Blockchain Economics

Joseph Abadi and Markus Brunnermeier

March 15, 2018

Abstract

Whether trustworthy record-keeping is better arranged through distributed ledger technology (DLT) or via a centralized intermediary depends on users’ ability to detect and respond to misconduct. Blockchains/DLT also rely on miners’ competition as miners’ free entry rules out any dynamic incentivization via franchise value, the core mechanism the traditional centralized intermediary arrangement relies on. A blockchain is cheaper when intermediary’s franchise value is not fragile, e.g. for a too-big-to-fail institution. While blockchains can keep track of transfer of ownership, proper enforcement of possession rights is still needed, except in the case of (fiat) cryptocurrencies.
1 Introduction

Fintech has the potential to revolutionize finance. Some observers even argue that blockchain technology is an invention as groundbreaking as the invention of double-entry bookkeeping in fourteenth-century Italy. Blockchains could drastically change record-keeping of financial transactions and ownership data. Traditionally, centralized entities have been responsible for maintaining records. These intermediaries are trusted not to distort ledgers in their own favor because they stand to lose their franchise values in the event that the public discovers fraudulent activity.

The emerging fintech industry has provided us with a radical alternative to record information: distributed ledger technology. Blockchains are ledgers written by decentralized, usually anonymous groups of agents rather than known centralized parties. Achieving consensus on such a ledger is important given that, in principle, anyone may write essentially anything on it. Consensus is reached by making the ledger publicly viewable and verifiable. Anyone who writes on or reads the ledger can quickly perform a cheap computation in order to confirm the correctness of a given transaction. However, as anonymously written ledgers, blockchains require identity management in the form of high computational costs. That is, those who write on the ledger must perform a computationally expensive task in order to do so. Otherwise it would be possible for individual entities to pretend they were a large number of entities, subverting the democratic nature of the distributed ledger. A critical issue is whether the computational cost of identity management is economically wasteful.

The key question we address is for which ledgers it is more economically efficient to use a blockchain and for which it is better to use a monopolistic intermediary. Currently, centralized entities such as banks are in charge of recording payments, exchanges intermediate securities issuance and trade, governments oversee land registries, and auction houses authenticate the provenance of luxury goods, among other activities. Writers on a given type of ledger can be incentivized to write honestly by other writers or by those who read or use the ledger and take actions in response to the reported history. Writers may report that other writers are acting dishonestly, but the ultimate power to discipline the writing community lies with the readers. If readers believe that records have been distorted, they may simply desert the ledger. That is, they can stop taking actions in response to the reported history, at which point any attempt to distort the ledger becomes irrelevant.

Each type of ledger imposes its own technological restrictions on the interactions between readers and writers. For example, for a monopolistic intermediary, the intermediary is the sole writer whereas the readers are its clients and possibly a regulatory agency. For a cryptocurrency, the writers who perform the required expensive computations (miners) may enter freely and the readers are the users of the currency. In addition to the two polar cases of centralized and decentralized record-keeping that we consider, there is a third type of ledger called a permissioned blockchain. Writers on a permissioned blockchain are granted special writing permissions, and the reading and writing protocols provide incen-
tives that lie somewhere in between those faced on anonymous blockchains and those faced by centralized entities.

We highlight two distinct channels through which the writer(s) can be disciplined. Writers have static incentives to act honestly because readers may discover they are making fraudulent reports. Readers then could immediately cease to act in response to those reports, thereby nullifying any gain from dishonest reporting. If writers have franchise values, they also have dynamic incentives to comply with the rules: readers may threaten to permanently exit the ledger, which destroys any franchise value the writers might have.

The principal tradeoff in determining which ledgers should be kept on “free entry” blockchains is precisely the tradeoff between the provision dynamic and static incentives. On the one hand, paying an extra fee in order to give an intermediary a sufficiently large franchise value distorts incentives and redistributes resources in a potentially undesirable way. On the other hand, due to the ability of writers to freely enter and leave the blockchain ecosystem, their incentives must be entirely static. Writers on a blockchain can never have a franchise value at stake when they choose to deviate, since more writers would enter if they could make positive profits. The electricity required to foster sufficient competition and provide static incentives to secure a blockchain is a pure waste of resources.

We outline the competitive mechanism that provides static incentives on a blockchain: in any static equilibrium with a sufficient number of writers, the writers must report honestly. Just as several competing firms produce more than would be optimal for a monopolist, when writers do not discipline each other by refusing to go along with fraudulent behavior, they attempt to distort the ledger more than is optimal in aggregate. Readers then discover this distortion with high probability, at which point they ignore the chain of fraudulent transactions. This reverses the dishonest writers’ gains and makes it more profitable to play honestly. Our theory sheds light on how the types of incentives necessary to ensure honest reporting differ across settings, such as in reporting payments, maintaining records of property ownership, or issuing contracts.

Our main findings are that a blockchain is cheap relative to a centralized intermediary when either (1) competition between blockchain writers renders consensus insensitive to a single writer’s actions, or (2) the intermediary’s reputation is resilient to deviations. This second condition suggests that markets intermediated by institutions that are too big to fail are better suited to intermediation via blockchain. More generally, if readers sometimes forgive a centralized intermediary for deviations, it reduces the intermediary’s incentives to report honestly, which necessitates payment of large rents to the intermediary. Additionally, we find that financial frictions are critical in order to keep a blockchain secure. If one agent is wealthy enough to buy all the computing power currently on the blockchain, she will do so. Whereas a decentralized group of agents obtains transaction fees associated with writing on the ledger, one agent who owns the entire network receives these fees plus monopolistic rents and is therefore willing to pay more for the computational resources.

Finally, we make the important point that in many settings transfers of possession as well as ownership must be guaranteed. 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 he holds the deed, his ownership of the house will be enforced. This concern is especially important in developing countries, where tracking and enforcing property rights is often an issue. A blockchain can guarantee a secure transfer of the deed, but it cannot guarantee the buyer’s right to use the house will be enforced. Another example is the debt market. A blockchain can be used to transfer ownership of debt, but does not guarantee the transfer of possession of cash when a debt comes due. Finally, in markets where goods can be counterfeited (such as in the markets for art or diamonds), a purchase does not guarantee possession of the genuine article unless it is possible to track the item’s origin. Luxury goods can be traded on a blockchain, but it is impossible to check whether they are counterfeit simply by looking at the ledger. Cryptocurrency is the outlier: a unit of virtual currency does not represent the right to possession of any asset, but rather has value because it is widely accepted as a medium of exchange.

When the concern is with a government that enforces property rights, having a blockchain with many writers does nothing to ensure the integrity of possession rights. A corrupt government can arrange transfers to the blockchain writers to ensure that they steal precisely the optimal amount and nothing more. This deviation is thus profitable for both the government and the writers. An example of this type of ledger is a land registry in a developing country, where the government may take advantage of poor record-keeping in order to cover up land seizures. In markets where intermediaries play an important role in disciplining agents, such as in a consumer debt market, using a blockchain is a poor choice. Writers never do anything that is not in their immediate best interest because new entrants compete away any future rewards. As such, writers can never commit to taking a costly action in order to punish agents in default.

However, in markets where issuers of contracts require an intermediary’s assistance in order to default, a blockchain provides security. Just as in the baseline model, if writers on the blockchain fail to discipline each other, they will collectively take bribes from issuers that exceed the optimal amount, readers will detect this activity, and the attempted fraud will be unsuccessful. In a currency market, for example, a counterfeiter would require the assistance of an intermediary in order to fool sellers into thinking a payment is genuine. The same logic applies to securities exchanges, where an issuer of fake securities may wish to bribe the exchange to assure buyers of their authenticity. Lastly, a blockchain can be useful in proving property ownership, which could be especially economically useful in developing nations. De Soto (1989) writes that bureaucratic impediments to property ownership in such countries prevent the poor from leveraging their assets and using them as productive capital.

**Related Literature.** 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 even if there are no writers who are compelled to play honestly, the network still becomes secure when there is a sufficient number of writers. This result obtains because the readers can threaten to ignore the ledger, rendering any attempt to steal useless. The ability of readers to leave the blockchain (in favor of some other system or complete autarky) is of first-order importance in reality and cannot be ignored. After all, blockchain systems were developed in part because of the lack of faith in traditional centralized institutions. 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.

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, including as malicious attacks. In our model, forks are exclusively attacks on the system and are ruled out by a novel mechanism: readers abandon the ledger when an attack succeeds. Cong and He (2017) show that decentralization leads to consensus, as in our paper, but the paper focuses 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.

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, since unlike Diamond (1984), there is no law of large numbers that obviates the need to “monitor the monitors.” In the computer science literature, Wüst and Gervais (2017) study the applicability of blockchain to several markets from an informal standpoint.

Some of the recent literature on blockchains in economics focuses on the security and the costs of the system. 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. 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 relating the cost of a blockchain directly to its security: in our model, the fee paid to a writer is essentially chosen by a mechanism designer, and the cost of the blockchain is proportional to the size of the fee needed to ensure sufficiently many writers enter.

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 blockchain security and compare it to a benchmark with a monopolistic intermediary in order to determine when blockchain is more efficient. Section 4 examines the uses of blockchain in markets where it is necessary to enforce possession rights. Section 5 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. 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. 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. An event such as this one is known as a “hard fork” and features prominently in our model.

On any blockchain, there are some rules that readers and writers tacitly agree to follow. 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.

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. 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. An example of such a situation is depicted in Figure 1.

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 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 detecting a deviation.

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.

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 currently 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.

An important question is whether we actually need PoW in order for the blockchain to function correctly. After all, it would be desirable to have a secure method of record-keeping without incurring the substantial costs associated with PoW. While some claim that any
attack on a blockchain is unprofitable because readers would detect the attack and ignore updates to the ledger, in this case it would be possible to secure the ledger using a single writer, meaning PoW provides a superfluous layer of security. That is, when readers are able to provide sufficient discipline, having a mechanism by which anonymous writers discipline each other is pointless. The mainstream models of blockchain security, such as Gervais et al. (2016), assume that as long as no single entity has a majority of the computing power, the blockchain will be secure because no writer will ever assist another in an attack. This logic embeds the assumption that writers do not collude with each other. However, if this were the case, again PoW would be rendered pointless. A permissioned blockchain with a sufficient number of writers would suffice to secure the blockchain under these conditions. Some in the blockchain community have expressed doubts that a permissioned blockchain could be trusted because of the possibility of collusion among writers, which is where a PoW-based system finally becomes important. We show that the free entry condition implies there will be no dynamic collusion between writers in any equilibrium on a PoW-based blockchain, which is not necessarily the case for a permissioned blockchain because there is no entry. In sum, PoW is useful when

- Readers cannot provide sufficient incentives for writers to act honestly by themselves;
- Writers are able to collude with one another.

3 Blockchain Intermediation

In this section, we set up the basic model and derive conditions under which a blockchain is secure. We compare the cost of securing a blockchain to the cost of incentivizing a monopolistic intermediary that plays a simple reputation game with its clients.

3.1 Setup—Static Model

Time is continuous, \( t \in [0, \infty) \). As time progresses, blocks appear at rate \( \eta \) and are added to a blockchain. At time \( t \), the blockchain consists of a tree \( B^t = (B_0, B_1, \ldots, B_n) \) of blocks that have arrived before time \( t \). It will be useful to denote the time at which block \( B_i \) arrived by \( t(B_i) \). A tree is defined as a partially ordered set (with relation \( \prec_t \)) such that

- Each block \( B_i \) has a unique maximal predecessor at time \( t \) (element \( B_{j_t(i)} \) s.t. \( B_{j_t(i)} \prec_t B_i \) and \( \not\exists B_{j'_t} \) s.t. \( B_{j'_t} \prec_t B_j \prec_t B_i \));
- \( j_t(i) = j_{t'}(i) \) for all \( t' > t \);
- There exists a minimal block \( B_0 \) such that \( B_0 \prec_t B_i \) for all \( t \), \( B_i \in B^t \).
For the remainder of the paper, we assume that the tree consists of only two chains $V$ and $I$, for “valid” and “invalid” (for reasons that will be clear later). A block in $B_i \in B^t$ on chain $j \in \{V, I\}$ has the property that for all $B'_i \in B'^t$ with $B_i$ on chain $j$, $B_i \prec_{t'} B'_i$.

Agents known as readers are responsible for “accepting” blocks. A Poisson process with arrival rate $\mu$ dictates the time at which readers accept a branch of the blockchain (called the “acceptance time”) and the game ends. If the acceptance time is $T$, readers accept a branch of the blockchain by choosing a terminal (maximal) block on the blockchain $B^T$ using a rule to be specified later. The accepted terminal block is denoted $B_{a(T)}$. The accepted chain consists of all blocks $B_j \prec_T B_{a(T)}$. Payoffs will be a function of the accepted chain of blocks.

There is a countable number of players known as writers. Writers search for blocks by exerting costly computational effort. Each writer owns a computer that generates $y$ units of computational power at cost $c(y)dt$ per unit time. For the remainder of the paper, we focus on the case

$$c(y) = \begin{cases} 
0 & y = 0 \\
c & y \in (0, 1] \\
+\infty & y > 1
\end{cases}$$

so in effect writers choose between spending resources $cdt$ for one unit of computing power or doing nothing to exert zero units of computational effort. Writers choose their computational effort $c \in \{0, c\}$ at time $t = 0$. This choice can alternatively be interpreted as an
entry decision. Given that blocks appear at rate $\eta$, each writer finds a block at rate $\eta M$ if $M$ writers enter at $t = 0$. At $t = 0$, writer $n$ must select a chain $m_n \in \{V,I\}$ on which to write. Once writer $n$ finds a block $B_k$ at time $t$, the block is appended to the tree on chain $m_n$. From now on, the time at which block $B$ is found will be denoted $t(B)$, and the block found at time $t$ will be $B(t)$. The writer who finds block $B$ is $m(B)$.

Writer $n$ also selects an action strategy $x_n \in [0,\bar{x}]$ at time $t = 0$. If the writer selects $x_n = 0$, any block $B_k$ found by $n$ is called a “valid” block. Otherwise, all blocks found by $n$ are called “invalid”. An action $x_n > 0$ is meant to represent transaction processing and verification activities that do not follow the blockchain’s baseline protocols. A larger $x$ denotes a greater deviation from those protocols. Let $b_{V,n}$, $b_{I,n}$ denote the number of blocks found by $n$ during the game on chains $V$ and $I$, respectively. Define $\varsigma_n = \{e_n, m_n, x_n\}$ to be the writer’s strategy, and let $\varsigma_{-n}$ denote the strategies of other writers. Then at time $T$, writer $n$ realizes a payoff of

$$v(\varsigma_n, \varsigma_{-n}) = 1\{B_{a(T)} \in V\} \phi b_{V,n} + 1\{B_{a(T)} \in I\} (\phi + x_n) b_{I,n}$$

That is, payoffs are awarded only on accepted blocks $B_i \prec_T B_{a(T)}$. The payoff depends implicitly on the actions of other writers through readers’ choice $B_{a(T)}$. For all valid blocks written, writer $n$ receives an exogenous writing fee $\phi$, and for each invalid block $B$ found, $n$ receives $\phi + x_n$, meaning a greater deviation from the blockchain’s rules yields a greater reward if the block is accepted. The structure of the game, including the timing and both types of chains, is illustrated in Figure 1.

The assumption that writers may only choose the valid or invalid chains is rooted in the details of the block verification procedure used in most blockchains. This assumption reflects the fact that writing computers are typically constructed to verify a pre-specified set of rules, but if an invalid block is detected, it is difficult to discern why a given block is invalid in the short period of time between blocks. In reality this process often takes hours, if not days. Therefore, there is no loss of generality in imposing that writers accept either all valid blocks or all invalid blocks.

With only two chains, the game turns into one in which seemingly honest writers compete against a coalition of writers trying to attack (or “fork”) the blockchain. It eliminates the need to specify a complicated acceptance rule for readers. Given that at any time, there is at most one fork of invalid blocks, readers’ decision reduces to whether to accept the valid chain or the invalid fork. Readers always accept the valid chain if it is longer than the invalid fork. We will assume that readers accept the invalid fork if it is longer than the valid chain with probability $1 - p(\hat{x})$, where

$$\hat{x} = \frac{1}{N_f} \sum_{m_n=I} x_n, \quad N_f \equiv |\{B : B \in I\}|$$

Here $N_f$ is the number of blocks in the invalid fork, so the probability that the invalid chain is accepted effectively depends only on the average action taken on the invalid fork. The probability function $p(\hat{x})$ is assumed to have the following properties (with $f \equiv -\log(1-p)$):
1. \( p(\bar{x}) = 1; \)

2. \( f'(x) = \frac{p'(\hat{x})}{1-p(\hat{x})} \) is positive and increasing in \( x \) for \( x \in [0, \bar{x}] \);

3. \( f''(\hat{x}) - f'(\hat{x})^2 \leq 0. \)

The first assumption states that when writers take the largest possible action, readers detect the deviation with certainty. The second implies that the larger the average action taken by writers, the greater the probability of detection. It also embeds a log-concavity assumption that will be necessary in order to derive conditions for optimal play. Intuitively, greater distortion by writers leads to a lower probability of acceptance, and there are decreasing returns to deviations from the protocol. The third assumption is needed only for technical reasons.

It is necessary to specify the entry decision of writers. Writers break even when following the protocol, so \( \frac{\phi}{c} = c \) in an equilibrium where writers play honestly, meaning \( M = \frac{n \phi}{c} \). Note that to ensure \( M \) is an integer, \( \phi \) must take values in a discrete set. Writers may also choose to sit out at time \( t = 0 \). When they do so, they receive no payoffs but also incur no costs.

Finally, we note that if computing power instead came from a market where writers were allowed to trade with each other, in any equilibrium a single writer would control all the computing power as long as there were no funding frictions. That is, if a single writer values a computer at price \( Q \) when \( M \) writers enter in equilibrium, that writer values \( M \) computers at a value greater than \( QM \). This is because when there are \( M \) writers, each receives fees in proportion to the power of a single computer. On the other hand, when one writer controls the blockchain with \( M \) computers, that writer receives the same fees but also obtains some monopolistic rents. Therefore, financial frictions are necessary for blockchain decentralization.

### 3.2 Equilibrium

In this section, we find the set of pure strategy symmetric equilibria. First, however, we must define a Nash equilibrium of this game.

Let \( s_n = (e_n, m_n, x_n) \) be writer \( n \)'s strategy, and denote the strategy of all writers other than \( n \) by \( s_{\neg n} \). The payoff function is

\[
    u(s_n, s_{\neg n}) = E \left[ 1\{N_I \geq N_V \} \left( (1 - p(\hat{x})) (\phi + x_n) b_{I,n} + p(\hat{x}) \phi b_{V,n} \right) + 1\{N_I < N_V \} \phi b_{V,n} \right]
\]

Equipped with this definition of the payoff function, we may define an equilibrium.

**Definition 1.** A Nash equilibrium of the game consists of strategies \( \{s_n\}_{n=1}^M = \{(e_n, m_n, x_n)\}_{n=1}^M \) such that for all \( n \),

\[
    u(s_n, s_{\neg n}) \geq u(s'_n, s_{\neg n})
\]
for all other strategies $s_n$ of player $n$.

Now we prove that in any equilibrium, all writers play blocks on the same chain. This result should not be interpreted as saying that forks are impossible—rather, it should be interpreted as stating that when writers have common knowledge of the possibility of an attack, either all writers attack or play honestly. Of course, forks do occur in reality, but they are in general agreed upon by a sub-community on a blockchain whose preferences are different from those of the majority (such as in the Ethereum hard fork described in Section 2). Furthermore, while it is certainly not the case that all writers on a given blockchain join any given attack, our model would interpret this fact as an issue of lack of common knowledge about the attack or heterogeneity in preferences among writers. For example, some writers may strictly prefer to play honestly.

Lemma 2. In any equilibrium where all writers choose the same action $x$, optimal play requires that all writing strategies be identical, $m_n = m_{n'} \forall n, n'$ such that $e_n = e_{n'} = c$.

All proofs are relegated to the Appendix. While it may at first seem surprising that there is no forking in equilibrium, the logic behind Lemma 2 is fairly simple. If a writer $n_1$ obtains a higher payoff than writer $n_2$, $n_2$ may mimic $n_1$’s strategy in order to obtain the same payoff as $n_1$ per block. By moving to the same chain as $n_1$, the number of writers on that chain becomes strictly larger and hence has a greater chance of being selected, so in fact under this deviation both $n_1$ and $n_2$ are strictly better off.

Here we will be primarily interested in equilibria where all players choose the same action $x$, which will henceforth be referred to as symmetric equilibria. Lemma 2 shows that all such equilibria can be described by a pair of actions $(m, x) \in \{V, I\} \times [0, \bar{x}]$. If $m = V$, then the choice of $x$ is irrelevant. On the other hand, if $m = I$, $x$ is pinned down by an optimization problem:

$$\max_x E \left[ \left( 1 - p \left( \frac{k - n}{k} x^* + \frac{n}{k} x \right) \right) \left( \phi + x \right) n \right]$$

where $k$ is the total number of blocks found, $n$ is the number of blocks found by one particular writer, and $x^*$ is the action taken by writers in equilibrium. The first-order condition is

$$\phi + x^* = \frac{E[n](1 - p(x^*))}{E[n] + p'(x^*)} = \frac{E[n]}{E[n] f'(x^*)}$$

After computing the expectations, this equation becomes

$$1 = \frac{f'(x^*)}{\kappa(M)} (\phi + x^*)$$

(2)

where $\frac{1}{\kappa(M)} = \frac{1}{M} + \frac{M-1}{M} E[k]^{-1}$ and $E[k] = \frac{n}{\mu}$. Given that $f$ is convex, this equation clearly has a unique solution $x^*$. Note that as $M$ increases, $\kappa(M)$ ranges from 1 to $E[k]$. 

13
Equation (2) can be seen as a formula equating the marginal benefit of distorting the ledger to the marginal cost. The marginal benefit of incrementing $x$ by one unit is 1. The cost of incrementing $x^*$ by one unit is equal to the payoff $\phi + x^*$ times the hazard rate $f'(x^*)$, since this is just the change in the probability that writers on the invalid chain will lose their payoffs multiplied by the payoff itself. The function $\kappa(M)$ is a measure of how much each individual writer’s action affects the probability that the invalid chain of blocks will be accepted. Thus the payoff loss perceived by an agent who increments $x^*$ by one unit is just the loss that occurs when $x^*$ is incremented by one unit divided by $\kappa(M)$. When $M$ is large, each writer perceives her actions to have a lower influence on this probability, so writers on the invalid chain tend to steal large quantities when they are numerous.

The first-order condition (2) works entirely through static incentives. When writers attempt to steal, they consider only the possibility that their current gains will be nullified—as the game is static and occurs during a single period, they have no franchise value to lose. Their payoffs are affected not only by their own choices to distort the ledger, but also others’ choices. We will show that just as several firms in competition tend to produce more than what is optimal for a monopolist, several competing writers on the invalid chain will distort the ledger more than what is optimal in aggregate. This force will prevent ledger distortion by making it unprofitable when several writers are present.

The key question to determine the cost of intermediation via blockchain is at what point writing on the invalid chain becomes unprofitable. That is, when the optimal action $x^*$ is sufficiently high, writers will be strictly better off by sitting out or writing on the valid chain, so there will not exist an equilibrium in which writers play on the invalid chain. Fortunately, a simple and intuitive result provides an upper bound on the required number of writers.

**Proposition 3.** Let $\tilde{\phi} = f'(0)^{-1}$, $\tilde{M} = \frac{\tilde{\phi}}{c}$. For all sufficiently large $M \leq \tilde{M}$, there is no symmetric equilibrium in which $m = I$.

This result shows that for $M$ sufficiently large, writers will always play on the valid chain. The writing fee just has to be large enough that a monopolistic writer would always choose $x = 0$, meaning that the highest possible profits are just those that would be obtained by honest writing. In this case, any attack on the blockchain will be unprofitable in expectation.

Note that this result does not imply that a blockchain is always less costly than a monopolistic intermediary. In this proposition, we consider a monopolistic writer with no franchise value to lose, so the writer has static but not dynamic incentives to cheat. When the writer has dynamic incentives as well, it is possible for monopolistic intermediation to be cheaper, as shown in the next section.

We now summarize the steps involved in securing the network through the addition of writers:

1. Each writer fails to internalize the effect his action has on others’ profits;
2. Writers steal more than what is optimal in aggregate;

3. The probability that readers reject the ledger increases;

4. Expected revenues on the invalid chain become lower than what writers need to break even;

5. Writers switch to the valid chain.

When writers fail to discipline each other by refusing to extend invalid chains, readers must discipline the writers. Readers are especially good at providing incentives when writers distort the ledger extensively, which is exactly what happens when there are many writers.

Figure 2 illustrates the mechanics behind the process described above. Aggregate revenues are much more sensitive to the distortion $x$ than individual revenues, since an individual perceives an influence on the aggregate action of only $\kappa(M)^{-1}$ in expectation. Thus individuals steal more than what is optimal. In the case depicted in figure 2, in fact, individual writers distort the ledger so much that it would be more profitable to play on the valid chain.
3.3 The monopolistic intermediation model

In this subsection, we present a benchmark model of intermediation by a monopolist who privately maintains a ledger and trades off the benefits of stealing with the costs of reputation loss. The ultimate question will be whether it is cheaper to prevent stealing using the franchise value of the intermediary or a the competition among writers that makes attacks unprofitable.

A monopolistic intermediary plays a repeated game with readers. Time is discrete, $t = 0, 1, \ldots$ and the monopolist discounts payoffs with discount factor $\delta$. In each period, the monopolist chooses an action $x \leq \bar{x}$ determining how much to distort the ledger it maintains. Payoffs within a given period are $\phi + x$, where $\phi$ is a fee earned by the intermediary. With probability $p(x)$, readers are informed that the intermediary stole from their accounts. Conditional on receiving this signal, readers collectively decide to stop doing business with the intermediary with probability $1 - q$ and forgive the intermediary with probability $q$.

The intermediary’s problem is then

$$\max_{x \leq \bar{x}} (\phi + x) + \delta(1 - p(x)(1 - q))(\phi + x) + \cdots = \max_{x \leq \bar{x}} \frac{\phi + x}{1 - \delta(1 - p(x)(1 - q))}$$

Under the assumptions made about the function $p$, this objective function is convex, so the intermediary chooses either $x = 0$ or $x = \bar{x}$ (as shown by the following lemma).

**Lemma 4.** The intermediary chooses either $x = 0$ or $x = \bar{x}$ in every period.

Given that the monopolist chooses either $x = 0$ or $x = \bar{x}$, it is easy to find the fee that prevents stealing altogether. The fee required by the intermediary is

$$\bar{\phi} = \frac{1 - \delta}{1 - \delta q} (\phi + \bar{x}) \Rightarrow \bar{\phi} = \frac{1 - \delta}{\delta(1 - q)} \bar{x}$$

This lemma is illustrated in Figure 3. When the fee earned by the intermediary is low, it is more profitable for the intermediary to play $x = \bar{x}$. However, when the fee is high, the intermediary plays $x = 0$. With a high fee, the intermediary puts a greater franchise value at risk when distorting the ledger, so it is less desirable to do so.

3.4 Cost-efficient intermediation

Now we are ready to compare the costs of intermediation by a monopolist and by a blockchain. For the remainder of this subsection, assume $p(x)$ is linear, i.e. $p(x) = \pi x$. Note that this implies $f(x) = -\log(1 - \pi x)$, $f'(x) = (\frac{1}{\pi} - x)^{-1}$, and $\bar{x} = \pi^{-1}$. Let $\bar{\phi}$ be the fee required to prevent stealing by the monopolist derived in the previous subsection, and define $\bar{M} = \frac{\bar{\phi}}{\bar{x}}$. Then any fee $\phi$ corresponding to a situation with $M$ writers can be written as $\phi = \frac{\bar{M}}{\bar{\phi}}$. 16
It follows from equation (2) that in any static equilibrium of the blockchain game where writers choose to play on the invalid chain, we must have

\[ x^*(M) = \frac{\kappa(M)}{1 + \kappa(M)} \pi - \frac{1}{1 + \kappa(M)} \frac{M - \phi}{M} \]  

(3)

Writers’ profits per block are then

\[ u_I(M) = \frac{\kappa(M)}{1 + \kappa(M)} \left( \pi^1 - \kappa(M)^{-1} \frac{M - \phi}{M} + (1 + \kappa(M)^{-1}) \frac{M - \phi}{M} \right) \left( 1 - \frac{\kappa(M)}{1 + \kappa(M)} - \frac{1}{1 + \kappa(M)} \frac{M - \phi}{M} \right) \]

\[ = \frac{\kappa(M)^{-1}}{(1 + \kappa(M)^{-1})^2} \pi^1 \left( 1 + \frac{1 - \delta}{\delta(1 - q)} \frac{M}{M} \right)^2 \]

On the other hand, the profits earned per block by honest writers are

\[ u_V(M) = \frac{1 - \delta}{\delta(1 - q)} \pi^{-1} \]

Let \( \omega = \frac{1 - \delta}{\delta(1 - q)} \). Then \( u_I(M) < u_V(M) \) if and only if

\[ \frac{\kappa(M)^{-1}}{(1 + \kappa(M)^{-1})^2} \frac{M - \omega}{M} < \frac{M - \omega}{(1 + \frac{M - \omega}{M})^2} \]
Restricting attention to the region of $M$ small enough that $\frac{\omega M}{M} \leq 1$, this inequality is equivalent to

$$\kappa(M)^{-1} < \frac{M}{M} \omega \quad (4)$$

If $\kappa(M)^{-1} < \omega$, there will always be a range of sufficiently large $M$ in which this inequality holds. Intermediation by blockchain is therefore cheaper than intermediation by a monopolist whenever $\kappa(M)\omega > 1$.

The intuition behind this result is (roughly) that $\kappa(M)^{-1}$ and $\omega^{-1}$ correspond to the sensitivities of payoffs to stealing perceived by writers and by a monopolist, respectively. When writers perceive a small sensitivity to stealing, they tend to steal in large amounts and collectively make stealing unprofitable. On the other hand, when a monopolist perceives a small sensitivity of payoffs to stealing, it is expensive to incentivize the monopolist because the monopolist earns high expected profits by stealing $\pi$ in every period.

This result also yields a formula for the optimal number of writers, which under the approximation $\kappa(M) \approx E[k]$ is

$$M_{opt} = \frac{\eta}{\pi c} \quad (5)$$

This extremely simple formula shows that the optimal number of writers is inversely proportional to the cost of writing and the readers’ sensitivity to theft $\pi$. When readers are sensitive to theft, the number of writers required to collectively destroy the profits of dishonest writing is low, since even the slightest increase in the amount stolen leads to a large jump in the probability that the transactions on the invalid chain will remain unrealized.

### 4 Ownership and possession in blockchains

Blockchains may also be useful in situations where a ledger is needed to keep track of the ownership of certificates that give the owner the right to possess something. For example, the deed to a house gives the owner the right to reside in that house, the title to a vehicle gives the owner the exclusive right to drive that vehicle, and a debt contract gives the owner possession of cash at some future date. While blockchain can confer ownership of contracts or certificates, nothing about blockchain guarantees that the issuer of a certificate will not default on her promise to deliver an asset. In this section, we show that this situation can be captured by a static game similar to the one considered above. The main result will be that blockchains may be helpful in situations where issuers wish to default on promises only when they are able to collude with the intermediary.

In this section, we examine two cases: one in which the blockchain writers face a monopolistic “enforcer” who may selectively choose not to enforce contracts, and another in which a mass of agents who may default on promises issue contracts on a blockchain.
4.1 Blockchain with government enforcement

We first consider a situation in which there is a government that may selectively enforce possession rights corresponding to certificates traded on a blockchain. There is a continuum of contracts $j \in [0,1]$ that the government may choose to enforce. The government may also bribe writers in order to interfere with the ledger and cover up its selective enforcement. In particular, at time $t = 0$ the government chooses a quantity $y \in [0,1]$ of contracts to enforce before writers play. Writers take an action $x \in [0,1]$ after observing $y$ corresponding to the number of contracts with which the writer interferes. The blockchain setup is as before: writer $n$ chooses to play on chain $m_n \in \{V,I\}$ at $t = 0$ and obtains payoffs from taking an invalid action only if $m_n = I$. The payoff for finding a block on the valid chain is always $\phi$ if the chain is accepted. On the other hand, the payoff for finding a block on the invalid chain is $\phi + \tau \min\{x,y\}$ when the invalid chain is accepted. That is, for each block found on the invalid chain, a writer is awarded transaction fees $\phi$ plus a bribe $\tau$ for interfering with any given contract (up to the number of contracts the government selects).

In this game, the valid chain is selected whenever it is longer than the invalid chain, and when the invalid chain is as long as the valid chain it is selected with probability $1 - p(\tau \hat{x})$, where again $\hat{x}$ denotes the average action taken by writers on that chain. The probability an attack will succeed is thus a function of the amount writers take in bribes. The government receives payoffs $U(0, y)$ when the valid chain is selected and $U(\hat{x}, y)$ when the invalid chain is selected. The function $U$ is assumed to be increasing in both its arguments.

This game can be solved by backwards induction. It should be clear that as before, in any symmetric equilibrium all writers must play on the same chain. The equilibrium in which all writers play on the valid chain is trivial, as the action $x_n$ taken by each $n$ is irrelevant. We thus analyze the equilibrium in which writers play on the invalid chain. Writers never optimally play $x > y$, since they do not receive additional bribes for increasing $x$ above $y$ and they strictly decrease the probability that the invalid chain will be accepted. Given $y$, writers solve

$$\max_{x \leq y} E\left[ (\phi + \tau x) \left( 1 - p(\tau (\frac{k-n}{k} x^* + \frac{n}{k} x)) \right) n \right]$$

The first-order condition in a symmetric equilibrium is

$$\phi + \tau x^* = \frac{\kappa(M)}{f'(\tau x^*)}$$

so writers play $\hat{x}(y) = \max\{x^*, y\}$ only if

$$(\phi + \tau \max\{x^*, y\})(1 - p(\tau \max\{x^*, y\})) \geq \phi$$

Otherwise, they must play on the valid chain, since playing on the invalid chain is unprofitable. Hence

$$\hat{x}(y) = \begin{cases} \max\{x^*(M), y\} & \text{if } \max\{x^*(M), y\} \leq \hat{x} \\ 0 & \text{if } \max\{x^*(M), y\} > \hat{x} \end{cases}$$
where $\tilde{x}$ satisfies $(\phi + \tau \tilde{x})(1 - p(\tau \tilde{x})) = \phi$.

Given writers’ optimal play, the government understands that writers will take action $\hat{x}(y)$ if it decides to play $y$. The government solves

$$\max_y U(\hat{x}(y), y)$$

Given that $\hat{x}(y) \leq y$, the government can always play $y$ small enough that $\hat{x}(y) < \tilde{x}$, so no matter what the number of writers, it is always possible for the government to arrange transfers to writers so that they distort the ledger. Furthermore, even when the writers do not distort the ledger, the government can always choose not to enforce some contracts. That is, at an optimum

$$\max_y U(\hat{x}, y) \geq \max_y U(0, y)$$

The reason that the network is insecure even with a large number of writers is that although the writers do not internalize their effects on aggregate profits and are always tempted to distort beyond the optimal amount, the government internalizes this force when choosing $y$. By choosing a small $y$, the government can cap the amount writers will distort the ledger, since they never do anything beyond what they are bribed to do. Thus blockchain is ineffective at dealing with a monopolistic enforcer of possession rights, and issues with enforcing possession may spill over to the integrity of ownership.

4.2 Blockchain with defaultable contracts

We now consider an environment in which defaultable contracts are traded on a blockchain. There is a unit mass $[0,1]$ of “issuers” who issue tradable certificates that promise delivery of a physical object. Issuers decide whether to default on their promises by taking an action $D \in \{0,1\}$, where $D = 1$ denotes default. These decisions are made at acceptance time $t = 0$ before writers decide on strategies. Let $D_i$ denote the decision of each issuer and let

$$D = \int_0^1 D_i di$$

be the measure of issuers who default.

Writers may take actions $x_n(i) \in \{0,1\}$, where $x_n(i) = 1$ represents a situation in which writer $n$ colludes with issuer $i$ in her efforts to default. Writers also choose $S_n(i) \in \{0,1\}$, that determine whether they provide service to issuer $i$. When $S_n(i) = 1$, the writer does not receive the transaction fee $\phi$ associated to the circulation of that issuer’s certificates. Let

$$S(B) = \int_0^1 S_{m(B)}(i) di$$
denote the measure of issuers who are provided service in block $B$. Writers receive a “bribe” $	au > 0$ from each issuer $i$ such that $x_n(i) = 1$ and $S_n(i) = 1$. A block found by $m$ at time $t$ appears to be invalid to all other writers if $x_n(i) = 1$ for any $i$, and all such blocks go on the invalid chain. Denote the average action $x$ taken in a block $B$ by

$$x(B) = \frac{1}{S(B)} \int_0^1 S_n(i)x_m(B)(i)di$$

Just as in the previous section, block rewards are realized on the invalid chain with probability $1 - p(\tau \hat{x})$ if the invalid chain is as long as the valid chain, where $\hat{x}$ is the average of $x(B)$ on the invalid chain. The probability of acceptance is again a function of the quantity of bribes the writers take.

Writers’ rewards are determined by their decisions to provide service and issuers’ default decisions. The reward a writer receives from a single block is

$$z(x_n(i), S_n(i), D_i) = \int_0^1 S_n(i)(\gamma(D_i)x_n(i) - 1\{x_n(i) = 1\})\tau di$$

where $\gamma(D) = D(\gamma - 1) + 1$ and $\gamma \in [0, 1]$. That is, when the issuer defaults, the fees received by the writer are reduced by a factor of $\gamma$. This assumption reflects the fact that widespread default by issuers on a blockchain may reduce the transaction fees that other users of the blockchain are willing to pay. The writer does not receive a bribe if the issuer does not default.

When a block found by writer $n$ is accepted, issuer $i$ realizes a payoff of

$$W_{n,i}(x_n(i), S_n(i), D_i) = S_n(i)(w_{D_i,x_n(i)} - 1\{x_n(i) = 1\})\tau$$

Note that $w_{D_i,x_n(i)}$ may take only four values: $w_{ij}$ for $i,j \in \{0,1\}$. Assume that $w_{11} - \tau \geq \max\{w_{10}, w_{00}\}$, so that the writer’s cooperation is desirable when the issuer defaults, and $w_{00} = w_{01}$, so that conditional on no default the issuer is indifferent to the writer’s decision. When $w_{10} > w_{00}$, default is a dominant action for issuers, so they always default in the static game. When $w_{00} > w_{10}$, issuers need to be assured of writers’ cooperation before defaulting.

Writers enter if it would be profitable to do so when all writers play valid blocks without denying service and issuers respond optimally. If $w_{00} \geq w_{10}$, this implies $M = \frac{\eta \phi}{c}$, and if $w_{00} < w_{10}$, we obtain $M = \frac{\eta \gamma \phi}{c}$.

This game can be solved by backwards induction. We first take the default decisions $D_i$ as given and determine writers’ optimal strategies. Note that it is never strictly optimal to deny service in the static game, since the writer’s payoff when providing service is never negative, whereas a writer who denies service receives a payoff of zero from that particular issuer’s transactions. Writers also never select $x_n(i) = 1$ when $D_i = 0$, since they do not
receive a bribe and that action strictly reduces the probability that the block is accepted. As before, writers solve an optimization problem:

\[
\max_{x \leq D} E \left[ (\gamma(D) \phi + \tau x) \left( 1 - p\left( \frac{k-n}{k} x^* + \frac{n}{k} x \right) \right) \right] n
\]

This is essentially the same problem faced by writers in the case without primary markets. In a symmetric equilibrium, the first-order condition is

\[
\gamma(D) \phi + \tau x^* = \frac{\kappa(M)}{f'(\tau x^*)}
\]

so this problem is isomorphic to the one without primary markets under the substitutions \(\phi \to \gamma(D) \phi, x^* \to \tau x^*\). Writers can never choose \(x > D\), so the action taken in a symmetric equilibrium is \(x_{eq} = \max\{\min\{x^*, D\}, 0\}\).

To determine issuers’ decisions, there are two cases to consider. First, if \(w_{00} < w_{10}\), it is clear that all issuers will play \(D = 1\) regardless of writers’ strategies. On the other hand, if \(w_{00} \geq w_{10}\), issuers default only if they expect that when they do so, writers will accept their bribes. Thus \(D \leq x^*\). However, if \(x^* > D\), it must be that writers will cooperate with each additional issuer who defaults, so given that \(w_{11} - \tau \geq w_{00}\), it cannot be that issuers are playing optimally. Therefore, \(x^* = D\) in any equilibrium when \(w_{00} \geq w_{10}\). This leads to the equation

\[
\gamma(x^*) \phi + \tau x^* = \frac{\kappa}{f'(\tau x^*)} \tag{6}
\]

In particular, if \(\gamma(x^*) = 1\), this is exactly the same model as the one without transfers of possession, and the same analysis of blockchain’s costs goes through.

This equivalence justifies our abstraction from the issue of possession in the previous sections. One example of a market in which issuers would require intermediaries’ assistance in order to default is the IPO market. A firm that wishes to issue fake shares in order to steal from investors would need to bribe the exchange to tell investors those shares are real. Another example is the market for paintings: the auction house would have to tell its clients that according to the transaction history it received, the painting that is for sale is the genuine article. Finally, a seller of a house who is liable for unpaid property taxes would have to bribe the title insurer to report all taxes as paid to the buyer.

In order to understand whether intermediation via blockchain can be dominant when default is a dominant action for issuers, it will be necessary to work in a dynamic setting. As noted previously, in a static setting issuers will always default. The question should be whether writers on a blockchain can provide incentives that will deter default through their ability to deny service to issuers in a repeated game.

### 4.3 The Dynamic Blockchain Game

Consider a setting in which the game presented in the last section is infinitely repeated. Each iteration of the static game occurs within a period called a “day.” Each day is denoted
by some $T \in \{0, 1, 2, \ldots \}$. Writers discount payoffs at rate $\delta$, and (when applicable) issuers discount payoffs at rate $\rho$. Histories of the game are defined recursively by $H_0 = \emptyset$, $H_t = H_{t-1} \times S^N \times S^I_1$, where $S$ and $S^I$ are the sets of pure strategies in the stage game for writers and issuers, respectively. The strategies we consider for writers at stage $t$ of the repeated game are functions $\sigma_t : H_t \rightarrow ([0, 1] \times \{V, I\} \times [0, 1]^{[0,1]})^N$. Writers may mix their entry decisions, but they play pure strategies for their mining and action decisions. Similarly, strategies for issuers are functions $\sigma^I_t : H_t \rightarrow \{0, 1\}^{[0,1]}$; that is, issuers just decide whether to default or not. Subgame-perfect Nash equilibria are defined in the usual way. To avoid unnecessary numerical complications, we focus on equilibria satisfying an exact free entry condition:

$$\pi(\sigma_{n,t}, \sigma_{-n,t}) = 0$$

for all $n$ and $t$. Without this condition, our main results go through with some qualifications relating to integer issues resulting from entry decisions. As long as the cost of entry is small, these integer issues should be mostly irrelevant.

Having observed that the free entry condition implies payoffs are equal to zero period-by-period, the main result of this section is almost immediate. The next proposition shows that writers play a static equilibrium in every period of any SPE.

**Proposition 5.** Let $\{\sigma_n\}_{n \in \mathbb{N}}, \{\sigma^I_i\}_{i \in [0,1]}$ be a SPE satisfying the exact free entry condition. Then in every period $t$,

$$\pi(\sigma_{n,t}, \sigma_{-n,t}) = \max_{\sigma'_{n,t}} \pi(\sigma'_{n,t}, \sigma_{-n,t})$$

The intuition behind this result is straightforward. If the free entry condition holds, writers’ continuation payoffs are equal to zero no matter what strategy they play in the current period. They cannot be rewarded or punished for selecting any particular strategy. Therefore, all writers play a static response to other agents’ strategies in every period.

Proposition 5 implies that even in a dynamic setting, writers may never deny service to issuers who default. When default is a dominant action, then, issuers will always default, since they know that writers cannot credibly threaten to punish them in the future. An anonymous blockchain with free entry is thus ineffective in situations where the intermediary plays an important role in disciplining issuers. An example of this type of market is a consumer debt market. Centralized intermediaries such as banks will restrict access to assets and borrowing opportunities when a consumer defaults on a mortgage. If this action is costly for the intermediary, writers on a blockchain can never commit to disciplining borrowers the same way a bank would, since the bank must maintain its reputation.

To illustrate this point, we explicitly outline an example where a monopolistic intermediary can commit to discipline issuers by denying service. For now, assume that the intermediary must play $x(i) = 0$ (for example, by assuming $\tau = 0$). We look for an equilibrium where
1. All issuers play $D = 0$ on the equilibrium path;

2. After a history at which issuer $i$ deviates, the intermediary denies service to $i$ for one period and the issuer plays $D = 1$;

3. If the intermediary deviates and fails to deny service to some issuer who played $i = 1$ in the previous period, all agents play static Nash for the remainder of the game.

All we need to do is check the incentive compatibility constraints in stages (1) and (2). In stage 1, issuers prefer not to deviate if

$$w_{10} + \frac{\rho^2}{1-\rho} w_{00} \leq \frac{1}{1-\rho} w_{00}$$

When the intermediary must deny service to $S$ issuers, its incentive compatibility constraint is

$$\gamma \phi (1 - S) \leq \frac{\delta}{1 - \delta} (1 - \gamma) \phi$$

because by providing service to the $S$ issuers to whom it is supposed to deny service, the intermediary obtains $\gamma \phi (1 - S)$ immediately, whereas it loses $\frac{\delta}{1 - \delta} (1 - \gamma) \phi$ in the long run given that all issuers default in every subsequent period. This implies

$$1 - S \leq \frac{1 - \gamma}{\gamma} \frac{\delta}{1 - \delta}$$

so it is in fact possible for a monopolistic intermediary to deny service to a positive mass of issuers, unlike in the case with a blockchain.

## 5 Conclusion

We show that with sufficiently many writers, a blockchain will always generate a consensus about the true history. Free entry renders any dynamic reward or punishment scheme (like the ones used to incentivize centralized entities) entirely useless on a blockchain. Hence, our argument relies on a novel mechanism: the disciplining of writers through static incentives. When writers do not discipline each other, competitive forces lead them to distort the ledger so much that readers almost certainly discover their misbehavior and abandon the ledger, rendering the fraud unprofitable. In markets where centralized intermediaries have weak dynamic incentives, this static competitive incentive is a more efficient way of securing the ledger. A leading example of an intermediary with weak dynamic incentives is a too-big-to-fail institution. Given that readers of the ledger cannot easily commit to punish a TBTF institution, large rents are required to ensure truthful reporting.

We highlight the important distinction between ownership and possession. Blockchains can only effect transfers of ownership, but the discipline imposed by the security of ownership on a blockchain can also prevent bad actors from defaulting on delivery of possession.
When sellers of counterfeit promises require an intermediary’s assistance in order to defraud buyers, intermediation by blockchain endogenously leads to integrity of possession as well as ownership. This aspect of blockchains is useful in securities markets, for example, since sellers of fake securities would require an exchange’s help to deceive buyers.

However, it is not always the case that a blockchain will lead to enforcement of possession rights. When a corrupt government has the ultimate power to selectively enforce contracts, a blockchain with many writers is as insecure as one with a single writer. The government can always implement its optimal outcome by arranging the correct transfers to writers. This finding is particularly relevant to weighing the usefulness of blockchain in providing ownership data for developing countries, especially in light of the popular claim that ownership data will be critical in addressing poverty in such countries. Furthermore, blockchains are inferior to monopolistic intermediation when intermediaries play an important role in disciplining their clients. Dynamic reward schemes are irrelevant to writers, so they will never take a costly disciplinary action in order to reap higher profits in the future. This feature of blockchain intermediation is important in debt markets, where punishment via exclusion from credit markets is often necessary to incentivize borrowers.

In this paper, we have outlined the mechanics securing 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.
Appendix

Proof of Lemma 2:

Proof. Suppose that in equilibrium, there exist two writers \( n, n' \) with \( e_n = e_{n'} = c \) such that \( m_n = V \) and \( m_{n'} = I \). Assume first that \( u(s_n, s_{-n}) \geq u(s_{n'}, s_{-n'}) \). Then if we set \( \tilde{s}_{n'} = (e_{n'}, V, x_{n'}) \) and let \( M_j(s) = \sum_{e_n = c} 1\{m_n = j\} \) for \( j \in \{V, I\} \) and an arbitrary strategy profile \( s \), we have

\[
\begin{align*}
    u(\tilde{s}_{n'}, s_{-n'}) &= E \left[ 1\{N_I \geq N_V\} \phi_{b, V, n} + 1\{N_I < N_V\} \phi_{b, V, n} | M_V(\tilde{s}) \right] \\
    &> E \left[ 1\{N_I \geq N_V\} \phi_{b, V, n} + 1\{N_I < N_V\} \phi_{b, V, n} | M_V(s) \right] \\
    &= u(\tilde{s}_{n'}, s_{-n'}) \\
    &\geq u(s_{n'}, s_{-n'})
\end{align*}
\]

The inequality on the second line holds because \( M_V(\tilde{s}) > M_V(s) \), where \( \tilde{s} = (\tilde{s}_{n'}, s_{-n'}) \). The inequality on the last line holds by assumption. Hence there is no such equilibrium. The logic in the case \( u(s_n, s_{-n}) < u(s_{n'}, s_{-n'}) \) is analogous. \( \square \)

Proof of Proposition 3:

Proof. Note that for any \( M > 1 \), \( x^*(M) > 0 \) when the writing fee is \( \bar{\phi} \). Aggregate expected profits earned by writers are then

\[
M(\bar{\phi} + x^*(M))(1 - p(x^*(M)))E[n] = (\bar{\phi} + x^*(M))(1 - p(x^*(M)))E[k]
\]

Consider the following maximization problem:

\[
\max_x E[(\bar{\phi} + x)(1 - p(x))k]
\]

This is the problem faced by a writer in the case \( M = 1 \). The solution satisfies

\[
\bar{\phi} + x^*(1) = f'(x^*(1))^{-1}
\]

Clearly, given the assumption that \( \bar{\phi} = f''(0)^{-1} \), the unique solution to this equation is \( x^*(1) = 0 \). But then, noting that the highest possible profits in this problem are \( \bar{\phi}E[k] \) and comparing this expression to the aggregate expected profits of writers above, we obtain

\[
\bar{\phi}E[k] > (\bar{\phi} + x^*(M))(1 - p(x^*(M)))E[k] \iff \bar{\phi} > (\bar{\phi} + x^*(M))(1 - p(x^*(M)))
\]

An individual writer’s cost of entering is \( \frac{1}{\bar{\phi}} E[k] \), so writers prefer to sit out rather than play on the invalid chain when \( M = \bar{M} \). Given continuity of \( f \), it must be that for all \( M \) sufficiently close to \( \bar{M} \), this is also the case. \( \square \)
Proof of Lemma 4:

Proof. The second derivative of the objective function in terms of \( f(x) = -\log(p(x)) \) is proportional to \( f''(x) - f'(x)^2 \), which is negative by assumption. Therefore, the objective function is convex, so the optimum must be a corner solution.

Proof of Proposition 5:

Proof. Suppose that for some \( n, t \) at some history \( h_t \in H_t \), \( \pi(\sigma_{n,t}, \sigma_{-n,t}) < \pi(\sigma'_{n,t}, \sigma_{-n,t}) \) for some alternative strategy \( \sigma'_{n,t} \). Then \( \pi(\sigma'_{n,t}, \sigma_{-n,t}) > 0 \), violating the condition of exact free entry.

References


