Discussion Paper Series – CRC TR 224

Discussion Paper No. 138
Project C 03

Can You Trust the Blockchain?
The (limited) Power of Peer-to-Peer Networks for Information Provision

Benedikt Franke [*]
Qi Gao [**]
André Stenzel [***]

November 2019

*Skema Business School - University of C^ote d'Azur, e-mail: benedikt.franke@skema.edu
** University of Mannheim, e-mail: qi.gao@bwl.uni-mannheim.de
*** University of Mannheim & MaCCI, e-mail: andre.stenzel@uni-mannheim.de

Funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) through CRC TR 224 is gratefully acknowledged.

Collaborative Research Center Transregio 224 - www.crctr224.de
Rheinische Friedrich-Wilhelms-Universität Bonn - Universität Mannheim

Can You Trust the Blockchain? The (limited) Power of Peer-to-Peer Networks for Information Provision[*]

Benedikt Franke[†]
Skema Business School

Qi Gao[‡]
University of Mannheim

André Stenzel[§]
University of Mannheim & MaCCI

November, 2019.

Abstract

We investigate the potentials and limits of privacy-preserving blockchain technology for the generation of information. In our model, heterogeneous firms can rely on traditional institutions or adopt a blockchain to inform the capital market. The blockchain leverages its peer-to-peer structure and disseminates aggregate information while ensuring the privacy of individual data entries. Within this system, firm-specific information provision depends on two critical factors: (i) the blockchain's fit for analyzing a given firm's data, and (ii) its reach into the economy as provided by the proportion of firms adopting the blockchain in equilibrium. The technology can improve information provision in two ways. The adoption decision itself may serve as a credible signal of a firm's valuation, and the blockchain may generate more information than traditional institutions when its reach is sufficiently high. However, we characterize an equilibrium in which high-value and low-value firms are present both inside and outside the blockchain, which limits both channels' ability to generate information. We show that the information provision can even fall below the benchmark case in which blockchain technology is not available.

JEL-Classification: D21, D40, M41, M48
Keywords: Adoption, blockchain, disclosure, information provision, peer-to-peer network

[*] We thank Anton Sobolev and seminar participants at the University of Bonn, Skema Business School, the University of Graz, and the University of Mannheim for their helpful comments and suggestions. Gao gratefully acknowledges funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) via TRR 266. Stenzel gratefully acknowledges funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) via CRC TR 224 (Project C03).

[†] Skema Business School – University of Côte d'Azur, e-mail: benedikt.franke@skema.edu.

[‡] University of Mannheim, e-mail: qi.gao@bwl.uni-mannheim.de

[§] University of Mannheim and MaCCI, e-mail: andre.stenzel@uni-mannheim.de

1 Introduction

The efficiency of financial markets hinges on investors' access to trustworthy information about the economic fundamentals of their investment opportunities. Recent innovations in computer science fuel the belief that new technologies can enhance the provision of such information. A prime example is the emerging technology behind blockchain, which is openly advertised as a "trust machine".[1] In this study, we investigate the potentials and limits of privacy-preserving blockchain technology to generate information for capital market participants.

We propose a model in which firms can adopt a privacy-preserving blockchain to generate information about firms' fundamentals. Crucially, the technology operates without revealing sensitive data about individual transactions or investments to competitors or the general public. Such private blockchains allow for restrictions in read and write permissions while still taking advantage of the peer-to-peer capabilities offered by the technology. This is in contrast to public blockchains, such as the blockchain behind the popular cryptocurrency Bitcoin, that make all data accessible, rendering them not suitable for settings in which firms face disclosure costs, deal with sensitive information, or have to consider legal issues concerning data privacy.[2] We demonstrate that privacy-preserving blockchains have the potential to provide trustworthy information about firms' fundamentals. However, it is not a given that this potential is realized.

In our model, heterogeneous firms choose between relying on traditional institutions or adopting a privacy-preserving blockchain for information provision. Firms may differ along two dimensions. They can be of high or low value, and exhibit a good or bad fit vis-a-vis the blockchain's ability to analyze a firm's data. Both traditional institutions and the blockchain generate a signal about a firm's value, which becomes available to the capital market. Outside the blockchain, the informativeness of the signal is fixed and type-independent. In contrast, inside the blockchain, the strength of the signal is firm-specific and depends on (i) the blockchain's *reach*, which is determined by the extent to which it is adopted, and (ii) the aforementioned *fit*. Importantly, firms' adoption decisions depend on the blockchain's firm-specific and endogenous relative strength compared to the traditional institutions.

Our setting gives rise to two potential channels for the blockchain to inform investors. First, the adoption decision itself may serve as a credible signal about a firm's valuation. Second, the blockchain may exceed the ability of traditional institutions in informing the

[1] See, The Economist (2015); Wall Street Journal (2016); Dow Jones Newswires (2018); The New York Times (2018).

[2] Bitcoin is often described as anonymous as it is possible to send and receive coins without any identifying information. Instead, sending and receiving happens under a pseudonym, which also means that perfect anonymity is not possible or at least complicated to achieve.

market about a firm's value due to the endogenous strength of its peer-to-peer capabilities. However, we provide conditions such that neither channel works well. Specifically, we characterize necessary and sufficient conditions for an equilibrium in which a mixture of low-value and high-value firms is present both inside and outside the blockchain. This implies that neither the signaling channel – due to the mix of firms both inside and outside – nor the information provision channel – due to limited adoption – can fully resolve the information asymmetry regarding firms' valuations. Importantly, we show that this equilibrium can lead to less information being provided to investors, as evidenced by the average mispricing in the capital market. Moreover, the more scalable the technology is, that is, the fewer firms are necessary for the blockchain's peer-to-peer capabilities to be efficient, the more likely it is that the equilibrium materializes. Our results highlight that blockchain technology does not unambiguously enhance the provision of trustworthy information, and might not necessarily be able to deliver on its promises.

From a business perspective, blockchain technology is envisioned to disrupt the fields of accounting, finance, and auditing (e.g., Dai and Vasarhelyi, 2017; Yermack, 2017; Cong and He, 2019; Cong et al., 2019; Cao et al., 2019). According to a recent survey by PwC, four out of five executives around the world (84%) report having blockchain initiatives underway, with a quarter of these having blockchain implementations live or pilot projects running. Innovations based on blockchain technology are close to seeing a more wide-spread dissemination, with the potential implications being of major interest to firms, investors, and regulators (Deloitte, 2018; KPMG, 2018; PwC, 2018). However, research on how fundamental traits of the technology affect its ability to deliver the desired outcomes – such as the stated improved access to trustworthy information for investors – is scarce.

At its core, a blockchain is a decentralized peer-to-peer network that maintains a continuously growing list of data records. All entries are cryptographically secured, and thus hardened against tampering and undocumented revision. While public blockchains achieve these features by distributing all data among participants, there are limits to how much information firms are willing or legally allowed to share. However, recent advances in cryptography enable privacy-preserving blockchains that take advantage of the technology without sacrificing data privacy.[3] For instance, private blockchains allow setting read and write permissions so that each participating firm could add data while being unable to see other participants' entries.[4] The system may still execute algorithms that can access all data available on the blockchain without revealing individual (sensitive) entries. As such, privacy-preserving blockchains offer a potential added value for providing

[3] Like public blockchains, private blockchains can feature a distributed infrastructure for data distribution, encryption, immutability, and privacy. However, access to the blockchain requires to be permitted, and they come without the consensus protocols as usually employed in public or federated blockchains.

[4] Alternatively, firms could run a privacy-ensuring sidechain in parallel to their primary blockchains or existing IT-infrastructures and executes task independently from the primary data structure.

information. They can leverage the blockchain's peer-to-peer structure and disseminate resulting *aggregate* information while ensuring privacy of *individual* data entries.

A prominent example are verification algorithms, such as zero-knowledge-proof protocols (e.g., Dai and Vasarhelyi, 2017; Wang and Kogan, 2018; Cao et al., 2019; EY, 2019).[5] These protocols verify business transactions based on the available data of all firms subscribed to a blockchain without sharing the underlying data itself and thus without revealing sensitive information in the process. Similarly, a blockchain can host machine learning algorithms for enhanced analytics that do not require pooling the data of participants (e.g., Vasarhelyi et al., 2015; Xu et al., 2015; EY, 2018).[6]

However, such tools, while potentially powerful, face inherent obstacles, which may inhibit their overall efficiency in providing information. Some business transactions result in recordings or data entries that are inherently difficult to analyze for a peer-to-peer mechanism.[7] As a brief example, cash-based transactions can in principle be verified by directly comparing the corresponding records of involved firms. In contrast, accrual-based business transactions like impairments are inherently challenging for such a system as they may lack a counter-party. Similar arguments apply to machine learning or other mechanisms. While the blockchain can enhance data analytics for more standardized investments for which various firms provide relevant data input, more idiosyncratic investments would suffer from intrinsic data limitations.

These considerations highlight two essential drivers resulting in a firm-specific degree to which the blockchain is able to provide information. First, the blockchain's ability to provide information depends on its reach, that is, its overall adoption. To exemplify this, suppose that only one of two firms involved in a cash transaction commits to the blockchain. The algorithm cannot access the data of both counter-parties and is hence unable to verify the business transaction via a direct peer-to-peer matching. In the case of machine learning, a more extensive coverage of firms implies more data points for the algorithm to analyze, improving its estimation capabilities. Essentially, the degree to which the blockchain is able to generate information depends on the endogenous adoption decisions of all firms. Second, as firms are heterogeneous in their activities, so is the fit, that is, the degree to which a peer-to-peer algorithm is able to generate information. In

[5] Several variations of zero-knowledge-proof protocols exist or are under development. For example, the cryptocurrency Zcash uses the zk-SNARKS protocol (*zero-knowledge succinct non-interactive argument of knowledge*) allowing one party to prove the validity of a transaction without releasing any sensitive information. In April 2019, EY released the second version of the EY Blockchain Analyzer (EY, 2018; EY, 2019). The suite is a proprietary solution enhancing EY's ability to perform an in-depth review of cryptocurrency business transactions, leveraging zero-knowledge proof blockchain transaction technology. Similar tools are used by the Dutch bank ING to validate customer information (Allision, 2018).

[6] For instance, the EY Blockchain Analyzer was designed to help audit teams in gathering transaction data from a blockchain and performing statistical analyses, such as identifying outliers (EY, 2018).

[7] Throughout the paper, we refer to a business transaction as an activity or event that affects the economic value of an entity. Moreover, in principle, a business transaction should concern at least one of the accounting elements – assets, liabilities, capital, income, or expenses.

our examples, the fit would be better for a firm with more cash-based transactions, and worse for a firm engaging in highly specific niche investments.[8] While the fit is determined by a firm's type, the reach and the overall firm-specific strength of the blockchain are endogenous.

A given firm's adoption decision depends on whether it seeks or hides from information provision, and the relative strength of the blockchain vis-a-vis traditional institutions. For instance, auditors, rating agencies, or analysts provide information by offering an opinion on a firm's economic situation based on their expertise and access to private information. In contrast, the blockchain makes use of all the available data in the system to learn about each firm's fundamentals in a privacy-preserving way. Given the blockchain's endogenous strength, it is ex-ante not clear which mechanism better informs investors.

We address these considerations by proposing a model in which heterogeneous firms can adopt a privacy-preserving blockchain that provides a signal of endogenous and firm-specific strength about participating firms' valuations. There are four types of firms in the model economy. Each firm is characterized by its value, which can be either high or low, and the blockchain's fit for analyzing a firm's data, which can be good or bad. After privately observing their type, firms simultaneously decide about joining the blockchain or abstaining and relying on traditional institutions.[9]

Inside the blockchain, the system automatically evaluates all participating firms while ensuring the privacy of individual records. We represent the information generated by this mechanism via a message sent to the public that either contains a firm's actual value or no information. The probability that a firm's value is correctly revealed – synonymous with the informativeness of the blockchain's signal – is endogenous and firm-specific, and depends on the fit and reach of the blockchain. Naturally, the information provision about a given firm improves the better the fit and the more extensive the reach of the blockchain. Outside the blockchain, a similar message is generated, with a firm's actual value being revealed with an exogenous probability shared by all firms. This information generation represents the average capabilities of all non-blockchain mechanisms and institutions that can provide information about a firm. It also implicitly incorporates a comparative advantage of traditional institutions in assessing transactions or investments that are inherently challenging to evaluate for the blockchain. Both systems come at a fixed cost, and the blockchain can either be costlier or cheaper than traditional institutions.

Firms aim to maximize their perceived valuation in the capital market. Naturally, high-value firms seek information provision to separate from low-value firms, while low-

[8] We provide a more detailed illustration of using privacy-preserving blockchain technology to generate information in Appendix A.

[9] It is in principle also possible to adopt a hybrid system where the blockchain is used on top of the traditional institutions. While we focus on the blockchain being a rival to existing institutions, our model is also able to speak to this scenario (see the end of Section 3).

value firms attempt to hide and pool with high-value firms (as in Akerlof, 1970; Verrecchia, 1983; Dye, 1985; Jung and Kwon, 1988). The availability of the blockchain allows for information provision via two channels. First, it is possible that information is revealed via the adoption decisions. If only high-value firms adopt (abstain from) the blockchain technology, observing the adoption decisions provides investors with perfect information about the firms' values. Second, investors observe the signals provided by the blockchain and traditional institutions. If the former is widely adopted, its information provision can exceed that of traditional institutions. However, the realization of this potential for information generation is complicated by low-value firms' incentives to avoid identification.

We start our analysis by considering a benchmark case in which traditional institutions are muted, and only the blockchain can provide information. If adoption costs are sufficiently high, only high-value firms join and separation occurs via the adoption decision. While the limited reach of the blockchain inhibits the signal strength, investors do not need to rely on this information to value firms. As adoption costs decrease, low-value firms with a bad fit increasingly enter the system. While this increases the reach of the blockchain, these firms are not always identified and thus, sometimes pooled with high-value firms. This enables them to recoup the adoption costs in expectation, which would not be the case for their good-fit counterparts who would for a given reach be more likely to be identified by the system. Therefore, low-value firms with good fit only join the blockchain for sufficiently low costs. In this case, the signaling value of the adoption decision becomes close to irrelevant. However, when lowering adoption costs, the blockchain will more extensively provide investors with information as it operates at (close to) peak performance due to its increasing reach. A key driver of the baseline results is that adopting the blockchain always leads to a weakly higher information provision relative to (only) relying on traditional institutions. Notably, the qualitative predictions of this baseline carry over to a setting featuring a hybrid model in which firms choose between solely relying on traditional institutions, or augmenting traditional institutions with an emerging blockchain.

We build on this baseline case by considering a general model in which traditional institutions are informative, and demonstrate the existence of new equilibrium constellations. In particular, we provide necessary and sufficient conditions for an equilibrium in which a mix of high-value and low-value firms is present both inside and outside the blockchain. The equilibrium features a mass of firms adopting the blockchain so that it provides more information relative to traditional institutions for firms with a good fit, while the reverse is true for firms with a bad fit. As a consequence, high-value firms with a good fit join, while high-value firms with a bad fit keep relying on traditional institutions. For low-value firms who seek to avoid information generation, the reverse holds. Moreover, the equilibrium can be sustained both when the blockchain is cheaper and when it is more costly than traditional institutions.

The existence of this equilibrium highlights the potential limits of a privacy-preserving blockchain as it exhibits several undesirable features. Most notably, it does not allow for separation of high-value and low-value firms via the adoption decision as a signaling device, nor via its actual information provision due to the limited reach of the blockchain. Crucially, when we assess the resulting equilibrium information provision, we find that this equilibrium can feature higher average mispricing compared to a setting in which the blockchain is not available. Moreover, the more efficient the blockchain technology is in utilizing firms' data, the more likely it is that the equilibrium materializes. In this regard, our paper can be seen as a warning sign. While we do not dispute the advantages a privacy-preserving blockchain can offer, it is not unambiguous that it will always improve the provision of trustworthy information. To the contrary, it can actually be harmful, lowering the degree to which information is provided to market participants, and increasing mispricing.

Our study contributes to the literature on emerging digital technologies in accounting and finance, and specifically to research on the disclosure and informational aspects of blockchain technology. Most studies concentrate on the technical feasibility of blockchains (e.g., Vukolić, 2015; Christidis and Devetsikiotis, 2016; Mingxiao et al., 2017) and discuss various applications, highlighting the potential benefits and obstacles associated with the upcoming technology (e.g., Dai and Vasarhelyi, 2017; Yermack, 2017; Wang and Kogan, 2018; Abadi and Brunnermeier, 2019; Fuller and Markelevich, 2019). These papers provide helpful guidance for how blockchain technology can be implemented in an accounting or finance context. For instance, Dai and Vasarhelyi (2017) emphasize that blockchain could enable a real-time, verifiable, and transparent accounting ecosystem. Specifically, it allows for a timely examination of potential errors or fraud by automatically verifying transactions using data from other participants in the blockchain. The blockchain in our model explicitly features the peer-to-peer capabilities of the technology.

A growing list of studies in finance and economics has started to explore the economic implications of adopting blockchain technology, such as cryptocurrencies or smart contracts (e.g., Fanning and Centers, 2016; Harvey, 2016; Yuan and Wang, 2016; Cong and He, 2019; Cong et al., 2019; Hinzen et al., 2019; Lyandres, 2019). Comparable research in accounting is still scarce. A notable exception is the recent paper by Cao et al. (2019) who focus on permissioned blockchains that auditors can integrate into their audit technology. They examine the effects of auditors' adoption and analyze competition, quality, and client misstatements in the audit market. In their setting, an outside party, such as a regulator, may have to select an equilibrium to ensure lower misstatements, audit effort, and regulatory costs.

We complement their study by investigating the impact of blockchain technology in a disclosure context. Instead of considering the blockchain to be under control by a third party, firms can freely adopt a privacy-preserving blockchain that runs autonomously and without control of a third party to inform the capital market. Firms' adoption decisions further depend on the blockchain's relative strength compared to existing institutions, which in turn determine the strength of the blockchain. Both models highlight the blockchain's peer-to-peer capabilities which imply complementarities in the firms' adoption decisions. However, the focus of the papers is different. We consider blockchain technology as a potential rival which challenges traditional institutions entrusted with informing capital market participants. In this sense, the two studies consider two distinct potential applications of blockchain technology. We document that partial adoption of blockchain technology – and hence a coexistence of the blockchain and traditional institutions – can occur in equilibrium which may overall be detrimental for the information provision to capital market participants. By focusing on firms' adoption decisions and their impact on the endogenous strength of the blockchain, our model also relates to the theoretical literature that takes a more positive approach toward the development of accounting-related institutions (Dye and Sridhar, 2008; Bertomeu and Magee, 2011, 2015a,b; Chen and Yang, 2018).

Lastly, our model speaks to the research concerning firms' ex-ante commitment to a disclosure regime (e.g., Ferreira et al., 2012; Hermalin and Weisbach, 2012; Heinle and Verrecchia, 2015; Edmans et al., 2016). For instance, Heinle and Verrecchia (2015) consider homogeneous firms that can commit to a disclosure regime but ex-post have some discretion about the information being revealed. In contrast, we consider heterogeneous firms that can commit to a regime – the blockchain – characterized by an endogenous probability of revealing a firm's value. The revelation probability depends on a firm's type and the other firms' equilibrium adoption decisions. Firms that do not subscribe to the system face an exogenous probability of being revealed, thereby featuring the possibility that the blockchain regime might provide more information about certain firm types than others, depending on the mix of firms entering the system.

The remainder of this paper is organized as follows. Section 2 describes the setup of the model and introduces the key assumptions. Section 3 contains the analysis of the baseline setting, laying out key mechanisms. In Section 4, we analyze the general model, before discussing the implications in Section 5. Section 6 concludes.

2 Model

Firm types We consider an economy populated by a mass of firms, which we normalize to one. Each firm has a privately known type that is characterized by its value

$v_i \in \{v_L, v_H\}$ and its fit for being analyzed by the blockchain $f_i \in \{f_b, f_g\}$. We denote a firm's type by $\theta_i \in \Theta \equiv \{Hg, Hb, Lb, Lg\}$ and its proportion in the economy by σ_θ. The proportions are common knowledge.

The valuation of a firm is relevant for the capital market. We normalize values to $v_L = 0$ for low-value firms (type L), and $v_H = 1$ for high-value firms (type H). Each firm's fit resembles the blockchain's fundamental ability to assess its data entries. We normalize the mass of data entries of each firm to one. Firms of type g have a good fit with a proportion of analyzable data entries $f_i = f_g$; for simplicity we set $f_g = 1$. For firms of type b, the proportion of in principle analyzable data entires is $f_b = \alpha \in (0, 1)$. In terms of notation, we use v_θ as the value of a firm of type θ, e.g., $v_{Hg} = v_{Hb} = v_H$, and similarly f_θ as the fit of type θ, e.g., $f_{Hb} = f_{Lb} = f_b$.

We impose no restrictions on σ_θ so that any correlation between the two dimensions of the firms' types is possible. Figure 1 summarizes the distribution of the four firm types.

		Fit		
		good	bad	
Firm value	high	σ_{Hg}	σ_{Hb}	σ_H
	low	σ_{Lg}	σ_{Lb}	σ_L
		σ_g	σ_b	

Figure 1: Distribution of firm types

Firm incentives Each firm aims to maximize its market valuation.[10] We denote the price an investor is willing to pay for a share in firm i by p_i and normalize the amount of shares being sold to 1. A firm's true valuation v_i is private information, and a firm cannot credibly inform the market via direct communication. However, information about a firm is transmitted via one of two channels. A firm can either choose to enter a blockchain or alternatively rely on traditional institutions. Both systems are costly, and we denote by $C \in \mathbb{R}$ the private relative cost of adopting the blockchain.[11] We denote by $D_i \in \{0, 1\}$ the decision of firm i to enter the blockchain ($D_i = 1$) or not ($D_i = 0$). Investors observe this decision. In addition, they observe a message generated by either the blockchain or traditional institutions. In this sense, the decision whether to enter the blockchain is synonymous with deciding between committing to one of two disclosure mechanisms.

Information provision Both the blockchain and traditional institutions can inform investors about a firm's value. We formalize the information provision via the informational content of a message m_i that is generated for each firm. The message may

[10] We take this objective as given. It is easy to provide a micro foundation, e.g., by having firms require additional capital that is raised via an equity issuance.

[11] For $C > 0$, adopting the blockchain is costlier relative to relying on traditional institutions. For $C < 0$, in contrast, the blockchain is cheaper and thus offers a cost advantage.

either reveal a firm's valuation, $m_i = v_i$, or be uninformative, $m_i = \emptyset$. The probability of revealing a firm's value represents the informativeness of the respective channel.

Inside the blockchain, the amount of information generated increases in the firm-specific fit and the amount of data available for analysis. This is captured by the blockchain revealing a firm's type with a firm-specific probability η_i, which naturally increases in the firm-specific fit f_i and the (equilibrium) reach of the blockchain ρ. The latter is equal to the equilibrium mass of firms adopting the blockchain, $\int \mathbb{1}_{D_i=1} di$. We let $Pr\{m_i = v_i | D_i = 1\} = \eta_i = \rho \cdot f_i$. For example, if only Hg-type firms and Hb-type firms adopt, an Hg-firm's type is revealed with probability $f_i \cdot \rho = 1 \cdot (\sigma_{Hg} + \sigma_{Hb}) = \sigma_H$, whereas an Hb-firm's type is revealed with probability $f_i \cdot \rho = \alpha \cdot \sigma_H$.

Outside the blockchain, the probability of generating information is independent of a firm's data profile. Traditional institutions provide a credible signal about a firm's type with exogenous probability $Pr\{m_i = v_i | D_i = 0\} = \gamma \in [0, 1)$. This assumption formalizes that traditional institutions may enjoy a comparative advantage in evaluating data entries that are difficult to assess via a privacy-preserving peer-to-peer mechanism.

Investor beliefs and pricing Investors observe a firm's adoption decision along with the generated message. They update their beliefs about a firm's valuation following Bayes' Rule and price firms according to their posteriors. We denote the pooling prices inside and outside the blockchain (equal to the posterior beliefs) following an uninformative message by p^I and p^O, i.e., $p^I = Pr\{v_i = 1 | D_i = 1 \wedge m_i = \emptyset\}$ and $p^O = Pr\{v_i = 1 | D_i = 0 \wedge m_i = \emptyset\}$.

Formally, this gives for the price p_i paid by investors of firm i:

$$p_i(D_i, m_i) = \begin{cases} v_i & \text{if} \quad m_i = v_i \\ p^I & \text{if} \quad m_i = \emptyset \wedge D_i = 1 \\ p^O & \text{if} \quad m_i = \emptyset \wedge D_i = 0 \end{cases} \tag{1}$$

Timing of the game At the beginning of the game, each firm i privately learns its type $\theta_i \in \{Hg, Hb, Lg, Lb\}$; all firms then simultaneously decide whether to join the blockchain ($D_i = 1$) or not ($D_i = 0$). For each firm, a message m_i is generated and made available to investors. The informational content of the message, characterized by the probability of revealing a firm's value, depends on the equilibrium actions of all firms as well as a firm's type (inside the blockchain), and on the strength of the traditional institutions (outside the blockchain), respectively. Subsequently, the market uses all available information, i.e., (i) whether a firm entered the blockchain, and (ii) the message m_i, to price a firm according to the posterior belief that it is of high value. Figure 2 summarizes the timing of the game.

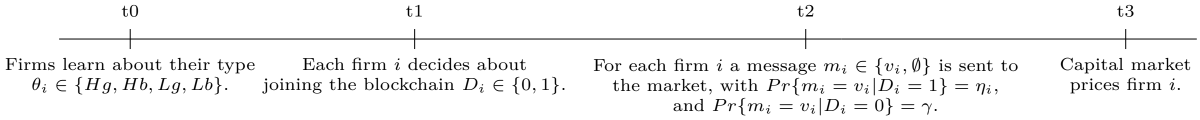

t0
t1
t2
t3
Firms learn about their type $\theta_i \in \{Hg, Hb, Lg, Lb\}$.
Each firm i decides about joining the blockchain $D_i \in \{0, 1\}$.
For each firm i a message $m_i \in \{v_i, \emptyset\}$ is sent to the market, with $Pr\{m_i = v_i | D_i = 1\} = \eta_i$, and $Pr\{m_i = v_i | D_i = 0\} = \gamma$.
Capital market prices firm i.

Figure 2: Timeline of events

Interpretation The model setup captures the fundamental traits of privacy-preserving peer-to-peer mechanisms. In the verification context, the fit parameter f_i represents a firm's proportion of verifiable transactions, such as cash transactions. The blockchain's signal is thus more informative the better the fit, i.e., the more verifiable transactions a firm has in principle. Additionally, informativeness increases the larger the reach, i.e., the more counter-parties are available for verification. Similarly, one can interpret the fit in the estimation context as a firm's proportion of standardized investments that can be assessed more easily via machine-learning. Again, the larger the reach the more relevant data of comparable investments is available to the system, enhancing its ability to successfully analyze the data. To accommodate such interpretations, we only have to assume that the transactions or relevant data records, respectively, are randomly distributed across firms in the model economy.[12]

2.1 Preliminaries

Equilibrium concept We look for symmetric Perfect Bayesian Equilibria, i.e., equilibria in which all firms of type θ play the same strategy. We focus on pure strategy equilibria.[13] To nonetheless formally allow for mixed strategy equilibria, we denote a *candidate strategy profile* by $\{q_{Hg}, q_{Hb}, q_{Lb}, q_{Lg}\}$, where q_θ refers to the probability that a firm of type θ joins the blockchain, $q_\theta = Pr\{D_\theta = 1\}$.

In any equilibrium in which there is a positive mass of firms both inside and outside the blockchain, i.e., where $0 < \sum_\theta q_\theta < 4$, the pooling prices p^I and p^O are determined by Bayes' Rule. We obtain

$$p^I = \frac{\sum_\theta (1-\eta_\theta)\cdot\sigma_\theta\cdot q_\theta\cdot v_\theta}{\sum_\theta (1-\eta_\theta)\cdot\sigma_\theta\cdot q_\theta} = \frac{\sum_\theta (1-\rho t_\theta)\cdot\sigma_\theta\cdot q_\theta\cdot v_\theta}{\sum_\theta (1-\rho t_\theta)\cdot\sigma_\theta\cdot q_\theta}, \tag{2}$$

$$p^O = \frac{\sum_\theta (1-\gamma)\cdot\sigma_\theta\cdot(1-q_\theta)\cdot v_\theta}{\sum_\theta (1-\gamma)\cdot\sigma_\theta\cdot(1-q_\theta)} = \frac{\sum_\theta \sigma_\theta\cdot(1-D_\theta)\cdot v_\theta}{\sum_\theta \sigma_\theta\cdot(1-D_\theta)}. \tag{3}$$

Note that the outside pooling price p^O is independent of γ as the probability of being identified is identical across firm types. If all firms join (do not join), the price outside

[12] We can easily relax this assumption which leaves all our qualitative predictions unchanged.

[13] As will become apparent, mixed strategy equilibria predominantly "fill in the gap" between pure strategy equilibria adding little economic meaning to our main message.

the blockchain (inside the blockchain) is determined by off-path beliefs.[14]

As each individual firm is atomistic, its decision whether to join the blockchain does not affect these pooling prices and is identical across firms of the same type. We can hence write the expected price p_θ^I when joining, and p_θ^O when not joining as

$$\begin{aligned} p_\theta^I = \quad & E[p_i|\theta_i = \theta \wedge D_i = 1] & = \eta_\theta \cdot v_\theta + (1-\eta_\theta) \cdot p^I, \qquad (4) \\ p_\theta^O = \quad & E[p_i|\theta_i = \theta \wedge D_i = 0] & = \gamma \cdot v_\theta + (1-\gamma) \cdot p^O, \qquad (5) \end{aligned}$$

where η_θ, p^I, and p^O are determined by all other firms' equilibrium decisions.

Adoption decisions p_θ^I and p_θ^O are important for a given firm's adoption decision – a firm joins whenever the benefits Δ_i exceed the cost C. Δ_i in turn is fully determined by a firm's type, $\Delta_i = \Delta_\theta = p_\theta^I - p_\theta^O$. Formally,

$$D_i = D_\theta = \begin{cases} 1 & \text{if} \quad \Delta_i > C \\ q_i \in [0,1] & \text{if} \quad \Delta_i = C \\ 0 & \text{if} \quad \Delta_i < C \end{cases}, \qquad (6)$$

where

$$\begin{aligned} \Delta_{Hg} \quad & = \quad \rho - \gamma + (1-\rho)p^I - (1-\gamma)p^O \\ \Delta_{Hb} \quad & = \quad \rho\alpha - \gamma + (1-\rho\alpha)p^I - (1-\gamma)p^O \\ & \text{and} \qquad\qquad\qquad\qquad\qquad\qquad\qquad (7) \\ \Delta_{Lb} \quad & = \quad (1-\rho\alpha)p^I - (1-\gamma)p^O \\ \Delta_{Lg} \quad & = \quad (1-\rho)p^I - (1-\gamma)p^O. \end{aligned}$$

The individual Δ_θ exhibit natural comparative statics. All of them are weakly increasing (decreasing) in the inside (outside) pooling price. For high-value firms, Δ_θ is increasing in ρ and decreasing in γ, while the reverse is true for low-value firms.

Ordering of firms' incentives Before turning to the analysis of potential equilibria, it is helpful to assess the relative incentives of different types to adopt the blockchain. This implies – under certain conditions – an "ordering" in the types' adoption decisions and hence restricts the set of potential equilibria. Naturally, high-value firms seek to be identified whereas low-value firms strive to avoid detection. Hg-type firms for whom the blockchain provides a better fit also have a weakly higher incentive to join the blockchain than Hb-type firms, while the reverse is true between Lg-type and Lb-type firms. These

[14] To characterize the full set of sustainable equilibria, it is hence natural to adopt the most pessimistic off-path beliefs, i.e., $p^I = 0$ ($p^O = 0$), to provide the strongest incentives to deter any deviations.

relations follow because the blockchain's ability to generate information about a firm's type increases in the firm-specific fit. Formally, this is captured by the following Lemma.

Lemma 1 *Hg-type firms benefit weakly more from joining the blockchain than Hb-type firms, while Lg-type firms benefit weakly less than Lb-type firms:*

$$\Delta_{Hg} \geq \Delta_{Hb} \text{ and } \Delta_{Lg} \leq \Delta_{Lb}. \tag{8}$$

Proof. See Appendix B.1. ■

We can also compare the adoption incentives of high-value and low-value firms of the same fit, i.e., Hg-types with Lg-types and Hb-types with Lb-types. These pairs – for given strategies of all other firms – have the same probability of being identified inside and outside the blockchain, respectively. The difference is that if they are identified, high-value types enjoy a valuation of 1, while low-value types are unable to gather funding. Thus, the relative attractiveness of the blockchain is driven by the relative degree of information generation. We obtain

$$\Delta_{Hg} - \Delta_{Lg} = \rho - \gamma \tag{9}$$

$$\Delta_{Hb} - \Delta_{Lb} = \rho\alpha - \gamma. \tag{10}$$

The ordering of adoption incentives between the pairs, as given by (9) and (10), is determined via the equilibrium reach of the blockchain ρ. This exemplifies the complementarity in firms' adoption decisions.

We also need to consider the relative incentives to join the blockchain between Hg-types and Lb-types, and Hb-types and Lg-types, respectively. These incentives depend not only on the primitives α and γ along with the endogenously determined reach ρ, but also on the endogenous pooling price p^I.

$$\Delta_{Hg} - \Delta_{Lb} = \rho - \gamma - (1-\alpha)\rho p^I \tag{11}$$

$$\Delta_{Hb} - \Delta_{Lg} = \rho\alpha - \gamma + (1-\alpha)\rho p^I. \tag{12}$$

The pairwise comparisons provide the basis for the subsequent equilibrium analysis in which we exploit the implied ordering regarding firms' adoption incentives.

3 Baseline setting

We start by investigating a baseline model in which there is no information provision by traditional institutions, i.e., where $\gamma = 0$, and the blockchain is relatively costly, i.e., $C > 0$. The analysis serves two main purposes. First, it allows to carve out key mechanisms driving individual firms' adoption decisions and equilibrium implications. Second, the results carry over to a hybrid setting in which blockchain technology can be added on top of traditional institutions. In terms of interpretation, one can think of situations in which traditional institutions cannot provide additional insights about a firm's transactions, e.g., due to a lack of knowledge or access to private information.

3.1 Analysis

Recall Lemma 1, which states that high-value firms with a good fit face weakly stronger adoption incentives than high-value firms with a bad fit as they seek to be identified. The opposite is true for low-value firms. In addition, if a positive mass of firms adopts the blockchain, information provision is strictly stronger inside the blockchain than outside. As a consequence, high-value firms always face stronger adoption incentives than low-value firms of the same fit. The following Lemma is thus imminent.

Lemma 2 (Ordering Baseline) *When traditional institutions do not provide information, i.e., for $\gamma = 0$, the benefits for type θ of joining the blockchain, Δ_θ, satisfy*

$$\Delta_{Hg} \geq \Delta_{Hb} \geq \Delta_{Lb} \geq \Delta_{Lg}. \tag{13}$$

Moreover, we obtain the following conditions for a strict ordering.

$$\begin{aligned} \rho > 0 \wedge p^I < 1 \quad &\Longrightarrow \quad \Delta_{Hg} > \Delta_{Hb} \\ \rho > 0 \quad &\Longrightarrow \quad \Delta_{Hb} > \Delta_{Lb} \\ \rho > 0 \wedge p^I > 0 \quad &\Longrightarrow \quad \Delta_{Lb} > \Delta_{Lg}. \end{aligned} \tag{14}$$

Proof. Follows from the preceding discussion and Lemma 1 in combination with (9) and (10) with $\gamma = 0$ and $\alpha \in (0, 1)$. ■

The ordering of the relative benefits of joining the blockchain are helpful because of (6). A firm of type θ strictly prefers to join whenever $\Delta_\theta > C$, strictly prefers not to join whenever $\Delta_\theta < C$, and is indifferent otherwise. Given that the relative benefits are ordered, the set of strategy profiles which may constitute equilibria is reduced. For example, whenever a positive fraction of Lb-types joins, i.e., $q_{Lb} \in (0, 1)$, it must be the case that $\Delta_{Lb} = C$ so that Lb-types are indifferent. If this holds in equilibrium, we also have $\rho > 0$ and hence $\Delta_{Hg} \geq \Delta_{HL} \overset{(14)}{>} \Delta_{Lb} = C$, i.e., all high-value types strictly prefer to join the blockchain.

By applying Lemma 2 together with the implications for ρ and p^I from considering a given candidate profile, we obtain Lemma 3.

Lemma 3 (Equilibrium Candidates Baseline) *The following pure-strategy profiles are potential equilibria*

$$\{1,1,1,0\}, \{1,1,0,0\}, \{1,0,0,0\}, \{0,1,0,0\}, \{0,0,0,0\}. \tag{15}$$

Proof. See Appendix B.2. ■

Proposition 1 characterizes conditions on C such that the candidates in (15) can be supported in equilibrium.

Proposition 1 (Equilibria Baseline) *The following pure strategy profiles can be supported in equilibrium depending on the cost C of adopting the blockchain technology.*

(i) For $C \in \left[\underline{C}, \bar{C}\right]$, $\{1,1,1,0\}$ can be supported in equilibrium.

(ii) For $C \in \left[1-\alpha\left(\sigma_{Hb}+\sigma_{Hg}\right), 1\right]$, $\{1,1,0,0\}$ can be supported in equilibrium.

(iii) There exists a unique $C^{\{1,0,0,0\}} \in \left(1-\left(\sigma_{Hg}+\sigma_{Hb}\right), 1\right)$ such that the pure strategy profile $\{1,0,0,0\}$ can be supported in equilibrium, and a unique $C^{\{0,1,0,0\}} \in \left(1-\left(\sigma_{Hg}+\sigma_{Hb}\right), 1\right)$ such that $\{0,1,0,0\}$ can be supported in equilibrium.

$\underline{C}$ and $\bar{C}$ are characterized by

$$\underline{C} = \sigma_{Lg}\frac{\sigma_{Lg}\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}))\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}))(\sigma_{Hb}+\sigma_{Lb})} \tag{16}$$

$$\bar{C} = (1-\alpha(1-\sigma_{Lg}))\frac{\sigma_{Lg}\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}))\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}))(\sigma_{Hb}+\sigma_{Lb})} \tag{17}$$

In addition, non-adoption, i.e., $\{0,0,0,0\}$ can be supported in equilibrium for any $C>0$ with the off-path belief that any any firm that joins the blockchain and is not identified is of low value.

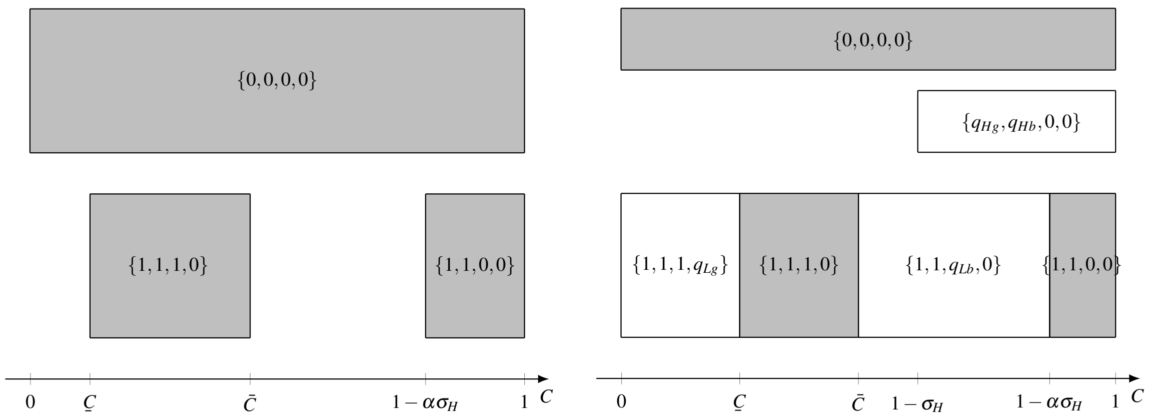
Proof. See Appendix B.3, which also characterizes the mixed-strategy equilibria. ■

Note that the equilibria in which only Hg-types or Hb-types join, respectively, are only sustainable when C satisfies a knife-edge condition. The other pure-strategy equilibria {1,1,1,0} and {1,1,0,0} are sustainable for a range of costs C, with {1,1,1,0} being sustainable for a disjoint and lower cost range than {1,1,0,0}.

3.2 Discussion

Pure strategy equilibria In the baseline, high-value firms have clear incentives to join the blockchain to separate. Low-value firms might enter the system to pool with the high-value firms as long as both the risk of being uncovered and the adoption costs are low enough. Figure 3a summarizes the pure-strategy equilibria across a range of possible costs C.[15]

Figure 3: Illustration of equilibrium constellations



(a) Pure strategies only

(b) Pure and mixed strategies

When adoption costs are low, high-value firms prefer to join the blockchain. Adoption is cheap and not adopting the blockchain indicates firms to be of low value in any equilibrium with a positive mass of adopting firms. Whenever $C \in \left[\underline{C}, \bar{C}\right]$, low-value firms with a bad fit also join in addition to high-value firms. These firms exhibit a sufficiently large probability of not being identified due to the blockchain's limited ability to analyze their data. Investors overprice these pooled low-value firms in the blockchain, compensating them for the adoption cost. Nevertheless, these types in turn increase the blockchain's reach and thus its ability to reveal firms' valuations in equilibrium. The blockchain is thus still capable of providing a largely informative message about a firm's type.

When adoption costs are sufficiently high, i.e., $C \in [1-\alpha\sigma_H, 1]$, the adoption decisions themselves serve as a perfect signal about the firms' value in equilibrium. High-value firms join the blockchain whereas low-value firms remain outside. In this case, separation of value-types is achieved via the adoption but does not rely on the peer-to-peer capabilities. Investors perceive firms inside the blockchain to be of high value irrespective of whether the system reveals their true valuation. Due to limited overall adoption, and thus a limited reach, this only occurs with an intermediate probability. Joining the blockchain is sufficiently costly so that it serves as a credible 'money-burning' signaling device. In this sense, separation could be achieved also by other signals that exhibit differential costs for high-value and low-value firms. As is common in these types of settings, high-value

[15] We abstract from depicting the equilibria characterized in Proposition 1.(iii) as they rely on knife-edge cost conditions.

firms may be adversely affected by the availability of the blockchain. For sufficiently high adoption costs, the gains from being correctly perceived as a high-value firm are more than offset by these costs.[16]

Mixed Strategy Equilibria While we focus on pure strategy equilibria for ease of presentation, we also characterize the emerging mixed-strategy equilibria in which at least one firm plays a mixed-strategy $q_\theta \in (0,1)$ in Appendix B.3. Results are illustrated in Figure 3b. There are two observations to be drawn from this figure. First, mixed-strategy equilibria of the form $\{1,1,1,q_{Lg}\}$ and $\{1,1,q_{Lb},0\}$ are sustainable below the cost range for $\{1,1,1,0\}$ and between the cost ranges for $\{1,1,1,0\}$ and $\{1,1,0,0\}$, respectively. The mixed-strategy equilibria naturally "fill in the gap" between the pure-strategy equilibria. Second, the mixed strategy profile $\{q_{Hg},q_{Hb},0,0\}$ emerges as equilibrium provided that $C > 1-\sigma_H$. Notably, it can overlap with $\{1,1,0,0\}$, $\{1,1,q_{Lb},0\}$, and $\{1,1,1,0\}$. The multiplicity here arises because of the complementarity of the firms' decisions. If all high-value firms join the blockchain, the price outside is low and high-value firms strictly prefer to signal their type by adopting the blockchain, provided that the costs are sufficient to deter *Lb*-types from entering. However, if not all high-value firms join, the price paid outside the blockchain increases and indifference for the high-value firms resulting in a partial adoption can be supported. This directly leads to an additional observation. Indifference between joining and not joining for these types can be supported at lower cost levels than with the pure strategy equilibrium $\{1,1,0,0\}$ because the pooling price p^O outside the blockchain is higher when high-value firms only partially adopt.

Hybrid system Our focus is on a setting in which the emerging blockchain technology rivals the traditional institutions. Nevertheless, our model can also accommodate a hybrid system in which the blockchain technology can be adopted on top of traditional institutions. Specifically, our model can capture such an co-existence by letting the traditional institutions generate information about a firm with exogenous probability γ while still conditioning the information provision on the adoption of the blockchain. To illustrate this, consider the case in which the blockchain sends an informative message with the firm-specific probability $\eta_i' = \gamma + (1-\gamma)\rho f_i$. With this formalization, any information generated by the blockchain would be added on top of the information provision by the traditional institutions, which remain in use even when the blockchain is adopted.

While we abstract from a full analysis of this setting for brevity, the important takeaway is that the qualitative results are identical to those in the baseline. The reason is that such a hybrid system provides weakly more information than the traditional institutions alone, which implies that the ordering of firms' incentives to join the blockchain

[16] For $C \to 1$, the $\{1,1,0,0\}$-equilibrium exists and features $p^I_\theta - C \to 0$ for $\theta \in \{Hg, Hb\}$. If the blockchain were unavailable, these two types would enjoy a strictly positive p^O_θ.

under the baseline remains intact. This can be seen best by defining Δ'_θ analogously to Δ_θ,

$$\begin{aligned}
\Delta'_{Hg} &= \rho(1-\gamma) + (1-\gamma-(1-\gamma)\rho)p^I - (1-\gamma)p^O \\
\Delta'_{Hb} &= \rho\alpha(1-\gamma) + (1-\gamma-(1-\gamma)\rho\alpha)p^I - (1-\gamma)p^O \\
&\text{and} \\
\Delta'_{Lb} &= (1-\gamma-(1-\gamma)\rho\alpha)p^I - (1-\gamma)p^O \\
\Delta'_{Lg} &= (1-(1-\gamma)\rho)p^I - (1-\gamma)p^O.
\end{aligned} \tag{18}$$

To see that this gives rise to the same ordering as in the original case with $\gamma = 0$ (see Lemma 2), observe that

$$\Delta'_{Hg} - \Delta'_{Hb} = \rho(1-\alpha)(1-\gamma)(1-p^I) \geq 0 \tag{19}$$

$$\Delta'_{Hb} - \Delta'_{Lb} = \rho\alpha(1-\gamma) \geq 0 \tag{20}$$

$$\Delta'_{Lb} - \Delta'_{Lg} = \rho(1-\alpha)(1-\gamma)p^I \geq 0. \tag{21}$$

Whenever the blockchain technology is added to traditional institutions by offering firms the decision between a hybrid system and a system exclusively relying on traditional institutions, the same equilibria as in the baseline emerge. In particular, the blockchain needs to be sufficiently costly to ensure full investor trust in the sense of perfect ex-post separation of firms according to their true valuations. However, investors in this case trust in the system, i.e., the signal of adopting it, and not in the informational content of the signal produced by the blockchain.

Interpretation Overall, the blockchain can achieve full separation of value types only through high implementation costs. In this case, the adoption decision itself provides a signal about the firms' values that dominates the actual information provision aspects of the blockchain's peer-to-peer capabilities. For low adoption costs, this cannot be achieved. In equilibrium, low-value firms balance the gains from being overpriced inside the blockchain in case of not being identified with the cost of adoption. Thus, particularly *Lb*-types with a bad firm-specific fit are likely to join. The blockchain in this case has value predominantly through its information provision capabilities, but does not achieve full separation of types ex-post. Information provision through this channel is maximized when adoption costs are sufficiently low so that even *Lg*-types join.

4 Generalized setting

Next, we lift the restriction muting outside information generation. The key difference is that the blockchain may now provide less information to investors than the outside system, which may affect the ordering of the type-specific adoption incentives. For $\gamma = 0$, the blockchain always provides strictly more information – in the sense of a higher probability of an informative message – for all firm types, provided that a positive mass of firms adopts the technology. The ordering captured by Lemma 2 directly follows. For $\gamma > 0$, this is no longer the case. For example, consider that $\gamma = \frac{1}{2}$ and less than half of the firms adopt the blockchain ($\rho < \frac{1}{2}$) in equilibrium. In this case, the probability that a firm's type is revealed is strictly higher outside than inside, irrespective of its type.

To illustrate the implications, consider the baseline case in which adoption costs are intermediate such that $\{1, 1, 1, 0\}$ is an equilibrium for $\gamma = 0$. Here, the blockchain provides an intermediate (type-varying) degree of information provision. Moreover, the outside pooling price is 0 as only low-value Lg-type firms remain outside the blockchain. The pooling price inside is strictly below 1, as is the implied expected payoff for high-value firms. However, for the same adoption cost C, this is no longer an equilibrium once γ increases sufficiently. For γ close to 1, high-value firms have a strict incentive not to adopt the blockchain. Their expected payoff outside approaches their true value of $v_H = 1$ even if they are perceived to be of low-value following a non-informative message. It is possible that high-value firms prefer to remain outside the blockchain as traditional institutions generate more information than the blockchain – non-adoption may thus even serve as a signal of high value.[17] These new tradeoffs provide scope for additional equilibria.

We split the subsequent analysis into the case in which the blockchain is relatively costlier ($C \geq 0$) and relatively cheaper ($C \leq 0$) than the traditional institutions.

4.1 Blockchain costlier than traditional institutions

For $C \geq 0$, the subset of possible pure strategy equilibria is given by the following Lemma.

Lemma 4 (Pure Strategy Equilibrium Candidates for $C \geq 0$) *For $C \geq 0$, any pure strategy equilibrium features a strategy contained in*

$$\{\{1,1,1,1\},\{1,1,1,0\},\{1,1,0,0\},\{1,0,1,0\},\{1,0,0,0\},\{0,1,0,0\},\{0,0,0,0\}\}. \quad (22)$$

[17] It is also possible that $\{0, 0, 1, 1\}$ can be supported in equilibrium, i.e., low-value firms adopt the blockchain while high-value firms rely on traditional institutions. This happens when the blockchain offers a sufficient cost advantage while traditional institutions are sufficiently strong to deter low-value firms from joining and pooling upon not being identified. Conversely, the proportion of low-value firms in the economy cannot be too high so that the blockchain's strength in equilibrium is limited and Hg-type firms do not enter the blockchain to reap the cost advantage while simultaneously being identified sufficiently often for this to be worthwhile.

Proof. See Appendix B.4. ■

As in the baseline case, non-adoption by all firms can always be supported for any $C \geq 0$ by inferring that any firm adopting the blockchain (which occurs off the equilibrium path) is of low value. Additionally, full adoption by all firms is sustainable only for $C = 0$. In general, the candidates in Lemma 4 show that, because adoption of the blockchain is costly vis-a-vis relying on traditional institutions, there is the possibility of adoption being a signal of a firm's value. As such, the candidates tend to have high-value firms adopting the blockchain and low-value firms abstaining. Interestingly, and in contrast to the baseline case, an equilibrium featuring a mix of high-value and low-value firm both inside and outside the blockchain, i.e., $\{1, 0, 1, 0\}$, emerges as a potential candidate. Proposition 2 summarizes the results, focusing on combinations in the γ-C-space that can support the respective candidates.

Proposition 2 (Pure Strategy Equilibria for $C \geq 0$) *The following pure strategy profiles can be supported in equilibrium depending on the adoption cost $C \geq 0$ and the degree of outside information generation γ.*

(i) There exist disjoint regions in the γ-C-space such that $\{1,1,0,0\}$ and $\{1,1,1,0\}$ can be supported in equilibrium. For γ for which both equilibria exist for differential C, $\{1,1,0,0\}$ requires a higher cost range than $\{1,1,1,0\}$.

(ii) If $\frac{\sigma_{Hb}\sigma_{Lb}}{\sigma_{Hg}\sigma_{Lg}} < 1$, there exists a region in the γ-C-space such that $\{1,0,1,0\}$ can be supported in equilibrium. This region is disjoint from the $\{1,1,0,0\}$-region, but may overlap with the $\{1,1,1,0\}$-region.

(iii) There exist (γ,C)-combinations such that $\{1,0,0,0\}$ and $\{0,1,0,0\}$ can be supported in equilibrium. In the γ-C-space, these combinations represent lines which are either identical ($\sigma_{Hg} = \sigma_{Hb}$) or do not cross.

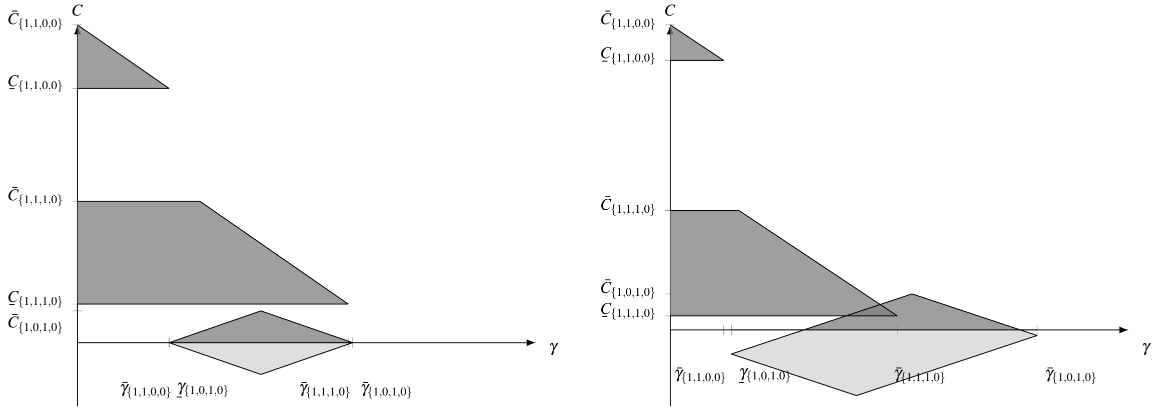
(iv) Irrespective of γ, $\{0,0,0,0\}$ is sustainable in equilibrium for all $C \geq 0$.

(v) For $C = 0$ and $\gamma < \alpha + (1 - \alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}}$, $\{1,1,1,1\}$ can be supported in equilibrium.

Proof. See Appendix B.5. ■

In Figure 4 we depict the regions supporting the equilibria. Note that we do not plot equilibria in which no firm or all firms adopt, respectively, nor equilibria that rely on knife-edge conditions, i.e., {1,0,0,0} and {0,1,0,0}, for ease of exposition. The main takeaway is that the region where adoption leads to perfect separation in the value dimension ({1,1,0,0}) and the region where *Lb*-types adopt in addition to high-value firms ({1,1,1,0}) are supported in equilibrium are disjoint. Moreover, an equilibrium with a mix of high and low value firms present both inside and outside the blockchain ({1,0,1,0}) may be

Figure 4: Illustration of equilibrium constellations



(a) Case 1

(b) Case 2

sustainable provided that sufficiently many good-fit types are present in the economy, i.e., $\frac{\sigma_{Hb}\sigma_{Lb}}{\sigma_{Hg}\sigma_{Lg}} < 1$. The region supporting this equilibrium may overlap with that supporting {1,1,1,0} but not with the perfectly separating {1,1,0,0} equilibrium. Moreover, it requires strictly positive outside information generation γ to "reward" Hb-types for not entering the blockchain, and simultaneously relatively low adoption costs C to incentivize Lb-types to enter and pool with Hg-types upon non-identification. As shown in the illustration, the mixed-type adoption, i.e., {1,0,1,0}, equilibrium may also materialize when adopting the blockchain is cheap relative to relying on traditional institutions. We next turn to the detailed analysis of this scenario.

4.2 Blockchain cheaper than traditional institutions

For $C \leq 0$, we again restrict the set of equilibrium candidates. For ease of interpretation, we denote the blockchain's cost advantage as relative adoption benefits $B \equiv -C \geq 0$.

Lemma 5 (Pure Strategy Equilibrium Candidates for $B \geq 0$) *For $B \geq 0$, any pure strategy equilibrium features a strategy contained in*

$$\{\{1,1,1,1\},\{1,0,1,1\},\{1,0,1,0\},\{0,0,1,1\},\{0,0,1,0\},\{0,0,0,1\},\{0,0,0,0\}\}. \quad (23)$$

Proof. See Appendix B.4. ■

Note that adoption by all firms can be supported for B sufficiently large, while non-adoption by all firms can be sustained provided that B is not too large. Proposition 3 summarizes the results.

Proposition 3 *The following pure strategy profiles can be supported in equilibrium depending on the adoption benefits $B \geq 0$ and the degree of outside information genera-*

tion γ.

(i) There exist regions in the γ-B-space such that {1,0,1,1} and {0,0,1,1} can be supported in equilibrium. These regions always overlap and when both equilibria coexist, {1,0,1,1} pareto-dominates from a firm's perspective. Moreover, there always exist (γ, B)-combinations such that {0,0,1,1} ({1,0,1,1}) can be supported in equilibrium while {1,0,1,1} ({0,0,1,1}) cannot.

(ii) If $\frac{\sigma_{Lb}\sigma_{Hb}}{\sigma_{Hg}\sigma_{Lg}} > \frac{(1-(\sigma_{Hg}+\sigma_{Lb}))^2}{(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))^2}$, there exists a region in the γ-B-space such that {1,0,1,0} can be supported in equilibrium. This region is disjoint from the {0,0,1,1} and {1,0,1,1} regions.

(iii) There exist (γ,B)-combinations such that {0,0,1,0} and {0,0,0,1} can be supported in equilibrium. In the γ-B-space, these combinations represent lines which are either identical ($\sigma_{Lg} = \sigma_{Lb}$) or do not cross.

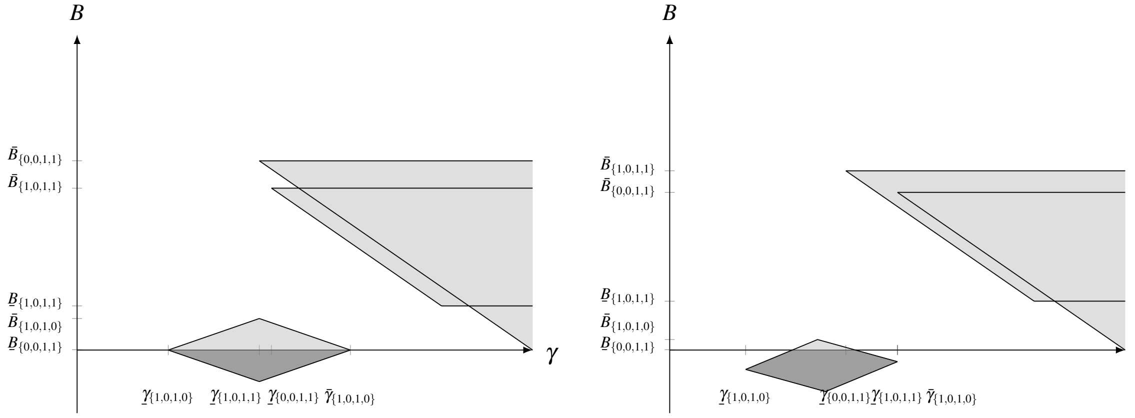
(iv) {1,1,1,1} is sustainable in equilibrium for $B \geq \max\left\{0, \gamma - \left(\alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}}\right)\right\}$.

(v) For (γ, B) such that $B \leq (1-\gamma)\sigma_H$, {0,0,0,0} is sustainable in equilibrium.

Proof. See Appendix B.6. ■

We illustrate the results in Figure 5. We again omit the full adoption and full non-adoption equilibria, as well as those relying on knife-edge conditions. There are three main takeaways. First, because adopting the blockchain provides cost savings, it is the non-adoption that may serve as a costly, and hence, credible signal of high firm value. Consequently, the pure-strategy equilibria for $B \geq 0$ largely mirror those sustainable for $C \geq 0$. Importantly, the equilibrium in which a mix of high and low value firms is present both inside and outside the blockchain can be sustained. Thus, the situation can occur irrespective of the whether the blockchain is more or less costly than traditional institutions. Second, its equilibrium region does not overlap with the other pure strategy equilibria (aside of full adoption or full non-adoption by all firms). However, there is instead substantial overlap between the other two equilibrium regions that feature full ({0,0,1,1}) and partial ({1,0,1,1}) separation along the value dimension. Third, whenever these regions overlap, the equilibrium which does not allow capital market participants to perfectly infer firms' valuations is weakly preferred by all firms. Hg-types prefer to be pooled with low-value firms and receive benefits B over earning a payoff of 1 outside (as they do in the {0,0,1,1}-equilibrium). On-path payoffs of Hb-types are unaffected, and those of low-value firms increase due to the presence of high-value firms in the blockchain.

Figure 5: Illustration of equilibrium constellations



(a) Case 1

(b) Case 2

5 Implications

5.1 An undesirable situation for information provision

A key insight of the generalized setting is the existence of an equilibrium in which high-value and low-value firms are present both inside and outside the blockchain, i.e., the equilibrium characterized by the strategy profile $\{1, 0, 1, 0\}$. In this equilibrium, the reach of the blockchain is intermediate, limiting its ability to generate information about firms. The blockchain can only outperform traditional institutions for which it has a good fit, but underperforms for firms for which it has an inherently bad fit. Moreover, the adoption decisions themselves are not an efficient means of separating high-value and low-value firms because representatives of both types adopt. As such, this equilibrium has the undesirable property that both channels through which the blockchain can inform investors may not be functioning to their full potential.

We next explicitly derive the necessary and sufficient conditions for its existence and assess the implications for the information provision to investors vis-a-vis a setting in which the blockchain technology is not available. Consider said strategy profile $\{1, 0, 1, 0\}$. If the profile is supported in equilibrium, it directly implies for the mass of firms joining the blockchain, ρ, and the pooling prices p^O and p^I that

$$\begin{aligned} \rho &= \sigma_{Hg} + \sigma_{Lb} \\ p^O &= \frac{\sigma_{Hb}}{\sigma_{Hb} + \sigma_{Lg}} \\ p^I &= \frac{(1 - \sigma_{Hg} - \sigma_{Lb})\sigma_{Hg}}{(\sigma_{Hg} + \sigma_{Lb})(1 - \sigma_{Hg} - \alpha\sigma_{Lb})}. \end{aligned} \tag{24}$$

In equilibrium, all firms must weakly prefer their respective adoption choice, leading to

$$\Delta_{Hg} \geq C \wedge \Delta_{Hb} \leq C \wedge \Delta_{Lb} \geq C \wedge \Delta_{Lg} \leq C. \tag{25}$$

For a non-empty range of costs C supporting this equilibrium, we hence require the necessary condition[18]

$$\min\{\Delta_{Hg}, \Delta_{Lb}\} \geq \max\{\Delta_{Hb}, \Delta_{Lg}\} \iff \rho \geq \gamma \geq \rho\alpha. \tag{26}$$

As the reach of the blockchain ρ is determined solely by the proportion of Hg-types and Lb-types, we obtain the necessary condition stated in Lemma 6.

Lemma 6 *To have a non-empty range of costs* C *supporting* $\{1, 0, 1, 0\}$ *as an equilibrium, it needs to hold that*

$$\sigma_{Hg} + \sigma_{Lb} \geq \gamma \geq \alpha \left(\sigma_{Hg} + \sigma_{Lb}\right). \tag{27}$$

Proof. Follows immediately from (26). ■

Lemma 6 highlights an important aspect: The worse the fit for Lb-type and Hb-type firms, i.e., the lower α, the more likely that the undesirable equilibrium can be supported.

For existence, the blockchain needs to provide a more informative signal than traditional institutions only for firms with a good fit. Hg-type firms, who seek informativeness adopt the blockchain, while Lg-type firms, who seek to avoid it, do not. The opposite needs to hold for firms with a bad fit. Consequently, the reach, which in this equilibrium coincides with the proportion of Hg-types and Lb-types, is intermediate. If there is no substantial heterogeneity in terms of the fit (in our model exemplified by α close to 1), there is a limited scope for the equilibrium to be supported. A similar rationale applies whenever traditional institutions are sufficiently strong (in which case Hg-type firms would typically prefer to rely on traditional institutions) or weak (in which case even Hb-type firms would typically prefer to adopt).

While Lemma 6 establishes that (27) is necessary for the strategy profile to be supported in equilibrium, the reverse argumentation implies that it is also sufficient. If (27) holds, there always exists a non-empty range of costs such that $\{1, 0, 1, 0\}$ can be supported in equilibrium.

Proposition 4 *Let* (27) *be satisfied. Then there exist* $\underset{\sim}{C}_b(\gamma), \tilde{C}_b(\gamma)$ *such that* $\{1, 0, 1, 0\}$ *can be supported in equilibrium for* $C \in \left[\underset{\sim}{C}_b(\gamma), \tilde{C}_b(\gamma)\right]$. *In addition,*

(i) $\exists \gamma \in [0, 1] : \tilde{C}_b(\gamma) > 0 \iff \frac{\sigma_{Hb}\sigma_{Lb}}{\sigma_{Hg}\sigma_{Lg}} < 1.$

[18] Note that $\Delta_{Hg} \geq \Delta_{Hb}$ and $\Delta_{Lb} \geq \Delta_{Lg}$ due to Lemma 1. This allows to obtain the equivalence by plugging in (9) and (10).

(ii) $\exists \gamma \in [0,1] : \underset{\sim}{C}_b(\gamma) < 0 \iff \frac{\sigma_{Lb}\sigma_{Hb}}{\sigma_{Hg}\sigma_{Lg}} > \frac{(1-(\sigma_{Hg}+\sigma_{Lb}))^2}{(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))^2}$

Proof. See Appendix B.7. The proofs for (i) and (ii) are contained in Appendix B.5 and Appendix B.6, respectively. ■

Notably, the undesirable equilibrium can be supported both when adopting the blockchain is – from a purely monetary perspective – cheaper than relying on traditional institutions, and when it is more expensive. The specific conditions such that this materializes are given in Proposition 4. Intuitively, a higher propensity of good-fit firms in the economy increases the likelihood that the undesirable equilibrium materializes for positive adoption costs, with the reverse true for negative adoption costs. Our analysis shows that it is not sufficient to, for example, subsidize the adoption of an economy-wide blockchain to rule out that such an undesirable equilibrium with inefficient information generation materializes.

Information provision The equilibrium originates in the heterogeneity in the blockchain's ability to analyze firms, which provides differential adoption incentives to firms with the same value but different fit. As only a subset of firms adopts the blockchain, the technology forfeits some strength of its peer-to-peer capabilities. This can result in some undesirable properties regarding equilibrium information provision to investors.

Indeed, information generation in this equilibrium is suboptimal even if the (endogenously determined) reach of the blockchain ρ is taken as given. Consider the objective that information generation should be maximized. For a given ρ, bad-fit types (Hb-types and Lb-types) should remain outside the blockchain as traditional institutions are better at ascertaining their value. In contrast, good-fit types (Hg-types and Lg-types) should adopt it. This is not the case. Low-value firms, who have an incentive to seek the lowest information generation, pick the opposite option.

Average Mispricing To assess this from a welfare perspective, we consider the induced mispricing in the capital market. When the blockchain is not available, all firms by construction rely on traditional institutions. With probability γ, they are hence priced correctly, while with probability $1-\gamma$ the mispricing is the absolute difference between their actual valuation and the pooling price, $p = (\sigma_{Hg} + \sigma_{Hb})$. This gives the following for the average mispricing AMP:

$$\begin{aligned} AMP_{noBC} &= (1-\gamma) \cdot \Big[(\sigma_{Hg}+\sigma_{Hb}) \cdot (1-p) + (1-\sigma_{Hg}-\sigma_{Hb}) \cdot (p-0)\Big] \\ &= 2(1-\gamma)(\sigma_{Hg}+\sigma_{Hb})(1-\sigma_{Hg}-\sigma_{Hb}). \end{aligned} \tag{28}$$

In contrast, the average mispricing in the $\{1,0,1,0\}$ equilibrium is

$$\begin{aligned} AMP_{\{1,0,1,0\}} &= \sigma_{Hg} \cdot (1-\rho) \cdot (1-p^I) + \sigma_{Lb} \cdot (1-\rho\alpha) \cdot (p^I - 0) \\ &+ \sigma_{Hb} \cdot (1-\gamma) \cdot (1-p^O) + \sigma_{Lg} \cdot (1-\gamma) \cdot (p^O - 0). \end{aligned} \tag{29}$$

Substituting in (24) and simplifying results in

$$AMP_{\{1,0,1,0\}} = 2\left[\frac{(1-\gamma)\sigma_{Hb}\sigma_{Lg}}{\sigma_{Hb}+\sigma_{Lg}} + \frac{\sigma_{Hg}\sigma_{Lb} \cdot (1-\sigma_{Hg}-\sigma_{Lb})(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})}\right]. \tag{30}$$

By comparing (28) and (30), we can show that the undesirable equilibrium may actually lead to lower information provision (as exemplified by the average mispricing).

Proposition 5 *The introduction of blockchain technology can lead to lower equilibrium information provision relative to the status quo in which all firms have to rely on traditional institutions. Formally, there exist parameter constellations such that* $\{1,0,1,0\}$ *can be supported in equilibrium and* $AMP_{noBC} < AMP_{\{1,0,1,0\}}$.

Proof. See Appendix B.8. ■

Proposition 5 contains one of the central messages of this paper. Not only can the availability of the blockchain as a rival to existing traditional institutions lead to a prima facie undesirable equilibrium in which the advantages of the blockchain's peer-to-peer capabilities for information provision cannot be fully exploited. On top of that, the overall level of information generation in the economy may be adversely affected. The availability of the blockchain technology may hence harm instead of help the provision of information to investors.

5.2 Scalability of blockchain technology

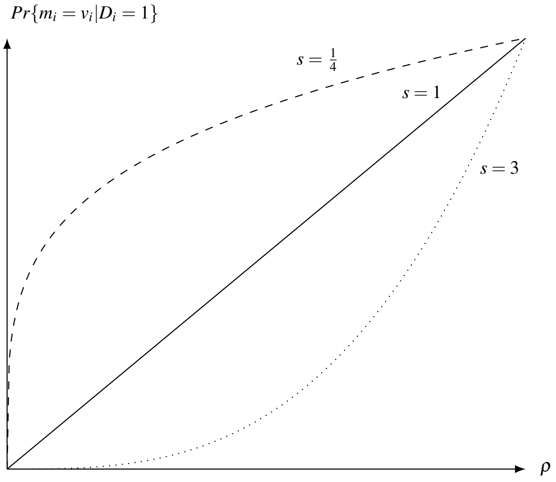
Within our model, the degree to which the blockchain's peer-to-peer capabilities depend on the reach of the blockchain, ρ, is linear – a mass ρ of firms adopting the blockchain in equilibrium leads to a probability $\rho \cdot t_i$ of identifying a firm's type. While this assumption simplifies the exposition and analysis, it is not necessary.

It is naturally of interest to consider alternatives as it adds to the discussion of the potential channels via which a blockchain's peer-to-peer capabilities generate information. Arguably, machine learning algorithms, which analyze a firm's data profile, are in principle able to perform well with even a comparatively low number of data points. In contrast, a direct verification of transactions requires a counterparty for each in principle verifiable transaction to be present. This speaks for a differential *scalability* of the blockchain's peer-to-peer capabilities depending on the specific application. We can in-corporate this aspect into our model by letting the firm-specific information provision in the blockchain be given by

$$Pr\{m_i = v_i | D_i = 1\} = \eta_i' = \rho^s \cdot f_i, \tag{31}$$

with s parametrizing the scalability of the blockchain technology. As $\rho \in [0, 1]$, a small (large) s implies that even a small (even a large) mass of firms in the blockchain allows the peer-to-peer capabilities to perform well (to only exhibit a limited performance). Figure 6 illustrates this aspect.

Figure 6: Illustration of scalability effect



While we abstract from solving the full model, we relate this formulation to the necessary and sufficient condition on γ for the emergence of the undesirable equilibrium. It is straightforward that the analogue to (27) in the modified setup is given by

$$(\sigma_{Hg} + \sigma_{Lb})^s \geq \gamma \geq \alpha(\sigma_{Hg} + \sigma_{Lb})^s. \tag{32}$$

Approximating the likelihood of the undesirable equilibrium being sustainable by the size of this interval $l(s) = (1 - \alpha)(\sigma_{Hg} + \sigma_{Lb})^s$, we have that

$$\frac{\partial l(s)}{\partial s} = \underbrace{(1 - \alpha)}_{>0} \cdot \underbrace{(\sigma_{Hg} + \sigma_{Lb})^s}_{>0} \cdot \underbrace{\log \overbrace{(\sigma_{Hg} + \sigma_{Lb})}^{<1}}_{<0} < 0. \tag{33}$$

This implies that a larger s decreases the range of γ for which the undesirable equilibrium, i.e., {1,0,1,0}, is sustainable. The more scalable the blockchain (the lower s), i.e., the fewer firms are necessary for the blockchain's peer-to-peer capabilities to be efficient, the more likely it is that the undesirable equilibrium materializes. When assessing the potential dangers of a particular blockchain vis-a-vis leading to an underprovision of information to market participants, it is hence essential to take into account the specific form in which the blockchain provides information. Perhaps surprisingly, the more efficient the blockchain technology is in analyzing firms' data, the more likely it is that the undesirable equilibrium occurs.

5.3 Additional considerations

Our results offer some empirical considerations and applications of our theory in particular contexts that relate to the fundamental traits of privacy-preserving blockchains.

A key premise of our model is that there is heterogeneity among firms regarding the blockchain's ability to generate information about them. In this context, the true firm-specific fit is not publicly known, i.e., firms' data profiles are not observable. This assumption is consistent with real-world observations. Empirical measures for the firm-specific fit of the blockchain may involve a firm's transaction profile (e.g., more business-to-business versus business-to-consumer transactions), type of investments (e.g., standard versus non-standard niche investments), accounting basis (e.g., more cash-based or accrual-based), or lifecycle (e.g., mature firms versus start-up firms). However, these proxies are imperfect, and there is still unobservable heterogeneity, which is the necessary ingredient for the model's mechanism to be present.

Our analysis shows that the blockchain's ability to analyze a firm's data becomes a particularly decisive factor as soon as the blockchain can rival traditional information provision for some firms, while underperforming for others. This is likely to apply to numerous settings. For instance, public firms face regulatory requirements and institutions ensuring a certain level of trustworthy information being generated, e.g., by publishing audited financial reports. This leads to a certain average information provision by traditional institutions. Nevertheless, as we have argued, the blockchain can inherently generate information more efficiently for some public firms by leveraging its peer-to-peer capabilities than for others (based on their data profile). More importantly, we show that information provision may be harmed by the emergence of blockchain technology. Specifically, this applies to the average information generation across firms and not just to specific individual firm types. Ending up in the undesirable equilibrium is more likely the higher the heterogeneity in terms of data profiles amongst the potential adopters, i.e., the lower the fit parameter α. In this sense, the emergence of privacy-preserving blockchains should be treated more cautiously by regulators in heterogenous industries than in industries with relatively homogeneous structures or business models.

We also characterize firms' adoption decisions over different levels of reliability and accuracy of traditional institutions, i.e., γ. Firms' adoption decisions depend on the blockchain's relative strength compared to traditional information provision. Consider private firms for which reliable financial data may not be publicly available. Information provision via traditional channels is limited, which translates to a low parameter γ in our model. In this case, we expect that the blockchain's ability to analyze a firm, α, actually plays a minor role. A low to intermediate reach of the blockchain will already be enough to outperform traditional institutions so that high-value private firms will join.

Private firms also provide a potentially interesting opportunity to study the channel through which the blockchain generates information. If adoption costs are low, low-value firms will join and try to pool with other high-value firms that adopt the technology as well. Thus, we would expect a strong push for adoption, with the group of firms joining only being of an average expected quality. However, we also expect a considerable number of low-value firms to be uncovered ex-post. In contrast, if costs are high, it discourages low-value firms from mimicking their high-value counterparts, and we anticipate that separation already occurs at the adoption. This implies that the average value of an adopting firm should be significantly higher than that of an average non-adopting firm.

6 Concluding remarks

Recent innovations in computer science have nurtured the belief that new technologies can enhance the provision of more information to capital market participants. While blockchain technology offers new ways to access and analyze previously separated firm data, it is not clear whether the technology can enhance information provision.

We propose a model in which firms can adopt a privacy-preserving blockchain that is able to generate aggregate information about a firm's value without revealing sensitive data about individual transactions to the public. Firms are heterogeneous in their valuation and the degree to which their data can be analyzed, and choose between relying on traditional institutions or adopting the blockchain for information provision.

Both traditional institutions and the blockchain generate a signal about a firm's value, which becomes available to the capital market. A novel aspect of the setting is that the blockchain's ability to provide information is firm-specific and endogenous. The strength of the signal depends on (i) the blockchain's aforementioned *fit* for analyzing a given firm's data, and (ii), its *reach* into the economy as determined by the proportion of adopting firms. These factors follow from the fundamental design of the technology and are inherent to privacy-preserving blockchains. Firms' adoption decisions depend on the blockchain's relative strength compared to traditional institutions, which in turn affects the reach of the blockchain and therefore the firm-specific strength.

Our setting gives rise to two potential channels for the blockchain to inform investors.

First, the adoption decision itself may serve as a credible signal about a firm's valuation. Provided that the blockchain generates more information than traditional institutions, high-value firms who seek to be identified have a stronger incentive to adopt the blockchain than low-value firms, who try to avoid it. Hence, if the blockchain is sufficiently costly, the emergence of the technology allows investors to separate high-value from low-value firms, without relying on the information provided by either the blockchain or the traditional institutions. Second, the blockchain may exceed the ability of traditional institutions to inform the market about a firm's value due to the strength of its peer-to-peer capabilities. This materializes when the blockchain is sufficiently cheaper than traditional institutions such that a high number of firms are incentivized to join in equilibrium. In this case, the adoption decision itself reveals little about a firm's actual value, but the information generated by the system does.

However, we provide necessary and sufficient conditions for an equilibrium in which neither channel works well. This equilibrium features a mixture of low-value and high-value firms present both inside and outside the blockchain. Importantly, we show that within this equilibrium, it is possible that the emergence of the blockchain technology leads to lower information provision compared to a scenario in which blockchain technology is not available. This is evidenced by the average mispricing in the capital market and implies that the emergence of blockchain technology is not an unambiguously good sign for capital market participants. Moreover, the more efficient the blockchain technology becomes in analyzing firms' data, the more likely it is that the equilibrium materializes.

While blockchain technology indeed has the potential to operate as a "trust machine" and enhance the generation of trustworthy information, it is not a given that this potential is realized. This is particularly important as there is no simple regulatory solution. Even mandating the adoption of a blockchain for all firms – which may not necessarily be feasible, particularly for small firms – is not unambiguously optimal. Our model highlights that whenever the fit of some low-value firms is sufficiently low, traditional institutions would outperform the autonomous mechanism in providing information to investors.

The paper naturally gives rise to several considerations for further research. Within our model, the traditional institutions are represented by a fixed degree of information provision. In practice, the agents behind these institutions will respond to the emergence of blockchain technology as a rival. While a formal analysis of a strategic best response is outside the scope of this paper, endogenizing the strength of these institutions and considering the resulting equilibrium impact on, e.g., the existing market structures, warrants further investigation. For instance, blockchain technology can open markets to entities like tech companies or consortiums offering blockchain-based services that can rival incumbents' business models.

References

Abadi, J. and Brunnermeier, M. (2019). Blockchain economics. *Working Paper.*

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84:488–500.

Allision, I. (2018). Ing bank launches zero-knowledge tech for blockchain privacy. *Coindesk*, 22 Oct 2018.

Bertomeu, J. and Magee, R. P. (2011). From low-quality reporting to financial crises: Politics of disclosure regulation along the economic cycle. *Journal of Accounting and Economics*, 52(2):209–227.

Bertomeu, J. and Magee, R. P. (2015a). Mandatory disclosure and asymmetry in financial reporting. *Journal of Accounting and Economics*, 59(2-3):284–299.

Bertomeu, J. and Magee, R. P. (2015b). Political pressures and the evolution of disclosure regulation. *Review of Accounting Studies*, 20(2):775–802.

Cao, S., Cong, L. W., and Yang, B. (2019). Auditing and blockchains: Pricing, misstatements, and regulation. *Working Paper.*

Chen, H. and Yang, L. (2018). Stability and regime change: The evolution of accounting standards. *Working Paper.*

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

Cong, L. W. and He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5):1754–1797.

Cong, L. W., Li, Y., and Wang, N. (2019). Tokenomics: Dynamic adoption and valuation. *Working Paper.*

Dai, J. and Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3):5–21.

Deloitte (2018). Deloitte's 2018 global blockchain survey.

Dow Jones Newswires (2018). Blockchain beyond the hype. *Dow Jones Newswires*, 19 Dec 2018.

Dye, R. A. (1985). Disclosure of nonproprietary information. *Journal of accounting research*, pages 123–145.

Dye, R. A. and Sridhar, S. S. (2008). A positive theory of flexibility in accounting standards. *Journal of Accounting and Economics*, 46(2-3):312–333.

Edmans, A., Heinle, M. S., and Huang, C. (2016). The real costs of financial efficiency when some information is soft. *Review of Finance*, 20(6):2151–2182.

EY (2018). Press release: EY announces blockchain audit technology.

EY (2019). Press release: EY releases zero-knowledge proof blockchain transaction technology to the public domain to advance blockchain privacy standards.

Fanning, K. and Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, 27(5):53–57.

Ferreira, D., Manso, G., and Silva, A. C. (2012). Incentives to innovate and the decision to go public or private. *The Review of Financial Studies*, 27(1):256–300.

Fuller, S. H. and Markelevich, A. (2019). Should accountants care about blockchain? *Working Paper.*

Harvey, C. (2016). Cryptofinance. *Working Paper.*

Heinle, M. S. and Verrecchia, R. E. (2015). Bias and the commitment to disclosure. *Management Science*, 62(10):2859–2870.

Hermalin, B. E. and Weisbach, M. S. (2012). Information disclosure and corporate governance. *The Journal of Finance*, 67(1):195–233.

Hinzen, F. J., John, K., and Saleh, F. (2019). Proof-of-work's limited adoption problem. *NYU Stern School of Business.*

Jung, W.-O. and Kwon, Y. K. (1988). Disclosure when the market is unsure of information endowment of managers. *Journal of Accounting research*, pages 146–153.

KPMG (2018). The changing landscape of disruptive technologies.

Lyandres, E. (2019). Product market competition with crypto tokens and smart contracts. *Available at SSRN 3395441.*

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., and Qijun, C. (2017). A review on consensus algorithm of blockchain. In *Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on*, pages 2567–2572. IEEE.

PricewaterhouseCoopers (2018). PwC's global blockchain survey 2018.

The Economist (2015). The trust machine – the promise of the blockchain. *The Economist*, 417(13).

The New York Times (2018). The hope and betrayal of blockchain. *The New York Times*, 4 Dec 2018.

Vasarhelyi, M. A., Kogan, A., and Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2):381–396.

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of accounting and economics*, 5:179–194.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In *International Workshop on Open Problems in Network Security*, pages 112–125. Springer.

Wall Street Journal (2016). Bitcoin is just the beginning. *Wall Street Journal*, 27 May 2016(A.9).

Wang, Y. and Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30:1–18.

Xu, K., Yue, H., Guo, L., Guo, Y., and Fang, Y. (2015). Privacy-preserving machine learning algorithms for big data systems. In *2015 IEEE 35th international conference on distributed computing systems*, pages 318–327. IEEE.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1):7–31.

Yuan, Y. and Wang, F.-Y. (2016). Towards blockchain-based intelligent transportation systems. In *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*, pages 2663–2668. IEEE.

Appendix for "Can You Trust the Blockchain? – The (limited) Power of Peer-to-Peer Networks for Information Provision"

This appendix contains the necessary proofs and additional explanations supplementing the analysis presented in the paper "Can You Trust the Blockchain? – The (limited) Power of Peer-to-Peer Networks for Information Provision".

A Economic setting

Most privacy-preserving peer-to-peer technologies share fundamental features that lead to a firm-specific strength for information provision. In principle, it depends on the fit of its peer-to-peer capabilities for analyzing each firm's data profile, and the reach of the blockchain. These factors directly follow from the fundamental features of the technology. Let us exemplify the functionality by referring to two mechanisms for which implementations already exist or are in development in the context of accounting, namely, zero-knowledge-proof verification protocols and machine learning.

Zero-knowledge-proof protocols allow blockchains to verify business transactions without revealing information to others inside or outside the blockchain.[19] Consider a business transaction between two parties, e.g., a purchase of raw materials. Both firms, the buyer and the seller, must record the transaction in their ledgers. The protocol automatically sends out a series of verification requests to prove that each firm has recorded the business transaction accordingly. These requests usually occur in the form of numerical problems, which do not allow any party to reconstruct the underlying information. Proof can only be reached if both firms' answers correspond to each other.[20] In terms of information provision, the central idea is that the blockchain can provide more information to the market, the more transactions are verified. For instance, the blockchain can "certify" disclosure after verifying the underlying business transactions.

However, verification naturally works better for some transactions than for others. A cash-based business transaction can in principle be verified by matching the respective recordings of both counter-parties, i.e., the record of the cash-inflow of one party can be used to confirm the record of the cash-outflow of the counter-party. In contrast, an accrual-based business transaction is inherently challenging for such a system. For example, an asset impairment represents a decline in a firm's economic value that is relevant to investors but does not involve a direct counter-party, which prevents immediate verification and leaves uncertainty. Moreover, the level of verification that can be achieved also hinges on the number of counter-parties participating in the blockchain. While a business transaction might be in principle verifiable, e.g., is cash-based, a direct comparison of the recordings of the two involved parties is only possible if both firms are subscribed to the system. If at least one of the two firms is not present, it is challenging for the algorithm to confirm the transaction as verification using peer-to-peer referencing is not possible.

[19] Several variations of zero-knowledge-proof protocols exist or are under development. For example, the cryptocurrency Zcash, a privacy-preserving cryptocurrency, uses the zk-SNARKS protocol (*zero-knowledge succinct non-interactive argument of knowledge*) allowing one party to prove the validity of a transaction without releasing any sensitive information.

[20] Verification works as the two counter-parties have different incentives and little interest to collude from an accounting point of view.

A blockchain does not only allow for peer-to-peer verification but also enables potential gains for data analytics. As such, a blockchain can enhance the capabilities of machine learning algorithms used for value estimations, trend analysis, or real-time analysis by providing privacy-ensuring access to the data of various firms that have previously been stored separately. Such analyses can be utilized to generate additional information about a firm's investments and economic value. Nevertheless, while being different in its functionality, machine learning faces similar limitations as other peer-to-peer mechanisms running on a privacy-preserving blockchain concerning its ability to provide viable information about some investments.

For somewhat standard investments, estimations are likely to be reliable once enough data points are available to the system. For instance, consider a firm purchasing a manufacturing machine that is also used by various industry peers. A machine learning algorithm is likely to produce a reliable value estimate for the new machinery, assuming that sufficient relevant data for the estimation is available on the blockchain. In contrast, "non-standardized", or rather firm-specific, investments usually lack the comparability with investments by other firms, limiting the ability to learn from other firms' data entries. Consider that the machine from above is highly customized; it will be challenging to estimate the value of such an investment given that only a minimal number of firms – if a firm at all – can provide relevant input to enhance the estimation. Moreover, the quality of the evaluation relies on the reach of the blockchain, i.e., the number of firms joining and thus, providing data to the system. Similar to the verification example, even if the algorithm faces a standard investment, it might not be able to produce a reliable estimate of a firm's value because of limited data availability. In contrast, if more firms with a comparable investment profile join the network, machine learning can leverage the increased sample size, lowering potential estimation errors.

The discussion above highlights the fit and the reach as two critical and fundamental factors that inherently shape a privacy-preserving blockchain's ability to generate information, making them key ingredients for our analysis. In principle, the strength of the blockchain increases, the higher the firm-specific fit and the larger the reach of the blockchain.

B Proofs

B.1 Proof of Lemma 1

Following (7), we obtain

$$\begin{aligned} \Delta_{Hg} - \Delta_{Hb} &= (1-\alpha)\rho(1-p^I) \geq 0 && \text{(B.1)} \\ \Delta_{Lg} - \Delta_{Lb} &= -(1-\alpha)\rho p^I \leq 0, && \text{(B.2)} \end{aligned}$$

where $\rho \geq 0$, and $p^I \in [0,1]$ are determined by the other firms' equilibrium decisions.

B.2 Proof of Lemma 3

This follows directly from the fact that any mixed-strategy profile which constitutes an equilibrium for $\gamma = 0$ and $C > 0$ must be contained in the set

$$\{\{q_{Hg}, q_{Hb}, 0, 0\}, \{1, 1, q_{Lb}, 0\}, \{1, 1, 1, q_{Lg}\}\} \tag{B.3}$$

as all other profiles violate Lemma 2. The only exception is $\{1, 1, 1, 1\}$ in which all firms adopt. However, this profile fails because it requires $C = 0$ – otherwise, Lg-types, which are revealed inside the blockchain with probability 1 and hence obtain an expected payoff of 0, would strictly prefer to not join, irrespective of the perceived quality outside the blockchain.

B.3 Proof of Proposition 1

We proceed through the three mixed strategy profiles from Lemma 3 and assess under which conditions they constitute equilibria. This also yields the pure strategy equilibria by considering $q_\theta \in \{0, 1\}$ as special cases.

Profile $\{q_{Hg}, q_{Hb}, 0, 0\}$ Consider first the special case $q_{Hg} = q_{Hb} = 0$ which requires $\Delta_\theta \leq C$, $\forall\theta$. As $C \geq 0$, and as an equilibrium strategy profile of $\{0, 0, 0, 0\}$ allows to freely specify the off-path belief about the value of unverified firms inside the blockchain, the belief that induces $p^I = 0$ always gives $\Delta_\theta = 0 - p^O < 0 \leq C$. This can therefore always be supported in equilibrium for any $C \geq 0$.

Thus, we can restrict attention to candidates where $q_{Hg} + q_{Hb} > 0 \implies \rho > 0$. If this constitutes an equilibrium, $p^I = 1$ and thus $\Delta_{Hg} = \Delta_{Hb}$. Any such equilibrium necessarily features $\Delta_{Hg} = \Delta_{Hb} \overset{(14)}{>} \Delta_{Lb} \geq \Delta_{Lg}$. We need to distinguish two cases: the case where high-value firms *strictly* prefer to join the blockchain, and the case where they are *indifferent*.

If they strictly prefer to join the blockchain, we have $\Delta_{Hg} = \Delta_{Hb} > C$ and thus $q_{Hg} = q_{Hb} = 1$, $p^I = 1$, $p^O = 0$. This can hence be supported in equilibrium whenever $C \in [\Delta_{Lb}, \Delta_{Hg})$ where the lower bound on C stems from the Lb-type being incentivized not to join the blockchain, and the upper bound from the high value-types being incentivized to join. We can compute these bounds explicitly and have that $\{1, 1, 0, 0\}$ can be supported in equilibrium whenever $C \in [1 - \alpha [\sigma_{Hg} + \sigma_{Hb}], 1)$.

If they are indifferent, we have $\Delta_{Hg} = \Delta_{Hb} = C$ and $p^I = 1$. This gives as a necessary condition

$$C = 1 - p^O = \frac{\sigma_{Lb} + \sigma_{Lg}}{(1 - q_{Hg})\sigma_{Hg} + (1 - q_{Hb})\sigma_{Hb} + \sigma_{Lb} + \sigma_{Lg}} \equiv \tilde{C}(q_{Hg}, q_{Hb}) \tag{B.4}$$

Clearly, $\tilde{C}(q_{Hg}, q_{Hb})$ is increasing in both q_{Hg} and q_{Hb}. For each $C \in \left(\tilde{C}(0, 0), \tilde{C}(1, 1)\right] = (1 - (\sigma_{Hb} + \sigma_{Hg}), 1]$, there hence exist $q_{Hg}, q_{Hb} \in [0, 1]$ with $q_{Hg} + q_{Hb} > 0$ such that $\{q_{Hg}, q_{Hb}, 0, 0\}$ constitutes an equilibrium. Notably, for $C = \tilde{C}(1, 1) = 1$, this is the pure strategy equilibrium $\{1, 1, 0, 0\}$. Moreover, $\tilde{C}(1, 0)$ and $\tilde{C}(0, 1)$ characterize the unique cost levels such that $\{1, 0, 0, 0\}$ and $\{0, 1, 0, 0\}$ can respectively be supported in equilibrium.

Profile $\{1, 1, q_{Lb}, 0\}$ In equilibrium, this implies $\rho > 0$, $p^O = 0$ and $p^I > 0$. It follows that $\Delta_{Hg} \geq \Delta_{Hb} > \Delta_{Lb} > \Delta_{Lg}$. We can explicitly compute p^I and obtain

$$p^I = \frac{(1-\rho)\sigma_{Hg} + (1-\rho\alpha)\sigma_{Hb}}{(1-\rho)\sigma_{Hg} + (1-\rho\alpha)(\sigma_{Hb} + q_{Lb}\sigma_{Lb})}. \tag{B.5}$$

We need to distinguish cases, specifically whether *Lb*-types strictly prefer to join the blockchain ($\Delta_{Lb} > C$), are indifferent ($\Delta_{Lb} = C$), or prefer not to join ($\Delta_{Lb} < C$).

For *Lb*-types to be indifferent, $C = \Delta_{Lb}$ is required. Plugging (B.5) into Δ_{Lb}, we obtain as a necessary condition

$$\begin{aligned} C &= (1-\rho\alpha)p^I \\ &= \tfrac{\big(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb})\big)\big[(\sigma_{Lg}+(1-q_{Lb})\sigma_{Lb})\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb}))\sigma_{Hb}\big]}{(\sigma_{Lg}+(1-q_{Lb})\sigma_{Lb})\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb}))(\sigma_{Hb}+q_{Lb}\sigma_{Lb})} \\ &\equiv \tilde{C}'(q_{Lb}) \end{aligned} \tag{B.6}$$

Inspection shows that $\tilde{C}'$ is decreasing in q_{Lb}. Thus, for each $C \in \Big[\tilde{C}'(1), \tilde{C}'(0)\Big]$, there exists a q_{Lb} such that $\{1, 1, q_{Lb}, 0\}$ can be supported in equilibrium. We can explicitly derive

$$\begin{aligned} \tilde{C}'(1) &= (1-\alpha(1-\sigma_{Lg}))\frac{\sigma_{Lg}\sigma_{Hg} + (1-\alpha(1-\sigma_{Lg}))\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg} + (1-\alpha(1-\sigma_{Lg}))(\sigma_{Hb}+\sigma_{Lb})} \equiv \bar{C} \\ \tilde{C}'(0) &= 1-\alpha\left(\sigma_{Hg}+\sigma_{Hb}\right) \end{aligned} \tag{B.7}$$

The case where $\Delta_{Lb} < C$ implies $q_{Lb} = 0$ and hence that we consider the profile $\{1, 1, 0, 0\}$ which has been covered previously. Whenever $\Delta_{Lb} > C$, we consider the profile $\{1, 1, 1, 0\}$ which, to be supported in equilibrium, requires $C \in \Big[\Delta_{Lg}, \tilde{C}'(1)\Big)$. We can explicitly write Δ_{Lg} in this case as

$$\Delta_{Lg} = (1-\rho)p^I = \sigma_{Lg}\frac{\sigma_{Lg}\sigma_{Hg} + (1-\alpha(1-\sigma_{Lg})\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg} + (1-\alpha(1-\sigma_{Lg})(\sigma_{Hb}+\sigma_{Lb})} \equiv \underline{C} \tag{B.8}$$

Including the limit case where the *Lb*-type is indifferent, $\{1, 1, 1, 0\}$ can hence be supported in equilibrium whenever $C \in \big[\underline{C}, \bar{C}\big]$.

Profile $\{1, 1, 1, q_{Lg}\}$ $q_{Lg} = 1$ is not feasible due to $C > 0$. Moreover, the case $q_{Lg} = 0$ was covered in the previous case. We can hence restrict attention to $q_{Lg} \in (0, 1)$ which requires that the *Lg*-type is indifferent. This is both necessary and sufficient as $q_{Lg} \in (0, 1)$ in this case implies $\rho > 0$, $p^O = 0$, $0 < p^I < 1$ and hence $\Delta_{Hg} > \Delta_{Hb} > \Delta_{Lb} > \Delta_{Lg}$.

C therefore needs to satisfy

$$\begin{aligned} C = \Delta_{Lb} &= (1-\rho\alpha)p^I \\ &= \tfrac{\big(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb})\big)\big[(\sigma_{Lg}+(1-q_{Lb})\sigma_{Lb})\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb}))\sigma_{Hb}\big]}{(\sigma_{Lg}+(1-q_{Lb})\sigma_{Lb})\sigma_{Hg}+(1-\alpha(1-\sigma_{Lg}-(1-q_{Lb})\sigma_{Lb}))(\sigma_{Hb}+q_{Lb}\sigma_{Lb})} \\ &\equiv \tilde{C}''(q_{Lg}) \end{aligned} \tag{B.9}$$

$\tilde{C}''$ is decreasing in q_{Lg}. For any $C \in \Big(\tilde{C}''(1), \tilde{C}''(0)\Big)$, there hence exists a $q_{Lg} \in (0, 1)$

such that $\{1, 1, 1, q_{Lg}\}$ is an equilibrium profile. We can derive

$$\tilde{C}''(1) = 0 \tag{B.10}$$

$$\tilde{C}''(0) = \sigma_{Lg}\frac{\sigma_{Lg}\sigma_{Hg} + (1 - \alpha(1 - \sigma_{Lg})\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg} + (1 - \alpha(1 - \sigma_{Lg})(\sigma_{Hb} + \sigma_{Lb})} = \underline{C}. \tag{B.11}$$

Summarizing the analysis yields the proposition.

B.4 Equilibrium Candidates

To identify the equilibrium candidates in the two cases, we first establish several helpful observations.

Lemma B.1 *Adoption (Non-Adoption) by all firms can be supported in equilibrium if and only if* $C \leq \min\{0, \alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - \gamma\}$ *(*$C \geq -(1-\gamma)\sigma_H$*).*

Proof. Consider adoption by all firms, i.e., $\{1, 1, 1, 1\}$. Good fit firms are identified with probability 1 and bad fit firms with probability α. On path, Hg-firms receive $1 - C$ whereas Lg-firms receive $-C$, while Hb-firms receive $\alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - C$ and Lb-firms $(1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - C$. If low-value firms do not adopt, they receive $(1-\gamma) \cdot p^O$, with p^O being determined by off-path beliefs. The most pessimistic off-path beliefs yield $p^O = 0$ so that for Lg-types it needs to hold that $-C \geq 0 \iff C \leq 0$. For high-value firms, the payoff outside is $\gamma + (1-\gamma) \cdot p^O$. By the same logic, we hence require $\alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - C \geq \gamma \iff C \leq \alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - \gamma$.
Consider next non-adoption by all firms, i.e., {0,0,0,0}. On-path, we obtain a payoff of $\gamma + (1-\gamma) \cdot \sigma_H$ for high-value firms, and $(1-\gamma)\sigma_H$ for low-value firms. Deviating and adopting gives an off-path payoff for all firms of $p^I - C$, as the reach of the blockchain is 0. This is determined by off-path beliefs. It is hence straightforward that non-adoption by all firms can be supported in equilibrium if and only if $(1-\gamma)\sigma_H \geq -C \iff C \geq -(1-\gamma)\sigma_H$. ■

Lemma B.2 *Any equilibrium in which only low-value types adopt (do not adopt) the blockchain requires* $C \leq 0$ *(*$C \geq 0$*).*

Proof. When only low-value types adopt the blockchain, they receive a payoff of $-C$. By deviating and not adopting, they receive at least a valuation of 0. Thus, $C \leq 0$ is a necessity. Similarly, they receive 0 when only low-value types do not adopt. Adopting the blockchain would at least yield a payoff of $-C$. This gives $C \geq 0$. ■

Lemma B.3 *Any equilibrium in which only high-value types adopt the blockchain requires* $C > 0$*. Any equilibrium in which only high-value types do not adopt requires* $C < 0$*.*

Proof. Consider first a conjectured equilibrium in which only high-value types adopt. Low-value types could obtain $1 - C$ by adopting. For $C \leq 0$, this always dominates non-adoption alternative which yields $(1-\gamma)p^O < 1$ as $p^O < 1$.

Consider next a conjectured equilibrium in which only high-value types do not adopt. Low-value types could obtain 1 by not adopting the blockchain. Adopting gives them $\underbrace{(1-\eta_i)\cdot p^I}_{<1} - C$, so $C < 0$ is necessary. ■

Using these results and Lemma 1, we can substantially restrict the set of equilibrium candidates, split according to whether adopting the blockchain is relatively cheaper or more costly than relying on traditional institutions. This is summarized in Table A.1.

Equilibrium Candidate	$C < 0$	$C \geq 0$
{1,1,1,1}	for $C \leq \min\{0, \alpha + (1-\alpha)\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lb}} - \gamma\}$, see Lemma B.1	potentially if $C = 0$
{1,1,1,0}	not possible, see Lemma B.2	possible
{1,1,0,1}	not possible b/w Lb and Lg as $\rho > 0$ and $p^I > 0$, see Lemma 1	
{1,0,1,1}	possible	not possible, see Lemma B.3
{0,1,1,1}	not possible b/w Hg and Hb as $\rho > 0$ and $p^I < 1$, see Lemma 1	
{1,1,0,0}	not possible, see Lemma B.2	possible
{1,0,1,0}	possible	
{0,1,1,0}	not possible b/w Hg and Hb as $\rho > 0$ and $p^I < 1$, see Lemma 1	
{1,0,0,1}	not possible b/w Lb and Lg as $\rho > 0$ and $p^I > 0$, see Lemma 1	
{0,0,1,1}	possible	not possible, see Lemma B.2
{0,1,0,1}	not possible b/w Hg and Hb as $\rho > 0$ and $p^I < 1$, see Lemma 1	
{1,0,0,0}	not possible, see Lemma B.3	possible
{0,1,0,0}	not possible, see Lemma B.3	possible
{0,0,1,0}	possible	not possible, see Lemma B.2
{0,0,0,1}	possible	not possible, see Lemma B.2
{0,0,0,0}	possible for $C \geq -(1-\gamma)\sigma_H$, see Lemma B.1	possible always, see Lemma B.1

Table A.1: Equilibrium Candidates

B.5 General Case – $C \geq 0$

For now, we consider $C \geq 0$. Given Table A.1, we restrict attention to the pure strategy equilibrium candidates {1,1,0,0}, {1,0,1,0} and {1,1,1,0}, as well as the knife-edge candidates {1,0,0,0} and {0,1,0,0}. {0,0,0,0} is always sustainable in equilibrium irrespective of γ and $C \geq 0$, while the condition for {1,1,1,1} follows immediately from Lemma B.1. We proceed by analyzing each candidate individually below. Throughout, we derive constraints on the combination of C and γ given the other fundamentals σ_θ and α such that a given candidate can be supported in equilibrium.

{1,1,0,0} If this constitutes an equilibrium, payoffs are given by $1 - C$ for high-value types, and 0 for low-value types. Both high-value types face the same deviation incentives as the detection probability outside the blockchain is independent of the fit; the payoffs from deviating and not adopting would be γ. We hence require $1-C \geq \gamma \iff C \leq 1-\gamma$.

Between the low-value types, the Lb-type faces a lower detection (and hence higher pooling) probability than the Lg-type upon joining the blockchain. To deter adoption by this type, we require $0 \geq (1-\alpha\sigma_H) \cdot 1 - C \iff C \geq 1 - \alpha\sigma_H$. This is independent of γ.

The region where {1,1,0,0} can be supported in equilibrium is hence given by a triangle in the γ-C-space. The upper left end of the triangle is at $\gamma = 0$, $C = 1$.

{1,1,1,0} Consider first the on-path payoffs. The Lg-type receives 0 as he is identified by the adoption decision. Within the blockchain, we have $\rho = 1 - \sigma_{Lg}$ and

$$p^I = \frac{(1-\rho)\sigma_{Hg} + (1-\rho\alpha)\sigma_{Hb}}{(1-\rho)\sigma_{Hg} + (1-\rho\alpha)(\sigma_{Hb}+\sigma_{Lb})} = \frac{\sigma_{Lg}\sigma_{Hg} + (1-\alpha+\alpha\sigma_{Lg})\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg} + (1-\alpha+\alpha\sigma_{Lg})(\sigma_{Hb}+\sigma_{Lb})} \quad \text{(B.12)}$$

and

$$\begin{aligned} \pi_{Hg} &= (1-\sigma_{Lg}) + \sigma_{Lg}p^I - C \\ \pi_{Hb} &= (1-\sigma_{Lg})\alpha + (1-\alpha+\alpha\sigma_{Lg})p^I - C \\ \pi_{Lb} &= (1-\alpha+\alpha\sigma_{Lg})p^I - C. \end{aligned} \quad \text{(B.13)}$$

We know that $\Delta_{Hg} \geq \Delta_{Hb}$ so that we need to consider three possible deviations.

(a) Hb-types not adopting the blockchain. This requires $\pi_{Hb} \geq \gamma$. Clearly, as $\pi_{Hb} \leq 1 - C$ (due to $p^I < 1$), this constraint gives a tighter upper bound on C than the bound for the {1,1,0,0} equilibrium. We obtain

$$\begin{aligned} & (1-\sigma_{Lg})\alpha + (1-\alpha+\alpha\sigma_{Lg})p^I - C \geq \gamma \\ \iff & C \leq (1-\sigma_{Lg})\alpha + (1-\alpha+\alpha\sigma_{Lg})p^I - \gamma \equiv \tilde{C}_{Hb}(\gamma). \end{aligned} \quad \text{(B.14)}$$

(b) Lb-types not adopting the blockchain. If they don't adopt, they receive 0. Deterring this requires $(1-\alpha+\alpha\sigma_{Lg})p^I - C \geq 0 \iff C \leq (1-\alpha+\alpha\sigma_{Lg})p^I \equiv \tilde{C}_{Lb}$. Note that this upper bound lies strictly below the lower bound on C in the {1,1,0,0} equilibrium. This is because that lower bound is given by

$$\begin{aligned} 1-\alpha\sigma_H &= 1-\alpha(1-\sigma_L) \\ &= 1-\alpha+\alpha\sigma_{Lg} + alpha\sigma_{Lb} \\ &> 1-\alpha+\alpha\sigma_{Lg} \\ &> (1-\alpha+\alpha\sigma_{Lg}) \cdot p^I. \end{aligned} \quad \text{(B.15)}$$

(c) Lg-types adopting the blockchain. If they adopt, they receive $\sigma_{Lg}p^I - C$, so that we require $C \geq \sigma_{Lg}p^I \equiv \tilde{C}_{Lg}$ to deter this. Note that $\tilde{C}_{Lg} < \tilde{C}_{Lb}$ due to $\sigma_{Lg} < 1$. Plugging in for p^I, we get

$$\tilde{C}_{Lg} = \sigma_{Lg}\frac{\sigma_{Lg}\sigma_{Hg} + (1-\alpha+\alpha\sigma_{Lg})\sigma_{Hb}}{\sigma_{Lg}\sigma_{Hg} + (1-\alpha+\alpha\sigma_{Lg})(\sigma_{Hb}+\sigma_{Lb})}.$$

We have hence characterized the region such that {1,1,1,0} can be sustained. This represents a trapezoid in the γ-C-space which lies strictly below the triangle characterizing the {1,1,0,0} equilibrium region.

{1,0,1,0} First, note that in this candidate equilibrium, $\hat{\rho} = \sigma_{Hg} + \sigma_{Lb}$, $\hat{p}^O = \frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}}$ and $\hat{p}^I = \frac{(1-\sigma_{Hg}-\sigma_{Lb})\sigma_{Hg}}{(1-\sigma_{Hg}-\sigma_{Lb})\sigma_{Hg}+(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))\sigma_{Lb}} = \frac{(1-\sigma_{Hg}-\sigma_{Lb})\sigma_{Hg}}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})}$.
The on-path payoffs are given by

$$\begin{aligned}
\pi_{Hg} &= (\sigma_{Hg} + \sigma_{Lb}) + (1 - \sigma_{Hg} - \sigma_{Lb})p^I - C \\
\pi_{Hb} &= \gamma + (1-\gamma)p^O \\
\pi_{Lb} &= (1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I - C \\
\pi_{Lg} &= (1-\gamma)p^O
\end{aligned}$$

We need to consider deviations by all four types.

(a) *Hg*-types not adopting. They would receive a payoff of $\gamma + (1-\gamma)p^O$. So we require that

$$\begin{aligned}
&(\sigma_{Hg} + \sigma_{Lb}) + (1 - \sigma_{Hg} - \sigma_{Lb})p^I - C \geq \gamma + (1-\gamma)p^O \\
\iff\ & C \leq \left[(\sigma_{Hg} + \sigma_{Lb}) + (1 - \sigma_{Hg} - \sigma_{Lb})p^I\right] - p^O - (1-p^O)\gamma \equiv \hat{C}_{Hg}(\gamma) \quad \text{(B.16)}
\end{aligned}$$

This gives an upper bound on C and is a linear constraint decreasing in γ.

(b) *Hb*-types adopting. They would receive $\alpha(\sigma_{Hg} + \sigma_{Lb}) + (1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I - C$, so we require

$$\begin{aligned}
&\gamma + (1-\gamma)p^O \geq \alpha(\sigma_{Hg} + \sigma_{Lb}) + (1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I - C \\
\iff\ & C \geq \left[\alpha(\sigma_{Hg} + \sigma_{Lb}) + (1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I\right] - p^O - (1-p^O)\gamma \equiv \hat{C}_{Hb}(\gamma). \quad \text{(B.17)}
\end{aligned}$$

This gives a lower bound on C and is a linear constraint decreasing in γ. Note that this constraint has the same slope and lies strictly below $\hat{C}_{hg}(\gamma)$.

(c) *Lb*-types not adopting. They would receive a payoff of $(1-\gamma)p^O$, so we require that

$$\begin{aligned}
&(1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I - C \geq (1-\gamma)p^O \\
\iff\ & C \leq (1 - \alpha(\sigma_{Hg} + \sigma_{Lb}))p^I - (1-\gamma)p^O \equiv \hat{C}_{Lb}(\gamma) \quad \text{(B.18)}
\end{aligned}$$

This gives an upper bound on C and is a linear constraint increasing in γ.

(d) *Lg*-types adopting. They would receive a payoff of $(1 - (\sigma_{Hg} + \sigma_{Lb}))p^I - C$, so we require that

$$\begin{aligned}
&(1-\gamma)p^O \geq (1 - (\sigma_{Hg} + \sigma_{Lb}))p^I - C \\
\iff\ & C \geq (1 - (\sigma_{Hg} + \sigma_{Lb}))p^I - (1-\gamma)p^O \equiv \hat{C}_{Lg}(\gamma) \quad \text{(B.19)}
\end{aligned}$$

Overall, this characterizes the region such that {1,0,1,0} can be sustained in equilibrium. So far, we have not imposed $C \geq 0$; it is always non-empty when allowing for both $C \geq 0$ and $C \leq 0$. To check whether this is an equilibrium for $C \geq 0$, note that the highest C at which this can be supported obtains for γ such that $\hat{C}_{Lb}$ and $\hat{C}_{Hg}$ intersect. This is given by $\gamma = \hat{\rho} - \hat{\rho}(1-\alpha)p^I$. Plugging in, we obtain

$$\gamma = \frac{(1-\sigma_{Hg})\alpha\sigma_{Hg} + (1 - 2\alpha\sigma_{Hg})\sigma_{Lb} - \alpha\sigma_{Lb}^2}{1 - \sigma_{Hg} - \alpha\sigma_{Lb}} \quad \text{(B.20)}$$

and thus as highest feasible C

$$\hat{C}^{max} = \frac{(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))(\sigma_{Hg}\sigma_{Lg}-\sigma_{Hb}\sigma_{Lb})}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})}. \tag{B.21}$$

Observe that $\hat{C}^{max} > 0 \iff \sigma_{Hg}\sigma_{Lg} > \sigma_{Hb}\sigma_{Lb}$. If this is violated, {1,0,1,0} cannot be sustained for positive C, irrespective of γ.

Finally, it can be established that the region supporting this equilibrium is disjoint from the one supporting {1,1,0,0}, but may overlap with {1,1,1,0} and even extend beyond it, i.e. be sustainable for γ-C-combinations which lie above the constraint given by $\tilde{C}_{Hb}$.[21]

{1,0,0,0} Note that only Hg-types join which implies $p^I = 1$. Hence, $\Delta_{Hg} = \Delta_{Hb}$ (see the proof of Lemma 1). Both high-value firms hence need to be indifferent between adopting and not adopting the blockchain, which implies that

$$\Delta_{Hg} = \Delta_{Hb} = 0 \iff 1-C = \gamma+(1-\gamma)p^O \iff C = \left(1-\frac{\sigma_{Hb}}{1-\sigma_{Hg}}\right)\cdot(1-\gamma), \tag{B.22}$$

where we used $p^O = \frac{\sigma_{Hb}}{1-\sigma_{Hg}}$. Amongst low-value types, Lb-types have a stronger incentive to deviate and adopt the blockchain due to the lower detection probability. Given $\rho = \sigma_{Hg}$, we hence require

$$(1-\gamma)\frac{\sigma_{Hb}}{1-\sigma_{Hg}} \geq (1-\alpha\sigma_{Hg}) - C \iff C \geq 1-\alpha\sigma_{Hg} - (1-\gamma)\frac{\sigma_{Hb}}{1-\sigma_{Hg}}. \tag{B.23}$$

The two conditions are compatible if and only if $\gamma \leq \alpha\sigma_{Hg}$.

{0,1,0,0} As only Hb-types join, we have $p^I = 1$ and thus $\Delta_{Hg} = \Delta_{Hb}$. This implies

$$\Delta_{Hg} = \Delta_{Hb} = 0 \iff 1-C = \gamma+(1-\gamma)p^O \iff C = \left(1-\frac{\sigma_{Hg}}{1-\sigma_{Hb}}\right)\cdot(1-\gamma), \tag{B.24}$$

where we used $p^O = \frac{\sigma_{Hg}}{1-\sigma_{Hb}}$. To deter low-value types (specifically Lb-types) from deviating, we require

$$(1-\gamma)\frac{\sigma_{Hg}}{1-\sigma_{Hb}} \geq (1-\alpha\sigma_{Hb}) - C \iff C \geq 1-\alpha\sigma_{Hb} - (1-\gamma)\frac{\sigma_{Hg}}{1-\sigma_{Hb}}. \tag{B.25}$$

The two conditions are compatible if and only if $\gamma \leq \alpha\sigma_{Hb}$.

B.6 General Case – $C \leq 0$

Consider now $C < 0$ and denote $B \equiv -C$ to ease the exposition. The conditions for {0,0,0,0} and {1,1,1,1} follow immediately from Lemma B.1. In addition to these full (non-)adoption equilibria, we only need to consider the following pure strategy profiles.

[21] We establish this by showing that the upper bound on the {1,0,1,0}-region lies below the upper bound of the {1,1,1,0}-region as given by $\tilde{C}_{Lb}$. This holds as (i) the lowest point of the region supporting {1,0,1,0} lies below the lower bound on {1,1,1,0}, and (ii) the difference between the lowest C and highest C in the {1,0,1,0}-region is lower than the difference between the lower and upper bound of the {1,1,1,0}-region. The detailed derivations are cumbersome and not very instructive. We thus omit them for brevity. They are available upon request, as is a Mathematica file verifying them.

$$\{1,0,1,1\}\,,\ \{1,0,1,0\}\,,\ \{0,0,1,1\}\,,\ \{0,0,1,0\}\,,\ \{0,0,0,1\}$$

We proceed through these equilibrium candidates one by one.

{0,0,1,1} Payoffs in this case are given by B for low-value types, and 1 for high-value types. Both low-value types face the same deviation incentives as the detection probability outside the blockchain is independent of the fit. The payoff from deviating and not adopting would be $(1-\gamma)\cdot 1$. Hence, the condition from the low-value types determining the existence of this equilibrium is $B \geq (1-\gamma)$.

Due to $\Delta_{Hg} \geq \Delta_{Hb}$, we only need to consider possible deviations by Hg-types. They would get $\rho + B$ upon adopting, where $\rho = \sigma_L$. So we also require $\sigma_L + B \leq 1 \iff B \leq 1-\sigma_L$. Note that this is independent of γ.

In the γ-B-space, the region supporting {0,0,1,1} as an equilibrium is thus given by a triangle, with the lower right end of the triangle at $\gamma = 1, B = 0$.

{1,0,1,1} First, consider the on-path payoffs. Hb-types receive 1. Inside the blockchain, the reach is given by $\tilde{\rho} = (1-\sigma_{Hb})$. Hence,

$$\tilde{p}^I = \frac{\sigma_{Hb}\sigma_{Hg}}{\sigma_{Hb}(\sigma_{Hg}+\sigma_{Lg}) + (1-\alpha+\alpha\sigma_{Hb})\sigma_{Lb}}. \tag{B.26}$$

Payoffs on the equilibrium path are therefore given by

$$\begin{aligned} \pi_{Hg} &= (1-\sigma_{Hb}) + \sigma_{Hb}\tilde{p}^I + B \\ \pi_{Lg} &= \sigma_{Hb}\tilde{p}^I + B \\ \pi_{Lb} &= (\alpha\sigma_{Hb} + (1-\alpha))\tilde{p}^I + B. \end{aligned} \tag{B.27}$$

As $\Delta_{Lb} \geq \Delta_{Lg}$, there are three deviations we need to consider.

(a) Hb-types adopting the blockchain. The Hb-type would obtain $\tilde{\rho}\alpha + (1-\tilde{\rho}\alpha)\tilde{p}^I + B = (1-\sigma_{Hb})\alpha + (\alpha\sigma_{Hb} + (1-\alpha))\tilde{p}^I + B$. To deter this deviation, we hence require

$$B \leq 1 - (1-\sigma_{Hb})\alpha + (\alpha\sigma_{Hb} + (1-\alpha))\tilde{p}^I \equiv \tilde{B}_{Hb}. \tag{B.28}$$

We can plug in for $\tilde{p}^I$ and simplify. This gives

$$\tilde{B}_{Hb} = (1-(1-\sigma_{Hb})\alpha)\frac{\sigma_{Hb}\sigma_{Lg} + (1-(1-\sigma_{Hb})\alpha)\sigma_{Lb}}{\sigma_{Hb}(\sigma_{Hg}+\sigma_{Lg}) + (1-(1-\sigma_{Hb})\alpha)\sigma_{Lb}}. \tag{B.29}$$

Notably, $\tilde{B}_{Hb}$ can lie both above or below the upper bound for the {0,0,1,1} equilibrium region given by $1-\sigma_L$. To see this, consider the parametrization given by $\sigma_{Hg} = \sigma_{Lg} = 0.2$, $\sigma_{Hb} = \sigma_{Lb} = 0.3$ and contrast $\alpha = \frac{5}{6}$ and $\alpha = \frac{2}{6}$.

(b) Hg-types not adopting the blockchain. This would give a payoff of 1, so that we require

$$B \geq 1 - \left[(1-\sigma_{Hb}) + \sigma_{Hb}\tilde{p}^I\right] \equiv \tilde{B}_{Hg} > 0. \tag{B.30}$$

Clearly, $\tilde{B}_{Hg} < \tilde{B}_{Hb}$ due to $\Delta_{Hg} > \Delta_{Hb}$ from Lemma 1.

(c) Lg-types not adopting the blockchain. This would yield $(1-\gamma)\tilde{p}^O$. To deter this deviation, we hence require

$$B \geq 1 - \gamma - \sigma_{Hb}\tilde{p}^I \equiv \tilde{B}_{Lg}(\gamma). \tag{B.31}$$

It immediately follows that $\tilde{B}_{Lg}(\gamma) < 1-\gamma$, i.e. that this constraint is more permissible regarding B than the constraint required to sustain the $\{0,0,1,1\}$-equilibrium. Thus, this equilibrium is sustainable for some γ-B-combinations where the other one is not, even if $\tilde{B}_{Hb}$ lies below the constraint for the {0,0,1,1} equilibrium.

{1,0,1,0} This analysis mirrors the one for $C \geq 0$ for this equilibrium candidate, see Appendix B.5. The constraints are identical to the ones obtained there, with $B = -C$. To summarize, we require

$$\begin{aligned}
B &\geq \gamma + (1-\gamma)\hat{p}^O - \left[(\sigma_{Hg}+\sigma_{Lb}) + (1-\sigma_{Hg}-\sigma_{Lb})\hat{p}^I\right] \equiv \hat{B}_{hg}(\gamma) && \text{(B.32)}\\
B &\leq \gamma + (1-\gamma)\hat{p}^O - \left[\alpha(\sigma_{Hg}+\sigma_{Lb}) + (1-\alpha(\sigma_{Hg}+\sigma_{Lb}))\hat{p}^I\right] \equiv \hat{B}_{hb}(\gamma) && \text{(B.33)}\\
B &\geq (1-\gamma)\hat{p}^O - (1-\alpha(\sigma_{Hg}+\sigma_{Lb}))\hat{p}^I \equiv \hat{B}_{Lb}(\gamma) && \text{(B.34)}\\
B &\leq (1-\gamma)\hat{p}^O - (1-(\sigma_{Hg}+\sigma_{Lb}))\hat{p}^I \equiv \hat{B}_{Lg}. && \text{(B.35)}
\end{aligned}$$

This does not yet impose $B \geq 0$. To address this, note that the maximal B, denoted $\hat{B}^{max}$, such that this is sustainable materializes at the intersection of $\hat{B}_{Lg} and \hat{B}_{Hb}$. This obtains at $\hat{\gamma} = \rho\alpha + \rho\hat{p}^I(1-\alpha)$. Plugging in, we obtain

$$\hat{\gamma} = \frac{\sigma_{Hg}\left(1-\sigma_{Lb}\left(1+\alpha^2\right)\right) + (1-\alpha\sigma_{Lb})\alpha\sigma_{Lb} - \sigma_{Hg}^2}{1-\sigma_{Hg}-\alpha\sigma_{Lb}}, \tag{B.36}$$

which in turn implies

$$\hat{B}^{max} = \frac{\sigma_{Lb}\sigma_{Hb}(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))^2 - \sigma_{Hg}\sigma_{Lg}(1-(\sigma_{Hg}+\sigma_{Lb}))^2}{(1-\sigma_{Hg}-\alpha\sigma_{Lb})(\sigma_{Hb}+\sigma_{Lg})(\sigma_{Hg}+\sigma_{Lb})} \tag{B.37}$$

Hence, we have that

$$\hat{B}^{max} > 0 \iff \frac{\sigma_{Lb}\sigma_{Hb}}{\sigma_{Hg}\sigma_{Lg}} > \frac{(1-(\sigma_{Hg}+\sigma_{Lb}))^2}{(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))^2}. \tag{B.38}$$

Finally, we establish that the {1,0,1,0} equilibrium region is disjoint from the other two pure strategy equilibria characterized above. For this, it is sufficient to show that

$$\gamma = \sigma_{Hg} + \sigma_{Lb} \implies \hat{B}_{lg}(\gamma) < \tilde{B}_{Lg}(\gamma). \tag{B.39}$$

This is because $\tilde{B}_{Lg}$ characterizes the most permissive constraint of {0,0,1,1} and {1,0,1,1}, while $\tilde{B}'_{Lg}(\gamma) = -1 < -\hat{p}^O = \hat{B}'_{Lg}(\gamma)$. As $\gamma = \sigma_{Hg} + \sigma_{Lb}$ characterizes the highest γ such that {1,0,1,0} can be supported, this is sufficient for disjointness.

We hence need to compare

$$\tilde{B}_{Lg}(\sigma_{Hg}+\sigma_{Lb}) = 1 - \sigma_{Hg} - \sigma_{Lb} - \sigma_{Hb}\tilde{p}^I \tag{B.40}$$

with

$$\hat{B}_{Lg}(\sigma_{Hg}+\sigma_{Lb}) = (1-\sigma_{Hg}-\sigma_{Lb})\,\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}} - (1-(\sigma_{Hg}+\sigma_{Lb}))\hat{p}^I \tag{B.41}$$

To do this, observe the following:

(i) $1 - \sigma_{Hg} - \sigma_{Lb} > (1 - \sigma_{Hg} - \sigma_{Lb})\,\frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}}$ as $\hat{p}^O = \frac{\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}} < 1$

(ii) $\sigma_{Hb} < 1 - (\sigma_{Hg} + \sigma_{Lb}) = \sigma_{Hb} + \sigma_{Lg}$

(iii) $\tilde{p}^I < \hat{p}^I$. Given $\hat{\rho} < \tilde{\rho}$, it follows that

$$\hat{p}^I = \frac{(1-\hat{\rho})\sigma_{Hg}}{(1-\hat{\rho})\sigma_{Hg} + (1-\alpha\hat{\rho})\sigma_{Lb}} > \frac{(1-\tilde{\rho})\sigma_{Hg}}{(1-\tilde{\rho})\sigma_{Hg} + (1-\alpha\tilde{\rho})\sigma_{Lb}} \tag{B.42}$$

and thus

$$\hat{p}^I > \frac{(1-\tilde{\rho})\sigma_{Hg}}{(1-\tilde{\rho})\sigma_{Hg} + (1-\alpha\tilde{\rho})\sigma_{Lb}} > \frac{(1-\tilde{\rho})\sigma_{Hg}}{(1-\tilde{\rho})\sigma_{Hg} + (1-\alpha\tilde{\rho})\sigma_{Lb} + (1-\tilde{\rho})\sigma_{Lg}} = \tilde{p}^I. \tag{B.43}$$

Combining (i), (ii) and (iii) yields $\hat{B}_{Lg}(\sigma_{Hg} + \sigma_{Lb}) < \tilde{B}_{Lg}(\sigma_{Hg} + \sigma_{Lb})$.

{0,0,0,1} In this case, only Lg-types join the blockchain and obtain a payoff of 0. This payoff would also be achieved by Lb-types joining, and therefore we require $\Delta_{Lg} = \Delta_{Lb} = 0$. With $p^O = \frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lg}}$, this gives

$$\Delta_{Lg} = \Delta_{Lb} = 0 \iff B = (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lg}}. \tag{B.44}$$

In addition, Hg-types must prefer to not adopt (Hb-types then are also deterred).

$$\sigma_{Lg} + B \leq \gamma + (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lg}} \iff B \leq \gamma + (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lg}} - \sigma_{Lg}. \tag{B.45}$$

The two conditions are compatible iff $\gamma \geq \sigma_{Lg}$.

{0,0,1,0} As before, we have $\Delta_{Lg} = \Delta_{Lb} = 0$. With $p^O = \frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lb}}$, this gives

$$\Delta_{Lg} = \Delta_{Lb} = 0 \iff B = (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lb}}. \tag{B.46}$$

To deter Hg-types, it also needs to hold that

$$\sigma_{Lb} + B \leq \gamma + (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lb}} \iff B \leq \gamma + (1-\gamma)\frac{\sigma_{Hg}+\sigma_{Hb}}{1-\sigma_{Lb}} - \sigma_{Lb}. \tag{B.47}$$

The two conditions are compatible iff $\gamma \geq \sigma_{Lb}$.

B.7 Proof of Proposition 4

Given (27), we know that $\min\{\Delta_{Hg}, \Delta_{Lb}\} \geq \max\{\Delta_{Hb}, \Delta_{Lg}\}$. Defining

$$\utilde{C}_b \equiv \max\{\Delta_{Hb}, \Delta_{Lg}\} \tag{B.48}$$

$$\tilde{C}_b \equiv \min\{\Delta_{Hg}, \Delta_{Lb}\}, \tag{B.49}$$

the proposition immediately follows. Given (24), we can explicitly derive $\Delta_{Hg}, \Delta_{Hb}, \Delta_{Lb}$ and Δ_{Lg} and obtain

$$
\begin{aligned}
\Delta_{Hb} &= \rho\alpha - \gamma + (1-\rho\alpha)p^I - (1-\gamma)p^O \\
&= \alpha(\sigma_{Hg}+\sigma_{Lb}) - \gamma + \frac{(1-\sigma_{Hg}-\sigma_{Lb})(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))\sigma_{Hg}}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})} - \frac{(1-\gamma)\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}} \qquad \text{(B.50)} \\
\Delta_{Lg} &= (1-\rho)p^I - (1-\gamma)p^O \\
&= \frac{(1-\sigma_{Hg}-\sigma_{Lb})^2\sigma_{Hg}}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})} - \frac{(1-\gamma)\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}} \qquad \text{(B.51)} \\
\Delta_{Hg} &= \rho - \gamma + (1-\rho)p^I - (1-\gamma)p^O \\
&= \sigma_{Hg}+\sigma_{Lb} - \gamma + \frac{(1-\sigma_{Hg}-\sigma_{Lb})^2\sigma_{Hg}}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})} - \frac{(1-\gamma)\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}} \qquad \text{(B.52)} \\
\Delta_{Lb} &= (1-\rho\alpha)p^I - (1-\gamma)p^O \\
&= \frac{(1-\sigma_{Hg}-\sigma_{Lb})(1-\alpha(\sigma_{Hg}+\sigma_{Lb}))\sigma_{Hg}}{(\sigma_{Hg}+\sigma_{Lb})(1-\sigma_{Hg}-\alpha\sigma_{Lb})} - \frac{(1-\gamma)\sigma_{Hb}}{\sigma_{Hb}+\sigma_{Lg}}. \qquad \text{(B.53)}
\end{aligned}
$$

B.8 Proof of Proposition 5

It suffices to provide one parametrization such that this holds while (27) is satisfied. Consider $\gamma = 0.3$, $\sigma_{Hg} = \sigma_{Lb} = 0.2$, $\sigma_{Hb} = \sigma_{Lg} = 0.3$, and $\alpha > 0$, where α is sufficiently small. Clearly, (27) holds as $\sigma_{Hg} + \sigma_{Lb} = 0.5 > \gamma > 0 \approx \alpha(\sigma_{Hg} + \sigma_{Lb})$ for small α. This implies that there exist C such that $\{1, 0, 1, 0\}$ is an equilibrium. Moreover, we have

$$AMP_{noBC} = \frac{7}{20} < \frac{9}{25} = AMP_{\{1,0,1,0\}}\Big|_{\alpha\to 0}, \qquad \text{(B.54)}$$

so that the inequality holds for α sufficiently small as $AMP_{\{1,0,1,0\}}$ is continuous in α.