Corporate Capture of Blockchain Governance*

Daniel Ferreira

London School of Economics, CEPR and ECGI

Jin Li

Hong Kong University, CEP

Radoslawa Nikolowa

Queen Mary University of London

May 2021

Abstract

We develop a theory of blockchain governance. In our model, the *proof-of-work system*, which is the most common set of rules for validating transactions in blockchains, creates an industrial ecosystem with specialized suppliers of goods and services. We analyze the interactions between blockchain governance and the market structure of the industries in the blockchain ecosystem. We show that the proof-of-work system may lead to a situation where some large firms in the blockchain industrial ecosystem – *blockchain conglomerates* – capture the governance of the blockchain.

Keywords: Governance, Blockchain Conglomerates, Industrial Ecosystem, Proof-of-Work

*We thank Benito Arruñada (discussant), Ulf Axelson, Will Cong, Giulio Fella, Jungsuk Han (discussant), Peter Kondor, Igor Makarov, Barry Nalebuff (discussant), Fahad Saleh (discussant), Jason Sturgess, Enrique Schroth (discussant), Kostas Zachariadis, and seminar participants at Carlos III, Bocconi, Bristol, U. of British Columbia, Corporate Finance Webinar, ESSEC, Frankfurt Goethe, U. of Illinois at Urbana-Champaign, LSE, Paris School of Economics, QMUL, SBFin webinar, Toulouse School of Economics, Vienna GSF, and conference participants at the AFA meetings (San Diego), Barcelona GSE Summer Forum, Bergen Fintech conference, EARIE (Barcelona), EFA (Lisbon), GSU-RFS FinTech Conference (Atlanta), Lubrafin meeting (Olhão), the Olin Business School Corporate Finance conference (early ideas), and SIOE (Stockholm) for comments and suggestions, and Bo Tang for research assistance.

1. Introduction

"*The greatest challenge that new blockchains must solve isn't speed or scaling – it's governance.*"[1]

All blockchains have rules that govern their operations. Blockchain stakeholders' views about the adequacy of the existing rules may change over time. Blockchains thus need a governance system for deciding how to change their rules. Similar to most political and corporate governance systems, blockchain governance typically relies on a combination of "voice" (i.e., voting) and "exit" (i.e., ceasing to use the blockchain). Some of the largest blockchains (such as Bitcoin) adopt a voice mechanism that assigns more "votes" to those stakeholders with more computational power. Such a system is called *proof-of-work.*[2] Exiting is also a governance mechanism. If some stakeholders such as users, merchants, or exchanges disagree with the majority of miners, these stakeholders may stop using the blockchain. In that case, the price of the coin may fall because of lower demand.

When designing a governance system, blockchains face a similar problem as corporations do: how to avoid capture by interest groups. In this paper, we develop a theory of governance in proof-of-work blockchains.[3] Our main result is that the proof-of-work system may lead to a situation where some large firms in the blockchain industrial ecosystem – *blockchain conglomerates* – capture the governance of the blockchain. We show that governance capture occurs even in the presence of alternative exit and voice governance mechanisms, such as market monitoring, stakeholder monitoring, and reputation building.

A blockchain is a system for electronic transactions, which are stored in blocks. Blockchains need rules to decide how to create new blocks. Such rules are called the *consensus mechanism*, which is part of the overall blockchain protocol. In the proof-of-work system, players, called *miners*, enter a competition where a single winner is allowed to add a block to the chain. To win, a miner must solve a mathematical puzzle that requires significant computational power. The probability that a miner is the first to find a solution is proportional to

[1] Kai Sedgwick, "Why Governance is the Greatest Problem for Blockchains to Solve," July 15, 2018, https://news.bitcoin.com/why-governance-is-the-greatest-problem-that-blockchains-must-solve/

[2] According to Nakamoto (2008), "*[proof-of-work] solves the problem of determining representation in majority decision making. (...) Proof-of-work is essentially one-CPU-one-vote*".

[3] Our focus is on permissionless blockchains (i.e., anyone can join the blockchain in any role). For a discussion of permissioned blockchains or public blockchains with permissioned record-keepers, see, e.g., Chod and Lyandres (2020) and Cong, Li, and Wang (2021).

the amount of computational power they allocate to the process of mining a block.

If there are two conflicting versions of the blockchain, miners "vote" for their preferred version by allocating their computational power to one of the chains. Typically, the chain with more computational power is likely to win; the losing chain is either abandoned or rebranded as a separate blockchain. Thus, the proof-of-work protocol is both a consensus mechanism and a "governance through voice" mechanism.[4]

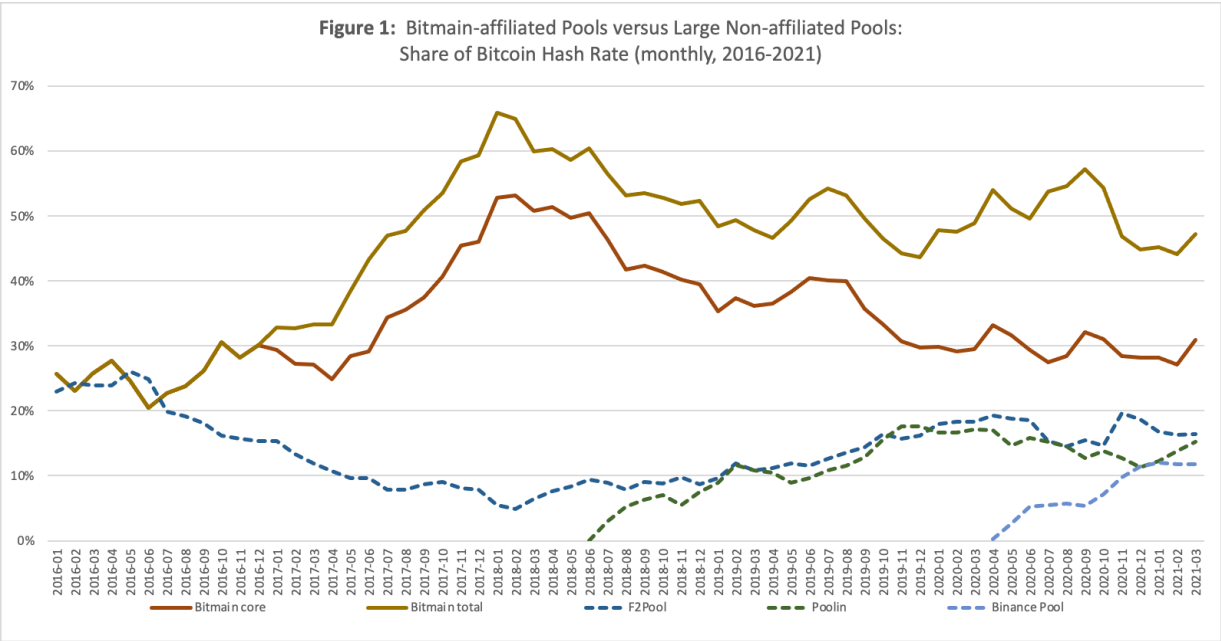
The emergence of mining as an economic activity has led to the development of an ecosystem of industries that supply goods and services to miners. Most mining is performed by specialized equipment that uses *application-specific integrated circuits* (ASIC), which are chips designed to perform a single function: block mining. In addition to specialized equipment, miners also buy mining services from *mining pools*, which are companies that sell insurance to miners. *Blockchain conglomerates* are firms that operate in multiple businesses of a blockchain industrial ecosystem. Our model shows how blockchain conglomerates – firms that produce equipment and manage mining pools – endogenously emerge.

We show that blockchain conglomerates have both the incentives and the means to capture the governance of blockchains. Blockchain conglomerates have an economic interest in pushing for rules and protocols that increase demand for their products and raise their profitability. Blockchain conglomerates can influence votes because their mining pools act as proxies for their miners. We show that firms that produce equipment have an advantage in operating large mining pools. Such an advantage makes it easier for conglomerates to control blockchain votes while making other governance mechanisms – market monitoring, stakeholder monitoring, and reputation building – less effective.

Our model fits the description of the Bitcoin mining ecosystem. Bitmain Technologies, a private Chinese (PRC) company founded in 2013, is the leader in the ASIC-based cryptocurrency mining hardware industry, with approximately 74.5% of the global market share (Bitmain Prospectus, 2018). ASICs became the dominant technology for mining Bitcoin in late 2015 (Eghbali and Wattenhofer (2019)). Bitmain is also a prominent player in other segments of the cryptomining ecosystem, such as mining pools. Figure 1 shows the evolution of the market shares of Bitmain's affiliated pools and those of other large pools until early 2021. Bitmain-affiliated pools' market shares have been consistently at or above 30% since

[4]Irresberger, John, Mueller, and Saleh (2021) show that proof-of-work is the leading consensus protocol among public blockchains (see their Figure 2).

October 2016.



Source: Authors' calculations (data from https://explorer.btc.com/btc/insights-pools). Bitmain core refers to pools in which Bitmain has known ownership stakes (AntPool, BTC.com, and ViaBTC). Bitmain total adds to the core pools those that are Bitmain's business partners (BTC.Top, OKExPool, Huobi.pool, and 1THash; see Table 1 for more details).

Bitmain has used its control over a substantial proportion of the *hash rate* (i.e., computational power allocated to mining) to leave its mark on the governance of blockchains. Control over the hash rate can be used to enforce a blockchain split (sometimes called a *hard fork*). The most famous hard fork of the Bitcoin blockchain was the one that created Bitcoin Cash on August 1, 2017, which resulted from unresolved disagreements among members of the Bitcoin community concerning changes to the size of blocks. A few prominent players in the Bitcoin ecosystem, including Bitmain, sponsored the creation of the new coin, which shared the same history as Bitcoin but had a larger block size. On November 15, 2018, Bitcoin Cash itself split into two competing blockchains. Bitmain rallied behind Bitcoin Cash ABC against Bitcoin Cash SV in what became known as the "hash wars." The prices of both currencies fell steeply right after the split, as did the prices of Bitcoin and other cryptocurrencies.

The model is as follows. Blockchain stakeholders regularly choose between two versions of the protocol. Miners, or mining pools that serve as proxies for miners, "vote" for a protocol proposal by allocating their hash rate (i.e., computational power) to one of the two proposals.

Mining requires computational power. Equipment firms produce specialized equipment that delivers more hash rate than the generic technology (e.g., CPU or GPU). Equipment producers care about the blockchain protocol because they design chips that are protocol-specific.

Mining pools offer differentiated services. Miners are heterogeneous in their preferences over mining pool attributes. Mining pools compete for miners by choosing fees. A blockchain conglomerate has incentives to compete aggressively with other mining pools in order to leave a larger surplus to miners and increase demand for equipment.[5]

We show that blockchain conglomerates have incentives to control a large share of the total hash rate. By doing so, they can vote for their preferred protocol. Conglomerates face a trade-off. On the one hand, an ASIC-friendly protocol implies lower production costs for equipment. On the other hand, such a protocol may negatively affect the coin price, reducing demand for equipment and pool services. We show that when the coin price is sufficiently high, conglomerates always capture the vote and choose the cost-reducing protocol, despite its negative price impact.

Our model also considers the governance role played by other blockchain stakeholders: (standalone) mining pools and individual miners. To prevent capture by a conglomerate, standalone mining pools may choose to compete aggressively for mining pool market share, thus reducing the conglomerate's share of the votes. We show that when the coin price is sufficiently high, standalone pools find it more costly to compete for market share, thus leading to an equilibrium with conglomerate capture.

Miners may vote with their feet and choose to leave mining pools that support value-destroying protocols. However, because miners are small, they have incentives to free-ride and leave the cost of monitoring to others. We show that, even if miners are sufficiently large to be pivotal, they may wish to join pools that support value-destroying protocols, provided that such pools offer miners better contractual terms.

In Section 2 we discuss the related literature and the relevant institutional details. In

[5] This competitive effect, also known as a *profit squeeze*, is found in Farrell and Katz (2000) and Chen and Nalebuff (2006). Equipment producers and mining pools are "complementors," in the sense used by Brandenburger and Nalebuff (1996).

Section 3 we present the model setup. In Section 4 we present the model solution. Section 5 concludes. All proofs are in the appendix. Additional material can be found in the Internet Appendix.

2. Related Literature and Institutional Details

2.1. Related Literature

We use as building blocks several ideas from three different literature areas: (i) corporate governance, (ii) industrial organization, and (iii) blockchain economics. Our main theoretical contribution is the development of a framework that embeds these elements in a unified model.

A decentralized, permissionless blockchain such as Bitcoin is a public service with diffuse ownership. There are no shareholders but instead multiple stakeholders, such as users, investors, miners, etc. Similar to large corporations with diffuse ownership, most stakeholders are small. As the corporate governance literature shows (Grossman and Hart, 1980; Shleifer and Vishny, 1986), small shareholders lack the motivation and the ability to monitor and improve corporate governance; diffuse ownership leads to free-riding by small shareholders. In our model, small stakeholders (such as individual miners) similarly free-ride on the monitoring efforts by others, leading to an equilibrium with insufficient monitoring.

In our model, few large stakeholders emerge. These are large equipment producers and mining pool operators. They play a significant role in blockchain governance, similar to the role played by large shareholders in corporate governance.[6] One issue with large shareholders is the possibility of tunneling resources from companies in which they have low cash flow rights to companies in which they have high cash flow rights (Johnson, La Porta, Lopez-de-Silanes, and Shleifer, 2000; Bertrand, Mehta, and Mullainathan, 2002). Similarly, in our model, a large blockchain conglomerate can tunnel blockchain surplus away from the mining pool business to its equipment business.

Our paper incorporates some of the insights found in the industrial organization litera-

[6] For the role of large shareholders in corporate governance, see Shleifer and Vishny (1986), Winton (1993), Zwiebel (1995), Burkart, Gromb, and Panunzi (1997, 2000), Bolton and von Thadden (1998), Maug (1998), Pagano and Roell (1998), Bennedsen and Wolfenzon (2000), Noe (2002), Brav and Mathews (2011), Edmans and Manso (2011), Levit and Malenko (2011), Malenko and Malenko (2019), Bar-Isaac and Shapiro (2020), and Edmans, Levit and Reilly (2019). See also Edmans (2014) for a review of this literature.

ture. Farrell and Katz (2000) and Chen and Nalebuff (2006) show that a monopolist has incentives to enter the market for a complementary good in order to squeeze the profits in that market, thus leaving more surplus to consumers. This surplus then increases the demand for the monopolist's good. Similar to our model, the literature on strategic motives for bundling also considers how firms can leverage their market power in one market to reinforce their market power in another market (Carbajo, De Meza, and Seidmann, 1990; Whinston, 1990; Nalebuff, 2004).

There is a growing theoretical literature on the economics of cryptomining. Starting with Dimitri (2017), a literature has developed on competition among miners that also produce their own equipment (see Arnosti and Weinberg, 2018; Ma, Gans, and Tourky, 2018; and Alsabah and Capponi, 2020). In such models, miners are Cournot oligopolists who compete by choosing computing power capacity. These papers discuss concentrated market shares but they do not discuss governance issues (i.e., how concentrated market shares affect the evolution of the protocol) or develop models of voting in blockchains. Differently from these papers, our model shows how blockchain conglomerates endogenously emerge and capture the governance of the blockchain. To the best of our knowledge, ours is also the first model of blockchain mining to take the interests of all relevant players in the mining industrial ecosystem – miners, mining pools, and equipment producers – into consideration.

Cong, He, and Li (2021) model how competition among pools affects equilibrium fees and pool sizes. A key social inefficiency in Cong, He, and Li's model is the "hash rate externality:" When miners invest in acquiring hash rate they do not internalize their effect on other miners, who then also want to acquire more hash rate, leading to an arms race. Cong, He, and Li (2021) show that mining pools partially internalize the hash rate externality. In our model, pools behave in a similar fashion; because they have some captive demand, they set higher prices and also partially internalize the hash rate externality. However, once a pool becomes owned by a firm that is also an equipment producer, this firm wants to set lower pool fees because the producer directly profits from selling more hash rate. Thus, in our model, the combination of mining pools and equipment producer in one firm exacerbates the hash rate externality.

We model the individual miners' decision to enter the mining business as in Budish (2018), who assumes free entry of miners (see also Prat and Walter (2021) for an alternative model of free entry of miners). Budish (2018) shows that proof-of-work is a very costly system for

sustaining trust; for honest behavior to be incentive-compatible, the cost of an attack (which is a flow) has to be higher than the benefit derived from attacking the blockchain (which is a stock).

Some previous theoretical work focuses on other aspects of blockchain technology. Huberman, Leshno, and Moallemi (2021) and Easley, O'Hara, and Basu (2019) develop models of mining that can be used to determine the equilibrium value of Bitcoin transaction fees. Biais, Bisière, Bouvard, and Casamatta (2019a) study competition among miners in proof-of-work blockchains as a coordination game and show that hard forks may occur in equilibrium. Hinzen, John, and Saleh (2021) study the adoption of proof-of-work blockchains. Arruñada and Garicano (2018) study the trade-off between coordination and the protection from expropriation in blockchain platforms. Abadi and Brunnermeier (2018) show that ledgers cannot simultaneously attain three desirable properties: correctness, decentralization, and cost-efficiency. Cong and He (2019) study the effect of blockchain technologies on how firms compete with one another. Pagnotta (2020) shows that Bitcoin's monetary rules can be welfare decreasing. For surveys of the economic literature on blockchains, see Biais, Bisière, Bouvard, and Casamatta (2019b), Chen, Cong, and Xiao (2020), and Halaburda, Haeringer, Gans, and Gandal (2021). For a broad set of facts on multiple cryptocurrencies, see Hu, Parlour, and Rajan (2019).

2.2. Institutional Details

The Bitcoin blockchain is a public ledger showing the history of all transactions involving transfers of bitcoins since the creation of the currency. This history is used to determine and verify the owners of each bitcoin (or fraction of it). When someone "spends" bitcoin, they send a message to some Bitcoin nodes (i.e., computers running Bitcoin code) to notify them of the occurrence of a particular transaction involving changes in the ownership of bitcoins. When a node receives information about a transaction, it verifies whether the transaction is valid by checking it against Bitcoin rules. The node then broadcasts the transactions to other connected nodes, which then repeat the process until all network nodes receive the relevant information about the transaction.

All *full nodes* keep a local copy of the whole ledger. The ledger takes the form of a uniquely ordered chain of blocks; blocks are sets of transactions. The ledger is updated by the addition of new blocks to the chain. Blocks have a maximum size and, once created,

cannot be changed by deleting, adding, or modifying transactions. Nodes of a particular type, called *miners*, create the blocks. Miners compete for the right to produce a new block by using their computational power to try to solve a particular mathematical problem. When a miner succeeds at solving the problem, the miner creates a block containing a set of recent transactions and information that allows others to verify that the miner has indeed found the correct solution to the mathematical problem. The miner then shares the block with other full nodes (only some full nodes are miners); all full nodes can easily verify whether the solution is correct. When nodes receive a new valid block with the right solution, they add that block to their local copy of the blockchain. Because nodes are connected to other nodes, information about the updated blockchain quickly propagates through the network, and nodes sequentially update their copies of the blockchain until every node (presumably) has the same copy. Miners that had been working on solving the same problem are then supposed to stop working on that problem and start the process of solving a new problem associated with the next block.

Anyone who runs an application that "implements" the Bitcoin protocol can use their computational power to "mine" blocks. Although entry into the mining business is unrestricted, the process of mining is costly. First, the miner must buy or rent hardware. While most miners used generic CPU or GPU equipment in the early years (Eghbali and Wattenhofer (2019)), currently, most mining is done by specialized hardware (called an *application-specific integrated circuit* [ASIC]), which is many times more efficient than GPUs or CPUs. Second, miners must pay for variable costs, including electricity. The mathematical problem is solved by brute force and cannot be made easier by coordinating miners, implying that the probability of a miner being the first to find a solution is proportional to the amount of computational power they allocate to the mining process. The Bitcoin algorithm is constantly adjusted (every 2016 blocks) so that the average time for successfully mining a block (the *block interval*) is approximately ten minutes. The miner who wins the competition receives all fees associated with the transactions in the block plus a fixed number of newly created bitcoins (the *block reward*); in early 2021, the block reward was 6.25 bitcoins.[7] Because winning miners have to demonstrate that they have found the correct solution, finding the solution is "proof" that they have "worked" on the problem by directing their hash rate to

[7]For studies focusing on Bitcoin transaction fees, see Huberman, Leshno, and Moallemi (2021), Easley, O'Hara, and Basu (2019), and Lehar and Parlour (2020).

it. This system is thus called *proof-of-work*.

As cryptomining evolved into a specialized economic activity, many other goods and services were created to support miners. One example is the provision of insurance to miners. Mining is a risky activity: miners pay up-front for electricity, equipment, and maintenance costs but are only rewarded if they win the competition by finding the "lucky hash," i.e., the solution to the mathematical problem associated with the current block. An individual miner who owns a single Bitcoin mining machine can expect to wait for decades before mining a single block. Mining pools help diversify the risks faced by small miners. Although the term "pool" suggests some form of cooperative arrangement, mining pools are actually private firms that sell services – such as insurance – to cryptominers. A miner who joins a mining pool directs his/her hash rate to the pool. Pool managers then make the decisions concerning which blocks to mine. Pool owners make profits by charging fees.

In Table 1, we show how some of the (historically) large Bitcoin mining pools differ in some dimensions. As of March 2021, the pools in Table 1 collectively accounted for 86% of the total hash rate employed. All but one pool (Binance) have known links to Bitmain Technologies, the largest mining ASIC producer.[8]

Pools differ in the types of contracts (usually referred to as "payment methods") they offer. The most popular contract is called *pay-per-share* (PPS), which has three different versions: "plain" PPS, *full pay-per-share* (FPPS), and *pay-per-share plus* (PPS+). In all of these contracts, miners split the expected block reward proportionally to their supplied hash rate, independently of whether the pool succeeds at winning the tournament. That is, PPS contracts offer full insurance.[9] In another standard (but far less common) contract (*pay-per-last-N-shares*), miners share rewards in proportion to their contributed hash rate in the last N rounds, but only when the pool is successful.

Of the largest mining pools, only two (AntPool and ViaBTC) offer a choice between

[8] AntPool and BTC.com are fully-owned subsidiaries of Bitmain. Bitmain is the largest investor in ViaBTC. Both F2Pool and BTC.TOP are partners of BitDeer, which is a Bitmain-sponsored cloud-mining service. The parent companies of Huobi.pool and OkExPool are strategic partners of Bitmain. Jihan Wu, Bitmain's founder and chairman, is also an adviser of Huobi (one of the largest cryptocurrency exchanges in the world and the owner of Huobi.pool).

[9] Under a plain PPS contract, only the block reward is paid to miners; the pool retains the transaction fees. Variations of PPS (PPS+ or FPPS) include the sharing of transaction fees. FPPS distributes expected transaction fees proportionally to the hash rate supplied and, thus, offers full insurance to miners. PPS+ contracts distribute realized transaction fees. Because transaction fees vary from block to block, PPS+ contracts entail some risk. Still, because the average transaction fees per block are much lower than the fixed block reward (typically about 1% of the block reward), the risk in such contracts is negligible.

different contracts. Only AntPool and ViaBTC offer contracts in which block reward payments depend on the pool's success. In contrast, all pools offer some version of PPS (full insurance). PPS fees vary; the lowest fee in March 2021 was provided by BTC.com: 1.5% for its full PPS contract.

At any given point in time, there are multiple copies of the Bitcoin blockchain. For example, suppose that two miners find the solution for the same block at about the same time and forward their blocks to their respective nearest nodes. Because it takes time for information to percolate through the network, not all nodes will receive the two competing blocks in the same order. Thus, members of the Bitcoin community will regularly encounter situations in which they need to decide between two or more different versions of the blockchain. How are such conflicts resolved? The typical answer is to postulate that the longest chain will eventually win; once it becomes clear that one chain is longer than all others, miners will abandon other chains and focus their efforts on the longest one. Blocks recently mined in abandoned chains – "orphan blocks" – are deemed invalid.

The longest chain solution is not a hard feature of Bitcoin. When choosing which chain to support, participants play a standard coordination game: if everyone is expected to support version A over B, it is individually optimal to support A. The longest-chain selection criterion is intuitive and may serve as a focal point, but in principle, other equilibria are possible. Biais, Bisière, Bouvard, and Casamatta (2019a) aptly name the longest-chain hypothesis *the blockchain folk theorem*. They show that there exist equilibria where a chain might bifurcate at some date, with two different versions of the blockchain coexisting forever. Recent evidence indicates that blockchain splits can be successful and command significant support among miners, such as in the case of Bitcoin Cash, a new blockchain created in 2017 as a bifurcation of the original Bitcoin blockchain. Biais, Bisière, Bouvard, and Casamatta (2019b) document 16 additional hard forks since then.

Blockchain splits are costly. Because of network externalities, splits may reduce the long-term value of a blockchain. In the short term, splits may negatively affect the liquidity of a cryptocurrency, increasing volatility and hindering adoption.[10]

A high degree of coordination is necessary to change the core rules of Bitcoin – what is called the Bitcoin protocol. Anyone can propose a change in rules through a Bitcoin

[10]For an analysis of the importance of liquidity in bitcoin trading, see Makarov and Schoar (2020), who show that bitcoin prices react strongly and persistently to order flows.

Improvement Proposal (BIP). Such proposals usually have to be vetted by some Bitcoin developers and then face a "vote" among miners. The proposal itself typically sets the requirements for agreement and adoption. For example, the proposal may stipulate that a particular change requires approval from a supermajority of miners (a typical number is 95%) during a given period (measured in blocks). Miners signal their support for a proposal in the blocks they solve. Once the threshold is achieved, the proposal is said to be "locked in," and it is activated at a predetermined later date. It is essential to keep in mind that this is again not a hard feature; proposals can secure support from a large number of miners and still be dropped. An example was the 2017 proposal called SegWit2x, which secured support from 100% of miners but was later dropped due to a lack of consensus among different Bitcoin stakeholders.

The relevant voice mechanism for choosing between alternative versions of the blockchain is by directing hash power to them. When different groups of miners cannot coordinate on a single set of rules, they can direct their hash power to competing versions of the blockchain, creating hard forks.

3. Model Setup

We first describe the workings of the governance of the blockchain and then introduce three types of stakeholders in the mining ecosystem: miners, equipment producers, and mining pools.

3.1. Governance

Blockchain rules are not immutable; they can be changed if there is sufficient agreement among blockchain stakeholders. We assume that blockchain stakeholders regularly choose between two proposals (i.e., versions of the blockchain protocol), here represented by $z \in \{\underline{z}, \overline{z}\}$. Let $r(z)$ denote the exchange rate between the blockchain coin and the dollar, i.e., the *coin price*. The coin price depends on how market participants value different attributes of the blockchain protocol. We define $r(z) = r + \Delta r(z)$, where r is the *coin price level* and $\Delta r(z)$ is the *price impact of the proposal*. Without loss of generality, let the price impact associated with proposal $\underline{z}$ be zero and that of proposal $\overline{z}$ be $\Delta r \geq 0$. That is, $r(\overline{z}) - r(\underline{z}) = \Delta r$, which is the (relative) price impact from swaying the vote.

Miners, or mining pools that serve as proxies for miners,"vote" for a proposal by allocating their *hash rate* (i.e., computational power) to one of the two proposals. We assume (realistically) that miners are typically long on the coin, thus they prefer higher coin prices. Mining pools also prefer higher coin prices, because higher coin prices increase demand for mining pool services (as we will show formally in the next section). Thus, mining pools have no incentives to vote for $\underline{z}$.

Let ε_l be the hash rate controlled by voter l at a given date. The interpretation is that ε_l is the hash rate over which l has "voting rights." For example, an individual miner may not be able to support a proposal if the miner directs some of their hash rate to a mining pool. We assume that voters' influence over the governance of the blockchain is proportional to the hash rate they control. Let $\varphi_l = \frac{\varepsilon_l}{n}$ denote the share of the overall hash rate controlled by voter l, where n is the total mass of hash rate in the network. The proposal with a simple majority of votes is implemented.

3.2. Miners

To model the behavior of miners, we use a modified version of Budish's (2018) model of bitcoin mining. Let ϕ denote the reward, in coin units, to the miner who wins a mining competition. Thus, in dollar terms, a miner who wins the competition earns $\phi r(z)$.

At any period, if miner i supplies n_i units of hash rate, their instantaneous probability of winning the reward is $\frac{n_i}{n}$, where n is the total hash rate in the blockchain. Hash rate is a continuous variable; $n_i \in \Re^+$ represents a mass of hash rate. Hash rate is a homogeneous good; mining equipment is only valued for its capacity of generating hash rate.

We model miners' decision to buy mining equipment as follows. At some time τ, each miner i simultaneously buys equipment that can produce (at most) n_i of hash rate per unit of time. We assume that mining equipment becomes obsolete (i.e., it fully depreciates) after T periods; miners only repurchase capacity after the existing stock fully depreciates.[11] That is, if miners buy equipment at time τ, they will buy equipment again only at time $\tau + T$. Let $\tau \in \{0, T, 2T, ..., \infty\}$ denote the dates when miners buy equipment. We call τ a *purchasing date*. A miner who buys equipment that can produce n_i for T periods pays an up-front cost in dollars of pn_iT (for notational simplicity, we assume no time discounting for periods between

[11] In reality, new mining rig models are introduced at regular intervals, which tends to make the existing equipment less competitive.

times τ and $\tau + T - 1$). That is, p denotes the up-front price of one unit of computational power, here assumed to be constant between two consecutive purchasing dates.

Let θ_i denote miner i's net cost per unit mass of hash rate, excluding the cost of the equipment. Mining has many sources of variable costs, such as electricity, storage, maintenance, mining pool fees, attention, and effort. In θ_i, we also include non-pecuniary benefits and costs, such as fun, speculative beliefs, preferences for gambling, risk aversion, and the insurance services provided by mining pools. Thus, when needed, we rewrite θ_i as the sum of its N individual components:

$$\theta_i = \theta_{i1} + \theta_{i2} + ... + \theta_{iN}. \tag{1}$$

Let δ denote the amount of time it takes to mine a block (also called the *block interval*); δ is a random variable. The blockchain protocol adjusts its difficulty level to keep the expected block interval constant at level $\overline{\delta}$. Without loss of generality, we normalize $\overline{\delta}$ to 1. That is, over the lifetime of the equipment, miners collectively expect to produce T blocks. For simplicity, we assume that the difficulty is adjusted instantaneously at each period; see the Internet Appendix for an explicit model of difficulty adjustment.[12] We also assume that miners use their equipment at full capacity for T periods. In the Internet Appendix, we show that the case in which miners do not always operate at capacity is similar to our baseline model.

We represent the expected payoff, as of purchasing date τ, of an individual miner who acquires hash rate n_i and uses their full capacity until $\tau + T$ by

$$V_i = \left(\frac{\phi r(z)}{n} - p - \theta_i \right) n_i T. \tag{2}$$

We define the per-period utility of a miner as $U_i \equiv \frac{V_i}{T}$.

3.3. Equipment Producers

General-purpose mining equipment (i.e., a CPU/GPU chip) that generates hash rate exists, and its dollar price per hash unit, c, is determined in a larger market; the size of the mining industry does not affect c. There are also producers of specialized equipment; these producers

[12] A similar assumption can be found in Pagnotta (2020). In reality, in the case of Bitcoin, the difficulty is adjusted every 2016 blocks, or about two weeks, to keep the average block interval at ten minutes.

own a technology that produces mining equipment at a constant unit cost $\underline{c} < c$ per hash. This equipment – also called an application-specific integrated circuit (ASIC) – is specific to mining some particular coins and cannot be used for any other purpose.

A key assumption is that equipment is only valued for its efficiency in mining. Some mining equipment may be more efficient than others (perhaps because of AsicBoost[13] or engineering prowess), but that only means that the more efficient equipment produces the same amount of hash rate at a lower cost (that is, at a lower $\underline{c}$).

For simplicity, we assume that there are only two firms that can become either equipment producers or mining pools, or both. Because hash rate is a homogeneous good, miners buy hash rate from producer j only if $p_j \leq \min\{p_1, p_2, c\}$, where p_j is the price per unit of hash rate set by Firm $j \in \{1, 2\}$. Let n_j denote the hash rate capacity per period sold by Firm j to individual miners.[14] The per-period profit of a firm that sells n_j of equipment at price p_j is

$$(p_j - \underline{c})n_j - \lambda(z), \tag{3}$$

where

$$\lambda(z) = \begin{cases} \underline{\lambda} & \text{if } z = \underline{z} \\ \overline{\lambda} & \text{if } z = \overline{z} \end{cases}, \tag{4}$$

is a (per period) fixed cost of production.

A key assumption is that $\lambda(z)$ depends on the blockchain protocol, here represented by z. We focus on the case in which $\overline{\lambda} > \underline{\lambda}$. In that case, equipment producers face a trade-off: Under $\overline{z}$ they face higher production costs, but may also expect higher demand for equipment because high $r(z)$ makes mining more profitable. Equipment producers care about the blockchain protocol because they design chips that are protocol-specific. For example, $\overline{z}$ could be a proposal to use a mining protocol that makes ASICs less efficient. This could be achieved by eliminating protocol weaknesses that give ASICs a performance advantage (such as AsicBoost) or by attempting to make the protocol ASIC-proof. An extreme example would be a move to a proof-of-stake protocol, as in the Ethereum 2.0 upgrade, which would make ASICs worthless (this case can be modelled as $\overline{\lambda} \to \infty$).

[13] AsicBoost is a technique that makes ASIC equipment faster.

[14] Here we assume that firms do not perform proprietary mining. In reality, self-mining by equipment producers represents a significantly smaller share of their revenues than does sales of equipment (see, e.g., Bitmain IPO Prospectus, 2018). In the Internet Appendix, we discuss the case in which firms may choose to self-mine and show conditions under which it may or may not arise in equilibrium.

Why would coin prices be higher under protocols that limit the advantages of specialized equipment? First, single-purpose specialized equipment represents a departure from the original idea of permissionless blockchains as a decentralized and democratic network. Thus, users may become less positive about a blockchain that shows signs of increasing mining centralization.[15] Second, some proposals that limit the appeal of specialized equipment aim at both increasing the speed of transaction processing and reducing the environmental cost of mining. Moving from proof-of-work to proof-of-stake is again an example here.

3.4. Mining Pools

Mining pools are profit-maximizing firms that offer services to miners and charge fees. The most obvious service that mining pools offer is insurance. Miners also assign value to pool services beyond insurance. For example, some pools offer a *solo* option (see Table 1), in which a miner uses the mining resources and software from the mining pool without buying insurance; the typical fee for this service is 1%.

Let f_j denote the fee per unit mass of hash rate charged by firm $j \in \{1, 2\}$. Individual miners can choose to direct some or all of their hash rate to mining pools. Pool managers then choose which blocks to mine using all the hash rate directed to their pool. Let m_j denote the amount of hash power directed to firm j at a given period. Firm j's (per-period) profit is thus $f_j m_j$.

As shown in Table 1, mining pools are not all alike; they differ in many dimensions. First, pools offer different types of contracts, and there is a limited amount of choice within each pool. Second, the level of transparency varies greatly across pools: for example, some pools do not post information on fees and contracts on their websites, and some pools' websites are in Chinese only. Third, pools differ in many technical aspects, such as server location, user interface, technical assistance, and the availability of merged mining.[16] Finally, the reputation of a pool is also an important consideration for miners; miners need to trust

[15] An example here is Bitcoin Gold, a hard fork of Bitcoin whose main goal was to change the proof of work algorithm so that ASICs cannot be used to mine Bitcoin Gold. According to its developers, "*ASICs tend to monopolize mining to a few big players, but GPU mining means anyone can mine again - restoring decentralization and independence*" (https://bitcoingold.org).

[16] For example, Poolin offers the option of automatically switching between Bitcoin and Bitcoin Cash mining depending on the expected profitability. Huobi.pool gives "Huobi.pool tokens" for free to their miners.

pools to honor the terms of the contract.[17]

We do not model the reasons for mining pools to offer differentiated services. Instead, we consider a model in which miners are heterogeneous in their preferences over mining pool attributes and mining pools compete for miners by choosing fees. At each mining period t, let υ_{ij} denote miner i's (per unit mass of hash rate) valuation of the unique combination of attributes offered by pool j.[18] Recall that f_j is the fee charged by firm j for each unit of hash rate. For each miner i, their period surplus from allocating one unit of hash rate to firm j is thus

$$s_{ij} = \upsilon_{ij} - f_j. \tag{5}$$

If miner i chooses firm j, we set $\theta_{i1} = -s_{ij}$ in (1). For simplicity, and without loss of generality, we normalize all other costs (and benefits) to zero; $\theta_{i2} = ... = \theta_{iN} = 0$. Thus, we can replace θ_i with $-s_{ij}$.

For simplicity, we assume that valuations υ_{ij} are independent and identically distributed across both miners and pools, with density function $g(\upsilon)$ over the support $[\underline{\upsilon}, \overline{\upsilon}]$, with $\underline{\upsilon} > 0$, $\overline{\upsilon}$ finite, cdf $G(\cdot)$ and mean μ. These assumptions imply that both pools are ex ante homogeneous in terms of the valuation of their attributes.[19] We assume that $\underline{\upsilon}$ is sufficiently high so that, in equilibrium, a miner always prefers to join one of the two pools instead of mining solo. That is, the two pools serve the whole market.[20]

3.5. Timing

We consider the problem of two firms, Firm 1 and Firm 2, which decide whether to operate in either the equipment market or the mining pool market, or in both markets. For simplicity, there are no one-time entry or exit costs, but note that $\lambda(z)$ is a fixed cost per period, thus it also doubles as an entry cost in the equipment market.

At each purchasing date τ, the timeline of actions is as follows.

Date 0: Firms simultaneously choose whether to enter each market.

[17] Complaints about lack of transparency in payments and accusations of fraud abound in Internet forums.

[18] Valuation υ_{ij} includes, among other things, i's preferences for different contracts, perhaps because of heterogeneity in liquidity and risk preferences.

[19] This is different from Cong, He, and Li's (2021) model in which mining pools have different levels of passive hash rate.

[20] For example, in the Internet Appendix we show that a sufficient condition for miners never to mine alone is $\underline{\upsilon} g(\underline{\upsilon})(c - \mu + \underline{\upsilon}) \geq c - \mu$.

Date 1: Firms choose their equipment prices and mining pool fees, simultaneously. Prices and fees are fixed for the whole mining cycle (i.e., from τ to $\tau + T - 1$).

Date 2: Miners decide whether to buy equipment. Each equipment producer pays production cost $n_j \underline{c} + \lambda(z)$, where n_j is the per-period equipment demand faced by producer j.

Date 3: Miners learn v_{ij} and choose which pool to join.

Date 4: Mining pools (and miners who do not join mining pools) vote over proposals $\underline{z}$ and $\overline{z}$; the proposal with the simple majority of votes is implemented. The winning proposal determines the coin price $r(z)$ for the whole mining cycle and the fixed production cost $\lambda(z)$ for the next mining cycle, which starts at purchasing date $\tau + T$.[21] Mining tournaments run for T periods, when the equipment is fully depreciated.

For simplicity, we assume that miners do not know their mining pool preferences v_{ij} before deciding whether to buy equipment. Although this assumption is not necessary for our results,[22] we note that this assumption is realistic in our application. When deciding whether to become a miner, potential miners may not know all the relevant characteristics of a mining pool. Mining pools' websites differ in the amount and quality of information they provide (see Table 1). In addition, other sources (such as comparison sites) often offer incomplete and conflicting information.[23] Finally, miners can only acquire a sense of the quality of the service through their experience with a particular pool.

4. Model Solution

We focus on solving for stationary (pure-strategy) equilibria in which equilibrium actions and outcomes are independent of history. In Subsection 4.7, we also discuss history-dependent equilibria. To solve for an equilibrium, we work backwards within each purchasing period τ.

[21] Results are identical if the fixed production cost changes immediately (at time $\tau + 1$).

[22] In the Internet Appendix, we show conditions under which our main results would arise without making assumptions about when miners learn their mining pool preferences.

[23] For example, according to Bitcoin Wiki, AntPool does not offer merged mining. However, cryptocompare.com states that AntPool offers merged mining for five different coins. We could not find any information on AntPool's website about the availability of merged mining.

4.1. Date 4

For any purchasing period τ, at Date 4, mining pools and solo miners (if any) vote over proposals $\underline{z}$ and $\overline{z}$. The coin price is then given by

$$r(z) = \begin{cases} r & \text{if } z = \underline{z} \\ r + \Delta r & \text{if } z = \overline{z} \end{cases}. \tag{6}$$

Because there are no entry or operating costs for mining pools, both firms operate mining pools for all periods $\tau \geq 0$. At each purchasing period τ, there are three cases to consider: (i) both firms enter the pool market only, (ii) both firms enter both markets and become conglomerates, (iii) only one firm becomes a conglomerate (for simplicity, in this case we call the conglomerate Firm 1).

Let φ_j denote the share of votes controlled by the mining pool run by Firm j. In all three cases, the outcome of the vote (and thus the price of the coin) can be predicted perfectly from knowledge of φ_1 and φ_2. In Case (i), proposal $\overline{z}$ always wins because mining pools strictly prefer a higher price $r(z)$, as this increases the demand for mining pool services. In Case (ii), proposal $\underline{z}$ minimizes both firms' production cost for the next mining cycle (by setting $\lambda = \underline{\lambda}$), without affecting equipment and pool services demand for the current period. Proposal $\underline{z}$ then wins if and only if $\varphi_1 + \varphi_2 > 0.5$. In Case (iii), let φ_1 denote the share of votes controlled by the mining pool run by Firm 1 (the conglomerate). If $\varphi_1 > 0.5$, Firm 1 chooses $\underline{z}$. If $\varphi_1 \leq 0.5$, proposal $\overline{z}$ wins the majority of votes and is implemented (for simplicity, we assume that proposal $\overline{z}$ wins if there is a tie). Because the equilibrium is history-independent, Firm 1 cannot commit to vote for proposal $\overline{z}$ (in Subsection 4.7, we consider history-dependent equilibria and state the conditions under which equilibrium with commitment is generally not possible).

4.2. Date 3

At Date 3, after miner i discovers v_{ij} for each firm $j \in \{1, 2\}$, the miner chooses which pool to join. To consider the simplest possible scenario, we assume that miners are atomistic, i.e., $n_i \to 0$ for all i (Later in Subsection 4.7, we consider the case in which miners are non-atomistic). Because miners are atomistic, miners know they cannot individually change the outcome of the vote at Date 4 by switching mining pools. Thus, miners will consider

only their net direct surplus when deciding which pool to join. Miner i's net direct surplus from joining a pool at Date 3 is given by[24]

$$s_i^* = \max_{j \in \{1,2\}} \upsilon_{ij} - f_j. \tag{7}$$

4.3. Date 2

At Date 2, miners do not yet know their types; thus, they also do not know which pool they would join after entry. The probability that miner i chooses Firm 1 over Firm 2 is $\Pr(\upsilon_{i1} - \upsilon_{i2} \geq f_1^* - f_2^*)$. Because all valuations are identically and independently distributed, the distribution of $\upsilon_{i1} - \upsilon_{i2}$ is symmetric with zero mean, with support $[-(\overline{\upsilon} - \underline{\upsilon}), (\overline{\upsilon} - \underline{\upsilon})]$. Let $H(.)$ denote the cumulative distribution function for $\upsilon_{i1} - \upsilon_{i2}$ (note that $H(0) = 0.5$). Note that in equilibrium, Firm 1's pool market share is $\varphi_1 = 1 - H(f_1 - f_2)$.

Let $E[s^* \mid f_1, f_2]$ denote the expectation (conditional on fees f_1 and f_2) of s_i^* as defined in (7). Because all miners are identical at this date,

$$E[s^* \mid f_1, f_2] = \int_{\underline{\upsilon}}^{\overline{\upsilon}} \int_{\underline{\upsilon}}^{\overline{\upsilon}} \max\{\upsilon_1 - f_1, \upsilon_2 - f_2\} g(\upsilon_1) g(\upsilon_2) d\upsilon_1 d\upsilon_2. \tag{8}$$

From (2), miner i's per-period expected payoff is

$$U_i = \left(\frac{\phi r(z)}{n} - p + E[s^* \mid f_1, f_2] \right) n_i, \tag{9}$$

where $p \equiv \min\{p_1, p_2, c\}$ (recall that hash rate is a homogeneous good). Assuming free entry of miners, equilibrium requires $U_i = 0$, which determines the equilibrium hash rate n:

$$n = \frac{\phi r(z)}{p - E[s^* \mid f_1, f_2]}. \tag{10}$$

As a sufficient condition to avoid infinite entry by miners, we assume $E[s^* \mid 0, 0] < \underline{c}$.

[24] Our modeling of the mining pool market is analogous to traditional random-utility discrete-choice differentiated goods models that are common in the industrial organization literature (e.g., Perloff and Salop, 1986).

4.4. Date 1

At Date 1, firms choose fees and equipment prices simultaneously to maximize their profits. Each pool controls the votes of its customers, implying that its share of the vote is $\varphi_1(f_1, f_2) = 1 - H(f_1 - f_2)$ for Firm 1 and $\varphi_2(f_1, f_2) = H(f_1 - f_2)$ for Firm 2. We have to consider three cases, as described above.

In Case (i), both firms are standalone pool operators. Clearly, they have no incentives to vote for $\underline{z}$, thus their profit functions (per unit of time) are

$$\begin{aligned} \Pi_1'(f_1, f_2) &= \phi(r + \Delta r) \frac{f_1 \varphi_1(f_1, f_2)}{c - E[s^* \mid f_1, f_2]}, \\ \Pi_2'(f_1, f_2) &= \phi(r + \Delta r) \frac{f_2 \varphi_2(f_1, f_2)}{c - E[s^* \mid f_1, f_2]}. \end{aligned} \tag{11}$$

Lemma 1 *If both firms enter the pool market only, in any stationary equilibrium with actions $\langle f_1', f_2' \rangle$ and outcomes n' and z', we have*

1. $f_1' = f_2' = f'$;
2. $n' = \frac{\phi(r+\Delta r)}{c - E[s^* | f', f']}$, *and*
3. $z' = \overline{z}$.

In this case, firms care only about their mining pool profits. They compete in fees in Bertrand fashion; profits are positive since firms offer differentiated services. Because firms are ex ante homogeneous, equilibrium pool fees are identical due to symmetry. As demand for services is higher when coin prices are higher (and so are profits), both firms vote for proposal $\overline{z}$.

In Case (ii), both firms enter the equipment market and the pool market. Under the assumption of full coverage of the market for mining pool services, both conglomerates control 100% of the hash rate and thus jointly capture the governance of the blockchain, in which case they both vote for $z = \underline{z}$. Both firms choose fees simultaneously. They also chooses the equipment price per hash rate, p_1 and p_2, simultaneously, subject to $\min\{p_1, p_2\} \leq c$. Let $I_{p_1 \leq p_2} = 1$ if $p_1 \leq p_2$ and zero otherwise. The firms' profit functions are:

$$\Pi_1''(p_1,p_2,f_1,f_2) = \phi r \frac{f_1\varphi_1(f_1,f_2)+(p_1-\underline{c})I_{p_1\leq p_2}}{\min\{p_1,p_2\}-E[s^* \mid f_1,f_2]} - \underline{\lambda}, \quad (12)$$

$$\Pi_2''(p_1,p_2,f_1,f_2) = \phi r \frac{f_2\varphi_2(f_1,f_2)+(p_2-\underline{c})(1-I_{p_1\leq p_2})}{\min\{p_1,p_2\}-E[s^* \mid f_1,f_2]} - \underline{\lambda}.$$

Lemma 2 *If both firms are conglomerates, in any stationary equilibrium with actions* $\langle p_1'', p_2'', f_1'', f_2''\rangle$ *and outcomes* n'' *and* z''*, we have*

1. $p_1'' = p_2'' = \underline{c}$ *and* $f_1'' = f_2'' = f''$*;*
2. $n'' = \frac{\phi r}{\underline{c}-E[s^*|f'',f'']}$*, and*
3. $z'' = \underline{z}$*.*

In this equilibrium, the hash rate price is set at its marginal cost $\underline{c}$. This is a consequence of Bertrand competition with a homogeneous good (hash rate). Again, firms are ex ante homogeneous and thus equilibrium pool fees are identical due to symmetry.

The next lemma shows that we can rank the profits in cases (i) and (ii) if $\underline{\lambda} = \Delta r = 0$, that is, if the fixed operating cost $\underline{\lambda}$ is zero and the vote has no price impact.

Lemma 3 *Suppose that* $\underline{\lambda} = \Delta r = 0$*. Equilibrium profits are higher when both firms are conglomerates than when when they are standalone mining pools:*

$$\Pi_j''(\underline{c},\underline{c},f'',f'') > \Pi_j'(f',f') \text{ for } j = 1,2. \quad (13)$$

This result is important because it partly explains why a firm may choose to become a conglomerate when competing against another conglomerate, despite the fact that Bertrand competition implies zero profit in the equipment market. Conglomerate competition reduces the equipment price from c to $\underline{c}$, which incentivizes miners to buy more equipment, thus increasing the overall demand for mining pool services. As long as $\underline{\lambda}$ and Δr are not too large, this spillover effect makes firms prefer the Case (ii) equilibrium to the Case (i) equilibrium.

In Case (iii), Firm 1 is a conglomerate that produces equipment and operates mining pools, while Firm 2 is a standalone pool.[25] If $f_1 < f_2$, then $\varphi_1 = 1 - H(f_1 - f_2) > 0.5$, thus

[25] As we focus on stationary equilibria, we do not consider the nonstationary case in which firms alternate between being conglomerates or standalone pools over time. This type of equilibrium is not economically interesting or realistic.

Firm 1 will win the vote at Date 4, implying $z = \underline{z}$. If $f_1 \geq f_2$, Firm 2 will win the vote at Date 4, implying $z = \overline{z}$. The outcome of the vote determines both $\lambda(z)$ for the next mining cycle (starting at $\tau + T$) and the coin price $r(z)$ at Date 4.

Define $\Delta\lambda \equiv \overline{\lambda} - \underline{\lambda}$ as an equipment producer's *private benefit* from controlling the vote. The private benefit measures a producer's cost saving if proposal $\underline{z}$ is chosen. Both firms choose pool fees simultaneously. Firm 1 also chooses the equipment price per hash rate, p_1, subject to $p_1 \leq c$. Let $I_{f_1 \geq f_2} = 1$ if $f_1 \geq f_2$ and zero otherwise. The firms' incremental profit functions are[26]

$$\begin{aligned} \Pi_1'''(p_1, f_1, f_2) &= \phi(r + I_{f_1 \geq f_2}\Delta r)\frac{f_1\varphi_1(f_1, f_2) + p_1 - \underline{c}}{p_1 - E[s^* \mid f_1, f_2]} - \underline{\lambda} - I_{f_1 \geq f_2}\Delta\lambda \qquad (14) \\ \Pi_2'''(p_1, f_1, f_2) &= \phi(r + I_{f_1 \geq f_2}\Delta r)\frac{f_2\varphi_2(f_1, f_2)}{p_1 - E[s^* \mid f_1, f_2]}, \end{aligned}$$

Suppose first $\Delta r = \Delta\lambda = 0$; that is, governance capture has no payoff implications for any of the players. We then have the following result:

Lemma 4 *Suppose that $\Delta r = \Delta\lambda = 0$. If Firm 1 is the sole conglomerate, in any stationary equilibrium with actions $\langle p_1^*, f_1^*, f_2^*\rangle$, we have that $f_1^* < f_2^*$.*

This lemma shows that when only Firm 1 is a conglomerate, its pool is larger than the pool of its competitor, even when voting has no payoff implications. Intuitively, this result arises because the conglomerate benefits more from offering low fees than does an independent pool. Lowering fees has three positive effects: (i) it allows the firm to acquire a larger share of the pool market, (ii) it increases the overall demand for pool services, (iii) it increases the demand for equipment. Only the conglomerate internalizes (iii); thus, it naturally wants to set lower fees than its competitor.

The theoretical intuition is as follows. The conglomerate faces a trade-off between surplus creation and surplus extraction. When the conglomerate lowers its pool fee, more miners enter the market. Because of network externalities, the entry of additional miners reduces the total surplus. Thus, for the conglomerate to benefit from lowering its pool fee, it must extract a larger fraction of this reduced surplus. This form of surplus capture can happen, for example, if Firm 2 (the independent pool) also lowers its fee in response to the fee set by

[26] For notational simplicity only, we assume no time discounting between purchasing dates. Alternatively, we can reinterpret $\lambda(z)$ as the present value of operational costs.

the equipment producer. Thus, the equipment producer "squeezes" Firm 2's profit. Farrell and Katz (2000) and Chen and Nalebuff (2006) develop models with a similar profit squeeze effect, although in different contexts.

In our model, and in reality as well, when choosing mining pools, miners care about fees and the characteristics (i.e., quality) of pool services. Thus, a mining pool may acquire market shares either by lowering fees or by increasing quality. For simplicity only, in our model, we take quality as given. The main empirical implication from Lemma 4 is that the blockchain conglomerate will have the largest market share.

The next lemma characterizes the equilibrium with one conglomerate for the general case where $\Delta r \geq 0$ and $\Delta\lambda \geq 0$.

Lemma 5 *If Firm 1 is the sole conglomerate, in any stationary equilibrium with actions* $\langle p_1''', f_1''', f_2''' \rangle$ *and outcomes* n''' *and* z'''*, we have*

1. $p_1''' = c$ *and* $f_1''' \leq f_2'''$*;*
2. $n''' = \frac{\phi r(z''')}{c - E\left[s^* | f_1''', f_2'''\right]}$*, and*
3. $z''' = \overline{z}$ *if* $f_1''' = f_2'''$ *and* $z''' = \underline{z}$ *if* $f_1''' < f_2'''$*.*

When there is one conglomerate (Firm 1), there are only two types of equilibria. In an equilibrium of the first type, Firm 1 captures the governance of the blockchain by setting $f_1''' < f_2'''$ and choosing $z''' = \underline{z}$. In the second type of equilibrium, both firms offer the same pool fees $f_1''' = f_2''' = f'''$ and $z''' = \overline{z}$; governance capture does not happen.

Lemma 4 shows that governance capture always arises when governance has no payoff implications. Thus, an equilibrium without capture can only occur if governance has payoff implications. In particular, such an equilibrium exists only if $\Delta r > 0$.

4.5. Date 0

At Date 0, firms make entry decisions. Both firms choose to become mining pools because there is no entry cost and mining pool profits are non-negative. There are three cases to consider as possible equilibria, which are Cases (i)-(iii) discussed above. Under the assumption that equilibria in Date 1 have the properties described in Lemmas 1 to 5, we can characterize the optimal entry decisions as follows.

If Firm 1 expects Firm 2 not to enter the equipment market, not entering this market is a best response for Firm 1 if and only if

$$\Pi_1'\left(f', f'\right) \geq \Pi_1'''\left(c, f_1''', f_2'''\right). \tag{15}$$

(Note that, by symmetry, Firm 2 also does not want to enter the equipment market). If this condition holds, we have that Case (i) is an equilibrium.

If Firm 2 expects Firm 1 to enter the equipment market, entering this market is a best response for Firm 2 if and only if

$$\Pi_2''\left(\underline{c}, \underline{c}, f'', f''\right) \geq \Pi_2'''\left(c, f_1''', f_2'''\right). \tag{16}$$

(Again, by symmetry, Firm 1 also wants to enter the equipment market). If this condition holds, we have that Case (ii) is an equilibrium.

If Firm 1 expects Firm 2 not to enter the equipment market, entering this market is a best response for Firm 1 if and only if

$$\Pi_1'''\left(c, f_1''', f_2'''\right) \geq \Pi_1'\left(f', f'\right). \tag{17}$$

If Firm 2 expects Firm 1 to enter the equipment market, not entering this market is a best response for Firm 2 if and only if

$$\Pi_2'''\left(c, f_1''', f_2'''\right) \geq \Pi_2''\left(\underline{c}, \underline{c}, f'', f''\right). \tag{18}$$

If conditions (17) and (18) hold, we have that Case (iii) is an equilibrium. In this case, the equilibrium is asymmetric – only one firm (Firm 1, for simplicity) enters both markets – despite the fact that both firms are exactly identical ex ante.

4.6. Equilibrium with Capture: Existence and Properties

Here we show conditions under which an equilibrium with capture exists. Governance capture requires that at least one firm chooses to enter the equipment market. Thus, we need the fixed cost of equipment under capture, $\underline{\lambda}$, to be sufficiently low so that at least one firm finds it profitable to enter this market. Once entry occurs, the existence of equilibria with capture

depends on the particular constellation of model parameters.

Suppose that, at Date 1, we are in Case (iii) (i.e., there is a single conglomerate). Let f_1''' and f_2''' denote a pair of equilibrium fees. For this to be an equilibrium with capture, we need that $f_1''' < f_2'''$. Such fees must also be best responses to one another, given the expected equilibrium proposal, $z''' = \underline{z}$:

$$f_1''' \in \arg\max_{f_1} \phi r \frac{f_1 \varphi_1 \left(f_1, f_2'''\right) + c - \underline{c}}{c - E\left[s^* \mid f_1, f_2'''\right]} - \underline{\lambda} \tag{19}$$

$$f_2''' \in \arg\max_{f_2} \phi r \frac{f_2 \varphi_2 \left(f_1''', f_2\right)}{c - E\left[s^* \mid f_1''', f_2\right]}. \tag{20}$$

As shown in Lemma 4, for a given proposal, equilibrium fees must indeed be such that $f_1''' < f_2'''$. This is a consequence of the conglomerate's incentives to squeeze the profits of its competitor. Note that f_1''' and f_2''' do not depend on r and $\underline{\lambda}$; fees are invariant to the blockchain protocol.

For pool fees (f_1''', f_2''') given by (19) and (20), we write the equilibrium profits of each firm as $r\pi_1''' - \underline{\lambda}$ and $r\pi_2'''$, where

$$\pi_1''' = \phi \frac{f_1''' \left(1 - H(f_1''' - f_2''')\right) + c - \underline{c}}{c - E\left[s^* \mid f_1''', f_2'''\right]} \tag{21}$$

$$\pi_2''' = \phi \frac{f_2''' H(f_1''' - f_2''')}{c - E\left[s^* \mid f_1''', f_2'''\right]}. \tag{22}$$

Proposition 1 *At Date 1 of period τ, suppose there is one conglomerate. An equilibrium with governance capture in the subgame starting in Date 1 exists if and only if pool fees (f_1''', f_2''') are given by (19) and (20), and the following conditions hold:*

$$\Delta\lambda \geq \Delta r \pi_1^d - r\left(\pi_1''' - \pi_1^d\right), \tag{23}$$

$$0 \geq \Delta r \pi_2^d - r\left(\pi_2''' - \pi_2^d\right), \tag{24}$$

where

$$\pi_1^d \equiv \max_{f_1 \in \left[f_2''', \overline{v}\right]} \phi \frac{f_1 \left(1 - H(f_1 - f_2''')\right) + c - \underline{c}}{c - E\left[s^* \mid f_1, f_2'''\right]}.$$

$$\pi_2^d \equiv \max_{f_2 \in \left[0, f_1'''\right]} \phi \frac{f_2 H(f_1''' - f_2)}{c - E\left[s^* \mid f_1''', f_2\right]}.$$

Conditions (19) and (20) imply that fees f_1''' and f_2''' are best responses to one another for a given blockchain protocol z. Conditions (23) and (24) imply that these fees are also best responses to one another when the equilibrium protocol depends on the fees. The intuition is as follows. For fees $f_1''' < f_2'''$ to constitute an equilibrium, alternative governance mechanisms must be ineffective. Within the model, there are two alternative governance mechanisms: market monitoring and competitor monitoring (in the next subsection, we consider extensions that allow for other governance mechanisms).

We first consider market monitoring. When proposal $\overline{z}$ is approved, coin prices increase by Δr (alternatively, we can think of proposal $\underline{z}$ having a negative price impact of Δr). That is, the coin market rewards good proposals and punishes bad proposals. Firm 1 benefit from higher coin prices, as these increase demand for both equipment and mining pool services. Thus, if Δr is sufficiently high, Firm 1 may be better off if $\overline{z}$ is approved. Condition (23) guarantees that Firm 1's private benefit $\Delta\lambda$ from governance capture compensates for the the net benefit from self-discipline. To understand the right-hand side of (23), note that if Firm 1 deviates and chooses $f_1^d \geq f_2'''$, $\overline{z}$ is approved and the coin price increases by Δr. However, its profit in coin units is reduced by $\pi_1''' - \pi_1^d > 0$.

The second alternative governance mechanism is monitoring by competitors. When proposal $\overline{z}$ is approved, Firm 2 benefits from higher demand for pool services caused by the increase in coin prices. Condition (24) guarantees that Firm 2's net benefit from controlling the vote is not strictly positive. To understand the right-hand side of (24), note that if Firm 2 deviates and chooses $f_2^d \leq f_1'''$, $\overline{z}$ is approved and the coin price increases by Δr. However, its profit in coin units is reduced by $\pi_2''' - \pi_2^d > 0$.[27]

The next result follows immediately from Proposition 1:

Corollary 1 *Alternative governance mechanisms are less effective if:*

1. *The private benefit ($\Delta\lambda$) is high,*
2. *The price impact of the vote (Δr) is low,*
3. *The coin price level (r) is high.*

[27] If we allowed the conglomerate also to self-mine (instead of selling all the equipment it produces), equilibria with capture can be sustained in some cases even when condition (24) does not hold.

Here, by less effective we mean that conditions (23) and (24) hold for a larger set of parameters.

Now we consider the equilibrium conditions for the whole game. We focus on equilibrium with capture.[28] The next proposition shows that conditions on a single parameter, the price level r, are sufficient to guarantee the existence of equilibria with capture.

Proposition 2 *A threshold $\widetilde{r}$ exists such that, if $r > \widetilde{r}$, stationary equilibria exist. In this case, there exist thresholds $\widetilde{\lambda}$ and $\widehat{\lambda} > 0$, with $\widehat{\lambda} \geq \widetilde{\lambda}$, such that, in an equilibrium:*

1. *If $\underline{\lambda} \leq \widetilde{\lambda}$, both firms jointly capture the governance of the blockchain;*
2. *if $\underline{\lambda} \in \left(\widetilde{\lambda}, \widehat{\lambda}\right]$, one firm alone captures the governance of the blockchain;*
3. *if $\underline{\lambda} > \widehat{\lambda}$, no firm enters the equipment market.*

This proposition implies that there always exists a pair $(r, \underline{\lambda})$ such that only equilibrium with governance capture exists. An immediate consequence of this proposition is as follows.

Corollary 2 *For sufficiently high coin prices (r), equilibria with capture exist even when the price impact Δr is arbitrarily large and/or the private benefit $\Delta\lambda$ is zero.*

This surprising result holds because the profit squeeze effect (represented by $r\left(\pi_j''' - \pi_j^d\right)$) increases the cost of alternative governance mechanisms (i.e., market monitoring and competitor monitoring). The profit squeeze effect is proportional to r, thus a larger r implies a higher cost of self-discipline (see condition (23)) and a higher cost for the competitor to monitor (see condition (24)).

A consequence of this corollary is that more successful blockchains – those with higher coin prices – are more susceptible to governance capture by blockchain conglomerates. Capture happens because alternative governance mechanisms are less effective when coin prices are high. This result serves as a cautionary note to the belief that the success of a blockchain leads to better incentive provision to market participants.[29]

4.7. Extensions: Other Governance Mechanisms

In this subsection, we consider two additional governance mechanisms: Reputation building and miner governance.

[28] In the proof of Proposition 2 we also show the conditions for equilibria without capture to exist.

[29] On a similar note, Budish (2018) shows that higher coin prices make double-spending attacks more likely.

4.7.1. Reputation

Thus far we have assumed that a conglomerate cannot commit to vote for proposal $\overline{z}$ at Date 4. We now consider the possibility that this commitment arises in equilibrium because of reputational concerns. For such an equilibrium to exist, any deviation by the conglomerate in its voting policy will lead to a future fall in coin prices, which leads to lower demand for equipment and pool services.

Suppose that $r \geq \widetilde{r}$ and $\underline{\lambda} \in \left[\widetilde{\lambda}, \widehat{\lambda}\right]$. Thus, from Proposition 2, an equilibrium in which Firm 1 alone captures the governance of the blockchain exists. To consider alternative equilibria, we now relax the assumption that equilibrium strategies and outcomes are independent of history.

Consider a candidate equilibrium for the subgame at Date 1 as follows. Fees $f_1 = f_1'''$ and $f_2 = f_2'''$ are as defined in (19) and (20), the protocol at each purchasing date τ is $z_\tau = \overline{z}$, and the equilibrium hash rate is

$$n = \frac{\phi(r + \Delta r)}{c - E\left[s^* \mid f_1''', f_2'''\right]}. \tag{25}$$

Thus, the equilibrium is such that Firm 1 has the largest market share but always votes for $\overline{z}$. Consider now a possible deviation from this equilibrium. If, at time τ, Firm 1 instead deviates and votes for $\underline{z}$, miners expect prices to fall from $r + \Delta r$ to r for all future periods. Thus, an equilibrium with $(\overline{z}, f_1''', f_2''')$ exists only if the following condition holds:

$$(r + \Delta r)\,\pi_1''' - \overline{\lambda} \geq r\pi_1''' - \underline{\lambda}. \tag{26}$$

The left-hand side is Firm 1's per period profit if it follows its equilibrium strategy. The right-hand side is Firm 1's per period profit if it deviates and votes for $\underline{z}$. If (26) does not hold, then Firm 1 prefers to deviate and choose $\underline{z}$ even if it loses its reputation for good governance forever. This will happen if $\Delta r \pi_1''' < \Delta\lambda$, that is, for sufficiently high private benefits or a sufficiently low price impact.

If condition (26) holds, there could be multiple equilibria: both history-dependent equilibria (reputation building) and history-independent equilibria (as discussed in Subsection 4.6) can exist. For a history-dependent equilibrium to be sustained, all potential miners must be aware of past governance decisions. This might be unrealistic in scenarios in which

the number of potential miners is very large.

4.7.2. Miner Governance

Because we have assumed that miners are atomistic, individual miners cannot vote with their feet and choose to join mining pools with the intent of changing the outcome of the vote. To allow for miner exit as a governance mechanism, we now assume that miners can form coalitions. Coalitions of miners can force all members to choose the same pool. Thus, these coalitions can potentially affect the outcome of the vote.

Consider an equilibrium in which Firm 1 alone captures the governance of the blockchain. After miners enter at Date 2, a mass of αn miners, where $\alpha \in (0,1)$, are matched randomly and form a coalition.[30] Then, each coalition member casts a vote for a mining pool. The coalition makes decisions by majority voting. If the majority votes for pool 1, then the coalition lets their miners choose the pools individually. Since this does not affect the outcome of the vote z, this decision maximizes total coalition surplus.

If the majority votes for pool 2, then the coalition mandates a fraction of their members to join pool 2, so that there is exactly 50% of the votes in favor of proposal $\overline{z}$. Again, this decision maximizes total coalition surplus.

The coalition is potentially pivotal. For the coalition to have the ability to change the outcome of a vote and thus disrupt the equilibrium, we need

$$\alpha + (1-\alpha) H(f_1 - f_2) \geq \frac{1}{2}. \tag{27}$$

To understand this condition, suppose that all miners in the coalition join Firm 2. Thus, the proportion of votes for proposal $\overline{z}$ is α (all the votes in the coalition) plus $(1-\alpha) H(f_1 - f_2)$ (all standalone miners who prefer Firm 2).

In addition to having the means for monitoring the mining pools, the coalition also needs to have the motive to do so. The median voter in the coalition is such that $v_{i1} - v_{i2} = 0$, thus the coalition chooses to force all members to choose pool 2 if

$$\frac{\phi(r + \Delta r)}{n} - f_2 \geq \frac{\phi r}{n} - f_1. \tag{28}$$

[30] In an equilibrium with two conglomerates, the coalition would need a fraction $\alpha > 0.5$ to be pivotal.

This condition guarantees that the majority of the coalition benefits if the coalition manages to flip the decision.

The following proposition establishes conditions for the existence of an equilibrium as described in Proposition 1 in the case where miners can form a coalition of size αn.

Proposition 3 *Suppose that a coalition of size $\alpha n'''$ of miners is formed randomly after entry. A stationary equilibrium with fees f_1''' and f_2''' given by (19) and (20) exists if and only if conditions (23) and (24) hold and at least one of the following holds:*

$$\alpha + (1-\alpha)\, H\left(f_1''' - f_2'''\right) < \frac{1}{2} \tag{29}$$

or

$$\frac{\phi \Delta r}{n'''} < f_2''' - f_1'''. \tag{30}$$

This proposition establishes conditions for an equilibrium with capture to exist even in the presence of alternative governance mechanisms, including market monitoring, competitor monitoring, and miner monitoring. Note that a higher equilibrium fee spread $f_2''' - f_1'''$ makes both (29) and (30) easier to be satisfied. If (29) holds, the coalition is not large enough to sway the vote, thus the free-riding incentives of individual miners dominate. If (30) holds, the median voter in the coalition prefers Firm 1's pool, and thus the best policy for the coalition is to let its members choose their preferred pool.

5. Conclusion

In this paper, we develop a model in which the proof-of-work protocol creates an industrial ecosystem where miners, mining services providers, and mining equipment producers have conflicting interests. Our model implies that the emergence of such stakeholders has a substantial effect on the governance of blockchains. We show that some stakeholders have incentives to control a large portion of the whole mining ecosystem. In particular, we show that blockchain conglomerates capture the governance of the blockchain.

According to our model, a dominant blockchain conglomerate invests in the mining ecosystem to encourage more individuals to become miners. This explanation corresponds to what Bitmain Technologies – the leading blockchain conglomerate in the Bitcoin mining ecosystem – states in its IPO prospectus:

> "*Catering to our customers' evolving needs, we supplement our core cryptocurrency mining ASIC chips design business with (...) our mining pool business. (...) Our mining pools reduce the risks and volatility of mining and facilitate a steady return for individual cryptocurrency miners, which encourage more participants to engage in mining activities.*"[31]

Our model has clear policy implications. We show that integration in the mining ecosystem is detrimental to the governance of the blockchain. In addition to its governance benefits, policies that forbid equipment producers from operating mining pools may have other social benefits. Because miners compete for a fixed prize, such policies can decrease the social deadweight cost of mining by reducing the amount of computational power and electricity allocated to it.

Our model suggests that Nakamoto's vision of blockchain governance is untenable. Because market power propagates through the mining ecosystem, corporate capture is in proof-of-work's DNA. If a large firm captures the governance of the blockchain, blockchain stakeholders have to trust one company to look after their interests. In that case, one may ask how a permissionless blockchain differs from a traditional financial intermediary as a provider of trust.

Not all blockchains use the proof-of-work protocol. For example, some blockchains rely instead on *proof-of-stake* protocols, in which the probability of becoming a block producer is proportional to one's "stake" in the network.[32] As our model is about proof-of-work, we do not consider these alternative protocols. However, our analysis has broader implications, which could also be relevant for understanding blockchain governance under alternative protocols. Our key message is that to understand the workings of the governance of a blockchain, we need to consider the structure of the ecosystem of industries that serve the block producers.

References

Abadi, J. and M. Brunnermeier. 2018. Blockchain Economics. *Working paper.*

[31] This quote is from Bitmain's IPO application to the Hong Kong Stock Exchange in September 2018.

[32] There is some evidence that such alternatives to proof-of-work are becoming more popular (Irresberger, John, Mueller, and Saleh, 2021). For economic analyses of the proof-of-stake concept, see Saleh (2021) and Roşu and Saleh (2021).

Alsabah, H., and A. Capponi. 2020. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. *Working paper.*

Arruñada, B. and L. Garicano. 2018. Blockchain: The Birth of Decentralized Governance. *Working paper.*

Arnosti, N. and S. M. Weinberg. 2019. Bitcoin: A Natural Oligopoly. *10th Innovations in Theoretical Computer Science.*

Bar-Isaac, H. and J. Shapiro. 2020. Blockholder Voting. *Journal of Financial Economics.* 136: 695-717.

Bennedsen, M. and D. Wolfenzon. 2000. The Balance of Power in Closely Held Corporations. *Journal of Financial Economics.* 58: 113-139.

Bertrand, M., P. Mehta. and S. Mullainathan. 2002. Ferreting out Tunneling: An Application to Indian Business Groups. *Quarterly Journal of Economics.* 117: 121-148.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2019a. The Blockchain Folk Theorem. *Review of Financial Studies.* 32: 1662-1715.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2019b. Strategic Interactions in Blockchain Protocols: A Survey of Game-theoretic Approaches. *Working paper.*

Bolton, P. and E-L. von Thadden. 1998. Blocks, Liquidity, and Corporate Control. *Journal of Finance.* 53: 1-25.

Brandenburger, A. and B. Nalebuff. 1996. *Co-opetition.* Harper Collins Business, New York.

Brav, A. and R. D. Mathews. 2011. Empty Voting and the Efficiency of Corporate Governance. *Journal of Financial Economics.* 99: 289–307.

Budish, E. 2018. The Economic Limits of Bitcoin and the Blockchain. *Working paper.*

Burkart, M., D. Gromb, and F. Panunzi. 1997. Large Shareholders, Monitoring, and the Value of the Firm. *Quarterly Journal of Economics.* 112: 693-728.

Burkart, M., D. Gromb, and F. Panunzi. 2000. Agency Conflicts in Public and Negotiated Transfers of Corporate Control. *Journal of Finance.* 55: 647-677.

Carbajo, J., D. De Meza, and D. J. Seidmann. 1990. A Strategic Motivation for Commodity Bundling. *Journal of Industrial Economics.* 38: 283-298.

Chen, L., L. W. Cong, and Y. Xiao. 2020. A Brief Introduction to Blockchain Economics. *Information for Efficient Decision Making*: *Big Data, Blockchain and Relevance.* edited by Kashi R Balachandran. World Scientific Publishers. pp. 1-40.

Chen, M. K. and B. Nalebuff. 2006. One-Way Essential Complements. *Working paper*, Yale University.

Chod, J. and E. Lyandres. 2020. A Theory of ICOs: Diversification, Agency, and Information Asymmetry. *Management Science*. forthcoming

Cong, L. W. and Z. He. 2019. Blockchain Disruption and Smart Contracts. *Review of Financial Studies.* 32: 3412-3460.

Cong, L. W., Z. He, and J. Li. 2021. Decentralized Mining in Centralized Pools. *Review of Financial Studies*. 34: 1191-1235.

Cong, L. W., Y. Li, and N. Wang. 2021. Token-based Platform Finance. *Working paper.*

Dimitri, N. 2017. Bitcoin Mining as a Contest. *Ledger.* 2: 31-37.

Easley, D., M. O'Hara, and S. Basu. 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics.* 134: 91-109.

Edmans, A. 2014. Blockholders and Corporate Governance. *Annual Review of Financial Economics.* 6: 23-50.

Edmans, A., D. Levit, and D. Reilly. 2019. Governance Under Common Ownership. *Review of Financial Studies.* 32: 2673-2719.

Edmans, A. and G. Manso. 2011. Governance Through Trading and Intervention: A Theory of Multiple Blockholders. *Review of Financial Studies.* 24: 2395-2428.

Eghbali, A. and R. Wattenhofer. 2019. 12 Angry Miners, in Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (Eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Springer, 391-398.

Farrell, J. and M. L. Katz. 2000. Innovation, Rent Extraction, and Integration in Systems Markets. *Journal of Industrial Economics.* 48: 413-432.

Grossman, J. and O.D. Hart. 1980. Takeover Bids, The Free-Rider Problem, and the Theory of the Corporation. The Bell Journal of Economics. 11: 42-64.

Halaburda, H., G. Haeringer, Gans J., and N. Gandal. 2020. The Microeconomics of Cryptocurrencies. *Journal of Economic Literature*. forthcoming

Hinzen, F. J., K. John, and F. Saleh. 2021. Bitcoin's Fatal Flaw: The Limited Adoption Problem. *Working paper*.

Hu, A., C. Parlour, and U. Rajan. 2019. Cryptocurrencies: Stylized Facts on a New Investible Instrument. *Financial Management*, 48: 1049-1068.

Huberman, G., J. Leshno, and C. Moallemi. 2021. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Review of Economic Studies.* forthcoming

Irresberger, F., K. John, Mueller, P.,and F. Saleh. 2021. The Public Blockchain Ecosystem: An Empirical Analysis. *Working paper*.

Johnson, S., R. La Porta, F. Lopez-de-Silanes, and A. Shleifer. 2000. Tunneling. *American Economic Review*. 90: 22-27.

Levit, D. and N. Malenko. 2011. Nonbinding Voting for Shareholder Proposals. *Journal of Finance.* 66: 1579-1614.

Lehar, A. and C. A. Parlour. 2020. Miner Collusion and the BitCoin Protocol. *Working paper*.

Ma J., J. S. Gans, and R. Tourky. 2018. Market Structure in Bitcoin Mining. *Working paper.*

Makarov, I. and A. Schoar. 2020. Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics*. 135: 293-319

Malenko, A. and N. Malenko. 2019. Proxy Advisory Firms: The Economics of Selling Information to Voters. *Journal of Finance.* 74: 2441-2490.

Maug, E. 1998. Large Shareholders as Monitors: Is There a Trade-off Between Liquidity and Control? *Journal of Finance.* 53: 65-98.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Nalebuff, B. 2004. Bundling as an Entry Barrier. *Quarterly Journal of Economics.* 119: 159-187.

Noe, T. 2002. Investor Activism and Financial Market Structure. *Review of Financial Studies.* 15: 289-318.

Pagano, M. and A. Röell. 1998. The Choice of Stock Ownership Structure: Agency Costs, Monitoring, and the Decision to Go Public. *Quarterly Journal of Economics.* 113: 187–225.

Pagnotta, E. 2020. Decentralizing Money: Bitcoin Prices and Blockchain Security. *Review of Financial Studies.* forthcoming.

Perloff, J. and S. Salop. 1985. Equilibrium with Product Differentiation. *Review of Economic Studies.* 52: 107-120.

Prat, J. and B. Walter. 2021. An Equilibrium Model of the Market for Bitcoin Mining. *Journal of Political Economy.* forthcoming

Roşu, I., and F. Saleh. 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science.* 67: 661-672.

Saleh, F. 2021. Blockchain Without Waste: Proof-of-Stake. *Review of Financial Studies.* 34: 1156-1190.

Shleifer, A., and R. W. Vishny. 1986. Large Shareholders and Corporate Control. *Journal of Political Economy.* 94: 461-488.

Whinston, M. 1990. Tying, Foreclosure, and Exclusion. *American Economic Review.* 80: 837-859.

Winton, A. 1993. Limitation of liability and the ownership structure of the firm. *Journal of Finance.* 48: 487-512.

Zwiebel, J. 1995. Block investment and partial benefits of corporate control. *Review of Economic Studies.* 62: 161–85.

6. Appendix

Preliminary result used in the proofs of Lemmas 1-5

Result 1 *Define* $E[s^* \mid f_1, f_2]$ *as in (8). Then we have*

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_1} = -(1 - H(f_1 - f_2)) \tag{31}$$

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_2} = -H(f_1 - f_2). \tag{32}$$

Proof. Note first that a standalone mining pool would never choose $f_j \geq \overline{v}$ as there would be no demand for its pool services. Similarly, a conglomerate would also never choose $f_j \geq \overline{v}$ as there would be no demand for its pool services and demand for equipment is increased if it sets any f_j lower than $\overline{v}$. Thus, in what follows, we only consider cases in which both f_1 and f_2 are strictly lower than $\overline{v}$.

Recall that $H(f_1 - f_2) = \Pr(v_1 - v_2 \leq f_1 - f_2)$. We then have

$$H(f_1 - f_2) = \begin{cases} 1 - G(\overline{v} - f_1 + f_2) + \int_{\underline{v}}^{\overline{v} - f_1 + f_2} G(v_2 + f_1 - f_2)\, g(v_2)\, dv_2 \text{ for } f_1 - f_2 > 0 \\ \int_{\underline{v} - f_1 + f_2}^{\overline{v}} G(v_2 + f_1 - f_2)\, g(v_2)\, dv_2 \text{ for } f_1 - f_2 \leq 0. \end{cases} \tag{33}$$

Recall that $E[s^* \mid f_1, f_2] = E[\max\{v_1 - f_1, v_2 - f_2\}]$. For $f_1 - f_2 > 0$, we have

$$\begin{aligned} E[s^* \mid f_1, f_2] = & \int_{\overline{v} - f_1 + f_2}^{\overline{v}} (v_2 - f_2) g(v_2)\, dv_2 \\ & + \int_{\underline{v}}^{\overline{v} - f_1 + f_2} \left[\int_{v_2 + f_1 - f_2}^{\overline{v}} (v_1 - f_1) g(v_1)\, dv_1 + G(v_2 + f_1 - f_2)(v_2 - f_2) \right] g(v_2)\, dv_2 \end{aligned}$$

which from (33) implies

$$E[s^* \mid f_1, f_2] = E[v \mid f_1, f_2] - (1 - H(f_1 - f_2)) f_1 - H(f_1 - f_2) f_2,$$

where

$$\begin{aligned} E[v \mid f_1, f_2] = & \int_{\underline{v}}^{\overline{v} - f_1 + f_2} \left[\int_{v_2 + f_1 - f_2}^{\overline{v}} v_1 g(v_1)\, dv_1 + G(v_2 + f_1 - f_2)\, v_2 \right] g(v_2)\, dv_2 \\ & + \int_{\overline{v} - f_1 + f_2}^{\overline{v}} v_2 g(v_2)\, dv_2. \end{aligned}$$

The partial effect of increasing f_1 on $E[s^* \mid f_1, f_2]$ is (after some simplification)

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_1} = -\int_{\underline{\upsilon}}^{\overline{\upsilon}-f_1+f_2} (1 - G(\upsilon_2 + f_1 - f_2)) g(\upsilon_2)\, d\upsilon_2 = -(1 - H(f_1 - f_2)).$$

By symmetry:

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_2} = -H(f_1 - f_2).$$

For $f_1 - f_2 \leq 0$, we have

$$\begin{aligned} E[s^* \mid f_1, f_2] = \; & G(\underline{\upsilon} - f_1 + f_2) \int_{\underline{\upsilon}}^{\overline{\upsilon}} (\upsilon_1 - f_1) g(\upsilon_1)\, d\upsilon_1 \\ & + \int_{\underline{\upsilon}-f_1+f_2}^{\overline{\upsilon}} \left[\int_{\upsilon_2+f_1-f_2}^{\overline{\upsilon}} (\upsilon_1 - f_1) g(\upsilon_1)\, d\upsilon_1 + G(\upsilon_2 + f_1 - f_2)(\upsilon_2 - f_2) \right] g(\upsilon_2)\, d\upsilon_2 \end{aligned}$$

which again gives us (after some simplification):

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_1} = -1 + \int_{\underline{\upsilon}-f_1+f_2}^{\overline{\upsilon}} G(\upsilon_2 + f_1 - f_2) g(\upsilon_2) d\upsilon_2 = -(1 - H(f_1 - f_2)).$$

Again, by symmetry:

$$\frac{\partial E[s^* \mid f_1, f_2]}{\partial f_2} = -H(f_1 - f_2).$$

■

Proof of Lemma 1

Proof. Both firms are standalone pool operators. The price per hash rate of the general purpose mining equipment is c. The firms have no incentives to vote for $\underline{z}$, thus $z' = \overline{z}$. From (10), it follows immediately that, at Date 2, demand for hash rate is:

$$n(f_1, f_2) = \frac{\phi(r + \Delta r)}{c - E[s^* \mid f_1, f_2]}, \tag{34}$$

where f_1 and f_2 are the fees announced at Date 1. At Date 1, the firms choose pool fees f_1 and f_2 simultaneously to maximize their profits given in (11), where $\varphi_1(f_1, f_2) = 1 - H(f_1 - f_2)$ and $\varphi_2(f_1, f_2) = H(f_1 - f_2)$. Using Result 1, the simplified first-order conditions are (after some rearranging):

$$f_1 h(f_1 - f_2) = 1 - H(f_1 - f_2) - \frac{f_1 (1 - H(f_1 - f_2))^2}{c - E[s^* \mid f_1, f_2]} \tag{35}$$

$$f_2 h(f_1 - f_2) = H(f_1 - f_2) - \frac{f_2 H(f_1 - f_2)^2}{c - E[s^* \mid f_1, f_2]}. \tag{36}$$

We subtract (36) from (35) to obtain

$$(f_1 - f_2)\, h(f_1 - f_2) = 1 - 2H(f_1 - f_2) - \frac{f_1(1 - H(f_1 - f_2))^2 - f_2 H(f_1 - f_2)^2}{c - E[s^* \mid f_1, f_2]},$$

which is also equivalent to

$$\begin{aligned} & (f_1 - f_2)\left[(c - E[s^* \mid f_1, f_2])\, h(f_1 - f_2) + H(f_1 - f_2)^2\right] \\ = \;& (c - E[\upsilon \mid f_1, f_2] - (f_1 - f_1)\, H(f_1 - f_2))\,(1 - 2H(f_1 - f_2)). \end{aligned} \tag{37}$$

This can be further rearranged as follows

$$\begin{aligned} & (f_1 - f_2)\left[(c - E[s^* \mid f_1, f_2])\, h(f_1 - f_2) + (1 - H(f_1 - f_2))\, H(f_1 - f_2)\right] \\ = \;& (c - E[\upsilon \mid f_1, f_2])\,(1 - 2H(f_1 - f_2)). \end{aligned} \tag{38}$$

Notice that $[(c - E[s^* \mid f_1, f_2])\, h(f_1 - f_2) + (1 - H(f_1 - f_2))\, H(f_1 - f_2)] > 0$ for any $f_1 \in (0, \overline{\upsilon})$ and $f_2 \in (0, \overline{\upsilon})$.[33] Assume that $H(f_1' - f_2') > 0.5$. Then, the right hand side of (38) is negative, which implies $f_1' < f_2'$, contradicting $H(f_1' - f_2') > 0.5$. Assume now that $H(f_1' - f_2') < 0.5$. Then the right-hand side of (38) is positive, which implies $f_1' > f_2'$, contradicting $H(f_1' - f_2') < 0.5$. Because $H(0) = 0.5$, (38) is only satisfied for $f_1' = f_2' = f'$.

We can now simplify the FOC (35) and solve for f':

$$(c - \widehat{\upsilon} + f')\,(0.5 - f' h(0)) - 0.25 f' = 0, \tag{39}$$

where

$$\widehat{\upsilon} = \int_{\underline{\upsilon}}^{\overline{\upsilon}} \left(\int_{\upsilon_2}^{\overline{\upsilon}} \upsilon_1 g(\upsilon_1)\, d\upsilon_1 + G(\upsilon_2)\, \upsilon_2 \right) g(\upsilon_2)\, d\upsilon_2, \tag{40}$$

which has the unique solution:

$$f' = \frac{-h(0)(c - \widehat{\upsilon}) + \frac{1}{4} + \sqrt{\left[h(0)(c - \widehat{\upsilon}) - \frac{1}{4}\right]^2 + 2h(0)(c - \widehat{\upsilon})}}{2h(0)}. \tag{41}$$

Replacing $f_1 = f_2 = f'$ in (34) defines n'. ■

[33] In Section 4.3 we assumed that $\underline{c} - E[s \mid 0, 0] > 0$.

Proof of Lemma 2

Proof. The conglomerates control 100% of the hash rate and thus jointly capture the governance of the blockchain, i.e., $z'' = \underline{z}$. The firms' profit functions are given by (12). Both firms choose pool fees f_1 and f_2 simultaneously. They also choose the equipment prices per hash rate, p_1 and p_2, simultaneously, subject to $\min\{p_1, p_2\} \leq c$. In the equipment market, firms compete for selling a homogenous good. From usual Bertrand competition reasoning, it follows that $p_1 = p_2 = \underline{c}$. From (10), it follows immediately that:

$$n(f_1, f_2) = \frac{\phi r}{\underline{c} - E[s^* \mid f_1, f_2]}. \tag{42}$$

We now show that $f_1'' = f_2'' = f''$. Using Result 1, the simplified first order conditions with respect to f_1 and f_2 are as follows:

$$f_1 h(f_1 - f_2) = (1 - H(f_1 - f_2) - \frac{f_1(1 - H(f_1 - f_2))^2}{\underline{c} - E[s \mid f_1, f_2]} \tag{43}$$

$$f_2 h(f_1 - f_2) = H(f_1 - f_2) - \frac{H(f_1 - f_2)^2 f_2}{\underline{c} - E[s \mid f_1, f_2]}. \tag{44}$$

Following the exact same steps as in the proof of Lemma 1, we find the unique solution:

$$f'' = \frac{-h(0)(\underline{c} - \widehat{v}) + \frac{1}{4} + \sqrt{\left[h(0)(\underline{c} - \widehat{v}) - \frac{1}{4}\right]^2 + 2h(0)(\underline{c} - \widehat{v})}}{2h(0)}. \tag{45}$$

Replacing $f_1 = f_2 = f''$ in (42) defines n''. ■

Proof of Lemma 3

Proof. Define $\pi(x) \equiv \phi \frac{0.5 f(x)}{x - \widehat{v} + f(x)}$, where $f(x)$ is given by

$$f(x) = \frac{-h(0)(x - \widehat{v}) + \frac{1}{4} + \sqrt{\left[h(0)(x - \widehat{v}) - \frac{1}{4}\right]^2 + 2h(0)(x - \widehat{v})}}{2h(0)},$$

and $\widehat{v}$ is given by (40). We start by proving that $\frac{\partial \pi}{\partial x} < 0$.

$$\frac{\partial \pi}{\partial x} = -\phi \frac{0.5}{(x - \widehat{v} + f(x))^2} \left[f(x) - (x - \widehat{v}) \frac{\partial f}{\partial x} \right] \tag{46}$$

where

$$\frac{\partial f}{\partial x}=\frac{-h\left(0\right)+\frac{h(0)^{2}(x-\widehat{v})+\frac{3}{4}h(0)}{\sqrt{\left[h(0)(x-\widehat{v})-\frac{1}{4}\right]^{2}+2h(0)(x-\widehat{v})}}}{2h\left(0\right)}. \tag{47}$$

We now find the sign of expression $f\left(x\right)-\left(x-\widehat{v}\right)\frac{\partial f}{\partial x}$:

$$f\left(x\right)-\left(x-\widehat{v}\right)\frac{\partial f}{\partial x}\Longleftrightarrow\frac{1}{2h(0)}\left(\frac{1}{4}+\frac{\frac{1}{4}^{2}+\frac{3}{4}h\left(0\right)\left(x-\widehat{v}\right)}{\sqrt{\left[h\left(0\right)\left(x-\widehat{v}\right)-\frac{1}{4}\right]^{2}+2h\left(0\right)\left(x-\widehat{v}\right)}}\right)>0. \tag{48}$$

Since $f\left(x\right)-\left(x-\widehat{v}\right)\frac{\partial f}{\partial x}>0$, it then follows that $\frac{\partial\pi}{\partial x}<0$.

For $\underline{\lambda}=\Delta r=0$, we have

$$\begin{aligned}\Pi_{j}^{\prime}\left(f^{\prime},f^{\prime}\right) &= r\pi\left(c\right) \\ \Pi_{j}^{''}\left(\underline{c},\underline{c},f^{\prime\prime},f^{\prime\prime}\right) &= r\pi\left(\underline{c}\right).\end{aligned} \tag{49}$$

From $\frac{\partial\pi}{\partial x}<0$ and $\underline{c}<c$, it then follows that $\Pi_{j}^{''}\left(\underline{c},\underline{c},f^{\prime\prime},f^{\prime\prime}\right)>\Pi_{j}^{\prime}\left(f^{\prime},f^{\prime}\right)$. ■

Proof of Lemma 4

Proof. Firms choose pool fees f_1 and f_2 simultaneously. The firms' profit functions (per unit of time) for $\Delta r=\Delta\lambda=0$ are

$$\Pi_{1}^{\prime\prime\prime}\left(p_{1},f_{1},f_{2}\right)=\phi r\frac{f_{1}\varphi_{1}\left(f_{1},f_{2}\right)+p_{1}-\underline{c}}{p_{1}-E\left[s^{*}\mid f_{1},f_{2}\right]}-\underline{\lambda}, \tag{50}$$

$$\Pi_{2}^{\prime\prime\prime}\left(p_{1},f_{1},f_{2}\right)=\phi r\frac{f_{2}\varphi_{2}\left(f_{1},f_{2}\right)}{p_{1}-E\left[s^{*}\mid f_{1},f_{2}\right]}, \tag{51}$$

A Nash equilibrium where firms choose fees simultaneously exists because the profit functions are continuous and fees belong to the compact set $[0,\overline{v}]$ (Glicksberg, 1952). For simplicity, we focus on equilibria in pure strategies, which can be shown to exist for a number of different functional form assumptions.

We first show that pure-strategy equilibria are always interior. As argued in the proof of Result 1, in any equilibrium, fees f_1 and f_2 are strictly lower lower than $\overline{v}$. To show that

fees must be greater than zero, write the simplified first-order condition for Firm 1 as:

$$\begin{aligned}&(c - E[s^* \mid f_1, f_2])(1 - H(f_1 - f_2)) = \\ &+f_1 h(f_1 - f_2)(c - E[s^* \mid f_1, f_2]) + [c - \underline{c} + f_1(1 - H(f_1 - f_2))](1 - H(f_1 - f_2)).\end{aligned} \tag{52}$$

For $f_1 = 0$, we have that

$$(\underline{c} - E[s^* \mid 0, f_2])(1 - H(0 - f_2)) > 0 \text{ for any } f_2 \in [0, \overline{v}], \tag{53}$$

which implies that Firm 1 can never choose $f_1 = 0$ in an equilibrium. Because $f_1 > 0$, $f_2 = 0$ is never a best response by Firm 2, as it leaves it with zero profit. Thus, in any pure-strategy equilibrium, fees are strictly positive. It follows that the first-order conditions must hold.

We now simplify the first-order conditions as follows:

$$f_1 h(f_1 - f_2) = 1 - H(f_1 - f_2) - \frac{[c - \underline{c} + f_1(1 - H(f_1 - f_2))](1 - H(f_1 - f_2))}{c - E[s^* \mid f_1, f_2]} \tag{54}$$

$$f_2 h(f_1 - f_2) = H(f_1 - f_2) - \frac{f_2 H(f_1 - f_2)^2}{c - E[s^* \mid f_1, f_2]}. \tag{55}$$

We subtract (55) from (54) and simplify:

$$(f_1 - f_2)\, h(f_1 - f_2) = (1 - 2H(f_1 - f_2) - \frac{(c - \underline{c})(1 - H(f_1 - f_2)) + (f_1 - f_2)\, H(f_1 - f_2)^2}{c - E[s^* \mid f_1, f_2]}, \tag{56}$$

or

$$\begin{aligned}&(f_1 - f_2)[h(f_1 - f_2)(c - E[s^* \mid f_1, f_2]) + (1 - H(f_1 - f_2))H(f_1 - f_2)] = \\ &\qquad (c - E[s^* \mid f_1, f_2])[1 - 2H(f_1 - f_2)) - (c - \underline{c})(1 - H(f_1 - f_2)].\end{aligned}$$

We replace $H(f_1 - f_2) = 0.5 + \epsilon$, where $\epsilon \in [-0.5, 0.5]$ and simplify (recall that $H(0) = 0.5$):

$$(f_1 - f_2)\left[h(f_1 - f_2)(c - E[s^* \mid f_1, f_2]) + (0.25 - \epsilon^2)\right] = -2\epsilon(c - E[s^* \mid f_1, f_2]) - (c - \underline{c})(0.5 - \epsilon) \tag{57}$$

If $f_1^* - f_2^* \geq 0$, we have that $\epsilon \geq 0$, that is, $H\left(f_1^* - f_2^*\right) \geq 0.5$. Since

$$h\left(f_1 - f_2\right)\left(c - E\left[s^* \mid f_1, f_2\right]\right) + \left(0.25 - \epsilon^2\right) > 0,$$

and since for $\epsilon \geq 0$ the right-hand side of equation (57) is negative, implying that $f_1^* - f_2^* < 0$, which is a contradiction. It thus follows that $f_1^* < f_2^*$ if both first-order conditions hold. ■

Proof of Lemma 5

Proof. Both firms choose pool fees f_1 and f_2 simultaneously. Firm 1 also chooses the equipment price per hash rate, p_1, subject to $p_1 \leq c$. Let $I_{f_1 \geq f_2} = 1$ if $f_1 \geq f_2$ and zero otherwise. The firms' profit functions (per unit of time) are given by (14).

First we prove that $p_1''' = c$.

$$\frac{\partial \Pi_1'''\left(p_1, f_1, f_2\right)}{\partial p_1} = \phi\left(r + I_{f_1 \geq f_2}\Delta r\right)\frac{\underline{c} - E\left[\upsilon \mid f_1, f_2\right] + H\left(f_1 - f_2\right) f_2}{\left(p_1 - E\left[s^* \mid f_1, f_2\right]\right)^2}. \tag{58}$$

Under the assumption that $\underline{c} - E\left[s \mid 0, 0\right] > 0$ (see Section 4.3), $\frac{\underline{c} - E[\upsilon|f_1, f_2] + H(f_1 - f_2) f_2}{(p_1 - E[s^*|f_1, f_2])^2} > 0$. This implies that Firm 1's profit is increasing in p_1 and thus the firm wants to choose the highest price possible, i.e., $p_1''' = c$. From (10), it then follows immediately that:

$$n\left(f_1, f_2\right) = \frac{\phi r\left(z'''\right)}{c - E\left[s^* \mid f_1, f_2\right]}. \tag{59}$$

We can rewrite the profits of Firm 1 and Firm 2 as follows

$$\Pi_1'''\left(c, f_1, f_2\right) = \left(r + I_{f_1 \geq f_2}\Delta r\right)\pi_1\left(f_1, f_2\right) - \underline{\lambda} - I_{f_1 \geq f_2}\Delta\lambda, \tag{60}$$

$$\Pi_2'''\left(c, f_1, f_2\right) = \left(r + I_{f_1 \geq f_2}\Delta r\right)\pi_2\left(f_1, f_2\right), \tag{61}$$

where

$$\pi_1\left(f_1, f_2\right) = \phi\frac{f_1\left(1 - H\left(f_1 - f_2\right)\right) + c - \underline{c}}{c - E\left[s^* \mid f_1, f_2\right]}, \tag{62}$$

and

$$\pi_2\left(f_1, f_2\right) = \phi\frac{f_2 H\left(f_1 - f_2\right)}{c - E\left[s^* \mid f_1, f_2\right]}. \tag{63}$$

Any equilibrium that implements proposal $\underline{z}$ must have $f_1''' < f_2'''$. Thus, we only need to show that an equilibrium that implements proposal $\overline{z}$ must be such that $f_1''' = f_2'''$. Consider

first a candidate equilibrium $f_1''' \geq f_2'''$ such that the following first-order conditions hold:

$$\frac{\partial \pi_1 \left(f_1''', f_2''' \right)}{\partial f_1} = 0 \tag{64}$$

$$\frac{\partial \pi_2 \left(f_1''', f_2''' \right)}{\partial f_2} = 0. \tag{65}$$

Lemma 4 implies that $f_1''' < f_2'''$ if both first-order conditions hold. Thus, if $f_1''' \geq f_2'''$, at least one first-order condition must not hold. Suppose that $f_1''' > f_2'''$. Then there is a profitable deviation for at least one of the two firms. To see this, note that if Firm 1's first-order condition does not hold in a candidate equilibrium, then the firm would want to increase or decrease its price by small $\varepsilon < f_1''' - f_2'''$, which would not change the outcome of the vote. The same logic applies to Firm 2. It follows that in an equilibrium where proposal $\overline{z}$ is implemented, we must have $f_1''' = f_2'''$. (In the proof of 2 we show the conditions for existence of equilibria with $f_1''' = f_2'''$ and with $f_1''' < f_2'''$).

Replacing $f_1 = f_1'''$ and $f_2 = f_2'''$ in 59 defines n'''. ■

Proof of Proposition 1

Proof. We derive necessary and sufficient conditions for the existence of equilibria with capture ($z''' = \underline{z}$) in Case (iii), i.e., the case where Firm 1 enters the pool and the equipment markets, while Firm 2 enters the pool market only. Capture occurs if and only if $f_1''' < f_2'''$.

Necessity. If $f_1''' < f_2'''$ holds in equilibrium, then f_1''' and f_2''' must be best responses to one another given the choice of $\underline{z}$, and thus satisfy (19) and (20).

While (19) and (20) guarantee that f_1''' and f_2''' are best responses to one another taking z as given, we also need to consider deviations that change z. For $z''' = \underline{z}$ to be an equilibrium, deviations – by either Firm 1 or Firm 2 – that lead to proposal $\overline{z}$ being adopted cannot to be profitable.

Define f_1^d as Firm 1's "best deviation" that implements $\overline{z}$:

$$f_1^d \in \arg \max_{f_1 \in \left[f_2''', \overline{v} \right]} \phi \frac{f_1 \left(1 - H(f_1 - f_2''') \right) + c - \underline{c}}{c - E \left[s^* \mid f_1, f_2''' \right]}. \tag{66}$$

Firm 1's best deviation yields profit $(r + \Delta r) \pi_1^d - \overline{\lambda}$, where π_1^d is defined in Proposition 1. This deviation is not (strictly) profitable if:

$$r \pi_1''' - \underline{\lambda} \geq (r + \Delta r) \pi_1^d - \overline{\lambda} \tag{67}$$

$$\iff \Delta\lambda \geq \Delta r \pi_1^d - r\left(\pi_1''' - \pi_1^d\right), \tag{68}$$

proving the necessity of condition (23).

Similarly, Firm 2's best deviation that implements implements $\overline{z}$ is

$$f_2^d \in \arg\max_{f_2 \in \left[0, f_1'''\right]} \phi \frac{f_2 H(f_1''' - f_2)}{c - E\left[s^* \mid f_1''', f_2\right]}. \tag{69}$$

Firm 2's best deviation yields profit $(r + \Delta r)\,\pi_2^d$, where π_2^d is defined in Proposition 1. This deviation is not (strictly) profitable if:

$$r\pi_2''' \geq (r + \Delta r)\,\pi_2^d \tag{70}$$

$$\Leftrightarrow 0 \geq \Delta r \pi_2^d - r\left(\pi_2''' - \pi_2^d\right), \tag{71}$$

proving the necessity of condition (24).

Sufficiency. If f_1''' and f_2''' are such that (19) and (20) hold, we know they are best responses to one another for a given z, and also that the first order conditions (64) and (65) must hold (because equilibrium must be interior, as shown in the proof of Lemma 4). We know from Lemma 4 that if (64) and (65) hold, we have that $f_1''' < f_2'''$. In addition, if (23) and (24) hold, f_1''' and f_2''' are globally best responses to one another, and thus constitute an equilibrium with capture. ■

Proof of Proposition 2

Proof. First, consider a candidate equilibrium (f_1''', f_2''') that satisfies conditions (19) and (20). Lemma 4 implies that $f_1''' < f_2'''$. For expositional simplicity, here we assume that an equilibrium with capture, when it exists, is unique in its class (i.e., there is no other set of fees that also constitutes an equilibrium with capture). This assumption is only to keep the notation burden low; the argument when multiple equilibria exist is exactly the same.[34]

Define

$$r_1 \equiv \max\left\{\frac{\Delta r \pi_1^d - \Delta\lambda}{\pi_1''' - \pi_1^d}, 0\right\} \tag{72}$$

and

$$r_2 \equiv \frac{\Delta r \pi_2^d}{\pi_2''' - \pi_2^d}. \tag{73}$$

[34] Our proof remains unchanged as long as the set of fees that satisfies (19) and (20) is finite.

Note that if $r \geq \max\{r_1, r_2\}$, both (23) and (24) hold. Proposition 1 then implies that, for $r \geq \max\{r_1, r_2\}$, (f_1''', f_2''') constitute an equilibrium with capture when there is only one conglomerate at Date 1.

To rule out equilibria without capture at Date 1, here we derive the conditions for the existence of such equilibria. In Case (iii), capture is avoided if $f_1 = f_2$. In that case, as shown in the proof of Lemma 5, the FOC of at least one of the two firms does not hold. There are two possible equilibria: *market monitoring equilibrium* and *competitor monitoring equilibrium*.

In a market monitoring equilibrium, consider a candidate equilibrium $f_1 = f_2 = f^m$ such that $\frac{\partial \pi_2}{\partial f_2} \mid_{f_1=f_2=f^m} = 0$, where $\pi_2(f_1, f_2)$ is defined in (63). Note that the fee for this candidate equilibrium is uniquely given by $f^m = f'$, as defined in (41). Note also that

$$\frac{\partial \pi_1(f_1, f_2)}{\partial f_1} \mid_{f_1=f_2=f'} = -(c - \underline{c})0.5 < 0 \tag{74}$$

(function $\pi_1(f_1, f_2)$ is defined in (62)). That is, Firm 1 would like to reduce its fee but refrains from doing so. For this to be an equilibrium, a deviation by Firm 1 which leads to proposal $\underline{z}$ being adopted should not be profitable. Define f_1^{dm} as Firm 1's "best deviation" that implements $\underline{z}$:

$$f_1^{dm} \in \arg\max_{f_1 \in [0,\overline{v}]} \pi_1(f_1, f'). \tag{75}$$

This deviation is not (strictly) profitable if:

$$(r + \Delta r)\pi_1(f', f') - \overline{\lambda} \geq r\pi_1\left(f_1^{dm}, f'\right) - \underline{\lambda} \tag{76}$$

$$\iff \Delta\lambda \leq \Delta r \pi_1(f', f') - r\left(\pi_1\left(f_1^{dm}, f'\right) - \pi_1(f', f')\right). \tag{77}$$

If condition (77) holds, an equilibrium with market monitoring exists: The conglomerate would like to reduce its fee but refrains from doing so to avoid the price impact of the proposal. Thus, market forces (i.e., the price impact) are sufficient to discipline the conglomerate and prevent governance capture.

In a competitor monitoring equilibrium, consider a candidate equilibrium $f_2 = f_1 = f^c$ such that

$$f^c \in \arg\max_{f_1 \in [f^c,\overline{v}]} \pi_1(f_1, f^c) \tag{78}$$

and

$$f^c \in \arg \max_{f_2 \in [0, f^c]} \pi_2 \left(f^c, f_2 \right). \tag{79}$$

These two conditions rule out deviations that would not change the voting outcome.

For $f_1 = f_2 = f^c$ to be an equilibrium: (i) a deviation by Firm 1 which leads to proposal $\underline{z}$ being adopted should not be profitable and (ii) a deviation by Firm 2 which leads to proposal $\underline{z}$ being adopted should not be profitable.

Define f_1^{dc} as Firm 1's "best deviation" that implements $\underline{z}$:

$$f_1^{dc} \in \arg \max_{f_1 \in [0, \overline{v}]} \pi_1 \left(f_1, f^c \right). \tag{80}$$

This deviation is not (strictly) profitable if:

$$\left(r + \Delta r \right) \pi_1 \left(f^c, f^c \right) - \overline{\lambda} \geq r \pi_1 \left(f_1^{dc}, f^c \right) - \underline{\lambda} \tag{81}$$

$$\iff \Delta \lambda \leq \Delta r \pi_1 \left(f^c, f^c \right) - r \left(\pi_1 \left(f_1^{dc}, f^c \right) - \pi_1 \left(f^c, f^c \right) \right) \tag{82}$$

Similarly, define f_2^{dc} as Firm 2's "best deviation" that implements $\underline{z}$:

$$f_2^{dc} \in \arg \max_{f_2 \in [0, \overline{v}]} \pi_2 \left(f^c, f_2 \right). \tag{83}$$

This deviation is not (strictly) profitable if:

$$\left(r + \Delta r \right) \pi_2 \left(f^c, f^c \right) \geq r \pi_2 \left(f^c, f_2^{dc} \right) \tag{84}$$

$$\iff \Delta r \pi_2 \left(f^c, f^c \right) \geq r \left(\pi_2 \left(f^c, f_2^{dc} \right) - \pi_2 \left(f^c, f^c \right) \right). \tag{85}$$

If conditions (82) and (85) hold, an equilibrium with competitor monitoring exists: The competitor (Firm 2) would like to increase its fee but refrains from doing so to prevent the conglomerate from becoming the largest pool and controlling the vote. The conglomerate also needs some self-discipline in this equilibrium: (82) is analogous to condition (77).

Now, define[35]

$$r_3 \equiv \max\left\{\frac{\Delta r \pi_1\left(f', f'\right) - \Delta\lambda}{\pi_1\left(f_1^{dm}, f'\right) - \pi_1\left(f', f'\right)}, 0\right\}, \tag{86}$$

$$r_4 \equiv \max\left\{\frac{\Delta r \pi_1\left(f^c, f^c\right) - \Delta\lambda}{\pi_1\left(f_1^{dc}, f^c\right) - \pi_1\left(f^c, f^c\right)}, 0\right\}, \tag{87}$$

and

$$r_5 \equiv \max \frac{\Delta r \pi_2\left(f^c, f^c\right)}{\pi_2\left(f^c, f_2^{dc}\right) - \pi_2\left(f^c, f^c\right)}. \tag{88}$$

Note that if $r > \max\left\{r_3, r_4, r_5\right\}$, neither market monitoring equilibrium or competitor monitoring equilibrium exists.

Now, if $r > \widehat{r} \equiv \max\left\{r_1, r_2, r_3, r_4, r_5\right\}$, when there is one conglomerate at Date 1, an equilibrium with capture exists while equilibria without capture do not exist. Thus, we have shown that $r > \widehat{r}$ is a sufficient condition for an equilibrium with capture to exist when there is only one conglomerate at Date 1. In addition, $r > \widehat{r}$ is also sufficient to rule out equilibria without capture in this case.

Now assume that $r > \widehat{r}$ and consider the entry decisions at Date 0. If Firm 2 expects Firm 1 to enter the equipment market, Firm 2 will also enter this market if and only if

$$r\phi \frac{H(0) f''}{\underline{c} - E\left[s^* \mid f'', f''\right]} - \underline{\lambda} \geq r\phi \frac{H(f_1''' - f_2''') f_2'''}{c - E\left[s^* \mid f_1''', f_2'''\right]} \tag{89}$$

$$\Leftrightarrow \underline{\lambda} \leq r\phi \left(\frac{0.5 f''}{\underline{c} - E\left[s^* \mid f'', f''\right]} - \frac{H(f_1''' - f_2''') f_2'''}{c - E\left[s^* \mid f_1''', f_2'''\right]}\right). \tag{90}$$

If condition (90) holds, both firms jointly capture the governance of the blockchain. Define $\widetilde{\lambda} \equiv r\phi\left(\frac{0.5 f''}{\underline{c} - E[s^* | f'', f'']} - \frac{H(f_1''' - f_2''') f_2'''}{c - E\left[s^* | f_1''', f_2'''\right]}\right)$. If $\underline{\lambda} \leq \widetilde{\lambda}$, then Firm 2's best response to Firm 1 entering the equipment market is also to enter this market. By symmetry, Firm 1 also wants to enter when Firm 2 enters. Thus, If $\underline{\lambda} \leq \widetilde{\lambda}$, an equilibrium in which both firms enter the equipment market exists.

[35] Again, for expositional simplicity only, we assume that f^c exists and is unique. If there are multiple f^c's, the argument below is unchanged, as long as we redefine the thresholds accordingly. If no f^c exists, the argument is simplified, as we do not need to consider this class of equilibrium.

If $\underline{\lambda} > \widetilde{\lambda}$, Firm 2 does not enter if it expects Firm 1 to enter. If Firm 1 expects Firm 2 not to enter the equipment market, Firm 1 will enter this market if and only if

$$\underline{\lambda} \leq \phi \left[r \frac{(1 - H(f_1''' - f_2'''))f_1''' + (c - \underline{c})}{c - E\left[s^* \mid f_1''', f_2'''\right]} - (r + \Delta r) \frac{0.5 f'}{c - E\left[s^* \mid f', f'\right]} \right]. \tag{91}$$

Let $\widehat{\lambda}' \equiv \phi \left[r \frac{(1 - H(f_1''' - f_2'''))f_1''' + (c - \underline{c})}{c - E\left[s^* | f_1''', f_2'''\right]} - (r + \Delta r) \frac{0.5 f'}{c - E[s^* | f', f']} \right]$. If $\underline{\lambda}$ is such that $\underline{\lambda} \geq \widetilde{\lambda}$ and $\underline{\lambda} \leq \widehat{\lambda}'$, one firm alone captures the governance of the blockchain.

To guarantee existence of equilibria with capture, we need to show that at least one of $\widehat{\lambda}'$ and $\widetilde{\lambda}$ is not strictly negative. If $\widetilde{\lambda} \geq 0$, equilibria in which both firms jointly capture the governance exist for all $\underline{\lambda} \leq \widetilde{\lambda}$. Suppose now that $\widetilde{\lambda} < 0$, i.e.,

$$\frac{0.5 f''}{\underline{c} - E\left[s^* \mid f'', f''\right]} < \frac{H(f_1''' - f_2''')f_2'''}{c - E\left[s^* \mid f_1''', f_2'''\right]}. \tag{92}$$

We now show that the following must hold:

$$\frac{(1 - H(f_1''' - f_2'''))f_1''' + (c - \underline{c})}{c - E\left[s^* \mid f_1''', f_2'''\right]} > \frac{0.5 f'}{c - E\left[s^* \mid f', f'\right]}. \tag{93}$$

We first need to prove that

$$\frac{H(f_1''' - f_2''')f_2'''}{c - E\left[s^* \mid f_1''', f_2'''\right]} \leq \frac{(1 - H(f_1''' - f_2'''))f_1''' + c - \underline{c}}{c - E\left[s^* \mid f_1''', f_2'''\right]}. \tag{94}$$

From the FOC (54), we obtain

$$\frac{(1 - H(f_1''' - f_2'''))f_1''' + c - \underline{c}}{c - E\left[s^* \mid f_1''', f_2'''\right]} = 1 - f_1''' \frac{h(f_1''' - f_2''')}{1 - H(f_1''' - f_2''')} \tag{95}$$

From the FOC (55), we obtain

$$\frac{H(f_1''' - f_2''')f_2'''}{c - E\left[s^* \mid f_1''', f_2'''\right]} = 1 - f_2''' \frac{h(f_1''' - f_2''')}{H(f_1''' - f_2''')} \tag{96}$$

Thus, if (94) does not hold, we have

$$1 - f_2''' \frac{h(f_1''' - f_2''')}{H(f_1''' - f_2''')} > 1 - f_1''' \frac{h(f_1''' - f_2''')}{1 - H(f_1''' - f_2''')} \tag{97}$$

$$f_2''' \frac{1}{H(f_1''' - f_2''')} < f_1''' \frac{1}{1 - H(f_1''' - f_2''')} \tag{98}$$

$$\frac{f_2'''}{f_1'''} < \frac{H(f_1''' - f_2''')}{1 - H(f_1''' - f_2''')} \tag{99}$$

Because

$$\frac{f_2'''}{f_1'''} > 1 \tag{100}$$

and

$$\frac{H(f_1''' - f_2''')}{1 - H(f_1''' - f_2''')} < 1, \tag{101}$$

then we have a contradiction, thus it must be that (94) holds.

From Lemma 3 we know that

$$\frac{0.5f''}{\underline{c} - E\left[s^* \mid f'', f''\right]} > \frac{0.5f'}{c - E\left[s^* \mid f', f'\right]}. \tag{102}$$

Thus (102) and (94) jointly imply that

$$\chi \equiv \frac{(1 - H(f_1''' - f_2'''))f_1''' + (c - \underline{c})}{c - E\left[s^* \mid f_1''', f_2'''\right]} - \frac{0.5f'}{c - E\left[s^* \mid f', f'\right]} > 0 \tag{103}$$

Define

$$r_6 = \frac{\Delta r}{\chi} \frac{0.5f'}{c - E\left[s^* \mid f', f'\right]} > 0 \tag{104}$$

Now, if $r > r_6$, we have that $\widehat{\lambda}' > 0$, thus an equilibrium with capture exists.

If Firm 1 expects Firm 2 not to enter the equipment market, Firm 1 will also not enter this market if and only if $\underline{\lambda} > \widehat{\lambda}'$. In that case no firm enters the equipment market and there is no capture of the governance of the blockchain.

To complete the proof, define $\widetilde{r} \equiv \max\{\widehat{r}, r_6\}$ and $\widehat{\lambda} \equiv \max\left\{\widehat{\lambda}', \widetilde{\lambda}\right\}$. ■

Proof of Proposition 3

Proof. Suppose there is an equilibrium with $f_2''' > f_1'''$, where f_1''' and f_2''' are given by (19) and (20). A necessary condition for such an equilibrium is that the coalition does not want to force its miners to coordinate and all choose Pool 2 instead. If (30) holds, then

the median voter in the coalition chooses Pool 1. Thus, the coalition will not coordinate its miners to switch to Pool 2. If condition (29) holds, even if the median voter in the coalition preferred that all miners switched to Pool 2, the coalition is not large enough to change the outcome of the vote. Thus, the coalition will not force some of its members to switch to Pool 2. ■

Table 1. Comparison of Mining Pools

Information from various Internet sources, as of April 2021.

	Mining Pools								
	AntPool	**BTC.com**	**F2Pool**	**Poolin**	**ViaBTC**	**Huobi.pool**	**OKExPool**	**BTC.TOP**	**Binance Pool**
Relationship with Bitmain	Fully-owned subsidiary	Fully-owned subsidiary	BitDeer partner	Founded by former Bitmain employees	Bitmain's associate company	Bitmain's strategic partner	Bitmain's strategic partner	BitDeer partner	Unrelated
Contracts offered (for BTC only)	PPS+, PPLNS, Solo	FPPS	PPS+	FPPS	PPS+, PPLNS, Solo	FPPS	FPPS	PPS	FPPS
Fees for BTC mining	4% for PPS+	1.5%	4%	2.5%	4.0% (PPS+)	Unknown	4%	Unknown	2.5%
Minimum threshold for payment (BTC)	0.001	0.005	0.001	0.005	0.01	Unknown	Unknown	0.01	Unknown
Server location	Asia	Asia, USA	Asia, USA	China, US, EU	Asia	Unknown	Unknown	Unknown	China, US, EU
Merged Mining coins	NMC, LTC, DOGE	NMC, RSK	NMC, SYS, DOGE	VCASH	NMC, SYS, EMC, ELA, DOGE	ELA	DOGE	Unknown	ELA, VCASH
Quality of information on website	Medium	Medium	Low	High	High	Low	Medium	No information	High
Fees available on website	No	No	No	Yes	Yes	No	No	No	Yes