NBER WORKING PAPER SERIES

DECENTRALIZED MINING IN CENTRALIZED POOLS

Lin William Cong
Zhiguo He
Jiasun Li

Working Paper 25592
http://www.nber.org/papers/w25592

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
February 2019, Revised January 2019

We thank Foteini Baldimtsi, Joseph Bonneau, Matthieu Bouvard, Bhagwan Chowdhry, Douglas Diamond, Hanna Halaburda, Wei Jiang, Evgeny Lyandres, Ye Li, Richard Lowery, Maureen O'Hara, George Panayotov, Fahad Saleh, Katrin Tinn, Liyan Yang, David Yermack, and Xin Wang for helpful discussions, as well as Tianshu Lyu, Zhenping Wang, Xiao Yin, and Xiao Zhang for excellent research assistance. We also thank seminar audiences at Ant Financial, Chicago Booth, CKGSB, Cleveland Fed, Columbia GSB, Cornell, CUNY Baruch, Duke, George Mason, HKU, University of Houston, University of Maryland, Michigan University, NYU, Tsinghua PBC, Princeton, Rice University, Stanford, UNC (Microeconomic Theory), Yale, as well as conference participants at Asian Development Bank Conference on FinTech, Becker Friedman Institute Conference on Cryptocurrencies and Blockchains, CEPR Gerzensee ESSFM Workshop, CIFFP, Credit and the Future of Banking Conference (Rigi Kaltbad), DataYes & ACM KDD China FinTech AI Workshop, Econometric Society NA Meeting, Georgia State FinTech Conference, Harvard CMSA Blockchain Conference, ISB Summer Conference, Midwest Finance Association Meeting, Northern Finance Association Meeting, SAIF Summer Institute, Simons Institute for the Theory of Computing at UC Berkeley, SFS Cavalcade Asia-Pacific, and 2nd Toronto FinTech Conference for helpful comments and discussions. This research was funded in part by the Ewing Marion Kauffman Foundation. The contents of this publication are solely the responsibility of the authors. We are equally grateful for funding from the Initiative on Global Markets, the Stigler Center, and the Center for Research in Security Prices at the University of Chicago, and from the Multidisciplinary Research (MDR) Initiative in Modeling, Simulation and Data Analytics at George Mason. The views expressed herein are those of the authors and do not necessarily reflect the views of the National Bureau of Economic Research.

Decentralized Mining in Centralized Pools
Lin William Cong, Zhiguo He, and Jiasun Li
NBER Working Paper No. 25592
February 2019, Revised January 2019
JEL No. D43,G2,G22,L13,L44

ABSTRACT

The rise of centralized mining pools for risk sharing does not necessarily undermine the decentralization required for permissionless blockchains: Each individual miner's cross-pool diversification and endogenous fees charged by pools generally sustain decentralization, because larger pools better internalize their externality on global hash rates, charge higher fees, attract disproportionately fewer miners, and thus grow more slowly. Instead, mining pools as a financial innovation escalate the arms race among competing miners and thus significantly increase the energy consumption of proof-of-work-based consensus mechanisms. Empirical evidence from Bitcoin mining supports our model predictions. The economic insights inform many other blockchain protocols as well as the industrial organization of mainstream sectors with similar characteristics but ambiguous prior findings.

Lin William Cong
Cornell University
Ithaca, NY 14853
will.cong@cornell.edu

Zhiguo He
University of Chicago
Booth School of Business
5807 S. Woodlawn Avenue
Chicago, IL 60637
and NBER
zhiguo.he@chicagobooth.edu

Jiasun Li
George Mason University School of Business
4400 University Drive, MSN 5F5
Fairfax, Virg 22030
United States
jli29@gmu.edu

1 Introduction

Digital transactions traditionally rely on central record-keepers, who are trusted to behave honestly and to be sophisticated enough to defend against cyber-vulnerabilities. Blockchains instead can decentralize record-keeping, with the best-known application being the P2P payment system Bitcoin (Nakamoto, 2008). The majority of (permissionless) blockchains thus far rely on various forms proof-of-work (PoW) protocols, often known as "mining," in which independent computers ("miners") dispersed all over the world spend resources and compete repeatedly for the right to record new blocks of transactions, and the winner in each round gets rewarded. Independent miners have incentives to honestly record transactions because rewards are valid only if their records are endorsed by subsequent miners.

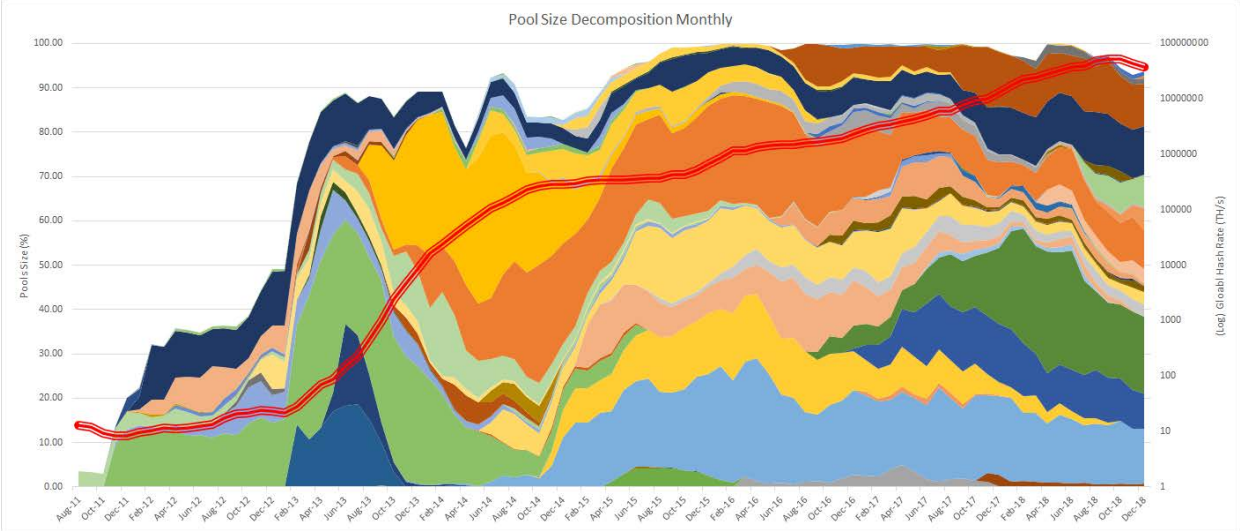
Compared to a centralized system, a blockchain has several advantages, including enhanced robustness to cyber-attacks or mechanical glitches from the removal of any "single point of failure" (e.g., Equifax scandal, Economist, 2017). A blockchain is also presumably less vulnerable to misbehaviors or censorships, as it shifts the trust on the stewardship of a central book-keeper to the selfish economic incentives of a large number of competitive miners. However, these advantages rely on adequate decentralization of the system, which is thus far only a *technological* possibility rather than a guaranteed *economic* reality. Indeed, while Nakamoto (2008) envisions perfect competition among independent computer nodes dispersed across the world, many cryptocurrencies have over the years witnessed a rise of "pooled mining" wherein miners partner together and share mining rewards, as opposed to "solo mining" wherein individual miners bear all idiosyncratic risks. Furthermore, the benefits of PoW blockchains come at high costs: practitioners and academics alike recognize well how crypto-mining increasingly consumes energy and affects the climate and environment.[1]

Bitcoin mining provides an illustration: Mining pools grew from constituting only 5% of global hash rates (a measure of computation power devoted to mining) in June 2011 to almost 100% since late 2015, as shown in Figure 1. The rise of mining pools also coincides with the explosive growth of global hash rates (plotted by the red line, in log scale). Meanwhile, some pools gained significant shares from time to time, with the best-known example being

[1] As of April 2018, aggregate electricity devoted to Bitcoin mining alone exceeds 60 TWh, roughly the annual energy consumed by Switzerland (Lee, 2018). The cryptocurrency forum Digiconomist provides similar estimates, noting that mining a single block consumes enough energy to power more than 28 U.S. homes for a full day (https://digiconomist.net/bitcoin-energy-consumption). Mora, Rollins, Taladay, Kantar, Chock, Shimada, and Franklin (2018) project that if Bitcoin follows the adoption pattern of other technologies, it could push global warming above 2 degrees Celsius within three decades. See also Rogers (2017).

Figure 1: **The evolution of size percentages of Bitcoin mining pools**

This graph plots (1) the growth of aggregate hash rates (right hand side vertical axis, in log scale) starting from June 2011 to Dec 2018; and (2) the size evolution of all Bitcoin mining pools (left hand side vertical axis) over this period, with pool size measured by each pool's hash rates as a fraction of global hash rates. Different colors indicate different pools, and white spaces indicate solo mining. Over time, Bitcoin mining has been increasingly taken over by mining pools, but no pool ever seems to dominate the mining industry for long. The pool hash rates data come from Bitcoinity and BTC.com, with details given in Section 5.



GHash.io that briefly reached over 51% of global hash rates in July 2014. Although such cases call into question whether a blockchain system can stay decentralized, none of the large pools emerged has snowballed into dominance for prolonged periods of time. Instead, Figure 1 reveals that pool sizes seem to exhibit a mean-reverting tendency, suggesting concurrent economic forces suppressing over-centralization.

Motivated by these observations, we study the centralization and decentralization forces in the evolution and industrial organization of mining pools, and relate them to the energy consumption of mining as well as classic economic theories. Specifically, we model miners' decision-making in acquiring and allocating hash rates into mining pools, together with the competition among pool managers who charge fees for providing risk-sharing services. We highlight two features of cryptocurrency mining that are key to understanding our results: (i) It is easy for profit-driven miners to participate in multiple mining pools, an interesting feature that contrasts with the traditional literature on labor and human capital in which each individual typically only holds one job; (ii) As will be explained shortly, the dynamic adjustment of mining difficulty required for ensuring a stable block production rate leads to an arms race, creating a negative externality in which each individual's acquisition of hash

rates directly hurts others' payoffs.

We first illustrate the significant risk-sharing benefit offered by mining pools to individual miners: under reasonable parameters, the certainty equivalent of joining a pool more than doubles that of solo mining. Absent other considerations, a larger pool also offers higher risk-sharing benefits. These results should be intuitive, since partnerships/cooperatives have been one of the most common organizational forms in humans history for risk sharing among individuals, and as in the insurance industry, risk sharing works better when the insurance provider covers a larger market. Yet, whereas in conventional settings the risk-sharing benefit is rarely separable from production technologies with increasing economy of scale, the total revenue in crypto-mining stays the same whether two miners join force or not. Mining pools thus emerge primarily for risk sharing, which allows us to pinpoint the interaction between risk sharing and competition.

While one may hastily conclude that a large pool would grow even larger, we prove otherwise: In a frictionless benchmark, perfect risk sharing could be obtained and the exact pool size distribution is irrelevant. The risk-sharing benefit *within* a large pool could be alternatively obtained through miner's diversification *across* multiple small pools—a general insight reminiscent of the Modigliani-Miller Theorem. Although investors (miners) are risk-averse, conglomerate firms (pools) for risk sharing do not necessarily emerge because investors (miners) can diversify on their own by holding a diversified portfolio (allocating hash rates to multiple pools). As a result, the folk wisdom in the blockchain community that pools become concentrated for better risk sharing is misguided, as long as miners can freely allocate their hash rates.[2]

Instead, as a financial innovation intended for better risk sharing, mining pools severely escalate the arms race in PoW blockchains, whose real consequence is an enormous additional amount of energy devoted to mining. Under reasonable model parameters, mining pools can elevate the global computation power devoted to mining by multiple times. Given that cryptocurrency mining diverts electricity and fossil fuel from other uses and leaves detrimental environmental impacts (e.g., Benetton, Compiani, and Morse, 2019; Li, Li, Peng,

[2]This counterfactual of progressive concentration or winner-takes-all is powerful because if it were true, it defeats the purpose of decentralized record-keeping. Dispelling the myth not only helps us understand the impact of risk-sharing and pools on the network distribution in PoW- and PoS-based blockchains (see Section 6.3), but also sets a precedent for further studies using rigorous economic analysis to challenge popular media/industry opinions about over-concentration. For example, Rosu and Saleh (2019) model the evolution of shares in a PoS cryptocurrency to challenge the common assertion that the rich's getting richer necessarily leads to dramatic concentrations in PoS blockchains.

Cui, and Wu, 2019; de Vries, 2019; Truby, 2018), our theory makes a timely contribution by linking for the first time energy consumption with the organization of mining pools, as opposed to the usual suspects such as rising cryptocurrency prices and advancements mining hardware.

Building on the insights from the frictionless benchmark, we introduce an empirically relevant friction: some "passive hash rates," however small, are not always optimally allocated in real time due to, for example, business relationship or inattention. This friction introduces pool heterogeneity and potential market power, and allows us to better understand the industrial organization of mining pools observed in practice, as well as its impact on the mining arms race. We characterize the equilibrium in a static setting and explain how the initial pool size distribution affects pool growth: A larger incumbent pool optimally charges a higher fee, which slows its percentage growth relative to smaller pools. In other words, if our model were dynamic, pool sizes mean-revert endogenously.

The central force behind this result is the arms race effect highlighted earlier: A larger pool has a larger impact on global hash rates and consequently charges a higher fee and accommodates proportionally less active hash rates, reminiscent of traditional oligopolistic models where larger producers charge higher prices and produce less.[3] Consequently, in the long run we expect a relatively decentralized market structure in the global mining industry may sustain and no single pool would grow too dominant.[4]

Empirical evidence from Bitcoin mining supports our theoretical predictions. Every month, we regress pool fees and log growth rates on the previous month's pool sizes, and find that pools with larger sizes to start with indeed charge higher fees and grow more slowly in percentage terms. We should not take such empirical patterns on size-fee and size-growth relationships for granted, as prior studies on mainstream sectors with similar characteristics find ambiguous or opposite patterns.[5] We further construct alternative measures for "passive

[3]Nevertheless, the interaction among risk-sharing externality within a pool, diversification across pools, and pool managers' local monopolistic power also distinguishes our model from earlier theoretical models such as Salop and Stiglitz (1977) or Varian (1980). In those settings, firms without economy of scale charge higher prices only to exploit uninformed consumers (i.e., passive miners in our setting).

[4]The escalation of the mining arms race and a miner's benefit from diversification across multiple pools are present irrespective of the "passive hash rates" friction, but the mean reversion in pool sizes relies on it.

[5]For instance, in the passive asset management industry that offers index funds to retail investors, larger funds actually charge lower fees (Hortaçsu and Syverson, 2004); and the recent literature on "superstar" firms finds increasing concentrations across various industries and hence a positive size-growth relationship in the past decades (Andrews, Criscuolo, Gal, et al., 2016; Autor, Dorn, Katz, Patterson, and Van Reenen, 2017). Our empirical results thus constitute a new piece of evidence to this debate on industrial organization economics (for more details, in Section 5.1).

hash rates" to better link our model to the dynamic evolution of pool sizes. Our findings hold in subsamples (i.e., 2012–2014, 2015–2016, and 2017–2018) and are robust to using these alternative measures.

In addition to the cross-section evidence on pool size, pool fees, and pool growth, we also note that the rise of mining pools indeed coincides with the explosion of global hash rates. Under reasonable parameters, we find that in equilibrium the encouragement of more hash rate acquisition induced by risk sharing trumps the discouragement from pool fees, and the presence of mining pools still significantly amplifies mining energy consumption.

Finally, we allow pool entry as in a contestable market, introduce aggregate risks, and extend the model insights to alternative proof-of-work or proof-of-stake protocols. We also discuss how other external forces that counteract over-concentration of pools could be added onto our framework.

Related literature. Our paper contributes to emerging studies on blockchains and distributed ledger systems (e.g., Harvey, 2016), especially cryptocurrency mining games (e.g., Biais, Bisiere, Bouvard, and Casamatta, 2018).[6] Dimitri (2017) and Ma, Gans, and Tourky (2018) model mining as a Cournot-type competition and R&D race. Prat and Walter (2018) examine the relationship between Bitcoin price and hash rate investment. Many studies also reveal that an adequate level of decentralization is crucial for the security of a blockchain (e.g., Nakamoto, 2008; Eyal and Sirer, 2014; Eyal, 2015).

These papers often follow the computer science literature to only consider one pool behaving strategically as a single decision-maker (e.g., Rosenfeld, 2011; Schrijvers, Bonneau, Boneh, and Roughgarden, 2016; Fisch, Pass, and Shelat, 2017). Moreover, almost all of them only consider risk-neutral miners or take mining pools as exogenously given singletons. In contrast, we emphasize risk-aversion—the rationale behind the emergence of mining pools in the first place, and characterize the full equilibrium wherein both miners and pools are strategic. Our findings on the creation and distribution of mining pools also connect with strands of literature on contracting and the theory of the firm.[7] Instead of focusing on a

[6]Other studies include Cong and He (2018) that examines informational tradeoffs in decentralized consensus generation and how they affect business competition. Several papers study the impact of blockchains on corporate governance (Yermack, 2017), holding transparency in marketplaces (Malinova and Park, 2016), security-trade settlements (Chiu and Koeppl, 2018), and auditing (Cao, Cong, and Yang, 2018). Also related are studies on initial coin offerings for project launch (Li and Mann, 2018), as well as cryptocurrency valuation and the economics of using tokens on platforms (Cong, Li, and Wang, 2018, 2019).

[7]Classical studies include Wilson (1968) on syndicates and Stiglitz (1974) on sharecropping. Recent

single pool, we analyze the contracting relationships among miners and pool managers and the interaction of multiple pools in an industrial organization framework.

Many blogs, think tank reports, and media articles have taken notice of the large energy consumption by cryptocurrency mining. They focus on Bitcoin prices and mining hardwares (e.g., ASICs versus GPUs, see Kugler, 2018), rather than modeling the mining industry and identifying the impact from mining pools, which could be equally important. Several studies recognize that costly mining serves to enhance network security (e.g. Chiu and Koeppl, 2019; Budish, 2018; Pagnotta and Buraschi, 2018); some also point to the social waste from high energy consumption by cryptocurrency mining in its current form (e.g. Benetton, Compiani, and Morse, 2019; Chiu and Koeppl, 2019; Saleh, 2019). We demonstrate how risk sharing affects the organization and energy consumption of the mining industry.

The novel economic forces we identify in the mining industry also closely relate to classic economic theories. In addition to the theory of the firm, the Modigliani-Miller insight, and oligopoly pricing as discussed earlier, active miners' hash rate allocation decisions shares the spirit of investors' capital allocation decisions to mutual funds as in Berk and Green (2004). The arms race nature of crypto-mining is also related to research on arms races in finance, notably Glode, Green, and Lowery (2012). Instead of emphasizing how the arms race can destroy value beyond the resources invested directly through adverse selection, we focus on how a financial innovation for risk sharing can exacerbate the arms race outcome. The hard-coded nature of a blockchain together with its transparency offers researchers a unique social science laboratory for analyzing and testing economic theories, for example, on risk sharing and competition, without the complication of agency issues.[8]

The rest of the paper proceeds as follows. Section 2 introduces the institutional details of PoW mining and stylized facts about mining pools. Section 3 sets up the model and analyzes a frictionless benchmark. Section 4 characterizes the equilibrium. Section 5 provides corroborating empirical evidence using Bitcoin data before Section 6 discusses broader implications and extensions. Section 7 concludes.

studies include Li (2015) on private information coordination.

[8]The arms race nature is also related to the long literature of contests and rent seeking (Nitzan, 1991; Konrad, 2007). The key difference here is the absence of moral hazard due to the observability of effort. We elaborate on all these points further in Section 2.6.

2 Mining Pools: Background and Principles

In this section, we provide background knowledge of the Bitcoin mining process, analyze the risk-sharing benefit of mining pools, and introduce typical pool-fee contracts. Mining in other PoW blockchains operates similarly.

2.1 Mining and Risky Rewards

Bitcoin mining is a process in which miners around the world compete for the right to record a brief history (known as block) of bitcoin transactions. The winner of the competition is rewarded with a fixed number of bitcoins (currently 12.5 bitcoins, or ₿12.5), plus any transactions fees included in the transactions within the block (see Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) for more details). To win the competition, miners have to find a piece of data (known as solution, or nonce), so that the hash (a one-way function) of the solution and all other information about the block (e.g., transaction details and the miners' own addresses) has an adequate number of leading zeros. The minimal required number of leading zeros determines the mining difficulty.

Under existing cryptography knowledge, the solution can only be found by brute force (enumeration). Once a miner wins the right to record the most recent history of bitcoin transactions, the current round of competition ends and a new one begins.

Technology rules that for all practical purposes the probability of finding a solution is not affected by the number of trials attempted. This well-known memoryless property implies that the event of finding a solution is captured by a Poisson process with the arrival rate proportional to a miner's share of hash rates globally (e.g., Eyal and Sirer, 2014; Sapirshtein, Sompolinsky, and Zohar, 2016). Specifically, given a unit hash cost c and a dollar award R for each block, the payoff to a miner who has a hash rate of λ_A operating over a period T is

$$X_{solo} - c\lambda_A T, \text{ where } X_{solo} = \tilde{B}_{solo} R \text{ with } \tilde{B}_{solo} \sim \text{Poisson}\left(\frac{1}{D}\frac{\lambda_A}{\Lambda}T\right). \tag{1}$$

Here, $\tilde{B}_{solo}$ is the number of blocks the miner finds within T—a Poisson distributed random variable capturing the risk that a miner faces in this mining game; Λ denotes global hash rate (i.e., the sum of hash rates employed by all miners, whether individual or pool); $D = 60 \times 10$ is a constant so that on average one block is created every 10 minutes.

The hash cost c in Eq.(1) is closely related to the energy used by computers to find the mining solution. More importantly, an individual or pool's success rate is scaled by the global hash rate Λ devoted to mining, capturing the dynamic adjustment of the mining difficulty so that one block is delivered per ten minutes on average.[9] As emphasized later, this constitutes the driving force for the mining "arms race" with negative externality.

Because mining is highly risky, any risk-averse miner has strong incentives to find ways to reduce risk. A common practice is to have miners mutually insure each other by forming a (proportional) mining pool. The next section describes how such a mining pool works.

2.2 Mining Pools and Risk Sharing

A mining pool combines the hash rates of multiple miners to solve one single cryptographic puzzle, and distributes the pool's mining rewards back to participating miners in proportion to their hash rate contributions.[10] The initiation process of a pool typically starts with the pool manager coming up with the hardware infrastructure, programming the necessary codes that implement the operations/compensations of the pool, and then marketing it to the miner community. Some mining pools were initiated by corporations, as in the case of one of the largest mining pools currently, AntPool, which was created by Bitmain Inc.

Ignoring fees that represent transfers among pool members for now, then following the previous example, the payoff to a participating miner with hash rate λ_A who joins a pool with existing hash rate Λ_B is

$$X_{pool} - c\lambda_A T, \text{ where } X_{pool} = \frac{\lambda_A}{\lambda_A + \Lambda_B}\tilde{B}_{pool}R \text{ with } \tilde{B}_{pool} \sim \text{Poisson}\left(\frac{\lambda_A + \Lambda_B}{\Lambda}\frac{T}{D}\right). \quad (2)$$

Pooled mining provides a more stable cash flow and reduces the risk a miner faces. Indeed,

Proposition 1 (Risk Sharing Dominance)**.** *X_{pool} second-order stochastically dominates X_{solo}, so any risk-averse miner strictly prefers X_{pool} over X_{solo}.*

For illustration, consider the symmetric case with $\lambda_A = \lambda_B$. Relative to solo mining, a miner

[9] This dynamic adjustment for scaling miners' winning probabilities is a common feature in both PoW and many PoS blockchains. It ensures network security and reduces block collision (Gervais, Karame, Wüst, Glykantzis, Ritzdorf, and Capkun, 2016; Vukolić, 2015).

[10] Because the number of candidate partial solutions is astronomical, it makes negligible difference to each participating miner's payoff whether the pool coordinates their mining efforts or simply randomizes the assignment of partial problems.

who conducts pooled mining is twice as likely to receive mining payouts with only half the rewards at each payment, generating a standard risk-sharing benefit.

Notice that there is no mechanical economy of scale in the mining process itself. Block generation follows a Poisson arrival given current cryptographic technologies, and the additive property of Poisson processes in turn implies that the total revenue stays the same whether two miners join force or not, that is, $\mathbb{E}[X(\lambda_1 + \lambda_2)] = \mathbb{E}[X(\lambda_1)] + \mathbb{E}[X(\lambda_2)]$. This additive property therefore allows us to isolate and test the effects of pure risk sharing.

2.3 Quantifying the Risk-Sharing Benefits of Pooled Mining

The risk-sharing benefits of joining a mining pool can be substantial. To assess the magnitude, we calculate the difference of certainty equivalents of solo mining and pooled mining for a typical miner. Throughout the paper we use preference with constant absolute risk aversion (CARA), i.e., exponential utility with risk-aversion parameter ρ:

$$u(x) \equiv \frac{1}{\rho}\left(1 - e^{-\rho x}\right). \tag{3}$$

All quantitative implications of our model will be calibrated based on widely accepted magnitudes of relative risk-aversion (CRRA) coefficient.

The certainty equivalent of the revenue from solo mining, CE_{solo}, can be computed as

$$CE_{solo} \equiv u^{-1}(\mathbb{E}[u(\tilde{X}_{solo})]) = \frac{\lambda_A}{\Lambda}\frac{1}{\rho}\left(1 - e^{-\rho R}\right)\frac{T}{D}. \tag{4}$$

Similarly, the certainty equivalent of the revenue from joining a mining pool, CE_{pool}, is

$$CE_{pool}\left(\Lambda_B\right) \equiv u^{-1}(\mathbb{E}[u(\tilde{X}_{pool})]) = \frac{(\lambda_A + \Lambda_B)}{\Lambda}\frac{1}{\rho}\left(1 - e^{-\rho R\frac{\lambda_A}{\lambda_A + \Lambda_B}}\right)\frac{T}{D}. \tag{5}$$

We highlight that this certainty equivalent depends on the pool size λ_B and a larger pool offers greater risk-sharing benefit.

We choose reasonable parameters to gauge the magnitude of the risk-sharing benefit of joining a pool. Suppose $\lambda_A = 13.5$(TH/s), which is what one Bitmain Antminer S9 ASIC miner (a commonly used chip in the Bitcoin mining industry) can offer; $\Lambda_B = 3,000,000$(TH/s), which is at the scale of one large mining pool; $R = \$100,000$ (฿12.5 reward + ∼฿0.5 transaction fees per block and \$8000 per BTC gives \$104,000); $\Lambda =$

$21,000,000$(TH/s), which is the prevailing rate; and $\rho = .00002$ (assuming a CRRA risk aversion of 2 and a wealth of \$100,000 per miner gives a corresponding CARA risk aversion of 0.00002). Take $T = 3600 \times 24$ which is one day. Then $CE_{solo} = 4.002$ and $CE_{pool} = 9.257$, which implies a difference of 5.255, about 57% of the expected reward $\mathbb{E}(\tilde{X}_{solo})$ (about 9.257). In other words, for a small miner, joining a large pool almost boost his risk-adjusted payoff by more than 131%.[11] Equally relevant, for more risk-averse miners (e.g. $\rho = .00004$), given the current mining cost parameters, joining a pool could turn a (certainty equivalent) loss into a profit.[12]

The risk-sharing benefit has two major implications. First, active miners with a given level of risk aversion would acquire hash rates more aggressively when mining in pools, which escalates the mining arms race and amplifies the energy consumption associated with cryptocurrency mining. Second, mining pools could charge fees (price) to miners, which in turn determine miners' optimal hash rates allocations (quantity). Before we develop a model to study the equilibrium fees and allocations under mining pool competitions, we first describe the various forms of fee contracts used in practice.

2.4 Fee Contracts in Mining Pools

Broadly speaking, different pools in practice offer three categories of fee contracts: *Proportional*, *pay per share* (PPS), and *cloud mining*. Table 4 in Appendix B gives a list of contracts currently used by major pools. As explained later, all contracts effectively have the same contracting variable—participating miners' hash rates, and the three categories mainly differ in two aspects: (i) the mapping from the contracting variable to payoff, and (ii) pool fees and the treatment of transaction fees. We proceed to describe the contracting variables and compare the mappings from contracting variables to payoffs. Other technical

[11] Even if we set $\rho = .00001$ (a miner with CRRA risk aversion of 2 and is twice as wealthy as the in-text example), joining this large pool increases his risk-adjusted payoff by more than 85%. The risk-sharing benefit can still be quantitatively large even for small pools. For a small mining pool with only one existing miner using a S9 ASIC chip so that $\Lambda_B = 13.5$, joining it still implies a difference in certainty equivalents of about 20% of the reward. All values above were chosen at the time when this paper was first written in early 2018, including the Bitcoin price of \$8,000. The risk-sharing benefit remains large even with a much lower Bitcoin price, which is \$3,600 around early 2019. When we replace \$8,000 with \$3,600, a small miner joining a large pool boosts his risk-adjusted payoff by more than 52%.

[12] Assuming a \$0.12 per kWh electricity cost, and 1375W/h for S9 (see here), the power consumption is $c = 1.375 \times 0.12/(3600 \times 13.5)$ per TH. Then $\frac{1}{D\rho}\frac{\lambda_A+\Lambda_B}{\Lambda}\left(1 - e^{-\rho R\frac{\lambda_A}{\lambda_A+\Lambda_B}}\right) - \lambda_A C = \$6.1 \times 10^{-5}$/s or \$5.3/day, while $\frac{1}{D\rho}\frac{\lambda_A}{\Lambda}\left(1 - e^{-\rho R}\right) - \lambda_A C = -\$2.0 \times 10^{-5}$/s or $-\$1.7$/day.

details are left out as they are not essential for understanding the rest of the paper.

Pool managers and mining rewards. A mining pool is often maintained by a pool manager, who takes a percentage cut from miners' rewards at payout; this cut is known as a pool fee, which differs across pool contracts. In practice, when contributing to the same pool under the same contract, all miners are subject to the same pool fee, regardless of the amount of hash rates they contribute. In other words, there is no price discrimination.

Furthermore, different pools also vary in how they distribute transaction fees in a block. These transaction fees are different from the pool fees that we focus on; as discussed in Section 2.1, the transaction fees are what Bitcoin users pay to miners for including their intended transactions into the newly mined block. While most pools keep transaction fees and only distribute the fixed rewards from new blocks, given the recent rise in transaction fees more pools now also share transactions fees. Our reduced form block reward R encompasses both types of rewards.

Effectively observable hash rates. All classes of fee contracts effectively use a miner's hash rate as a contracting variable. Although in theory a miner's hash rate is unobservable to a remote mining pool manager, computer scientists have designed ways to approximate it with high precision by counting so-called partial solutions. A partial solution, like a solution itself, is a piece of data such that the hash of all information about the block and the partial solution has at least an adequate number of leading zeros. The required number of leading zeros in lower for a partial solution than that for a full solution. One can view partial solutions as "trials" and the solution as "the successful trial." Counting the number of partial solutions hence amounts to measuring hash rates with some measurement error.

Crucially, while various contracts may use different partial solutions or weigh them differently, the approximation error between the measured hash rate and a miner's true hash rate can be kept arbitrarily small with little cost. For economists, if one interpret "mining" as "exerting effort," then an important implication is that the principal (pool manager) can measure the actual hash rate (miner's effort) in an arbitrarily accurate way, rendering moral hazard issues irrelevant. All team members' effort inputs are perfectly observable and contractible, and the only relevant economic force is risk sharing, in stark contrast to Hölmstrom (1979).

Fee contracts. As mentioned, the more than ten types of fee contracts fall into three categories: proportional, pay per share (PPS), and cloud mining.

One predominant category entails proportional-fee contracts.[13] Under these contracts, each pool participant only gets paid when the pool finds a solution. The pool manager charges a fee $f \in [0,1]$ of the block reward R, and then distributes the remaining reward $(1-f)R$ in proportion to each miner's number of partial solutions found (and hence proportional to their actual hash rates). More specifically, the payoff for any miner with hash rate λ_A joining a pool with an existing hash rate λ_B and a proportional fee f is

$$\frac{\lambda_A}{\lambda_A+\Lambda_B}(1-f)\tilde{B}R - c\lambda_A T, \text{ with } \tilde{B} \sim \text{Poisson}\left(\frac{\lambda_A+\Lambda_B}{\Lambda}\right)\frac{T}{D}. \tag{6}$$

Another popular category involves pay-per-share (PPS) contracts: each pool participant gets paid a fixed amount immediately after finding a partial solution (again, in proportion to the hash rate). Hence the PPS contract corresponds to "hourly wages;" or, all participating miners renting their hash rates to the pool. Following the previous example, given a PPS fee f_{PPS}, the participating miner's payoff is simply $r \cdot \lambda_A$ with

$$r = \frac{RT}{D\Lambda}(1-f_{PPS}) \tag{7}$$

being the rental rate while giving up all the random block reward. As shown, in practice the PPS fee is quoted as a fraction of the expected reward per unit of hash rate (which equals $\frac{R}{\Lambda}\frac{T}{D}$). Cloud mining, which essentially makes miners rent hash rates from the pool, does exactly the opposite: a miner pays a fixed amount upfront to acquire some hash rate from the pool, and then gets paid as if conducting solo mining.

Our theory focuses on proportional fees only, though the analysis easily extends to the case of hybrid of proportional and PPS fees. There are two reasons for our modeling choice. First, in practice, about 70% of pools adopt proportional fees, and 28% pools use proportional fees exclusively. The second reason, which is conceptually more important, is that a pure

[13] In practice, the most common proportional contract is Pay-Per-Last-N-Shares (PPLNS), which counts each pool participant's share within the last N partial solutions submitted by all pool participants, instead of within the total number of partial solutions submitted in a given round before the pool finds a block. Other contracts that fall under the proportional category may discount partial solutions submitted long before the next block is found (e.g., as in geometric method). These alternative methods are adopted to prevent pool-hopping, a point important in practice yet irrelevant to our analysis, as all these methods approximate each pool participants' pay share according to her actual hash rate share.

Table 1: **Evolution of Pool Sizes and Fees**

This table summarizes the evolution of mining pool sizes and fees from 2011 to 2018. We report total hash rates in Column A, total number of mining pools in Column B, and in Column C the fraction of hash rates contributed by top-5 pools (i.e., sum of the top five pools hash rates over the market total hash rates, including those from solo miners). In Column D, we report the average fee weighted by hash rates charged by mining pools. In Column E, we report the fraction of mining pools that use proportional fees; the fraction is calculated as the number of pools that use proportional fees divided by the number of pools with non-missing information on fee contracts. Column F and G give the simple averages of proportional fees and average total fees charged by top-5 pools, respectively; and Column H and Column I are simple averages across all pools. The pool hash rates information comes from Bitcoinity and BTC.com. The fee contract information is obtained from Bitcoin Wiki. All fee and size data are downloaded until December 2018. Over time more hash rates have been devoted to Bitcoin mining, and a majority of mining pools offer proportional contracts. The largest five pools on average charge higher fees.

Year	Hash Rate (PH/s) (A)	# of Pools (B)	% of Top 5 (C)	Avg. Fee (%), Size-weighted (D)	Frac. (%) Pools w. Prop. Fee (E)	Fee (%)			
						Top 5		All	
						Prop. (F)	Ave. (G)	Prop. (H)	Ave. (I)
2011	0.01	7	7.63	0.72	85.98	0.28	0.28	0.28	0.25
2012	0.02	15	34.66	2.69	60.03	0.66	1.76	0.65	1.56
2013	1.48	23	71.01	2.73	61.20	1.58	2.29	1.16	2.02
2014	140.78	33	70.39	0.94	73.19	1.33	1.13	0.88	2.38
2015	403.61	43	69.67	1.73	81.97	1.10	1.31	0.84	1.33
2016	1,523.83	36	75.09	2.60	78.74	1.48	2.15	0.97	1.67
2017	6,374.34	43	62.25	1.44	89.85	2.00	1.43	1.45	1.33
2018	36,384.60	40	69.15	1.31	70.24	1.08	1.62	0.99	1.47

form of PPS or cloud mining only involves risk allocation between miners and the pool manager. Under our framework, miners and pool managers with a homogeneous risk aversion gain nothing from adopting PPS or cloud mining. In contrast, a proportional fee contract provides risk-sharing benefits.

2.5 Stylized Facts about Mining Pools

Table 1 provides an overview of the mining industry. Total hash rates in Bitcoin mining (Column A), the number of identified mining pools (Column B), and the concentration of mining pools (Column C, the total market share of the top-5 pools sorted by hash rate) have mostly been increasing since 2011. From an individual miner's perspective, Column D gives the average pool fee (including proportional, PPS, and others) weighted by hash rate

for each year, which offers a gauge of the overall cost of joining mining pools. Column E gives the fraction of hash rates in the mining pools thatuse proportional fees.

The remaining four columns focus on the evolution and magnitude of pool fees which fall in the range of a couple percentage points. Columns F and G are for top-5 pools while Columns H and I for all pools. The stylized fact revealed by comparing "Top 5" and "All" is that fees charged by top-5 pools are higher than the average fees charged by pools of all sizes. This is one salient empirical pattern that motivates our paper.[14]

2.6 Unique Characteristics of the Crypto-mining Industry

The aforementioned institutional background should make apparent a few unique characteristics of the crypto-mining industry as compared to traditional ones. First, while agents in traditional industries can decide how much effort or input to provide, they can rarely work for multiple firms at the same time (the concept of diversification), except for sharing economies or on-demand labor platforms such as Uber. Blockchains lend a setting where labor diversification manifests itself in the most transparent way.

Moreover, even when agents' labor input (hash power in our case) could be fully diversified, traditional industries typically feature economy of scale in a mechanical way, typically via fixed overhead costs. In contrast, in the crypto-mining industry, there is another strong force favoring the economy of scale—namely, risk-sharing—which is far less mechanical than the standard fixed overhead costs. In that sense, mining pools presents an environment where we can better isolate the impact of risk-sharing.

Last but not least, whereas one has to worry about agency issues such as shirking in traditional (labor) contracting, mining pools can measure effort inputs in an accurate way by counting partial solutions and therefore are essentially free of moral hazard.

Neglecting the above features often leads many practitioners and policy-makers to hold beliefs that mining pools would eventually lead to over-concentration and the dominance of a single pool. Some people are unaware that miners can allocate hash rates across pools; if each miner could only join one pool, then in practice a larger pool would always charge a low enough fee to attract more miners, leading to a single pool dominating the entire industry.

[14] Proportional fees are in general lower than "average fee" which is the average of proportional fees, PPS fees, and others. The reason is simple: PPS contracts offer zero risk exposure to participating miners, so risk-averse miners are willing to pay a higher PPS fee than that of proportional contracts (or equivalently, pool managers charge more from miners for bearing more risk).

This is not what we find in our setting, as our model formally shows.

3 An Equilibrium Model of Mining Pools

We now model multiple pool managers competing in fees to attract active miners. We first derive a benchmark result: in a frictionless environment where all miners can actively acquire hash rates and allocate them to different pools, risk sharing itself does not lead to centralization, simply because miners can diversify themselves across pools. The exact distribution of pool sizes actually does not matter in this case.

Pool size distribution starts to matter when pools retain passive hash rates that are not optimally allocated across pools. In Section 4, we show that pools with larger passive hash rates charge higher fees, leading to slower pool growth, and then confirm these key theoretical predictions in Section 5 with data from Bitcoin mining pools. We also highlight how mining pools aggravate the mining arms race and potentially waste energy.

3.1 Agents and the Economic Environment

In our static model, both pool managers and individual miners have the same CARA utility function given in Eq.(3) and use proportional-fee contracts.

Pool managers and passive mining. There are M mining pools controlled by different managers; we take these incumbent pools as given and study pool entry later in Section 6.1. Pool $m \in \{1, \cdots, M\}$ has existing passive hash rates $\Lambda_{pm} > 0$ (p stands for passive mining).

In the case of Bitcoin, although it involves little cost to re-adjust hash rates allocations, inattention could generate inertia that leads to passive hash rates sticking to a pool (e.g., Forum, 2014). Passive hash rates may also come from early strategic investors of a pool, "loyalty fans," or "relationship clients" (e.g., Torpey, 2016). In practice, a significant portion of Λ_{pm} may also belong to the pool manager himself, which can be incorporated by modifying the fee expression. As we explain in Section 5, our qualitative results do not rely on the exact link between the passive hash rates Λ_{pm} and the pool size because we find that in the data, pools of larger sizes have more (but not disproportionally more) passive hash rates, a condition sufficient for our predictions on pool growth. We also consider alternative proxies for Λ_{pm} in Section 5.2.

Given the significant risk-sharing benefit to individual miners illustrated in Section 2, managers of pools $\{m\}_{m=1}^{M}$ post (proportional) fees $\{f_m\}_{m=1}^{M}$ simultaneously to attract Λ_{am} active miners and maximize their expected utility, $\mathbb{E}\left[u(\tilde{B}_m f_m R)\right]$, which can be expressed using the certainty equivalent as

$$\max_{f_m \in [0,1]} \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\rho \Lambda(f_m, f_{-m})} \left(1 - e^{-\rho R f_m}\right), \tag{8}$$

where Λ_{am} (a stands for active mining) is the hash rate contribution to pool m from all (symmetric) active miners.

It is worth emphasizing that when setting fees, the oligopolistic pool managers understand the impact of fee levels on the global hash rate Λ and hence their own expected utility. In other words, pool managers partially internalize the arms-race externality.

Active miners. There is a continuum of active homogeneous miners of total measure N, each of whom can acquire hash rate with a constant unit cost c. In other words, while mining pools may enjoy market power, active miners are competitive.[15]

Taking the fee vector $\{f_m\}_{m=1}^{M}$ and passive hash rates $\{\Lambda_{pm}\}_{m=1}^{M}$ as given, these active miners can acquire and allocate hash rates to the above m pools. Optimal allocation among existing pools, rather than a binary decision of participation or not, plays a key role in our analysis. In practice, some miners do recognize this benefit of allocating hash rates across many pools, even though no formal justifications are given.[16]

For an active miner facing $\{\Lambda_{pm}\}_{m=1}^{M}$ and $\{f_m\}_{m=1}^{M}$, the payout when allocating a hash rate of λ_m to pool m is

$$X_m = \frac{\lambda_m}{\Lambda_{am} + \Lambda_{pm}} \tilde{B}_m (1 - f_m) R. \tag{9}$$

Recall that throughout the paper we use lower case λ to indicate individual miner's decisions while upper case Λ_m for hash rates at the pool level. Our continuum specification of miners implies that for each individual miner, λ_m is infinitesimal relative to the pool size Λ_m; this is why λ_m does not show up in the denominator of Eq.(9). Finally, an infinitesimal miner

[15] We discuss in an earlier draft the case where active miners are endowed with fixed hash rates, which does not change our findings concerning the industrial organization of mining pools.

[16] See forum discussions: "*Mining pools are used primarily to reduce variance, and the larger the pool, the more effective it is for this purpose. There is a simple way to decrease the variance further: Mine in multiple pools.*"

with infinitesimal risk tolerance would not solo mine, as long as $f_m < 1$ for some pool m.[17]

As a result, the active miner chooses $\{\lambda_m\}_{m=1}^M$ to maximize

$$\mathbb{E}\left[u\left(\sum_{m=1}^{M} X_m - C\sum_{m=1}^{M}\lambda_m\right)\right] = \mathbb{E}\left[u\left(\sum_{m=1}^{M}\left(\frac{\lambda_m \tilde{B}_m(1-f_m)}{\Lambda_{am}+\Lambda_{pm}}\right)R - C\sum_{m=1}^{M}\lambda_m\right)\right],$$

where we have denoted cT as C. Since our analysis works under any choice of T, for brevity of notation we further normalize $T/D = 1$. The certainty equivalent calculation based on exponential preference in Eq.(3) implies that the hash allocation to each pool decouples from one another, and the optimization is equivalent to

$$\max_{\lambda_m \geq 0}\left[\frac{\Lambda_{am}+\Lambda_{pm}}{\rho\Lambda}\left(1 - e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}\right) - C\lambda_m\right], \forall m, \tag{10}$$

where the global hash rate Λ is

$$\Lambda = \sum_{m=1}^{M}(\Lambda_{am}+\Lambda_{pm}). \tag{11}$$

In the miner's objective (10), the global hash rate Λ scales down the winning probability of each participating hash rate, so that in aggregate the block generation process is kept at a constant. This is a feature of many PoW blockchain protocols such as Bitcoin and the negative externality is important for understanding our results later.

In our setup, we have implicitly assumed that the infinitesimal active miners remain customers of mining pools and do not become pool managers themselves. This is consistent with the following two facts: first, most miners who participate in pools simply run lightweight nodes that specialize in solving proof-of-work puzzles (instead of running full nodes verifying all transactions); second, setting up and maintaining a mining pool (e.g., setting up robust networking with DDoS defenses, database tracking miner contributions, and friendly user interfaces) is an elaborate process beyond most miners' sophistication.

[17] Formally, each miner with $\Sigma\lambda_m \cdot di$ hash rates has a risk tolerance of $\frac{1}{\rho}\cdot di$ (or, an absolute risk aversion of $\frac{\rho}{di}$, where di is the measure of an infinitesimal miner so that $\int di = N$ (as a result, the aggregate risk tolerance of miners is $\frac{N}{\rho}$). The certainty equivalent of solo mining of an infinitesimal miner, which is given in Eq.(4), can be shown to be of a lower order than Eq.(10).

3.2 Definition of Equilibrium

We focus on a class of symmetric subgame perfect equilibria in which homogeneous active miners adopt identical strategies. The notion of the "subgame" comes from active miners reacting to the fees posted by the M pools. In other words, all (homogeneous) active miners take symmetric best responses to any (on- and off-equilibrium) fees and each pool faces an aggregate demand function (of the fee vector).

Definition. *A symmetric subgame perfect equilibrium in which homogeneous players take identical strategies is a collection of* $\{f_m\}_{m=1}^M$ *and* $\{\lambda_m\}_{m=1}^M$ *so that*

(1) ***Optimal fees:*** $\forall m \in \{1, 2, \cdots, M\}$, f_m *solves pool manager* m*'s problem in (8), given* $\{f_{-m}\}$ *set by other pool managers;*

(2) ***Optimal hash rates allocations:*** *Given* $\{f_m\}_{m=1}^M$ *and* $\{\Lambda_m\}_{m=1}^M$, $\{\lambda_m\}_{m=1}^M$ *solve every active miner's problem in (10);*

(3) ***Market clearing:*** $N\lambda_m = \Lambda_{am}$.

3.3 A Frictionless Benchmark

The initial size distribution of mining pools is directly captured by passive hash rates $\{\Lambda_{pm}\}_{m=1}^M$ in our model. To highlight the role of passive hash rates, we first analyze a frictionless benchmark without passive mining.

Proposition 2 (Irrelevance of Pool Size Distribution)**.** *Suppose* $\forall m \in \{1, 2, ..., M\}$, $\Lambda_{pm} = 0$. *The following allocation constitutes a unique class of symmetric equilibria:*

(1) Pool managers all charge zero fees: $f_m = 0$ *for all* $m \in \{1, 2, ..., M\}$*;*

(2) Active miners choose any allocation $\{\lambda_m\}_{m=1}^M$ *so that the global hash rates* Λ *satisfies*

$$\Lambda = N \sum_{m=1}^{M} \lambda_m = \frac{R}{C} e^{-\rho R/N}. \tag{12}$$

In this class of equilibria, every active miner owns an equal share of each mining pool, and the exact pool size distribution $\{\Lambda_{pm}\}_{m=1}^M$ *is irrelevant.*

Proposition 2 shows a stark irrelevance result of pool size distribution for the purpose of risk sharing. In this class of equilibria, the global hash rate that miners acquire is $\Lambda = \frac{R}{C} e^{-\rho R/N}$, so that for each miner the marginal benefit of acquiring additional hash rate hits the constant acquisition cost C. Under zero fees, each individual miner maximizes his

objective in (10). Fixing the total hash rate Λ in this economy, the allocation among pools reaches full risk sharing among all miners.[18] Pool managers charge zero fees due to Bertrand competition, otherwise one pool manager can cut her fee to steal the entire market, thanks to the identical services the pools provide without passive hash rates.

Fallacy of risk sharing and pools. Numerous discussions in the blockchain community have focused on the centralization implications of mining pools, i.e., how better risk sharing provided by larger pools would attract even more hash rates and lead to further concentration. Proposition 2 rejects this fallacy based on a Modigliani-Miller insight: In a frictionless market, investors can perfectly diversify on their own, nullifying the risk-sharing rationale for conglomerates. In other words, as long as miners can join pools in a frictionless way, one should not expect a single large pool to emerge.

In practice, reallocating between pools involves simply changing some parameters in the mining script and hence participating in multiple pools entails negligible transaction cost.[19] As a result, joining m pools with proper weights, so that each miner owns equal share of each pool, is equivalent to joining a single large pool with the aggregate size of these m pools. Precisely because individuals can allocate their hash rates to diversify by themselves, forming large pools is unnecessary for risk-sharing purposes.

Given that miners in practice increasingly recognize the diversification benefits of mining in multiple pools, our theoretical insight has practical relevance in that over-concentration should not be a concern absent other frictions.[20] We show later that even though the key

[18] An alternative way to obtain full risk sharing is through "insurance" contracts with purely financial transfers. Such contracts could in theory allow each miner to solve their individual problems and therefore get rid of the over-concentration concern. Such contracts are however difficult to implement in reality, due to costly-to-observe hash rates, and are rarely used. Another alternative is P2P pools, which require all participating miners to run full nodes. They constitute a negligible market share.

[19] There is a key difference between Bitcoin mining pools and traditional firms that provide valuable insurance to workers against their human capital risks (e.g., Harris and Holmstrom, 1982; Berk, Stanton, and Zechner, 2010): In the Bitcoin mining industry, it is easy for miners to allocate their computational power across multiple pools, just like in standard portfolio allocation problems in financial investment. In contrast, it is much harder for workers to hold multiple jobs.

[20] Our insight is also shared by some practitioners, though no formal argument or analysis has been put forth. For example, an interesting forum post remarks that mining in multiple pools "*not only helps variance for individual miners, but is healthier for the network. In the current standard usage, there is a 'the rich get richer, the poor get poorer' tendency where larger pools are more attractive and thus grow even larger, and all else being equal, the equilibrium is a single huge pool (thankfully, all else is not equal). If miners adopt the proposed strategy, the tendency will be to maintain the status quo distribution, so pools can rise and fall based on their merits. Miners will enjoy the low variance of a single huge pool, without the centralization of power problem.*"

friction $\Lambda_{pm} > 0$ gives market power to pools, the natural forces in the resulting monopolistic competition also counteract over-concentration.

Pool collusion? Potential collusion among a subset of pool managers does not change the result. In the benchmark setting, competition between two parties (potentially colluding groups) would drive the equilibrium fee to zero and render the distribution of pool size irrelevant. Even if all incumbent managers collude, new entrants (once we allow them in Section 6.1) would present a similar competitive force. Collusion only matters when we introduce the passive mining friction Λ_{pm}. Still, to the extent that pool managers share the benefits from collusion, we can simply view colluding pools as one pool with a larger Λ_{pm}.

4 Equilibrium Characterization and Implications

We now incorporate the passive mining friction $\Lambda_{pm} > 0$ and characterize the equilibrium quantity and distribution of mining activities; Λ_{pm} introduces heterogeneity across pools, pins down the equilibrium pool-size distribution, and reveals how mining pools affect the arms race in a realistic setting with market powers. We impose a simple parametric assumption.

Assumption 1. $\rho R < N$.

In our model, the aggregate risk tolerance of a measure N of CARA active miners is $\frac{N}{\rho}$. Assumption 1 essentially requires that the implied CRRA risk aversion, which is $W\frac{\rho}{N}$ with W being the aggregate wealth of Bitcoin community, be below $\frac{W}{R}$, with R being the dollar reward of each block. This trivially holds for reasonable CRRA coefficients (e.g., 2.)

4.1 Active Miners' Hash Rates Allocations

Since each infinitesimal individual active miner within the continuum takes the fee vector f_m, and more importantly the pool m's total hash rates $\Lambda_m = \Lambda_{am} + \Lambda_{pm}$ as given, the first order condition from miners' maximization (10) gives,

$$\underbrace{\frac{R(1-f_m)}{\Lambda}}_{\text{risk-neutral valuation}} \underbrace{e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}}_{\text{risk aversion discount}} = \underbrace{C}_{\text{marginal cost}} . \tag{13}$$

The left (right) hand side gives the marginal benefit (cost) of allocating λ_m to a pool with size $\Lambda_m = \Lambda_{am} + \Lambda_{pm}$, wherein the first term is the risk-neutral valuation of the marginal benefit to hash rate: reward times the probability of winning ($\frac{1}{\Lambda}$), adjusted by proportional fee. The second term captures the miner's risk-aversion discount. Fixing allocation λ_m, the larger the pool size Λ_m he participates in, the smaller the discount—as illustrated in Section 2.3; fixing the pool size, the risk-aversion discount however worsens with his allocation λ_m. Since the optimal allocation rule equates marginal benefit with marginal cost, the better risk-sharing benefit from a larger pool leads to a higher active hash rate allocation.

In equilibrium we have $\Lambda_{am} = N\lambda_m$, therefore

$$\frac{\lambda_m}{\Lambda_{pm}} = \max\left\{0, \frac{\ln \frac{R(1-f_m)}{C\Lambda}}{\rho R(1-f_m) - N \ln \frac{R(1-f_m)}{C\Lambda}}\right\}, \tag{14}$$

where zero captures the corner solution of a pool not attracting any active miners (e.g., when f_m is high enough). Equation (14) leads to the following lemma that relates pool fees to the equilibrium active hash-rate allocation in each pool.

Lemma 1 (Active Mining Allocation)**.** *In any equilibrium, and for any two pools m and m',*

1. *If $f_m = f_{m'}$, then $\frac{\lambda_m}{\Lambda_{pm}} = \frac{\lambda_{m'}}{\Lambda_{pm'}}$;*
2. *If $f_m > f_{m'}$ then we have $\frac{\lambda_m}{\Lambda_{pm}} \leq \frac{\lambda_{m'}}{\Lambda_{pm'}}$. If in addition $\lambda_{m'} > 0$, then $\frac{\lambda_m}{\Lambda_{pm}} < \frac{\lambda_{m'}}{\Lambda_{pm'}}$.*

Lemma 1 tells that pools that charge the same fee grow at the same proportion and pools that charge higher fees grow more slowly.

4.2 Pool Managers' Fee-setting

For pool managers, the objective in (8) can be written as

$$\frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\Lambda(f_m, f_{-m})}\left(1 - e^{-\rho R f_m}\right) = \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\Lambda_{am}(f_m) + \Lambda_{pm} + \Lambda_{-m}}\left(1 - e^{-\rho R f_m}\right), \tag{15}$$

where $\Lambda_{-m} = \sum_{m' \neq m}(\Lambda_{am'} + \Lambda_{pm'})$ is the global hash rate minus pool m's. Compared to the miner's problem in (10), pool managers engage in a monopolistic competition, and take into consideration that f_m not only affects their own pools' hash rates but also the global

hash rate. Plugging Eq. (14) into Eq. (15) gives

$$\underbrace{\frac{1-e^{-\rho R f_m}}{\Lambda(f_m)} \cdot \max\left\{1, \frac{\rho R(1-f_m)}{\rho R(1-f_m) - N \ln \frac{R(1-f_m)}{C\Lambda(f_m)}}\right\}}_{\text{value per unit of initial size } \Lambda_{pm}} \cdot \underbrace{\Lambda_{pm}}_{\text{initial size}} \tag{16}$$

Eq.(16) illustrates the dependence of global hash rate on pool fees: when each pool manager sets the fee to maximize her value per unit of initial size Λ_{pm}, she also takes into account the impact of her fee on global hash rates $\Lambda(f_m)$.

Proposition 3 characterizes a monotonicity property between a pool's passive hash rate and the optimal fee it charges in equilibrium.

Proposition 3 (Endogenous Pool Fees)**.** *$\forall m, n \in \{1, \cdots, N\}$ such that $\Lambda_{am} > 0$ and $\Lambda_{an} > 0$, $\Lambda_{pm} > \Lambda_{pn}$ implies $f_m^* > f_n^*$. In words, among pools that grow, a larger pool charges a higher fee.*

We hereafter focus on pools who set fees strictly less than one and hence do attract active miners in equilibrium. Note that if a pool charges $f_m = 1$, it would not attract active miners and grow. Therefore a growing pool must charge an interior fee less than one. Notice that in the data pools charge fees at an order of several percentage points (see Table 1).

The intuition for Proposition 3 is that pools with more initial passive hash rates take into account their larger "global hash rate impacts." To see this, suppose pool managers ignore the fee impact on global hash rate and view $\Lambda(f_m)$ as a constant, then the optimal choice of f_m should maximize the term "value per unit of Λ_{pm}," which is independent of Λ_{pm}, leading to all managers charging the same fee.[21]

However, pool managers who behave as oligopolies understand that $\Lambda'(f_m) < 0$; they take into account the fact that charging a lower fee brings more active miners, pushing up the global hash rates Λ and hurting their pools' profit. In the extreme, a monopolist pool manager fully internalizes the cost of higher global hash rates. Because every unit of active hash rate affects the aggregate hash rates equally, on the margin, a larger pool who takes into account her "global hash rate impact" has a stronger incentive to raise fees and curb the increase in mining difficulty, analogous to firms with larger market power charging higher

[21] This implies that unlike Varian (1980) (which shows that a larger store exploiting their uninformed consumers would charge higher fees), a pool manager exploiting a larger initial passive mining does not charge a higher fee. Moreover, exploiting the passive mining is not the main driver for the equilibrium fees charged, another feature distinguishing our paper from earlier studies such as Varian (1980).

prices and producing less. Note, this result is not driven by that pool managers benefit from charging a higher fee to get higher revenues from the passive miners. In fact, absent active mining and the "global hash rate impact," all pools would charge the same fee $f = 1$ to maximize revenue from passive miners.[22]

We next discuss two implications of the equilibrium: (i) mining pools as a financial innovation escalate the mining arms race (Section 4.3), and (ii) there is a mean-reverting force in pool growth (Section 4.4).

4.3 Financial Innovation and the Crypto Arms Race

Recall that absent mining pools, there is no solo minin—an artifact of our modeling choice of the continuum of infinitesimal miners (see Footnote 17). To find an estimate of solo mining similar to that in a model with N discrete active miners, and to compare mining activities with and without mining pools in an empirically relevant manner, we define solo mining as active miners acting in groups of unit measures, and then apply the optimality condition (13) so that no active miner would like to acquire more hash rates. Then the total global hash rate under solo mining only is $\Lambda_{solo} \equiv \frac{R}{C} e^{-\rho R}$.

It is clear that Λ_{solo} is significantly smaller than the total global hash rate with full risk sharing, $\frac{R}{C} e^{-\rho R/N}$ for large N. In fact, with mining pools, the aggregate hash power Λ_{pool} is always greater than that in an equilibrium without mining pools Λ_{solo}, and strictly so if mining pools attract all active hash rates in equilibrium. To see this, in an equilibrium with mining pools, any active miner in a pool must find the marginal net benefit of mining solo to be weakly negative, i.e., $\frac{R}{\Lambda_{pool}} e^{-\rho R} - C = C(\frac{\Lambda_{solo}}{\Lambda_{pool}} - 1) \leq 0$ where we have used Λ_{solo} just defined above. When there is no solo mining in equilibrium, this inequality is strict.

A higher global hash rates arises in our model because mining pools severely escalate the arms race in PoW blockchains, whose real consequence is an enormous additional amount

[22] In practice, a significant portion of Λ_{pm} may belong to the pool manager himself, and we can easily incorporate this case in our model by replacing f_m in (8) with $\hat{f}_m$, so that

$$\hat{f}_m = \frac{\Lambda_{am}}{\Lambda_{am} + \Lambda_{pm}} f_m + \frac{\Lambda_{pm}}{\Lambda_{am} + \Lambda_{pm}} \alpha(f_m),$$

where $\alpha(f) \in [f, 1]$ is weakly increasing in f. One useful way to understand this function is the following: Suppose the manager owns a fraction π of the passive mining power, while the rest $1 - \pi$ comes from other fee-paying loyalty passive miners. Then $\alpha(f) = \pi + (1 - \pi)f$ is increasing in f, which is a special case of a monotone $\alpha(f)$. $\alpha(f) = f$ in our baseline model and hence $\hat{f}_m = f_m$; taking $\alpha(f) \to 0$ would allow us to see that all our main results go through even when pool managers do not exploit the initial passive hash.

of energy devoted to mining. Our model is an example of a financial innovation/vehicle seemingly beneficial to individual miners yet in aggregate lower their welfare (which in the model is the opposite of global hash rates). Miners' welfare losses become significant precisely when the risk-sharing benefit of mining pools is large—say, when the risk-aversion ρ is high, or the measure of active miners N is large.

We caution that the conclusion on miners' welfare does not necessarily extend to social welfare because we do not explicitly model the security benefits of proof-of-work.[23] Considering such benefits would not change our theoretical insights here. More generally, specific to Bitcoin today, any other potential social benefits from mining are unlikely to exceed the cost of energy consumption (e.g., Benetton, Compiani, and Morse, 2019).

This economic force, already transparent in the frictionless benchmark, is of first-order importance for PoW-based blockchain consensus generation. The equilibrium global hash rates are lower in the main model with frictions because active miners face positive fees that discourage their hash rate acquisition. However, under reasonable parameter choices, the implied global hash rates with mining pools can still multiply that without mining pools.

For illustration, it suffices to study the case with pools of homogeneous size, and compare the resulting endogenous global hash rates to the solo mining case as well as the frictionless benchmark. Say $\Lambda_{pm} = \Lambda_p > 0$ for all $m \in \{1, ..., M\}$, and focus on the situation where fees take interior solutions. After some simplifications of the first-order conditions of (8) and (10), one can show that the endogenous fee f^* (charged by all pools) solves

$$\rho R\left(1-f\right)\left(1-z\left(f\right)\right) = N \ln \frac{R\left(1-f\right)z\left(f\right)}{C \cdot M\Lambda_p},$$

and the equilibrium global hash rates Λ can be obtained by

$$\Lambda = \frac{M\Lambda_p}{z(f^*)} \text{ with } z\left(f\right) \equiv \frac{\left(M-1\right)\left(1-e^{-\rho Rf}\right)\left[N-\rho R\left(1-f\right)\right]}{Me^{-\rho Rf}\rho^2 R^2\left(1-f\right)-\left(M-1\right)\left(1-e^{-\rho Rf}\right)}.$$

Figure 2 provides a quantitative illustration. Each panel in Figure 2 plots the endogenous

[23] Had we modeled the security benefits of mining, it is possible that for sufficiently high risk aversion and under certain parameter ranges, the risk-sharing innovation from mining pools could promote efficient levels of mining. Our modeling choice is motivated by the goal to illustrate in a simple and transparent way the economic forces of risk-sharing and monopolistic competition, which are important in the crypto-mining industry. Doing so makes transparent the insight that better risk sharing leads to more aggressive investment, which is economically relevant in general, for example, in the context of information aggregation in the financial markets (Li, 2017).

global hash rates, as a function of reward R, under three scenarios: (i) solo mining without pools; (ii) full risk-sharing implied by Proposition 2 without passive mining friction; and (iii) monopolistic competition with passive hash rates as initial pool size, with $M = 2$. Panels A and B plot the global hash rates Λ for two risk-aversion coefficients ρ; Panels C and D plot Λ for two values of the active miner measure N.

First, we observe that for solo mining, the implied global hash rates increase with reward R initially but decrease when R is sufficiently large. In our model, R scales with expected reward as well as risk, and the decreasing global hash rates is an artifact of CARA preference which has no wealth effect.[24] Second, when we compare Panel A (B) with C (D) which feature $N = 10$ and $N = 100$ respectively, they by definition have the same solo mining outcomes, but their full risk-sharing hash rates differ by at most a factor of 1.4. The relative small factor is expected from standard portfolio theory: quantitatively further risk diversification provides little benefit when an individual is already diversified across about 20 assets (pools, in our setting; see Figure 7.10 on page 254 in Fama, 1976).

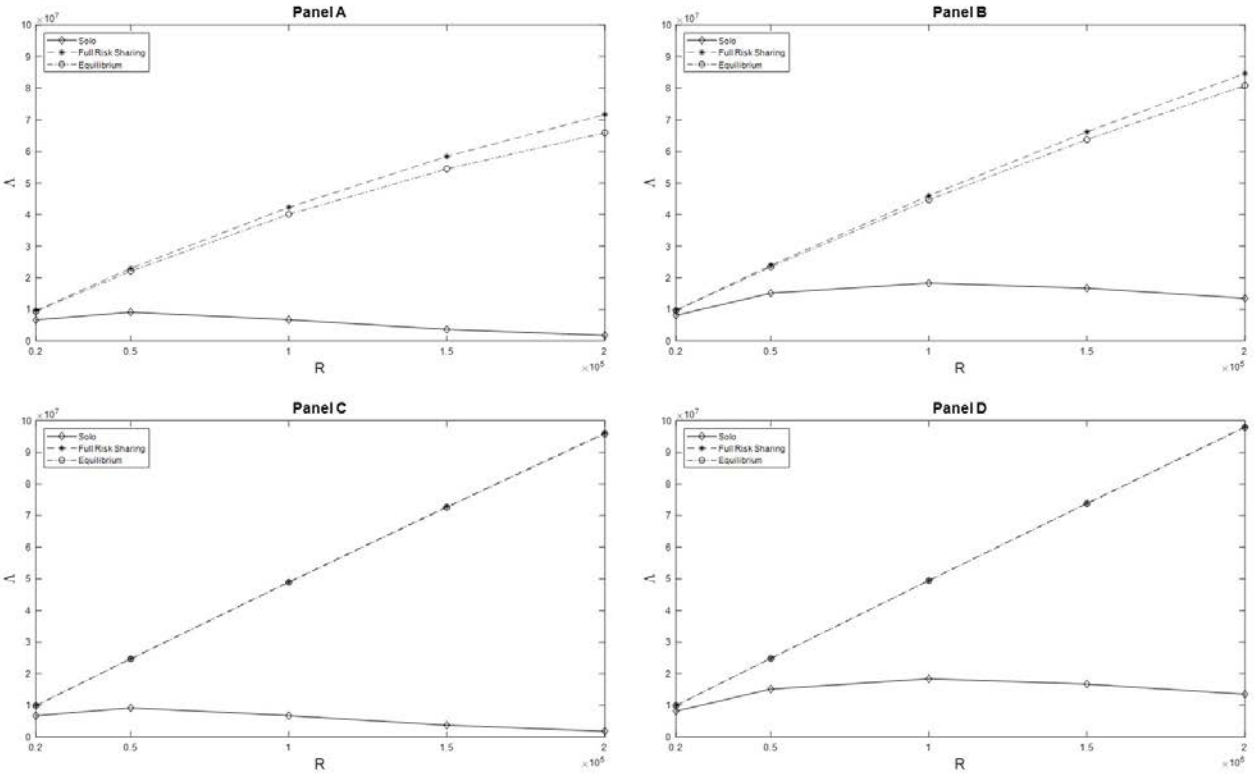
Now we move on to the equilibrium outcome under mining pools with passive hash rates. Relative to solo mining, both the full risk-sharing and the mining-pool equilibrium produce about five times the global hash rates for $\rho = 2 \times 10^{-5}$ and $R = 10^5$, for both levels of N. This wedge gets amplified greatly for $R = 2 \times 10^5$, which is reasonable for Bitcoin's peak price in December 2017: the hash rates with mining pools rise to about ten times that with only solo mining. The arms race escalates when miners are more risk-averse.

As expected, the homogeneous two-pool equilibrium generates lower global hash rates compared to the full risk-sharing equilibrium. Intuitively, pool managers with some market power take into account the arms race effect and hence discourage active miners' hash rate acquisition by raising their fees. Even when we give the best chance of this market-power force to produce a countervailing effect by considering the lowest possible of number of pools (here, $M = 2$), quantitatively there is no big difference from the full risk-sharing case. In fact, the difference between the full risk-sharing and two-pool cases becomes invisible when N is large (Panel C and D). Intuitively, when there are more competing active miners (i.e., N is large), pools engage in a more aggressive competition which is the root of the arms

[24] In a standard portfolio decision problem, a CARA agent without wealth effect will always demand the same amount of dollar exposure from a risky asset, independent of its size. As a result, the CARA agent's optimal share exposure goes down with the size of risky asset. In our model, the hash rates roughly correspond to the share exposure in a standard portfolio problem.

Figure 2: **Global Hash Rates under Solo, Full Risk Sharing, and Equilibrium**

Global hash rates Λ is plotted against block reward R under various parameters. We consider symmetric M pools each with passive hash rates $\Lambda_p = 3 \times 10^6$. The common parameter is $C = 0.002$, and other parameters are given as following. Panel A: $M = 2, N = 10, \rho = 2 \times 10^{-5}$; Panel B: $M = 2, N = 10, \rho = 1 \times 10^{-5}$; Panel C: $M = 2, N = 100, \rho = 2 \times 10^{-5}$; Panel D: $M = 2, N = 100, \rho = 1 \times 10^{-5}$.



race.

The takeaway from Figure 2 is that no matter whether we consider the friction of passive mining, the emergence of mining pools as a form of financial innovation escalates the mining arms race and contributes to its explosive growth in energy consumption in recent years. Note that while pooled mining and the increase in hash rates are both correlated with the rising price of Bitcoin, the force through which mining pools significantly amplify the global hash rates is in place at any price levels.

4.4 Equilibrium Pool Growth

We now state one of main result regarding the pool size distribution, which follows directly from Lemma 1 and Proposition 3.

Proposition 4 (Pool Growth Rate). *A pool with a larger initial Λ_{pm} has a (weakly) lower growth rate $\frac{\Lambda_{am}}{\Lambda_{pm}}$.*

This result implies that profit-maximizing mining pools do not create excessive centralization because a natural force from the market power of larger pools combined with the arms race nature of the mining technology limits their growth.

For illustration, Figure 3 studies a three-pool equilibrium with comparative statics for the endogenous fees charged by pool managers $\{f_1, f_2, f_3\}$ as well as equilibrium pool net growth $\{\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}, \Lambda_{a3}/\Lambda_{p3}\}$. Without loss of generality, we assume $\Lambda_{p1} > \Lambda_{p2} > \Lambda_{p3}$.

Panel A presents how the equilibrium fees respond to exogenous changes in the risk aversion ρ of this economy, and Panel B presents how the equilibrium fees vary with the unit hash rate acquisition cost C. Not surprisingly, when risk aversion increases, individual miners' demands for risk sharing increase, and mining pools charge higher fees as shown in Panel A of Figure 3. At the same time, larger pools charge higher fees, as predicted by Proposition 3. Panel C shows that larger pools hence grows more slowly.

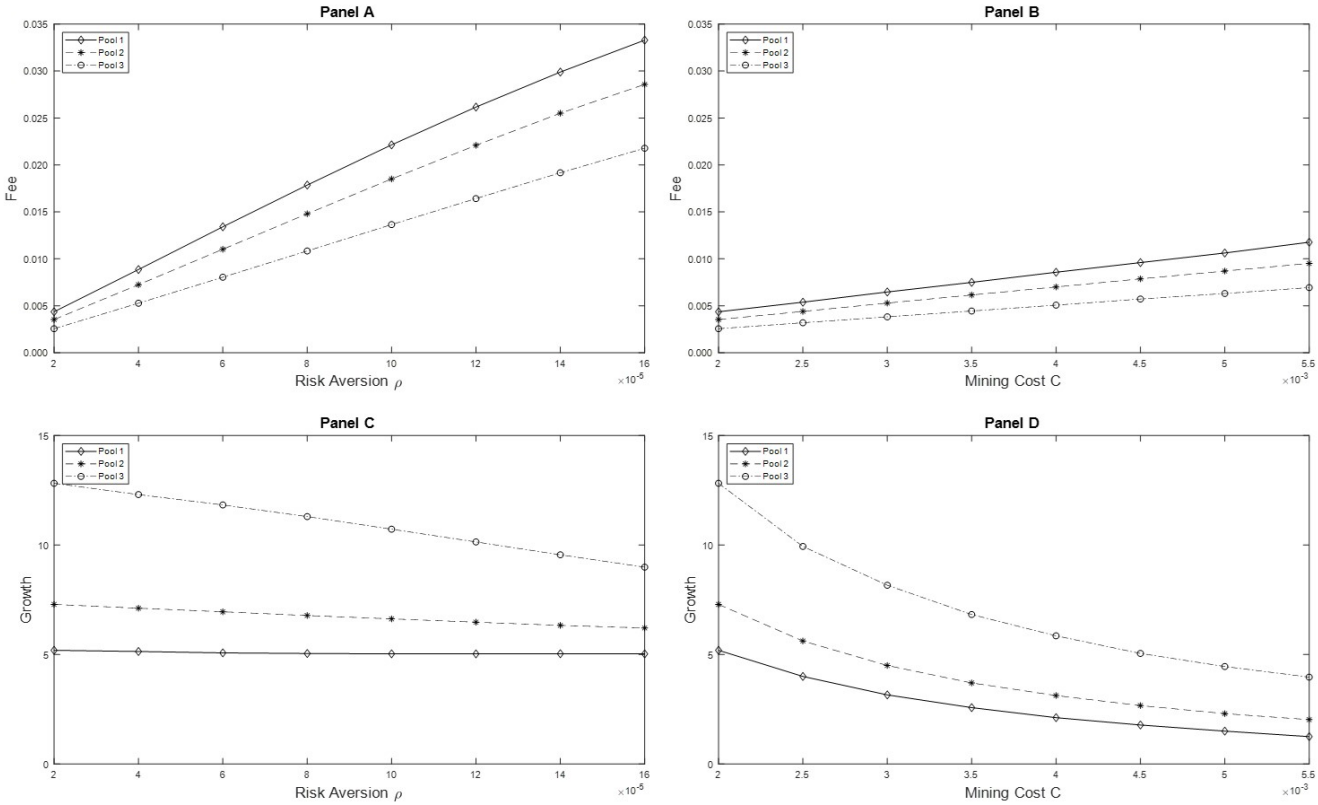
Panel B and D illustrate how the equilibrium outcomes change when we vary the constant hash rate acquisition cost C. As the hash rate acquisition cost C decreases, more active hash rates enter, and pool managers have stronger incentives to lower fees to compete for them. Fees and pool growths across pools are similar to other panels.

Importantly, this absence of dominant pools over time implies that the market power and internalization of mining externalities by pool managers (discussed in Section 4.3) are small relative to the extent risk sharing through mining pools encourages individuals to acquire additional hash rate. Consequently, even though Figure 2 depicts homogeneous pools, the aggravation of the mining arms race would not be mitigated much in the presence of heterogeneous pools.

When a constant fraction of miners do not adjust their hash rate contributions across pools—similar to common assumptions in the earlier literature (e.g., Calvo, 1983; Burdzy, Frankel, and Pauzner, 2001; He and Xiong, 2012), Proposition 4 implies that a larger pool grows at a slower rate. This sufficient condition of the constant fraction, however, is not necessary. In later empirical discussions, we prove that the implication on pool size growth remains valid as long as a larger pool has a higher absolute amount yet a *weakly* lower percentage of passive hash rates, a condition we verify in the data.

Figure 3: **Comparative Statics of Pool Fees and Growth**

Equilibrium fees $\{f_1, f_2, f_3\}$ and the net pool growth rates $\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}$, and $\Lambda_{a3}/\Lambda_{p3}$ are plotted against miner risk aversion ρ and unit hash rate cost C, respectively. The baseline parameters are: $R = 1 \times 10^5$, $\Lambda_{p1} = 3 \times 10^6, \Lambda_{p2} = 2 \times 10^6$, $\Lambda_{p3} = 1 \times 10^6$, and $N = 100$. In Panel A and C: $C = 0.002$. In Panel B and D: $\rho = 2 \times 10^{-5}$.



5 Empirical Evidence from Bitcoin Mining

Our theoretical analyses so far offer three predictions. First, global hash rates grow significantly as mining pools increasingly dominate the Bitcoin mining industry, as illustrated in Figure 1. This section provides supporting evidence for the other two cross-sectional predictions, that a pool with a larger size to start with tends to (i) charge a higher fee, and (ii) grow more slowly in percentage terms.

5.1 Data Description and Empirical Results

Our data consist of two major parts, one on pool fee/reward type dispersion and the other on pool size evolution. In the first part, information about fee contracts is obtained from Bitcoin Wiki. We scrape the entire revision history of the website (479 revisions in total)

Figure 4: **Empirical Relationships of Pool Sizes, Fees, and Growths**

This figure shows the scatter plots of *Proportional Fees* (Panel A) and the changes in *logSize* (Panel B) against lagged *logSize* for 2012-2014, 2015-2016, and 2017-2018, respectively. Red lines are the fitted OLS lines, with *t*-stat reported at the bottom. Data sources and descriptions are given in Section 5.

and carry forward a panel of pool fee evolutions over time.[25] Pool fees are aggregated to monthly frequency by simple average. In the second part, a pool's size (share of hash rates) is estimated from block-relay information recorded on the public blockchain (see BTC.com). Specifically, we count the number of blocks mined by a particular pool over a month, to be divided by the total number of newly mined blocks globally over the same month; the ratio gives the pool's monthly estimated hash rate share. The two parts are then merged to construct a comprehensive panel on pool size and fee evolution. Table 1 in Section 2 has provided summary statistics of the data.

Figure 4 shows scatter plots for our sample: Panel A presents the relationship between proportional fee and lagged pool size, and Panel B between subsequent pool size growth rate and lagged pool size. For robustness, we divide our sample into three windows (2012-2014, 2015-2016, and 2017-2018) and present the scatter plots for each window.[26] As predicted by our theory, Panel A shows that a larger pool tends to charge a higher fee (Proposition 3), and Panel B shows that a larger pool tends to grow at a slower pace (Proposition 4). We report detailed regression results in Table 2. Throughout the paper our panel regressions always include a monthly fixed effect, and cluster standard errors at the month level, as our identification comes mainly from the cross-section.

Before moving onto the next section, we emphasize that the above empirical patterns we find in the cryptocurrency mining industry—i.e., a positive size-fee relation and a negative size-growth relation—should not be taken for granted. For instance, in the passive asset management industry that offers index funds to retail investors, larger funds actually charge lower fees; Hortaçsu and Syverson (2004) provide a search-based mechanism to explain this empirical regularity. Moreover, while earlier studies on the size-growth relation indeed document that larger firms grow less (due to labor turnovers and the accumulation of industry-specific human capital) (Caves, 1998; Rossi-Hansberg and Wright, 2007), the recent literature on "superstar" firms finds increasing concentrations (and associated labour productivity divergence and labor share decline) across various industries and hence a positive size-growth relationship in the past decades (Andrews, Criscuolo, Gal, et al., 2016; Autor, Dorn, Katz, Patterson, and Van Reenen, 2017). Our empirical results thus constitute a piece

[25] Two large pools are missing from the Wiki: Bixin (which was available in the wiki as HaoBTC prior to Dec 2016), and BTC.top, for which we fill their information through direct communication with the pools. Bitfury, which is also missing from the Wiki, is dropped as it is a private pool not applicable to our analysis.

[26] We simply divide a seven-year sample into windows of 3-2-2, because there are fewer mining pools in the beginning of our sample as shown in Table (1).

Table 2: **Pool Size, Fee, and Growth: Regression Results**

This table reports results from regressing *Proportional Fee* (Panel A) and the changes in *logSize* (Panel B) on lagged *logSize*, respectively. At each month t, $Proportional\ Fee_{i,t}$ and $\Delta logSize_{i,t} = logSize_{i,t} - logSize_{i,t-1}$ and $Proportional\ Fee_{i,t}$ are regressed on $logSize_{i,t-1}$ over 2012-2014, 2015-2016, 2017-2018, and the entire sample period 2012-2018. We include a monthly fixed effect as we focus on cross-section pattern, and standard errors are clustered by month. Data sources and their descriptions are given in Section 5.

	Panel A: *Proportional Fee*			
	2012-2014 (1)	2015-2016 (2)	2017-2018 (3)	2012-2018 (4)
logSize	0.16***	0.24***	0.09***	0.16***
	(4.95)	(8.63)	(4.18)	(7.67)
Adjusted R^2	-0.007	0.078	-0.052	-0.002
Month FE	Yes	Yes	Yes	Yes
Observations	286	147	140	573

	Panel B: $\Delta logSize$			
	2012-2014	2015-2016	2017-2018	2012-2018
$\log Size$	-0.05**	-0.03*	-0.02	-0.03***
	(-2.35)	(-1.90)	(-1.36)	(-3.23)
Adjusted R^2	0.013	-0.004	0.031	0.016
Month FE	Yes	Yes	Yes	Yes
Observations	499	562	644	1705

t statistics in parentheses

$^* : p < 0.10, ^* * : p < 0.05, ^* ** : p < 0.01$

of new evidence to this debate on industrial organization economics.

5.2 Measuring Passive Hash Rates and Robustness

We note that when linking our theory to data, Figure 4 effectively uses a pool's lagged size to approximate its passive size, with an underlying assumption that a pool's passive hash rates are always proportional its size (as discussed in Section 3.1).

Our main theoretical predictions that larger pools or pools with larger passive hash rates charge higher fees and grow more slowly are still valid even without this assumption because we can directly use alternative measures for passive hash rates within a pool to test our theory predictions. Moreover, to the extent that our alternative measures are effective, we

can validate our earlier baseline empirical findings using initial pool sizes without requiring constant proportionality, as long as a larger pool has a higher absolute amount yet a *weakly* lower percentage of passive hash rates.

Measuring passive hash rates. Whether we use alternative measures of passive hash rates directly or link empirical pool sizes to passive hash rates, we need to quantify the size of passive hash rates within a pool. We construct several measures from transactions records on the blockchain, following the procedures below:

1. The coinbase transaction in each block identifies a pool manager's address. We then scan the entire blockchain to extract all transactions sent from each pool manager's address, and label them as paychecks to the pool's contributing miners.

2. Within each pool, we classify the contributing miners' addresses based on observed transacting behaviors. Specifically, we define loyalty addresses as ones that have only appeared in a unique pool manager's paychecks, and seed (relationship) addresses as the top 10 (10%) addresses receiving the most bitcoins from the pool manager within a month, respectively.

3. We measure a pool's loyalty size (the share of its loyalty addresses' total hash rates within global hash rates) for a particular month as the ratio between (i) the amount of bitcoins received by all of its loyalty addresses divided by one minus the prevailing pool fee, and (ii) the total amount of bitcoin created globally over the month.[27] Seed sizes and relationship sizes are similarly defined.

We use a pool's loyalty, seed, and relationship sizes as alternative proxies for the size of the pool's passive hash rates (Λ_{pm} in the model), reflecting various possible interpretations of passive hash rates: First, if an address only ever contributes to one pool, it cannot belong to an active miner who actively optimizes hash rate allocation over time. Second, some pools are created by a few larger miners who provide "seed" hash rates and tend to stick to their pool. Finally, like firms in any industry, a pool naturally interacts with its largest clients/investors to build long-term relations.

[27] For (i), if fee information is missing for a pool in a particular month, we divide the amount by one minus the average fee across all pools within that month.

We caution that since passive hash rates cannot be perfectly observed, all three measures are noisy approximations. Potential sources of noises include: some paycheck transactions may actually be "personal" transactions from pool managers; a miner could have multiple addresses or change addresses at will so a single address may not fully capture how a user transacts; some large active miners may have even more hash rates than "seed" or "relationship" miners. That said, we hope our various passive measures taken together can provide a more accurate inference.

Robustness of empirical findings on pool fee and size dynamics. We use each of the above proxies for passive hash rate to validate one sufficient condition for our earlier empirical findings to hold without assuming that passive hash rates is a fixed proportion of lagged pool size. Formally, the condition requires that two pools m, m' with sizes $S_{m,t} > S_{m',t}$ in month t satisfy

$$\Lambda_{pm,t} > \Lambda_{pm',t} \text{ and } \frac{\Lambda_{pm,t}}{S_{m,t}} \leq \frac{\Lambda_{pm',t}}{S_{m',t}}. \tag{17}$$

To see this, first Proposition 3 implies that

$$\Lambda_{pm,t} > \Lambda_{pm',t} \Rightarrow f_{m,t+1} > f_{m',t+1}$$

for $S_{m,t} > S_{m',t}$, which is the positive size-fee relationship (consistent with Panel A). Furthermore, by Proposition 4 we have

$$\Lambda_{pm,t} > \Lambda_{pm',t} \Rightarrow \frac{\Lambda_{am,t+1}}{\Lambda_{pm,t}} < \frac{\Lambda_{am',t+1}}{\Lambda_{pm',t}}.$$

Then using $\Lambda_{am,t+1} + \Lambda_{pm,t} = S_{m,t+1}$ together with the second condition in (17), we have

$$\frac{S_{m,t+1}}{S_{m,t}} < \frac{S_{m',t+1}}{S_{m',t}},$$

which is our negative size-growth relationship (consistent with Panel B).

We calculate the correlations between the passive size/share and the pool size based on the three alternative proxies of passive hash rates, where passive share is defined as passive size divided by pool size. We find a strong positive correlation between passive size and pool size: 0.72 for loyalty, 0.86 for seed, and 0.90 for relationship, all statistically significant at the 1% level. This supports the first condition in (17). For passive share, we find weak

Table 3: **Passive Size, Pool Fee, and Growth: Regression Results**

This table reports results from regressing *Proportional Fee* (Panel A) and either the change in *logSize* or *Active_Growth* (Panel B) on alternative measures of a pool's lagged passive hash rates, including loyalty size, seed size, and relationship size (Columns (2)-(4), respectively). The dependent variable in Panel B column (1) is $\Delta logSize$, while that in column (2)-(4) is $Active\_Growth_{i,t} = \frac{PoolSize_{i,t} - PassiveSize_{i,t-1}}{PassiveSize_{i,t-1}}$, with $PassiveSize$ respectively defined. For example, in column (2), $Active\_Growth_{i,t} = \frac{PoolSize_{i,t} - LoyaltySize_{i,t-1}}{LoyaltySize_{i,t-1}}$. Standard errors are clustered by month. Data sources and their descriptions are given in Section 5.

	Panel A: *Proportional Fee*			
	log Pool Size (1)	log Loyalty Size (2)	log Seed Size (3)	log Relationship Size (4)
Coefficient	0.16***	0.12***	0.17***	0.20***
t statistics	(7.67)	(8.17)	(6.23)	(10.19)
Adjusted R^2	-0.002	-0.077	-0.096	0.013
Monthly FE	Yes	Yes	Yes	Yes
# Obs.	573	396	413	413
	Panel B: $\Delta logSize$ or $\Delta Active\_Growth$			
Coefficient	-0.03***	-9.73***	-0.36***	-0.34***
t statistics	(-3.23)	(-20.49)	(-11.66)	(-16.21)
Adjusted R^2	0.016	0.429	0.128	0.170
Monthly FE	Yes	Yes	Yes	Yes
# Obs.	1705	1154	1287	1287

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

correlations with ambiguous signs across three measures: 0.10 for loyalty, -0.25 for seed, and 0.06 for relationship (with the first two being statistically significant at 1% level), indicating little systematic pattern relating passive share and pool size. These empirical patterns corroborate condition (17) and hence lend support to Table 2 as a valid empirical test for our main theoretical predictions.

Robustness of theory predictions using alternative measures directly. Table 3 provides additional robustness results when we directly use alternative measures of passive hash rates. In Panel A and B, we reproduce Table 2 by replacing pool size with alternative passive size measures. In other word, we regress pool fees and growths on passive sizes, where passive sizes are approximated by loyalty, seed, and relationship sizes, respectively.

The results in Table 3 are consistent with our theoretical predictions with strong sig-

nificance. To calculate growth properly as described in Proposition 4, we use the ratios of active sizes over lagged passive sizes, on lagged passive sizes.[28] The results using various measures of passive hash rates collectively indicate the robust positive relationship between pool (passive) size and fee as well as the negative relationship between pool (passive) size and growth, just as our model predicts.

6 Discussions and Extensions

In this section, we first show that mining pools' market powers survive pool entry, followed by discussions on how our model applies to alternative blockchain systems such as proof-of-stake. Along the way, we also present an economist's perspective on several important issues including the nature of risk as well as other centralization and decentralization forces.

6.1 Entry and Market Power of Mining Pools

Thus far, we have exogenously specified that some pool managers have endowed passive hash rates. In this section, we show that our results are robust to potential entry of competing pools and a pool's passive hash rates give it an intrinsic market power. In other words, the incumbent pools engage in a monopolistic competition even in face of potential entry, and as a result full risk-sharing cannot be obtained in equilibrium.

Denote by M^I the number of incumbent pools, and M^E the (potentially endogenous) number of entrant pools with some passive hash rates; $M \equiv M^I + M^E$ is then the total number of (potential) mining pools. For simplicity, we illustrate with a setting of homogeneous potential entrants in a two-stage game: in the first stage each potential entrant pool decides whether to incur $K \geq 0$ and enter; the entrants and incumbents then play the second stage game as pool managers like in our baseline model. In addition to the setup cost $K \geq 0$, when making the entry decisions, each entrant also simultaneously makes a binary decision

[28] Because this ratio can become abnormally large for pools with small estimated passive sizes, we use 90% winsorization. Our results are robust to using alternative thresholds (the top 25/50 and 25%/50% largest addresses) to redefine seed and relationship addresses. We, however, caution that this strong significance in Panel B may be partially caused by a mechanical negative link between the left-hand side and right-hand side variables. In fact, when Condition (17) holds, it is valid to regress $\Delta logSize$ directly on passive hash rates to talk about pool growth, and we find similar results. Note that the growth-size relationship in Table 2 may suffer from the same mechanical issue. Nevertheless, the literature on firm size dynamics which uses the same specification of Table 2 and, as we discuss in Section 5.1, still finds mixed results. Our findings therefore add to the literature by providing unambiguous results concerning the cypto-mining industry.

whether to incur an addition acquisition cost $K' > 0$ for some initial passive hash rates. More specifically, entrants could enter with $\Lambda_p^E = 0$ (after incurring $K \geq 0$) or $\Lambda_p^E = \Delta$ where $\Delta > 0$ is a positive constant (after incurring $K + K' > 0$).[29] The case of free entry corresponds to $K = 0$.

First, without loss of generality, at most one pool without passive hash rates ($\Lambda_p^E = 0$) enters, and just breaks even to cover the entry cost K. This is because multiple entrants without passive hash rates would compete away their mining profits.[30] Second, only a finite number of pools with passive rates Δ enter in equilibrium because of bounded total mining revenue and positive acquisition cost for Λ_p^E. Entry of pools with passive hash rates stops when it is no longer profitable to acquire passive hash rates and enter. In summary, there could be a finite number of pools entering with passive hash rates, plus at most one without (as explained in the paragraph above).

Independent of the exact equilibrium number of entrant pools M^I, as to be further explained below, the industrial organization of mining pools with an endogenous number of incumbent pools is qualitatively similar to our baseline model with exogenous M: Each pool exerts its monopolist power by charging a positive fee to its active miners. As in any monopolistic competition, entry continues until the profits cannot cover the entry costs.

Monopolistic competition and incumbent pools' market powers. We now examine the economic impact on the the incumbent and entrant pools' market powers from entry. In our model, because risk-averse active miners face a portfolio diversification problem, incumbent pools with $\Lambda_{pm} > 0$ always charge strictly positive fees to some active miners even when facing competitions from entrant pool(s). In other words, incumbents always retain some market power even under free entry.

Proposition 5 (Market Power of Incumbent Pools)**.** *In an equilibrium with active mining in some pools, every pool with passive hash rates charges a strictly positive fee and attracts a strictly positive measure of active hash rates, even when $K = 0$.*

If a pool with strictly positive passive hash rates counterfactually charges zero fee, the marginal benefit to an active miner from allocating the first infinitesimal hash rate to this

[29] The market for passive hash rates, as indicated in Section 5.2, could be quite different from that of active hash rates. We leave the micro-foundation for the acquisition of passive hash rates to future research.

[30] Even for free entry ($K = 0$), Proposition 2 implies the size distribution of entrant pools is irrelevant from active miners' perspective, and equilibrium outcomes for active miners' allocation and payoff are equivalent to the case with one pool entering and charging zero fee.

pool equals to the risk-neutral valuation, $\frac{R}{\Lambda}$, which exceeds the active miner's marginal cost (see Eq. (13)). As a result, the pool in question can profitably deviate to charge a strictly positive fee while retaining this active miner. This logic implies that in equilibrium all pools with strictly positive passive hash rates—incumbent or entrant—charge strictly positive fees.

Different from a standard perfectly competitive market wherein Bertrand-type price competition allows entrant firms to compete away all profits from the incumbents, pools with strictly positive passive hash rates face a monopolistic competition: The unique diversification opportunity a pool with strictly positive passive hash rates offers to active miners makes it a product with "superior quality" and hence an imperfect substitute to other pools.

Because of pool managers' market power from the passive-hash-rate friction, active miners never achieve full risk sharing, resulting in a welfare distortion. That said, the lack of full risk sharing alleviates the arms race and reduces energy consumption, albeit by a small amount, as we discuss earlier.

6.2 The Nature of Risk

Given that risk sharing drives the formation of mining pools, several issues regarding the nature of the risk are worth discussing. First, a miner's underlying mining risk $\tilde{B}$, i.e., whether and when a miner finds the solution, is idiosyncratic. Our paper emphasizes the importance of diversification, rather than pricing idiosyncratic risk (via pools). Idiosyncratic risk matters little for pricing exactly because agents diversify it away.

The idiosyncratic nature of mining risk may also lead to a hasty conclusion: risk-averse agents who are well-diversified on their financial wealth should be neutral to idiosyncratic risk if they can engage in an infinitesimal amount of mining. This claim is incorrect because the celebrated asset pricing result holds only when agents can trade infinitesimal "shares" of assets with idiosyncratic risks (which, in a way, is similar to participating in mining pools). But in our model, without participating in pools, acquiring an infinitesimal amount of hash rate shrinks the probability of winning toward zero without changing the magnitude of (risky) reward.[31] If this reward is significant relative to the agent's consumption, then

[31] In standard asset pricing models, an agent with utility function u who consumes $\widetilde{C}$ and faces an asset with idiosyncratic payoff $\widetilde{R}$ and price p, solves $\max_\epsilon \mathbb{E}\left[u\left(\widetilde{C}+\epsilon\widetilde{R}-\epsilon p\right)\right]$. Then the Euler equation gives the risk-neutral pricing $p=\mathbb{E}[\widetilde{R}]$ if $\widetilde{R}$ is idiosyncratic. However, in our mining technology, the miner who can acquire infinitesimal hash rates solves $\max_\epsilon \epsilon\mathbb{E}\left[u\left(\widetilde{C}+R-\epsilon p\right)\right]+(1-\epsilon)\mathbb{E}\left[u\left(\widetilde{C}-\epsilon p\right)\right]$, as he receives

risk-diversification benefits remain for this lottery with infinitesimal winning probability.

Second, there is anecdotal evidence that miners are under-diversified for their idiosyncratic mining incomes. It is also important to realize that throughout our observation period, the mining income often represents a significant source of the miner's total income, justifying the relevance of diversifying the idiosyncratic risk in this context.[32] Furthermore, as in the discussion of the now famous "fallacy of large numbers" by Samuelson (1963) and a further treatise by Ross (1999), mining over a long period of time does not help in general.

Third, why do blockchain protocols randomize the allocation of newly minted cryptocurrencies or crypto-tokens to start with? Although outside our model, we believe the design is motivated by the need to ensure proper ex-post incentives of record-generation once a miner has mined a block. If a miner always gets paid deterministic rewards in proportion to his hash rate no matter who successfully mines the block, then a successful miner who puts in very little hash rate (and thus gets very little reward) worries less about not being endorsed by subsequent miners because the benefit of mis-recording could outweigh the expected cost of losing the mining reward.

Finally, we can easily introduce systematic risk in the mining reward $\tilde{R}$, which these days is predominantly determined by the price of the Bitcoin. If—and this is a big if—Bitcoin ever becomes an important private money that is free from inflation (due to rule-based supply), as some advocates envision, then its exchange rate against fiat money would presumably be driven by macroeconomic shocks such as inflation. It constitutes an interesting future study to analyze the role of systematic risk in our framework, especially when $\tilde{R}$ offers some diversification benefits for investors in the financial market.

6.3 General Implications for Consensus Protocols

Other proof-of-work blockchains Our model can help us better understand the centralizing and decentralizing forces in other prominent proof-of-work blockchains, such as Ethereum, Bitcoin Cash (BCH), Litecoin (LTC), and ZCash (ZEC). They have all witnessed the rise of mining pools and similar trends in their mining industrial organizations.

R with probability ϵ. The curvature of u enters in the valuation $p = \frac{\mathbb{E}[u(\widetilde{C}+R)-u(\widetilde{C})]}{\mathbb{E}[u'(\widetilde{C})]}$.

[32] The recent introduction of future contracts on CBOE and CME may alleviate this problem in a significant way, but it is unclear how long it takes for the miner community to actively trading on the future contracts or for more derivatives and insurance products to be introduced.

Proof-of-stake protocols A popular alternative to the PoW protocol is the Proof-of-Stake (PoS) protocol. In many PoS systems, independent nodes are randomly selected to append the blockchain, just like in PoW, with the probability of being selected determined by the amount of "stakes" held, rather than the amount of computing power consumed. Early examples include Nxt and BlackCoin, where the calculation of "stake" involves the amount of crypto assets held as well as Peercoin, where the calculation of "stake" involves how long a crypto asset has been held (coin age).

Our model's implications for the industrial organization of players in the decentralized consensus generation process applies to such PoS systems equally well. This is because of PoS's similar features of risky rewards and negative externality. The same risk-sharing motive should drive the formation of "staking pools." This indeed happens: The largest players such as StakeUnited.com, simplePOSpool.com, and CryptoUnited typically charge a proportional fee of 3% to 5%. An individual's problem of allocating her stake is exactly the same as in (10), with λ_m indicating the amount of stake allocated to pool m. All our results go through, except that in PoS the consensus generation process does not necessarily incur a high energy consumption, and the exact operation within a pool adjusts accordingly.

Recent trends in the blockchain sphere are consistent with our model predictions: For example, in light of the high energy associated with PoW protocols, Ethereum plans to switch from PoW to PoS (Eth 2.0 and Casper). Recognizing mining pools' inevitable rise, systems such as EOS adopts delegated-Proof-of-Stake (DPoS) in its consensus generation process, in which a small group of validators can take control of the network: DPoS stakeholders vote for delegates (typically referred to as block producers or witnesses) who maintain consensus records and share rewards with their supporting stakeholders, in proportion to their stakes after taking cuts, just like the pool managers in our model who charge fees and give out proportional rewards to individual miners.[33]

6.4 Centralization in Decentralized Systems

In this paper we focus on risk sharing and market power as centralizing and decentralizing forces. This perspective does not preclude other forces. For example, Chapman, Garratt,

[33]Delegates on LISK, for example, offer up to more than 90% shares of the rewards to the voters. As of Oct 2018, about 80 percent offer at least 25% shares (https://earnlisk.com/). Some DPoS-based systems such as BTS and EOS traditionally have delegates paying little or no rewards to stakeholders, but that is changing. See, for example, https://eosuk.io/2018/08/03/dan-larimer-proposes-new-eos-rex-stake-reward-tokens/.

Hendry, McCormack, and McMahon (2017), de Vilaca Burgos, de Oliveira Filho, Suares, and de Almeida (2017), and Cong and He (2018) discuss how the concern for information distribution could make nodes in blockchain networks more concentrated.

The blockchain community has also proposed several reasons for why a mining pool's size may be kept in check: (1) Ideology: Bitcoin miners, at least in the early days, typically have strong crypto-anarchism backgrounds, so centralization is against their ideology. We think this force is unlikely to be first-order as Bitcoin develops into a hundred-billion-dollar industry. (2) Sabotage: just like the single-point-of-failure problem in traditional centralized systems, large mining pools also attract sabotages, such as decentralized-denial-of-service (DDoS) attacks from peers (e.g., Vasek, Thornton, and Moore, 2014). While sabotage concerns could affect pool sizes, they are outside the scope of this paper. (3) Trust crisis: it has been argued that Bitcoin's value builds on it being a decentralized system. Over-centralization by any single pool may lead to a collapse in Bitcoin's value, which is not in the interest of the pool in question. Empirical evidence for this argument, however, is scarce. We find no significant correlation between the HHI of the mining industry with bitcoin prices. Nor do we find any price response to concerns about the potential GHash.IO 51% attack around July in 2014.

We do not rule out other potential explanations for our empirical findings. For example, higher prices for larger pools could be attributed to product differentiation or larger pools being more trustworthy. However, we argue that these alternative channels are less likely to be the key drivers for the empirical patterns. Crypto-mining represents a setting that products are not differentiated in the traditional sense. Products are differentiated in the sense that larger pools provide greater risk-sharing services, which our model accounts for. Larger pools' enjoying greater trust also does not imply that they grow more slowly.[34]

7 Conclusion

Our paper's contribution is three-fold. First, we formally develop a theory of mining pools that highlights risk sharing as a natural centralizing force. When applied to proof-of-work-based blockchains, our theory reveals that financial innovations that improve risk sharing can escalate the mining arms race and increase energy consumption. Second, we

[34]We thank an anonymous referee for suggesting these alternative channels and pointing out why they are unlikely the key drivers.

explain why a blockchain system could remain decentralized over time and find empirical evidence from the Bitcoin mining industry that support our theory. Albeit not necessarily the only explanation for the industry evolution, ours closely ties to risk sharing which gives rise to mining pools in the first place. Our model therefore serves as a backbone upon which other external forces (e.g., DDoS attacks) could be added. Finally, our paper adds to the literature on industrial organization by incorporating the network effect of risk sharing into a monopolistic competition model and highlighting in the context of cryptocurrency mining the roles of risks and fees in firm-size distribution.

As one of the first economics papers on mining pools, we have to leave many interesting topics to future research, such as potential pool collusion outside the mining market and alternative pool objectives. Anecdotally, there is speculation that a large pool ViaBTC, along with allies AntPool and BTC.com pool, are behind the recent promotion of Bitcoin Cash, a competing cryptocurrency against Bitcoin. Hence these pools' behavior in Bitcoin mining may not necessarily be profit-maximizing. We also do not consider the ramification of concentration along the vertical value chain of mining. For instance, Bitmain, the owner of AntPool and BTC.com, as well as a partial owner of ViaBTC, is also the largest Bitcoin mining ASIC producer who currently controls 70% of world ASIC supply. Because we focus on pool formation and competition, we leave open an orthogonal (geographic) dimension of mining power concentration: locations with cheap electricity, robust networks, and a cool climate tend to attract disproportionately more hash rates. In this regard, our findings constitute first-order benchmark results rather than foregone conclusions.

References

Andrews, Dan, Chiara Criscuolo, Peter N Gal, et al., 2016, The best versus the rest: the global productivity slowdown, divergence across firms and the role of public policy, Discussion paper, OECD Publishing.

Autor, David, David Dorn, Lawrence F Katz, Christina Patterson, and John Van Reenen, 2017, Concentrating on the fall of the labor share, *The American Economic Review* 107, 180.

Benetton, Matteo, Giovanni Compiani, and Adair Morse, 2019, Cryptomining: Local evidence from china and the us, *Working paper*.

Berk, Jonathan B, and Richard C Green, 2004, Mutual fund flows and performance in rational markets, *Journal of political economy* 112, 1269–1295.

Berk, Jonathan B, Richard Stanton, and Josef Zechner, 2010, Human capital, bankruptcy, and capital structure, *The Journal of Finance* 65, 891–926.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, 2018, The blockchain folk theorem, .

Budish, Eric, 2018, The economic limits of bitcoin and the blockchain, Discussion paper, National Bureau of Economic Research.

Burdzy, Krzysztof, David M Frankel, and Ady Pauzner, 2001, Fast equilibrium selection by rational players living in a changing world, *Econometrica* 69, 163–189.

Calvo, Guillermo A, 1983, Staggered prices in a utility-maximizing framework, *Journal of monetary Economics* 12, 383–398.

Cao, Sean, Lin William Cong, and Baozhong Yang, 2018, Auditing and blockchains: Pricing, misstatements, and regulation, *Working Paper. Submission invited.*

Caves, Richard E, 1998, Industrial organization and new findings on the turnover and mobility of firms, *Journal of Economic Literature* 36, 1947–1982.

Chapman, James, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon, 2017, Project jasper: Are distributed wholesale payment systems feasible yet?, *Financial System* p. 59.

Chiu, Jonathan, and Thorsten V Koeppl, 2018, Blockchain-based settlement for asset trading, *Review of Financial Studies* Forthcoming.

——— , 2019, The economics of cryptocurrencies–bitcoin and beyond, .

Cong, Lin William, and Zhiguo He, 2018, Blockchain disruption and smart contracts, *Review of Financial Studies* Forthcoming.

Cong, Lin William, Ye Li, and Neng Wang, 2018, Tokenomics: Dynamic adoption and valuation, *BFI Working Paper.*

——— , 2019, Tokenomics and platform finance, *Working Paper.*

de Vilaca Burgos, Aldenio, Jose Deodoro de Oliveira Filho, Marcus Vinicius Cursino Suares, and Rafael Sarres de Almeida, 2017, Distributed ledger technical research in central bank of brazil, .

de Vries, Alex, 2019, Renewable energy will not solve bitcoins sustainability problem, *Joule* 3, 893–898.

Dimitri, Nicola, 2017, Bitcoin mining as a contest, *Ledger* 2, 31–37.

Easley, David, Maureen O'Hara, and Soumya Basu, 2017, From mining to markets: The evolution of bitcoin transaction fees, .

Economist, The, 2017, Learning the lessons of equihack, *The Economist September 16, 2017* September 16, 14.

Eyal, Ittay, 2015, The miner's dilemma, in *Security and Privacy (SP), 2015 IEEE Symposium on* pp. 89–103. IEEE.

——— , and Emin Gün Sirer, 2014, Majority is not enough: Bitcoin mining is vulnerable, in *International Conference on Financial Cryptography and Data Security* pp. 436–454. Springer.

Fama, Eugene F, 1976, *Foundations of finance: portfolio decisions and securities prices* (Basic Books (AZ)).

Fisch, Ben, Rafael Pass, and Abhi Shelat, 2017, Socially optimal mining pools, in *International Conference on Web and Internet Economics* pp. 205–218. Springer.

Forum, Bitcoin, 2014, Confused about which mining pool to join and stick with, *Bitcon Forum* February 4.

Gervais, Arthur, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun, 2016, On the security and performance of proof of work blockchains, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* pp. 3–16. ACM.

Glode, Vincent, Richard C Green, and Richard Lowery, 2012, Financial expertise as an arms race, *The Journal of Finance* 67, 1723–1759.

Harris, Milton, and Bengt Holmstrom, 1982, A theory of wage dynamics, *The Review of Economic Studies* 49, 315–333.

Harvey, Campbell R, 2016, Cryptofinance, *Working Paper*.

He, Zhiguo, and Wei Xiong, 2012, Dynamic debt runs, *Review of Financial Studies* 25, 1799–1843.

Hölmstrom, Bengt, 1979, Moral hazard and observability, *The Bell journal of economics* pp. 74–91.

Hortaçsu, Ali, and Chad Syverson, 2004, Product differentiation, search costs, and competition in the mutual fund industry: A case study of s&p 500 index funds, *The Quarterly Journal of Economics* 119, 403–456.

Huberman, Gur, Jacob D Leshno, and Ciamac C Moallemi, 2017, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, .

Konrad, Kai A, 2007, Strategy in contests-an introduction, *WZB-Markets and Politics Working Paper No. SP II* 1.

Kugler, Logan, 2018, Why cryptocurrencies use so much energy: and what to do about it, *Communications of the ACM* 61, 15–17.

Lee, Sherman, 2018, Bitcoin's energy consumption can power an entire country – but eos is trying to fix that, Discussion paper, https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#45c9a5e91bc8.

Li, Jiasun, 2015, Profit-sharing, wisdom of the crowd, and theory of the firm, *Discussion Paper*.

——— , 2017, Profit sharing: A contracting solution to harness the wisdom of the crowd, .

Li, Jingming, Nianping Li, Jinqing Peng, Haijiao Cui, and Zhibin Wu, 2019, Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, *Energy* 168, 160–168.

Li, Jiasun, and William Mann, 2018, Initial coin offering and platform building, .

Ma, June, Joshua S Gans, and Rabee Tourky, 2018, Market structure in bitcoin mining, Discussion paper, National Bureau of Economic Research.

Malinova, Katya, and Andreas Park, 2016, Market design for trading with blockchain technology, *Available at SSRN*.

Mora, Camilo, Randi L Rollins, Katie Taladay, Michael B Kantar, Mason K Chock, Mio Shimada, and Erik C Franklin, 2018, Bitcoin emissions alone could push global warming above 2°c, *Nature Climate Change* p. 1.

Nakamoto, Satoshi, 2008, Bitcoin: A peer-to-peer electronic cash system, .

Nitzan, Shmuel, 1991, Collective rent dissipation, *The Economic Journal* 101, 1522–1534.

Pagnotta, Emiliano, and Andrea Buraschi, 2018, An equilibrium valuation of bitcoin and decentralized network assets, .

Prat, Julien, and Benjamin Walter, 2018, An equilibrium model of the market for bitcoin mining, .

Rogers, Adam, 2017, The hard math behind bitcoin's global warming problem, *WIRED* Dec 15, 2017, https://www.wired.com/story/bitcoin–global–warming/.

Rosenfeld, Meni, 2011, Analysis of bitcoin pooled mining reward systems, *arXiv preprint arXiv:1112.4980*.

Ross, Stephen A, 1999, Adding risks: Samuelson's fallacy of large numbers revisited, *Journal of Financial and Quantitative Analysis* 34, 323–339.

Rossi-Hansberg, Esteban, and Mark LJ Wright, 2007, Establishment size dynamics in the aggregate economy, *American Economic Review* 97, 1639–1666.

Rosu, Ioanid, and Fahad Saleh, 2019, Evolution of shares in a proof-of-stake cryptocurrency, *Available at SSRN 3377136*.

Saleh, Fahad, 2019, Blockchain without waste: Proof-of-stake, Discussion paper, working Paper.

Salop, Steven, and Joseph Stiglitz, 1977, Bargains and ripoffs: A model of monopolistically competitive price dispersion, *The Review of Economic Studies* 44, 493–510.

Samuelson, Paul A, 1963, Risk and uncertainty: A fallacy of large numbers, .

Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar, 2016, Optimal selfish mining strategies in bitcoin, in *International Conference on Financial Cryptography and Data Security* pp. 515–532. Springer.

Schrijvers, Okke, Joseph Bonneau, Dan Boneh, and Tim Roughgarden, 2016, Incentive compatibility of bitcoin mining pool reward functions, in *International Conference on Financial Cryptography and Data Security* pp. 477–498. Springer.

Stiglitz, Joseph E, 1974, Incentives and risk sharing in sharecropping, *The Review of Economic Studies* 41, 219–255.

Torpey, Kyle, 2016, An interview with viabtc, the new bitcoin mining pool on the blockchain, *Bitcoin Magazine* p. Sept 16.

Truby, Jon, 2018, Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies, *Energy research & social science*.

Varian, Hal R, 1980, A model of sales, *The American Economic Review* 70, 651–659.

Vasek, Marie, Micah Thornton, and Tyler Moore, 2014, Empirical analysis of denial-of-service attacks in the bitcoin ecosystem, in *International Conference on Financial Cryptography and Data Security* pp. 57–71. Springer.

Vukolić, Marko, 2015, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in *International Workshop on Open Problems in Network Security* pp. 112–125. Springer.

Wilson, Robert, 1968, The theory of syndicates, *Econometrica* pp. 119–132.

Yermack, David, 2017, Corporate governance and blockchains, *Review of Finance* 21, 7–31.

Appendix A. Proofs of Lemmas and Propositions

A1. Proof of Proposition 1

Proof. It is easy to verify that $\mathbb{E}[X_{pool}] = \mathbb{E}[X_{solo}]$. Hence it suffices to show that X_{solo} is a mean-preserving spread of X_{pool}. To see this, note that

$$\begin{aligned} X_{solo} &= (\tilde{B}^A_{solo} + \tilde{B}^B_{solo})R - \tilde{B}^B_{solo}R \;=\; \tilde{B}_{pool}R - \tilde{B}^B_{solo}R \\ &= \frac{\lambda_A}{\lambda_A+\lambda_B}\tilde{B}_{pool}R + \frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \\ &= X_{pool} + \left(\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R\right) \end{aligned}$$

and

$$\mathbb{E}\left[\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \mid X_{pool}\right] = 0, \tag{18}$$

where $\tilde{B}^i_{solo}$, $i \in \{A, B\}$, denotes the number of blocks a miner/pool with hash rate λ_i finds within time T. Equation (18) holds because

$$\mathbb{E}\left[\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \mid \tilde{B}_{pool} = n\right] = \frac{\lambda_B}{\lambda_A+\lambda_B}nR - \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}_{pool} = n\right]R$$

while

$$\begin{aligned} \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}_{pool} = n\right] &= \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}^A_{solo} + \tilde{B}^B_{solo} = n\right] = \sum_{k=1}^{n} k \frac{\left(e^{-\lambda_B}\frac{\lambda_B^k}{k!}\right)\left(e^{-\lambda_A}\frac{\lambda_A^{n-k}}{(n-k)!}\right)}{e^{-(\lambda_A+\lambda_B)}\frac{(\lambda_A+\lambda_B)^n}{n!}} \\ &= \sum_{k=1}^{n} k \frac{n!}{k!(n-k)!}\left(\frac{\lambda_B}{\lambda_A+\lambda_B}\right)^k\left(\frac{\lambda_A}{\lambda_A+\lambda_B}\right)^{n-k} = \frac{\lambda_B}{\lambda_A+\lambda_B}n \end{aligned}$$

□

A2. Proof of Proposition 2 and Its Generalization

Proof. We prove the more general case with potential entrant pools, as discussed in Section 6.1. We start with the individual miner's problem in Eq. (10). When $\Lambda_{pm} = 0$, the derivative with respect to λ_m is

$$\frac{1}{\Lambda}R(1-f_m)e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}}} - C \tag{19}$$

Note that in a symmetric equilibrium, $\Lambda_{am} = N\lambda_m$. Therefore the marginal utility of adding hash rate to pool m is simply

$$\frac{1}{\Lambda}R(1-f_m)e^{-\rho R(1-f_m)/N} - C, \tag{20}$$

which is strictly monotonic (either decreasing or increasing) in f_m over $[0,1]$. Then an equilibrium must have each f_m be the same for all incumbent pools, otherwise a miner can profitably deviate by moving some hash rate from one pool to another. If all incumbent pools charge positive fees, then at least one pool manager can lower the fee by an infinitesimal amount to gain a non-trivial measure of hash rate, leading to a profitable deviation. Therefore, $f_m = 0 \; \forall \; m \in \{1, 2, \cdots, M^I\}$, where M^I denotes the number of incumbent pools. We use M to denote the total number of entrant and incumbent pools.

Now suppose we have entrants who can enter by incurring a fixed cost K. Then they have to charge zero fee because otherwise all miners would devote all hash rates to incumbents who charge zero fees. Therefore if K is positive, there will be no entrants as they cannot enter and recoup the setup cost; even if $K = 0$, while potential entrants are indifferent about whether to enter or not and any number of entrants could be an equilibrium outcome, in all equilibria pools charge zero fees and attract the same amount of total hash rates, and the exact size distribution of pools is irrelevant.

For individual miners to be indifferent about whether to acquire more hash rate or not, the global hash rate Λ has to equalize the marginal benefit of hash rate with its marginal cost C, which leads to $\Lambda = \frac{R}{C}e^{-\rho R/N}$. Therefore the payoff to each miner is

$$\frac{1}{\rho\Lambda}\left[\sum_{m=0}^{M}\Lambda_{am}\left(1-e^{-\rho R\frac{\lambda_m}{\Lambda_{am}}}\right)\right] - \frac{R}{N}e^{-\rho R/N} = \frac{1}{\rho}(1-e^{-\rho R/N}) - \frac{R}{N}e^{-\rho R/N}, \tag{21}$$

where we have used the fact that $\sum_{m=0}^{M}\Lambda_{am} = \Lambda$, the sum of all hash rates of active miners in consideration with an aggregate measure N. And the utility from mining in pools is strictly positive, as it is easy to show that RHS is strictly positive when $R > 0$. So miners indeed join these pools. The exact distribution of pool size does not matter as long as $\sum_{m=0}^{M}\lambda_m = \Lambda/N = \frac{R}{NC}e^{-\rho R/N}$. □

A3. Proof of Lemma 1

Proof. Obviously, for pools charging the same f_m, the RHS of (14) is the same, implying $\frac{\lambda_m^*}{\Lambda_{pm}}$ is the same. Now, because of fully flexible hash rate acquisition for all miners, in equilibrium

(13) implies that

$$R(1-f_m) = C\Lambda e^{\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} \leq C\Lambda e^{\rho R(1-f_m)/N} < C\Lambda e, \tag{22}$$

where the last inequality follows Assumption 1. This implies that the RHS of (14), if positive, has negative partial derivative with respect to f_m. Therefore, among pools with positive active mining, those charging higher fees would have lower net growths $\frac{\lambda_m}{\Lambda_{pm}}$ in equilibrium. □

A4. Proof of Proposition 3

The following lemma is useful for the proof of Proposition 3.

Lemma (A1). *$\forall m$ such that. $f_m < 1$, pool managers' FOC holds in equilibrium:*

$$\rho R e^{-\rho R f_m}\left(1 - \frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right) - \left(1-e^{-\rho R f_m}\right)\frac{N}{\rho R(1-f_m)^2}\left(1-\ln\frac{R(1-f)}{C\Lambda}\right)$$
$$- \left(1-e^{-\rho R f_m}\right)\frac{\frac{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}+\frac{N}{\rho R(1-f_m)}\right)}{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)^2}\frac{N}{\rho R(1-f_m)^2}(\ln\frac{R(1-f_m)}{C\Lambda}-1)\Lambda_{pm}}{\Lambda + \sum_{m'}\frac{\frac{N}{\rho R(1-f_{m'})}}{\left(1-\frac{N}{\rho R(1-f_{m'})}\ln\frac{R(1-f_{m'})}{C\Lambda}\right)^2}\Lambda_{pm'}} = 0. \tag{23}$$

Proof. Substitute

$$\frac{d\Lambda}{df_m} = -\frac{\frac{\partial}{\partial f_m}\left(\Lambda - \frac{1}{1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}}\Lambda_{pm} - \Lambda_{-m}\right)}{\frac{\partial}{\partial\Lambda}\left(\Lambda - \frac{1}{1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}}\Lambda_{pm} - \Lambda_{-m}\right)} = \frac{\frac{1}{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)^2}\frac{N}{\rho R(1-f_m)^2}(\ln\frac{R(1-f_m)}{C\Lambda}-1)\Lambda_{pm}}{1+\sum_{m'}\frac{\frac{N}{\rho R(1-f_{m'})}}{\Lambda\left(1-\frac{N}{\rho R(1-f_{m'})}\ln\frac{R(1-f_{m'})}{C\Lambda}\right)^2}\Lambda_{pm'}}$$

into the derivative of pool m's objective $\Lambda_{pm}\frac{1-e^{-\rho R f_m}}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)}$ with respect to f_m:

$$\Lambda_{pm}\left(\frac{\rho R e^{-\rho R f_m}}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)} - \frac{\left(1-e^{-\rho R f_m}\right)\frac{N}{\rho R(1-f_m)^2}\left(1-\ln\frac{R(1-f)}{C\Lambda}\right)}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)^2}\right.$$
$$\left. - \frac{\left(1-e^{-\rho R f_m}\right)\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}+\frac{N}{\rho R(1-f_m)}\right)}{\Lambda^2\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)^2}\frac{d\Lambda}{df_m}\right),$$

and factor out nonzero terms. □

Proof of Proposition 3. We prove the proposition by contradiction. Suppose a larger pool charges a weakly lower fee. From (23) in Lemma A1, we know that $\forall m$ such that $f_m < 1$

$$\frac{\Lambda_{pm}}{\Lambda^* + \sum_{m'} \frac{\frac{N}{\rho R(1-f^*_{m'})}}{\left(1-\frac{N}{\rho R(1-f^*_{m'})}\ln\frac{R(1-f^*_{m'})}{C\Lambda^*}\right)^2}\Lambda_{pm'}} = \tag{24}$$
$$\frac{\left(1-\frac{N}{\rho R(1-f^*_m)}\ln\frac{R(1-f^*_m)}{C\Lambda^*}\right)^2}{\left(1-\frac{N}{\rho R(1-f^*_m)}\ln\frac{R(1-f^*_m)}{C\Lambda^*}+\frac{N}{\rho R(1-f^*_m)}\right)}\left(1-\frac{\rho^2R^2(1-f^*_m)^2e^{-\rho Rf^*_m}\left(1-\frac{N}{\rho R(1-f^*_m)}\ln\frac{R(1-f^*_m)}{C\Lambda^*}\right)}{(1-e^{-\rho Rf^*_m})\,N\left(1-\ln\frac{R(1-f^*_m)}{C\Lambda^*}\right)}\right).$$

Because in the cross-section the left-hand side of (24) is larger for pools with larger Λ_{pm} (its numerator equals Λ_{pm} and denominator is independent of m), to arrive at a contradiction, we only need to show that the RHS of (24) as a function of f^*_m (keeping Λ^* fixed because we are doing a cross-section comparison across pools) is increasing, i.e.,

$$\frac{\partial}{\partial f}\left[\frac{\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}\right)^2}{\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}+\frac{N}{\rho R(1-f)}\right)}\left(1-\frac{\rho^2R^2(1-f)^2e^{-\rho Rf}\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}\right)}{(1-e^{-\rho Rf})\,N\left(1-\ln\frac{R(1-f)}{C\Lambda^*}\right)}\right)\right]>0. \tag{25}$$

This is true because we can prove a set of stronger results:

$$\frac{\partial}{\partial f}\left[\frac{\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}\right)}{\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}+\frac{N}{\rho R(1-f)}\right)}\right]>0, \text{ and} \tag{26}$$
$$\frac{\partial}{\partial f}\left[\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}\right)\left(1-\frac{\rho^2R^2(1-f)^2e^{-\rho Rf}\left(1-\frac{N}{\rho R(1-f)}\ln\frac{R(1-f)}{C\Lambda^*}\right)}{\left(1-e^{-\rho Rf}\right)N\left(1-\ln\frac{R(1-f)}{C\Lambda^*}\right)}\right)\right]>0. \tag{27}$$

To see this, notice that the left-hand side of (26) is

$$\frac{\frac{N}{(1-f)^2\rho R}-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}}{-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}+\frac{N}{(1-f)\rho R}+1}-\frac{\left(\frac{2N}{(1-f)^2\rho R}-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right)\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{\left(-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}+\frac{N}{(1-f)\rho R}+1\right)^2} \tag{28}$$
$$= \frac{N\left(\frac{N}{(1-f)\rho R}-1\right)}{(1-f)^2\rho R\left(-\frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}+\frac{N}{(1-f)\rho R}+1\right)^2}, \tag{29}$$

which is positive when $N>(1-f)\rho R$. This inequality always holds as $N>\rho R$ (Assumption 1).

Meanwhile, the left-hand side of (27) is

$$\left(\frac{(1-f)^2R^3\rho^3e^{f\rho R}\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)^2\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)}-\frac{(1-f)^2\rho^2R^2\left(\frac{N}{(1-f)^2\rho R}-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)}\right.$$
$$\left.+\frac{2(1-f)\rho^2R^2\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)}+\frac{(1-f)\rho^2R^2\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)^2}\right)\times\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)$$
$$+\left(\frac{N}{(1-f)^2\rho R}-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right)\left(1-\frac{(1-f)^2\rho^2R^2\left(1-\frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)}\right), \tag{30}$$

which is equal to

$$\frac{A\left(1-\frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)^2+\left(\frac{N\sqrt{e^{f\rho R}-1}\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}{(1-f)\sqrt{\rho R}}-\frac{(1-f)\sqrt{R^3\rho^3}(N-(1-f)\rho R)\left(1-\frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\sqrt{e^{f\rho R}-1}\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}\right)^2}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}, \tag{31}$$

where

$$A=\frac{(1-f)\rho^2R^2}{N^2\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)^2}\times\left((1-f)N^2\rho R\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)^2+\right.$$
$$\left.N^2\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)+(1-f)^2\rho^2R^2\left(N\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)+N-(1-f)\rho R\right)\left(1-\frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)\right). \tag{32}$$

And $A>0$ when $N>(1-f)\rho R$, which always holds because $N>\rho R$ (Assumption 1).

Notice that

$$1-\frac{N}{\rho R(1-f_m^*)}\ln\frac{R(1-f_m^*)}{C\Lambda^*}>0, \tag{33}$$

because otherwise

$$C\Lambda^*\leq R(1-f_m^*)e^{-\frac{\rho R(1-f_m^*)}{N}}<R(1-f_m^*)e^{-\rho R(1-f_m^*)\frac{\Lambda_{am}^*}{N(\Lambda_{am}^*+\Lambda_{pm})}}\leq C\Lambda^*,$$

which is a contradiction.[35] Then for equilibrium $\{f_m^*\}$, Assumption 1 and (33) imply that the denominator of (31) is also positive. Therefore (31) is positive (and thus (27) is true). □

[35] The last inequality comes from active miners' FOC.

A5. Proof of Proposition 4

Proof. Combine Lemma 1 and Proposition 3. □

A6. Proof of Proposition 5

Proof. From the perspective of an active miner, given fee f_m charged by pool m, the marginal benefit of allocating the first infinitesimal hash rate to this pool can be calculated by setting λ_m and Λ_{am} to zero in $\frac{R(1-f_m)}{\Lambda} e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}$ in Eq. (13), which gives exactly the post-fee risk-neutral valuation,

$$\frac{R(1-f_m)}{\Lambda}. \tag{34}$$

Suppose, counterfactually, that a pool with positive passive hash rates charges zero fee $f_m = 0$; then the risk-neutral valuation $\frac{R}{\Lambda}$ in Eq. (34) must exceed the marginal cost C in any equilibrium with strictly positive active mining. This is because active mining in some pool requires Eq.(13) to hold with equality; then, the fee cost and risk-aversion discount imply that

$$\frac{R}{\Lambda} > \frac{R(1-f_m)}{\Lambda} e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} = C.$$

As a result, this pool will find it strictly optimal to charge a strictly positive fee. In fact, this logic implies that in equilibrium all pools with strictly positive $\Lambda_{pm} > 0$—whether incumbent or entrant—charge strictly positive fees. □

Appendix B. A List of Mining Pool Fee Types

Source: Bitcoin Wiki, edited for grammars.

- CPPSRB: Capped Pay Per Share with Recent Backpay.
- DGM: Double Geometric Method. A hybrid between PPLNS and geometric reward types that enables the operator to absorb some of the variance risk. Operator receives a portion of payout on short rounds and returns it on longer rounds to normalize payments.
- ESMPPS: Equalized Shared Maximum Pay Per Share. Like SMPPS, but equalizes payments fairly among all those who are owed.
- POT: Pay On Target. A high-variance PPS variant that pays on the difficulty of work returned to the pool rather than the difficulty of work served by the pool.
- PPLNS: Pay Per Last N Shares. Similar to proportional, but instead of looking at the number of shares in the round, instead looks at the last N shares, regardless of round boundaries.
- PPLNSG: Pay Per Last N Groups (or shifts). Similar to PPLNS, but shares are grouped into shifts which are paid as a whole.
- PPS: Pay Per Share. Each submitted share is worth a certain amount of BTC. Since finding a block requires current difficulty level of shares on average, a PPS method with 0% fee would be 12.5 BTC divided by current difficulty. It is risky for pool operators, hence the fee is typically the highest.
- PROP: Proportional. When block is found, the reward is distributed among all workers proportionally to how many shares each of them has found.
- RSMPPS: Recent Shared Maximum Pay Per Share. Like SMPPS, but the system aims to prioritize the most recent miners first.
- SCORE: Score based system involves a proportional reward, weighed by time submitted. Each submitted share is worth more in the function of time t since the start of current round. For each share, the score is updated by: score += exp(t/C). This makes later shares worth much more than earlier shares, thus the miners score quickly diminishes when they stop mining on the pool. Rewards are calculated proportionally to scores (and not to shares). (At slushs pool C=300 seconds, and scores are normalized hourly).
- SMPPS: Shared Maximum Pay Per Share. Like Pay Per Share, but never pays more than the pool earns.

Table 4: **Selected Pool Reward Contracts**

Name	**Reward Type**	**Transaction fees**	**Prop. Fee**	**PPS Fee**
AntPool	PPLNS & PPS	kept by pool	0%	2.50%
BTC.com	FPPS	shared	4%	0%
BCMonster.com	PPLNS	shared	0.50%	
Jonny Bravo's	PPLNS	shared	0.50%	
Slush Pool	Score	shared	2%	
BitMinter	PPLNSG	shared	1%	
BTCC Pool	PPS	kept by pool		2.00%
BTCDig	DGM	kept by pool	0%	
btcmp.com	PPS	kept by pool		4%
Eligius	CPPSRB	shared	0%	
F2Pool	PPS	kept by pool		3%
GHash.IO	PPLNS	shared	0%	
Give Me COINS	PPLNS	shared	0%	
KanoPool	PPLNSG	shared	0.90%	
Merge Mining Pool	DGM	shared	1.50%	
Multipool	Score	shared	1.50%	
P2Pool	PPLNS	shared	0%	
MergeMining	PPLNS	shared	1%	

Source: Bitcoin wiki