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

October 2019

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. Our main result is that the proof-of-work system leads to a situation where the governance of the blockchain is captured by a large firm.

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

[*] We thank Benito Arruñada (discussant), Ulf Axelson, Will Cong, Giulio Fella, Peter Kondor, Igor Makarov, Jason Sturgess, Enrique Schroth (discussant), Kostas Zachariadis, and seminar participants at Carlos III, Bristol, U. of British Columbia, ESSEC, U. of Illinois at Urbana-Champaign, LSE, QMUL, and conference participants at the Barcelona GSE Summer Forum, EARIE (Barcelona), EFA (Lisbon), 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]

Bitcoin's founder Satoshi Nakamoto (2009) describes the need to trust intermediaries (such as banks) and central authorities (such as the central bank) as "*the root problem with conventional currency.*" The main motivation for the introduction of the Bitcoin blockchain was thus the creation of a "*system for electronic transactions without relying on trust*" (Nakamoto, 2008). A blockchain that does not rely on trust requires rules that can be enforced in a decentralized manner. As blockchain stakeholders' views about the adequacy of the existing rules evolve, these rules may change over time. Blockchains thus also 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., to stop using the blockchain). The largest blockchains adopt a voice mechanism that assigns more "votes" to those stakeholders with more computational power. Such a system is called *proof-of-work*: "*[proof-of-work] solves the problem of determining representation in majority decision making. (...) Proof-of-work is essentially one-CPU-one-vote*" (Nakamoto, 2008).

In this paper, we develop a theory of governance in proof-of-work blockchains.[2] We use the model to investigate the feasibility of governance without trust, as originally envisioned by Nakamoto. Our main result is that the proof-of-work system may lead to a situation where the governance of the blockchain is captured by a large corporate stakeholder.

In the proof-of-work system, players, called *miners*, enter a competition where a single winner is allowed to add a *block* (a set of transactions) to the chain. To win, a miner must solve a mathematical puzzle that requires significant computational power. The probability of a miner being the first to find a solution is proportional to the amount of computational power they allocate to the process of mining a block.

The proof-of-work system is more than just a mechanism for validating transactions. If there are two conflicting versions of the same blockchain, with each version having its

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

[2] Our focus is on permissionless blockchains (i.e., no permission is needed to join the blockchain in any role). For a discussion of governance in permissioned blockchains or public blockchains with permissioned record-keepers, see Chod and Lyandres (2018) and Cong, Li, and Wang (2019).

own set of rules, miners collectively "vote" for their preferred version by allocating their computational power to one of the chains. Typically, the chain with more computational power is the one more likely to win; the losing chain is either abandoned or rebranded as a separate blockchain.

If stakeholders such as users, merchants or exchanges disagree with the majority of miners, an option available to these stakeholders is to stop using this specific version of the blockchain. Thus, exit is also a governance mechanism. This mechanism has limitations. First, blockchain usage has network externalities: a blockchain is more valuable when there are more adopters.[3] Second, there are significant coordination issues, leading to multiple equilibria (Biais, Bisière, Bouvard, and Casamatta, 2019; Arruñada and Garicano, 2018). Stakeholders who consider exiting face a trade-off: they can either stay in an inefficient network or exit and risk coordination failures. Because exit is not a perfect governance mechanism, miners (who are the only ones with "votes") typically have significant influence on the governance of blockchains.

Nakamoto's vision of blockchain governance apparently did not anticipate that block mining would become a specialized activity. The emergence of mining as an important economic activity has led to the development of an ecosystem of industries that supply goods and services to miners. These goods and services providers are also stakeholders of the blockchain community, and they could affect the governance of the blockchain. They have economic interests to push for rules and protocols that increase demand for their products, raising their profitability.

In our model, we analyze the interactions between blockchain governance and the market structure of the industries in the mining ecosystem. Most mining is performed not by CPU, but by specialized equipment that uses *application-specific integrated circuits* (ASIC), which are chips designed to perform a single function: block mining. Examples of mining services include services sold by *mining pools,* which are essentially companies that sell insurance to miners, and *cloud mining*, through which miners can mine blocks without the need to own mining equipment.

The model is as follows. Mining requires computational power to generate tentative solutions to the mining puzzle. Each tentative solution is called a *hash.* By making ex ante investments in R&D, firms can develop the ability to produce specialized equipment that

[3] For an analysis of the limited adoption problem, see Hinzen, John, and Saleh (2019).

delivers more hashes per unit of time (*the hash rate*) than the existing available technology (e.g., CPU or GPU). Hash rate (which is a measure of computational power) is a homogeneous good. The combination of ex ante sunk R&D costs and a homogeneous good creates a first-mover advantage: A firm that enters early in this market is likely to remain as a profitable incumbent. Even a small entry cost may be sufficient to deter further entry (Stiglitz, McFadden, and Peltzman, 1987). The model thus implies that a single firm dominates the market for specialized mining equipment.

Mining pools offer differentiated services. Miners are heterogeneous in their preferences over mining pool attributes, and differentiated mining pools compete for miners by choosing fees. All else constant, lower pool fees leave more surplus to miners, making mining a more attractive activity, thus increasing demand for specialized mining equipment. That is, the equipment producer and the mining pools are "complementors," in the sense of Brandenburger and Nalebuff (1996). The equipment producer benefits from lower pool fees by selling more equipment. The equipment producer thus has incentives to "squeeze" the mining pools, that is, to take actions that would reduce profits in the pool services market (Farrell and Katz, 2000; Chen and Nalebuff, 2006).

We consider two types of profit squeezes. First, if the equipment producer already owns and operates a mining pool, it competes more aggressively with the other mining pools, resulting in a lower average fee in that market. Second, an equipment producer that does not own a mining pool has strong incentives to enter that market. In either case, the conclusion is that the equipment producer ends up controlling a large share of the mining pool services market. Mining pool managers typically decide how to allocate their pools' hash rate in case there are two competing versions of the blockchain. Thus, by acquiring a large share of the pool services market, the equipment producer has a disproportionate influence on the governance of the blockchain.

We show that the equipment producer has economic incentives to control a large share of hash rate even if there is no stakeholder disagreement about how the rules of the blockchain should change. That is, blockchain governance capture is a by-product of the equipment producer's incentives to squeeze the profits of the mining pools. If other stakeholders disagree with the equipment producer, the latter has an additional motive for acquiring control over votes: the equipment producer now wants to steer decisions towards its preferred direction. We show that, in this case, the equipment producer not only controls a large share of the mining pool services market but may also choose to *self-mine* (i.e., proprietary mining of blocks) in order to acquire a larger share of the votes. Interestingly, self-mining occurs in equilibrium even if the equipment producer has no comparative advantage at mining.

Our model fits the description of the Bitcoin mining ecosystem, where a dominant specialized equipment producer is also the largest player in the pool services market. Bitmain Technologies, a private Chinese (PRC) company, is the clear leader in the ASIC-based cryptocurrency mining hardware industry, with approximately 74.5% of the global market share (Bitmain Prospectus, 2018). Bitmain is also a large player in other segments of the crypto-mining ecosystem. Bitmain fully owns and operates two of the largest mining pools, Antpool and BTC.com, and is also the main investor in another large mining pool, ViaBTC.[4]

Large stakeholders face a trade-off between the value of their stake in the blockchain and the private benefits they extract from it. For example, an equipment producer is likely to oppose proposals that make the use of specialized mining equipment costlier. ASIC mining is less efficient in the Ethereum network precisely because stakeholders have supported upgrades that make ASIC mining more difficult. Consequently, for maximizing the social value of the blockchain, one cannot rely on a large stakeholder's private incentives.

There have been a number of instances when Bitmain has used its control over a substantial proportion of the hash rate 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, as the result of unresolved disagreements among members of the Bitcoin community concerning changes to the size of blocks. A few large players in the Bitcoin ecosystem, including the Bitmain-affiliated pool ViaBTC, sponsored the creation of the new currency, which shared the same history as Bitcoin but had a larger block size. In 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." Prices of both currencies fell steeply right after the split, as did the prices of Bitcoin and other cryptocurrencies. Blockchain splits are costly. Because of network externalities, splits may reduce the long-run value of a blockchain. In the short run, splits may negatively affect

[4] Figure 1 in the Appendix shows a snapshot of mining pool market shares in September 2018. For detailed evidence on the evolution of mining pool market shares, see Romiti, Judmayer, Zamyatin, and Haslhofer (2019).

the liquidity of a cryptocurrency, increasing volatility and hindering adoption.[5]

There is a growing theoretical literature on the economics of cryptomining. Budish (2018) shows that proof-of-work is a very costly system for sustaining trust; in order for honest behavior to be incentive compatible, the cost of an attack (which is a flow) has to be higher than the benefit from attacking the blockchain (which is a stock). Ma, Gans, and Tourky (2018) and Alsabah and Capponi (2019) analyze competition among miners in proof-of-work blockchains in which miners can invest in equipment through R&D. Huberman, Leshno and Moallemi (2017) and Easley, O'Hara, and Basu (2019) develop models of mining that can be used to determine the equilibrium value of Bitcoin transaction fees. Cong, He, and Li (2018) model how competition among pools affects equilibrium fees and pool sizes. Prat and Walter (2018) model miners' decision to invest in specialized equipment. We differ from this literature by modelling a mining ecosystem that includes miners, mining pools, and equipment producers. We also differ from the previous literature by focusing on the governance of blockchains.

Some previous theoretical work also focuses on the economic limitations of the blockchain technology. 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 be sustained in equilibrium. 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 (2018) study the effect of blockchain technologies on the way in which firms compete with one another. For surveys of the economic literature on blockchain, see Biais, Bisière, Bouvard, and Casamatta (2019b), Chen, Cong, and Xiao (2019), and Halaburda and Haeringer (2019).

Our paper incorporates some of the insights found in the industrial organization literature. 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

[5] For an analysis of the importance of liquidity in bitcoin trading, see Makarov and Schoar (2019), who show that bitcoin prices react strongly and persistently to order flows.

their market power in another market (Whinston, 1990; Carbajo, De Meza, and Seidmann, 1990; Nalebuff, 2004).

Our paper is also related to the theoretical literature on the impact of large shareholders on corporate governance, especially through intervention and voting. Examples include 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 (2019), and Edmans, Levit and Reilly (2019). See also Edmans (2014) for a review of this literature.

2. Institutional Details

Since the introduction of Nakamoto's (2008) version of blockchain technology, many different applications have been proposed, such as contracts and corporate record keeping (Yermack, 2017; Cong and He, 2018). To date, the most developed application of blockchain technology is Bitcoin, which is a virtual currency operating through a blockchain.

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 current ownership of each unit (or fraction) of bitcoin. When someone "spends" bitcoin, they send a message to some Bitcoin nodes (i.e., computers running Bitcoin software) notifying 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. Transactions are then broadcast to other connecting 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. Blocks are created by a particular type of nodes, called *miners*. Miners compete for the right to create a new block by using their computational power to try to solve a particular mathematical problem.

When a miner succeeds at solving the problem, it 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 for the mathematical problem. The miner then shares the newly created block with other full nodes (only some full nodes are miners); all full nodes are able to easily verify whether the solution is correct. When nodes receive a new valid block with the correct 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 installs a software that "implements" the Bitcoin protocol can use their computational power to "mine" blocks. Although entry in 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, 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.[6] Second, miners must pay for variable costs, among which electricity is the most important one. The mathematical problem is solved by brute force, implying that the probability of a miner being the first to find a solution is proportional to the amount of computational power – called the hash rate – they allocate to the process of mining a block relative to the total active hash rate in the Bitcoin mining network. The Bitcoin algorithm is constantly adjusted so that the average time for successfully mining a block is approximately ten minutes. The miner who wins the competition for mining the current block receives all transaction fees associated with the transactions in the block plus a fixed number of newly created bitcoins; in 2019, this number was 12.5 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 it. This system is thus called *proof-of-work*.

As cryptomining evolved into a specialized economic activity, a number of other goods

[6] Eghbali and Wattenhofer (2019) estimate that the market share of ASIC mining of bitcoins is essentially 100% since 2015.

[7] For studies focusing on Bitcoin transaction fees, see Huberman, Leshno and Moallemi (2017), Easley, O'Hara, and Basu (2019), and Lehar and Parlour (2019).

and services were created to support miners. The most important of these new activities is the provision of insurance to miners. Mining is a risky activity: miners pay up-front electricity, equipment and maintenance costs but are only rewarded (in cryptocurrencies) if they win the competition for 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 were created as an attempt to diversify the risks faced by small miners. Although the term "pool" suggests some form of cooperative arrangement, mining pools are best described as private firms that sell insurance to cryptominers. A miner who joins a mining pool directs his/her hash rate to the pool. Pools compensate their miners with fees proportional to the hash rate they provide. Pool managers then make the decisions concerning which blocks to mine. Pool owners make profits by retaining part of the rewards from successfully mined blocks.

Some firms also specialize in operating mining farms, which are large centers where mining equipment is stored and monitored. Mining farm operators act as custodians of third-parties' machines and usually operate and monitor the equipment. Finally, individuals can also engage in mining without even owning any equipment: cloud mining services allow anyone to rent equipment (which is stored in a mining farm) and mine cryptocurrencies.

At any given point in time there are multiple copies of the Bitcoin blockchain, and by design, conflicting versions of the blockchain will coexist. 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 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.

Bitcoin commentators often give the impression that the longest chain solution is a hard feature of Bitcoin. It is not; it is just a hypothesis. 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. Although many Bitcoin experts still deny that such splits can be long-lasting, recent evidence indicates that blockchain splits can be successful and command significant support among miners, such as 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.

A high degree of coordination is necessary for changing the core rules of Bitcoin – what is called the Bitcoin protocol. Anyone can propose a change in rules through a Bitcoin 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 say that a certain change requires the 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 important to keep in mind that this is again not a hard feature; it is possible for proposals to 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 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. Setup

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

3.1. Blockchain Governance

A blockchain may have many stakeholders. Stakeholders can be users, miners, or companies in the blockchain ecosystem, such as equipment producers or mining pools. Let l denote a generic blockchain stakeholder. At the end of each period, the blockchain network collectively chooses between two proposals (i.e., two chains), A and B, which represent two different sets of rules governing the blockchain. For example, A may be a proposal to increase the maximum block size, while B is the status quo. Each stakeholder has a preference for one of the two proposals; let $z_l \in \{A, B\}$ denote stakeholder l's preference. If stakeholder l's preferred proposal is chosen, they receive utility $b_l > 0$; otherwise they receive zero. Although we assume that the private benefit b_l is exogenous, in reality, such benefit could arise endogenously, for example, if the proposal refers to the adoption of a particular technology that benefits some types of stakeholders more than others.[8]

Stakeholders "vote" for a proposal by allocating *hash rate* (i.e., computational power) to one of the two chains. Let ε_l be the hash rate controlled by stakeholder l. 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. For simplicity, we assume that hash power is a continuous variable so that $\varepsilon_l \in \Re^+$ represents a mass of hash power.

We initially model the governance of the blockchain in reduced form; we assume that stakeholders' 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 stakeholder l, where n is the total mass of hash rate in the blockchain. The probability that stakeholder l's preferred proposal is implemented is $I\left(\varphi_l, \varphi_{-l}\right)$, where φ_{-l} is the vector of the hash rate shares controlled by all other stakeholders. We assume that this *influence function* is nondecreasing in φ_l, that is, a stakeholder who controls a larger share of the hash rate has (weakly) larger influence on the governance of the blockchain. Given $I\left(\varphi_l, \varphi_{-l}\right)$, l's expected payoff from the choice of proposals is $b_l I\left(\varphi_l, \varphi_{-l}\right)$. We choose to model the decentralized governance system in reduced form for expositional simplicity only. In Section 5, we provide a full microfoundation for the influence function $I\left(\varphi_l, \varphi_{-l}\right)$.[9]

[8] For example, there have been proposals to make blockchains such as Ethereum "ASIC-proof." It is in the interest of ASIC producers to vote against such proposals.

[9] Our approach here resembles that of Becker (1985), who models political influence by means of a reduced-form influence function.

3.2. Miners

To model the behavior of miners, we use an off-the-shelf model of bitcoin mining (here, we follow Budish (2018)). A period is defined as the time it takes to mine a block.[10] At the beginning of each period, miner i rents mass n_i of hash rate that allows them to try to mine a block. Miners need equipment. Let $p > 0$ denote the per period rental cost of the equipment per unit mass of hash rate.

Let s_i denote miner i's direct surplus from mining per unit mass of hash rate, including nonpecuniary benefits (e.g., speculative beliefs, preferences for gambling, risk aversion) minus electricity and other costs. The net direct surplus s_i excludes the rental cost of the equipment. Let r denote the reward to the miner who wins the mining competition; if miner i supplies n_i units of hash rate, their probability of winning the reward is $\frac{n_i}{n}$, where n is the total hash rate in the blockchain. We represent the period payoff of an active individual miner by[11]

$$U_i = \left(\frac{r}{n} - p + s_i\right) n_i + b_i I\left(\varphi_i, \varphi_{-i}\right). \tag{1}$$

3.3. Equipment Producers

A general-purpose mining equipment (i.e., a CPU/GPU chip) exists and its rental price 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 are endowed with a technology to produce mining equipment at a constant unit cost $\underline{c} < c$. This equipment – also called an application-specific integrated circuit (ASIC) – is specific to mining some particular cryptocurrencies and cannot be used for any other purpose.

There are K potential equipment producers, indexed by $k \in \{1, ..., K\}$. Let n'_k denote the amount of computational power per period sold by Firm k to individual miners and let n_k denote the amount of computational power used by Firm k for self-mining. Firm k's payoff from self-mining per unit of computational power (i.e., hash rate) is:

$$U_k = \left(\frac{r}{n} - \underline{c} + \sigma_k\right) n_k + b_k I\left(\varphi_k, \varphi_{-k}\right), \tag{2}$$

[10] We assume that the level of difficulty does not change throughout the period.

[11] For tractability, we assume that utility is linear in the expected reward; heterogeneity in risk preferences is captured in reduced form by s_i.

where σ_k is Firm k's net direct surplus from mining.

The total utility of an equipment producer that both self-mines and sells n'_k of equipment at price p is thus

$$\pi_k = (p - \underline{c})n'_k + U_k. \tag{3}$$

Let $t \in \{0, 1, 2, ..., \infty\}$ denote a mining period. At $t = 0$, there are no incumbents in the market for specialized mining equipment. At $t = k$, exactly one firm – Firm k – has the option to enter this market by paying an once-and-for-all sunk cost ι. That is, Firm k has a first-mover advantage with respect to all firms such that $k' > k$. In particular Firm 1 has a first-mover advantage over all other firms.

3.4. Mining Pools

We now introduce a third type of stakeholder: Mining pools. Pools are profit-maximizing firms that offer services to miners and charge fees. 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.

Why would individual miners join mining pools? The most obvious service that mining pools offer is insurance. In one typical contract (*pay-per-share*), miners received a regular income proportional to their supplied hash rate, independently of whether the pool succeeds at wining the tournament. In another 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. There are many other methods of payment; mining pools tend to specialize and offer only a small subset of those. Mining pools also differentiate themselves in a number of additional attributes, such as user interface, the possibility of merge mining, location, technical specifications, customer service, reputation, mode of voting, etc.

Here, 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 differentiated mining pools compete for miners by choosing fees. At each mining period t, let v_{ij} denote i's valuation of the unique combination of attributes offered by pool j.[12] Let f_j denote the fee charged by pool j. For each miner i, their surplus from

[12] Valuation v_{ij} includes, among other things, i's preferences for different methods of payments, perhaps because of heterogeneity in liquidity and risk preferences.

joining pool j is thus

$$s_{ij} = v_{ij} - f_j. \tag{4}$$

We assume that miners do not know their exact valuation v_{ij} before deciding whether to enter the mining market. To consider the simplest possible scenario, we assume that, for a given pool, valuations are independent and identically distributed, with density function $g(v)$ over the support $[\underline{v}, \overline{v}]$, with $\underline{v} > 0$, $\overline{v}$ finite, cdf $G(\cdot)$ and mean μ.

When choosing between proposals at the end of the period, each mining pool has the right to vote on behalf of all members of their pool. However, in practice pool managers may have limited influence on the votes in their current pools, either because pools may offer miners the option to express their preferences (e.g., as is case with Slushpool) or because miners may withdraw their hash rate if they disagree with the direction proposed by their mining pool manager. We assume that pool managers have control over a fraction $\alpha \in \left(0, \frac{1}{2}\right)$ of the votes in their pools; a fraction $(1 - \alpha)$ of the votes in a pool are controlled by the individual miners. One interpretation is that α measures the proportion of stakeholders who are indifferent towards voting, possibly because they are indifferent between the two proposals (i.e., if $b_i \to 0$) or because they understand they cannot affect the outcome of the vote (i.e., they know they are not pivotal). We assume that α is less than $\frac{1}{2}$ to make sure that no mining pool can control more than 50% of the votes. This assumption is immaterial for the qualitative results we derive.

Let m_j denote the amount of hash power directed to pool j. Pool j's (per period) utility is thus

$$\Pi_j = f_j m_j + b_j I\left(\varphi_j, \varphi_{-j}\right), \tag{5}$$

where $\varphi_j = \frac{\alpha m_j}{n}$.

4. Economic Incentives for Governance Capture

In this section, we solve for the equilibrium of the game played by all blockchain ecosystem stakeholders. We are interested in understanding how their pure economic motives may lead to concentration of voting power. Thus, in this section we assume that private benefits of control are zero for everyone.

4.1. Equipment Market Equilibrium

Here, we consider the decisions of equipment producers concerning entry, quantities and prices. For now, we assume that equipment producers are single-business companies. Later in Subsection 4.2, we allow equipment producers to diversify and become mining pool operators.

4.1.1. Single Equipment Producer

To study the equilibrium in this market, we work backwards: we first solve for the equilibrium taking as given a particular market structure (single versus multiple producers), and then we analyze the decision to enter into market.

Suppose there is a single incumbent equipment producer – Firm k – at time $t \geq k$. We assume that miners learn about their mining surplus only after they rent equipment and commit to enter. Let s denote the miners' ex ante (i.e., pre-entry) expectation of s_i and σ denote the equipment producer's ex ante expectation of σ_k. We assume that $\underline{c} > \max\{s, \sigma\}$. Without this condition, miners may wish to mine even for negative expected rewards, leading to infinite demand for hash rate and no equilibrium.

The overall hash rate is $n_k + n'_k$, where n_k is mass of hash rate used by Firm k for self-mining and n'_k is the hash rate of all other miners.[13] The equipment producer chooses a price p per unit of hash rate produced by its machines. Individual miners will rent the specialized equipment only if $p \leq c$, otherwise they prefer to rent the cheaper generic equipment. From (1), miner i's (pre-entry) expected payoff is (recall that $b_i = 0$ in this section)

$$E\left(U_i\right) = \left(\frac{r}{n_k + n'_k} - \min\{p, c\} + s\right) n_i. \tag{6}$$

Assuming free entry of miners, miners will supply more hash rate unless $E\left(U_i\right) \leq 0$. Thus, in equilibrium, either $E\left(U_i\right) = 0$, in which case individual miners supply a positive amount of hash rate, or $E\left(U_i\right) < 0$, in which case Firm k is the only miner.

Note that if $p > c$, then p does not affect the entry condition for individual miners, because they would not buy equipment from Firm k. Thus, without loss of generality, we assume that the equipment producer will not choose $p > c$. With this simplification, we can

[13] This already anticipates the result that all miners will use specialized equipment in equilibrium and will thus buy equipment from the single producer. This result follows immediately from the assumption that $c > \underline{c}$.

write the equipment producer's problem as

$$\max_{p,n_k,n'_k} (p-\underline{c})n'_k + \left(\frac{r}{n_k+n'_k} - \underline{c} + \sigma\right) n_k, \tag{7}$$

subject to

$$\begin{align}
\frac{r}{n_k+n'_k} - \min\{p,c\} + s &\leq 0 \tag{8}\\
p &\leq c \tag{9}\\
n_k, n'_k &\geq 0. \tag{10}
\end{align}$$

The producer's profit contains two terms: the profit from selling equipment (if any) and the profit from self-mining. The next proposition characterizes the equilibrium in this market when there is a single equipment producer.

Proposition 1 *The optimal price is $p^* = c$. There are three cases:*

1. *If $\sigma < s$, then $n'^*_k = \frac{r}{c-s}$ and $n^*_k = 0$.*
2. *If $\sigma > s$, then $n'^*_k = 0$ and $n^*_k = \frac{r}{c-s}$.*
3. *If $\sigma = s$, then any $n_k^{'*}$ and n^*_k such that $n^*_k + n'^*_k = \frac{r}{c-s}$ is a solution.*

This proposition illustrates three key results. First, the optimal price is c. The equipment producer would like to sell few units of computational power at a very high price because miners impose an externality on one another, and thus, the total surplus decreases with the amount of hash rate supplied. However, the producer cannot charge a price that is higher than the next-best alternative, which is priced at c. Second, the equipment producer self-mines only if $\sigma > s$ because whoever has a (nontransferable) comparative advantage at mining (i.e., the party with higher net direct surplus) does all the mining. Third, the total hash rate is always determined by the entry condition for individual miners, even when the equipment producer is the sole miner.

Proposition 1 implies that to focus on the case in which producers sell most of their equipment (as in the case of Bitmain), we need to assume $\sigma < s$. In the next subsection, we show that when $\sigma < s$, only one firm will enter the market for specialized equipment. This firm will then behave as in Part 1 of Proposition 1. In Subsection 4.2, we present our main results assuming a single equipment producer. Readers may skip to that subsection without any loss in continuity.

4.1.2. Competition among Equipment Producers

We now consider the case of multiple incumbent equipment producers. For simplicity, we assume that there are only two incumbent firms (call them k and z); the extension to more than two firms is straightforward. If the equipment producers sell to individual miners, they compete with one another by setting prices. If they self-mine, ex ante, both of them expect the same net direct surplus σ.

Proposition 2 *There are three cases:*

1. *If $\sigma < s$, then $n_k'^* + n_z'^* > 0$ and $n_k^* = n_z^* = 0$; both firms have zero profit.*
2. *If $\sigma > s$, then $n_k'^* = n_z'^* = 0$ and $n_k^* = n_z^* > 0$; both firms enjoy positive profits.*
3. *If $\sigma = s$, then there are multiple equilibria, such that if $n_k'^* + n_z'^* > 0$, profits are zero, and if $n_k'^* + n_z'^* = 0$, profits are strictly positive.*

In Case 1, the equipment firms have no special advantage at mining; thus, in equilibrium, both of them sell all of their equipment. Because they compete by setting prices, in equilibrium, prices must equal marginal cost, and thus profits are zero. In Case 2, the equipment firms enjoy larger direct surplus than individual miners; thus, in equilibrium, both firms self-mine and do not sell equipment to individual miners. The equipment firms compete with one another by setting quantities, and thus, they enjoy positive profits in equilibrium.[14] Note also that in any equilibrium in which the amount of computational power sold is strictly positive, profits are zero for both firms and $\sigma \leq s$.

We now consider the decision to enter into the mining equipment market. We have the following result:

Proposition 3 *In any equilibrium with a positive number of individual miners, at most one specialized equipment producer enters the market.*

[14] Dimitri (2017) models competition among nonatomistic miners as Cournot competition and shows that miners have positive profits in equilibrium. See also Alsabah and Capponi (2019) for a model where equipment producers compete by choosing their hash rates for self-mining.

The intuition is as follows. Because the specialized equipment is a homogeneous good, price competition drives profits to zero. Unless a firm expects to have positive profits in this market, it will not pay a positive sunk cost to enter. Thus, the firm with a first-mover advantage is the only one that could enter the market in equilibrium (as in Stiglitz, McFadden, and Peltzman, 1987).

For the remainder of the paper, we assume that the equipment producer does not have a comparative advantage in mining; that is, we set $\sigma < s$. From Proposition 2, if there are two incumbent producers, there is a positive number of individual miners and profits are zero. Proposition 3 thus implies that there is only one incumbent equipment producer in equilibrium. From Proposition 1, we then have that the equipment producer does not self-mine.

4.1.3. Mining with Specialized Equipment: Summary

The model in this section illustrates a number of interesting features of the game played between equipment producers and individual miners. It is useful to summarize its main lessons:

(i) Because ASIC chips are essentially a homogeneous good, even a very small sunk cost could prevent entry when there already is an incumbent, thus naturally leading to a structure with a single first-mover incumbent that makes positive profits.[15] This is in line with the observed market structure in the Bitcoin ecosystem: the leading cryptocurrency mining ASIC producer – Bitmain Technologies – has approximately 74.5% of the market for specialized equipment. Bitmain entered this market early in 2013; all of its current competitors entered the market more recently than Bitmain and are all very small.

(ii) The producer of specialized equipment will charge as much as the next best alternative (e.g., GPU) for each unit of computational power, thus extracting from miners all the surplus created by its more efficient equipment. The equipment producer is a constrained monopolist. If it were unconstrained, it would always like to sell fewer machines at higher prices.

(iii) The equilibrium amount of computational power (i.e., the hash rate used for mining) is the same with or without the specialized equipment. Thus, the deadweight cost from mining is lower in an equilibrium with specialized equipment.

[15] In practice, the most important source of fixed costs for an ASIC producer is investment in R&D. For example, in 2018, approximately 32% of Bitmain's employees were full-time engineers in research and development.

(iv) A specialized equipment producer has a comparative advantage at mining in the sense that it faces lower equipment costs than individual miners. However, this comparative advantage is transferable: miners can buy (or rent) the more efficient equipment from the producer. Thus, this type of comparative advantage does not affect the identity of the miners. Comparative advantages that are nontransferable (i.e., reflected in s and σ, such as local electricity costs) determine who becomes a miner.[16]

4.2. Equilibrium with Mining Pools

4.2.1. Competition among Mining Pools

For simplicity, we only consider the case in which there are at most two mining pools; the case with multiple mining pools is conceptually similar. We first assume that there are two incumbent mining pools and one of the mining pools is fully owned by a single equipment producer, which we call Pool 1. Later, in Subsection 4.2.2, we analyze players' decisions to enter the mining pool business, including the equipment producer's decision to enter this market.

For each period t, the timeline of actions is as follows.

Date 1: Pools choose their fees, f_1 and f_2, simultaneously.

Date 2: Miners enter the mining market and rent hash rate from the producer at price c (see Proposition 1).

Date 3: Miners learn their υ_{ij} and then choose which pool to join.

Date 4: Voting on proposals occurs and payoffs are realized.

To solve for the equilibrium, let us first consider a candidate equilibrium with a pair of fees (f_1^*, f_2^*). At Date 4, let $\varphi_j(f_1^*, f_2^*)$, $j = 1, 2$, denote the equilibrium proportion of hash rate controlled by Pool j. Pool 1's influence on the voting outcome is measured by $I(f_1^*, f_2^*) \equiv I(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*))$.

At Date 3, after miner i discovers υ_{ij} for each pool $j \in \{1, 2\}$, the miner chooses which pool to join. We assume that $\underline{\upsilon}$ is sufficiently high so that, in equilibrium, a miner always prefers one of the two pools to mining without a pool; that is, the market is fully served by

[16] With cloud mining, even comparative advantages in electricity costs are transferable.

the two pools.[17] Thus, miner i's net direct surplus from mining at Date 3 is given by:

$$s_i^* = \max_{j\in\{1,2\}} \upsilon_{ij} - f_j. \tag{11}$$

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

At Date 2, miners do not yet know their types; thus, they also do not know which fees they would pay after entry. The probability that miner i will choose Pool 1 over Pool 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 $[-\left(\overline{\upsilon} - \underline{\upsilon}\right), \left(\overline{\upsilon} - \underline{\upsilon}\right)]$. Let $H(.)$ denote the cumulative distribution function for $\upsilon_{i1} - \upsilon_{i2}$ (note that $H(0) = 0.5$).

At Date 2, let s denote the expectation of s_i^* as defined in (11). Because all miners are identical at this date, $s = \mu - E[f^*]$, where

$$E[f^*] \equiv f_1^* \left(1 - H(f_1^* - f_2^*)\right) + f_2^* H(f_1^* - f_2^*). \tag{12}$$

Note that, in equilibrium, Pool 1's market share is $1 - H(f_1^* - f_2^*)$. This implies that $\varphi_1\left(f_1^*, f_2^*\right) = \alpha\left[1 - H(f_1^* - f_2^*)\right]$ and $\varphi_2\left(f_1^*, f_2^*\right) = \alpha H(f_1^* - f_2^*)$.

As mentioned before, because we want to focus on the case in which the equipment producer does not have a comparative advantage at mining, we assume that $\sigma < s$; Proposition 1 then implies that there is no self-mining in equilibrium ($n_1 = 0$) and $p = c$. The equilibrium hash rate $n_1' = n^*$ is determined by the free entry condition as in (8):

$$n^* = \frac{r}{c - \mu + E[f^*]}. \tag{13}$$

At Date 1, mining pools anticipate the behavior of miners as given in (13) and choose fees simultaneously to maximize their profits. Pools' problem is to

$$\max_{f_1} \Pi_1\left(f_1, f_2\right) + \pi\left(f_1, f_2\right) = \frac{r f_1\left(1 - H(f_1 - f_2)\right)}{c - \mu + e\left(f_1, f_2\right)} + \frac{r\left(c - \underline{c}\right)}{c - \mu + e\left(f_1, f_2\right)}, \tag{14}$$

[17] For example, it can be shown that if fees are strategic complements, a sufficient condition for the miners never to mine alone is $\underline{\upsilon} g\left(\underline{\upsilon}\right)\left(c - \mu + \underline{\upsilon}\right) \geq c - \mu$.

$$\max_{f_2} \Pi_2 \left(f_1, f_2\right) = \frac{r f_2 H(f_1 - f_2)}{c - \mu + e\left(f_1, f_2\right)}, \tag{15}$$

where

$$e\left(f_1, f_2\right) \equiv f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2). \tag{16}$$

The next proposition presents our main result:

Proposition 4 *In any equilibrium, the equipment producer is the stakeholder with the greatest influence on the governance of the blockchain.*

This proposition shows that when the equipment producer owns a mining pool, it offers the lower fee and its pool is larger than the pool of its competitor. Because the equipment producer has the largest market share, it is the player with the greatest influence on the governance of the blockchain.

Intuitively, this result arises because the equipment producer benefits more from offering low fees than does an independent pool. Lowering fees has three positive effects: (i) it allows the firm lowering the fee to acquire a larger share of the pool market, (ii) it increases the overall demand for pool services, and (iii) it increases the demand for equipment. Only the equipment producer internalizes (iii); thus, it will choose lower fees than its competitor. Thus, the producer has incentives to squeeze the profits in the pool market.

Because we assume that mining pool managers derive no private benefits from the adoption of specific proposals, this proposition implies that blockchain governance capture is a by-product of the equipment producer's economic incentives to squeeze the profits of the mining pools.

Proposition 4 shows that market power in the market for mining equipment spills over to the market for mining services. Conditional on being an incumbent in the pool market, the equipment producer always operates the largest mining pool. If the equipment producer is not an incumbent in the pool market, it will have strong incentives to enter this market, as we show in the next subsection.

Proposition 4 also holds in more general settings. Under reasonable assumptions, the result that the equipment producer operates the largest mining pool can be extended to cases with different functional forms; see the analysis in the Appendix.

4.2.2. Entry in the Mining Pool Market

We now consider the entry decision in the mining pool market. We start at some time t when there is only one incumbent firm in the mining pool market. This firm is an independent mining pool.

At period t, we slightly modify the timeline to allow for entry:

Date 0: There is one incumbent mining pool. A second pool can enter this market by paying a once-and-for-all sunk cost κ.

Date 1: Pools choose their fees simultaneously.

Date 2: Miners enter the mining market and rent hash rate from the producer at price c.

Date 3: Miners learn their υ_{ij} and then choose which pool to join.

Date 4: Voting on proposals occurs, and payoffs are realized.

To simplify the analysis, here, we assume that only one firm may enter at time t and, if it does, no other firm may enter in subsequent periods. The potential entrant is either the equipment producer or an independent pool.

We assume that there are two ownership structures upon entry. The choice between the two ownership structures is only relevant for the equipment producer. The first ownership structure is such that the equipment producer firm has full control rights and cash flow rights over the pool. In the second ownership structure, the equipment producer has full cash flow rights but no control rights over the pool. If it enters with full control rights, the equipment producer will set fees as in (14); that is, it internalizes the effect of the fees on the mining equipment profit. If instead it enters without control rights, the pool manager maximizes profits in the pool market only, without taking into account any side effects on the equipment market, in which case both pools will have the same size.[18]

The option to choose between the two different modes of entry matters. In the previous section, we have only considered the more natural case in which the equipment producer has full control rights over the choices made by its pool. In some cases, however, the producer may prefer not to have control over fees, as we show in the next proposition:

[18] Entering without control is a realistic possibility. For example, Bitmain Technologies is the largest financial investor in ViaBTC pool, but control rights are concentrated in the hands of a few owners not related to Bitmain.

Proposition 5 *The equipment producer may be better off entering the pool market without control over fees than entering with control over fees.*

To understand the intuition, suppose that the equipment producer can set the prices of its own pool. Because the producer has incentives to squeeze the profits of the other pool, the producer will choose a price that is lower than the price chosen by an independently managed pool. However, this lower price leads to losses for the equipment producer in the pool market; that is, the producer "self-squeezes" its own profit. If the loss in the pool business is too large, the equipment producer may prefer to commit to choosing a higher pool fee. Entering without control is a way of making such a commitment.[19]

The possibility demonstrated by Proposition 5 is, however, unlikely to be of practical importance if private benefits are large. This is because by entering the pool market without controlling the mining pool, the equipment producer would also surrender its right to vote on proposals. If such rights are sufficiently valuable, the equipment producer would always prefer to enter with control rights.

We now make the following assumption:

Assumption 1 *Competition lowers prices:*

$$(c-\mu)\left(\frac{1}{h(0)}-2\underline{\upsilon}\right)<\underline{\upsilon}\left(2\underline{\upsilon}-\frac{1}{2}\right). \tag{17}$$

Condition (17) is necessary and sufficient for equilibrium fees to fall after the entry of a new pool. Alternatively, we could have assumed that the parameters are such that pool fees are strategic complements, which is a sufficient (but not necessary) condition for competition to lower prices. However, strategic complementarity is a stronger assumption than condition (17); thus, our results hold even in the absence of strategic complementarity.

Proposition 6 *If condition (17) holds, the equipment producer has stronger incentives to enter the mining pool market than does an independently owned pool.*

This proposition shows that, as long as more competition implies lower prices, for any constellation of parameters for which an independent firm finds it profitable to enter the pool

[19] Gawer and Henderson (2007) study Intel's use of organizational structure and processes as a means to commit not to squeeze the profits of independent suppliers and thus induce efficient R&D investment in the complementary goods.

market, the equipment producer also profits from entering this market. There are parameter values for which only the equipment producer profits from entering.[20]

The intuition for Proposition 6 is as follows. If Assumption 1 holds, entry by any type of firm reduces the average fee, thus increasing the demand for mining equipment. Only the equipment producer internalizes this effect, and thus, the producer is willing to absorb lower profits in the pool market.

In the proof of Proposition 6, we show that the equipment producer's incentive to enter relative to an independent entrant is

$$RI \equiv r\left(c-\underline{c}\right)\frac{f^0-f^*}{\left(c-\mu+f^*\right)\left(c-\mu+f^0\right)}>0,$$

where f^0 is the equilibrium fee without entry and f^* is the equilibrium fee after entry by an independent firm. We also show that f^0 and f^* are independent of r and $\underline{c}$.

We thus have the following comparative statics:

Result 1 *The equipment producer has stronger incentives to enter when it is more efficient (i.e., lower $\underline{c}$):*

$$\frac{\partial RI}{\partial \underline{c}}=-\frac{f^0-f^*}{\left(c-\mu+f^*\right)\left(c-\mu+f^0\right)}<0$$

Result 2 *The equipment producer has stronger incentives to enter when mining rewards are higher (i.e., higher r).*

$$\frac{\partial RI}{\partial r}=\left(c-\underline{c}\right)\frac{f^0-f^*}{\left(c-\mu+f^*\right)\left(c-\mu+f^0\right)}>0$$

These two results show that the equipment producer's incentives to enter the pool market become stronger as the equipment producer becomes more efficient (lower $\underline{c}$) and as the blockchain becomes more successful, that is, as crypto prices increase (higher r). Our model thus predicts that corporate capture of governance is more likely in more valuable blockchains.

[20] The analysis so far assumes that there is an incumbent equipment producer that can also enter the mining pool market. This option to enter does not affect the equilibrium in the equipment market as described in Subsection 4.1. In particular, there will be at most one equipment producer entering the market. This producer's entry condition is slightly modified to take into account the option value of entering the pool market at some future date.

5. Governance Capture with Private Benefits

We now consider the case in which private benefits are non-zero. Our goal is to derive the conditions under which Proposition 4 holds with positive private benefits.

5.1. Voting on Proposals

In this subsection, we provide an explicit model of voting on proposals. This model is meant as a microfoundation for the influence function $I\left(\varphi_l, \varphi_{-l}\right)$ introduced in Subsection 3.1.

We assume that proposals are chosen by a majority rule, in which only active miners can vote. In practice, "voting" occurs by miners directing their hash rate to one of the two competing chains; here, we assume that the minority chain is abandoned.[21] The aggregate distribution of miners' preferences over proposals is unknown until Date 4, when voting happens. Let ρ denote the proportion of stakeholders such that $z_l = A$. For simplicity only, we assume that ρ is uniformly distributed over the support $[0, 1]$. That is, at each period t, a new ρ is independently drawn from a uniform distribution. The realized value of ρ is never directly revealed, but it might be inferred ex post from the voting outcome.

We first consider a fully decentralized benchmark; that is, there are only individual miners and no mining pools. Let n be the mass of computational power. For simplicity, we assume that the number of miners is sufficiently large that we may think of each miner as having measure zero (alternatively, we could assume that there is a continuum of mass n of miners). A consequence of this assumption is that individual miners understand that they cannot affect the outcome of the vote, and thus, their decision to enter the mining market is independent of their private benefits. We therefore assume that active miners are drawn randomly from the population of stakeholders. By the Law of Large Numbers, the mass of miners such that $z_i = A$ is also ρ. Because of majority voting, and assuming that all active miners vote according to their preferences, proposal A is chosen only if $\rho \geq \frac{1}{2}$.

We proceed in three steps. First, we take market shares as given and solve for the voting game. Second, we endogenize market shares as in Section 4.2. Finally, we also consider the case in which the equipment producer may find it optimal to self-mine.

[21] In reality, if no chain is abandoned, then a blockchain splits into two new chains.

5.2. Exogenous Market Shares

As in Section 4.2, there are two incumbent mining pools: Pool 1, which is owned by the equipment producer, and Pool 2, which is an independent pool. In this subsection, we take market shares as exogenously given.

Let $1-H$ denote Pool 1's market share and H denote Pool 2's market share. Thus, the votes controlled by Pool 1 and Pool 2 are $\varphi_1 = \alpha(1-H)$ and $\varphi_2 = \alpha H$, respectively.

Suppose that the fully decentralized voting outcome is different from what Pool 1 would choose. What is the probability that Pool 1's proposal is adopted in such a case? We need to consider two cases:

Case 1. Suppose that the majority of stakeholders prefer proposal A, that is, $\rho \geq \frac{1}{2}$. Suppose that Pool 1 and Pool 2 prefer proposal B. Then, the probability that Pool 1's preferred proposal wins the vote is

$$\Pr\left((1-\alpha)\rho \leq \frac{1}{2} \mid \rho \geq \frac{1}{2}\right) = \frac{\frac{1}{2(1-\alpha)} - \frac{1}{2}}{\frac{1}{2}} = \frac{\alpha}{1-\alpha}. \tag{18}$$

Similarly, if the majority prefers proposal B ($\rho \leq \frac{1}{2}$), and both pools prefer A, then the probability that Pool 1's preferred proposal wins the vote is

$$\Pr\left(\alpha + (1-\alpha)\rho \geq \frac{1}{2} \mid \rho \leq \frac{1}{2}\right) = \frac{\alpha}{1-\alpha}. \tag{19}$$

Case 2. Suppose that the majority of stakeholders and Pool 2 prefer proposal A. If Pool 1 prefers B, then the probability that Pool 1's preferred proposal wins the vote is

$$\Pr\left(\alpha H + (1-\alpha)\rho \leq \frac{1}{2} \mid \rho \geq \frac{1}{2}\right) = \max\left\{\frac{\alpha(1-2H)}{1-\alpha}, 0\right\}. \tag{20}$$

Similarly, if the majority and Pool 2 prefer proposal B and if Pool 1 prefers A, then the probability that Pool 1's preferred proposal wins the vote is

$$\Pr\left(\alpha(1-H) + (1-\alpha)\rho \geq \frac{1}{2} \mid \rho \leq \frac{1}{2}\right) = \max\left\{\frac{\alpha(1-2H)}{1-\alpha}, 0\right\}. \tag{21}$$

There are two reasons for decisions to differ from those obtained in the fully decentralized benchmark. The first one is *proxy voting*: Because some miners delegate their rights to vote to the mining pools, pools become nonatomistic and thus can impose their preferences some times. The importance of proxy voting is measured by α. The second reason is *concentration of voting rights*. In our model, since there are only two pools, concentration is minimized when market shares are equal (i.e., $H = \frac{1}{2}$) and is maximized when a single pool controls all the market ($H = 1$ or $H = 0$).

Note that when $H = \frac{1}{2}$, if there is disagreement among pools, the biases cancel each other out, and the fully decentralized outcome is obtained.

5.3. Endogenous Market Shares

We now incorporate voting rights motives into pools' objective functions. For simplicity, we assume that $\{z_1, z_2\}$ – the mining pools' preferences over proposals – are distributed independently from the z_l's of the other stakeholders, $l \neq 1, 2$. Let ϕ denote the probability of disagreement between the pools, that is, $z_1 \neq z_2$.

The influence functions of the pools can be explicitly written as

$$I\left(f_1, f_2\right) = \frac{1 - 2\alpha H(f_1 - f_2)\phi}{2\left(1 - \alpha\right)} \tag{22}$$

$$I\left(f_2, f_1\right) = \frac{1 - 2\alpha\left(1 - H(f_1 - f_2)\right)\phi}{2\left(1 - \alpha\right)}. \tag{23}$$

The influence functions are increasing in one's market share in the pool market, consistent with the assumption made in Subsection 3.1. We can now see how the choice of fees affects pools' influence on the governance of the blockchain: Lower fees imply more influence.

We now solve for the equilibrium with mining pools as in Subsection 4.2. All steps are unchanged, except for the those at Date 1, when mining pools choose fees simultaneously to maximize their payoffs:

$$\max_{f_1} \Pi_1\left(f_1, f_2\right) + \pi\left(f_1, f_2\right) + b_1 I\left(f_1, f_2\right) \tag{24}$$

$$\max_{f_2} \Pi_2\left(f_1, f_2\right) + b_2 I\left(f_2, f_1\right), \tag{25}$$

where $\Pi_j\left(f_1, f_2\right)$, $j = 1, 2$, and $\pi\left(f_1, f_2\right)$ are given by (14) and (15).

In Subsection 4.2, we show that equilibrium market shares are asymmetric, and that Pool 1 – the equipment producer – has the larger market share. The next proposition shows that this result continues to hold unless b_2 is sufficiently larger than b_1.

Proposition 7 *If $b_1 \geq b_2$, in any equilibrium, the equipment producer is the stakeholder with the greatest influence on the governance of the blockchain.*

As in Proposition 4, the equipment producer (Pool 1) has a purely economic motive for setting low fees: Lower fees attract more miners to the market and thus increase demand for mining equipment. Now, both the equipment producer and the independent pool (Pool 2) have an additional governance motive for setting lower fees: They both want to gain market share to increase the probability of winning the vote on the proposal. Because the strength of this last motive is proportional to their private benefits, unless b_2 is sufficiently larger than b_1, the equipment producer's economic incentives to lower fees will dominate, implying that in equilibrium the equipment producer charges lower fees and thus has the larger share of the pool market.

Although we have assumed that private benefits are exogenous, it is reasonable to expect $b_1 \geq b_2$ in reality. For example, some proposals may affect the equipment producer directly, such as changes that make the protocol less compatible with the existing specialized equipment. Because the equipment producer controls a large share of the whole mining ecosystem, there are many more ways in which proposals can directly affect its payoff than that of independent pools.

As both b_1 and b_2 converge to zero, equilibrium market shares converge to those in Proposition 4. If b_1 is small but not exactly zero, the equipment producer will still have a disproportionate impact on governance of the blockchain.

5.4. Self-Mining

We have assumed that the equipment producer has no comparative advantage at mining; that is, σ is sufficiently small. Proposition 1 then implies that the equipment producer does not self-mine. In the next proposition, we show that this result no longer holds if the equipment producer's private benefits of control are sufficiently large.

Proposition 8 *In any equilibrium, a sufficient condition for the equipment producer to self-mine is:*

$$\frac{b_1}{2\left(1-\alpha\right)} > \frac{r\left(\mu-\sigma\right)}{c-\mu}. \tag{26}$$

Intuitively, if b_1 is sufficiently large, the equipment producer is willing to give up some profits in the sales of equipment in order to self-mine and increase the probability that it wins the vote. To understand the right-hand side of (26), note that $\mu - \sigma$ is a measure of the comparative advantage at mining that individual miners have over the equipment producer. As this advantage increases, it would take a larger private benefit to induce the producer to self-mine. Incentives to self-mine are also curbed when mining rewards are high, i.e., when r is large. A larger r implies that mining is more attractive; thus, there is potentially more demand for equipment. This increase in potential demand increases the shadow cost of self-mining. Similarly, $c - \mu$ is a measure of individual miners' net cost of mining. A lower net cost of mining increases demand for equipment and thus reduces the equipment producer's incentives to self-mine.

6. Conclusion

In this paper, we develop a model in which the proof-of-work system creates an industrial ecosystem where miners, mining equipment producers, and mining services providers 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 ecosystem. In particular, we show that the governance of the blockchain is captured by the dominant equipment producer.

What factors explain the influence of specialized equipment producers on blockchain governance? We show that the combination of a homogeneous good (computational power) and sunk entry costs (R&D costs) leads to a situation in which a large firm dominates the market for specialized mining equipment. Such a firm then has incentives to enter the mining pool market in order to squeeze the profits of other mining pools and thus increase the demand for its own equipment. Such incentives are stronger as the equipment producer becomes more efficient and as the blockchain becomes more successful, that is, as crypto prices increase.

According to our model, the equipment producer invests in the mining ecosystem in order to encourage more individuals to become miners. This explanation corresponds to what Bitmain Technologies – the leading specialized cryptomining equipment producer – 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.*"[22]

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 allocated to mining.

To avoid governance capture, blockchain stakeholders could consider alternative governance systems. The most popular alternative to proof-of-work is *proof-of-stake*, which is a system where the probability that a node is selected for block validation is proportional to that node's "stake" in the network.[23] It is, however, not clear that such a system would avoid the problem of corporate capture. First, by design, this system gives more power to larger players. Second, such a system may also create its own industrial ecosystem where specialized equipment producers play an important role (O'Leary, 2018). In such a case, the problems highlighted by our model would still be relevant. Another governance structure that has been suggested is *delegated proof-of-stake*. In such a system, blockchain stakeholders vote for delegates who then directly monitor the blockchain (an example is EOS). This system essentially replicates the traditional governance structure of corporations, in which shareholders vote for corporate directors, who then monitor management. Such a system is very different from the direct democracy envisioned by Nakamoto; it is essentially a system of representative democracy.

Our model suggests that Nakamoto's vision on blockchain governance is untenable. Because market power propagates through the blockchain ecosystem, corporate capture is in proof-of-work's DNA. If the governance of the blockchain is captured by a large firm, blockchain stakeholders have to trust one company to look after their interests. In that case,

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

[23] The definition of stake varies across different implementations. For an economic analysis of the proof-of-stake concept, see Saleh (2018)

one may ask how a permissionless blockchain differs from a traditional financial intermediary as a provider of trust.

References

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

Alsabah. H., and A. Capponi. 2019. 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.*

Bar-Isaac, H., and J. Shapiro. 2019. Blockholder Voting. *Journal of Financial Economics.* forthcoming.

Becker, G.S. 1985. Public Policies, Pressure Groups, and Deadweight Costs. *Journal of Public Economics.* 28: 329-347.

Bennedsen, M and D. Wolfenzon. 2000. The Balance of Power in Closely Held Corporations. *Journal of Financial Economics. 58:* 113-39.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2019a. The Blockchain Folk Theorem. *Review of Financial Studies.* 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 EL. 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. 2019. A Brief Introduction to Blockchain Economics. *Working paper.*

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

Chod, J., and E. Lyandres. 2018. A Theory of ICOs: Diversification, Agency, and Information Asymmetry. *Working paper.*

Cong, L. W. and Z. He. 2018. Blockchain Disruption and Smart Contracts. *Review of Financial Studies.* forthcoming.

Cong, L. W., Z. He and J. Li. 2018. Decentralized Mining in Centralized Pools. *Working paper.*

Cong, L. W., Y. Li, and N. Wang. 2019. Token-based Corporate 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.* forthcoming.

Edmans, A. and G. Manso. 2011. Governance Through Trading and Intervention: A Theory of Multiple Blockholders. *Review of Financial Studies.* 24: 2395-428.

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.

Gawer, A. and R. Henderson. 2007. Platform Owner Entry and Innovation in Complementary Markets: Evidence from Intel. *Journal of Economics & Management Strategy.* 16: 1–34.

Halaburda, H., and G. Haeringer. 2018. Bitcoin and Blockchain: What we Know and What Questions are Still Open. *Working paper.*

Hinzen, F. J., K. John, and F. Saleh. 2019. Proof-of-Work's Limited Adoption Problem. *Working paper.*

Huberman, G., J. Leshno, and C. Moallemi. 2017. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Working Paper.*

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

Lehar, A. and C. A. Parlour. 2019. Liquidity Demand and Bitcoin Transaction Fees. *Working paper.*

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

Makarov, I., and A. Schoar. 2019. Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics.* forthcoming.

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.

Nakamoto, S. 2009. Bitcoin Open Source Implementation of P2P Currency. Available at: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

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.

O'Leary, R. R. 2018. The Creator of Proof-of-Stake Thinks He Finally Figured It Out. *Coindesk.* https://www.coindesk.com/the-creator-of-proof-of-stake-thinks-he-finally-figured-it-out.

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.

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

Prat, J., and B. Walter. 2018. An Equilibrium Model of the Market for Bitcoin Mining. Working paper.

Romiti, M., A. Judmayer, A. Zamyatin, and B. Haslhofer. 2019. A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares. *Working paper.*

Saleh, F. 2018. Blockchain Without Waste: Proof-of-Stake. *Working paper.*

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

Stiglitz, J., D. McFadden and S. Peltzman. 1987. Technological Change, Sunk Costs, and Competition. *Brookings Papers on Economic Activity.* 1987(3): 883-947.

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.

Yermack, D. 2017. Corporate Governance and Blockchains. *Review of Finance.* 21: 7-31.

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

7. Appendix

Proposition 1.

Proof. Firm k's problem is to

$$\max_{p,n_k,n_k'} \pi_k = (p-\underline{c})n_k' + \left(\frac{r}{n_k+n_k'} - \underline{c} + \sigma\right) n_k, \tag{27}$$

subject to

$$\begin{aligned} \frac{r}{n_k+n_k'} - \min\{p,c\} + s &\leq 0 \qquad (28) \\ p &\leq c \qquad (29) \\ n_k, n_k' &\geq 0. \qquad (30) \end{aligned}$$

First, note that (29) implies $\min\{p,c\} = p$. Suppose now (28) is slack in equilibrium, then we must have $n_k' = 0$. The profit function becomes

$$\pi_k = r + (\sigma - \underline{c})\, n_k, \tag{31}$$

and the producer's profit decreases with n_k, which implies that (28) must eventually bind. Thus (28) cannot be slack. Because (28) binds, then we can rewrite the profit function as

$$\pi_k = (p-\underline{c})\,(n_k+n_k') + (\sigma - s)\, n_k. \tag{32}$$

If $(\sigma - s) < 0$, then the producer wants the minimum possible n_k, which implies $n_k = 0$, and thus

$$n_k' = \frac{r}{p-s}. \tag{33}$$

Replacing (33) in the profit function yields:

$$\pi_k = r\frac{p-\underline{c}}{p-s}. \tag{34}$$

Since

$$\frac{\partial \pi_k}{\partial p} = r\frac{\underline{c}-s}{(p-s)^2} > 0, \tag{35}$$

constraint $p \leq c$ binds. In either case, $p^* = c$.

If $(\sigma - s) > 0$, then the producer wants the maximum possible n_k, which implies $n'_k = 0$, which requires $p = c$ and

$$n_k = \frac{r}{c - s}. \tag{36}$$

Finally, if $(\sigma - s) = 0$ then any n_k and n'_k such that $n_k + n'_k = \frac{r}{c-s}$ is a solution. ■

Proposition 2.

Proof. Firm k's problem is to

$$\max_{p_k, n_k, n'_k} \pi_k = (p_k - \underline{c})n'_k + \left(\frac{r}{n_k + n'_k + n_z + n'_z} - \underline{c} + \sigma \right) n_k, \tag{37}$$

subject to

$$\begin{aligned} \frac{r}{n_k + n'_k + n_z + n'_z} - \min\{p_k, p_z, c\} + s &\leq 0 & (38) \\ p_k &\leq \min\{p_z, c\} & (39) \\ n_k, n'_k &\geq 0. & (40) \end{aligned}$$

Firm z's problem is symmetric.

First, note that, in an equilibrium where both firms sell a positive number of machines, it must be that $p_k = p_z = p$. This follows from usual Bertrand competition reasoning: if, say, $p_k < p_z$, all miners would buy only from Firm k. Furthermore, it must be that $p = \underline{c}$. If not, there is a profitable deviation: a firm may reduce its price by small $\varepsilon > 0$ and capture the whole market.

We need to consider three cases.

Case 1: $(\sigma - s) < 0$. (i) Suppose first that $n'_k + n'_z > 0$. Then it follows that $p = \underline{c}$ and thus we have

$$\frac{r}{n_k + n'_k + n_z + n'_z} - \underline{c} + s = 0. \tag{41}$$

The profit function becomes

$$\pi_k = \left(\frac{r}{n_k + n'_k + n_z + n'_z} - \underline{c} + \sigma \right) n_k, \tag{42}$$

which is strictly negative for any $n_k > 0$, implying that we must have $n^*_k = n^*_z = 0$. This is the only equilibrium with positive sales $n'^*_k + n'^*_z > 0$.

Thus, in any equilibrium with positive sales, there is no self mining and profits are zero ($p = \underline{c}$).

(ii) Suppose now that $n_k'^* = n_z'^* = 0$. Let $p = \min\{p_k, p_z\}$, and without loss of generality, suppose $p = p_k$. If $n_k'^* = n_z'^* = 0$ in equilibrium, the miners' utility per unit of computational power is

$$\frac{r}{n_k^* + n_z^*} - p_k + s < 0. \tag{43}$$

Firm k's profit is

$$\pi_k = \left(\frac{r}{n_k^* + n_z^*} - \underline{c} + \sigma \right) n_{k.} \tag{44}$$

For an equilibrium, we need $\pi_k \geq 0$. Define

$$\widehat{p} = \frac{r}{n_k^* + n_z^*} + s. \tag{45}$$

For π_k to be positive while (43) holds, $p_k > \widehat{p} > \underline{c}$.

We now show that this cannot be an equilibrium. Consider a deviation where Firm k sets $p_k = \widehat{p}$ and chooses $n_k = 0$. The firm will then sell an amount n_k' such that

$$\frac{r}{n_z^* + n_k'} - \widehat{p} + s = 0, \tag{46}$$

which implies $n_k' = n_k^*$. The profit is then

$$(\widehat{p} - \underline{c}) n_k^* = \left(\frac{r}{n_k^* + n_z^*} - \underline{c} + s \right) n_k^* > \left(\frac{r}{n_k^* + n_z^*} - \underline{c} + \sigma \right) n_k^*, \tag{47}$$

thus this is a profitable deviation. Thus, there is no equilibrium with zero sales.

We conclude that, if $\sigma - s < 0$, all equilibria require $n_k^* = n_z^* = 0$ and both firms make zero profit.

Case 2: $\sigma - s > 0$. (i) Suppose first that $n_k'^* = n_z'^* = 0$. The maximization problem becomes

$$\max_{n_k} \pi_k = \left(\frac{r}{n_k + n_z} - \underline{c} + \sigma \right) n_k, \tag{48}$$

and the first-order condition is

$$\frac{r}{n_k + n_z} - \underline{c} + \sigma - \frac{r n_k}{(n_k + n_z)^2} = 0. \tag{49}$$

In a symmetric equilibrium

$$n_k^* = n_z^* = \frac{r}{4\left(\underline{c} - \sigma\right)}, \tag{50}$$

provided that the free entry condition is slack:

$$2\left(\underline{c} - \sigma\right) < c - s, \tag{51}$$

and total profit is then

$$\pi = \frac{r}{4\left(\underline{c} - \sigma\right)}\left[2\left(\underline{c} - \sigma\right) - \underline{c} + \sigma\right] = \frac{r}{4}. \tag{52}$$

If (51) does not hold, we have

$$n_k^* = n_z^* = \frac{r}{2\left(c - s\right)}, \tag{53}$$

and the profit is

$$\pi = \frac{r\left(c - \underline{c} + \sigma - s\right)}{2\left(c - s\right)}. \tag{54}$$

We now show that this is an equilibrium. Define

$$\widehat{p} = \frac{r}{n_k^* + n_z^*} + s. \tag{55}$$

Consider a deviation where Firm k sets $p_k = \widehat{p}$ and chooses $n_k = 0$. The firm will then sell an amount n_k' such that

$$\frac{r}{n_k' + n_z^*} - \widehat{p} + s = 0, \tag{56}$$

which implies $n_k' = n_k^*$. Firm k's profit is then

$$(\widehat{p} - \underline{c})n_k^* = \left(\frac{r}{n_k^* + n_z^*} - \underline{c} + s\right)n_k^* < \left(\frac{r}{n_k^* + n_z^*} - \underline{c} + \sigma\right)n_k^*, \tag{57}$$

thus no profitable deviation exists.

(ii) Suppose now that $n_k'^* + n_z'^* > 0$. The entry constraint must be binding:

$$\frac{r}{n_k'^* + n_z'^* + n_k^* + n_z^*} - \underline{c} + s = 0. \tag{58}$$

Because $p = \underline{c}$, Firm k's profit is

$$\left(\frac{r}{n_k'^* + n_z'^* + n_k^* + n_z^*} - \underline{c} + \sigma\right) n_k^* = (\sigma - s) n_k^* > 0 \tag{59}$$

so there is a profitable deviation, which is to increase n_k'. Thus, this cannot be an equilibrium.

We conclude that, if $\sigma - s > 0$, all equilibria require $n_k'^* = n_z'^* = 0$ and both firms make positive profit.

Case 3: $\sigma - s = 0$. Using the same arguments as in Cases 1 and 2, it can be shown that both types of equilibria are possible in this zero measure case. ■

Proposition 3.

Proof. At $t = 0$, there are no incumbents in the market for specialized mining equipment. At $t = 1$, Firm 1 has the option to enter this market by paying an once-and-for-all sunk cost ι. At $t = 2$, Firm 2 can now enter after paying the same cost ι, and so on for periods $t > 2$. That is, Firm 1 has a first-mover advantage over all other firms.

Let δ denote the common discount rate. Proposition 2 implies that in any equilibrium with two firms and $n_1'^* + n_2'^* > 0$, profits are zero for both firms, and $\sigma \leq s$. Thus, assume $\sigma \leq s$. At $t = 2$, suppose that Firm 1 is an incumbent. If Firm 2 enters, it enjoys zero profit in perpetuity (we assume that Firm 1 does not exit after Firm 2 enters) and pays entry cost ι, thus it will not enter in this case. At $t = 3$, the same reasoning implies that Firm 3 will also not enter if either Firm 1 or Firm 2 is an incumbent, and so on for $t > 3$. Thus, if Firm 1 enters, no firm at periods $t = 2, 3, ...$ will enter. Thus Firm 1 chooses to enter if and only if

$$\frac{r\left(c - \underline{c}\right)}{\delta\left(c - s\right)} \geq \iota. \tag{60}$$

If condition (60) does not hold, Firm 1 will not enter. Firm 2 then faces the same problem as Firm 1, and also chooses not to enter, and so on for $t > 2$. Thus, equilibrium is such that only Firm 1 enters if and only if (60) holds, otherwise no firm enters. ■

Proposition 4

Proof. The two pools choose f_1 and f_2, such that:

$$\max_{f_1} \Pi_1\left(f_1, f_2\right) + \pi\left(f_1, f_2\right) = \frac{r f_1\left(1 - H(f_1 - f_2)\right)}{c - \mu + e\left(f_1, f_2\right)} + \frac{r\left(c - \underline{c}\right)}{c - \mu + e\left(f_1, f_2\right)}, \tag{61}$$

$$\max_{f_2} \Pi_2 \left(f_1, f_2\right) = \frac{r f_2 H(f_1 - f_2)}{c - \mu + e\left(f_{1,} f_2\right)}, \tag{62}$$

where

$$e\left(f_{1,} f_2\right) \equiv f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2). \tag{63}$$

Let $H^* \equiv H(f_1^* - f_2^*)$ and $h^* \equiv h(f_1^* - f_2^*)$. Assuming that an interior solution exists, the simplified first-order conditions are:

$$\left(c - \mu + f_2^* H^*\right)\left(1 - H^*\right) - f_1^* h^* \left(c - \mu + f_2^*\right) - (c - \underline{c})(1 - H^* - (f_1^* - f_2^*)h^*) = 0 \tag{64}$$

$$\left(c - \mu + f_1^* \left(1 - H^*\right)\right) H^* - f_2^* h^* (c - \mu + f_1^*) = 0, \tag{65}$$

From equations (64) and (65) we express f_1^* and f_1^* as follows:

$$f_1^* = \left(\frac{c - \mu + f_2^* H^*}{c - \mu + f_2^*}\right) \frac{(1 - H^*)}{h^*} - \frac{(c - \underline{c})(1 - H^* - (f_1^* - f_2^*)h^*)}{(c - \mu + f_2^*)h^*} \tag{66}$$

$$f_2^* = \left(\frac{c - \mu + f_1^* \left(1 - H^*\right)}{c - \mu + f_1^*}\right) \frac{H^*}{h^*} \tag{67}$$

We replace $H^* = 0.5 + \epsilon$ and simplify:

$$f_1^* = \left(\frac{c - \mu + f_2^*(0.5 + \epsilon)}{c - \mu + f_2^*}\right) \frac{(0.5 - \epsilon)}{h^*} - \frac{(c - \underline{c})\left(0.5 - \epsilon\right)}{(c - \mu + f_2^*)h^*} + \frac{(f_1^* - f_2^*)(c - \underline{c})}{(c - \mu + f_2^*)} \tag{68}$$

$$f_2^* = \left(\frac{c - \mu + f_1^* \left(0.5 - \epsilon\right)}{c - \mu + f_1^*}\right) \frac{(0.5 + \epsilon)}{h^*} \tag{69}$$

We subtract (69) from (68) and simplify:[24]

$$h^* \left(f_1^* - f_2^*\right) \left(\underline{c} - \mu + f_2^*\right) = \left(c - \mu\right) \frac{-2\epsilon\left(c - \mu + f_2^*\right) + \left(f_1^* - f_2^*\right)(0.5 - \epsilon)^2}{\left(c - \mu + f_1^*\right)} - \left(c - \underline{c}\right)\left(0.5 - \epsilon\right) \tag{70}$$

which implies

$$h^* \left(f_1^* - f_2^*\right) f_2^* \left(\frac{\underline{c} - \mu}{f_2^*} + 1 - \frac{(c - \mu)(0.5 - \epsilon)^2}{f_2^* h^* (c - \mu + f_1)}\right) = -\left(c - \mu\right) \frac{2\epsilon\left(c - \mu + f_2^*\right)}{\left(c - \mu + f_1^*\right)} - (c - \underline{c})(0.5 - \epsilon). \tag{71}$$

From the first-order condition (69), we obtain $f_2^* h^* \left(c - \mu + f_1^*\right) = \left(c - \mu + f_1^* \left(0.5 - \epsilon\right)\right)\left(0.5 + \epsilon\right)$

[24] There are many steps of algebra here; a step-by-step derivation of this equation is found in the Internet Appendix.

and we can further simplify (71):

$$h^*\left(f_1^*-f_2^*\right)f_2^*\left(\frac{\underline{c}-\mu}{f_2^*}+1-\frac{(c-\mu)(0.5-\epsilon)^2}{\left(c-\mu+f_1^*(0.5-\epsilon)\right)(0.5+\epsilon)}\right)=-\left(c-\mu\right)\frac{2\epsilon\left(c-\mu+f_2^*\right)}{\left(c-\mu+f_1^*\right)}-(c-\underline{c})(0.5-\epsilon). \tag{72}$$

Suppose now that $\epsilon \geq 0$, that is $H^* \geq 0.5$. Since

$$f_2^*\left(\frac{\underline{c}-\mu}{f_2^*}+1-\frac{(c-\mu)\left(0.5-\epsilon\right)^2}{\left(c-\mu+f_1^*\left(0.5-\epsilon\right)\right)\left(0.5+\epsilon\right)}\right)>0, \tag{73}$$

and since for $\epsilon \geq 0$ the right-hand side of equation (72) is negative, it follows that $f_1^* < f_2^*$, which is in contradiction with $H^* \geq 0.5$.

Since $\varphi_1(f_1^*, f_2^*) = \alpha\left(1-H^*\right)$ and $\varphi_2(f_1^*, f_2^*) = \alpha H^*$ and $H^* < 0.5$, it follows that $\varphi_1(f_1^*, f_2^*) > \varphi_2(f_1^*, f_2^*)$ and $I\left(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*)\right) > I\left(\varphi_2(f_1^*, f_2^*), \varphi_1(f_1^*, f_2^*)\right)$. ■

Proposition 4 in a more general setting.

Suppose we assume some generic functional forms for π, Π_1 and Π_2. The assumptions we make in the next Proposition are stronger than what we need; we make them to simplify the argument:

Proposition 9 *Let* $\pi\left(f_1, f_2\right)$ *denote the profit in the market for equipment and let* $\Pi_1\left(f_1, f_2\right)$ *and* $\Pi_2\left(f_1, f_2\right)$ *denote the profit functions in the pool market, for firms* 1 *and* 2 *respectively. Assume the following:*

1. $\Pi_1(f_1, f_2) = \Pi_2(f_2, f_1)$ *(pool profit functions are symmetric),*

2. $\frac{\partial \pi}{\partial f_1} < 0$ *(lower fees in the pool market increase profit in the market for mining equipment),*

3. $\frac{\partial^2 \Pi_1(f_1,f_2)}{\partial f_1 \partial f_2}, \frac{\partial^2 \Pi_2(f_1,f_2)}{\partial f_1 \partial f_2} > 0$ *(pool fees are strategic complements), and*

4. $\frac{\partial^2 \Pi_1(f_1,f_2)}{\partial f_1^2}, \frac{\partial^2 \Pi_2(f_1,f_2)}{\partial f_2^2} < 0$ *(the pool profit function is globally concave).*

Then, the equipment producer is the stakeholder with the greatest influence on the governance of the blockchain.

Proof. The first-order conditions that determine the equilibrium fees are:

$$\begin{aligned} \frac{\partial \Pi_1 \left(f_1^*, f_2^*\right)}{\partial f_1} + \frac{\partial \pi \left(f_1^*, f_2^*\right)}{\partial f_1} &= 0 & (74) \\ \frac{\partial \Pi_2 \left(f_1^*, f_2^*\right)}{\partial f_2} &= 0. & (75) \end{aligned}$$

Suppose that the equilibrium is such that $f_1^* > f_2^*$. Then, because of strategic complementarities, we have

$$\frac{\partial \Pi_2 \left(f_2^*, f_2^*\right)}{\partial f_2} < 0. \tag{76}$$

Symmetry implies

$$\frac{\partial \Pi_2 \left(f_2^*, f_2^*\right)}{\partial f_2} = \frac{\partial \Pi_1 \left(f_2^*, f_2^*\right)}{\partial f_1} < 0. \tag{77}$$

Now, concavity implies

$$\frac{\partial \Pi_1 \left(f_2^*, f_2^*\right)}{\partial f_1} > \frac{\partial \Pi_1 \left(f_1^*, f_2^*\right)}{\partial f_1}, \tag{78}$$

and therefore

$$\frac{\partial \Pi_1 \left(f_1^*, f_2^*\right)}{\partial f_1} < 0. \tag{79}$$

But because $\frac{\partial \pi(f_1, f_2)}{\partial f_1} < 0$, (79) contradicts (74). Thus,there cannot be an equilibrium where $f_1^* \geq f_2^*$.[25] This implies that $f_1^* < f_2^*$, and $n_1^* > n_2^*$, where n_1^* is the equilibrium number of miners who join Pool 1 and n_2^* is the equilibrium number of miners who join Pool 2. Since $\varphi_1(f_1^*, f_2^*) = \frac{\alpha n_1^*}{n^*}$ and $\varphi_2(f_1^*, f_2^*) = \frac{\alpha n_2^*}{n^*}$, it follows that $\varphi_1(f_1^*, f_2^*) > \varphi_2(f_1^*, f_2^*)$ and $I\left(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*)\right) > I\left(\varphi_2(f_1^*, f_2^*), \varphi_1(f_1^*, f_2^*)\right)$. ■

Proposition 5

Proof. We start by characterizing the equilibrium when 2 independent pools compete in the pool market. As before $b_j = 0$ for $j = \{1, 2\}$. Each pool maximizes its expected profit:

$$\max_{f_1} \Pi_1 = \frac{r f_1 \left(1 - H(f_1 - f_2)\right)}{c - \mu + f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2)} \tag{80}$$

$$\max_{f_2} \Pi_2 = \frac{r f_2 H(f_1 - f_2)}{c - \mu + f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2)} \tag{81}$$

[25] The case of $f_1^* = f_2^*$ is trivial to rule out by using only symmetry and $\frac{\partial \pi(f_1, f_2)}{\partial f_1} < 0$.

Let $H^* \equiv H(f_1^* - f_2^*)$ and $h^* \equiv h(f_1^* - f_2^*)$, the simplified first order conditions are:

$$\left(c - \mu + f_2^* H^*\right)\left(1 - H^* - f_1^* h^*\right) - f_1^* \left(1 - H^*\right) f_2^* h^* = 0, \tag{82}$$

$$\left(c - \mu + f_1^* \left(1 - H^*\right)\right)\left(H^* - f_2^* h^*\right) - f_2 H^* f_1^* h^* = 0. \tag{83}$$

From the first order conditions we can express f_1^* and f_2^* as follows

$$f_1^* = \frac{\left(c - \mu + f_2^* H^*\right)\left(1 - H^*\right)}{\left(c - \mu + f_2^*\right) h^*}, \tag{84}$$

$$f_2^* = \frac{\left(c - \mu + f_1^* \left(1 - H^*\right)\right) H^*}{\left(c - \mu + f_1^*\right) h^*}. \tag{85}$$

From (84) and (85)

$$\left(f_1^* - f_2^*\right)\left(1 + \tfrac{(c-\mu)\left(f_1^* - f_2^*\right)H^*(1-H^*)}{h^*\left(c-\mu+f_1^*\right)\left(c-\mu+f_2^*\right)}\right) = \tfrac{(c-\mu)^2(1-2H^*)}{h^*\left(c-\mu+f_1^*\right)\left(c-\mu+f_2^*\right)} \tag{86}$$

which is equivalent to

$$\left(f_1^* - f_2^*\right)\left(1 + \tfrac{f_2^*(c-\mu)\left(f_1^* - f_2^*\right)(1-H^*)}{\left(c-\mu+f_1^*(1-H^*)\right)\left(c-\mu+f_2^*\right)}\right) = \tfrac{f_2^*(c-\mu)^2(1-2H^*)}{\left(c-\mu+f_1^*(1-H^*)\right)\left(c-\mu+f_2^*\right)H^*}. \tag{87}$$

First we note that $\left(1 + \tfrac{f_2^*(c-\mu)\left(f_1^* - f_2^*\right)(1-H^*)}{\left(c-\mu+f_1^*(1-H^*)\right)\left(c-\mu+f_2^*\right)}\right) > 0$. Assume that $H^* > 0.5$, then the right hand side of (87) is negative which would imply that $f_1^* < f_2^*$,which contradicts $H^* > 0.5$. Assume now that $H^* < 0.5$, then the right hand side of (87) is positive which would imply $f_1^* > f_2^*$,which contradicts $H^* < 0.5$.Since $H(0) = 0.5$, (87) is only satisfied for $f_1^* = f_2^* = f^*$. We can now simplify (84) as follows

$$\left(c - \mu + 0.5 f^*\right)\left(0.5 - f^* h(0)\right) - 0.5 f^{*2} h(0) = 0 \tag{88}$$

$$\Leftrightarrow f^{*2} + f^* \left(c - \mu - 0.25\right) - \frac{\left(c - \mu\right) 0.5}{h(0)} = 0 \tag{89}$$

$$f^* = \frac{\sqrt{\left(c - \mu - 0.25\right)^2 + \frac{2(c-\mu)}{h(0)}} - \left(c - \mu - 0.25\right)}{2}. \tag{90}$$

Note that f^* is independent of r and $\underline{c}$.

The equipment producer is better off entering the market without full control, rather than entering the market with full control if:

$$\frac{r\left(c-\underline{c}\right)}{c-\mu+e[f_1^*,f_2^*]}+\frac{rf_1\left(1-H^*\right)}{c-\mu+e[f_1^*,f_2^*]}<\frac{r\left(c-\underline{c}\right)}{c-\mu+f^*}+\frac{r0.5f^*}{c-\mu+f^*}, \tag{91}$$

where f_1^* and f_2^* are the equilibrium fees and $(1-H^*)$ (*resp.* H^*) is the equilibrium market share of Pool 1 (*resp.* Pool 2) in the case where Pool 1 is fully controlled by the equipment producer, and f^* is as in equation (90). ■

Proposition 6

Proof. Suppose that an independent pool enters the market. Let Π^I denote the equilibrium profit of that pool gross of entry costs. Suppose instead that the equipment producer is the entrant. Let Π^C denote the equilibrium profit in the pool market (gross of entry costs) of the producer if it enters with full control rights. If it instead enters without control rights, its profit is identical to that of an independent entrant, Π^I. Let π_1^I denote the equilibrium profit in the equipment market if an independent pool enters the pool market. Let π_1^C denote the equilibrium profit in the equipment market if the pool that enters the pool market is fully controlled by the equipment producer. Finally, let π_1 denote the equilibrium profit in the equipment market if there is only one pool in the market.

An independently-owned pool enters the mining pool market if:

$$\Pi^I\geq\kappa \tag{92}$$

The equipment producer enters the mining pool market if:

$$\max\left\{\Pi^I+\pi_1^I,\Pi^C+\pi_1^C\right\}-\pi_1\geq\kappa \tag{93}$$

A sufficient condition for the equipment producer to have higher incentives to enter the pool market relative to an independent pool is:

$$\pi_1^I>\pi_1 \tag{94}$$

$$\frac{r(c-\underline{c})}{c-\mu+f^*}>\frac{r(c-\underline{c})}{c-\mu+f^0}, \tag{95}$$

where f^* is the equilibrium fee with two independent pools and f^0 is the equilibrium fee chosen by a monopolist pool. Since the fee chosen by a monopolist pool is always such that $f^0 \geq \underline{\upsilon}$, then a sufficient condition for (95) to hold is:

$$f^* < \underline{\upsilon} \Leftrightarrow \sqrt{(c-\mu-0.25)^2 + \frac{2(c-\mu)}{h(0)}} < 2\underline{\upsilon} + (c-\mu-0.25)\,. \tag{96}$$

which holds because of Assumption 1.

The equipment producer's incentive to enter relative to an independent pool is therefore given by:

$$RI = \frac{r(c-\underline{c})}{c-\mu+f^*} - \frac{r(c-\underline{c})}{c-\mu+f^0} = r(c-\underline{c})\frac{f^0-f^*}{(c-\mu+f^*)(c-\mu+f^0)} > 0. \tag{97}$$

■

Proposition 7.

Proof. Mining pools choose fees simultaneously to maximize their profits:

$$\max_{f_1} \Pi_1(f_1, f_2) + \pi(f_1, f_2) + \frac{b_1}{2(1-\alpha)}\left[1 - 2\alpha H(f_1 - f_2)\phi\right] \tag{98}$$

$$\max_{f_2} \Pi_2(f_1, f_2) + \frac{b_2}{2(1-\alpha)}\left[1 - 2\alpha\left(1 - H(f_1 - f_2)\right)\phi\right], \tag{99}$$

where ϕ is the probability that Pool 1 and Pool 2 disagree on their preferred proposal. Let $H^* \equiv H(f_1^* - f_2^*)$ and $h^* \equiv h(f_1^* - f_2^*)$, the simplified first order conditions are as follows:

$$(c-\mu+f_2^*H^*)(1-H^*) - f_1^*h^*(c-\mu+f_2^*) - (c-\underline{c})(1-H^*-(f_1^*-f_2^*)h^*) - \tfrac{b_1\alpha\phi h^* n^2}{(1-\alpha)r} = 0, \tag{100}$$

$$(c-\mu+f_1^*(1-H^*))H^* - f_2^*h^*(c-\mu+f_1^*) - \tfrac{b_2\alpha\phi h^* n^2}{(1-\alpha)r} = 0. \tag{101}$$

From equations (100) and (101) we express f_1^* and f_1^* as follows

$$f_1^* = \left(\tfrac{c-\mu+f_2^*H^*}{c-\mu+f_2^*}\right)\tfrac{(1-H^*)}{h^*} - \tfrac{(c-\underline{c})(1-H^*-(f_1^*-f_2^*)h^*)}{(c-\mu+f_2^*)h^*} - \tfrac{b_1\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r}, \tag{102}$$

$$f_2^* = \left(\tfrac{c-\mu+f_1^*(1-H^*)}{c-\mu+f_1^*}\right)\tfrac{H^*}{h^*} - \tfrac{b_2\alpha\phi n^2}{(1-\alpha)(c-\mu+f_1^*)r}. \tag{103}$$

Let $H^* \equiv 0.5 + \epsilon$, then (102) and (103) can be rewritten as follows:

$$f_1^* = \left(\frac{c-\mu+f_2^*(0.5+\epsilon)}{c-\mu+f_2^*}\right) \frac{(0.5-\epsilon)}{h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{(c-\mu+f_2^*)h^*} + \frac{(f_1^*-f_2^*)(c-\underline{c})}{(c-\mu+f_2^*)} - \frac{b_1\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r} \tag{104}$$

$$f_2^* = \left(\frac{c-\mu+f_1^*(0.5-\epsilon)}{c-\mu+f_1^*}\right) \frac{(0.5+\epsilon)}{h^*} - \frac{b_2\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r} \tag{105}$$

We subtract (105) from (104) and simplify:

$$\begin{aligned}(f_1^* - f_2^*)\left(\underline{c} - \mu + f_2^*\right) = \; & \frac{(0.5-\epsilon)\Big(c-\mu+f_2^*(0.5+\epsilon)\Big)\Big(c-\mu+f_1^*\Big)}{h^*\Big(c-\mu+f_1^*\Big)} - \frac{\alpha\phi\Big(b_1(c-\mu+f_1^*)-b_2(c-\mu+f_2^*)\Big)n^2}{(1-\alpha)(c-\mu+f_1^*)r} \\ & - \frac{(0.5+\epsilon)\Big(c-\mu+f_1^*(0.5-\epsilon)\Big)\Big(c-\mu+f_2^*\Big)}{h^*\Big(c-\mu+f_1^*\Big)} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*}\end{aligned} \tag{106}$$

$$\begin{aligned}(f_1^* - f_2^*)\left(\underline{c} - \mu + f_2^*\right) = \; & \frac{\Big(-2\epsilon(c-\mu)^2-\Big(f_1^*-f_2^*\Big)(c-\mu)\Big(0.5^2-\epsilon^2\Big)+f_1^*(c-\mu)(0.5-\epsilon)-f_2^*(c-\mu)(0.5+\epsilon)\Big)}{h^*\Big(c-\mu+f_1^*\Big)} \\ & - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} - \frac{\alpha(\phi_2+\phi_3)((b_1-b_2)(c-\mu))n^2}{(1-\alpha)(c-\mu+f_1^*)r} - \frac{\alpha(\phi_2+\phi_3)\Big(b_1f_1^*-b_2f_2^*\Big)n^2}{(1-\alpha)(c-\mu+f_1^*)r} \\ (f_1^* - f_2^*)\, f_2^* \left(\frac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)(0.5-\epsilon)^2}{f_2^* h^*(c-\mu+f_1)}\right) = \; & -\frac{2\epsilon(c-\mu)\Big(c-\mu+f_2^*\Big)}{\Big(c-\mu+f_1^*\Big)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} \\ & - \frac{\alpha\phi(b_1-b_2)(c-\mu)n^2}{(1-\alpha)(c-\mu+f_1^*)r} - \frac{\alpha\phi\Big(b_1f_1^*-b_2f_2^*\Big)n^2}{(1-\alpha)(c-\mu+f_1^*)r}.\end{aligned} \tag{107}$$

For $b_1 = b_2 = b$:

$$(f_1^* - f_2^*)\, f_2^* \left(\frac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)(0.5-\epsilon)^2}{f_2^* h^*(c-\mu+f_1)} + \frac{\alpha\phi b n^2}{f_2^*(1-\alpha)(c-\mu+f_1^*)r}\right) = -\frac{2\epsilon(c-\mu)\Big(c-\mu+f_2^*\Big)}{\Big(c-\mu+f_1^*\Big)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*}. \tag{108}$$

The rest of the proof is the same as for Proposition 4. ■

Proposition 8.

Proof. Let $\beta \equiv \frac{n}{n+n'}$, where n is the amount of computational power used by the equipment producer for self-mining and n' is the amount of computational power sold by the equipment producer. In this setting the share of hash rate controlled by Pool 1 (the pool owned by the equipment producer) is:

$$\varphi_1 = \beta + (1-\beta)\alpha(1-H)$$

In the voting game we consider four cases, depending on the preferences of Pool 1 and Pool 2.

Case 1: $z_1 = z_2 = A$. The fraction of votes for proposal A is

$$\beta + (1-\beta)\left(\alpha + (1-\alpha)\rho\right). \tag{109}$$

Case 2: $z_1 = A$ and $z_2 = B$. The fraction of votes for proposal A is

$$\beta + (1-\beta)\left(\alpha(1-H) + (1-\alpha)\rho\right). \tag{110}$$

Case 3: $z_1 = B$ and $z_2 = A$. The fraction of votes for proposal A is

$$(1-\beta)\left(\alpha H + (1-\alpha)\rho\right). \tag{111}$$

Case 4: $z_1 = z_2 = B$. The fraction of votes for proposal A is

$$(1-\beta)(1-\alpha)\rho. \tag{112}$$

The probability that Pool 1's preferred proposal is adopted is then:

$$I = \begin{cases} \frac{1-2\alpha H(1-\beta)\phi}{2(1-\alpha)(1-\beta)} & \text{if } \beta < \frac{0.5-\alpha}{1-\alpha} \\ 1 - \frac{0.5-\alpha(1-H)-\beta(1-\alpha(1-H))}{2(1-\alpha)(1-\beta)}\phi & \text{if } \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} > \beta \geq \frac{0.5-\alpha}{1-\alpha} \\ 1 & \text{if } \beta \geq \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} \end{cases}, \tag{113}$$

where ϕ is the probability that the two Pools disagree (that is, Case 2 and Case 3). It follows that

$$\frac{\partial I}{\partial \beta} = \begin{cases} \frac{1}{2(1-\alpha)(1-\beta)^2} & \text{if } \beta < \frac{0.5-\alpha}{1-\alpha} \\ \frac{0.5\phi}{2(1-\alpha)(1-\beta)^2} & \text{if } \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} > \beta \geq \frac{0.5-\alpha}{1-\alpha} \\ 0 & \text{if } \beta \geq \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} \end{cases}. \tag{114}$$

The expected profit of the equipment producer is:

$$\Pi_1 + \pi_1 = \frac{r\left[c - \underline{c} + f_1(1-H) - \beta\left(\mu - f_2 H - \sigma\right)\right]}{c - \mu + f_1(1-H) + f_2 H} + b_1 I \tag{115}$$

and therefore the first order condition with respect to β (the amount of self mining) is

$$\frac{\partial\left(\Pi_1+\pi_1\right)}{\partial\beta}=-\frac{r\left(\mu-f_2H-\sigma\right)}{c-\mu+f_1\left(1-H\right)+f_2H}+b_1\frac{\partial I}{\partial\beta}=0. \tag{116}$$

There will be some level of self mining in equilibrium if, for $\beta=0$,

$$\frac{\partial\left(\Pi_1+\pi_1\right)}{\partial\beta}=-\frac{r\left(\mu-f_2H-\sigma\right)}{c-\mu+f_1\left(1-H\right)+f_2H}+b_1\frac{\partial I}{\partial\beta}>0, \tag{117}$$

that is,

$$-\frac{r\left(\mu-f_2H-\sigma\right)}{c-\mu+f_1\left(1-H\right)+f_2H}+\frac{b_1}{2\left(1-\alpha\right)}>0. \tag{118}$$

If $\frac{b_1}{2(1-\alpha)}>\frac{r(\mu-\sigma)}{c-\mu}$, then condition (118) always holds and $\beta>0$ in equilibrium. ■

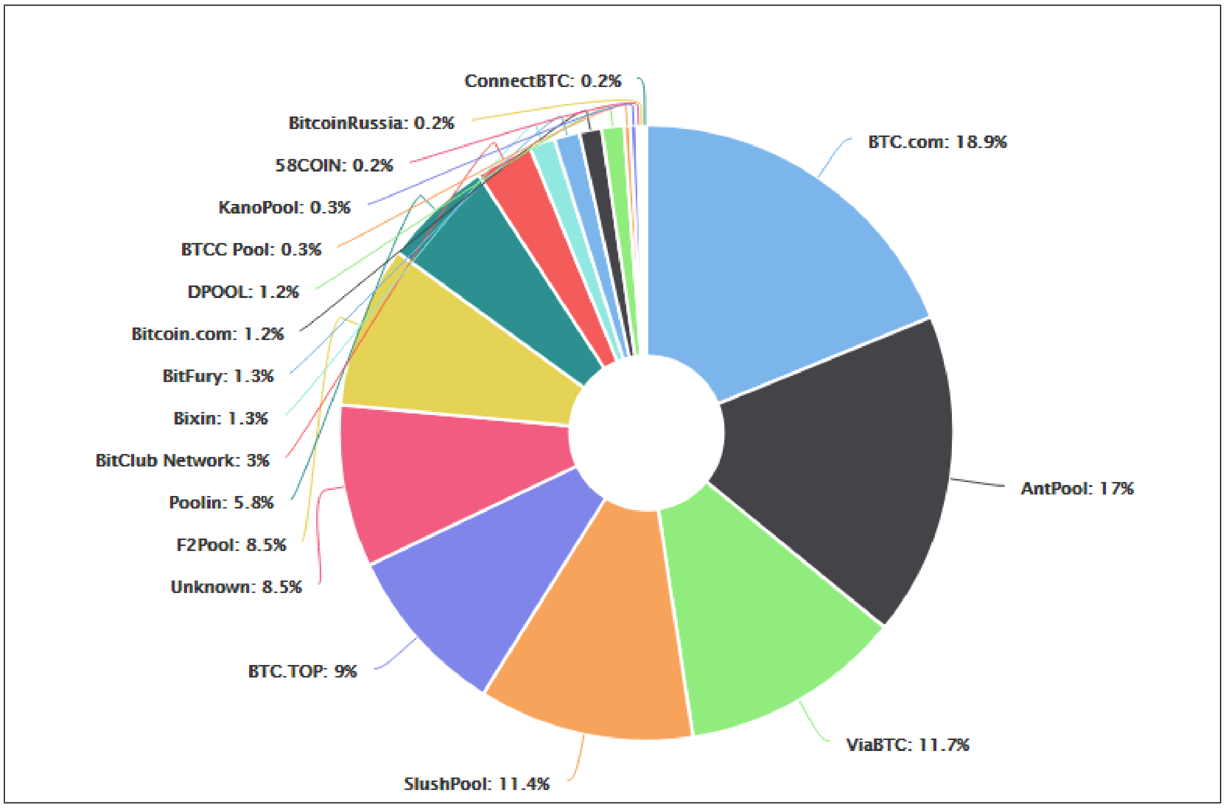

Figure 1. Bitcoin Hashrate Distribution (September 2018)