V_{L\varnothing}\left(D_L^{\text{fb}}\right) = (1-b_L)\frac{1}{4}\left(\alpha_L - \frac{c}{1-b_L}\right)^2$,inequality (89) implies

$$\left(\frac{c}{1-b_L}\right)^2 < 2\alpha_L\left(\frac{c}{1-b_L} - \frac{c}{1-b_H}\right) \tag{90}$$

Finally, the fact that $b_L > b_H$ together with (90) imply the desired inequality (87).

The fact that $\left\{D_L^{\text{fb}}, \max\left(q, Q_H^{\text{fb}}\right), d, q\right\}$ satisfy conditions (75)-(76) means that they constitute an SE. It remains to prove that there is no other SE of class ∅-Ƀ in which the high type would be better off. This is obviously true if $q \leq Q_H^{\text{fb}}$ in which case the high type achieves his first best. Now suppose that $q > Q_H^{\text{fb}}$. Because $V_{H\text{B}}(Q)$ is decreasing for $Q > q > Q_H^{\text{fb}}$, such an equilibrium would have to have a belief threshold $\bar{q} < q$. However, a threshold $\bar{q} < q$ cannot be an equilibrium belief because there exists $\hat{Q} \in (\bar{q}, q)$such that $V_{L\text{B}}(\hat{Q}) > V_{L\text{Ƀ}}(q) = V_{L\varnothing}(D_L^{\text{fb}})$, i.e., the low type could increase his payoff by adopting blockchain, borrowing/ordering $\hat{Q}$, and being perceived as the high type.

Next, we prove part (1)(b). The only difference from part (1)(a) is that when condition (27) does not hold, we cannot exclude an SE of class ∅-∅. In particular, when the belief threshold is $q = \infty$, the SE characterized in Proposition 1 remains to be a SE even in the presence of blockchain technology. (Because the lender considers each firm using blockchain to be a low type, no firm has incentive to ever use supplier financing.) Finally, as we established in Proposition 1, there is no SE of class ∅-∅ in which the high type would be better off relative to the equilibrium given in (17).

We now switch our focus to (2). Any PE must be of class ∅-∅ or Ƀ-Ƀ. We prove that no PE of class ∅-∅ can survive the intuitive criterion (IC). (The proof that no PE of class Ƀ-Ƀ survives the IC is analogous and available upon request.) Let D_P be any PE loan. We can assume WLOG that $D_P \leq \overline{D}_H$ because all payoffs become constant for $D \geq \overline{D}_H$. At D_P, the bank is uncertain about the firm type and, thus, charges a fair price by pooling. Hence, the fair interest at the PE is

$$r\left(D_P\right) = \frac{hb_H c Q_H\left(D_P\right) + (1-h)\, b_L c Q_L\left(D_P\right)}{h\left(1-b_H\right) + (1-h)\left(1-b_L\right)}, \tag{91}$$

and the value of equity at the PE is

$$\begin{aligned} V_{i\varnothing}\left(D_P\right) &= \left(1-b_i\right)\left(\left(\alpha_i - c - Q_i\left(D_P\right)\right) Q_i\left(D_P\right) - r\left(D_P\right)\right), & (92) \\ \text{where } Q_L\left(D_P\right) &= \min\left\{\frac{1}{2}\left(\alpha_L - c\right), \frac{D_P}{c}\right\} \text{ and } Q_H\left(D_P\right) = \frac{D_P}{c}. & (93) \end{aligned}$$

We will show that for any PE bank loan D_P, there exists an order quantity Q such that the low type would not switch from borrowing D_P without blockchain to ordering Q using blockchain even if the lender perceived this action with the high type, whereas the high type would, i.e.,

$$\begin{aligned} V_{L\varnothing}\left(D_P\right) &> V_{L\text{Ƀ}}\left(Q|H\right), & (94) \\ \text{and } V_{H\varnothing}\left(D_P\right) &< V_{H\text{B}}\left(Q|H\right), & (95) \end{aligned}$$

where $V_{i\text{B}}(Q|H)$ is the equity value of type i using blockchain when the lender believes the firm is high type, i.e.,

$$V_{i\text{B}}(Q|H) = \begin{cases} (1-b_i)\left(\left(\alpha_i - Q - \frac{c}{1-b_H}\right)Q\right) & \text{if } Q \le \frac{1}{2}\alpha_i, \\ (1-b_i)\left(\frac{1}{4}\alpha_i^2 - \frac{c}{1-b_H}Q\right) & \text{if } Q > \frac{1}{2}\alpha_i. \end{cases} \tag{96}$$

The existence of Q that satisfies (94) and (95) means that D_P cannot be a PE that survives the IC. (If the lender believes that a firm ordering Q using blockchain is of the low type, its belief does not survive the IC. If the lender believes that a firm ordering Q using blockchain is of the high type, D_P is not an equilibrium at all.) Before finding Q that satisfies (94) and (95), we find q such that

$$V_{L\varnothing}(D_P) = V_{L\text{B}}(q|H), \tag{97}$$

and $V_{L\text{B}}(\quad|H)$ is decreasing at q. To do so, we need to consider two cases.

Case 1. Suppose $D_P \le \frac{1}{2}(\alpha_L - c)c$. If the desired q exists, it must fall into one of two subcases.

Subcase 1a. Suppose $q \le \frac{1}{2}\alpha_L$. Eq. (97) becomes

$$\left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} = \left(\alpha_L - q - \frac{c}{1-b_H}\right)q. \tag{98}$$

The quadratic equation (98) is guaranteed to have a real solution by assumption (2). Consider the larger of the two roots of (98). Condition $q \le \frac{1}{2}\alpha_L$ becomes

$$\alpha_L\left(\alpha_L - 2\frac{c}{1-b_H}\right) \le 4\left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c}. \tag{99}$$

Subcase 1b. Suppose $q > \frac{1}{2}\alpha_L$. Eq. (97) becomes

$$\left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} = \frac{1}{4}\alpha_L^2 - \frac{c}{1-b_H}q, \tag{100}$$

which gives us a unique q. Condition $q > \frac{1}{2}\alpha_L$ becomes NOT (99).

Thus, we found q that satisfies (97), and it is given by the larger root of (98) if (99) holds, and by (100) otherwise. It is straightforward to show that $V_{L\text{B}}(\quad|H)$ is decreasing at this q.

Case 2. Suppose $D_P > \frac{1}{2}(\alpha_L - c)c$. If the desired q exists, it must fall into one of two subcases.

Subcase 2a. Suppose $q \le \frac{1}{2}\alpha_L$. Eq. (97) becomes

$$\frac{1}{4}(\alpha_L - c)^2 - \frac{hb_Hc\frac{D_P}{c}+(1-h)b_Lc\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} = \left(\alpha_L - q - \frac{c}{1-b_H}\right)q. \tag{101}$$

The quadratic equation (101) is guaranteed to have a real solution by assumption (2). Consider the larger of the two roots of (101). Condition $q \le \frac{1}{2}\alpha_L$ becomes

$$2\alpha_L\frac{b_H}{1-b_H}c + c^2 \ge 4\frac{hb_Hc\frac{D_P}{c} + (1-h)b_Lc\frac{1}{2}(\alpha_L - c)}{h(1-b_H) + (1-h)(1-b_L)}. \tag{102}$$

Subcase 2b. Suppose $q > \frac{1}{2}\alpha_L$.Eq. (97) becomes

$$\frac{1}{1-b_H}q = \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) + \frac{hb_H\frac{D_P}{c} + (1-h)\,b_L\frac{1}{2}\left(\alpha_L - c\right)}{h\left(1-b_H\right) + \left(1-h\right)\left(1-b_L\right)}, \tag{103}$$

which gives us a unique q. Condition $q > \frac{1}{2}\alpha_L$ becomes NOT (102).

Thus, we found q that satisfies (97), and it is given by the larger root of (101) if (102) holds, and by (103) otherwise. It is straightforward to show that $V_{L\mathrm{B}}(\quad|H)$ is decreasing at this q.

Because $V_{L\mathrm{B}}(\quad|H)$ is concave on $\mathbb{R}^+$ and decreasing at q, eq. (97) implies that condition (94) is satisfied for any $Q > q$. Thus, it remains to find $Q > q$ that satisfies condition (95). We consider two instances.

Instance A. Suppose $q \leq D_p/c$. We will show that $Q = D_p/c + \epsilon$ satisfies (95). Because $V_{H\mathrm{B}}(\quad|H)$ is continuous, it is enough to show that

$$V_{H\varnothing}\left(D_P\right) < V_{H\mathrm{B}}\left(\frac{D_P}{c}\middle| H\right). \tag{104}$$

Using (91), (92) and (96), the inequality becomes

$$D_P + \frac{hb_H D_P + (1-h)\,b_L c Q_L\left(D_P\right)}{h\left(1-b_H\right) + \left(1-h\right)\left(1-b_L\right)} > \frac{1}{1-b_H}D_P, \tag{105}$$

where $Q_L\left(D_P\right) = \min\left\{\frac{1}{2}\left(\alpha_L - c\right), \frac{D_P}{c}\right\}$. If $Q_L\left(D_P\right) = \frac{D_P}{c}$, inequality (105) simplifies into $1 < \frac{1-b_H}{h(1-b_H)+(1-h)(1-b_L)}$, which is straightforward. If $Q_L\left(D_P\right) = \frac{1}{2}\left(\alpha_L - c\right)$, inequality (105) simplifies into

$$\frac{(1-h)\,b_L\frac{1}{2}\left(\alpha_L - c\right)c}{h\left(1-b_H\right) + \left(1-h\right)\left(1-b_L\right)} > \left(\frac{b_H}{1-b_H} - \frac{hb_H}{h\left(1-b_H\right) + \left(1-h\right)\left(1-b_L\right)}\right)D_P. \tag{106}$$

Inequality (106) follows from (2) and the fact that $D_P \leq \overline{D}_H$.

Instance B. Suppose $q > D_p/c$. We will show that $Q = q+\epsilon$ satisfies (95). Because $V_{H\mathrm{B}}(\quad|H)$ is continuous, it is enough to show that

$$V_{H\varnothing}\left(D_P\right) < V_{H\mathrm{B}}\left(q|H\right). \tag{107}$$

Re Subcase 1a. Condition (107) becomes

$$\left(\alpha_H - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} < \left(\alpha_H - q - \frac{c}{1-b_H}\right)q. \tag{108}$$

Using (98), inequality (108) simplifies into $\frac{D_P}{c} < q$. This last inequality follows from the definition of q as the larger root of (98) and assumption (2).

Re Subcase 1b. In this case, the RHS of condition (107) depends on the range of q, so we need to consider two situations.

(i) Suppose $q \leq \frac{1}{2}\alpha_H$. Condition (107) becomes

$$\left(\alpha_H - c - \frac{D_P}{c} - \frac{hb_H c + (1-h) b_L c}{h(1-b_H) + (1-h)(1-b_L)}\right)\frac{D_P}{c} < \left(\alpha_H - q - \frac{c}{1-b_H}\right) q. \tag{109}$$

Using (100), inequality (109) simplifies into

$$\frac{1}{4}\alpha_L^2 + (\alpha_H - \alpha_L)\frac{D_P}{c} < (\alpha_H - q)\, q. \tag{110}$$

Inequality (110) follows from the facts that $D_P \leq \frac{1}{2}(\alpha_L - c)\, c$ and $\frac{1}{2}\alpha_L < q \leq \frac{1}{2}(\alpha_H)$.

(ii) Suppose $q > \frac{1}{2}\alpha_H$. Condition (107) becomes

$$\left(\alpha_H - c - \frac{D_P}{c} - \frac{hb_H c + (1-h) b_L c}{h(1-b_H) + (1-h)(1-b_L)}\right)\frac{D_P}{c} < \frac{1}{4}\alpha_H^2 - \frac{c}{1-b_H} q. \tag{111}$$

Using (100), inequality (111) simplifies into $D_P < \frac{1}{2}\frac{\alpha_L + \alpha_H}{2} c$, which follows from the fact that $D_P \leq \frac{1}{2}(\alpha_L - c)\, c$.

Re Subcase 2a. Condition (107) becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \frac{hb_H c\frac{D_P}{c} + (1-h) b_L c \frac{1}{2}(\alpha_L - c)}{h(1-b_H) + (1-h)(1-b_L)} < \left(\alpha_H - q - \tfrac{c}{1-b_H}\right) q. \tag{112}$$

Using (101), inequality (112) simplifies into

$$\left(\alpha_L - c - \frac{D_P}{c}\right)\frac{D_P}{c} < (\alpha_H - \alpha_L)\left(q - \frac{D_P}{c}\right) + \frac{1}{4}(\alpha_L - c)^2. \tag{113}$$

Because $q > \frac{D_P}{c}$, this is clearly true.

Re Subcase 2b. The RHS of condition (107) depends on the range of q, so we need to consider two situations.

(i) Suppose $q \geq \frac{1}{2}(\alpha_H)$. Condition (107) becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \frac{hb_H c\frac{D_P}{c} + (1-h) b_L c \frac{1}{2}(\alpha_L - c)}{h(1-b_H) + (1-h)(1-b_L)} < \frac{1}{4}\alpha_H^2 - \tfrac{c}{1-b_H} q. \tag{114}$$

Using (103), this simplifies into

$$\left(\alpha_H - c - \frac{D_P}{c}\right)\frac{D_P}{c} + \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c < \frac{1}{4}\alpha_H^2. \tag{115}$$

Inequality (115) follows from the facts that

$$\left(\alpha_H - c - \frac{D_P}{c}\right)\frac{D_P}{c} \leq \frac{1}{4}(\alpha_H - c)^2$$

and $b_H < b_L$.

(ii) Suppose $q < \frac{1}{2}\alpha_H$. Condition (107) becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \frac{hb_H c\frac{D_P}{c} + (1-h) b_L c \frac{1}{2}(\alpha_L - c)}{h(1-b_H) + (1-h)(1-b_L)} < \left(\alpha_H - q - \tfrac{c}{1-b_H}\right) q. \tag{116}$$

Using (103), this simplifies into

$$\left(\alpha_H - c - \frac{D_P}{c}\right)\frac{D_P}{c} < (\alpha_H - q)\, q - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c. \tag{117}$$

If $D_P \geq \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c$, in order to show (117), it is enough to show that $\left(\alpha_H - \frac{D_P}{c}\right)\frac{D_P}{c} < (\alpha_H - q)\, q$. This is true because $D_P/c < q < \frac{1}{2}\alpha_H$. Next, suppose that $D_P < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c$. Because $\frac{1}{2}\alpha_L < q < \frac{1}{2}(\alpha_H)$, in order to show (117), it is enough to show that

$$\left(\alpha_H - c - \frac{D_P}{c}\right)\frac{D_P}{c} < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c. \tag{118}$$

Because $D_P \leq \overline{D}_H = \frac{1}{2}(\alpha_H - c)\, c$, there are two possibilities: (a) $D_P \leq \frac{1}{2}(\alpha_H - c)\, c < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c$, or (b) $D_P < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c \leq \frac{1}{2}(\alpha_H - c)\, c$. If (a) holds, in order to show (118), it is enough to show that

$$\frac{1}{4}(\alpha_H - c)^2 < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c. \tag{119}$$

Inequality (119) is equivalent to $\alpha_H - \alpha_L < 2c$, which follows directly from (a). If (b) holds, in order to show (118), it is enough to show that

$$\left(\alpha_H - c - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)\right)\frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) c. \tag{120}$$

Inequality (120) is equivalent to $\alpha_H - \alpha_L + \frac{1}{4}c > 0$, which is clearly always true. ■

Proof of Theorem 1: (i) Suppose $b_H \leq b^{\text{se}}$. It follows directly from Proposition 3 that in the absence of blockchain, no separation is possible.

(ii) Suppose $b^{\text{se}} < b_H < b^{\text{cr}}$. We show that $\mathcal{C}_{\text{Ƀ}} < \mathcal{C}_{\varnothing}$ and thus the LCSE of class $\varnothing - \text{Ƀ}$ is the unique LCSE. If $b_H < b^{\text{cr}}$, we have $b_H < b^0$ and $b_H < b^{\varnothing}$. By the definition of b^0, $b_H < b^0$ implies that

$$D_H^{\text{fb}} < \frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right)\frac{1-b_H}{1-b_L}\frac{b_L}{b_H} = d,$$

where the equality follows from Proposition 3 and $b_H < b^{\varnothing}$. Therefore, $D_H^{\text{se}} = d > D_H^{\text{fb}}$ according to Proposition 3. In other words, firm H overorders, implying that $\mathcal{C}_{\varnothing} > 0$.

We now turn our attention to the $\varnothing$-Ƀ equilibrium. There are two cases depending on q:

- $q \leq Q_H^{\text{fb}}$, implying $\widetilde{Q}_H^{\text{se}} = Q_H^{\text{fb}}$, and $\mathcal{C}_{\text{Ƀ}} = 0 < \mathcal{C}_{\varnothing}$.

- $q > Q_H^{\text{fb}}$, implying $\widetilde{Q}_H^{\text{se}} = q$. Note that in this case, we have $c\, q < d$. We can express the signaling costs as

$$
\begin{aligned}
\mathcal{C}_{\text{Ƀ}} &= V_H^{\text{fb}} - V_{H\text{Ƀ}}^{\text{se}} \\
&= V_H^{\text{fb}} - V_{H\text{Ƀ}}(q) \\
&= V_H^{\text{fb}} - V_H(q, x_H(q), r_{\text{Ƀ}}(q)) \\
&\le V_H^{\text{fb}} - V_H(q, q, r_{\text{Ƀ}}(q)) \\
&= V_H^{\text{fb}} - V_H\left(q, q, c\, q \frac{b_H}{1-b_H}\right) \\
&< V_H^{\text{fb}} - V_H\left(\frac{d}{c}, \frac{d}{c}, d \frac{b_H}{1-b_H}\right) \\
&= V_H^{\text{fb}} - V_H\left(Q_H(d), Q_H(d), r_\varnothing(d)\right) \\
&= V_H^{\text{fb}} - V_{H\varnothing}(d) \\
&= V_H^{\text{fb}} - V_{H\varnothing}^{\text{se}} = \mathcal{C}_\varnothing,
\end{aligned}
$$

where all equalities follow by definition. The "$\le$" step follows from $x_H(q)$ being the equity-maximizing production choice, whereas q is simply a feasible production choice. Furthermore, the "$<$" step follows from $V_H(Q, Q, c\, Q \frac{b_H}{1-b_H})$ being strictly concave quadratic attaining its maximum at Q_H^{fb} (see Section 4.1), in conjunction with $Q_H^{\text{fb}} < q < d/c$.

(iii) Suppose $b_H \ge b^{\text{cr}}$. We show that $\mathcal{C}_{\text{Ƀ}} = \mathcal{C}_\varnothing$ and thus there are two LCSE's: the LCSE of class $\varnothing - \text{Ƀ}$ and that of class $\varnothing - \varnothing$. We distinguish two cases.

- If $b_H \ge b^\varnothing$, then $c\, q = d$. Moreover, by our analysis of the $\varnothing$-$\varnothing$ equilibrium in Section 4.2, we conclude that there is no cash burning. Similarly, by our analysis of the Ƀ-Ƀ equilibrium in Section 4.3, in conjunction with $b_H \ge b^\varnothing \ge b^{\text{Ƀ}}$, we conclude that there is no inventory either. Consequently, under both equilibria the firm borrows the same amount, orders and processes the same quantity. Thus, $\mathcal{C}_{\text{Ƀ}} = \mathcal{C}_\varnothing$.

- If $b_H < b^\varnothing$, we also get that $b^0 = b^{\text{cr}} \le b_H$. As we argued in (a), $b_H < b^\varnothing$ implies
$$\frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right) \frac{1-b_H}{1-b_L} \frac{b_L}{b_H} = d, \quad \text{and} \quad c\, q < d.$$
At the same time, $b^0 \le b_H$ implies that
$$D_H^{\text{fb}} \ge \frac{c}{2}\left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right) \frac{1-b_H}{1-b_L} \frac{b_L}{b_H} = d.$$
Therefore, $D_H^{\text{se}} = D_H^{\text{fb}}$ and $\mathcal{C}_\varnothing = 0$. Finally,
$$c\, q < d \le D_H^{\text{fb}} = c\, Q_H^{\text{fb}},$$
implying that $q < Q_H^{\text{fb}} = \widetilde{Q}_H^{\text{se}}$ and $\mathcal{C}_{\text{Ƀ}} = 0$. ■

Proof of Lemma 1: For action A (resp. B), the unique least-cost separating equilibrium is given by $A^\star = 1/a_L$ (resp. $B^\star = 1/b_L$). To see this for action A, for example, note that conditions (7)-(8) can be expressed here as $1 \le 2 - a_H A^\star$ and $1 \ge 2 - a_L A^\star$. When the latter is satisfied with equality, we get $A^\star = 1/a_L$ and the former is satisfied as $1 = 2 - a_L A^\star < 2 - a_H A^\star$. The resulting signaling costs are $a_H A^\star = a_H/a_L$. Similarly, for action B the costs are b_H/b_L. Given that they are nonnegative and bounded, we let the cost parameters, without a loss of generality, lie in the unit hypercube. Then, we can express the set $\mathbb{A}$ as

$$\mathbb{A} = \left\{ (a_H, a_L, b_H, b_L) \in [0,1]^4 \; : \; a_H > b_H,\; a_L > b_L,\; a_H < a_L,\; b_H < b_L,\; \frac{a_H}{a_L} < \frac{b_H}{b_L} \right\}.$$

The set $\mathbb{B}$ is similarly defined, but with the last inequality being flipped, $\frac{a_H}{a_L} > \frac{b_H}{b_L}$. Therefore,

$$\mu(\mathbb{A}) = \int_0^1 \int_0^{a_L} \int_0^{a_H} \int_{b_L \frac{a_H}{a_L}}^{b_L} \mathrm{d}b_H \mathrm{d}b_L \mathrm{d}a_H \mathrm{d}a_L + \int_0^1 \int_0^{a_L} \int_{a_H}^{a_L} \int_{b_L \frac{a_H}{a_L}}^{a_H} \mathrm{d}b_H \mathrm{d}b_L \mathrm{d}a_H \mathrm{d}a_L = \frac{1}{48}.$$

Similarly, we obtain $\mu(\mathbb{B}) = \frac{3}{48}$, and the proof is complete.

In conclusion, let us make two technical remarks. First, as with our previous analysis, note that pooling equilibria in this generic example can be eliminated through the Cho and Kreps (1987) intuitive criterion refinement. In particular, suppose without a loss of generality that there exists a pooling equilibrium at which both types take action $A = A^P$. The payoff of type i at this equilibrium is $1 + h - a_i A^P$, where h is the proportion of high types in the population. Consider action $A^D = \frac{1}{2}\left(\frac{1-h+a_L A^P}{a_L} + \frac{1-h+a_H A^P}{a_H}\right)$, which clearly satisfies (i) $1 + h - a_L A^P > 2 - a_L A^D$ and (ii) $1 + h - a_H A^P < 2 - a_H A^D$. Condition (ii) implies that action A^D cannot be associated with the high type. This is because if it were, the high type would deviate to A^D, and A^P wouldn't be an equilibrium. Condition (i) implies that associating action A^D with anything but the high type would violate the intuitive criterion. This is because the low type would not deviate to A^D even if it meant to be perceived as the high type, whereas the high type would. Thus, A^P cannot be an equilibrium that survives the intuitive criterion.

Second, let us also consider the case wherein Spence's assumption that $a_H < a_L$ and $b_H < b_L$ does not necessarily hold, and let $\mathbb{A}'$ and $\mathbb{B}'$ be now the sets over which the respective action is preferred. We will show that $\frac{\mu(\mathbb{A}')}{\mu(\mathbb{A}')+\mu(\mathbb{B}')} = \frac{3}{8}$. If $a_H > a_L$ and $b_H > b_L$, neither action allows for signaling. If $a_H < a_L$ and $b_H > b_L$, then it is only possible to signal through A, and conversely, if $a_H > a_L$ and $b_H < b_L$, then it is only possible to signal through B. Considering all these posibilities, we get that $\mathbb{A}' = \mathbb{A} \cup \left\{(a_H, a_L, b_H, b_L) \in [0,1]^4 \; : \; a_H > b_H,\; a_L > b_L,\; a_H < a_L,\; b_H > b_L\right\}$. The set $\mathbb{B}$ is similarly augmented to obtain $\mathbb{B}'$. The claim then follows from straightforward integration. ■

Proof of Proposition 4: We prove the result by contradiction. Suppose that there exists a separating equilibrium $(Q_L^{\rm fb}, Q_H^{\rm se})$ with a consistent belief threshold q. Note that q being a SE belief threshold implies $Q_H^{\rm se} \geq q > Q_L^{\rm fb}$. The following two conditions must be satisfied at this SE

$$\begin{aligned} V_{L\mathbb{B}}\left(Q_L^{\rm fb}\right) &\geq V_{L\mathbb{B}}\left(Q_H^{\rm se}\right), &(121)\\ \text{and } V_{H\mathbb{B}}\left(Q_L^{\rm fb}\right) &\leq V_{H\mathbb{B}}\left(Q_H^{\rm se}\right). &(122)\end{aligned}$$

Recall that

$$V_{i\mathbb{B}}(Q) = \begin{cases} (1-b_i)\left((\alpha_i - \min\{Q, \frac{1}{2}\alpha_i\})\min\{Q, \frac{1}{2}\alpha_i\} - \frac{cQ}{1-b_H}\right) & \text{if } Q \geq q, \\ (1-b_i)\left((\alpha_i - \min\{Q, \frac{1}{2}\alpha_i\})\min\{Q, \frac{1}{2}\alpha_i\} - \frac{cQ}{1-b_L}\right) & \text{o/w.} \end{cases} \tag{123}$$

Using (123), conditions (121)-(122) can be written as

$$\begin{aligned} \frac{cQ_H^{\rm se}}{1-b_H} - \frac{cQ_L^{\rm fb}}{1-b_L} &\geq (\alpha_L - \min\{Q_H^{\rm se}, \frac{1}{2}\alpha_L\})\min\{Q_H^{\rm se}, \frac{1}{2}\alpha_L\} - (\alpha_L - \min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_L\})\min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_L\},\\ \frac{cQ_H^{\rm se}}{1-b_H} - \frac{cQ_L^{\rm fb}}{1-b_L} &\leq (\alpha_H - \min\{Q_H^{\rm se}, \frac{1}{2}\alpha_H\})\min\{Q_H^{\rm se}, \frac{1}{2}\alpha_H\} - (\alpha_H - \min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_H\})\min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_H\}.\end{aligned}$$

These two conditions then imply

$$\begin{aligned} &(\alpha_H - \min\{Q_H^{\rm se}, \frac{1}{2}\alpha_H\})\min\{Q_H^{\rm se}, \frac{1}{2}\alpha_H\} - (\alpha_H - \min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_H\})\min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_H\} \geq\\ &(\alpha_L - \min\{Q_H^{\rm se}, \frac{1}{2}\alpha_L\})\min\{Q_H^{\rm se}, \frac{1}{2}\alpha_L\} - (\alpha_L - \min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_L\})\min\{Q_L^{\rm fb}, \frac{1}{2}\alpha_L\}. \end{aligned} \tag{124}$$

Noting that $Q_L^{\rm fb} < \frac{1}{2}\alpha_L$ and $\frac{1}{2}\alpha_H < \frac{1}{2}\alpha_L$, one of the following cases must occur.

Case 1: $Q_L^{\rm fb} \leq \frac{1}{2}\alpha_H$.

Subcase 1a: $Q_H^{\rm se} \leq \frac{1}{2}\alpha_H$. Inequality (124) becomes

$$\alpha_H \geq \alpha_L, \tag{125}$$

which is a contradiction.

Subcase 1b: $\frac{1}{2}\alpha_H < Q_H^{\rm se} \leq \frac{1}{2}\alpha_L$. Inequality (124) becomes

$$\begin{aligned} \left(\alpha_H - \frac{1}{2}\alpha_H\right)\frac{1}{2}\alpha_H - \alpha_H Q_L^{\rm fb} &\geq (\alpha_L - Q_H^{\rm se})Q_H^{\rm se} - \alpha_L Q_L^{\rm fb}, &(126)\\ \Longrightarrow \left(\alpha_H - \frac{1}{2}\alpha_H\right)\frac{1}{2}\alpha_H - \alpha_H Q_L^{\rm fb} &> (\alpha_L - \frac{1}{2}\alpha_H)\frac{1}{2}\alpha_H - \alpha_L Q_L^{\rm fb} &(127)\\ \Longleftrightarrow \alpha_H\left(\frac{1}{2}\alpha_H - Q_L^{\rm fb}\right) &> \alpha_L\left(\frac{1}{2}\alpha_H - Q_L^{\rm fb}\right), &(128)\end{aligned}$$

which is a contradiction because $\frac{1}{2}\alpha_H \geq Q_L^{\rm fb}$ and $\alpha_H < \alpha_L$.

Subcase 1c: $Q_H^{\rm se} > \frac{1}{2}\alpha_L$. Inequality (124) becomes

$$\frac{1}{4}\alpha_H^2 - \alpha_H Q_L^{\rm fb} \geq \frac{1}{4}\alpha_L^2 - \alpha_L Q_L^{\rm fb}, \tag{129}$$

which is a contradiction because $\frac{1}{4}\alpha^2 - \alpha Q_L^{\text{fb}}$ is strictly increasing in α iff $\alpha > 2Q_L^{\text{fb}}$, and $2Q_L^{\text{fb}} \leq \alpha_H < \alpha_L$.

Case 2: $\frac{1}{2}\alpha_H < Q_L^{\text{fb}} < \frac{1}{2}\alpha_L$.

Subcase 2a: $\frac{1}{2}\alpha_H < Q_H^{\text{se}} \leq \frac{1}{2}\alpha_L$. Inequality (124) becomes

$$(\alpha_L - Q_L^{\text{fb}})Q_L^{\text{fb}} \geq (\alpha_L - Q_H^{\text{se}})Q_H^{\text{se}}, \tag{130}$$

which is a contradiction because $(\alpha_L - Q)Q$ is strictly increasing for $Q \leq \frac{1}{2}\alpha_L$ and $Q_L^{\text{fb}} < Q_H^{\text{se}} \leq \frac{1}{2}\alpha_L$.

Subcase 2b: $Q_H^{\text{se}} > \frac{1}{2}\alpha_L$. Inequality (124) becomes

$$(\alpha_L - Q_L^{\text{fb}})Q_L^{\text{fb}} \geq \frac{1}{4}\alpha_L^2, \tag{131}$$

which is a contradiction because $\frac{1}{4}\alpha_L^2 = \max_Q(\alpha_L - Q)Q$ and $Q_L^{\text{fb}} < \frac{1}{2}\alpha_L = \arg\max_Q(\alpha_L - Q)Q$. ■

Proof of Corollary 1: Suppose $b_H \geq b^{\varnothing}$. Thus, $b_H \geq \min\{b^0, b^{\varnothing}\} = b^{\text{cr}}$. According to Theorem 1, we have $\mathcal{C}_{\text{B}} = \mathcal{C}_{\varnothing}$. Next, suppose $b_H < b^{\varnothing}$. According to Theorem 1, we have:

(i) If $b_H \leq b^{\text{se}}$, then no SE exists absent blockchain.

(ii) If $b^{\text{se}} < b_H < \min\{b^0, b^{\varnothing}\}$, then $\mathcal{C}_{\text{B}} < \mathcal{C}_{\varnothing}$.

(iii) If $\min\{b^0, b^{\varnothing}\} \leq b_H$, then $\mathcal{C}_{\text{B}} = \mathcal{C}_{\varnothing}$.

This is equivalent to the following:

(i) If $b_H \leq b^{\text{se}}$, then no SE exists absent blockchain.

(ii) If $b^{\text{se}} < b_H < b^0$, then $\mathcal{C}_{\text{B}} < \mathcal{C}_{\varnothing}$.

(iii) If $b^0 \leq b_H$, then $\mathcal{C}_{\text{B}} = \mathcal{C}_{\varnothing}$.

Using the definition of b^{se}, $b_H \leq b^{\text{se}}$ iff $\alpha_H \leq \alpha^{\text{se}}$. Using the definition of b^0 and the proof of Proposition 3, $b_H < b^0$ iff $D_H^{fb} < d$ iff $\left(\alpha_H - \frac{c}{1-b_H}\right) < \left(\alpha_L - \frac{1}{2}\left(c + \frac{c}{1-b_L}\right)\right) \frac{1-b_H}{1-b_L}\frac{b_L}{b_H}$ iff $\alpha_H < \alpha^{\text{cr}}$. Thus, the above subcases (i)-(iii) are equivalent to subcases (i)-(iii) in Corollary 1. ■

Proof of Corollary 2: If the firm can convert input inventory back in cash without any loss, building inventory is cheap talk and the equivalence of two signaling games follows. ■

Proof of Proposition 5: The only non-trivial effect of the fixed and variable costs of inventory signaling is on the applicability of the intuitive criterion to eliminate potential pooling equilibria. Namely, we need to prove that no PE of class ∅-∅ can survive the IC. (The proof that no PE of class Ƀ-Ƀ can survive the IC is a straightforward extension, where the deviations from the PE under consideration are all within inventory signaling and, thus, the cost of transparency becomes irrelevant.) Let $D_P \leq \overline{D}_H$ be any given PE loan. Recall that at a PE, the fair interest, $r(D_P)$, and the value of equity, $V_{i\varnothing}(D_P)$, are given by (91) and (92), respectively. We will show that for any PE loan D_P, there exists an order quantity Q such that the low type would not switch from borrowing D_P to adopting blockchain and ordering Q even if the lender associated this move with the high type, whereas the high type would, i.e.,

$$V_{L\varnothing}(D_P) > V_{L\mathrm{B}}(Q|H) - \Phi, \tag{132}$$

$$\text{and } V_{H\varnothing}(D_P) < V_{H\mathrm{B}}(Q|H) - \Phi, \tag{133}$$

where $V_{i\mathrm{B}}(Q|H)$ is the equity value of type i using blockchain when the lender believes the firm is high type, i.e.,

$$V_{i\mathrm{B}}(Q|H) = \begin{cases} (1-b_i)\left(\left(\alpha_i - Q - \frac{c(1+\phi)}{1-b_H}\right)Q\right) & \text{if } Q \leq \frac{1}{2}\alpha_i, \\ (1-b_i)\left(\frac{1}{4}\alpha_i^2 - \frac{c(1+\phi)}{1-b_H}Q\right) & \text{if } Q > \frac{1}{2}\alpha_i. \end{cases} \tag{134}$$

The existence of Q that satisfies (132) and (133) means that D_P cannot be a PE that survives the IC. In particular, if the lender believes that a firm ordering Q using blockchain is of the low type, the belief does not survive the IC. If the lender believes that a firm ordering Q using blockchain is of the high type, D_P is not an equilibrium at all.) Before finding Q that satisfies (132) and (133), consider q such that

$$V_{L\varnothing}(D_P) = V_{L\mathrm{B}}(q|H) - \Phi, \tag{135}$$

and $V_{L\mathrm{B}}(\quad|H)$ is decreasing at q. There are several cases to consider.

Case 1. Suppose $D_P \leq \frac{1}{2}(\alpha_L - c)c$.

Subcase 1a. If

$$\left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} > \frac{1}{4}\left(\alpha_L - \frac{c(1+\phi)}{1-b_H}\right)^2 - \frac{\Phi}{1-b_L},$$

then (135) has no solution, and any Q satisfies (132). Otherwise, eq. (135) has a solution.

Subcase 1b. If

$$\frac{1}{4}\left(\alpha_L - \frac{c(1+\phi)}{1-b_H}\right)^2 - \frac{\Phi}{1-b_L} \geq \left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} \geq \frac{1}{4}\alpha_L\left(\alpha_L - 2\frac{c(1+\phi)}{1-b_H}\right) - \frac{\Phi}{1-b_L},$$

then eq. (135) becomes

$$\left(\alpha_L - c - \frac{D_P}{c} - \frac{hb_Hc+(1-h)b_Lc}{h(1-b_H)+(1-h)(1-b_L)}\right)\frac{D_P}{c} = \left(\alpha_L - q - \frac{c(1+\phi)}{1-b_H}\right)q - \frac{\Phi}{1-b_L}, \tag{136}$$

and its larger root satisfies $q \leq \frac{1}{2}\alpha_L$. Because $V_{L\mathrm{B}}(\quad|H)$ is decreasing beyond this q, any $Q > q$ satisfies condition (132).

Subcase 1c. If

$$\left(\alpha_L - c - \tfrac{D_P}{c} - \tfrac{hb_H c+(1-h)b_L c}{h(1-b_H)+(1-h)(1-b_L)}\right)\tfrac{D_P}{c} < \frac{1}{4}\alpha_L\left(\alpha_L - 2\tfrac{c(1+\phi)}{1-b_H}\right) - \tfrac{\Phi}{1-b_L},$$

then eq. (135) becomes

$$\left(\alpha_L - c - \tfrac{D_P}{c} - \tfrac{hb_H c+(1-h)b_L c}{h(1-b_H)+(1-h)(1-b_L)}\right)\tfrac{D_P}{c} = \frac{1}{4}\alpha_L^2 - \tfrac{c(1+\phi)}{1-b_H}q - \tfrac{\Phi}{1-b_L}, \tag{137}$$

and its unique root satisfies $q > \frac{1}{2}\alpha_L$. Because $V_{LB}(\quad|H)$ is decreasing beyond this q, any $Q > q$ satisfies condition (132).

Case 2. Suppose $D_P > \frac{1}{2}(\alpha_L - c)\,c$.

Subcase 2a. If

$$\frac{1}{4}(\alpha_L - c)^2 - \tfrac{hb_H D_P+(1-h)b_L c\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} > \frac{1}{4}\left(\alpha_L - \tfrac{c(1+\phi)}{1-b_H}\right)^2 - \tfrac{\Phi}{1-b_L},$$

then (135) has no solution, and any Q satisfies (132). Otherwise, eq. (135) has a solution.

Subcase 2b. If

$$\frac{1}{4}\left(\alpha_L - \tfrac{c(1+\phi)}{1-b_H}\right)^2 - \tfrac{\Phi}{1-b_L} \geq \frac{1}{4}(\alpha_L - c)^2 - \tfrac{hb_H D_P+(1-h)b_L c\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} \geq \frac{1}{4}\alpha_L\left(\alpha_L - 2\tfrac{c(1+\phi)}{1-b_H}\right) - \tfrac{\Phi}{1-b_L},$$

eq. (135) becomes

$$\frac{1}{4}(\alpha_L - c)^2 - \tfrac{hb_H D_P+(1-h)b_L c\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} = \left(\alpha_L - q - \tfrac{c(1+\phi)}{1-b_H}\right)q - \tfrac{\Phi}{1-b_L}, \tag{138}$$

and its larger root satisfies $q \leq \frac{1}{2}\alpha_L$. Because $V_{LB}(\quad|H)$ is decreasing beyond this q, any $Q > q$ satisfies condition (132).

Subcase 2c. If

$$\frac{1}{4}(\alpha_L - c)^2 - \tfrac{hb_H D_P+(1-h)b_L c\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} < \frac{1}{4}\alpha_L\left(\alpha_L - 2\tfrac{c(1+\phi)}{1-b_H}\right) - \tfrac{\Phi}{1-b_L},$$

eq. (135) becomes

$$\frac{1}{4}(\alpha_L - c)^2 - \tfrac{hb_H D_P+(1-h)b_L c\frac{1}{2}(\alpha_L-c)}{h(1-b_H)+(1-h)(1-b_L)} = \frac{1}{4}\alpha_L^2 - \tfrac{c(1+\phi)}{1-b_H}q - \tfrac{\Phi}{1-b_L}, \tag{139}$$

and its unique root satisfies $q > \frac{1}{2}\alpha_L$. Because $V_{LB}(\quad|H)$ is decreasing beyond this q, any $Q > q$ satisfies condition (132).

So far, we found a set of Q's that satisfy condition (132) in each of the above cases. Next, we will find Q's that also satisfy (133) in each of these cases.

Regarding Case 1. When $\frac{1}{2}(\alpha_L - c) > \frac{D_P}{c}$, then using (91) and (92), we have

$$V_{H\varnothing}(D_P) = (1 - b_H)\left(\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c}\right). \tag{140}$$

Regarding Subcase 1a. We show that condition (133) is satisfied by $Q^* = \arg\max_Q V_{H\not{B}}(Q|H)$, i.e., $V_{H\varnothing}(D_P) < \max_Q V_{H\not{B}}(Q|H) - \Phi$. Using (140) and (134), this inequality becomes

$$\begin{aligned}
\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} &< \max_Q \left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - Q\right) Q - \tfrac{\Phi}{1-b_H} \\
\Leftrightarrow \left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} &< \frac{1}{4}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right)^2 - \tfrac{\Phi}{1-b_H},
\end{aligned}$$

which follows from eq. (24).

Regarding Subcase 1b. We need to consider two situations.

1b(i). Suppose $q < \arg\max_Q V_{H\not{B}}(Q|H)$. Condition (133) is satisfied by $Q^* = \arg\max_Q V_{H\not{B}}(Q|H)$, i.e., $V_{H\varnothing}(D_P) < \max_Q V_{H\not{B}}(Q|H) - \Phi$, which we already proved above.

1b(ii). Suppose $q \geq \arg\max_Q V_{H\not{B}}(Q|H)$. We will show that condition (133) is satisfied by $Q = q + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\not{B}}(q|H) - \Phi$. Because $q < \frac{1}{2}\alpha_L < \frac{1}{2}\alpha_H$, the desired inequality can be written as

$$\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} < \left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - q\right) q - \tfrac{\Phi}{1-b_H}. \tag{141}$$

To prove this inequality, we need to consider two cases.

1b(ii)A. Suppose $\frac{D_P}{c} \leq q$. Inequality (141) follows from condition (136) and some algebra.

1b(ii)B. Suppose $\frac{D_P}{c} > q$. Using (24), inequality (141) is true if

$$\begin{aligned}
&\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} + \frac{1}{4}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right)^2 \\
< \;&\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - q\right) q + \frac{1}{4}\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)^2.
\end{aligned} \tag{142}$$

Because $\frac{D_P}{c} > q \geq \arg\max_Q V_{H\not{B}}(Q|H) = \frac{1}{2}\left(\alpha_H - \frac{c(1+\phi)}{1-b_H}\right) > \frac{1}{2}\left(\alpha_H - \frac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)$, inequality (142) is true if

$$\begin{aligned}
&\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - q\right) q + \frac{1}{4}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right)^2 \\
< \;&\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - q\right) q + \frac{1}{4}\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)^2 \\
\Leftrightarrow \;&\frac{1}{4}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right)^2 < \frac{1}{4}\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)^2 + \left(\tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{c(1+\phi)}{1-b_H}\right) q.
\end{aligned} \tag{143}$$

Because $\frac{c}{h(1-b_H)+(1-h)(1-b_L)} > \frac{c(1+\phi)}{1-b_H}$ and $q \geq \frac{1}{2}\left(\alpha_H - \frac{c(1+\phi)}{1-b_H}\right)$, inequality (143) is true if

$$\frac{1}{4}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right)^2 < \frac{1}{4}\left(\alpha_H - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)^2 + \left(\tfrac{c}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{c(1+\phi)}{1-b_H}\right)\frac{1}{2}\left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H}\right),$$

which simplifies into $\left(\frac{c}{h(1-b_H)+(1-h)(1-b_L)} - \frac{c(1+\phi)}{1-b_H}\right)^2 > 0$.

Regarding Subcase 1c. We need to consider two situations.

1c(i). Suppose $q < \arg\max_Q V_{H\text{B}}(Q|\,H)$. Condition (133) is satisfied by $Q^* = \arg\max_Q V_{H\text{B}}(Q|\,H)$, i.e., $V_{H\varnothing}(D_P) < \max_Q V_{H\text{B}}(Q|\,H) - \Phi$, which we already proved above.

1c(ii). Suppose $q \geq \arg\max_Q V_{H\text{B}}(Q|\,H)$. We will show that condition (133) is satisfied by $Q = q + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\text{B}}(q|\,H) - \Phi$. To evaluate $V_{H\text{B}}(q|\,H)$, we need to consider two situations.

1c(ii)A. Suppose $\frac{1}{2}\alpha_L < q \leq \frac{1}{2}\alpha_H$. The desired inequality becomes

$$\left(\alpha_H - \tfrac{D_P}{c} - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)\tfrac{D_P}{c} < \left(\alpha_H - q - \tfrac{c(1+\phi)}{1-b_H}\right)q - \tfrac{\Phi}{1-b_H}. \tag{144}$$

Using (137), inequality (144) is true if

$$\frac{1}{4}\alpha_L^2 + (\alpha_H - \alpha_L)\tfrac{D_P}{c} < (\alpha_H - q)\,q,$$

which follows from the facts that $\frac{D_P}{c} \leq \frac{1}{2}(\alpha_L - c)$ and $\frac{1}{2}\alpha_L < q \leq \frac{1}{2}\alpha_H$.

1c(ii)B. Suppose $q > \frac{1}{2}\alpha_H$. The desired inequality becomes

$$\left(\alpha_H - \tfrac{D_P}{c} - \tfrac{c}{h(1-b_H)+(1-h)(1-b_L)}\right)\tfrac{D_P}{c} < \frac{1}{4}\alpha_H^2 - \tfrac{c(1+\phi)}{1-b_H}q - \tfrac{\Phi}{1-b_H}. \tag{145}$$

Using (137), inequality (145) is true if $\frac{D_P}{c} < \frac{1}{4}(\alpha_H + \alpha_L)$, which follows from the fact that $D_P \leq \frac{1}{2}(\alpha_L - c)\,c$.

Regarding Case 2. When $\frac{1}{2}(\alpha_L - c) \leq \frac{D_P}{c}$, then using (91) and (92), we have

$$V_{H\varnothing}(D_P) = (1-b_H)\left(\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{hb_Hc\frac{D_P}{c} + (1-h)b_Lc\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)}\right). \tag{146}$$

Regarding Subcase 2a. We show that condition (133) is satisfied by $Q = D_P/c$, i.e., $V_{H\varnothing}(D_P) < V_{H\text{B}}\left(\frac{D_P}{c}\middle|\,H\right) - \Phi$. Using (146) and (134), the desired inequality becomes

$$\begin{aligned}\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{hb_Hc\frac{D_P}{c} + (1-h)b_Lc\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)} \quad &< \quad \left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{\Phi}{1-b_H} \\ \Leftrightarrow \left(\tfrac{b_H+\phi}{1-b_H} - \tfrac{hb_H}{h(1-b_H)+(1-h)(1-b_L)}\right)D_P \quad &< \quad \tfrac{(1-h)b_Lc\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)} - \tfrac{\Phi}{1-b_H}.\end{aligned}$$

Since $D_P \leq \overline{D}_H = \frac{c}{2}(\alpha_H - c)$, it is enough to show this for $D_P = \frac{c}{2}(\alpha_H - c)$, in which case the inequality simplifies into (23).

Regarding Subcase 2b. We need to consider two situations.

2b(i). Suppose $q \leq D_P/c$. Condition (133) is satisfied by $Q = D_P/c + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\text{B}}\left(\frac{D_P}{c}\middle|\,H\right) - \Phi$, which we already proved above.

2b(ii). Suppose $q > D_P/c$. We will show that condition (133) is satisfied by $Q = q + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\text{B}}(q|\,H) - \Phi$. Because $q \leq \frac{1}{2}\alpha_L < \frac{1}{2}\alpha_H$, the desired inequality can be written as

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{hb_Hc\frac{D_P}{c} + (1-h)b_Lc\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)} < \left(\alpha_H - \tfrac{c(1+\phi)}{1-b_H} - q\right)q - \tfrac{\Phi}{1-b_H}.$$

Using (138), the above inequality becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} + \alpha_L q - \tfrac{\Phi}{1-b_L} < \alpha_H q - \frac{\Phi}{1-b_H} + \frac{1}{4}\left(\alpha_L - c\right)^2. \tag{147}$$

Because $\left(\alpha_L - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} < \tfrac{1}{4}\left(\alpha_L - c\right)^2$ for any D_P, inequality (147) is true if

$$\alpha_L\left(q - \tfrac{D_P}{c}\right) - \tfrac{\Phi}{1-b_L} < \alpha_H\left(q - \tfrac{D_P}{c}\right) - \tfrac{\Phi}{1-b_H},$$

which is clearly true.

Regarding Subcase 2c. We need to consider two situations.

2c(i). Suppose $q \leq D_P/c$. Condition (133) is satisfied by $Q = D_P/c + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\mathrm{B}}\left(\tfrac{D_P}{c}\middle| H\right) - \Phi$, which we already proved above.

2c(ii). Suppose $q > D_P/c$. We will show that condition (133) is satisfied by $Q = q + \epsilon$, i.e., $V_{H\varnothing}(D_P) < V_{H\mathrm{B}}(q|\,H) - \Phi$. To evaluate $V_{H\mathrm{B}}(q|\,H)$, we need to consider two situations.

2c(ii)A. Suppose $q \geq \frac{1}{2}\alpha_H$. The desired inequality becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{hb_H c\frac{D_P}{c} + (1-h)b_L c\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)} < \frac{1}{4}\alpha_H^2 - \tfrac{c(1+\phi)}{1-b_H}q - \tfrac{\Phi}{1-b_H}. \tag{148}$$

Using (139), inequality (148) is true if

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} + \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c < \frac{1}{4}\alpha_H^2,$$

which follows from $\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} \leq \tfrac{1}{4}\left(\alpha_H - c\right)^2$.

2c(ii)B. Suppose $q < \frac{1}{2}\alpha_H$. The desired inequality becomes

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} - \tfrac{hb_H c\frac{D_P}{c} + (1-h)b_L c\frac{1}{2}(\alpha_L - c)}{h(1-b_H)+(1-h)(1-b_L)} < \left(\alpha_H - q - \tfrac{c(1+\phi)}{1-b_H}\right)q - \tfrac{\Phi}{1-b_H}. \tag{149}$$

Using (139), inequality (149) is true if

$$\left(\alpha_H - c - \tfrac{D_P}{c}\right)\tfrac{D_P}{c} < \left(\alpha_H - q\right)q - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c. \tag{150}$$

If $D_P \geq \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c$, inequality (150) follows from the fact that $D_P/c < q < \frac{1}{2}\alpha_H$. Next, suppose that $D_P < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c$. Because $\frac{1}{2}\alpha_L < q < \frac{1}{2}\alpha_H$, in order to show (150), it is enough to show that

$$\left(\alpha_H - c - \frac{D_P}{c}\right)\frac{D_P}{c} < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c. \tag{151}$$

Because $D_P \leq \overline{D}_H = \frac{1}{2}\left(\alpha_H - c\right)c$, there are two possibilities: (a) $D_P \leq \frac{1}{2}\left(\alpha_H - c\right)c < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c$, or (b) $D_P < \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c \leq \frac{1}{2}\left(\alpha_H - c\right)c$. If (a) holds, in order to show (151), it is enough to show that

$$\frac{1}{4}\left(\alpha_H - c\right)^2 < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c. \tag{152}$$

Inequality (152) is equivalent to $\alpha_H - \alpha_L < 2c$, which follows directly from (a). If (b) holds, in order to show (151), it is enough to show that

$$\left(\alpha_H - c - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)\right)\frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right) < \left(\alpha_H - \frac{1}{2}\alpha_L\right)\frac{1}{2}\alpha_L - \frac{1}{2}\left(\alpha_L - \frac{1}{2}c\right)c,$$

which simplifies into $\alpha_H - \alpha_L + \frac{1}{4}c > 0$, which is clearly true. This completes the proof that no PE can survive the IC.

The rest of the result follows from Theorem 1 and the fact that the total payoff of a firm using blockchain strictly decreases in both ϕ and Φ.■

Proof of Proposition 6: We only prove that the LCSE (existence, uniqueness, and firms' actions) of the cash signaling game characterized in Proposition 1 does not change under a general belief structure. The proof for the inventory signaling game follows the same structure and is omitted for brevity.

A. We first prove that if $b_H > b^{\text{se}}$, then $\{D_L^{\text{se}}; D_H^{\text{se}}\}$ characterized in Proposition 1 is the unique LCSE of the cash signaling game under an arbitrary belief structure (25). We know that $\{D_L^{\text{se}}; D_H^{\text{se}}\}$ together with the belief set $[d, \infty)$ is a SE under (25) because the belief set $[d, \infty)$ is a special case of $\mathcal{H}_\varnothing$. To demonstrate that $\{D_L^{\text{se}}; D_H^{\text{se}}\}$ are the *unique least-cost* SE actions under (25), we use a proof by contradiction. Suppose there exists some $\{\mathbf{D}^*, \mathcal{H}_\varnothing\}$ that is a SE such that $D_H^* \neq D_H^{\text{se}}$ and

$$V_{H\varnothing}(D_H^*) \geq V_{H\varnothing}(D_H^{\text{se}}). \tag{153}$$

Recall that $D_H^{\text{se}} = \max\left(d, D_H^{\text{fb}}\right)$. If $D_H^{\text{se}} = D_H^{\text{fb}}$, inequality (153) is clearly false. Next suppose that $D_H^{\text{se}} = d > D_H^{\text{fb}}$. Because for any $D > D_H^{\text{se}}$, we have $V_{H\varnothing}(D) < V_{H\varnothing}(D_H^{\text{se}})$, inequality (153) implies that $D_H^* < d$. Clearly, $D_H^* \neq D_L^{\text{fb}}$, and so there are two cases.

A(i) $D_H^* > D_L^{\text{fb}}$. The fact that $\mathcal{H}_\varnothing \supset D_H^*$ where $D_H^* \in (D_L^{\text{fb}}, d)$ implies that $V_{L\varnothing}(D_H^*) > V_{L\varnothing}(D_L^{\text{fb}})$, i.e., the low type has incentive to signal high by choosing D_H^*, and $\mathcal{H}_\varnothing$ cannot be a SE belief set.

A(ii) $D_H^* < D_L^{\text{fb}}$. In this case,

$$V_{i\varnothing}(D) = \begin{cases} (1-b_i)\left((\alpha_i - D/c)D/c - D - D\dfrac{b_H}{1-b_H}\right) & \text{if } D \in \mathcal{H}_\varnothing \\ (1-b_i)\left((\alpha_i - D/c)D/c - D - D\dfrac{b_L}{1-b_L}\right) & \text{o/w.} \end{cases}$$

We have

$$\begin{aligned} V_{H\varnothing}(D_H^*) &\geq V_{H\varnothing}(D_L^{\text{fb}}) \Longrightarrow \\ (1-b_H)\left((\alpha_H - D_H^*/c)D_H^*/c - \frac{D_H^*}{1-b_H}\right) &\geq (1-b_H)\left((\alpha_H - D_L^{\text{fb}}/c)D_L^{\text{fb}}/c - \frac{D_L^{\text{fb}}}{1-b_L}\right) \Longrightarrow \\ (1-b_L)\left((\alpha_L - D_H^*/c)D_H^*/c - \frac{D_H^*}{1-b_H}\right) &> (1-b_L)\left((\alpha_L - D_L^{\text{fb}}/c)D_L^{\text{fb}}/c - \frac{D_L^{\text{fb}}}{1-b_L}\right) \Longrightarrow \\ V_{L\varnothing}(D_H^*) &> V_{L\varnothing}(D_L^{\text{fb}}). \end{aligned}$$

Thus, even in this case, the low type has incentive to signal high by choosing D_H^*, and $\mathcal{H}_\varnothing$ cannot be a SE belief set.

B. Next, we prove that if $b_H \leq b^{\text{se}}$, then the cash signaling game under an arbitrary belief structure (25) has no SE. We do so again by contradiction. Suppose $\{\mathbf{D}^*, \mathcal{H}_\varnothing\}$ is a SE. There are two cases.

B(i) $D_H^* > D_L^{\text{fb}}$. We know from the proof of Proposition 1 that the low type would prefer to borrow any $D > D_L^{\text{fb}}$ if it meant being perceived as high to borrowing D_L^{fb}, so $D_H^* \notin \mathcal{H}_\varnothing$, which is a contradiction.

B(ii) $D_H^* < D_L^{\text{fb}}$. The same argument as in A(ii) can be made to show that $\mathcal{H}_\varnothing$ cannot be a SE belief set. ■