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

January 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 two-way 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

1. Introduction

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

All blockchains have rules that govern their operations. As blockchain stakeholders' views about the adequacy of the existing rules evolve, these rules may change over time.

*We thank Ulf Axelson, Giulio Fella, Peter Kondor, Igor Makarov, Jason Sturgess, Kostas Zachariadis, and seminar participants at LSE, QMUL, and the early ideas session of the Olin Business School Corporate Finance conference for comments and suggestions, and Bo Tang for research assistance.

[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/

Blockchains thus need a governance system for deciding how to change rules. When designing such a system, blockchains face a similar problem as corporations do, which is how to avoid capture by interest groups. Corporations address this problem by a combination of direct voting by shareholders and monitoring by boards of directors. By contrast, stakeholders of public blockchains typically do not delegate monitoring to boards or other centralized governance committees.[2] Instead, the decision making process is governed by some form of direct voting by stakeholders.

The *proof-of-work system* is the main decentralized governance mechanism adopted by the largest blockchains.[3] In the proof-of-work system, players, called *miners*, enter into 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 computer power they allocate to the process of mining a block. The proof-of-work system is more than just a mechanism for validating transactions. For example, if there are competing versions of the same blockchain, each version with its own set of rules, miners collectively "vote" for their preferred set of rules by allocating their computing power to one of the chains. According to Bitcoin's founder Satoshi Nakamoto (2008), "*[the proof-of-work] solves the problem of determining representation in majority decision making. (...) Proof-of-work is essentially one-CPU-one-vote.*"

Nakamoto's vision on 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 can 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. Will the emergence of such stakeholders have a substantial effect on blockchain governance? If so, what factors determine their importance? Will Nakamoto's vision on blockchain governance be preserved?

In this paper, we develop a theory of blockchain governance that addresses these ques-

[2] There are some exceptions. An example of centralized governance in distributed blockchains is the "delegated proof-of-stake" system, which is used by EOS, among others. In such a system, stakeholders vote for delegates who then directly monitor the blockchain.

[3] The second most popular system is called *proof-of-stake*. We briefly discuss proof-of-stake in Section 8.

tions. 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 our model, we analyze the two-way interactions between blockchain governance and the market structure of the industries in the mining ecosystem. Most of 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.

Consistent with what we observe empirically in proof-of-work blockchains such as Bitcoin, in our model the proof-of-work system creates a mining ecosystem with specialized equipment producers and mining pool operators. We show that, in this ecosystem, a single firm dominates the market for specialized mining equipment. The dominant equipment producer thus has incentives to foster competition in the mining pool services market, because lower prices for pool services make mining more attractive and thus increase the demand for mining equipment. The equipment producer can lower prices for pool services by entering the pool services market. Our model then predicts that the equipment producer is also a large player in the mining pool services market. Since the managers of the mining pools decide which blocks to mine, by controlling a large share of the mining pool market the equipment producer has a disproportionate influence on the governance of the blockchain. That is, the governance of the blockchain is captured by a large corporate stakeholder.

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 delivers more hashes per unit of time (the hash rate) than the existing available technology (e.g. CPU or GPU). Hash rate 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).

Mining pools offer differentiated services. Pools differentiate themselves in a number of attributes, such as the method of payment, software used, technical specifications, size, and geographic location. In the model, 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. Lower fees provide incentives for more agents to become miners, 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 (see Farrell and Katz, 2000).

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 market. The dominant equipment producer thus controls a significant fraction of the hash rate, which gives the producer a disproportionate influence on the governance of the blockchain.

We show that the equipment producer has incentives to control a large share of the pool market 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.

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) analyze competition among miners in proof-of-work blockchains as a standard model of R&D racing. Huberman, Leshno and Moallemi (2017) develop a model of mining

that can be used to determine the equilibrium value of Bitcoin transaction fees. In all of these models, the equilibrium number of miners is determined by a free-entry condition. Following this literature, in this paper we use a similar baseline model of mining in which the equilibrium number of miners is also determined by free entry. Also related to our work is Cong, He, and Li (2018), who model how competition among pools affects equilibrium fees and pool sizes. 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 (2018) 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 (2017) 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.

Our paper incorporates some of the insights found in the industrial organization literature. Farrell and Katz (2000) show that a monopolist has incentives to enter in the market for a complementary good in order to squeeze the profits in that market, thus leaving more surplus to consumers. This surplus then increases the demand for the monopolist's good. Similar to our model, the literature on strategic motives for bundling also considers how firms can leverage their market power in one market to reinforce their market power in another market (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. Examples include Shleifer and Vishny (1986), Winton (1993), Zwiebel (1995), Burkart, Gromb, and Panunzi (1997, 2000), Bolton and von Thadden (1998), Maug (1998), Bennedsen and Wolfenzon (2000), Noe (2002), and Edmans and Manso (2011). See also Edmans (2014) for a review of this literature.

2. Institutional Details

Since the introduction of Nakamoto's (2008) version of the 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 the blockchain technology is Bitcoin, which is a virtual currency operating through a blockchain. In 2018, the largest cryptocurrencies were Bitcoin, Ether (Ethereum), XRP (Ripple), Bitcoin Cash, and EOS.[4]

2.1. Bitcoin Basics

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 also 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 or not 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

[4]See www.coinmarketcap.com.

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 in the early years most miners used generic CPU or GPU equipment, currently most mining is done by specialized hardware (called application specific integrated circuit – ASIC), which is many times more efficient than GPUs or CPUs. Second, miners must pay for variable costs, of 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 computer 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 about 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 2018, this number was 12.5 bitcoins. 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.

2.2. The Mining Ecosystem

As cryptomining evolved into a specialized economic activity, a number of other goods and services were created to support miners. The most important of such new activities is the provision of insurance to miners. Mining is a risky activity: miners pay upfront 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. The probability of winning such a contest is equal to the proportion of a miner's hash rate (the number of hash guesses per second) to the total hash rate in the network. In 2018, an individual miner who owned a single Bitcoin mining

machine would 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 that are 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.

The largest and most influential player in the Bitcoin mining ecosystem is Bitmain Technologies. Bitmain is a private Chinese (PRC) company whose main business is the design of ASIC chips for mining cryptocurrencies and the sale of mining hardware, also known as "mining rigs." By 2018, Bitmain was the clear leader in ASIC-based cryptocurrency mining hardware industry, with about 74.5% of the global market share (Bitmain Prospectus, 2018). No other company had more than 6% of this market. Bitmain's share of the market is so large that many refer to Bitmain as a monopolist. For our purposes, what is important is that Bitmain has some market power, in the sense of being able to price above marginal cost. Given that Bitmain changes prices frequently following changes to Bitcoin prices, it does indeed look as if Bitmain has substantial market power.

Other than ASIC chip design, Bitmain is also a large player in other segments of the cryptomining 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. Figure 1 shows the Bitcoin hash rate distribution in September 2018. Bitmain also operates mining farms and cloud-mining services. Bitmain's voluntary disclosure of hash rate indicates that the company's proprietary mining activity was responsible for about 3-4% of all hash power used for mining bitcoins in 2018. According to the information disclosed in its IPO documents, Bitmain derived more than 94% of its revenue from sales of mining hardware in 2018.

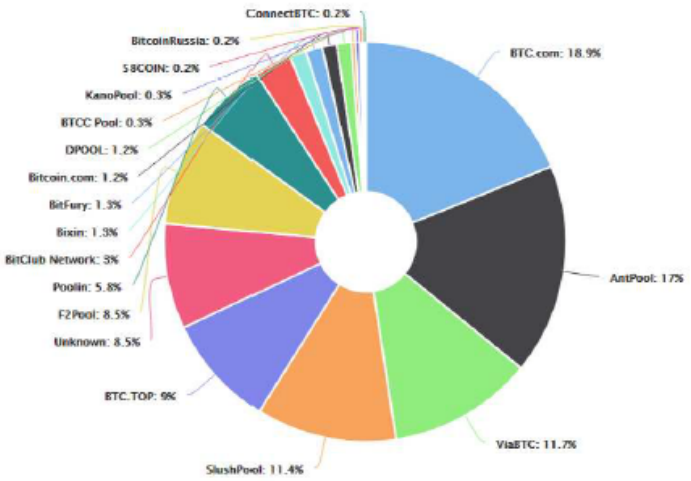

Figure 1. Bitcoin Hashrate Distribution (September 2018)

2.3. Bitcoin Governance

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 (2018), in what is arguably the first complete game-theoretical analysis of the mining game, 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.

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 super-majority of miners (a typical number is 95%) during a given period (measured in blocks). Miners signal their support for a proposal by adding a line to 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 term "voting" is used loosely in Bitcoin governance. Sometimes voting means signaling support for a proposal through messages included in blocks. Sometimes it means running competing software which are ready for future changes should they be agreed, and sometimes it means the decision to adopt an agreed change by upgrading software and following the new rules. What is important for our analysis is the fact that miners play a significant role in the governance of Bitcoin. First, miners are the only ones that can signal support for a particular BIP through mining blocks. Thus, a BIP that doesn't secure sufficient support from miners is essentially dead, even if other players (e.g., developers, exchanges, wallets, etc.) back it. Second, miners can collectively choose to support alternative versions of the blockchain by directing some of their hash power to them. When different groups of stakeholders cannot coordinate on a single set of rules, they can direct their hash power to competing versions of the blockchain, creating what is called a *hard fork*. Leading examples of hard forks that led to currency splits include Bitcoin Cash (August 2017), Bitcoin Gold (October 2017), Bitcoin

Private (February 2018), and the November 2018 "hash wars" that led to the split between Bitcoin Cash ABC and Bitcoin Cash SV.

The outcome that blockchain stakeholders fear the most is a hard fork. Despite this fact, hard forks have occurred, with very damaging consequences, as evidenced by the Bitcoin Cash hash wars in late 2018. Due to its tight grip on the Bitcoin ecosystem, many believe that Bitmain has an outsized influence on the governance of Bitcoin and other related cryptocurrencies, including the ability to create and support hard forks (as an example, Bitmain took the side of Bitcoin Cash ABC, which is the currency widely believed to have "won" the hash wars). Samson Mow (CSO of Blockstream) writes:[5]

> "*Jihan (Bitmain's CEO) does have a lot of control for now, and much of that is simply due to mining centralization. As Bitmain is so vertically integrated, from selling ASICs, to operating mining farms, to running mining pools, he can prevent network upgrade and attempt to hijack the Bitcoin brand with things like Bitcoin Cash.*"

3. Setup

3.1. A Simple Model of Mining

For our benchmark model, 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.[6] At the beginning of each period, players called *miners* rent units of computational power that allow them to try to mine a block. Let $c > 0$ denote the rental cost of the equipment per unit of computational power. In each period, miners who wish to be active pay c in advance for the equipment. For now, we assume that the mining equipment (also known as mining rigs) is a general purpose CPU/GPU chip, thus its rental price c is determined in a larger market; the size of the bitcoin mining industry does not affect c.

Let s denote the net direct surplus from mining, including nonpecuniary benefits (e.g. speculative beliefs, preferences for gambling, risk aversion) minus electricity and other costs. The net direct surplus s excludes the rental cost of the equipment. We normalize miners' outside payoff to zero and assume $c > s$ (otherwise an infinite amount of miners would enter).

[5] http://fortune.com/2017/08/25/bitcoin-mining/

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

Let n denote the number of units of computational power that are active in the mining business. Individual miners are small: for simplicity, we assume that each miner can buy at most one unit of computational power. Thus, n can be also interpreted as the number of miners who are active in a given period.

Let r denote the reward to the miner who wins the mining competition. We represent the period payoff of an active individual miner by

$$U = \frac{r}{n} - c + s. \tag{1}$$

For now, we take both c and s as exogenous. Later we will endogenize each term separately.

Free entry of miners determines the equilibrium number of miners (for simplicity, here we ignore integer constraints):

$$n^* = \frac{r}{c - s}. \tag{2}$$

Free entry implies that all rents from mining are dissipated by competition among miners (see e.g. Budish, 2018). Equation 2 determines the total amount of computational units in the network, n^*, that is, the total hash rate for a given mining period.

3.2. Blockchain Governance

A blockchain may have many stakeholders. Stakeholders can be users, miners, or companies in the blockchain ecosystem, such as exchanges, wallets, mining pools, etc. Each stakeholder may have views about the rules of the blockchain. Differences in views can arise due to differences in preferences, payoff structures, and information.

Let i denote a generic blockchain stakeholder. At the end of each period the blockchain network collectively chooses between two proposals: 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 $z_i \in \{A, B\}$ denote stakeholder i's preference. If stakeholder i's preferred proposal is chosen, they receive utility $b_i > 0$, otherwise they receive zero. Although we assume that the private benefit b_i 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.

A stakeholder's influence over the governance of the blockchain is proportional to the hash rate they control. Suppose that stakeholder i controls hash rate n_i. Let $\varphi_i = \frac{n_i}{n^*}$ denote the proportion of the overall hash rate controlled by stakeholder i. We denote the probability that stakeholder i's preferred proposal is implemented by $I\left(\varphi_i, \varphi_{-i}\right)$, where φ_{-i} is the vector of all other hash rate ratios for all other stakeholders. We assume that this influence function is non decreasing in φ_i, that is, a stakeholder that controls a larger share of the hash rate has (weakly) larger influence on the governance of the blockchain. Given $I\left(\varphi_i, \varphi_{-i}\right)$, i's expected payoff from the choice of proposals is $b_i I\left(\varphi_i, \varphi_{-i}\right)$. We choose to model the decentralized governance system in reduced form for expositional simplicity only. In Section 7, we provide a full microfoundation for the influence function $I\left(\varphi_i, \varphi_{-i}\right)$.[7]

For simplicity, we ignore the effect that influence over proposals may have on a stakeholder's decision to become a miner. Formally, we can either assume that private benefits are sufficiently small (i.e. $b_i \to 0$) or, alternatively, that small individual miners have zero probability of being pivotal in equilibrium:

$$I\left(\frac{1}{n^*+1}; \frac{1}{n^*+1}, ..., \frac{1}{n^*+1}\right) - I\left(0; \frac{1}{n^*}, ..., \frac{1}{n^*}\right) = 0. \tag{3}$$

For the remaining of the paper, we keep the assumption that individual miners do not consider their impact on proposals when deciding to become a miner.

4. A Model of Mining with Specialized Equipment

We now modify the model by introducing a new type of player: Equipment producers 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.

Suppose there are K equipment producers, indexed by $k \in \{1, ..., K\}$. For simplicity, we assume that $b_1 = ... = b_K = 0$, that is, equipment producers enjoy no private benefits from the choice between proposals A or B; we relax this assumption only in Section 7. Let n_k denote the amount of computational power 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

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

from self mining per unit of computational cost is:

$$U_k = \frac{r}{\sum_{k=1}^{K} (n_k + n'_k)} - \underline{c} + s'_k, \tag{4}$$

where s'_k is firm k's net direct surplus from mining. Again we assume $\underline{c} > \max\{s, s'_1, ..., s'_K\}$.

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.

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 this market.

4.1. Single Equipment Producer

If there is a single incumbent equipment producer – Firm k – at time $t \geq k$, we can rewrite (4) as

$$U_k = \frac{r}{n_k + n'_k} - \underline{c} + s'_k. \tag{5}$$

The equipment producer chooses a price p for its machines. Because the producer can also self mine, the free-entry condition for individual miners becomes

$$\frac{r}{n_k + n'_k} - \min\{p, c\} + s \leq 0, \tag{6}$$

that is, miners either enter with zero profit, in which case they buy the cheapest equipment available and pay $\min\{p, c\}$, or they do not enter. 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 write the equipment producer's problem as

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

subject to

$$\frac{r}{n_k + n'_k} - \min\{p, c\} + s \leq 0 \tag{8}$$

$$p \leq c \tag{9}$$

$$n_k, n'_k \geq 0. \tag{10}$$

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 $s'_k < s$, then $n_k^* = \frac{r}{c-s}$ and $n_k'^* = 0$.*
2. *If $s'_k > s$, then $n_k^* = 0$ and $n_k'^* = \frac{r}{c-s}$.*
3. *If $s'_k = s$, 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, due to the fact that miners impose an externality on one another, and thus total surplus decreases with the number of miners. 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 $s'_k > s$, because whoever has a (non-transferrable) comparative advantage at mining (i.e., the party with higher net direct surplus) does all the mining. Third, the total number of miners is always determined by the entry condition for individual miners, even when the equipment producer is the sole miner.

4.2. 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 l); 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, they both enjoy the same net direct surplus $s'_k = s'_l = s'$.

Proposition 2 *There are three cases:*

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

In Case 1, the equipment firms have no special advantage at mining, thus in equilibrium they both 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.[8] Note also that in any equilibrium in which the amount of computational power sold is strictly positive, profits are zero for both firms and $s' \leq s$.

4.3. Entry in the Specialized Equipment Industry

We now consider the decision to enter into the mining equipment market. 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.

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.*

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).

[8] Dimitri (2017) models competition among non-atomistic miners as Cournot competition and also shows that miners have positive profits in equilibrium.

For the remaining of the paper, we assume that the equipment producer does not have a comparative advantage in mining, that is we set $s' < s$. 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.

4.4. 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. This is in line with the observed market structure in the Bitcoin ecosystem: the leading cryptocurrency mining ASIC producer – Bitmain Technologies – has about 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 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.

(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 transferrable: miners can buy 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 non-transferrable (i.e. reflected in s and s', such as local electricity costs) determine who becomes active miners.[9]

[9] With cloud mining, even comparative advantages in electricity costs are transferrable.

5. A Model of Mining with Mining Pools

We now introduce a third type of player: Mining pools. Pools differentiate themselves in a number of attributes, such as the method of payment, software used, technical specifications, size, and geographic location. We thus 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 υ_{ij} denote i's valuation of the unique combination of attributes offered by pool j.[10] Let f_j denote the fee charged by pool j. For each miner i, their surplus from joining pool j is thus

$$s_{ij} = \upsilon_{ij} - f_j. \tag{11}$$

We assume that miners do not know their exact valuation υ_{ij} before deciding whether to enter or not the mining market. To consider the simplest scenario possible, we assume that, for a given pool, valuations are independent and identically distributed, with density function $g(\upsilon)$ over the support $[\underline{\upsilon}, \overline{\upsilon}]$, with $\underline{\upsilon} > 0$, $\overline{\upsilon}$ finite, cdf $G(\cdot)$ and mean μ. As in the previous section, we assume $\mu < \underline{c}$, otherwise there would be an infinite number of active miners.

For simplicity, we consider the case in which there are only two incumbent mining pools. We assume that one of the mining pools is fully owned by the equipment producer, which we call Pool 1. In Section 6 we analyze players' decisions to enter the mining pool business, including the equipment producer's decision to enter this market.

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

[10] As there are no dynamic interactions in the game played by pools, we drop time subscripts to save on notation.

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.

For each period t, the time line 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 computational power from the producer at price c (see Proposition 1).

Date 3: Miners learn their v_{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. The probability that Pool 1's preferred proposal is adopted is $I(f_1^*, f_2^*) \equiv I(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*))$.

At Date 3, after miner i discovers v_{ij} for each pool $j \in \{1, 2\}$, the miner chooses which pool to join. We assume that $\underline{v}$ is sufficiently high so that, in equilibrium, a miner always prefers one of the two pools to mining without a pool.[11] Thus, the miner's problem at Date 3 is to:

$$s_i = \max_{j \in \{1,2\}} v_{ij} - f_j. \tag{12}$$

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 $\Pr(v_{i1} - v_{i2} \geq f_1^* - f_2^*)$. Because all valuations are identically and independently distributed, the distribution of $v_{i1} - v_{i2}$ is symmetric with zero mean, with support $[-(\overline{v} - \underline{v}), (\overline{v} - \underline{v})]$. Let $H(.)$ denote the cumulative distribution function for $v_{i1} - v_{i2}$ (note that $H(0) = 0.5$).

At Date 2, let $E(s_i)$ denote the expectation of s_i as defined in (12). Because all miners

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

are identical at this date, then $E(s_i) = \mu - E[f^*]$, where

$$E[f^*] \equiv f_1^* \left(1 - H(f_1^* - f_2^*)\right) + f_2^* H(f_1^* - f_2^*). \tag{13}$$

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

Because we have assumed $s' < s = \mu - E[f^*]$, Proposition 1 implies that there is no self-mining in equilibrium ($n_1' = 0$) and $p = c$. The number of miners $n_1 = n^*$ who decide to enter at this date is determined by the free entry condition as in (6):

$$n^* = \frac{r}{c - \mu + E[f^*]}. \tag{14}$$

At Date 1, mining pools anticipate the behavior of miners as given in (14), and choose fees simultaneously to maximize their profits. Here we assume that pools care only about their profits, i.e., we assume they have zero private benefits ($b_1 = b_2 = 0$). We relax this assumption in Section 7.

Pools' problem is to

$$\max_{f_1} \Pi_1(f_1, f_2) + \pi(f_1, f_2) = \frac{r f_1 \left(1 - H(f_1 - f_2)\right)}{c - \mu + e(f_1, f_2)} + \frac{r(c - \underline{c})}{c - \mu + e(f_1, f_2)}, \tag{15}$$

$$\max_{f_2} \Pi_2(f_1, f_2) = \frac{r f_2 H(f_1 - f_2)}{c - \mu + e(f_1, f_2)}, \tag{16}$$

where

$$e(f_1, f_2) \equiv f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2). \tag{17}$$

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 a larger number of miners than does an independent pool. The equipment

producer benefits not only from having more customers in the pool market but also from higher demand for its equipment. Thus, the producer has incentives to squeeze the profits in the pool market; it does so by lowering prices so that more agents enter the mining market and rent computational power from the equipment producer. 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 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 Section 6.

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. To see this, 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 5 *Let $\pi(f_1, f_2)$ denote the profit in the market for equipment and let $\Pi_1(f_1, f_2)$ and $\Pi_2(f_1, f_2)$ 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.

6. 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 modify slightly the time line 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 computational power from the producer at price c.

Date 3: Miners learn their v_{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 (25), 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.[12]

The option to choose between the two different modes of entry matters. In the previous sections, 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:

[12]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 few owners not related to Bitmain.

Proposition 6 *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. But 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.[13]

The possibility demonstrated by Proposition 6 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:*

$$(c-\mu)\left(\frac{1}{h(0)}-2\underline{\upsilon}\right)\leq\underline{\upsilon}\left(2\underline{\upsilon}-\frac{1}{2}\right). \tag{18}$$

Condition (18) is necessary and sufficient for equilibrium fees to fall after the entry of a new pool. Alternatively, we could have assumed 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 (18), thus our results go through even in the absence of strategic complementarity.

Proposition 7 *If condition (18) holds, the equipment producer has stronger incentives to enter the mining pool market than an independently owned pool does.*

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

[13] 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.

The intuition for Proposition 7 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, thus the producer is willing to absorb lower profits in the pool market.

In the proof of Proposition 7, we show that the equipment producer's incentive to enter relative to an independent entrant is

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

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 blockchain becomes more successful, that is, as crypto prices increase (higher r) and the equipment producer becomes more efficient (lower $\underline{c}$).

7. Voting on Proposals

In this section, we provide an explicit model of voting on proposals. This model is meant as a microfoundation for the influence function $I\left(\varphi_i, \varphi_{-i}\right)$ introduced in Subsection 3.2.

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.[14] 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 $z_i = A$. 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. Suppose that the number of active miners is n; active miners are drawn randomly from the population of stakeholders. For simplicity, we assume that n 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). By the Law of Large Numbers, the proportion of active 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 $\rho \geq \frac{1}{2}$.

In contrast with the fully decentralized benchmark, a mining pool may have a direct effect on the outcome of the vote. As explained in Section 5, pool managers have control over a fraction $\alpha \in \left(0, \frac{1}{2}\right)$ of the votes in their pools. Here, in contrast with Section 5, we assume that $b_j > 0$, for pool $j = 1, 2$.

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 5. Finally, we also consider the case in which the equipment producer may find it optimal to self-mine.

7.1. Exogenous Market Shares

As in Section 5, 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. Because the mining pools are not atomistic, their preferences for proposals can affect the outcome of the vote. As mining pool managers are also stakeholders, they have their own private benefits (that is, $b_j > 0$).

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

Suppose that the fully decentralized 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

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

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

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

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

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

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

$$\Pr\left(\alpha(1-H) + (1-\alpha)\,\rho \geq \frac{1}{2} \mid \rho \leq \frac{1}{2}\right) = \max\left\{\frac{\alpha(1-2H)}{1-\alpha}, 0\right\}. \tag{22}$$

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 non-atomistic 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 obtains.

7.2. 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_i's of the other stakeholders, $i \neq 1, 2$. Let ϕ denote the probability that $z_1 \neq z_2$.

The influence functions of the pools can be explicitly written as

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

$$I(f_2, f_1) = \frac{1 - 2\alpha(1 - H(f_1 - f_2))\phi}{2(1-\alpha)}. \tag{24}$$

At Date 1, mining pools choose fees simultaneously to maximize their payoffs:

$$\max_{f_1} \Pi_1(f_1, f_2) + \pi(f_1, f_2) + b_1 I(f_1, f_2) \tag{25}$$

$$\max_{f_2} \Pi_2(f_1, f_2) + b_2 I(f_2, f_1), \tag{26}$$

where $\Pi_j(f_1, f_2)$, $j = 1, 2$, and $\pi(f_1, f_2)$ are given by (15) and (16).

In Section 5, 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 8 *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.

7.3. Self-Mining

We have assumed that the equipment producer has no comparative advantage at mining, that is, s' 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 9 *In any equilibrium, a sufficient condition for the equipment producer to self-mine is:*

$$\frac{b_1}{2(1-\alpha)} > \frac{r(\mu - s')}{c - \mu}. \tag{27}$$

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 (27), note that $\mu - s'$ is a measure of the comparative advantage at mining that individuals 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. Similar, $c - \mu$ 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.

8. 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.

Our model fits the description of the bitcoin mining ecosystem, where the dominant specialized equipment producer is also the largest player in the pool services market. There has been a number of instances when Bitmain Technologies – the leading cryptomining ASIC chip designer – has used its control over a substantial proportion of the hash rate to leave its mark on the governance of blockchains. Control over hash rate can be used to enforce hard forks. Hard forks can lead to significant losses to blockchain stakeholders. 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.

What factors explain the influence of specialized equipment producers on blockchain governance? We show that the combination of a homogeneous good (hash rate) and sunk entry cost 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 become stronger as the blockchain becomes more successful, that is, as crypto prices increase and the equipment producer becomes more efficient.

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 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.*"[15]

Our model also 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. 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.[16] 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 large 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.

A proof-of-work blockchain is a record-keeping technology based on decentralized trust (Casey and Vigna, 2018). 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, one may ask how a decentralized blockchain differs from a traditional financial intermediary as a provider of trust.

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

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

References

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

Arruñada, B. and L. Garicano. 2017. Hard Forks: Coordinating Change in Blockchain Platforms. *Working Paper.*

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. 2018. The Blockchain Folk Theorem. *Review of Financial Studies.* forthcoming.

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.

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.

Casey, M. J. and P. Vigna. 2018. In Blockchain we Trust. *MIT Technology Review.* 121(3): 10-16.

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.*

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

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

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

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

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

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

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

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

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

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

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

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

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

Shleifer, Andrei, and Robert 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.

9. Appendix: Proofs

Proposition 1.

Proof. Firm k's problem is to

$$\max_{p,n_k,n'_k} \pi_k = (p - \underline{c})n_k + \left(\frac{r}{n_k + n'_k} - \underline{c} + s'_k\right) n'_k, \tag{28}$$

subject to

$$\begin{aligned} \frac{r}{n_k + n'_k} - \min\{p, c\} + s &\leq 0 && (29)\\ p &\leq c && (30)\\ n_k, n'_k &\geq 0. && (31) \end{aligned}$$

First, note that (30) implies $\min\{p, c\} = p$. Suppose now (29) is slack in equilibrium, then we must have $n_k = 0$. The profit function becomes

$$\pi_k = r + (s'_k - \underline{c})\, n'_k, \tag{32}$$

and the producer's profit decreases with n'_k, which implies that (29) must eventually bind. Thus (29) cannot be slack. Because (29) binds, then we can rewrite the profit function as

$$\pi_k = (p - \underline{c})(n_k + n'_k) + (s'_k - s)\, n'_k. \tag{33}$$

If $(s'_k - s) < 0$, then the producer wants the minimum possible n'_k, which implies $n'_k = 0$, and thus

$$n_k = \frac{r}{p - s}. \tag{34}$$

Replacing (34) in the profit function yields:

$$\pi_k = r\frac{p - \underline{c}}{p - s}. \tag{35}$$

Since

$$\frac{\partial \pi_k}{\partial p} = r\frac{\underline{c} - s}{(p - s)^2} > 0, \tag{36}$$

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

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

$$n'_k = \frac{r}{c - s}. \tag{37}$$

Finally, if $(s'_k - s) = 0$ 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

$$\max_{p, n_k, n'_k} \pi_k = (p_k - \underline{c})n_k + \left(\frac{r}{n_k + n'_k + n_l + n'_l} - \underline{c} + s'\right) n'_k, \tag{38}$$

subject to

$$\begin{aligned} \frac{r}{n_k + n'_k + n_l + n'_l} - \min\{p_k, p_l, c\} + s &\leq 0 && (39)\\ p_k &\leq \min\{p_l, c\} && (40)\\ n_k, n'_l &\geq 0. && (41) \end{aligned}$$

Firm l's problem is symmetric.

First, note that, in an equilibrium where both firms sell a positive number of machines, it must be that $p_k = p_l = p$. This follows from usual Bertrand competition reasoning: if, say, $p_k < p_l$, 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: $(s' - s) < 0$. (i) Suppose first that $n^* \equiv n_k + n_l > 0$. Then it follows that $p = \underline{c}$ and thus we have

$$\frac{r}{n_k + n'_k + n_l + n'_l} - \underline{c} + s = 0. \tag{42}$$

The profit function becomes

$$\pi_k = \left(\frac{r}{n_k + n'_k + n_l + n'_l} - \underline{c} + s' \right) n'_k, \tag{43}$$

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

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

(ii) Suppose now that $n^* = 0$. Let $p = \min\{p_k, p_l\}$, and without loss of generality, suppose $p = p_k$. The entry condition is

$$\frac{r}{n'_k + n'_l} - p + s < 0. \tag{44}$$

Firm k's profit is

$$\pi_k = \left(\frac{r}{n'_k + n'_l} - \underline{c} + s' \right) n'_k. \tag{45}$$

Define $n^{**} = n'_k + n'_l$. Because

$$\frac{r}{n^*} - \underline{c} + s = 0, \tag{46}$$

if $n^{**} \geq n^*$ then we would have

$$\pi_k = \left(\frac{r}{n^{**}} - \underline{c} + s' \right) n'_k < 0, \tag{47}$$

which cannot be optimal. Thus, we must have $n^{**} < n^*$. Then, we also have

$$\frac{r}{n^{**}} - p + s < 0, \tag{48}$$

requires $p > \widehat{p} > \underline{c}$, where

$$\widehat{p} = \frac{r}{n^{**}} + s. \tag{49}$$

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

$$\frac{r}{n'_l + n_k} - \widehat{p} + s = 0, \tag{50}$$

which implies $n_k = n'_k$. The profit is then

$$(\widehat{p} - \underline{c})n'_k = \left(\frac{r}{n^{**}} - \underline{c} + s\right) n'_k > \left(\frac{r}{n^{**}} - \underline{c} + s'\right) n'_k, \tag{51}$$

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

We conclude that, if $s' - s < 0$, all equilibria require $n'_k = n'_l = 0$ and both firms make zero profit.

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

$$\max_{n'_k} \pi_k = \left(\frac{r}{n'_k + n'_l} - \underline{c} + s'\right) n'_k, \tag{52}$$

and the first-order condition is

$$\frac{r}{n'_k + n'_l} - \underline{c} + s' - \frac{r n'_k}{\left(n'_k + n'_l\right)^2} = 0. \tag{53}$$

In a symmetric equilibrium, $n'_k = n'_l = n'$ where

$$n' = \frac{r}{4\left(\underline{c} - s'\right)}, \tag{54}$$

provided that the free entry condition is slack:

$$2\left(\underline{c} - s'\right) < c - s. \tag{55}$$

Total profit is then

$$\pi = \frac{r}{4\left(\underline{c} - s'\right)}\left[2\left(\underline{c} - s'\right) - \underline{c} + s'\right] = \frac{r}{4}. \tag{56}$$

If (55) does not hold, we have

$$n' = \frac{r}{2\left(c - s\right)}, \tag{57}$$

and the profit is

$$\pi = \frac{r\left(c - \underline{c} + s' - s\right)}{2\left(c - s\right)}. \tag{58}$$

We now show that this is 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

$$\frac{r}{n_k + n'_l} - \widehat{p} + s = 0, \tag{59}$$

which implies $n_k = n'_k$. Firm k's profit is then

$$(\widehat{p} - \underline{c})n'_k = \left(\frac{r}{n^{**}} - \underline{c} + s\right) n'_k < \left(\frac{r}{n^{**}} - \underline{c} + s'\right) n'_k, \tag{60}$$

thus no profitable deviation exists.

(ii) Suppose now that $n^* > 0$. The entry constraint must be binding:

$$\frac{r}{n_k + n'_k + n_l + n'_l} - \underline{c} + s = 0. \tag{61}$$

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

$$\left(\frac{r}{n_k + n'_k + n_l + n'_l} - \underline{c} + s'\right) n'_k = (s' - s)n'_k > 0 \tag{62}$$

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

We conclude that, if $s' - s > 0$, all equilibria require $n_k = n_l = 0$ and both firms make positive profit.

Case 3: $s' - s = 0$. 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. 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 $s' \leq s$. Thus, assume $s' \leq s$. 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

$$\frac{r\left(c - \underline{c}\right)}{\delta\left(c - s\right)} \geq \iota. \tag{63}$$

If condition (63) 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 (63) holds, otherwise no firm enters. ■

Proposition 4

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

$$\max_{f_1} \Pi_1\left(f_1, f_2\right) + \pi\left(f_1, f_2\right) = \frac{r f_1\left(1 - H(f_1 - f_2)\right)}{c - \mu + e\left(f_1, f_2\right)} + \frac{r\left(c - \underline{c}\right)}{c - \mu + e\left(f_1, f_2\right)}, \tag{64}$$

$$\max_{f_2} \Pi_2\left(f_1, f_2\right) = \frac{r f_2 H(f_1 - f_2)}{c - \mu + e\left(f_1, f_2\right)}, \tag{65}$$

where

$$e\left(f_1, f_2\right) \equiv f_1\left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2). \tag{66}$$

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

$$\left(c - \mu + f_2^* H^*\right)\left(1 - H^*\right) - f_1^* h^*\left(c - \mu + f_2^*\right) - \left(c - \underline{c}\right)(1 - H^* - (f_1^* - f_2^*)h^*) = 0 \tag{67}$$

$$\left(c - \mu + f_1^*\left(1 - H^*\right)\right) H^* - f_2^* h^*(c - \mu + f_1^*) = 0, \tag{68}$$

From equations (67) and (68) we express f_1^* and f_1^* as follows:

$$f_1^* = \left(\frac{c - \mu + f_2^* H^*}{c - \mu + f_2^*}\right)\frac{\left(1 - H^*\right)}{h^*} - \frac{\left(c - \underline{c}\right)(1 - H^* - (f_1^* - f_2^*)h^*)}{(c - \mu + f_2^*)h^*} \tag{69}$$

$$f_2^* = \left(\frac{c - \mu + f_1^*\left(1 - H^*\right)}{c - \mu + f_1^*}\right)\frac{H^*}{h^*} \tag{70}$$

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

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

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

We subtract (72) from (71) and simplify:

$$(f_1^* - f_2^*)\,(\underline{c} - \mu + f_2^*) = \frac{(0.5-\epsilon)\left(c-\mu+f_2^*(0.5+\epsilon)\right)\left(c-\mu+f_1^*\right)}{h^*\left(c-\mu+f_1^*\right)} = \tag{73}$$

$$-\frac{(0.5+\epsilon)\left(c-\mu+f_1^*(0.5-\epsilon)\right)\left(c-\mu+f_2^*\right)}{h^*\left(c-\mu+f_1^*\right)} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} = \tag{74}$$

$$\frac{\left(-2\epsilon(c-\mu)^2 - \left(f_1^*-f_2^*\right)(c-\mu)\left(0.5^2-\epsilon^2\right) + f_1^*(c-\mu)(0.5-\epsilon) - f_2^*(c-\mu)(0.5+\epsilon)\right)}{h^*\left(c-\mu+f_1^*\right)} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} = \tag{75}$$

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

which implies

$$(f_1^* - f_2^*)\, f_2^* \left(\tfrac{\underline{c}-\mu}{f_2^*} + 1 - \tfrac{(c-\mu)(0.5-\epsilon)^2}{f_2^* h^* (c-\mu+f_1)} \right) = -\frac{2\epsilon(c-\mu)\left(c-\mu+f_2^*\right)}{\left(c-\mu+f_1^*\right)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} \tag{76}$$

Since $f_2^* h^* \left(c - \mu + f_1^*\right) = \left(c - \mu + f_1^*\,(0.5-\epsilon)\right)(0.5+\epsilon)$ we can further simplify:

$$(f_1^* - f_2^*)\, f_2^* \left(\tfrac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)(0.5-\epsilon)^2}{\left(c-\mu+f_1^*(0.5-\epsilon)\right)(0.5+\epsilon)} \right) = -\frac{2\epsilon(c-\mu)\left(c-\mu+f_2^*\right)}{\left(c-\mu+f_1^*\right)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*}. \tag{77}$$

First we consider the case where $\epsilon = 0$, that is $H^* = 0.5$. We simplify (77) accordingly

$$(f_1^* - f_2^*)\, f_2^* \left(\frac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)\,0.5}{(c-\mu+f_1^* 0.5)} \right) = -\frac{(c-\underline{c})0.5}{h(0)}. \tag{78}$$

Since $\left(\tfrac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)0.5}{\left(c-\mu+f_1^* 0.5\right)} \right) > 0$, from (78) it follows that $f_1^* < f_2^*$, which is in contradiction with $H^* = 0.5$.

Second we consider the case where $\epsilon > 0$, that is $H^* > 0.5$. Since

$$f_2^* \left(\frac{\underline{c}-\mu}{f_2^*} + 1 - \frac{(c-\mu)\,(0.5-\epsilon)^2}{(c-\mu+f_1^*\,(0.5-\epsilon))\,(0.5+\epsilon)} \right) > 0, \tag{79}$$

and since for $\epsilon > 0$ the right hand side of equation (77) is negative it follows that $f_1^* < f_2^*$, which is in contradiction with $H^* > 0.5$.

Finally we consider the case where $\epsilon < 0$, that is $H^* < 0.5$. In this case we can have a solution where $f_1^* < f_2^*$. So if a solution exist it must be such that $f_1^* < f_2^*$ and $H^* < 0.5$.

Since $\varphi_1(f_1^*, f_2^*) = \alpha(1 - H^*)$ 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 $I(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*)) > I(\varphi_2(f_1^*, f_2^*), \varphi_1(f_1^*, f_2^*))$. ■

Proposition 5.

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

$$\frac{\partial \Pi_1(f_1^*, f_2^*)}{\partial f_1} + \frac{\partial \pi(f_1^*, f_2^*)}{\partial f_1} = 0 \tag{80}$$

$$\frac{\partial \Pi_2(f_1^*, f_2^*)}{\partial f_2} = 0. \tag{81}$$

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

$$\frac{\partial \Pi_2(f_2^*, f_2^*)}{\partial f_2} < 0. \tag{82}$$

Symmetry implies

$$\frac{\partial \Pi_2(f_2^*, f_2^*)}{\partial f_2} = \frac{\partial \Pi_1(f_2^*, f_2^*)}{\partial f_1} < 0. \tag{83}$$

Now, concavity implies

$$\frac{\partial \Pi_1(f_2^*, f_2^*)}{\partial f_1} > \frac{\partial \Pi_1(f_1^*, f_2^*)}{\partial f_1}, \tag{84}$$

and therefore

$$\frac{\partial \Pi_1(f_1^*, f_2^*)}{\partial f_1} < 0. \tag{85}$$

But because $\frac{\partial \pi(f_1, f_2)}{\partial f_1} < 0$, (85) contradicts (80). Thus,there cannot be an equilibrium where $f_1^* \geq f_2^*$.[17] 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 $I(\varphi_1(f_1^*, f_2^*), \varphi_2(f_1^*, f_2^*)) > I(\varphi_2(f_1^*, f_2^*), \varphi_1(f_1^*, f_2^*))$. ■

Proposition 6

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

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:

$$\max_{f_1} \Pi_1 = \frac{r f_1 \left(1 - H(f_1 - f_2)\right)}{c - \mu + f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2)} \tag{86}$$

$$\max_{f_2} \Pi_2 = \frac{r f_2 H(f_1 - f_2)}{c - \mu + f_1 \left(1 - H(f_1 - f_2)\right) + f_2 H(f_1 - f_2)} \tag{87}$$

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

$$\left(c - \mu + f_2^* H^*\right)\left(1 - H^* - f_1^* h^*\right) - f_1^* \left(1 - H^*\right) f_2^* h^* = 0, \tag{88}$$

$$\left(c - \mu + f_1^* \left(1 - H^*\right)\right)\left(H^* - f_2^* h^*\right) - f_2 H^* f_1^* h^* = 0. \tag{89}$$

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

$$f_1^* = \frac{\left(c - \mu + f_2^* H^*\right)\left(1 - H^*\right)}{\left(c - \mu + f_2^*\right) h^*}, \tag{90}$$

$$f_2^* = \frac{\left(c - \mu + f_1^* \left(1 - H^*\right)\right) H^*}{\left(c - \mu + f_1^*\right) h^*}. \tag{91}$$

From (90) and (91)

$$\left(f_1^* - f_2^*\right)\left(1 + \frac{(c-\mu)\left(f_1^* - f_2^*\right) H^* (1 - H^*)}{h^* \left(c - \mu + f_1^*\right)\left(c - \mu + f_2^*\right)}\right) = \frac{(c-\mu)^2 (1 - 2H^*)}{h^* \left(c - \mu + f_1^*\right)\left(c - \mu + f_2^*\right)} \tag{92}$$

which is equivalent to

$$\left(f_1^* - f_2^*\right)\left(1 + \frac{f_2^* (c-\mu)\left(f_1^* - f_2^*\right)(1 - H^*)}{\left(c - \mu + f_1^* (1 - H^*)\right)\left(c - \mu + f_2^*\right)}\right) = \frac{f_2^* (c-\mu)^2 (1 - 2H^*)}{\left(c - \mu + f_1^* (1 - H^*)\right)\left(c - \mu + f_2^*\right) H^*}. \tag{93}$$

First we note that $\left(1 + \frac{f_2^* (c-\mu)\left(f_1^* - f_2^*\right)(1 - H^*)}{\left(c - \mu + f_1^* (1 - H^*)\right)\left(c - \mu + f_2^*\right)}\right) > 0$. Assume that $H^* > 0.5$, then the right hand side of (93) 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 (93) is positive which would imply $f_1^* > f_2^*$,which contradicts $H^* < 0.5$.Since $H(0) = 0.5$, (93) is only satisfied for $f_1^* = f_2^* = f^*$. We can now simplify (90) as follows

$$\left(c - \mu + 0.5 f^*\right)\left(0.5 - f^* h(0)\right) - 0.5 f^{*2} h(0) = 0 \tag{94}$$

$$\Leftrightarrow f^{*2} + f^{*}\left(c - \mu - 0.25\right) - \frac{\left(c-\mu\right)0.5}{h(0)} = 0 \tag{95}$$

$$f^{*} = \frac{\sqrt{\left(c-\mu-0.25\right)^{2} + \frac{2(c-\mu)}{h(0)}} - \left(c-\mu-0.25\right)}{2}. \tag{96}$$

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:

$$\frac{r\left(c-\underline{c}\right)}{c-\mu+e[f_1^{*}, f_2^{*}]} + \frac{r f_1\left(1-H^{*}\right)}{c-\mu+e[f_1^{*}, f_2^{*}]} < \frac{r\left(c-\underline{c}\right)}{c-\mu+f^{*}} + \frac{r0.5f^{*}}{c-\mu+f^{*}}, \tag{97}$$

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 (96). ■

Proposition 7

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:

$$\Pi^{I} \geq \kappa \tag{98}$$

The equipment producer enters the mining pool market if:

$$\max\left\{\Pi^{I} + \pi_1^{I}, \Pi^{C} + \pi_1^{C}\right\} - \pi_1 \geq \kappa \tag{99}$$

A sufficient condition for the equipment producer to have higher incentives to enter the pool

market relative to an independent pool is:

$$\pi_1^I \geq \pi_1 \tag{100}$$

$$\frac{r(c-\underline{c})}{c-\mu+f^*} \geq \frac{r(c-\underline{c})}{c-\mu+f^0}, \tag{101}$$

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 $f^0 \geq \underline{v}$,then a sufficient condition for (101) to hold is:

$$f^* \leq \underline{v} \Leftrightarrow \sqrt{(c-\mu-0.25)^2 + \frac{2(c-\mu)}{h(0)}} < 2\underline{v} + (c-\mu-0.25). \tag{102}$$

Under Assumption 1 condition (102) always holds.

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

$$RI = \frac{r(c-\underline{c})}{c-\mu+f^*} - \frac{r(c-\underline{c})}{c-\mu+f^0} = r(c-\underline{c})\frac{f^0-f^*}{(c-\mu+f^*)(c-\mu+f^0)}. \tag{103}$$

■

Proposition 8.

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

$$\max_{f_1} \Pi_1(f_1,f_2) + \pi(f_1,f_2) + \frac{b_1}{2(1-\alpha)}\left[1-2\alpha H(f_1-f_2)\phi\right] \tag{104}$$

$$\max_{f_2} \Pi_2(f_1,f_2) + \frac{b_2}{2(1-\alpha)}\left[1-2\alpha\left(1-H(f_1-f_2)\right)\phi\right], \tag{105}$$

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:

$$(c-\mu+f_2^*H^*)(1-H^*) - f_1^*h^*(c-\mu+f_2^*) - (c-\underline{c})(1-H^*-(f_1^*-f_2^*)h^*) - \tfrac{b_1\alpha\phi h^* n^2}{(1-\alpha)r} = 0, \tag{106}$$

$$(c-\mu+f_1^*(1-H^*))H^* - f_2^*h^*(c-\mu+f_1^*) - \tfrac{b_2\alpha\phi h^* n^2}{(1-\alpha)r} = 0. \tag{107}$$

From equations (106) and (107) we express f_1^* and f_1^* as follows

$$f_1^* = \left(\frac{c-\mu+f_2^* H^*}{c-\mu+f_2^*}\right)\frac{(1-H^*)}{h^*} - \frac{(c-\underline{c})(1-H^*-(f_1^*-f_2^*)h^*)}{(c-\mu+f_2^*)h^*} - \frac{b_1\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r}, \tag{108}$$

$$f_2^* = \left(\frac{c-\mu+f_1^*(1-H^*)}{c-\mu+f_1^*}\right)\frac{H^*}{h^*} - \frac{b_2\alpha\phi n^2}{(1-\alpha)(c-\mu+f_1^*)r}. \tag{109}$$

Let $H^* \equiv 0.5+\epsilon$, then (108) and (109) can be rewritten as follows:

$$f_1^* = \left(\frac{c-\mu+f_2^*(0.5+\epsilon)}{c-\mu+f_2^*}\right)\frac{(0.5-\epsilon)}{h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{(c-\mu+f_2^*)h^*} + \frac{(f_1^*-f_2^*)(c-\underline{c})}{(c-\mu+f_2^*)} - \frac{b_1\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r} \tag{110}$$

$$f_2^* = \left(\frac{c-\mu+f_1^*(0.5-\epsilon)}{c-\mu+f_1^*}\right)\frac{(0.5+\epsilon)}{h^*} - \frac{b_2\alpha\phi n^2}{(1-\alpha)(c-\mu+f_2^*)r} \tag{111}$$

We subtract (111) from (110) and simplify:

$$\begin{aligned}(f_1^*-f_2^*)(\underline{c}-\mu+f_2^*) = \; & \frac{(0.5-\epsilon)\big(c-\mu+f_2^*(0.5+\epsilon)\big)\big(c-\mu+f_1^*\big)}{h^*\big(c-\mu+f_1^*\big)} - \frac{\alpha\phi\big(b_1(c-\mu+f_1^*)-b_2(c-\mu+f_2^*)\big)n^2}{(1-\alpha)(c-\mu+f_1^*)r} \\ & - \frac{(0.5+\epsilon)\big(c-\mu+f_1^*(0.5-\epsilon)\big)\big(c-\mu+f_2^*\big)}{h^*\big(c-\mu+f_1^*\big)} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*}\end{aligned} \tag{112}$$

$$\begin{aligned}(f_1^*-f_2^*)(\underline{c}-\mu+f_2^*) = \; & \frac{\big(-2\epsilon(c-\mu)^2-\big(f_1^*-f_2^*\big)(c-\mu)\big(0.5^2-\epsilon^2\big)+f_1^*(c-\mu)(0.5-\epsilon)-f_2^*(c-\mu)(0.5+\epsilon)\big)}{h^*\big(c-\mu+f_1^*\big)} \\ & - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} - \frac{\alpha(\phi_2+\phi_3)((b_1-b_2)(c-\mu))n^2}{(1-\alpha)(c-\mu+f_1^*)r} - \frac{\alpha(\phi_2+\phi_3)\big(b_1f_1^*-b_2f_2^*\big)n^2}{(1-\alpha)(c-\mu+f_1^*)r}\end{aligned} \tag{113}$$

$$\begin{aligned}(f_1^*-f_2^*)f_2^*\left(\frac{\underline{c}-\mu}{f_2^*}+1-\frac{(c-\mu)(0.5-\epsilon)^2}{f_2^*h^*(c-\mu+f_1)}\right) = \; & -\frac{2\epsilon(c-\mu)\big(c-\mu+f_2^*\big)}{\big(c-\mu+f_1^*\big)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*} \\ & - \frac{\alpha\phi(b_1-b_2)(c-\mu)n^2}{(1-\alpha)(c-\mu+f_1^*)r} - \frac{\alpha\phi\big(b_1f_1^*-b_2f_2^*\big)n^2}{(1-\alpha)(c-\mu+f_1^*)r}\end{aligned}. \tag{113}$$

For $b_1 = b_2 = b$:

$$(f_1^*-f_2^*)f_2^*\left(\frac{\underline{c}-\mu}{f_2^*}+1-\frac{(c-\mu)(0.5-\epsilon)^2}{f_2^*h^*(c-\mu+f_1)}+\frac{\alpha\phi bn^2}{f_2^*(1-\alpha)(c-\mu+f_1^*)r}\right) = -\frac{2\epsilon(c-\mu)\big(c-\mu+f_2^*\big)}{\big(c-\mu+f_1^*\big)h^*} - \frac{(c-\underline{c})(0.5-\epsilon)}{h^*}. \tag{114}$$

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

Proposition 9.

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 equilibrium proportion of hash rate controlled by

Pool 1 (the pool owned by the equipment producer) is:

$$\varphi_1(f_1^*, f_2^*, \beta^*) = \beta^* + (1-\beta^*)\alpha(1-H^*)$$

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

$$\beta + (1-\beta)\left(\alpha + (1-\alpha)\rho\right). \tag{115}$$

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

$$\beta + (1-\beta)\left(\alpha(1-H) + (1-\alpha)\rho\right). \tag{116}$$

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

$$(1-\beta)\left(\alpha H + (1-\alpha)\rho\right) \tag{117}$$

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

$$(1-\beta)(1-\alpha)\rho \tag{118}$$

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

$$I(f_1, f_2, \beta) = \begin{cases} \frac{1-2\alpha H(1-\beta)\phi}{2(1-\alpha)(1-\beta)} & \text{if } \beta < \frac{0.5-\alpha}{1-\alpha} \\ 1 - \frac{0.5-\alpha(1-H)-\beta(1-\alpha(1-H))}{2(1-\alpha)(1-\beta)}\phi & \text{if } \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} > \beta \geq \frac{0.5-\alpha}{1-\alpha} \\ 1 & \text{if } \beta \geq \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} \end{cases}, \tag{119}$$

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

$$\frac{\partial I(f_1, f_2, \beta)}{\partial \beta} = \begin{cases} \frac{1}{2(1-\alpha)(1-\beta)^2} & \text{if } \beta < \frac{0.5-\alpha}{1-\alpha} \\ \frac{0.5\phi}{2(1-\alpha)(1-\beta)^2} & \text{if } \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} > \beta \geq \frac{0.5-\alpha}{1-\alpha} \\ 0 & \text{if } \beta \geq \frac{0.5-\alpha+\alpha H}{1-\alpha+\alpha H} \end{cases}. \tag{120}$$

The expected profit of the equipment producer is:

$$\Pi_1 + \pi_1 = \frac{r\left[c - \underline{c} + f_1\left(1 - H\right) - \beta\left(\mu - f_2 H - s^{'}\right)\right]}{c - \mu + f_1\left(1 - H\right) + f_2 H} + b_1 I(f_1, f_2, \beta) \tag{121}$$

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

$$\frac{\partial\left(\Pi_1 + \pi_1\right)}{\partial\beta} = -\frac{r\left(\mu - f_2 H - s^{'}\right)}{c - \mu + f_1\left(1 - H\right) + f_2 H} + b_1 \frac{\partial I(f_1, f_2, \beta)}{\partial\beta} = 0. \tag{122}$$

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

$$\frac{\partial\left(\Pi_1 + \pi_1\right)}{\partial\beta} = -\frac{r\left(\mu - f_2 H - s^{'}\right)}{c - \mu + f_1\left(1 - H\right) + f_2 H} + b_1 \frac{\partial I(f_1, f_2, \beta)}{\partial\beta} > 0, \tag{123}$$

that is

$$-\frac{r\left(\mu - f_2 H - s^{'}\right)}{c - \mu + f_1\left(1 - H\right) + f_2 H} + \frac{b_1}{2\left(1 - \alpha\right)} > 0. \tag{124}$$

If $\frac{b_1}{2(1-\alpha)} > \frac{r(\mu - s')}{c - \mu}$, then condition (124) always holds and $\beta > 0$ in equilibrium. ■