Blockchain Economics*

Joseph Abadi and Markus Brunnermeier†

August 25, 2018

Abstract

When is record-keeping better arranged through distributed ledger technology (DLT) than through a traditional centralized intermediary? The ideal qualities of any record-keeping system are (i) correctness, (ii) decentralization, and (iii) cost efficiency. We point out a *Blockchain Trilemma*: no ledger can satisfy all three properties simultaneously. A centralized ledger writer extracts rents due to its monopoly on the ledger. Its franchise value dynamically incentivizes honest reporting. Decentralized ledgers provide static incentives for honesty through computationally expensive Proof-of-Work algorithms but eliminate rents through "fork competition." Portability of information between "forks" and competition among miners fosters competition *among decentralized ledgers* that is fiercer than traditional competition. However, fork competition can engender instability and miscoordination. While DLT can keep track of ownership transfers, enforcement of possession rights is often better complemented by centralized record-keeping.

Keywords: DLT, Blockchain, Digital Economics, Platform Economics, Cryptocurrencies, "Fork Competition", Contestable Markets

*We are grateful for helpful comments from Zhiguo He, Stephen Morris, Ulrich Müller, and seminar participants at the St. Louis Fed, Princeton, the NYU Intermediation Conference, and the BIS.

†Abadi: Department of Economics, Princeton University, jaabadi@princeton.edu, Brunnermeier: Department of Economics, Princeton University, markus@princeton.edu

1 Introduction

Traditionally, records have been maintained by centralized entities. Distributed Ledger Technology (DLT) has provided us with a radical alternative to record information. DLT has the potential to be as groundbreaking as the invention of double-entry bookkeeping in fourteenth-century Italy. It could revolutionize record-keeping of financial transactions and ownership data.

Blockchains are a particular type of distributed ledger written by decentralized, usually anonymous groups of agents rather than known centralized parties. Consensus is attained by making the ledger publicly viewable and verifiable. Ideally, a ledger should (i) record all information correctly and do so (ii) in a cost efficient and (iii) fully decentralized manner to avoid any concentration of power. In this paper we point out a "Blockchain Trilemma": it is impossible for any ledger to fully satisfy the three properties shown in Figure 1 simultaneously.

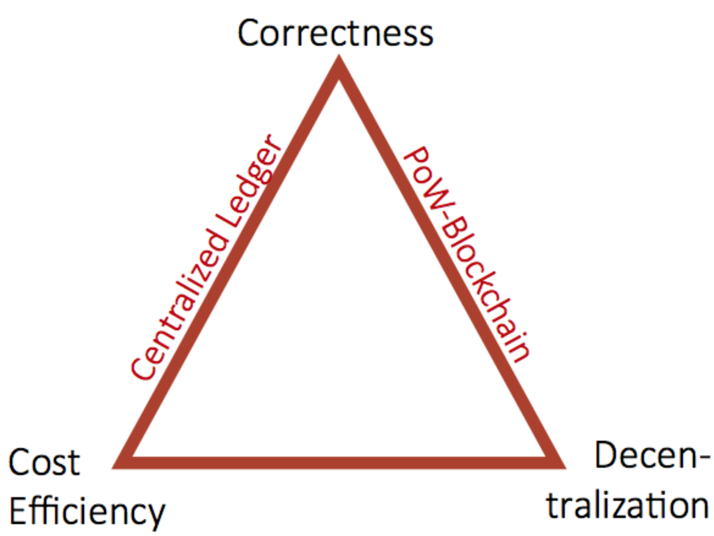

Figure 1: The Blockchain Trilemma.

Traditional ledgers, managed by a single centralized intermediary, forgo the desired feature of decentralization. The correctness of the ledger is maintained by limiting competition. A centralized ledger writer is incentivized to report honestly because he does not wish to jeopardize his future profits and franchise value. That is, a centralized ledger writer is dynamically incentivized. In contrast, decentralized ledgers promote competition but entail real inefficiencies. Competition completely erodes writers' future profits and franchise values. Consequently, dynamic incentivization of decentralized ledger writers is impossible. The ledger's correctness must rely on a mechanism that provides purely static incentives.

Blockchains allow two forms of competition that lead to two distinct inefficiencies. (i) First, there is free entry of ledger writers. As anybody can become a ledger writer (or miner) on a public blockchain, a consensus mechanism is needed to determine the true history written on the ledger (from possibly conflicting reports). Applying a majority rule is complicated by the fact that individual entities can masquerade as a large number of entities for free, subverting the democratic nature of the distributed ledger. To limit this problem and ensure honest record-keeping, ledger writers must typically perform computationally expensive tasks in order to record information and validate others' reports. The cost of writing on the ledger gives writers static incentives not to report dishonestly. (ii) Second, information on the existing ledger is made portable to possibly competing ledgers via "fork competition". A proposer of a new ledger can "fork off" an existing blockchain by establishing different rules while retaining all the information contained in the original blockchain. Fork competition erodes the rents of a ledger monopolist, but also comes at a cost: too many competing blockchains may coexist. The community of users/readers may be split among too many different ledgers (or cryptocurrencies) and fail to fully exploit positive network externalities. This entails a true efficiency loss, above and beyond the redistributive rent extraction associated with a monopolistic ledger writer or the waste of computational resources resulting from free entry. Finally, current technology limits the scalability of blockchain technology, a third cost.

We emphasize that fork competition eliminates inertia in the adoption of new, competing ledgers. In a traditional setting, ledger users are anchored to an incumbent ledger by the centralized intermediary's monopoly on the information contained in the ledger. Those with high stakes in the existing ledger are reluctant to switch to a competitor. Network externalities amplify this informational anchor, making even those with low stakes in the existing ledger unwilling to switch. When network externalities are strong, the market ceases to be contestable– even with free entry of competing ledgers, the incumbent's advantage is so great that it is able to extract full surplus from users. Fork competition eliminates the anchor on the established ledger due to the portability of information. Network externalities then play no role in amplifying inertia, and the market is *always* contestable: competing forks of the blockchain are at no disadvantage whatsoever against the established ledger.

While in most of our analysis we assume that readers use only one ledger for analytical tractability, our qualitative results extend to an environment in which readers "multi-home" by using several different ledgers simultaneously as in Rochet and Tirole (2003). Even when readers are permitted to use several different ledgers, there is an informational anchor on the established ledger that prevents adoption of new ledgers. This anchor is present as long as there is some cost to using several ledgers, but it vanishes as the cost of using an additional ledger goes to zero.

In addition to the polar cases of completely centralized traditional ledgers and completely decentralized blockchains, there is a third type of ledger called a “permissioned” blockchain that shows promise in many applications. The writers of a permissioned blockchain are known agents rather than anonymous miners, so Proof-of-Work is unnecessary. Permissioned blockchains then seemingly break the Trilemma: they allow for fork competition, like anonymous blockchains, but completely eliminate the waste of resources. We show that the impediments to entry of writers on a permissioned blockchain substantially weaken fork competition. Permissioned writers have franchise values and therefore can collude to prevent competing forks from surviving, whereas dynamic punishment schemes that sustain collusion are impossible when there is free entry of writers.

Finally, we make the important point that while blockchains guarantee transfers of *ownership*, some sort of enforcement is required to ensure transfers of *possession*. For example, in a housing market the owner of the house is the person whose name is on the deed, but the possessor of the house is the person who resides in it. The buyer of the deed needs to be certain that once she holds the deed, her ownership of the house will be enforced. In the stock market, the purchaser of a share has ownership of future dividends but not necessarily possession, since the delivery of dividends needs to be enforced. Broadly, blockchains can record obligations. Punishing those who default on their obligations is another matter. While it is difficult to provide static incentives for blockchain writers to impose discipline on users of the ledger, centralized intermediaries’ incentives can be appropriately aligned: if a centralized intermediary fails to guarantee transfers of possession, the ledger’s users can abandon the ledger, destroying the intermediary’s franchise value.

Blockchains have applications that reach far beyond the realm of cryptocurrencies and tokens. For instance, blockchains could be used in the fintech space to track consumers’ transaction and credit histories. Permissioned blockchains have also been suggested as a tool to manage supply chains and track the delivery of items in real time. There are several potential applications of blockchains that, if pursued, will require enforcement by intermediaries or legal entities. Banks could use blockchains to track interbank loans or manage their clients’ collateral, both of which require mechanisms to ensure debtors will repay their creditors. Governments may also turn to blockchains to maintain land registries, which could be useful in developing countries where the primary institutional friction is overly bureaucratic record-keeping processes, but seems likely to be unhelpful when the issue is instead that the government enforces ownership selectively.

Related Literature. The paper most closely related to ours is Biais et al. (2017), which studies the stability of a blockchain-based system. It shows that while the strategy of mining the longest chain proposed by Nakamoto (2008) is in fact an equilibrium, there are other equilibria in which the blockchain forks, as observed empirically. In that model, forks occur for several reasons and are interpreted as causing instability. Writers' payoffs when forking depend exogenously on the number of writers who choose a given branch of the fork. In our model, writers' payoffs are instead determined by readers' preferences, which puts more discipline on exactly how and when a fork may occur. Cong and He (2017) focus mostly on the issue of how ledger transparency leads to a greater scope for collusion between users of the system. In contrast, we consider collusion between writers of the blockchain rather than users and show that collusion can occur only when entry of writers is constrained.

Some of the recent literature on blockchains in economics focuses on the security and the costs of the system. Easley, O'Hara, and Basu (2017) use a game-theoretic framework to analyze the emergence of transaction fees in Bitcoin and the implications of these fees for mining costs. The R&D race between Bitcoin mining pools is described in Gans, Ma, and Tourky (2018), who argue that regulation of Bitcoin mining would reduce the overall costs of the system and improve welfare. Huberman, Moallemi, and Leshno (2017) study transaction fees in Bitcoin and conclude that the blockchain market structure completely eliminates the rents that a monopolist would extract despite the fact that only one miner processes transactions at a time. We depart from these analyses by endogenizing the mechanism used by the blockchain: in our model, users of the system essentially choose between competing mechanisms on different branches of a blockchain fork. The cost of implementing a given mechanism is pinned down by the free entry condition.

Our framework uses a global game of the type pioneered by Carlsson and van Damme (1993) in order to select a unique equilibrium. Rather than review the massive literature on global games here, we refer the reader to Morris and Shin (2001) for an extensive and general analysis of the global games framework. We use techniques from the more recent literature on global games with non-Gaussian private values pioneered by Sakovics and Steiner (2012) and advanced by Drozd and Serrano-Padial (2017). Our work is also related to the recent literature on the importance of network externalities in blockchain payment systems. Sockin and Xiong (2018) show that strategic complementarities in cryptocurrency holdings lead to fragile equilibria with different cryptocurrency prices. Cong, Li, and Wang (2018) argue that expectations of growth in a blockchain's participation impact the current price of its native token. Our paper differs from these studies in that we analyze the importance of network externalities for arbitrary blockchains rather than just cryptocurrency blockchains and show that these externalities interact with the replicability of information on a blockchain in an important way.

We also relate to the literature on cryptocurrencies. Chiu and Koeppl (2017) develop a macroeconomic model in which the sizes of cryptocurrency transactions are capped by the possibility of a double-spend attack and derive optimal compensation schemes for writers. Schilling and Uhlig (2018) study cryptocurrency pricing in a monetary model and derive necessary conditions for speculation to occur in equilibrium. Pagnotta and Buraschi (2018) derive a pricing framework for cryptocurrencies that explicitly accounts for the interplay between demand for the currency and the cryptographic security provided by miners.

Recent computer science literature has studied blockchain security extensively. Most papers in computer science, such as Gervais et al. (2016), study how to defend against "double-spend" attacks or other types of attacks that could be undertaken by a single individual who holds control over a large portion of the network's computing power. The conclusion of studies in the computer science literature is that a large fraction of the blockchain writers must always play honestly in order for the network to be secure. In such models, writers are prevented from deviating by other writers who discipline them. Writers are implicitly prevented from colluding in any way. In contrast, we study a more general type of attack without explicitly referring to double-spending. Our model shows that the cost of operating a blockchain is intrinsically linked to the cost of preventing attacks, no matter what they may be. Furthermore, our model shows that the implicit assumption of no collusion is unnecessary. The impossibility of dynamic collusion between writers on a blockchain is a characteristic that emerges naturally from the free entry condition.

Finally, our paper is related to the literature on optimal intermediation structures. Most notably, Diamond (1984) shows that when monitoring is costly, it is most efficient to use a single intermediary. In contrast, in our framework it is optimal to have several intermediaries because competition in writing on the ledger yields outcomes that are more desirable for the blockchain's users. In the computer science literature, Wüst and Gervais (2017) study the applicability of blockchain to several markets from an informal standpoint.

The rest of the paper is structured as follows. Section 2 discusses the basics of blockchain technology. In Section 3, we present the baseline model of a static choice between ledgers. We analyze a specific example where agents choose between two branches of a blockchain fork and another example in which agents choose between traditional ledgers in order to spell out the tradeoffs between decentralization and cost-efficiency. Section 4 extends the static model to a repeated setting and studies permissioned blockchain as well as the security features of traditional ledgers and blockchains. Section 5 discusses practical issues related to blockchain technology including some points that we do not address in our formal model, such as the transfer of physical assets on a blockchain. Section 6 concludes.

2 Blockchain Technology

In this section we outline how blockchains work and the distinguishing features of blockchains with anonymous writers.

2.1 What is a blockchain?

A blockchain is a ledger in which agents known as writers (or nodes) take turns recording information. This information could consist of payment histories, contracts outlining wagers between anonymous parties, or data on ownership of domain names, among other applications. As discussed later, there are many possible algorithms to select the current writer. The ledger consists of a tree of blocks that contains all the information recorded by writers starting from the first block, which is called the *genesis block*. Each branch of the tree corresponds to a chain leading back to the genesis block (hence the name "blockchain").

A chain of blocks leading back to the genesis summarizes a state. Readers and writers of the ledger must reach a consensus about which state is considered the valid state. Typically, the community coordinates on the longest chain of blocks as the valid state, as suggested in Nakamoto (2008). Each writer is periodically allowed to add a block to the tree. Writers usually extend only the consensus chain, and readers will act only in response to events on that chain. A writer's decision to extend a given chain can be seen as a signal that the writer accepts that chain as valid. Writers are rewarded for achieving consensus through readers' acceptance of the chain they extend. In general, writers accrue rewards and transaction fees for each block added to the tree, so these rewards are realized only if those fees are on the consensus chain.

However, it is in principle possible for readers and writers to coordinate on a chain other than the longest one or even for different communities to coordinate on separate chains. A "hard fork" occurs when part (or all) of the community decides to change the rules governing the blockchain. To do so, they start their own blockchain that builds off of the old chain, but they ignore any writers who do not follow the new rules. Similarly, writers who use the old rules will ignore all writers who use the new ones, so the blockchain effectively forks and becomes two blockchains. The data contained in the original chain is included in both of the new blockchains, but neither blockchain uses data that was recorded on the other after the fork occurred. Hard forks will feature prominently in our model and will intensify competition between ledgers by allowing information from the original blockchain to be replicated on a competing ledger.

For example, in 2016 the Ethereum community split after a hack that stole \$55 million from investors in a contract on that blockchain. Some Ethereum users argued that the currency should be returned to the investors, whereas others believed the blockchain should be immutable. The users who believed the currency should be returned ignored all blocks occurring after the hack and built their own chain on which the hack never occurred. After this point, both sides began ignoring the blocks built by the other side, and each part of the community considered only its own chain to be the valid chain.

On any blockchain, there are some rules that readers and writers tacitly agree to follow. These rules are written into the code distributed by the software developers for that blockchain. For example, cryptocurrency transactions are signed cryptographically by the sender of the transaction. Whenever blockchain writers receive a message to add a given transaction to a block, they can perform a cheap computation to verify that the sender properly signed the transaction. If the verification fails, the transaction is considered fraudulent. Writers who follow the rules will refuse to add any such transaction to a block. In general, blockchain security algorithms work so that it is inexpensive for writers to confirm that the rules are being followed. If a previous writer added fraudulent transactions to a block at the end of the longest chain, the consensus algorithm prescribed by Nakamoto (2008) specifies that all other writers should ignore that particular block and refuse to put other blocks on top of it.

Another example of rules that blockchain users agree to follow are the rules for writers' compensation. For instance, Bitcoin miners are awarded a certain number of coins for finding a block. All other writers must check that the miner who found the last block did not attempt to circumvent the blockchain's policies by minting more coins than what is allowed. In most of our analysis we will suppose that the network is sufficiently secure to ensure that the rules are followed. We focus on which rules for writer compensation emerge in equilibrium when there is scope for competition between ledgers. In an extension of our model, we examine how the rules are enforced in the first place.

An attack on a blockchain involves the addition of blocks that are somehow invalid. Either the blocks contain outright fraudulent transactions, or they are added somewhere other than the end of the longest valid chain. It is clear that attackers stand to gain by adding fraudulent transactions to their blocks simply because such a strategy allows them to steal from others as long as other readers and writers go along with the attack, but these attacks are usually automatically detected by all users of the system. It is perhaps less obvious why an attacker would want to add valid blocks somewhere other than the end of the longest chain. The key observation is that this type of attack permits dishonest actors to reverse transactions or records written on the longest valid chain. If an attacker or group of attackers controls the majority of the computing power on the network, even if this group's chain of blocks begins behind the longest valid chain written on by others, eventually the length of the attackers' chain will exceed that of the other chain. At this point it becomes the longest valid chain. All writers (both the honest ones and the attackers) then write on the attackers' chain.

In cryptocurrency blockchains, this type of attack is commonly referred to as a double-spend attack. An attacker will spend some currency on the longest valid chain, wait to obtain the goods purchased, and then begin building an alternative chain on which the currency was never spent, absconding with both the goods and the money. Double-spends are by far the largest security concern of the cryptocurrency community. This type of attack is also possible when the blockchain in question handles assets other than currency. For example, a financial institution that loses money on a trade may wish to reverse the history of transactions including that trade. Our model extension embeds double spending, but it encompasses a broader class of attacks.

2.2 The Types of Blockchains

There are three main types of blockchains. In a private blockchain, a single centralized entity has complete control over what is written on the ledger. That is, there is only one writer. The readers in this situation could be the public, the entity's clients, or a regulator. Different groups may also have different types of read privileges on the ledger: for example, a regulator would likely need to see the entire ledger, whereas a client may be content to see only those transactions that are relevant to her. There is no need for identity management with a private blockchain, since only one entity is permitted to write on the ledger. Therefore, there are no computational costs and the system functions similarly to a privately maintained database that gives read privileges to outsiders. In this system, the writer is disciplined entirely by the readers, who may decide to punish the writer in some way when the writer changes the ledger's rules (or fee structure) or if they detect some sort of fraudulent activity. One way in which this sort of punishment could arise in reality is if an online platform like Amazon decides to raise subscription rates for vendors and vendors respond by switching to a competitor.

A permissioned blockchain is one in which the write privilege is granted not to one entity, but to a consortium of entities. These entities govern the policies of the blockchain and are the only ones permitted to propagate and verify transactions. The read privilege may be granted to the public or kept private to some extent. The permissioned writers take turns adding blocks to the chain according to a predefined algorithm, so again costly identity management is unnecessary. The writers on a permissioned blockchain are disciplined by readers, just as in a private blockchain, but they are also disciplined by other writers. If one writer deviates and begins validating fraudulent ledger entries by including them in his block, other writers may ignore him and refuse to extend his chain. If a writer proposes a change of the blockchain's policies, other writers may prevent such a change by writing according to the existing policies.

The third and most common type of blockchain is a public blockchain. In a public blockchain, both the read and write privileges are completely unrestricted. Writers are disciplined exactly as in permissioned blockchains. All users of the network are anonymous. However, when writers are allowed to be anonymous, some sort of identity management is necessary. Otherwise, it would be possible for a small entity to pretend to be a large entity, allowing it to add blocks more often than others and hence giving it significant power over which chain of transactions is accepted as valid. This type of attack is known as a "Sybil attack." The typical approach to identity management is to force writers to prove they have accomplished a computationally difficult task before permitting them to write on the ledger. This method is known as Proof-of-Work (PoW) and is used by most major cryptocurrency blockchains, such as Bitcoin, Ethereum, and Litecoin. In order to incentivize writers to perform these expensive computations, they are usually rewarded with seignorage and transaction fees for each block added to the chain. The structure of a blockchain's rewards gives rise to the free entry condition for that particular blockchain. The costs of writers' rewards tend to be economically large. For example, the Bitcoin blockchain currently uses more electricity than Hungary.

3 Ledger Choice Model

In this section, we present a general model of ledger choice as a coordination game. Our objective is to be able to capture a variety of settings in which readers choose among competing ledgers with different rules or policies. Our leading example applies our model to study competition between two branches of a blockchain fork. We then contrast the model of two competing blockchains with a model in which two traditional ledgers compete. We also examine a hybrid model of competition between a traditional ledger and a blockchain, and in the next section we extend the model to a dynamic setting and analyze the differences between a permissionless blockchain and a permissioned blockchain. The specific examples of competition between different types of ledgers will illustrate the tradeoffs suggested by the Blockchain Trilemma.

We focus on the importance of coordination because many types of ledgers are useful only if they are widely used. For example, consumers will want to hold a fiat currency only if it is accepted by most vendors. Another situation in which coordination is important is when the ledger contains information about user's creditworthiness (such as Alibaba's Sesame credit score system)– users will not have an incentive to build up their credit score if there are no lenders. Throughout, we will abstract from the specific details of the coordination motive.

There are two ledgers A and B. There is a continuum of agents $i \in [0,1]$ known as readers, who are users of the service offered by the ledger. There is a set of agents $j \in \mathcal{M}$ known as writers. These agents correspond to those who maintain the ledger. For a cryptocurrency blockchain, these agents would be miners. For a traditional payments ledger, a single centralized intermediary (such as the Federal Reserve or a bank) is usually the sole writer. Finally, there are two agents known as proposers, P^A and P^B. These proposers are responsible for choosing the rules under which the ledger operates. Software developers are the "proposers" for a blockchain. When a part of the community wants to fork the blockchain, a developer will write commonly accepted code that implements the desired changes to the rules. On the other hand, for a traditional ledger the proposer is also the writer. That is, the monopolist who runs the ledger also decides on the rules. In what follows, we will allow for the possibility that some writer $j \in M$ is also one of the proposers.

Readers must choose the extent to which they participate on ledgers A and B. Reader i chooses an action $\varphi_i = (\varphi_i^A, \varphi_i^B) \in [0,1]^2$, where φ_i^l is the reader's usage of ledger $l \in \{A, B\}$. Readers will desire to coordinate with other readers, so their utility functions will depend on $\phi^l = \int_0^1 \varphi_i^l di$ for $l \in \{A, B\}$.

Readers are heterogeneous in their *fundamental* preferences for ledgers. Each reader is assigned a type $s_i = (s_i^A, s_i^B)$. Here s_i^l is meant to represent the *stake* that agent i has in ledger l. The stake that a reader has in a given ledger should be interpreted as the amount of information pertaining to that reader that is encoded in the ledger. For any ledger that keeps track of asset holdings, a reader's stake is simply the set of assets held by that reader, with larger asset holdings being interpreted as a higher stake. However, a reader's stake does not necessarily have to represent the market value of some asset. A reader with a high stake may also be a consumer who has built up a high credit score in a credit registry or a financial institution with a complex set of contracts with other institutions written down in a particular ledger. Stakes could even be interpreted as ratings on e-commerce websites or contacts on social media platforms. We denote the population CDF of stakes s by $Q(s)$.

There is also a common value component ζ in readers' preferences. This component can be understood as parametrizing differences between fundamental features of the two ledgers, such as technological efficiency. When $\zeta > 0$, the common value induces a preference for A among all readers, and when $\zeta < 0$, readers prefer B. While parameter ζ itself does not play a significant role in our analysis, the introduction of uncertainty about this parameter will lead to equilibrium selection.

Each proposer P^l chooses a fundamental parameter $L^l \in \mathcal{L}^l$ determining the revenues earned by writers and charged to readers. A simple way of thinking about L^l is as an explicit fee charged to readers by the writer(s) of the ledger, but more broadly L^l could be interpreted as an implicit fee. Such implicit fees could arise, for instance, if a monopolist who runs a ledger chooses to sell readers' data to an outside party. The fundamental parameter L^l could also represent a goverment's choice of policy, such as inflation. For example, a government may wish to inflate away its debt, but doing so could be costly for people who hold the currency, who may then collectively decide to abandon the national currency altogether (as in Zimbabwe). Henceforth we will refer to L^l as a fee for ease of exposition.

Writer j will choose a ledger $l \in W_j \subset \{A, B\}$ and take an action $a_j \in \mathcal{A}_j$ to write on the ledger. In our applications, the action a_j will refer either to an expenditure of computational resources to ensure cryptographic security of the ledger (proof-of-work) or an action taken by a dishonest writer to distort the ledger (such as a double spend or outright fraud by a monopolist). That is, the actions taken by writers will capture two points of the Blockchain Trilemma: cost efficiency and correctness.

A reader's utility depends on (i) her own action φ, (ii) her stakes s, (iii) others' participation choices $\phi = (\phi^A, \phi^B)$, (iv) the common value ζ, (v) the fundamental parameter $L = (L^A, L^B)$ chosen by proposers, and (vi) actions a taken by writers. In general, a reader's utility function can be written as

$$u(\varphi, s, \phi, \zeta, L, a)$$

A writer's utility when writing on ledger l depends on the action a_j^l taken by that writer, the actions a_{-j}^l taken by other writers on the same ledger, usage of the ledger ϕ^l, and the fee L^l. The corresponding utility function will be denoted by

$$w^l(a_j^l, a_{-j}^l, \phi^l, L^l)$$

Finally, the utility of proposer P^l is given by by a function $v(\phi^l, L^l)$.

The game is played in periods $t = 0, 1, 2, \ldots$. Each period has three subperiods $\tau = 0, 1, 2$. The timing of the game is as follows:

$\tau = 0$: Proposers P^A and P^B choose L^A and L^B, respectively.

$\tau = 1$: Readers first observe previous actions and their own types s_i. They then choose actions φ.

$\tau = 2$: Writers observe previous actions and choose a ledger $l \in W_j$ and take actions $a_j \in \mathcal{A}$. Payoffs are realized.

3.1 Characterization of equilibrium with arbitrary competing ledgers

We now prove properties of equilibrium that will hold in all of the settings we consider. First, we show that as noise about the common value vanishes, readers' play is uniquely pinned down in equilibrium. We also characterize the multiplicity of equilibria in a benchmark setting where readers' types are identical. Here we restrict attention to pure-strategy Perfect Bayesian equilibria of the ledger choice game. For a formal definition of Perfect Bayesian equilibrium, we refer the reader to Fudenberg and Tirole (1991).

In the following analysis, we impose the restriction that readers must choose either A or B when choosing a ledger, not both. In the notation of the previous section, they choose $\varphi \in \{(1,0),(0,1)\}$. Under this assumption, it is natural to consider

$$\tilde{u}(s,\phi,\zeta,L,a) \equiv u(A,s,\phi,\zeta,L,a) - u(B,s,\phi,\zeta,L,a)$$

(with some abuse of notation). Readers choose A when they expect $\tilde{u}$ to be positive and B when they expect $\tilde{u}$ to be negative. For ease of notation, we will henceforth denote a choice of A as $\varphi = 1$ or $\varphi = A$ and set $\phi = \int_i \varphi_i di$ to be the proportion of readers who choose A.

We will also take writers' actions (as a function of ϕ and L) to be known by readers at $\tau = 1$. In our main applications, readers will know the actions writers must take in equilibrium at $\tau = 2$ by backwards induction. In this section, then, we focus on the equilibrium of the game played by readers. We defer the discussion of the equilibrium among proposers until later, as it will depend on the particular application. Finally, we render readers' individual types one-dimensional rather than two-dimensional by assuming that u depends on the stakes s_i^A and s_i^B only through their difference $s_i^A - s_i^B$, and denote this difference by s_i henceforth.[1]

The assumptions that (1) readers may choose only one ledger, and (2) readers' stakes are fixed and nontradable are stark and merit further discussion. Although readers may choose only one ledger in our benchmark model, we later extend the model to allow readers to use both ledgers simultaneously, and most of our main results carry over in that framework. We assume that readers choose only one ledger primarily for ease of exposition.

The assumption that readers' stakes are non-transferable is suitable in some cases, such as when the ledger contains information about readers' types or reputations. For example, vendors on online platforms cannot trade their reputation scores to other vendors, and users of credit registries cannot transfer their credit scores amongst themselves. However, in the case of currency, this assumption is completely counterfactual: if two people with stakes in different currencies trade those currencies with each other, they relinquish their stakes in one ledger to obtain a stake in another. We remedy this issue by later presenting a more explicit model in which the ledger contains currency holdings and show that, although the results are somewhat more complicated, the main intuition regarding the importance of information portability and free entry of writers continues to hold.

[1] In our applications, this assumption will be without loss of generality.

In the following results, we will focus on the case where network externalities are "strong" in the sense that the only stable equilibria are those in which all readers choose A or all choose B.[2] These cases are particularly important because there are multiple equilibria, so we will need to develop a method of selecting among them. In our applications of the model, we will also consider cases in which network externalities are weak, but in those cases the equilibrium will be unique regardless, meaning equilibrium selection is irrelevant.

Concretely, we focus on regions of the parameter all readers play the same action, it is individually rational for any type s to follow suit. Furthermore, mixed equilibria where some readers play A and others play B are not robust to small perturbations of strategies.

To select among equilibria, we use a global games framework and introduce incomplete information about the common value ζ. Formally, we assume that each reader i receives a signal $x_i = \zeta + \sigma\eta_i$, where η is uniformly distributed on $[-\frac{1}{2}, \frac{1}{2}]$. We typically work in the limit $\sigma \to 0$, so there is an arbitrarily small amount of noise in agents' signals.[3] Incomplete information about this value could be motivated by, for example, uncertainty about the properties of the ledger's technology. With incomplete information about ζ, readers' types become two-dimensional. An individual reader's type can be summarized by $\theta_i = (x_i, s_i)$.

The main property of equilibria that we can prove at this point is that equilibria will take a "cutoff" form: there will be threshold values $k(s)$ such that all agents with $x_i < k(s_i)$ choose ledger B and all readers with $x_i > k(s_i)$ choose ledger A. These cutoffs will be decreasing in s, meaning agents with larger stakes in ledger A will be more likely to choose A. This is true as long as the actions taken by writers are the same on ledgers A and B. That is, readers sort themselves across ledgers according to their preferences. Those whose fundamental preferences for A are above a certain bound will choose A and all other readers will switch to B.

Proposition 1. *There is an essentially unique equilibrium of the game played by readers at $t = 1$ holding fixed the actions of writers at $t = 2$. There exist weakly monotonically decreasing cutoffs $k(s)$ such that all readers with $x_i > k(s_i)$ choose $\varphi_i = A$ and all readers with $x_i < k(s_i)$ choose $\varphi_i = B$.*

The proof of Proposition 1 relies on standard techniques from the global games literature with heterogeneous preferences, as in Sakovics and Steiner (2012) or Drozd and Serrano-Padial (2017). The logic behind the proof is as follows. In this setup, there are certain types s whose fundamental preferences for ledger A are so strong that it is a dominant action to choose A even if all other agents choose B. We call this set of types a "dominance region." Then some other types who strongly prefer A will choose A as well, since on top of their

[3]Readers' priors over ζ become irrelevant in this limit.

fundamental preference for A they know that all types in the dominance region choose A. This logic can be iterated to derive a unique equilibrium under certain conditions. The actions of types with extreme fundamental preferences are "contagious" and induce even types with mild preferences for one ledger over the other to take a given action. It is possible to find the set of types who choose B in exactly the same way.

We can provide a sharper characterization of equilibrium when network externalities are strong. Before doing so, we define an important symmetry property of readers' utility functions.

Definition 1. *Let $\chi = (\zeta, L, a(\phi, L))$. Define $\tilde{u}$ to be **symmetric** at χ if $\tilde{u}(s = 0, \phi, \chi) = -\tilde{u}(s = 0, 1 - \phi, \chi)$ for all (φ, ϕ). Define $\tilde{u}$ to be **asymmetric towards** A at χ if there exists a symmetric $\tilde{u}'$ such that $\tilde{u} \geq \tilde{u}'$.*

When $\tilde{u}$ is symmetric, it simply means that readers consider the fundamentals of the two ledgers to be equivalent, so differences in the utilities they obtain from using the two ledgers are due only to differences in stakes and participation on each ledger. By contrast, when $\tilde{u}$ is asymmetric towards A, readers prefer the fundamentals of A to those of B.

Equipped with this definition of symmetry, we may prove our main result regarding the properties of the equilibrium played by readers.

Proposition 2. *When network externalities are strong, all types $s \in \operatorname{supp} Q$ share the same cutoff k. This cutoff satisfies two properties.*

1. *Let $\chi = (\zeta, L, a)$ and consider the type $s = 0$ (types with the same stake in A and B). If u is symmetric at χ, then when $\operatorname{supp} Q = \{0\}$, $k = \zeta$.*

2. *If $\tilde{u}$ is asymmetric towards A and $\operatorname{supp} Q \subset \mathbb{R}_+$, $k < \zeta$.*

The characterization of equilibria in games with strong network externalities demonstrated by Proposition 2 is actually quite natural. First, the proposition states that when network externalities are strong, all agents must use the same cutoff k (so that all readers choose the same ledger in equilibrium). If there exist fundamentals (ζ, L, a) of the two ledgers are such that readers would be indifferent between them in the absence of network externalities, the cutoff k is equal to ζ as long as all readers' stakes are equal to zero. Put simply, readers coordinate on the ledger with more favorable fundamentals when their stakes do not anchor them to one ledger. On the other hand, when readers' stakes in A are larger than their stakes i B, $k < \zeta$, meaning readers may coordinate on A even when the fundamentals (ζ, L, a) favor B.

When readers have larger stakes on one of the two ledgers, that ledger has a competitive advantage in the coordination game played by readers. For example, if A is an established ledger and B is a newly proposed one, A will have an advantage over B unless the information from A is ported over to B. Later, in our analysis of the differences between blockchain and centralized systems of record-keeping, we will emphasize the enhanced portability of information allowed by blockchain. In that sense, blockchain will also alter the equilibrium of the game played by readers. However, the differences between the two systems are not limited to the equilibrium of the game played by readers– there will be differences in the play of writers and proposers as well.

3.2 Competition between distributed ledgers

In this section, we present our baseline model of competition between blockchain ledgers and analyze the equilibria of the stage game. In reality, this competition corresponds to a "hard fork," in which some of the blockchain's writers decide to build their own blockchain with new protocols off of a previously existing (parent) blockchain. Critically, a hard fork preserves all of the data in the parent blockchain. This observation will be crucial for our conclusions: the ability of writers to change the rules of the blockchain but keep readers' stakes in the network intact will allow for perfect competition between ledgers. There will be no inertia in switching ledgers because readers will lose nothing by doing so as long as all other readers switch as well. Blockchains will enhance competition between ledgers, but they will come at the cost of proof-of-work, the first (and most important) cost of decentralization. This example will thus illustrating one aspect of the decentralization-cost efficiency tradeoff postulated in the Trilemma.

The model of blockchain competition falls within the general class of models of ledger competition described earlier. In the game, readers must coordinate on a ledger (branch of a blockchain fork), which corresponds to choosing a ledger A or B. We take A to be the branch that keeps the rules of the existing blockchain. This branch has fees L^A and readers have stakes s_i^A on that branch. That is, we constrain the proposer P^A to choose L^A. This proposer can be thought of as one of the original developers of the blockchain. The proposer on branch B may choose a new fee $L^B \geq 0$ after observing ζ at $\tau = 0$ (so proposers have perfect information about ζ). Furthermore, in a hard fork, all of the information on the original blockchain is *carried over to the new blockchain*, meaning that readers' stakes on ledger B are $s_i^B = s_i^A$ for all i, so $s_i = s_i^A - s_i^B = 0$. In this sense, the established ledger A has no informational advantage over the entrant ledger B. Proposer P^B can be thought of as a blockchain software developer who wants to fork the blockchain and therefore chooses new protocols but keeps all users' data intact. If participation on the ledger proposed by P^B

is ϕ^B, P^B receives a payoff $-\tilde{u}(s = 0, \phi, \zeta, L^B, C)$, where g_P is a decreasing function of L_B. The proposer's payoff is assumed to come from an appreciation of the developer's stake when the proposed ledger is adopted, so proposers' incentives are aligned with readers'.[4]

In this setting, the set M of writers is a continuum $[0, M]$, where M is taken to be large. We assume there are two branches of the fork, branch A and branch B. Writers are responsible for cryptographically securing the ledger, and they are given some surplus for contributing computing power to the blockchain. At $\tau = 2$, writer j chooses a ledger $l_j \in \{A, B\}$ and an amount of computational power $c_j \leq 1$ to contribute to that ledger. We assume that writers can observe readers' actions before making a decision because in practice, this is often exactly what happens. Cryptocurrency "mining pools" are set up to automatically mine on whatever blockchain yields the highest profits at that moment. To the extent that the token price on a blockchain proxies for participation on that blockchain, mining pools essentially condition their decisions on users' actions.

Writers pay a linear cost $f(c) = c$ of generating computational power. Let $C^l = \int\limits_{l_{j'}=l} c_{j'} dj'$ be the total computational power contributed to branch l of the fork, and denote the participation on that fork by ϕ^l. Then a writer's net profits when contributing computing power c_j to branch l are

$$w(c_j, C^l, \phi^l, L^l) = \frac{c_j}{C^l} \phi^l L^l - c_j$$

when $C^l > 0$ and $-c_j$ otherwise. The writer's revenues are proportional to participation and the fundamental parameter L^l but are inversely proportional to the computational power contributed by other writers. This revenue function captures two features shared most blockchains. Namely, (1) the total rewards given to writers are fixed, and (2) those rewards tend to be more valuable when the blockchain has been adopted by a larger group of users.

The first important feature of the equilibrium with blockchain competition is that writers' actions are pinned down by the free entry condition. Optimizing w with respect to c_j, we see that the optimal computing effort c_j^* is given by

$$c_j^* = \begin{cases} 1 & C^l < \phi^l L^l \\ \in [0, 1] & C^l = \phi^l L^l \\ 0 & C^l > \phi^l L^L \end{cases}$$

[4]The assumption that the proposer's incentives are aligned with those of readers is not overly restrictive in this context. As we will show, free entry of blockchain writers implies that no matter what the fee structure, writers will not earn positive profits, so there is no way that the proposer could benefit writers by choosing a higher fee.

Hence in equilibrium it must be that writers break even:

$$C^l = \phi^l L^l \tag{1}$$

We later show that this result extends to all equilibria of the full dynamic game. Intuitively, with free entry writers will compete to write on the ledgers used by readers and do not leave opportunities for profit on the table. Free entry thus distinguishes a public blockchain from a permissioned blockchain, which, as we show later, can feature equilibria in which writers collude in order to suppress competing ledgers.

Readers prefer ledgers that are cryptographically secure. Their preferences for cryptographic security are parametrized by a bounded utility function $\tilde{u}(s, \phi, \zeta, L, C)$ (where $C = (C^A, C^B)$) that depends on writers' actions only through the ratios $\frac{C^l}{\phi^l}$,[5] is increasing in the ratio $\frac{C^A}{\phi^A}$, and is decreasing in the ratio $\frac{C^B}{\phi^B}$. That is, readers value security in terms of the amount of computational power committed to the blockchain per user, so they prefer ledger l when more computing power is committed to that ledger. For now, we keep this dependence exogenous and discuss the benefits of fork competition. In our discussion of attacks on the blockchain we outline how it can be endogenized and discuss the tradeoff between free entry of writers and costly proof-of-work in greater detail.

Now that we have set up the blockchain game, we may prove our main result about equilibria of the blockchain competition stage game.

Proposition 3. *Suppose that network externalities are strong and that there exists $\bar{\zeta}$ such that $\tilde{u}$ is symmetric taking as given equal fees on the two ledgers $L^B = L^A$ and optimal equilibrium play by writers, $C^l = \phi^l L^l$. Then if there exists $L^B \geq 0$ such that $\tilde{u}$ is asymmetric towards B at $\bar{\zeta}$ with fees $L = (L^A, L^B)$ and optimal equilibrium play by writers, there exists a unique equilibrium of the stage game when $\zeta \leq \bar{\zeta}$. In this equilibrium, proposer P^B announces*

$$\tilde{L}^B = \arg\min_{L^B} \tilde{u}(s = 0, \phi = 0, \zeta, L, C(\phi, L)),$$

all readers and writers choose ledger B, and writers break even.

Proposition 3 is a remarkable result. It states that in a setting in which there is an opportunity to fork a blockchain, readers will always choose the branch of the fork on which writers receive the lowest revenues, and proposers (developers) will propose rules that are beneficial to readers rather than writers.[6] Figure 2 depicts an example of the equilibrium of

[5] Of course, some value must be assigned to the function at $\phi^l = 0$. This value can be essentially arbitrary so long as readers' utility when $C^l = 0$ does not change with ϕ^l. That is, when no computing power is contributed, readers' utility is independent of participation.

the blockchain game. Of course, the result that proposers suggest protocols that are beneficial to readers depends partly on the assumption that proposers' incentives are aligned with those of readers, but in a setting with free entry of writers this assumption is not overly restrictive. Writers always make zero profits, so proposing a ledger that increases writers' revenues is pointless. Furthermore, readers choose to switch to ledger B only because they do not stand to lose their stakes when doing so. The replicability of information on ledger B completely removes an obstacle to switching ledgers. We will show that when information cannot be replicated on a competing ledger, readers' stakes impede switching to a ledger where writers earn lower revenue.

Proposition 3 highlights the benefits of a blockchain. When all readers' fundamental preferences for an alternative ledger are identical, the absence of switching costs induces full coordination on the competing ledger. There is perfect competition among ledgers in that as long as it is feasible to make ledger B even slightly more desirable than ledger A, the competing ledger will win out over the existing one. Remarkably, there is perfect competition between ledgers. Coordination inefficiencies are precluded under these assumptions, but in the next subsection we discuss how coordination can break down when readers have heterogeneous fundamental preferences.

Popular discussion has largely focused on the ways in which blockchains can decrease essentially exogenous costs, such as by inducing faster consensus about a ledger's contents. This result shows that there is an *endogenous* channel through which blockchain reduces the cost of maintaining a ledger: the synergy between *portability of information* and *competition among writers*. When information can be ported to an outside ledger, readers will want to use that ledger if writers are paid lower fees. Individually, writers are better off writing on a ledger with high fees, but competitive forces drive writers to undercut each other by writing on the ledger with lower fees. Writers know that all readers will use the outside ledger when there are enough writers to secure it, so the end result is that all writers must switch to the outside ledger. The downside of a blockchain is that while in a traditional setting writers' fees simply represent a (possibly distortionary) transfer, in the case of blockchain writers' fees are a pure waste of resources. We later examine under what conditions a traditional ledger maintained by a monopolist induces a large extraction of rent.

[6] Note that the hypothesis $\zeta \leq \bar{\zeta}$ is not restrictive. It just states that if agents are ex-ante neutral or prefer ledger B, there will be a unique equilibrium in which they all switch to ledger B. A good benchmark is the case $\zeta = \bar{\zeta}$.

3.3 A realistic "hard fork"

In this section, we analyze a hard fork that is more realistic than the type highlighted in the preceding analysis where *all* users of the blockchain switch to one branch of the fork and the other is completely abandoned. In reality, hard forks usually lead to a split of the community. For example, the Ethereum community split after hackers stole cryptocurrency from a smart contract. Although the majority of the blockchain's users joined the segment of the community that decided to fork, a significant percentage of users continued to use the original blockchain. The Bitcoin blockchain has also been forked by the (significantly less popular) cryptocurrencies Bitcoin Cash and Bitcoin Gold, both of which changed the rules of Bitcoin in order to benefit users. In these cases, many users of Bitcoin refused to actively use the new cryptocurrencies because they felt that the changes to the rules were actually detrimental or compromised the security of the blockchain. This section will focus on the tradeoff between fork competition and network externality inefficiencies, the second cost of decentralization. Although fork competition can benefit users, we will show that it can also lead to inefficient miscoordination, or "too many ledgers" in equilibrium.

The key mechanism that will underlie realistic hard forks in our model is preference heterogeneity. Although in the benchmark model agents are heterogeneous in their preferences, we take a limit in which this heterogeneity vanishes. We now consider a model identical to the benchmark with the exception of the specification of types. Readers' types are now given by

$$\theta_i = (x_i, f_i)$$

where $f_i \in \{0, f\}$. The type f_i reflects a preference for forking: readers with $f_i = f$ dislike all forks equally, and readers with $f_i = 0$ are not averse to forking the existing blockchain.[7] Types f_i are independently and identically distributed across readers with $\Pr(f_i = \eta) = \mu$. Types x_i are distributed uniformly in the interval $[\zeta - \frac{\sigma}{2}, \zeta + \frac{\sigma}{2}]$ as before. Readers observe both x_i and f_i.

In what follows, it will be convenient to adopt a particular form for readers' utility function $\tilde{u}$ in order to derive analytical results. We assume

$$\tilde{u}(s, f, \phi, \zeta, L, C) = \underbrace{s + f}_{\text{stake}} + \underbrace{\kappa(2\phi - 1)}_{\text{network externalities}} + \underbrace{\zeta}_{\text{fundamentals}} - \left(\underbrace{\alpha(L^A - L^B)}_{\text{fees}} - \underbrace{(g(\frac{C^A}{\phi}) - g(\frac{C^B}{1-\phi}))}_{\text{crypto security}} \right) \tag{2}$$

[7] We adopt this specification for simplicity. Allowing for η_i to depend on the announced fundamental parameters L_A and L_B would not change the main results. Anecdotal evidence suggests that there are indeed blockchain users who are fundamentally averse to forking.

Here the utility function is simply represented as a linear sum of the five components of readers' preferences. While f_i is not strictly speaking a stake, it enters into readers' individual preferences in the same way. Parameter κ governs the strength of network externalities and parameter α determines readers' aversion to fees. Function g (which is at this point exogenous) relates readers' utility to the cryptographic security of the ledger. Note that this utility function is symmetric when $\zeta = 0$, $L^A = L^B$, and $C^l = \phi^l L^l$ as defined in Definition 1. Throughout, we will continue to use a similar utility function in order to illustrate properties of equilibrium in our applications.

Let $\tilde{g}(L) = g(L) - \alpha L$. Note that if there exists $L^B \geq 0$ such that $\tilde{g}(L^B) > \tilde{g}(L^A) + f$, we obtain the same result as in Section 3.2. Proposer P^B will propose such an L^B and all readers will switch to branch B. In this case, there exists a feasible fee L^B that is better than L^A by such a wide margin that all readers, including those who dislike forks, prefer ledger B with parameter L^B.

We therefore consider only the case in which all $L^B \geq 0$ satisfy $\tilde{g}(L^B) < \tilde{g}(L^A) + f$. In fact, the only situation in which multiple equilibria would arise under complete information is if

$$f + \tilde{g}(L^A) - \tilde{g}(L^B) \geq \kappa(1 - 2\mu) \geq \tilde{g}(L_A) - \tilde{g}(L_B)$$

We derive the unique equilibrium under these conditions. The results are summarized in Proposition 4.

Proposition 4. *Suppose readers face ledgers with fees L^A, L^B, $W^l \geq L^l$ writers commit to branch l at $\tau = 2$, and a fraction μ of readers are of type $f_i = f$. Then if*

$$f + \tilde{g}(L^A) - \tilde{g}(L^B) \geq \kappa(1 - 2\mu) \geq \tilde{g}(L^A) - \tilde{g}(L^B)$$

the essentially unique equilibrium at $\tau = 1$ is of one of two types.

1. *If $f \leq \kappa$, then all readers choose branch A if $\tilde{g}(L^A) - \tilde{g}(L^B) > \mu f$ and branch B if $\tilde{g}(L^A) - \tilde{g}(L^B) < \mu f$.*

2. *If $f > \kappa$, readers of type $f_i = f$ choose branch A iff $f - (\tilde{g}(L^A) - \tilde{g}(L^B)) > (1 - \mu)\kappa$ and readers of type $f_i = 0$ choose branch B iff $\tilde{g}(L^A) - \tilde{g}(L^B) > \mu\kappa$. That is, the miscoordination equilibrium of the complete information game is selected when $f > \kappa$ if such an equilibrium exists.*

This proposition essentially shows that when readers' fundamental aversion to forking is strong relative to the coordination motive, the blockchain is vulnerable to a hard fork that splits the community. Intuitively, when network externalities are weak relative to some readers' dislike of forks, readers who are averse to forks will still prefer not to leave the existing ledger even if all other readers join the new fork. Put another way, coordination motives are a source of strength for a blockchain: when network externalities are weak, coordination among the blockchain community becomes fragile and the community is susceptible to a split.

The possibility of a hard fork that splits the community has important implications for welfare. When no fork is proposed, all readers obtain utility $\mu f - \tilde{g}(L^A) + \kappa$. When a fork is proposed and a community split occurs, on the other hand, readers obtain average utility

$$\mu(f - \tilde{g}(L^A) + \kappa\mu) + (1-\mu)(-\tilde{g}(L^B) + \kappa(1-\mu))$$

Relative to the case with no forking, the welfare gains or losses are

$$(1-\mu)(\tilde{g}(L^A) - \tilde{g}(L^B)) - 2\kappa\mu(1-\mu)$$

The first term is the fundamental benefit readers of type $f_i = 0$ obtain by switching to B, and the second term is the coordination loss associated with the split. Hence the fork is detrimental to welfare if

$$2\kappa\mu > \tilde{g}(L^A) - \tilde{g}(L^B)$$

The results of the previous section and this one highlight the main tradeoff relevant for determining whether a blockchain is worthwhile. Although a blockchain greatly enhances competition between ledgers and lowers fees, it may also induce an undesirable breakdown of coordination. The possibility of miscoordination is especially strong when network externalities are weak but the welfare losses are large only when coordination matters, so miscoordination should be a concern when network externalities lie in an intermediate range.

3.4 Competition between traditional ledgers

In this section, we analyze a competition between a ledger maintained by a monopolist and an outside ledger. The differences between this setting and one with two distributed ledgers will clarify exactly how fork competition differs from standard competition; i.e., what exactly is accomplished by decentralization. We first begin by assuming that the monopolist is the incumbent in the sense that readers have a stake in the monopolist's ledger but not the outside ledger. There are just two writers: the monopolist $\mathcal{M}$ on ledger A and an outside writer (entrant) $\mathcal{O}$ on ledger B. In this case, the writers are also the proposers $P^A = \mathcal{M}$ and $P^B = \mathcal{O}$. Each writer may only write on her own ledger. At $t = 1$, the incumbent may choose a fundamental parameter $L^A \geq 0$ and the the entrant chooses $L^B \geq 0$. Reader i has stakes $s_i^A \geq 0$ on ledger A and $s_i^B = 0$ on ledger B. Readers have no stake in the outside writer's ledger and that writer is unable to replicate the stakes in the monopolist's ledger due to information frictions. Writers do not take actions at $\tau = 2$.

Readers have preferences summarized by

$$\tilde{u}(s, \phi, \zeta, L) = s + \zeta + \kappa(2\phi - 1) - \alpha L \tag{3}$$

Readers' types s_i have a cross-sectional distribution $Q(s)$ that is uniform on the interval $[S - \frac{d}{2}, S + \frac{d}{2}]$. Here S is the average stake and d is the dispersion of stakes. It is important to distinguish between situations in which network externalities are strong enough to generate multiplicity and situations in which network externalities are weak. There is multiplicity if and only if $d > \kappa$. We will henceforth assume in this section that the true realization of the common value ζ is zero, but that this is unknown to readers.

The monopolist receives a fee L^A from each reader who participates. The monopolist's objective function is

$$\max_{L^A \geq 0} \phi L^A$$

where ϕ denotes participation on ledger A. Similarly, the entrant's objective function is

$$\max_{L^B \geq 0} (1 - \phi) L^B$$

In order to proceed, we must determine how the writers' choices of L^A and L^B map to participation ϕ. Proposition 5 provides an answer.

Proposition 5. *When $d > \kappa$, all readers for whom*

$$\frac{1}{2} + \kappa^{-1}\Big(s_i - \alpha(L^A - L^B)\Big) > Q(s_i)$$

choose to remain on ledger A, and all other readers choose ledger B. When $d < \kappa$, all readers choose A if $\alpha(L^A - L^B) < S$ and B if $\alpha(L^A - L^B) > S$.

First, we consider the simpler case in which $d < \kappa$. In this case, network externalities are so strong that all readers will end up choosing the same ledger regardless of how invested they are in ledger A. Proposition 5 shows that when network externalities are strong, the incumbent and entrant effectively compete à la Bertrand. Each will try to undercut the other as long as it is possible to do so. However, the incumbent has a competitive advantage corresponding to the average stake S readers have in its ledger. Therefore, in equilibrium the entrant must choose $L^B = 0$, and the incumbent monopolist chooses L^A just small enough so that readers do not switch to B. By Proposition 5, this yields

$$L^A = \frac{S}{\alpha} \tag{4}$$

In this case, the profits earned by the monopolist depend only on the average stake and α, which parametrizes readers' aversion to fees. When the average stake is higher, the monopolist has a larger competitive advantage because there is greater inertia in switching ledgers.

Now we consider the case in which $d > \kappa$. By Proposition 5, when the monopolist selects L^A, all readers for whom $\frac{1}{2} + \kappa^{-1}\Bigg(s_i - \alpha(L^A - L^B)\Bigg) > Q(s_i) = \frac{s-S}{d} + \frac{1}{2}$ choose to remain on ledger A. To find the cutoff type s^* who is indifferent between remaining on the monopolist's ledger and leaving, we solve

$$\frac{1}{2} + \kappa^{-1}(s - \alpha(L_A - L_B)) = \frac{s-S}{d} + \frac{1}{2}$$

which implies

$$s^* = \frac{d}{d-\kappa}\Bigg(\alpha(L_A - L_B) - \kappa(\frac{S}{d} - 1)\Bigg) \tag{5}$$

so long as the expression on the right-hand side is in the range $[0, S]$. This yields $Q(s^*) = \frac{s^*-S}{d} + \frac{1}{2}$, so we obtain an expression for participation in the monopolist's ledger as a function of L_A:

$$\phi(L^A, L^B) = 1 - Q(s^*(L^A, L^B)) = \frac{S + \frac{d}{2} - \frac{\kappa}{2} - \alpha(L^A - L^B)}{d-\kappa}$$

Then the monopolist's problem reduces to

$$\max_{L^A} \Bigg(S + \frac{d}{2} - \frac{\kappa}{2} - \alpha(L^A - L^B)\Bigg)L^A$$

which yields

$$L^A = \frac{S + \frac{d}{2} - \frac{\kappa}{2} + \alpha L^B}{2\alpha} \tag{6}$$

The rents extracted by the monopolist are increasing in the average stake on its ledger because when the average stake is higher, readers must be charged a higher fee before they become indifferent between leaving the ledger and losing their stakes. A high dispersion of stakes also allows the monopolist to extract high fees because when there is a wide distribution of stakes, the sensitivity of the monopolist's revenues to L^A is low. There are fewer marginal readers, so an upwards adjustment of L^A does not result in a large exodus of readers from ledger A. Finally, when the parameter L^B is large, readers are reluctant to leave ledger A because they know that they will be charged high fees on the outside ledger regardless, so the monopolist enjoys higher profits.

On the other hand, a strong coordination motive can be detrimental to the monopolist's business. If the coordination motive is strong, when a single marginal reader leaves the ledger it induces many other readers to leave as well. In this case, the sensitivity of participation to L^A is high. Clearly, it will also be the case that when readers' preferences are sensitive to L^A, the monopolist must set a lower L^A.

Recall that with a blockchain, the fundamental parameter that is chosen in equilibrium depends only on readers' fundamental preferences– the ledger that is best for readers is chosen automatically. In the traditional environment, when even partial competition is possible, network externalities work as a disciplining device against the incumbent monopolist. That is, network externalities enhance the importance of ledgers' fundamental parameters when replication of information and perfect, blockchain-style competition between writers is impossible.

Now we analyze the entrant's problem. Participation on the entrant's ledger is

$$\frac{\frac{d}{2} - \frac{\kappa}{2} - S + \alpha(L^A - L^B)}{d - \kappa}$$

The entrant's problem is then

$$\max_{L^B \geq 0} \left(\frac{d}{2} - \frac{\kappa}{2} - S + \alpha(L^A - L^B) \right) L^B$$

The first-order condition of this problem is

$$L^B = \frac{\frac{d}{2} - \frac{\kappa}{2} - S + \alpha L^A}{2\alpha} \tag{7}$$

The monopolist will choose this value of L^B as long as $S - \alpha L^A \leq \frac{1}{2}(d - \kappa)$. Otherwise, the first-order condition is satisfied only for negative L^B, which is impossible, so the entrant sets $L^B = 0$.

Equation 7 shows that the entrant will extract high rents if the dispersion in readers' stakes is large or if the incumbent also extracts large rents. When the dispersion in readers' stakes is large, the sensitivity of the entrant's revenues to L^B is low, as in the case where the monopolist is the incumbent. That is, dispersion in stakes is harmful to readers no matter which ledger they ultimately choose. When the fundamental parameter L^A on the incumbent's ledger is large, readers are more willing to stomach high fees charged by the entrant, so L^B is higher.

The entrant's rents are decreasing in the strength of the coordination motive κ, the mean stake on the incumbent's ledger S, and readers' sensitivity to fundamentals α. Network externalities discipline both the incumbent and the entrant– when these externalities are strong, an increase in L^B tends to cause a domino effect that results in a large mass of readers leaving ledger B. The fee charged by the entrant is also decreasing in the mean stake S on the incumbent's ledger because that stake gives the incumbent a competitive advantage, so the entrant must charge a lower fee in order to capture a significant segment of the market.

In order to find the equilibrium of the game between the incumbent monopolist and the entrant, we simply combine their first-order conditions. Hence we simultaneously solve equations 6 and 7. This yields

$$L^A = \frac{1}{2\alpha}(d-\kappa) + \frac{1}{3\alpha}S,\ L^B = \frac{1}{2\alpha}(d-\kappa) - \frac{1}{3\alpha}S \tag{8}$$

Then participation on each ledger is

$$\phi^A = \phi = \frac{1}{2} + \frac{1}{3}\frac{S}{d-\kappa},\ \phi^B = 1-\phi = \frac{1}{2} - \frac{1}{3}\frac{S}{d-\kappa}$$

We need $0 \leq \phi^A, \phi^B \leq 1$ and $L^l \geq 0$ for $l \in \{A, B\}$. A necessary and sufficient condition is

$$S \leq \frac{3}{2}(d-\kappa) \tag{9}$$

This inequality is a *no-entry bound.* If this inequality does not hold, the incumbent A is in fact able to retain all readers even when $L^B = 0$. That is, the stakes readers have in ledger A endogenously prevent entry by even the most competitive entrant. While network externalities discipline the fees charged by the incumbent, inequality 9 shows that they actually impede entry by competitors as well. When the participation of others is important to readers, it is difficult for a competitor to enter because it cannot attract enough readers to get itself off the ground. On the other hand, when readers' stakes on ledger A are dispersed, it is easier for the entrant to attract the readers with the least to lose by switching, which in turn induces switching by other readers. When the no-entry bound holds,

$$L^A = L^{NE} = \frac{1}{\alpha}\left(S - \frac{1}{2}(d-\kappa)\right) \tag{10}$$

The incumbent sets L^A to be the highest value such that all readers participate in the ledger. We have the following results regarding the case with no entry.

Proposition 6. *The no-entry bound on the average stake S is decreasing in the strength of the coordination motive κ and increasing in the dispersion of stakes d. Readers' welfare under the no-entry bound is decreasing in S, increasing in d, and decreasing in κ.*

Now we turn to the case in which there is entry. Equation 8 clarifies that dispersion in stakes and the strength of the coordination motive κ affect the fees charged on both ledgers symmetrically. When the coordination motive is powerful, both monopolists are disciplined by the fact that a higher fee will cause a large loss of clientele through spillover effects. When one reader leaves a ledger, other nearly marginal readers follow suit because of the importance of coordination. On the other hand, dispersion in stakes has the opposite effect. When readers' stakes are heterogeneous, only a small mass of readers will be marginal for any given fee, so an increase in the fee does not cause a large loss in a monopolist's client base.

The mean stake S has an asymmetric effect on monopolist's fees. An increase in S increases L^A while decreasing L^B. When the mean of readers' stakes on ledger A is high, there is a competitive wedge between ledgers A and B. Monopolist $\mathcal{M}$ can extract higher rents than the entrant $\mathcal{O}$ because readers' stake in ledger A acts as an inertial force preventing them from leaving.

We have outlined three types of equilibria: one type in which $d < \kappa$ does not hold and all readers choose ledger A, an equilibrium in which there is no entry even though $d > \kappa$, and an equilibrium with entry. We can now collect our results to determine how the incumbent monopolist's fees vary across the spectrum of equilibria.

Proposition 7. *The incumbent monopolist charges fees*

$$L^A = \begin{cases} \frac{1}{\alpha}S & \kappa > d \\ \frac{1}{\alpha}S - \frac{1}{2\alpha}(d-\kappa) & d - \frac{2}{3}S \leq \kappa < d \\ \frac{1}{3\alpha}S + \frac{1}{2\alpha}(d-\kappa) & \kappa < d - \frac{2}{3}S \end{cases}$$

These fees are decreasing in κ *for* $\kappa < d - \frac{2}{3}S$ *and increasing in* κ *for* $\kappa > d - \frac{2}{3}S$.

The main insight of Proposition 7 is that the equilibrium fee charged by the incumbent monopolist is non-monotonic in the strength κ of network externalities. When the coordination motive is weak, fees are decreasing in κ because a stronger coordination motive leads to a more powerful domino effect causing readers to switch ledgers. Once κ reaches a threshold level, network externalities become strong enough to prevent entry, so a larger κ actually leads to higher fees because the barrier to entry becomes stronger. When network externalities are more powerful still, the fees charged by the monopolist depend only on its competitive advantage, i.e. the average stake in its ledger, because there is no threat of entry. The market essentially ceases to be contestable, and the monopolist extracts the maximum possible surplus from readers.

Overall, this situation is quite different from the case where two forks of a blockchain compete against one another. When two forks of a blockchain compete, the combination of portability of information and competition between writers drives fees down as far as they can go while still providing sufficient incentives for writers to secure the network. The equilibrium outcome is independent of the distribution of readers' stakes. Welfare losses come mostly from the waste of computational resources and miscoordination due to forking (which tends to occur when network externalities are weak). Under traditional monopolistic competition, even when there is competition both the monopolists may charge high fees. If there is no possibility of entry, strong network externalities protect the incumbent and increase distortionary rents. The incumbent further enjoys high rents because of its monopoly on information, which is detrimental to readers' welfare. Taken together, these results suggest that blockchains should be used as ledgers when coordination motives among users are strong or when switching costs in a traditional setting are high.

3.5 Multi-Homing

Up until this point, for analytical tractability we have made the extreme assumption that readers use only one of the two ledgers. We now extend the analysis to allow readers to use both ledgers simultaneously. The main results of our analysis go through: readers' stakes in a traditional centralized ledger anchor them to it and hinder competition, but the portability of information permitted by a blockchain removes this barrier to entry.

As in the benchmark model, there are two ledgers A and B and three time periods, $\tau = 0, 1, 2$. However, readers are allowed to "multi-home" and choose to use both ledgers at $\tau = 1$. In particular, readers now have four possible choices $\{\emptyset, A, B, A \cup B\}$ instead of just two. Here $\emptyset$ and $A \cup B$ represent the choice not to use either ledger and the choice to use both ledgers, respectively. A reader who uses ledger l pays a cost αL^l. By choosing just one ledger (say A), a reader obtains utility from interacting with all other readers who chose A or $A \cup B$. If that reader then chooses to participate in ledger B as well, the marginal gain in utility is just the utility obtained from interacting with readers who chose B. That is, a reader who chooses $A \cup B$ does not get utility from coordinating twice with other readers who chose $A \cup B$; utility is gained only by interacting with a new set of readers.

Formally, suppose that $\phi^{\emptyset}, \phi^A, \phi^B, \phi^{A\cup B}$ are the proportions of readers who choose the strategies $\emptyset, A, B, A \cup B$, respectively. Then (neglecting cryptographic security) the utilities obtained by choosing $\emptyset, A, B$, and $A \cup B$ are given by

$$u^{\emptyset} = 0, \quad u^A = s_i^A + \kappa(\phi^A + \phi^{A\cup B}) - \alpha L^A$$

$$u^B = s_i^B + \kappa(\phi^B + \phi^{A\cup B}) - \alpha L^B, \quad u^{A\cup B} = s_i^A + s_i^B + \kappa(\phi^A + \phi^B + \phi^{A\cup B}) - \alpha(L^A + L^B)$$

If there is complete information about payoff parameters, there will be multiple equilibria in this game. As such, we must introduce an arbitrarily small amount of noise in readers' information structure in order to obtain unique predictions. We suppose readers observe a signal ζ of the "fundamentals" of ledger B such that the expected cost of using B is $\alpha L^B + \zeta$. Again, readers observe ζ with an arbitrarily small amount of noise. This information structure leads to the equilibrium described in Proposition 8.

Proposition 8. *Suppose B is the entrant ledger in the sense that $s_i^B = 0$ for all i. Let Q be the CDF of s_i^A. There are two equilibrium outcomes: one in which all readers use only A and another in which all readers use B and some multi-home. For a given L_A, there is a cutoff value $\overline{L}^B(L^A)$ such that readers all choose B whenever $L^B < \overline{L}^B(L^A)$, and no reader chooses B otherwise. The cutoff value is*

$$\overline{L}^B(L^A) = \frac{Q(\alpha L^A)}{2 - Q(\alpha L^A)}(\alpha L^A - E[s|s \leq \alpha L^A])$$

This cutoff value is increasing under a first-order shift upwards of the CDF Q.

This proposition outlines two features of the equilibrium. First, in any equilibrium where some reader uses B, *all* readers use B. This is because readers have no initial stakes in B, so their preferences for B are homogeneous. If one reader finds that using B is worth the cost, then the same is true for all readers. On the other hand, some readers with large stakes in A will choose to continue to use A even after a large portion of the population has abandoned the ledger.

Second, readers' stakes still anchor them to ledger A as in our previous results. As expected, the anchor on A is stronger when readers' stakes in A are higher. The formula for the cutoff is also useful in a situation where readers' stakes on both ledgers are the same (as in a blockchain). For example, if we simply take $s_i = 0$ for all i, in which case the formula simplifies to $\overline{L}^B(L^A) = L^A$, meaning that as in our benchmark model, the ledger more favorable to readers is always selected. In order to obtain the result that competition among ledgers is restricted, however, we now must also assume that the proposer of ledger B cannot feasibly run a ledger with $L^B = 0$. That is, there must be some lower bound $\underline{L}^B$ on the fee charged by proposer B. As long as $\overline{L}^B(L^A) < \underline{L}^B$, ledger B will not emerge. There are several reasons why there may be a lower bound on L^B– there could be some economic cost to producing a viable ledger, or, as we discuss in the next section, incentive issues may require ledger writers to earn rents.

3.6 Currency competition

In this section, we briefly describe a model of currency competition and show that despite the fact that we relax the restrictive assumptions made in our benchmark model, the main intuition that the ability to fork a blockchain enhances competition goes through. Our model of currency competition is based on the Lagos-Wright (2005) model, which is a workhorse in monetary economics. We assume there are two currencies A and B, and that readers must pay a participation cost $\chi^l \geq 0$ to "adopt" currency l. Readers are permitted to adopt one currency, both, or neither. The participation cost can be thought of as effort expenditure required in order to recognize counterfeits, collect information about temporary price fluctuations, or understand the monetary policy of a given currency, for example. For simplicity, we will assume $\chi^A = 0$.[8] That is, readers do not have to pay a cost to adopt the established currency and hence always adopt it. The only decision they make is whether to adopt B.

Define ϕ^l to be the fraction of readers who adopt only currency l and $\phi^\cup$ be the fraction of readers who adopt both. Let $\psi^l = \phi^l + \phi^\cup$. After adopting currency l, readers may immediately spend their stakes s_i^l in a centralized market and receive $g(\psi^l)s_i^l$ units of goods, where $g(\psi^l)$ is the price of the currency in terms of goods when ψ^l readers adopt.[9] After the initial period, readers also trade in a decentralized market in which they need to use currency. In each period, readers hold real balances in each currency they adopt in order to trade in the decentralized market. If two readers meet and share a common currency, they trade and receive surplus S. Readers who adopt a single currency also pay an inflation cost $f^{\pi,l}(\phi, \pi^l)$ that can depend on others' participation decisions for two reasons: participation influences the probability of meeting others in the decentralized market and also determines the quantity of real balances that readers hold. The inflation cost is increasing in inflation and usually will decrease with participation in currency l. Readers who adopt both currencies pay an inflation cost $f^{\pi,\cup}(\phi, \pi^A, \pi^B)$. The utility a reader obtains by adopting only currency k is then

$$u^l(s^l, \phi, \chi^l) = g(\psi^l)s + \frac{\delta}{1-\delta}(\psi^L S - f^{\pi,l}(\phi, \pi^l)) - \chi^l$$

The utility of adopting both currencies is

$$u^\cup(s^A, s^B, \phi, \chi) = g(\psi^A)s^A + g(\psi^B)s^B + \frac{\delta}{1-\delta}(\psi^\cup S - f^{\pi,\cup}(\phi, \pi^A, \pi^B)) - \chi^A - \chi^B$$

where $\psi^\cup \equiv \phi^A + \phi^B + \phi^\cup$.

[8] The results extend to some situations in which $\chi^A > 0$, but assumptions on the parameter space are necessary to restrict the set of equilibria of the complete information game.

[9] While readers could conceivably sell their entire initial stake in the currency without paying any sort of

The surplus that agent i gets by adopting currency B as well as A is

$$u^{\cup}(s^A, s^B, \phi, \chi) - u^A(s^A, \phi, \chi^A) = g(\psi^B)s^B + \frac{\delta}{1-\delta}(\phi^B S + f^{\pi,A}(\phi, \pi^A) - f^{\pi,\cup}(\phi, \pi^A, \pi^B)) - \chi^B \tag{11}$$

When there is incomplete information about χ^B and the utility function described above is supermodular, when network externalities are sufficiently strong a global games refinement implies the existence of a cutoff χ^{B*} such that when $\chi^B < \chi^{B*}$, all agents will choose to adopt B.

Proposition 9. *When the utility function in equation eq: monetary utility describes a supermodular game with strong network externalities, there exists a cutoff χ^{B*} such that all readers adopt B when $\chi^B < \chi^{B*}$. This cutoff is lowest when readers have no initial stake in currency B.*

Proposition 9 states that the cutoff participation cost below which readers adopt currency B is higher when readers have an initial stake in the ledger. That is, if readers are initially endowed with some of the new currency (as they would be after a blockchain fork, but not after an initial coin offering) they are more likely to adopt it. This is because by refusing to adopt the new currency, readers are essentially leaving some money on the table when they have an initial stake. This additional incentive to adopt could help a currency that is superior to an established one along some dimension (e.g. lower inflation) to gain widespread recognition.

4 Dynamic Ledger Choice

We now consider the full equilibrium of the repeated ledger choice game. We show that, remarkably, readers and writers must play the static equilibrium of Proposition 3 in every period of the blockchain ledger choice game. In short, this is because the free entry condition guarantees that writers cannot be rewarded or punished by any dynamic scheme. Therefore, writers will not be able to collude with each other on an outcome that is beneficial to them. Importantly, this property of permissionless blockchains with free entry will not carry over to permissioned blockchains where only certain known parties write on the ledger. On a permissioned blockchain, it will be possible for collusion between writers to prevent low fees from emerging.

substantial effort cost, when readers are unaware of the intricacies of a given currency it is possible that they will trade that currency at a loss due to an asymmetric information problem.

4.1 Permissionless blockchain

The repeated game with a permissionless blockchain is played in periods $t = 1, 2, \ldots$. On each day, proposers, readers, and writers play the stage game. Readers are short-lived and die after one period, but writers and proposers P^A, P^B live forever and discount payoffs at rate δ. Histories of this game are defined recursively. Let $\mathcal{H}^1 = \{\emptyset\}$. Then define

$$\mathcal{H}^T = \mathcal{H}^{T-1} \times \mathbb{R}_+ \times [0, 1] \times [0, M]^2 \times \mathbb{R}_+$$

The observable quantities are whether the initial writer chose on day T chooses to propose a fork (where 1 indicates that a fork was proposed), which fork $L^B \geq 0$ was proposed, how many readers chose branch A, and how much computing power was committed to each branch. The last $\mathbb{R}_+$ represents the parameter L^l on the ledger kl chosen by the majority of readers at $\tau = 1$, which becomes the reference parameter on branch A in the next period. That is, when readers choose a particular fork of the blockchain, that chain is extended and becomes the default for developers to build off of if they want to fork in the future. The histories $\mathcal{H}^{t,\tau}$ that are publicly observable within subperiod τ of period t are defined in the obvious way. Readers observe their own private signals and writers observe the entire history of their private signals.

We define subgame-perfect equilibrium in the usual way. We now show that in any SPE of the repeated game, writers always make zero profits from contributing computing power to the blockchain. The unique SPE of the repeated game will then be one in which agents play the unique SPE of the static game.

Proposition 10. *In any SPE of the repeated game, writers make zero profits. The unique SPE is the equilibrium of Proposition 1 played in every period t.*

4.2 Permissioned Blockchain

We now consider the case of a permissioned blockchain. One might think that a permissioned blockchain strictly dominates a permissionless blockchain in any application, since it allows the replication of information just like a permissionless blockchain but does not involve any waste of computational resources. If the set of equilibria with permissioned and permissionless blockchains were the same, in a sense permissioned blockchains would break the Trilemma by eliminating the usual waste of resources. However, free entry of writers on a permissionless blockchain actually helps to sustain equilibria that are beneficial to readers because they eliminate the possibility of collusion among writers. The computational costs of a permissionless blockchain can then be seen as the costs of allowing for free entry. On a permissioned blockchain, there is no free entry: the consortium of entities that are allowed to write on the ledger jointly decide whether to admit new members, and then those new members are identified to the blockchain's readers. The lack of free entry represents a failure of true decentralization. In the case of permissioned blockchain, the synergy between replicability of information and competition between writers fails because competition between writers is imperfect, since writers earn rents.

In order to capture this situation, we present a simple model of a permissioned blockchain. The model is similar to the baseline model with the exception that there is a finite number of writers who do not incur computational costs. Play occurs in periods $t = 1, 2, \dots$, and each day consists of subperiods $\tau = 0, 1, 2$ just as in the benchmark ledger choice model. There are proposers P^A, P^B who choose fixed parameters $L^A > L^B$, respectively, in each period. They both choose stakes $\hat{S}$ (which are irrelevant because information is always replicated across branches of the fork). Here branch A can be seen as the reference ledger. Our main result will be that with a permissioned blockchain, it will be possible for writers to prevent forking to branch B.

There are $M \in \mathbb{N}$ writers who discount payoffs at rate δ and a continuum of short-lived readers $i \in [0, 1]$. The timing is as follows. At $\tau = 0$, proposers announce L^A and L^B. At $\tau = 1$, after learning writers' decisions, readers individually choose a fork $l \in \{A, B\}$ of the blockchain. Writers choose a branch of the fork at $\tau = 2$. Readers receive a payoff of zero if no writer chooses the branch of the fork that they chose at $\tau = 1$.

In this setting, there is no question of computational security because there are no computational problems to be solved. Therefore, readers' preferences can be represented by

$$\tilde{u}(s, \phi, \zeta, L) = s + \zeta + \kappa(2\phi - 1) - \alpha L$$

Writers obtain payoffs $\frac{1}{W^l}\phi^l L^l$ if they write on a branch with participation ϕ^l, fees L^l, and W^l writers.

Now we show that when δ is sufficiently large or M is sufficiently small, there is a SPE of this game in which all writers choose ledger A and a new ledger is never proposed. This is in contrast to the permissionless blockchain case, in which readers and writers would always coordinate on ledger B if $L^B < L^A$. Consider the following equilibrium conjecture:

1. After any history in which all writers chose A in all previous periods, all writers choose A.

2. After any history in which some writer chose B in some previous period, all writers choose B.

Within a given day, writers have an incentive to announce B because then all readers switch to B and they obtain all the revenues on branch B. However, afterwards they receive lower payoffs because all writers play B, and they cannot deviate to obtain higher payoffs because readers will choose B in every period.

Formally, the incentive constraint that must be satisfied in order for the specified strategy profile to be an equilibrium is

$$L^B + \frac{\delta}{M(1-\delta)} L^B \leq \frac{1}{M(1-\delta)} L^A$$

This inequality can be rearranged to obtain

$$\frac{L^A}{L^B} \geq \delta + (1-\delta)M \tag{12}$$

This inequality holds when $\frac{L^A}{L^B}$ is sufficiently large. Playing A is incentive compatible when L^A is large relative to L^B because when a writer decides to play B, she takes an immediate payoff of B but loses future rents proportional to L_A. This inequality is also satisfied for large δ or low M. When writers are patient or competition between writers is weak, they have an incentive to conform to equilibrium play.

To restate the main point, there is nothing inherent in the blockchain data structure itself that impedes rent-seeking behavior. Adding a costly identity management system to allow for free entry of writers in fact increases the costs of using the ledger for a *given* set of policies. However, perfect competition among writers combined with the fact that blockchains can be forked *endogenously* decreases the cost of using a ledger because it allows for the selection of rules that are most beneficial to readers. With a permissioned blockchain, there is no computational cost of verification, so it is possible to maintain a decentralized, immutable ledger with no single point of failure without any waste of resources whatsoever. However, when there is no computational expenditure involved in managing a blockchain, writers must earn rents, so collusion via dynamic punishment schemes can reduce incentives for writers to choose non-distortionary policies that are beneficial to readers. Decentralization is critical to competition precisely because it prevents collusion.

4.3 Blockchain security

Traditional ledgers have been criticized for being opaque and vulnerable to fraud. One of the principal advantages of blockchain protocols is that the ledger is resilient to fraud by a single bad actor. In this section, we analyze the security of both traditional ledgers maintained by monopolists and blockchains. We outline a simple model of blockchain security and compare the security of a blockchain to that of a ledger written by a monopolist. We show that while centralized intermediaries have *dynamic* incentives not to distort their own ledgers, blockchain writers' incentives are *static*, which makes it expensive to incentivize honest reporting. We discuss the tradeoff between correctness and monopolistic rent extraction on the one hand and that between correctness and decentralization on the other, showing how proof-of-work costs arise naturally.

The model of blockchain security is based on the repeated ledger choice game. As before, there are two proposers P^A and P^B and a continuum of readers $i \in [0, 1]$. We depart from the earlier model in that we allow for some "large" writers who each command a positive measure of computing power. There is a large writer J with unlimited computing capacity and a continuum $j \in [0, M]$ of infinitesimally small writers with computing power dj. This assumption is meant to capture "51% attacks" in which an entity or mining pool able to control a majority of a blockchain's computing power mounts a malicious attack on the network in order to reap financial gains. We will also assume the large writer lives for only one period. We do this in order to abstract away from dynamic punishments for large writers who can attack the network. This assumption is reasonable because (1) large writers would not be able to profitably attack the blockchain on a regular basis given that others would join the attacks and drive their profits to zero, and (2) even if the blockchain completely shut down these writers could simply choose to attack another blockchain.

In subperiod $\tau = 0$ of each day t, proposers P^A and P^B announce a fixed fundamental parameter L. For simplicity, we will assume $L = M$ so that in an equilibrium with no attacks, small writers always expend their entire computing power. The proposals differ in readers' stakes. On ledger A, readers' stakes are $s_{i,t}$, whereas on ledger B, readers' stakes are $s_{i,t-1}$. Here $s_{i,t}$ represents the stakes on the longest chain in the blockchain, whereas $s_{i,t-1}$ represents forking the blockchain back to the state in the previous period. The ability to fork the blockchain backwards will discipline writers who engage in fraudulent activity because their gains will be nullified when such a backwards fork occurs. Subperiod $\tau = 1$ is the same as in the benchmark model. Readers choose a ledger at $\tau = 1$ after learning their types.[10]

The main difference from the benchmark model is at $\tau = 2$. In each period, an attack is possible on ledger A with some small probability $\mu > 0$. We assume an attack is unlikely to ensure that small writers do not play as if the blockchain is constantly under attack, which would imply that they take large losses in periods where attacks succeed and make positive profits when they fail (in contrast to what happens in reality). When an attack is possible, the large writer chooses an action $h_J \in [0, \overline{h}]$ as well as computing power at $t = 2$. The action

[10] In reality, blockchains have forked after an attack on the network was discovered. Most famously, the Ethereum blockchain forked in 2016 after hackers stole roughly \$50 million from a smart contract on the blockchain.

h_J represents the writer's *honesty*: a smaller h_J represents a larger distortion of the ledger attempted by writer J. In order for the attack to have a chance of succeeding, the large writer must choose computing power $c_J > \int c_j dj$, so that the computing power provided by the large writer is sufficient to overwhelm the rest of the network. The type of attack modeled here is one in which the large writer creates an invalid fork of the blockchain on which he distorts the ledger while small writers write on a valid fork. Readers are initially fooled by large writers' reports[11]and transact according to the invalid chain because it has greater proof-of-work.[12]

In each period $t > 0$, a public signal $y_t \in \{0, 1\}$ is revealed. The signal takes value 1 with probability $p(h_{J,t-1})$, where $h_{J,t-1}$ is the action h_J played by the large writer at $t-1$. We assume that

$$\frac{d}{dh}\frac{p(h)}{1-p(h)} \leq 0$$

i.e., the hazard rate is nonincreasing. This signal could correspond to news media revealing that an attack on the blockchain has occurred, large numbers of people realizing that their accounts on the ledger have been compromised and spreading word of the attack, or participants with a vested interest in the blockchain communicating evidence of the attack to the community. In this setting, the assumption $y \in \{0, 1\}$ will be without loss of generality– the equilibrium will be the same regardless of whether readers can perfectly observe $h_{J,t-1}$.

Readers' preferences are as before. Their fundamental preferences for each branch of the fork are given by $u_{i,t} = \zeta - \gamma E[\overline{h} - h_{J,T-1}|\{y_s\}_{s=1}^t]$. The term ζ is a (small) preference for the longer chain, reflecting the fact that readers prefer a ledger that does not omit the most recent information. The term $-\gamma E[\overline{h} - h_{J,t-1}|\{y_s\}_{s=1}^t]$ corresponds to the fact that readers' stakes are impacted by the attack and they can essentially reverse their losses from the *previous* distortion of the ledger by forking from a point in the blockchain before the distortion occurred. Readers receive a noisy signal $x_i = \zeta + \sigma\eta_i$ of the common value as before, and their only signals of $h_{J,t-1}$ are the public signals y_t. The extent to which h_t is informative about $h_{J,t-1}$ in equilibrium determines what readers learn from the public signal. Readers' types are hence given by $\theta_i = (x_i, y_t)$. Small writers receive revenues $\frac{c_j}{C^l}\phi^l L^l$ when writing on ledger l unless a successful attack occurs, in which case they receive zero. Again, because attacks are infrequent, small writers can neglect the possibility of an attack. Proposers' actions are fixed, so we do not model their preferences. When the large writer

[12]If readers were perfectly able to observe misconduct on the blockchain (as is the case for some blockchains that are not storage-intensive), there would be no possibility of an attack in the first place. In this case, though, a traditional intermediary could arrange the same outcome by being the sole writer on a blockchain of its own with the same protocols, meaning a blockchain would be unnecessary for security.

[12]A 51% attack works because readers look for the longest chain of blocks, so despite the fact that small writers are sending reports as well, these reports are initially ignored by readers.

attacks ledger A successfully at time $t-1$, he receives revenues $\frac{L+\overline{h}-h}{M}\phi_t^A$ where ϕ_t^A denotes the participation on ledger A at time t. If readers abandon ledger A on the next day, writers get nothing from their attack.

In a period after no attack has occurred and no attack is possible, the equilibrium is as in Proposition 3. Readers prefer the longer chain slightly, so all readers coordinate on that branch of the fork and writers break even. When no attack occurred in the previous period but an attack is possible at $\tau = 2$, play at $\tau = 1$ must be the same as in Proposition 3 because readers and writers are not aware of the possibility of an attack.

In order to understand large writers' incentives at $\tau = 2$ of period $t-1$, we must analyze the equilibrium after an attack at time t. At $\tau = 1$, the public signal y_t is realized. When $y_t = 0$, the equilibrium must be the one described in Proposition 3. Given that readers slightly prefer the longer chain, the attack is successful and large writers profit. The equilibrium is different when $y_t = 1$, however. Let $h^* = E[h_{J,t-1}|y_t = 1]$ and note that $h^* < \overline{h}$. Then when ζ is sufficiently small, we have

$$u_i = \zeta - \gamma(\overline{h} - h^*) < 0$$

so were are in the same case as Proposition 3 with $\bar{\zeta} = \zeta - \gamma(\overline{h} - h^*) < 0$. Hence all readers switch to branch B (the fork of the blockchain in which the attack is rolled back) and the attackers receive zero.

We may now analyze the large writer's choices at $t = 2$ when an attack is possible. Of course, the only interesting case is the case in which the large writer chooses $c_J = M$ and $h_J < \overline{h}$. We look for conditions under which he never does so in equilibrium. We have argued that whenever $y_t = 1$, the attack is not successful. When the attack is successful, the large writer gets fees L plus the revenue $\overline{h} - h$ from the distortion. Therefore, the large writer must solve

$$\max_h (1 - p(h))(L + h)$$

The first-order condition implies

$$1 = -\frac{p'(h^*)}{1 - p(h^*)}(L + \overline{h} - h^*) \tag{13}$$

This equation implies that since $L = M$, an equilibrium in which writers attempt to steal may exist only when the hazard rate $H(h) \equiv -\frac{p'(h)}{1-p(h)}$ is uniformly low, i.e. $H(h) < \frac{1}{L}$ for all $h \in [0, \overline{h}]$. By our earlier assumption that $H(h)$ is nonincreasing, a sufficient condition to ensure $h^* = \overline{h}$ is

$$H(0) \geq \frac{1}{L}$$

When the hazard rate is large, the probability of detection is high enough to completely dissuade the large writer from even attempting an attack. Note that this condition is satisfied for sufficiently large L, meaning that when the fee earned by blockchain writers is high, even agents with the ability to subvert the network prefer not to attack it because they stand to lose the fee that they would earn through honest writing. The second force that prevents cheating by writers is that even if $h^* < \overline{h}$, it may be that profits earned through ledger distortion are negative. This occurs when

$$(1 - p(h^*))(L + \overline{h} - h^*) - L = (1 - p(h^*))(\overline{h} - h^*) - p(h^*)L < 0$$

This second condition reflects the fact that even if the large writer's fee is not large enough to dissuade him from distorting the ledger, the cost L of mounting a 51% attack is enough to render the attack unprofitable. In equilibrium, the cost of the attack L is equal to the fee earned through honest writing, but conceptually they are two distinct objects. Proposition 11 summarizes these findings:

Proposition 11. *The large writer chooses not to attack the blockchain if and only if*

$$\max_h (1 - p(h))(\overline{h} - h) - p(h)L \leq 0$$

A sufficient condition that guarantees this inequality will hold is

$$H(0) \equiv -\frac{p'(0)}{1 - p(0)} \geq \frac{1}{L}$$

This bound on L (the first cost of blockchain) characterizes the tradeoff between decentralization and cost efficiency required to maintain correctness.

Proposition 11 has a striking implication. When the probability of detection is sufficiently large, it is unnecessary to set up an expensive fee structure for writers that leads to a large waste of computational resources. Writers will abstain from distorting the ledger regardless because each marginal unit of computational power spent on an attack earns less on average than one spent on writing honestly. The cost of conducting an attack, which is exactly equal to the fee earned in equilibrium, acts as further protection against attacks. Crucially, in this framework the equilibrium is unique– readers always abandon the ledger after detecting an attack. The uniqueness of equilibrium is a direct consequence of fork competition. If an attack makes all readers worse off they will coordinate on an alternative ledger on which the attack never happened but the rest of the information on the ledger is intact. Competition among writers will cause writers to coordinate on that ledger as well, and the attacker will get nothing. As we will show, this mechanism is quite different from the one that secures a traditional ledger.

4.4 Monopolistic ledger security

Now we analyze the case where a monopolist is able to distort its own ledger while facing competition from a fixed outside ledger. The structure of the game is similar to the dynamic blockchain game where the ledger can be attacked by a group of writers. There is a monopolist who discounts payoffs at rate δ, a manager of the outside ledger, and a continuum $i \in [0, 1]$ of readers who live for one period. On each day t at $\tau = 0$, the monopolist proposes a fixed fee L^A and the outside proposer announces a fixed L^B. Readers choose a ledger at $\tau = 1$. At $\tau = 2$, each writer chooses its own ledger.

As in the blockchain model of security, the monopolist is able to distort the ledger at $\tau = 2$ of each period. The monopolist chooses an action $h \in [0, \overline{h}]$ at $\tau = 2$ and immediately receives a payoff of $\phi_t^A(\overline{h} - h)$ (in addition to the fees it usually receives). The structure of public signals is also the same as in the blockchain model. In each period t, a public signal $y_t \in \{0, 1\}$ is observed at $\tau = 2$ with probability $\Pr(y_t = 1|a) = p(h_{t-1})$. When the monopolist's distortion is severe, it both affects more agents directly and is more likely to be revealed to the public. Readers' fundamental preferences for ledger A are given by $\tilde{u}_{i,t} = s_i + \zeta - \gamma E[(\overline{h} - h_t)|\{y_s\}_{s=1}^t]$, where s_i is reader i's stake on ledger A and readers receive signals $x_i = \zeta + \sigma\eta_i$ as usual. As in the example with a blockchain, a reader's utility is decreased when the monopolist distorts the ledger and plays $a_t > 0$. These preferences differ from those in the blockchain security example in an important way. Reader's stakes in the ledger at $t - 1$ are not relevant. This is because readers do not have the option to fork to a ledger on which the distortion that occurred at $t - 1$ never happened. The monopolist's action to distort the ledger is *final*. Whereas in the blockchain model readers' play was affected by public signals because it was informative about the utility gains from switching to the alternative ledger, in this model public signals matter only because they affect readers' expectations about the continuation play. Expectations of future attacks can affect readers' actions because the monopolist is able to distort the ledger in all periods.

There will be multiple equilibria because there is no mechanism to pin down readers' expectations of future play. However, we can establish a lower bound on the fee required by the monopolist to ensure that $a = 0$ is played in all periods, which is a proxy for the cost of maintaining a ledger under a centralized intermediary above and beyond the rents extracted due to its competitive advantage. We will assume that readers punish the monopolist in the harshest way possible– they play on ledger B in all future periods after the public signal $y_t = 1$

is realized. In order to ensure this is an equilibrium for readers, it suffices to assume that there is an action $\tilde{h}$ the monopolist can take so that $\max_i s_i - \gamma(\overline{h} - \tilde{h}) - \alpha(L^A - L^B) < 0$, meaning even the type who is most anchored to ledger A by a personal stake in the system prefers to leave the ledger when readers expect $\tilde{h}$ to be played going forward. The expectations that justify this equilibrium, then, are

$$E[\overline{h} - h_t | \{y_s\}_{s=1}^t] = \begin{cases} 0 & y_s = 0 \; \forall \; s \leq t \\ \overline{h} - \tilde{h} & \exists \; s \leq t, \; y_s = 1 \end{cases}$$

If we wish to derive a lower bound on L^A, we may also assume that participation on the monopolist's ledger is $\phi = 1$ whenever $y_s = 0$ for all $s \leq t$. The monopolist's problem is stationary: as long as $y_t = 1$ has not been realized, the monopolist can achieve some value V in expectation, and after $y_t = 1$ is realized the monopolist gets zero. Hence the monopolist solves

$$\max_h \; \overline{h} - h + \delta(1 - p(h))V$$

The first-order condition is

$$1 = -p'(h^*)\delta V$$

When the monopolist plays h^*, we have $V = \frac{L_A + \overline{h} - h^*}{1 - \delta(1 - p(h^*))}$. A sufficient condition for a unique optimum $h^* \in [0, \bar{h}]$ to exist is then just $\frac{d}{dh} - \frac{p'(h)(L_A + \overline{h} - h)}{1 - \delta(1 - p(h))} > 0$. This condition is similar to the increasing hazard rate assumption made in the previous section. To ensure the monopolist plays $h^* = \overline{h}$, we need

$$-\frac{\delta p'(0)}{1 - \delta(1 - p(0))} \geq \frac{1}{L^A}$$

For small δ, this condition is usually significantly weaker than the one derived in the previous section for blockchain security, so when the monopolist is punished as harshly as possible, it is not necessary to pay the monopolist as much in fees as blockchain writers. The intuition for this result is simple: while a blockchain writer is punished for misbehavior only through nullification of the profits obtained by attacking the blockchain, a monopolist is punished via the destruction of its franchise value, which consists of all future fees earned through honest play. This result is restated in Proposition 12.

Proposition 12. *There is a threshold value of L^A such that the monopolist never distorts the ledger:*

$$L^A = -\frac{1 - \delta(1 - p(0))}{\delta p'(0)}$$

Proposition 12 says that the monopolist's ability to distort the ledger imposes an endogenous lower bound on its fees above and beyond the bound due to the barriers to entry resulting from readers' stakes on the ledger. The less likely the monopolist is to be detected in its deviations, the higher this bound must be. It is worth noting that while the fee required for correctness provides a sharp bound on the cost of a blockchain (due to fork competition), the fee charged by a monopolist may be far from this bound. If the rents earned by a monopolist are large, there is no force to push the fee it charges down to the level derived in Proposition 12.

There are several drawbacks that make the security of a traditional ledger less robust than that of a blockchain, however. First, in a setting with a traditional ledger equilibrium is not unique, so while it may be the case that under the harshest possible punishment scheme it is not necessary to pay an intermediary large fees to obtain ledger security, the equilibrium fee required to ensure good behavior may be much higher. Second, the signal structure $p(h)$ may well be more revealing for a blockchain than for a traditional ledger, since blockchains are designed specifically to provide transparency about attacks on the ledger. Finally, in this case the assumption that signals y_t are either zero or one is not without loss of generality. A richer signal structure would lead to even greater multiplicity that would allow the monopolist to "nickel and dime" readers by proving to them that although she is distorting the ledger, she is not doing so to the extent that readers would prefer to switch to a competitor and lose their stakes in the established ledger. Fork competition is thus important in securing a ledger as well as forcing competition among writer compensation schemes.

Another interesting difference between securing a blockchain and securing a traditional ledger is that the equilibrium in the blockchain game is unique and independent of the nature of public signals while in the traditional setting there are multiple equilibria, and the set of equilibria depends on the information structure. This dichotomy stems from the fact that past actions can be "rewound" by a fork on a blockchain but not on a traditional ledger. The equilibrium in the blockchain game is backwards-looking: readers decide whether they want to switch to a different ledger on which an attack never occurred, meaning their actions are determined by their expectations of malevolent writers' *past* actions. The equilibrium in the game with a traditional ledger is forward-looking: the public signal acts as a coordinating device that determines readers' expectations of the intermediary's *future* actions, but there is no possibility of undoing past events. The uniqueness of equilibrium in the blockchain game can be seen as a security feature. When any attack is revealed to the public, it will always be undone via a blockchain fork. Multiplicity of equilibrium in the game with a centralized intermediary means there are no such guarantees in the traditional setting.

5 Enforcement

In this section, we discuss some practical matters and present results related to the application of blockchain when enforcement is necessary. The issue with distributed ledgers is that while they are useful for transferring *ownership* of assets, they do not necessarily guarantee transfers of *possession*. Consider a simple example in which a buyer wishes to purchase a car from a seller on a blockchain. In this case, ownership of the car would be represented by a token in the seller's account on the blockchain. The blockchain's writers would be able to transfer ownership of the token to the buyer, but they would not be able to verify that the buyer was physically in possession of the car after the transaction. To ensure transfers of possession, it is necessary to have some entity that enforces contracts on the blockchain when those contracts involve the transaction of physical assets. This type of enforcement would likely be the role of some centralized entity, which would then have to explicitly make reference to the cases in which it would enforce blockchain contracts.

The need for an enforcer alongside a distributed ledger raises two issues. First, while several commentators claim that distributed ledger technology will benefit those in developing countries without strong property rights, one needs to identify why property rights are weak in the first place before concluding that a distributed ledger is the solution. If the government is overly bureaucratic and incapable of setting up good institutions to track property rights, then a distributed ledger is an effective alternative. However, if the government is corrupt to the point that it would outright refuse to enforce some contracts in a publicly available database, a distributed ledger will be useless. Again, the readers of the ledger are the ultimate source of discipline, so a distributed ledger is useful only insofar as it helps them to discipline a corrupt government (through greater disclosure of information, most likely). If the enforcer is itself a private firm, such as a bank that enforces debt obligations, it may be optimal for the enforcer to maintain the ledger as well. The enforcer will have an incentive to fulfill its obligation for fear of losing the privilege of maintaining the ledger.

The second issue is that the enforcer must choose which forks of a blockchain to support. An enforcing entity cannot simply commit to enforce contracts on all forks because the same physical asset may be promised to two different individuals on different forks of the blockchain. The enforcer could say it will enforce all contracts so long as certain policies are followed, which prevents hard forks that change blockchain's rules. Of course, this enforcement policy would be detrimental because it would essentially destroy the potential for competition between ledgers. Furthermore, if an attack on the blockchain were to occur, such as the one on the Ethereum blockchain in 2016, the enforcer would have enormous power to resolve the issue in its own favor.

We have two formal results corresponding to these two issues. We fully lay out the model with enforcement in the Appendix but present the main elements here. The only change to the benchmark dynamic model is that a fourth subperiod $\tau = 3$ is added to each day on which an agent known as the "enforcer" takes an action $e \in [0, 1]$. In each period, the enforcer earns a fee proportional to the participation in its ledger that does not depend on the action e. Readers prefer the enforcer to play larger values of e, but by playing e the enforcer incurs a utility cost of e. Deviations from $e = 1$ are detected on the next day with probability $q(e)$. Readers have the option to abandon the ledger and get zero utility at any time.

First, we show that there is a synergy between writing the ledger and enforcing its contents. An agent who both writes and enforces the ledger may distort the ledger by choosing an action h as in Section 4.4 and choosing an enforcement level e. The probabilities of detection of these two actions are independent. We can then compare this situation to one in which there is a continuum of blockchain writers in charge of reporting the ledger's contents and a separate enforcer. Proposition 13 summarizes the incentive compatibility constraints in the two situations.

Proposition 13. *When the enforcer also writes the ledger, the fee L earned by this entity must satisfy*

$$L \geq \left(\frac{1}{\delta} - 1\right) \max\left\{ -\frac{1}{p'(0)}, \ -\frac{1}{q'(1)} \right\} \tag{14}$$

where p is the detection function for distortion of a centralized ledger. On the other hand, when the ledger is written by a blockchain and enforced by a centralized entity, the fees L_W and L_E earned by blockchain writers and the enforcer, respectively, must satisfy

$$L_W \geq -\frac{1}{p_B'(0)}, \ L_E \geq -\left(\frac{1}{\delta} - 1\right)\frac{1}{q'(1)} \tag{15}$$

where p_B is the detection function for distortions of the blockchain.

Clearly, the bound on the fee L derived in 14 is less than $L_E + L_W$ in (15) when δ is reasonably large. When distortion of the ledger and lack of enforcement are strategic substitutes, bundling reporting and enforcement together reduces the fee required to incentivize honest behavior. The fee only needs to be large enough that the intermediary will not choose the more attractive of the two deviations, after which the incentive compatibility condition for the other type of deviation is automatically satisfied. Furthermore, bundling is beneficial because it eliminates the waste of resources required by a blockchain. The only case in which it may be beneficial to keep writing and enforcement unbundled is if (1) the p function is much more sensitive for blockchains than standard ledgers, and (2) the cost of enforcement $\frac{1}{q'(1)}$ is small relative to the cost of honest reporting.

Our second result is that when there is a centralized enforcer, there is no longer a unique equilibrium with a blockchain in which the ledger that is best for readers is always selected. There are "dictatorial" equilibria in which the enforcer effectively decides which branch of a fork is chosen.

Proposition 14. *With a centralized enforcer, there is always an equilibrium in which the ledger preferred by the enforcer is chosen by all readers.*

We defer the proof of this proposition to the Appendix, but the intuition is simple. The enforcer just threatens not to enforce contracts on any branch of a fork that uses policies of which it does not approve. Readers will not want to coordinate on any ledger that the enforcer will ignore, so they use the one selected by the enforcer. The existence of a centralized entity that is indispensable for the proper functioning of the ledger destroys the benefits that come with decentralizing the writing function.

6 Conclusion

We present a general model of ledger competition and apply it to understand when a blockchain is more economically beneficial than a traditional ledger managed by a centralized intermediary. Our analysis of the tradeoffs between centralized and decentralized record-keeping is guided by the Blockchain Trilemma. We focus the analysis of our static model on the tradeoff between decentralization and cost efficiency. We find that with a blockchain, the rules that are most beneficial to readers of the ledger always emerge in equilibrium via hard forks. This surprising result arises due to the combination of portability of information and competition between writers that are possible with a blockchain. Readers are not reluctant to abandon an older version of a blockchain because all the information contained in the old blockchain is contained in the new one with updated policies, so writers compete to write on the blockchain preferred by readers. A centralized intermediary that maintains a traditional ledger, on the other hand, is able to extract rents from readers by exploiting their desire to keep their stakes in the established ledger. When the coordination motive is sufficiently strong, entry by a competing traditional ledger is ruled out altogether, which suggests that blockchains may help lower intermediaries' rents in situations where the coordination motive is strong. This result suggests that, for example, retail platforms like Amazon's might be better suited to a blockchain, since the coordination motive among buyers and sellers is powerful. Decentralized ledgers do have costs, however. In addition to the waste of resources required by proof-of-work, there is a second cost of blockchains: miscoordination inefficiencies. Blockchains forks can lead to a split of the community and too many competing ledgers in equilibrium.

We also present an extension of our static model to a repeated setting. This extension allows us to show that there is no possibility of collusion among writers of a permissionless blockchain in the repeated game. Free entry of writers rules out any sort of dynamic reward and punishment scheme, so writers must play myopically in every period. Thus the optimal outcome for readers emerges with a permissionless blockchain even in the repeated game. By contrast, collusion is possible among writers of a permissioned blockchain because they earn rents in equilibrium. With a permissioned blockchain, it is not always the case that writers' rents are competed down by hard forks. Permissioned blockchains, then, do not break the Trilemma because they fail to fully meet the decentralization criterion due to lack of free entry.

We also explicitly examine the costs of incentivizing writers to report honestly (correctness). On the one hand, centralized intermediaries are incentivized dynamically by ensuring that the future profits they will earn are high enough to guarantee they do not want to risk losing them. On the other hand, blockchain writers must be incentivized statically by raising the proof-of-work to the point that attacks become unprofitable.

We highlight the important distinction between ownership and possession. Blockchains can only effect transfers of ownership, but when enforcement of possession rights is required it is often more efficient to bundle writing and enforcement duties in a single centralized intermediation structure.

In this paper, we have outlined the incentive mechanisms of two particularly important types of ledgers. What we have not developed so far is a general theory of the interactions between writers and readers on an arbitrary ledger. An investigation of the optimal technological restrictions on the communication between writers and readers is a fruitful avenue for future research.

References

[1] Rossella Argenziano. Differentiated networks: Equilibrium and efficiency. *RAND Journal of Economics*, 39(3):747–769, 2008.

[2] Bruno Biais, Christophe Bivière, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. Working Paper, 2017.

[3] Hans Carlsson and Eric van Damme. Global games and equilibrium selection. *Econometrica*, 61(5):989–1018, 1993.

[4] Christian Catalini and Joshua Gans. Some simple economics of the blockchain. 2017.

[5] Jonathan Chiu and Thorsten Koeppl. The economics of cryptocurrencies– bitcoin and beyond. Working Paper, 2017.

[6] William Lin Cong and Zhiguo He. Blockchain disruption and smart contracts. Working Paper, 2017.

[7] William Lin Cong, Ye Li, and Neng Wang. Tokenomics: Dynamic adoption and valuation. Working Paper, 2018.

[8] Douglas Diamond. Financial intermediation and delegated monitoring. *The Review of Economic Studies*, 51(3):393–414, 1984.

[9] Lukasz Drozd and Ricardo Serrano-Padial. Credit enforcement cycles. Working Paper, 2017.

[10] David Easley, Maurenn O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. Working Paper, 2017.

[11] David Frankel, Stephen Morris, and Ady Pauzner. Equilibrium selection in global games with strategic complementarities. *Journal of Economic Theory*, 108(1):1–44, 2003.

[12] Drew Fudenberg and Jean Tirole. Perfect bayesian equilibrium. *Journal of Economic Theory*, 53(2):236–260, 1991.

[13] Arthur Gervais, Ghassan Kharame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[14] BitFury Group. Public versus private blockchains. Whitepaper, 2015.

[15] Gur Huberman, Jacob Leshno, and Ciamac Moallemi. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Working Paper, 2017.

[16] Ricardo Lagos and Randall Wright. A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, 113(3):463–484, 2005.

[17] June Ma, Joshua Gans, and Rabee Tourky. Market structure in bitcoin mining. NBER Working Paper, 2018.

[18] Paul Milgrom and John Roberts. Rationalizability, learning, and equilibrium in games with strategic complementarities. *Econometrica*, 58(6):1255–1277, 1990.

[19] Stephen Morris and Hyun Song Shin. Unique equilibrium in a model of speculative currency attacks. *American Economic Review*, 88(3):587–597, 1998.

[20] Stephen Morris and Hyun Song Shin. Global games: Theory and applications. 2001.

[21] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[22] Emiliano Pagnotta and Andrea Buraschi. An equilibrium valuation of bitcoin and decentralized network assets. Working Paper, 2018.

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

[24] Joszef Sakovics and Jakub Steiner. Who matters in coordination problems. *American Economic Review*, 102(7):3439–3461, 2012.

[25] Linda Schilling and Harald Uhlig. Some simple bitcoin economics. Working Paper, 2018.

[26] Michael Sockin and Wei Xiong. A model of cryptocurrencies. Working Paper, 2018.

A Proofs

Proof of Proposition 1:

Proof. This proposition is an immediate consequence of Lemma B.1 in Appendix B. □

Proof of Proposition 2:

Proof. This proposition follows from Theorem B.1 in Appendix B □

Proof of Proposition 3:

Proof. We prove the proposition by backwards induction.

τ=**2**: At $t = 2$, writers know the value of ϕ^l, $l \in \{A, B\}$. We show that $C^l = \phi^l L^l$ in equilibrium. Suppose first that $C^l < \phi^l L^l$. Then since M is large, there exists a writer j such that $c_j < 1$, but writer j could make profits by setting $c_j = 1$ because

$$\frac{1}{C^l}\phi^l L^l - 1 > 0$$

Now suppose $C^l > \phi^l L^l$. This means that any writer j for whom $c_j > 0$ would benefit by setting $c_j = 0$, since

$$\frac{c_j}{C^l}\phi^l L^l - c_j = (\frac{1}{C^l}\phi^l L^l - 1)c_j < 0$$

Hence $C^l = \phi^l L^l$.

τ=**1**: We will guess and verify that in any equilibrium, $\tilde{u}(s = 0, \phi, \zeta, L, C)$ is asymmetric towards B. Writers' optimal play at $\tau = 2$ implies that $\frac{C^l}{\phi^l} = \underline{C}$ for each branch of the fork. Then it must be that P^B selects L^B such that

$$\tilde{u}(s = 0, \phi = \frac{1}{2}, \zeta, L, C = (\phi L^A, (1-\phi)L^B)) \leq 0$$

and $\tilde{u}$ is asymmetric towards B in equilibrium. According to Theorem B.1, type s_i's cutoff signal $k(s_i)$ is $x_i \geq 0$, so as long as $\zeta \leq 0$, all readers will have such signals when σ is sufficiently close to zero. Therefore all readers play B.

τ=**0**: Now we confirm our guess that the proposer selects such a value L^B if possible. The equilibrium derived above shows that whenever $\tilde{u}$ is asymmetric towards B for the announced L^B, the proposer obtains a payoff of $\tilde{u}(s = 0, \phi = 0, \zeta, L, C(\phi = 0, L))$. It is never possible for the proposer to obtain a higher payoff by choosing L^B such that $\tilde{g}(L^B) \geq L_A$. Then it must be that the proposer chooses the lowest possible L_B in order to maximize payoffs, so

$$L_B = \arg\min_{L^B} \tilde{u}(s = 0, \phi = 0, \zeta, L, C(\phi, L)$$

□

Proof of Proposition 4:

Proof. These statements follow from Proposition B.4. □

Proof of Proposition 5:

Proof. The equilibrium follows from Propositions B.2 and B.3. □

Proof of Proposition 6:

Proof. These properties are a result of equations 9 and 10. □

Proof of Proposition 7

Proof. This proposition follows from equations 4, 10, and 8. □

Proof of Proposition 8:

Proof. See Appendix C.2. □

Proof of Proposition 10

Proof. First we show that at any history $h^{t,2}$, on either branch l of the fork, the total computing power contributed by writers must be $\phi^l L^l$. Suppose that $C^l < \phi^l L^l$. Then there must be some writer j who contributes $c_j < 1$. By deviating to $c_j = 1$ on branch l, this writer can achieve positive profits in the current period. Furthermore, this writer's deviation does not affect any publicly observable signal in the future history, since the writer is of measure zero. An analogous argument shows that C^l cannot be greater than $\phi^l L^l$, so $C^l = \phi^l L^l$ at any history.

Second, we must check that proposers play static best responses. Given that both readers and writers play the same strategies that they do in the stage game, a proposer can maximize her flow of payoffs by playing the same L^B as in the stage game. □

Proofs of Proposition 11 and Proposition 12:

Proof. Proposition 11 follows directly from optimality condition 13. Proposition **??** follows from the analysis in Section 4.4. □

Proof of Propositions 13 and 14:

Proof. See Appendix C.3. □

B Global Games with Heterogeneous Preferences

There is a continuum of players $i \in [0,1]$ who play a one-shot coordination game in which they choose between two options, A and B. Players' fundamental preferences consist of heterogeneous private values $\theta_i \in \mathbb{R}$ for choice A. There is also a common value τ that affects players' preferences for A. We assume that θ is iid across players with distribution $F(\theta)$. For now, we assume F is a discrete distribution with finite support but later take the limit of a continuous distribution F. Players' preferences can be described by the function

$$v(\theta, \tau, \phi)$$

where ϕ is the proportion of players who choose A. That is, there is a coordination motive. When $v(\theta, \tau, \phi) > 0$, it is a best response for a player of type θ to choose A. Conversely, a player of type θ should choose B if $v(\theta, \tau, \phi) < 0$. We additionally impose a symmetry assumption. Assumption B.1 summarizes the restrictions on v:

Assumption B.1. *We make the following assumptions about v:*

1. *Function $v(\theta, \tau, \phi)$ is increasing in θ;*
2. *Function $v(\theta, \tau, \phi)$ is increasing in τ;*
3. *Function v is **symmetric** in the sense that $v(0,0,\phi) = -v(0,0,1-\phi)$.*

Henceforth we will assume that players have incomplete information about the common value τ. We assume players have an improper uniform prior over τ[13]and receive signals $s_i = \tau + \sigma\eta_i$ ($\sigma > 0$), where η_i is iid across players and independent of τ. The noise term η_i is distributed with CDF $H(\eta)$ with support on the interval $[-\frac{1}{2}, \frac{1}{2}]$. In what follows, we will frequently consider the limit $\sigma \to 0$.

By Theorem 5 in Milgrom and Roberts (1990), this is a supermodular game. Therefore, if the signal profile is $\mathbf{s}$, there are largest and smallest rationalizable strategy profiles $\underline{\mathbf{k}}(\mathbf{s})$ and

[13]The results do not change if we instead assume τ is uniformly distributed on an interval of finite length as long as that interval is sufficiently large.

$\overline{\mathbf{k}}(\mathbf{s})$. Furthermore, every equilibrium strategy profile $\mathbf{k}(\mathbf{s})$ satisfies $\underline{\mathbf{k}}(\mathbf{s}) \leq \mathbf{k}(\mathbf{s}) \leq \overline{\mathbf{k}}(\mathbf{s})$. Given that agents observe only their own signals, it must be that all agents play cutoff strategies: for each type θ, there is a signal $k(\theta)$ such that θ plays A if $s_i > k(\theta)$ and plays B if $s_i < k(\theta)$. When agents play a cutoff equilibrium $\mathbf{k}$, we will denote the expected utility derived from playing A for the cutoff type $k(\theta)$ by $E[v|\mathbf{k}, k(\theta)]$. The equilibrium condition is just

$$E[v|\mathbf{k}, k(\theta)] = 0 \tag{16}$$

for all θ. The following lemma establishes that there is a unique equilibrium in cutoff strategies. The proof is essentially the same as that in Drozd and Serrano-Padial (2017).

Lemma B.1. *If $\boldsymbol{k}$ is a cutoff strategy equilibrium and $\Delta > 0$, then $E[v|\boldsymbol{k}, k(\theta)] < E[v|\boldsymbol{k} + \Delta, k(\theta) + \Delta]$.*

Proof.

$$\begin{aligned}
E[v|\mathbf{k}, k(\theta)] &= \int_{k(\theta)-\frac{\sigma}{2}}^{k(\theta)+\frac{\sigma}{2}} v\Big(\theta, \tau, \int_{\theta'} \Big(1 - H\big(\frac{k(\theta') - \tau}{\sigma}\big)\Big) dF(\theta')\Big) h\big(\frac{k(\theta) - \tau}{\sigma}\big) d\tau \\
&< \int_{k(\theta)-\frac{\sigma}{2}}^{k(\theta)+\frac{\sigma}{2}} v\Big(\theta, \tau + \Delta, \int_{\theta'} \Big(1 - H\big(\frac{k(\theta') - \tau}{\sigma}\big)\Big) dF(\theta')\Big) h\big(\frac{k(\theta) - \tau}{\sigma}\big) d\tau \\
&= \int_{k(\theta)+\Delta-\frac{\sigma}{2}}^{k(\theta)+\Delta+\frac{\sigma}{2}} v\Big(\theta, \tau, \int_{\theta'} \Big(1 - H\big(\frac{k(\theta') + \Delta - \tau}{\sigma}\big)\Big) dF(\theta')\Big) h\big(\frac{k(\theta) + \Delta - \tau}{\sigma}\big) d\tau \\
&= E[v|\mathbf{k} + \Delta, k(\theta) + \Delta]
\end{aligned}$$

□

From Lemma B.1 it is immediate to see that there is a unique equilibrium. Suppose that $\underline{\mathbf{k}} < \overline{\mathbf{k}}$. Let $\hat{\Delta} = \max_{\theta} \overline{k}(\theta) - \underline{k}(\theta)$, and let $\hat{\theta}$ be the value of θ that achieves this maximum. Then

$$E[v|\underline{\mathbf{k}}, \underline{k}(\hat{\theta})] < E[v|\underline{\mathbf{k}} + \hat{\Delta}, \underline{k}(\hat{\theta}) + \hat{\Delta}] \leq E[v|\overline{\mathbf{k}}, \overline{k}(\hat{\theta})]$$

where the last inequality comes from the fact that $\overline{\mathbf{k}} \leq \underline{\mathbf{k}} + \hat{\Delta}$.

In what follows, it will be useful to define the following object: for all $\theta \in \Theta$, where Θ is some set contained in the support of F, set

$$\psi(\tau, \Theta) = \frac{1}{\sum\limits_{\Theta} f(\theta)} \sum_{\Theta} H\left(\frac{k(\theta) - \tau}{\sigma}\right) f(\theta)$$

This expression is the expectation of the number of agents in Θ who play B given the common value τ. We now prove an important lemma (called the "Belief Constraint") about the function ψ due to Sakovics and Steiner (2012) and Drozd and Serrano-Padial (2017):

Lemma B.2. *For any subset $\Theta \subset supp(F)$ and any $z \in [0, 1]$,*

$$\frac{1}{\sum\limits_{\Theta} f(\theta)} \sum_{\Theta} \Pr(\psi(\tau, \Theta) < z | s = k(\theta)) f(\theta) = z$$

Proof. Begin by defining "virtual types" $\delta(s, \theta) = s - k(\theta)$. This reduces the two-dimensional type space to a one-dimensional one. Agents play A whenever $\delta(s, \theta) > 0$ and B when $\delta(s, \theta) < 0$. With this definition,

$$\psi(\tau, \Theta) = \Pr(\delta(s, \theta) < 0 | \tau, \Theta)$$

First we show that $\Pr(\psi(\tau, \Theta) \leq z | \delta(s_i, \theta_i) = 0) = z$. This property is due to Morris and Shin (2003). For brevity, we will denote $\delta(s_i, \theta_i)$ by δ_i.

Define $\tilde{\eta}_i = \frac{\delta_i - \tau}{\sigma}$, and denote the distribution of $\tilde{\eta}$ conditional on $\theta \in \Theta$ by $\tilde{H}$. This variable is iid across players. We have

$$\begin{aligned}
\Pr(\psi(\tau, \Theta) < z | \delta_i = 0) &= \Pr(\Pr(\delta_j > 0 | \tau) < z | \delta_i = 0) \\
&= \Pr\left(\Pr\left(\tilde{\eta}_j < -\frac{\tau}{\sigma}\right) < z | \delta_i = 0\right) \\
&= \Pr\left(1 - \tilde{H}\left(-\frac{\tau}{\sigma}\right) < z | \delta_i = 0\right) \\
&= \Pr(1 - \tilde{H}(\tilde{\eta}_i) < z) \\
&= \Pr(\tilde{\eta}_i > \tilde{H}^{-1}(1 - z)) \\
&= 1 - \tilde{H}(\tilde{H}^{-1}(1 - z)) = z
\end{aligned}$$

Now to complete the proof, observe that

$$\Pr(\psi(\tau, \Theta) < z | \delta = 0) = \sum_{\Theta} \Pr(\psi(\tau, \Theta) < z | s = k(\theta)) \Pr(\theta | \delta = 0, \Theta)$$

Given the uniform prior over τ, the information environment is translation-invariant, so

$$\Pr(\theta|\delta = 0, \Theta) = \frac{f(\theta)}{\sum\limits_{\Theta} f(\theta')}$$

That is, knowing $\delta = 0$ yields no additional information about θ, since each type is equally likely to observe $\delta = 0$. Hence

$$\frac{1}{\sum\limits_{\Theta} f(\theta)} \sum_{\Theta} \Pr(\psi(\tau, \Theta) < z | s = k(\theta)) f(\theta) = z$$

as desired. $\square$

Up until this point, none of the results have depended on taking the limit $\sigma \to 0$. Now we specialize to the case considered in the text where σ becomes arbitrarily small and define $\mathbf{k}^\sigma$ to be the threshold equilibrium played for variance parameter σ. Correspondingly, we denote a specific type θ's cutoff by $k^\sigma(\theta)$. We then define

$$A_\theta(z|\mathbf{k}^\sigma, \Theta) = \Pr(\psi(\tau, \Theta) < z | s = k^\sigma(\theta))$$

to be the *strategic belief* of type θ– that is, it is the probability that type θ assigns to the event that a proportion less than z of agents in Θ play action B. Now we prove the final lemma we will need before proving the main result (due to Drozd and Serrano-Padial (2017)).

Lemma B.3. *There exist a unique partition $\Theta_1, \ldots, \Theta_S$ and thresholds $k_1 > \cdots > k_S$ such that, as $\sigma \to 0$, $k^\sigma(\theta) \to k_i$ uniformly for all $\theta \in \Theta_i$ and all $i \in \{1, \ldots, S\}$. Furthermore, the cutoffs k_i satisfy the limit conditions*

$$\int\limits_0^1 v\left(\theta, k_i, 1 - 2 \sum_{\Theta_j, j<i} f(\theta') - 2z \sum_{\Theta_i} f(\theta')\right) dA_\theta(z|\boldsymbol{k}, \Theta_i) = 0$$

where $\boldsymbol{k}$ denotes the set of limit cutoffs.

Proof. Fix $\tilde{\sigma} > 0$ and define a partition of types $\Theta_1, \ldots, \Theta_S$ by placing two types θ, θ' in the same equivalence class whenever $|k^{\tilde{\sigma}}(\theta) - k^{\tilde{\sigma}}(\theta')| < \tilde{\sigma}$. Define $Q^{\tilde{\sigma}}_\theta(\chi|\mathbf{k}^{\tilde{\sigma}}, z) = \Pr(\tau \leq \chi | s = k^{\tilde{\sigma}}(\theta), \psi(\tau, \Theta_i) = z)$ (for $\theta \in \Theta_i$) to be type $k^{\tilde{\sigma}}(\theta)$'s belief about τ conditional on the event that a proportion z of players in the same equivalence class of the partition play B. We have

$$E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] = \int_0^1 \int_{k^{\tilde{\sigma}}-\frac{\tilde{\sigma}}{2}}^{k^{\tilde{\sigma}}+\frac{\tilde{\sigma}}{2}} v\left(\theta, \chi, 1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2z\sum_{\Theta_i} f(\theta)\right) dQ_\theta^{\tilde{\sigma}}(\chi|\mathbf{k}^{\tilde{\sigma}}, z) dA_\theta(z|\mathbf{k}^{\tilde{\sigma}}, \Theta_i)$$

The term in the integrand is bounded by $v\left(\theta, k^{\tilde{\sigma}} \pm \frac{\tilde{\sigma}}{2}, 1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2z\sum_{\Theta_i} f(\theta)\right)$, so

$$E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] \le \int_0^1 v\left(\theta, k^{\tilde{\sigma}} + \frac{\tilde{\sigma}}{2}, 1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2z\sum_{\Theta_i} f(\theta)\right) dA_\theta(z|\mathbf{k}^{\tilde{\sigma}}, \Theta_i) \tag{17}$$

and

$$E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] \le \int_0^1 v\left(\theta, k^{\tilde{\sigma}} - \frac{\tilde{\sigma}}{2}, 1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2z\sum_{\Theta_i} f(\theta)\right) dA_\theta(z|\mathbf{k}^{\tilde{\sigma}}, \Theta_i) \tag{18}$$

Note that as $\tilde{\sigma} \to 0$, the right-hand side of (2) converges to the right-hand side of (3) as long as dA_θ is bounded, which is shown in Lemma 8 of Drozd and Serrano-Padial (2017).

Now, for each i, take some arbitrary $\theta_i \in \Theta_i$ and set $k_i = k^{\tilde{\sigma}}(\theta_i)$. As σ is taken to zero from $\tilde{\sigma}$, set cutoffs $\hat{\mathbf{k}}_\sigma^{\tilde{\sigma}}$ so that $\Delta_{\theta_i, \theta_i'} = \frac{k_i - \hat{k}_\sigma^{\tilde{\sigma}}(\theta_i')}{\sigma} = \frac{k_i - k^{\tilde{\sigma}}(\theta_i')}{\tilde{\sigma}}$ for all $\theta_i' \in \Theta_i$. Note that $A_\theta(z|\hat{\mathbf{k}}_\sigma^{\tilde{\sigma}}, \Theta_i)$ is constant as $\sigma \to 0$ under these transformed cutoffs. Then as $\sigma \to 0$,

$$E[v|\mathbf{k}_\sigma^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] \to \int_0^1 v\left(\theta, k_i, 1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2z\sum_{\Theta_i} f(\theta)\right) dA_\theta(z|\mathbf{k}_\sigma^{\tilde{\sigma}}, \Theta_i)$$

Fix $\epsilon > 0$. If we pick $\tilde{\sigma}$ close to zero, we can ensure that

$$\left|E[v|\mathbf{k}_\sigma^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] - E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)]\right| < \epsilon$$

for all $\sigma < \tilde{\sigma}$. This is because the solution of the system of equations $E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] = 0$ can be seen as the correct choice of $k^{\tilde{\sigma}}(\theta_i)$ and $\Delta_{\theta_i, \theta_i'}$ for each i holding Θ_i fixed (which is possible as long as $\tilde{\sigma}$ is sufficiently small). The solution to this system of equations lies in a compact set, so for small $\tilde{\sigma}$ the limit condition will not differ from the equilibrium condition $E[v|\mathbf{k}^{\tilde{\sigma}}, k^{\tilde{\sigma}}(\theta)] = 0$ by more than ϵ. Therefore the limit condition holds as $\tilde{\sigma} \to 0$. □

In order to proceed, we will need to define a stable equilibrium of the complete information game.

Definition B.1. *A* ***stable*** *equilibrium of the complete information game is a strategy profile $a(\theta)$ if there exists $\epsilon > 0$ such that for all $\epsilon' < \epsilon$, if a fraction ϵ' of players' choices are changed from the prescription of $a(\theta)$, the remaining players' best responses are to continue to play according to $a(\theta)$.*

We now prove the main theorem.

Theorem B.1. *Suppose that in the complete information game, for any value of τ there are at most two pure strategy (stable) equilibria: one in which all players choose A and one in which all players choose B. In the limit $\sigma \to 0$, the equilibrium strategies are given by a cutoff k common to all players such that*

1. *When $\theta_i = 0$ for all i with certainty, $k = 0$;*

2. *When $F(0) = 0$ and $F(\theta) < 1$ for some $\theta > 0$, $k < 0$.*

Proof. First note that as $\sigma \to 0$, the cutoff used by all agents must be the same. Suppose that there are two groups of types Θ_1 and Θ_2 such that types in Θ_1 use k_1 and types in Θ_2 use $k_2 > k_1$ as $\sigma \to 0$. Then there would be an equilibrium of the complete information game in which types in Θ_1 choose A and types in Θ_2 choose B when $\tau \in [k_1, k_2]$. By assumption, this equilibrium must be unstable. For $s \in [k_1 - \frac{\sigma}{2}, k_1 + \frac{\sigma}{2}]$, there is uncertainty about whether other types in Θ_1 will play A. For $s \in [k_1 - \frac{\sigma}{2}, k_1 + \frac{\sigma}{2}]$, there is uncertainty about whether other types in Θ_2 will play B. In fact, the belief constraint implies that some cutoff type must believe at least half of all others in Θ_1 will play B (or at least half of all others in Θ_2 will play A). By the definition of an unstable equilibrium, there must then always be some cutoff type who wants to deviate from the equilibrium cutoff strategy. Hence an unstable equilibrium cannot be the equilibrium selected in the limit, meaning there must be a cutoff common to all agents.

The rest of the proof follows from Lemma B.3. The cutoff k must satisfy the limit condition

$$\int_0^1 v\left(\theta, k, 1 - 2z \sum_{\Theta} f(\theta')\right) dA_\theta(z|k) = 0$$

for all $\theta \in \Theta$. When $\Theta = \{0\}$ the belief constraint (Lemma B.2) implies that $dA_\theta(z|k) =$

$dA(z|k) = zdz$. Then we have

$$\int_0^1 v(0, k, 1 - 2z) z dz = 0$$

From the symmetry assumption in Assumption B.1 it is immediate that this condition is satisfied when $k = 0$.

On the other hand, when there is a positive mass of agents with $\theta > 0$, we have

$$\sum_{\Theta} f(\theta) \int v\Big(\theta, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) dA_\theta(z|k) = 0$$

by summing over θ. Then by the assumption that v is increasing in θ,

$$\begin{aligned}\sum_{\Theta} f(\theta) \int v\Big(\theta, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) dA_\theta(z|k) &> \sum_{\theta} f(\theta) \int v\Big(0, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) dA_\theta(z|k) \\ &= \int v\Big(0, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) \Big(\sum_{\theta} f(\theta) dA_\theta(z|k)\Big) \\ &= \int v\Big(0, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) z dz\end{aligned}$$

where the first equality is obtained by noting that the integrand is independent of θ and the second follows from the belief constraint. Note that if $k \geq 0$, then the right-hand side is nonnegative, meaning that $\int v\Big(\theta, k, 1 - 2z \sum_{\Theta} f(\theta')\Big) dA_\theta(z|k)$ must certainly be positive. Thus the limit condition can only be satisfied by some $k < 0$. □

We may specialize the results to a case in which the function v is linear in order to derive further analytical expressions characterizing the equilibrium. From now on, we assume that

$$v(\theta, \tau, \phi) = \theta + \tau + \kappa\phi$$

The following proposition describes the main results in this linear case.

Proposition B.1. *In the limit $\sigma \to 0$, the equilibrium strategies are given by a monotone partition $\Theta_1, \ldots, \Theta_S$ of Θ and cutoffs $k_1 > \cdots > k_S$ such that*

(i) For all $\theta \in \Theta_i$, $k(\theta) = k_i$;

(ii) $-\underline{\theta}_i - \kappa(1 - 2F(\underline{\theta}_i)^-) \leq k_i \leq -\overline{\theta}_i - \kappa(1 - 2F(\overline{\theta}_i))$

(iii) $k_i + \kappa\left(1 - 2\sum_{\Theta_j, j<i} f(\theta) - \sum_{\Theta_i} f(\theta)\right) = -E[\theta|\theta \in \Theta_i]$ *for all* i.

where $\underline{\theta}_i = \min \Theta_i$, $\overline{\theta}_i = \max \Theta_i$.

Proof. Point (i) is a consequence of Lemma B.3. We now show the partition is monotone. Suppose that $\theta_1 > \theta_2$ but $\theta_2 \in \Theta_j$, $\theta_1 \in \Theta_m$ with $j > m$. Then

$$-\theta_1 \geq k_m + \kappa(1 - 2\sum_{\Theta_n, n \leq m} f(\theta)) \geq k_j + \kappa(1 - 2\sum_{\Theta_i, i<j} f(\theta)) \geq -\theta_2$$

a contradiction. From this it immediately follows that

$$-\underline{\theta}_i - \kappa(1 - 2F(\underline{\theta}_i)^-) \leq k_i \leq -\overline{\theta}_i - \kappa(1 - 2F(\overline{\theta}_i))$$

which is point (ii).

To see (iii), note that Lemma 3 implies that for all $\theta \in \Theta_i$,

$$0 = k_i + \theta + \kappa\left(1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2\sum_{\Theta_i} f(\theta) \int_0^1 z dA_\theta(z|\mathbf{k}, \Theta_i)\right)$$

Multiplying by $\frac{f(\theta)}{\sum_{\Theta_i} f(\theta')}$ on both sides and moving the θ term to the left-hand side,

$$\begin{aligned} -E[\theta|\theta \in \Theta_i] &= k_i + \kappa\left(1 - 2\sum_{\Theta_j, j<i} f(\theta) - 2\sum_{\Theta_i} f(\theta) \int_0^1 z d\left(\frac{1}{\sum_{\Theta_i} f(\theta)} \sum_{\Theta_i} f(\theta) dA_\theta(z|\mathbf{k}, \Theta_i)\right)\right) \\ &= k_i + \kappa\left(1 - 2\sum_{\Theta_j, j<i} f(\theta) - \sum_{\Theta_i} f(\theta)\right) \end{aligned}$$

where the second line follows from Lemma B.2, the belief constraint. This is precisely the desired result. □

Equipped with Proposition B.1, we may now prove some properties of equilibria when the distribution F satisfies certain conditions. We consider three scenarios:

1. F is continuous and $\theta + \kappa(1 - 2F(\theta))$ is monotonically increasing;

2. F has a symmetric, single-peaked density f and $\theta + \kappa(1 - 2F(\theta))$ is non-monotonic;

3. F is a two-point discrete distribution.

The next three propositions characterize the equilibrium in these three cases. Henceforth we assume H is the uniform distribution on $[-\frac{1}{2}, \frac{1}{2}]$.

Proposition B.2. *When F is continuous and $\theta + \kappa(1-2F(\theta))$ is a monotonically increasing function, the cutoffs $k(\theta)$ satisfy $k(\theta) = -\theta - \kappa(1-2F(\theta))$.*

Proof. We show that the partition described in Proposition B.1 must consist of singletons in this case. Suppose that $\theta_1 < \theta_2$ are the boundaries of equivalence class i of the partition. By property (ii) of Theorem 4, we have

$$-\theta_1 - \kappa(1 - 2F(\theta_1)) \leq k_i \leq -\theta_2 - \kappa(1 - 2F(\theta_2))$$

By assumption, $-\theta_1 - \kappa(1-2F(\theta_1)) > -\theta_2 - \kappa(1-2F(\theta_2))$, so this is impossible. Hence the partition is indeed a collection of singletons, and $k(\theta) = -\theta - \kappa(1-2F(\theta))$ (again by property (ii)). □

Proposition B.3. *Suppose F has a symmetric, single-peaked density f and $\theta + \kappa(1-2F(\theta))$ is non-monotonic. Let $\hat{\theta} = \arg\max_{\theta} f(\theta)$. The equilibrium is characterized by a parameter Δ such that*

- *$k(\theta) = -\theta - \kappa(1-2F(\theta))$ for $\theta \notin [\hat{\theta} - \Delta, \hat{\theta} + \Delta]$,*
- *$k(\theta) = -\hat{\theta} - \kappa(1 - F(\hat{\theta} - \Delta) - F(\hat{\theta} + \Delta))$ for $\theta \in [\hat{\theta} - \Delta, \hat{\theta} + \Delta]$,*
- *The parameter Δ is the unique nonzero solution to*

$$\Delta = \kappa(F(\hat{\theta} + \Delta) - F(\hat{\theta} - \Delta))$$

Proof. Observe that under the assumptions on F, there must be only one interval $[\underline{\theta}, \overline{\theta}]$ where $\theta + \kappa(1-2F(\theta))$ is decreasing. All θ in this interval must belong to the same equivalence class of the partition described in Proposition B.1. We show this by contradiction. If $\theta \in [\underline{\theta}, \overline{\theta}]$ is at the upper boundary of an equivalence class Θ_i, then by point (ii) of Proposition B.1 we have

$$k_i \leq -\theta - \kappa(1 - 2F(\theta)) < k_{i+1}$$

which is impossible because the cutoffs are monotonically decreasing in i.

Hence the entire increasing region $[\underline{\theta}, \overline{\theta}]$ belongs to a single equivalence class of the partition. At the boundaries of the equivalence class containing that interval, $k(\theta)$ must be continuous (which follows by again applying the argument showing that there cannot be two equivalence classes containing points in the increasing region). By the argument in Proposition B.2, there cannot be an equivalence class of the partition containing only points in the decreasing region, so it must be that the partition consists of a single equivalence class $[\underline{\theta}, \overline{\theta}]$ containing all values of θ in the increasing region and singletons for all θ outside that interval.

Let $k(\theta) = k$ for $\theta \in [\underline{\theta}, \overline{\theta}]$. Point (iii) of Theorem 4 implies that

$$k = -\left(E[\theta|\underline{\theta} \leq \theta \leq \overline{\theta}] + \kappa(1 - F(\underline{\theta}) - F(\overline{\theta}))\right) \tag{19}$$

Continuity of the cutoff at the boundaries of the interval implies

$$-\big(\underline{\theta} + \kappa(1 - 2F(\underline{\theta}))\big) = k = -\big(\overline{\theta} + \kappa(1 - 2F(\overline{\theta}))\big)$$

Rearranging these expressions, we find

$$\frac{\overline{\theta} + \underline{\theta}}{2} = E[\theta|\underline{\theta} \leq \theta \leq \overline{\theta}] \tag{20}$$

$$\frac{\overline{\theta} - \underline{\theta}}{2} = \kappa(F(\overline{\theta}) - F(\underline{\theta})) \tag{21}$$

The symmetry of the density f and (5) imply that $E[\theta|\underline{\theta} \leq \theta \leq \overline{\theta}] = \hat{\theta}$ and there exists Δ such that $\underline{\theta} = \hat{\theta} - \Delta$, $\overline{\theta} = \hat{\theta} + \Delta$. Then (4) reduces to

$$k(\theta) = -\hat{\theta} - \kappa(1 - F(\hat{\theta} - \Delta) - F(\hat{\theta} + \Delta))$$

for $\theta \in [\hat{\theta} - \Delta, \hat{\theta} + \Delta]$ and (5) reduces to

$$\Delta = \kappa(F(\hat{\theta} + \Delta) - F(\hat{\theta} - \Delta))$$

as desired. Finally, we must show that there is a unique nonzero solution Δ to the above equation. The derivative of the left-hand side with respect to Δ is 1, and the derivative of the right-hand side is $2\kappa f(\hat{\theta} + \Delta)$ by the symmetry of f. The derivative of the right-hand side is greater than 1 for $\Delta = 0$ (since $\theta + \kappa(1 - 2F(\theta))$ is increasing at $\hat{\theta}$) and monotonically decreasing towards zero, so there is a unique crossing point. □

Proposition B.4. *When F is a two-point distribution with support $\{\theta_L, \theta_H\}$ (and $\theta_L < \theta_H$) such that* $\Pr(\theta = \theta_L) = \mu$, $\Pr(\theta = \theta_H) = 1 - \mu$, *the equilibrium cutoffs are*

- $k(\theta) = -(\mu\theta_L + (1 - \mu)\theta_H)$ *for all* θ *if* $\theta_H - \theta_L \leq \kappa$,
- $k(\theta_L) = -(\theta_L + (1 - \mu)\kappa)$ *and* $k(\theta_H) = -(\theta_H - \mu\kappa)$ *if* $\theta_H - \theta_L > \kappa$.

Proof. There are two possible cases when the support of F consists of two points: either $k(\theta_L) = k(\theta_H)$ or $k(\theta_L) > k(\theta_H)$. We first suppose that the cutoffs are equal and derive the restriction $\theta_H - \theta_L = \kappa$ in that case. Recall from Lemma B.3 that when $k(\theta_H) = k(\theta_L) = k$,

$$0 = k + \theta_H + \kappa\Big(1 - 2\int_0^1 z dA_{\theta_H}(z|k)\Big) = k + \theta_L + \kappa\Big(1 - 2\int_0^1 z dA_{\theta_L}(z|k)\Big)$$

We will derive an expression that allows us to evaluate the integrals on the right-hand side in terms of the cutoffs for small σ.

Consider the equilibrium with finite, nonzero σ. We have

$$\begin{aligned}
E[v|\mathbf{k}^\sigma, k^\sigma(\theta_H)] = &\int_{k^\sigma(\theta_H)-\frac{\sigma}{2}}^{k^\sigma(\theta_H)+\frac{\sigma}{2}} \Big(\tau + \theta_H + \kappa\Big) h\Big(\frac{k(\theta_H) - \tau}{\sigma}\Big) d\tau \\
&- 2\kappa \int_{k^\sigma(\theta_H)-\frac{\sigma}{2}}^{k^\sigma(\theta_H)+\frac{\sigma}{2}} \Big(\mu(1 - H(\frac{k(\theta_L) - \tau}{\sigma})) + (1-\mu)(1 - H(\frac{k(\theta_H) - \tau}{\sigma}))\Big) h\Big(\frac{k^\sigma(\theta_H) - \tau}{\sigma}\Big) d\tau \\
&= \kappa^\sigma(\theta_H) + \theta_H + \kappa(1 - \mu(1 + \Delta_{H,L}^2) - (1-\mu)) \\
&= \kappa^\sigma(\theta_H) + \theta_H - \kappa\mu\Delta_{H,L}^2
\end{aligned}$$

where the third line uses the fact that H is the uniform distribution on $[-\frac{1}{2}, \frac{1}{2}]$. Similarly, we find

$$E[v|\mathbf{k}^\sigma, k^\sigma(\theta_L)] = \kappa^\sigma(\theta_L) + \theta_L + \kappa(1-\mu)\Delta_{H,L}^2$$

Suppose that as $\sigma \to 0$, $\Delta_{H,L} \equiv \frac{k(\theta_H) - k(\theta_L)}{\sigma} \to \xi$. Then these equations imply

$$k + \theta_H - \kappa\mu\xi^2 = k + \theta_L + \kappa(1-\mu)\xi^2$$

so

$$\theta_H - \theta_L = \kappa\xi^2$$

Clearly, $\xi^2 \in [0, 1]$, so we obtain

$$\theta_H - \theta_L \leq \kappa$$

when the cutoffs are equal.

Now consider the case in which the cutoffs are not equal. Then when $\sigma \to 0$, the cutoff type $k(\theta_H)$ is certain that all type θ_L players received signals below $k(\theta_L)$, and type $k(\theta_L)$ is certain that all type θ_H players received signals above $k(\theta_H)$. The equilibrium conditions are then

$$0 = k(\theta_H) + \theta_H + \kappa(1 - 2\mu - (1 - \mu)) = k(\theta_L) + \theta_L + \kappa(1 - \mu)$$

by part (iii) of Proposition B.1. Rearranging, we get

$$k_L - k_H = (\theta_H - \kappa\mu) - (\theta_L + \kappa(1 - \mu))$$

Given that $k_L > k_H$, we must have

$$\theta_H - \theta_L > \kappa$$

which completes the proof. □

C Additional Results

C.1 Competition between a monopolist and a blockchain

Now we turn to competition between a monopolist and a blockchain. The primary difference from the previous example of competition between two centralized entities is that the agent who proposes the fee structure for a blockchain does not care about the fees earned by writers because writers always break even. Rather, the proposer's incentives are aligned with those of readers. As before, the proposer can be thought of as a developer of blockchain software who has a large stake in the network that appreciates when others use the blockchain platform. Formally, there are two ledgers A (monopolist) and B (blockchain) with proposers $P^A = \mathcal{M}$, who is also the writer on ledger A, and $P^B = \mathcal{D}$ (for "developer") who is not a blockchain writer. Proposers P^A and P^B choose parameters $L^A, L^B \geq 0$ at $\tau = 0$. The stakes on proposer P^A's ledger are uniformly distributed on $[S - \frac{d}{2}, S + \frac{d}{2}]$, and the stakes on P_B's ledger are all equal to zero. When a blockchain competes against a monopolist, there is still perfect competition between blockchain writers, but the blockchain cannot replicate the information contained on the monopolist's ledger.

As in the baseline blockchain model, there is a continuum of writers $j \in [0, M]$. However, there is no longer incomplete information. When readers' stakes on ledger A are distributed in an interval of finite length, an arbitrarily small amount of noise in agent's beliefs will have no effect on the equilibrium. Nevertheless, despite this change to the model, the equilibrium played by writers will be the same as in the baseline model of a blockchain fork.[14] Furthermore, blockchain writers cannot write on the monopolist's ledger, so they all must commit to ledger B at $\tau = 1$. The equilibrium at $\tau = 2$ is just like the equilibrium in the case of monopolistic competition so long as Condition SC is satisfied, which again reduces to the inequality $d \geq \kappa$. To see this, note that in this setting the distribution of types is simply the distribution of stakes on ledger A and apply Proposition 1.

We then have equilibrium play along any path for $\tau \geq 1$, so solving the model reduces to solving the proposers' optimization problems at $\tau = 0$. The monopolist behaves as if facing a fixed outside ledger with parameter L^B, so the optimal L^A is again given by 6. However, P^B has different preferences than an entrant monopolist. As in the baseline blockchain model, P^B's preferences are given by readers' utility function $\tilde{u}$. If there is a value L^{B*} that is uniformly best for readers (with utility function $\tilde{u}$) given optimal play by writers, proposer P^B will choose it. The monopolist then chooses

$$L^A = \frac{\frac{d}{2} - \frac{\kappa}{2} + S + \alpha L^{B*}}{2\alpha}$$

as long as

$$S + \alpha L^{B*} \leq \frac{3}{2}(d - \kappa)$$

This inequality is the no-entry bound in the presence of a blockchain. Note that the no-entry bound is tighter when L^*_B is larger. This is because when the minimum feasible computational power required to support a blockchain is large, the compensation necessary to attract writers (and thus the minimum blockchain fee) will be higher, thereby dissuading readers from using the blockchain.

The fee charged on the blockchain will be lower than that charged by an entrant monopolist precisely when L^{B*} is less than the expression given in 8 for the entrant's fee. Furthermore, in this case the lower fee charged on the blockchain will induce the incumbent monopolist to drop its fee below what it would charge when facing an entrant monopolist. The condition for a blockchain to lower fees on both ledgers is

$$L^{B*} < \frac{1}{2\alpha}(d - \kappa) - \frac{1}{3\alpha}S$$

A blockchain lowers costs for readers when the computational expenditure required to placate readers' need for cryptographic security is small, when the dispersion of readers' stakes on the monopolist's ledger is high, or when the coordination motive is weak. Surprisingly, a blockchain tends to lower costs when the average stake on a monopolist's ledger is small. This is because when stakes on a monopolist's ledger are large, an entrant monopolist would optimally charge a low fee in order to induce switching by readers. Hence when the incumbent already charges high fees, competition by a traditional intermediary should be enough to lower costs to readers. Blockchain is useful primarily when entrants into the market have incentives

[14] Indeed, the $\tau = 2$ part of the proof of Proposition 3 is independent of the information structure so long as all writers observe participation on the ledger.

to charge high fees. Free entry of blockchain writers implies that there is no incentive for a proposer to choose a policy that gives writers large fees because all writers break even regardless. The feature of the blockchain that allows it to more effectively compete with traditional intermediaries is that it strips writers of their market power.

C.2 Multi-Homing

Here we prove results related to the model in Section 3.5. First we describe the equilibria of the complete information game.

Proposition C.1. *Suppose B is the entrant ledger in the sense that $s_i^B = 0$ for all i. There are two equilibria in the complete information game as long as $\min\{\alpha L^A, \alpha L^B\} < \min\{\kappa, \max_i s_i^A\}$: there is one in which all readers choose only A, and there is one in which all readers choose B and some readers multi-home.*

Proof. First note that a strategy profile in which all readers choose A is indeed an equilibrium: we have

$$u^A = s_i^A + \kappa - \alpha L^A > \max\{u^\emptyset, u^B, u^{A\cup B}\}$$

for all i since $u^B = -\alpha L^B$ and $u^{A\cup B} = u^A - \alpha L^B$.

Now suppose that there is some equilibrium with $\phi^B > 0$. Then

$$u^B = \kappa(\phi^{A\cup B} + \phi^B) - \alpha L^B > 0$$

If some agents multi-home (i.e. $\phi^{A\cup B} > 0$), then it must be that

$$u^{A\cup B} = s_i^A + \kappa(\phi^A + \phi^{A\cup B} + \phi^B) - \alpha(L^A + L^B) > s_i^A + \kappa(\phi^A + \phi^{A\cup B}) - \alpha L^A = u^A$$

which implies

$$\kappa\phi^B - \alpha L^B > 0 \Rightarrow \kappa(\phi^{A\cup B} + \phi^B) - \alpha L^B > 0$$

Therefore, if some agents multi-home, then all agents must choose B. However, if no agents multi-home, then $\phi^{A\cup B} = 0$, so we still have that if some agents choose only B, then all agents must choose B.

Now we show that some agents must multi-home. Even if $\phi^A + \phi^{A\cup B} = 0$, we have

$$u^{A\cup B} - u^B = s_i^A - \alpha L^A > 0$$

for some i by assumption. Hence in any equilibrium where some agents choose only B, all agents must choose B or multi-home.

Finally, by the argument above it is evident that there can be no equilibrium in which all agents either choose A or multi-home. In this case, all agents would find it optimal to choose B, so all agents would multi-home, which cannot be an equilibrium. $\square$

Proposition 1 shows that when ledger B is used by some, all readers must use it. This may seem like a somewhat extreme result, but it can be modified by assuming that readers have heterogeneous preferences for the properties of ledgers A and B. In such a case, there would be equilibria in which some readers choose A, some readers choose B, and some readers multi-home, which is arguably closer to the empirically relevant case.

Note that there is a discontinuity at $L^A = L^B = 0$. In that case, the only trembling-hand perfect equilibrium is one in which all readers multi-home. When the cost of using a ledger is even $\epsilon > 0$, though, this ceases to be an equilibrium at all.

Since we want to obtain unique predictions about equilibrium play, we now turn to a setting with incomplete information. Suppose that readers derive fundamental utility $-(\alpha L^B + \zeta)$ from using ledger B, where ζ is unknown. As in the benchmark model, readers receive signals $x_i = \zeta + \sigma\epsilon_i$, where the distribution of ϵ_i has support on $[-\frac{1}{2}, \frac{1}{2}]$. We now consider the global games refinement.

C.3 Simultaneous ledger choice

We consider a game in which readers choose among their four possible strategies simultaneously. This game is more complicated because (1) we need to show it can be cast as a supermodular game, and (2) we need to determine what the cutoff strategies look like (since they are no longer a choice between just two options). We state without proof that the game is supermodular under the following parametrization: identify the set $\{0, 1\}^2$ with readers' choices by taking any element with first coordinate 1 to as a strategy where the reader chooses A and any element with second coordinate 0 as a strategy where the reader chooses B.

As the noise in the signals of ζ approaches zero, the equilibrium play of the complete information game is recovered. Therefore, there must be a cutoff $\overline{k}$ such that all readers with $s_i > \alpha L^A$ choose only A when $x_i > \overline{k}$ and multi-home when $x_i < \overline{k}$, and readers with $s_i < \alpha L^A$ choose only A when $x_i > \overline{k}$ and choose only B when $x_i < \overline{k}$.

We characterize the cutoff equilibrium and derive the fee L^B required for some readers to choose ledger B.

Proposition C.2. *For a given L^A, there is a cutoff value $\overline{L}^B(L^A)$ such that readers all choose B whenever $L^B < \overline{L}^B(L^A)$, and no reader chooses B otherwise. The cutoff value is*

$$\overline{L}^B(L^A) = \frac{Q(\alpha L^A)}{2 - Q(\alpha L^A)}(\alpha L^A - E[s|s \leq \alpha L^A])$$

This cutoff value is increasing under a first-order shift upwards of the CDF Q.

Proof. At the cutoff, readers with $s_i > \alpha L^A$ are indifferent between choosing only A and multi-homing. Hence

$$0 = \int_0^1 \left((s + \kappa(1 - Q(\alpha L^A) + Q(\alpha L^A)(1 - z)) - \alpha L^A) - (s + \kappa - \alpha(L^A + L^B) - \overline{k}) \right) dA_s(z|\mathbf{k})$$

This yields

$$\alpha L^B + \overline{k} = \kappa Q(\alpha L^A) \int_0^1 z dA_s(z|\mathbf{k})$$

for $s > \alpha L^A$. This condition immediately yields $L^B \leq \frac{\kappa}{\alpha} Q(\alpha L^A)$.

By contrast, readers with $s < \alpha L^A$ choose between using only A or only B at the cutoff. Their indifference condition is

$$0 = \int_0^1 \left((s + \kappa(1 - Q(\alpha L^A) + Q(\alpha L^A)(1 - z)) - \alpha L^A) - (\kappa Q(\alpha L^A) z - \alpha L^B - \overline{k}) \right) dA_s(z|\mathbf{k})$$

This condition implies

$$\alpha L^B + \overline{k} = \alpha L^A - s + \kappa \int_0^1 (2Q(\alpha L^A) z - 1) dA_s(z|\mathbf{k})$$

We can combine the two equations for the cutoff and integrate over s to obtain

$$(1 - Q(\alpha L^A) + \frac{1}{2} Q(\alpha L^A))(\alpha L^B + \overline{k}) = \frac{1}{2} Q(\alpha L^A)(\alpha L^A - E[s|s \leq \alpha L^A] - \kappa) + \kappa Q(\alpha L^A) \int_0^1 z \int dA_s dQ$$

By Lemma B.2, $\int_0^1 z \int dA_s dQ = \frac{1}{2}$. Then after some rearrangement, we finally obtain

$$\alpha L^B + \overline{k} = \frac{Q(\alpha L^A)}{2 - Q(\alpha L^A)} (\alpha L^A - E[s|s \leq \alpha L^A]) \tag{22}$$

so if any reader uses B in equilibrium, L^B must be less than or equal to the right-hand side. □

As expected, the anchor on A is stronger when readers' stakes in A are higher. The formula for the cutoff is also useful in a situation where readers' stakes on both ledgers are the same (as in a blockchain). For example, if we simply take $s_i = 0$ for all i, the formula simplifies to

$$\overline{k} = \alpha(L^A - L^B) \tag{23}$$

Then when $\zeta \approx 0$ (as we assume throughout) we find that even in the presence of multi-homing, the ledger with the lower fee wins out.

C.4 Enforcement

Dictatorial equilibrium with an enforcer: In this section, we describe a model of ledger choice with enforcement issues. In addition to proposers, readers, and writers, there is a fourth type of agent known as an enforcer. This agent must take a costly action in a new subperiod $\tau = 3$ in order to enforce obligations written down in the ledger. Formally, the enforcer exerts effort e to enforce obligations and receives fees ϕL_E if ϕ readers choose its ledger. For simplicity, in this section we assume that readers choose between using a given ledger A and not using a ledger at all. Readers get payoff $s_i + \kappa\phi - \alpha(L_W + L_E)$ when they use the ledger and the enforcer chooses to enforce at $t = 3$ and payoff $-\alpha(L_W + L_E)$ otherwise (where L_W is the fee earned by writers). They may also choose not to use the ledger at all, in which case they get zero.

Of course, the enforcer has no incentive to take the costly action in the stage game, since the payment to the enforcer is not contingent on whether he takes the costly action. We assume, as in our dynamic setting, that the game is played on days $t = 0, 1, \ldots$. We now illustrate the presence of an enforcer can undermine the decentralization that is central to blockchain's benefits.

Intuitively, the need for enforcement (whether by a government or some other agency) is detrimental to decentralization because this entity can threaten to stop enforcing agreements unless the blockchain adopts certain protocols, thereby destroying the mechanism by which blockchain selects the outcome most beneficial to readers. Blockchains that operate under conditions favorable to readers will be dysfunctional because the enforcer will refuse to recognize them. In our model, this type of equilibrium can be captured in a simple way: suppose that there is a policy L_W^* preferred by the enforcer. The enforcer receives an additional benefit $V(L_W^*)$ whenever policy L_W^* is proposed. If the proposer in period t announces L_W^*, the enforcer takes the costly action to enforce at $\tau = 3$ of period t. Otherwise, the enforcer refuses to take the costly action in all subsequent periods, and readers stop using the ledger.

Checking incentive compatibility of this strategy profile is simple. The enforcer may deviate either by choosing not to enforce in periods where he is supposed to or by enforcing when he is not supposed to. Clearly, the latter deviation is always suboptimal, since readers do not use the ledger in any future period regardless of what the enforcer does. For it to be optimal to enforce along the equilibrium path, we must have

$$e \leq \frac{\delta}{1-\delta}(L_E - e + V(L_W^*))$$

That is, the one-shot benefit of shirking enforcement duties must exceed the enforcer's stream of future profits plus the benefits it receives when L_W^* is played on future days.

There is no incentive for any other agent to deviate from the prescribed strategy profile. Readers play myopically, so they choose A whenever the enforcer is expected to take the costly action and exit otherwise. Writers always make zero profits, so they have no incentive to deviate. Proposers get nothing if they propose anything other than L_W^*, so they also play according to the equilibrium prescription.

Of course, this equilibrium is not unique, but it illustrates that, unlike in the case without enforcement, there is not a unique equilibrium in which the best outcome for readers is always realized. The equilibrium becomes dynamic rather than static because despite the fact that *writing* is decentralized, *enforcement* is not decentralized. A single centralized enforcer that is crucial to the functioning of the blockchain may be able to subject the blockchain's policies to its will because, unlike other agents, it can threaten to prevent the blockchain from functioning properly.

Synergy between writing and enforcement: We can also consider a situation in which the enforcer, writer, and proposer are the same entity (analogously to the case without enforcement where monopolistic intermediaries were both writers and proposers). The goal is to determine whether there is a synergy between writing and enforcement in the sense that the rents required by an intermediary who performs both functions are less than those needed to compensate two separate entities who write on the ledger and enforce its contents.

The intermediary takes an action $h \in [0, \overline{h}]$ to distort the ledger and an action $e \in [0, 1]$ to enforce obligations. Deviations from the "honest" strategy $(h, e) = (0, 1)$ go undetected with probability $\tilde{p}(h, e) = (1 - p(h))(1 - q(e))$, where $p(h)$ is increasing in h and $q(e)$ is increasing in e. We further assume $p(\overline{h}) = 1$ and $q(1) = 1$, so $\tilde{p}(x, e) = 0$ when the intermediary plays honestly. The analysis in the previous section was equivalent to the assumption that $1 - q(e) = \mathbf{1}\{e < 1\}$, so the enforcer always chose $e \in \{0, 1\}$.

The intermediary obtains benefit $v(h, e)$ from taking action (h, e) in addition to a fee L that it receives every period (independent of its actions). We assume strategic substitutability between distortion of the ledger and lack of enforcement:

$$v(h, e) = \overline{h} - h - e$$

Under the harshest punishment, then, the intermediary solves

$$V = \max_{h,e} \tilde{V}(h,e) = \max_{x,e} \frac{L + \overline{h} - h - e}{1 - \delta(1 - p(h)))(1 - q(e))}$$

We may now derive bounds on the fee L such that the writer-enforcer plays honestly. The derivatives of the intermediary's objective function satisfy

$$\frac{\partial}{\partial h}\tilde{V}(h,e) = -(1 - \delta(1 - p(x))(1 - q(e))) - \delta p'(x)(L + \overline{h} - h - e)$$

$$\frac{\partial}{\partial e}\tilde{V}(h,e) = -(1 - \delta(1 - p(x))(1 - q(e))) - \delta q'(e)(L + \overline{h} - h - e)$$

If the intermediary plays honestly, it must be that $\tilde{V}$ is nondecreasing in e and nonincreasing in x at $(x,e) = (0,1)$. Hence we must have

$$L \geq \left(\frac{1}{\delta} - 1\right) \max\left\{ -\frac{1}{p'(0)},\ -\frac{1}{q'(1)} \right\} \tag{24}$$

We can now compare this situation to one in which the ledger is written by a decentralized group of blockchain writers and enforced by an outside entity. We assume that readers abandon the ledger whenever any type of deviation is detected, whether it is by the writers or the enforcer. The enforcer earns a fee L_E per period and solves

$$\max_e \frac{L_E - e}{1 - \delta q(e)}$$

As in the benchmark model of blockchain security, large blockchain writers solve

$$\max_x (1 - p(h))(L_W + \overline{h} - h)$$

where L_W is the aggregate fee earned by blockchain writers. The incentive compatibility conditions that come out of the enforcer's and writers' optimization problems are

$$L_E \geq -\left(\frac{1}{\delta} - 1\right)\frac{1}{q'(1)}$$

$$L_W \geq -\frac{1}{p'(0)}$$