# From Griefing to Stability in Blockchain Mining Economies

Yun Kuen Cheung[1], Stefanos Leonardos[2], Georgios Piliouras[2], and Shyam Sridhar[2]

[1] *Royal Holloway University of London,* yunkuen.cheung@rhul.ac.uk
[2] *Singapore University of Technology and Design,* {stefanos_leonardos, georgios}@sutd.edu.sg, shyam_sridhar@mymail.sutd.edu.sg



**Abstract**

We study a game-theoretic model of blockchain mining economies and show that *griefing*, a practice according to which participants harm other participants at some lesser cost to themselves, is a prevalent threat at its Nash equilibria. The proof relies on a generalization of evolutionary stability to non-homogeneous populations via *griefing factors* (ratios that measure network losses relative to deviator's own losses) which leads to a formal theoretical argument for the dissipation of resources, consolidation of power and high entry barriers that are currently observed in practice.

A critical assumption in this type of analysis is that miners' decisions have significant influence in aggregate network outcomes (such as network hashrate). However, as networks grow larger, the miner's interaction more closely resembles a distributed production economy or *Fisher market* and its stability properties change. In this case, we derive a *proportional response (PR)* update protocol which converges to market equilibria at which griefing is irrelevant. Convergence holds for a wide range of miners risk profiles and various degrees of resource mobility between blockchains with different mining technologies. Our empirical findings in a case study with four mineable cryptocurrencies suggest that risk diversification, restricted mobility of resources (as enforced by different mining technologies) and network growth, all are contributing factors to the stability of the inherently volatile blockchain ecosystem.

## 1 Introduction

With more than 4000 circulating cryptocurrencies, currently valued above the staggering amount of $1 trillion [46], and countless other decentralized applications running on them [51], the underlying blockchain technologies are attracting increasing attention. However, a (still persisting) barrier in their wider public adoption is the uncertainty regarding their stability and long-term sustainability. Understanding these factors is important both for the success of permissionless blockchains and for the acceptance of cryptocurrencies as a means for widespread monetary transactions [12, 4, 32].

The critical actors for the stability of the blockchain ecosystem are the miners who provide their costly resources (e.g., computational power in Proof of Work (PoW) or units of the native cryptocurrency in Proof of Stake (PoS) protocols) to secure consensus on the growth of the blockchain [33, 9, 5]. Miners act in a self-interested, decentralized manner and may enter or leave these networks at any time. For their service, miners receive monetary rewards in return, typically in the form of transaction fees and newly minted coins of the native cryptocurrency in proportion to their individual resources in the network [33, 14, 17].

The total amount of these resources, their distribution among miners, and the consistency in which they are provided are fundamental factors for the reliability of all blockchain supported applications. However, despite their importance, miners' incentives to allocate and distribute

their resources among various blockchains are yet far from understood. Existing studies [31, 34, 28, 53] and online resources that reflect investor and blockchain related sentiment [42, 54], all provide compelling evidence that the *allocation of mining resources in the blockchain economy* is a still largely under-explored area.

**Model and contribution** Motivated by the above, we study a game-theoretic model of the mining economy (comprising a single or multiple co-existing blockchains) and reason about miners' resource allocations. Our starting point is the work of [3] who derive the unique *Nash Equilibrium* (NE) allocations under the proportional reward scheme that applies to most Proof of Work (PoW) and Proof of Stake (Pos) protocols (Theorem 1). Our first observation is that at the predicted NE levels, active miners are still incentivised to deviate (by increasing their resources) in order to achieve higher *relative payoffs*. While behaving sub-optimally in terms of their absolute payoffs, the loss that a deviating miner incurs to themselves is overcompensated by a larger market share and a higher loss that is incurred to each other individual miner and hence, to the rest of the network as a whole (Theorem 6, Corollary 7).

This practice, in which participants of a network cause harm to other participants, even at some cost to themselves, is known as *griefing*.[1] Our main technical insight is that griefing is closely related to the game-theoretic notion of *evolutionary stability*. Specifically, we quantify the effect of a miner's deviation via the *(individual) Griefing Factors (GF)*, defined as the ratios of network (or individual) losses over the deviator's own losses (Definition 3), and show that an allocation is *evolutionary stable* if and only if all its individual GFs are less than 1 (Lemma 5).[2] We call such allocations *(individually) non-griefable* (Definition 4). This equivalence for homogeneous populations (i.e., for miners having equal mining costs) for which evolutionary stability is defined. However, as GFs are defined for arbitrary populations (not necessarily homogeneous), it provides a way to generalize evolutionary stable allocations as individually non-griefable allocations. Rephrased in this framework, our result states that the NE allocation is always individually griefable by miners who unilaterally increase their resources (Theorem 6).

The previous evolutionary argument provides a theoretical explanation for the increasing dissipation of mining resources (above optimal levels) in PoW protocols and an alternative rationale for the concentration of mining power in few entities that is observed in both PoW and PoS protocols [3, 39, 40]. A distinctive feature of this *over-mining* behavior in comparison to in-protocol adversarial behavior, e.g., [37, 30, 1, 49], is that it does not directly compromise the functionality of the blockchain. When a single miner increases their resources, the safety of the blockchain also increases. However, this practice has multiple negative byproducts as it generates a trend towards market concentration, dissipation of resources and high entry barriers.

With griefing being a concern for instability at the NE allocations (and increased dissipation of resources being a concern at the non-griefable or evolutionary stable allocations (Section 2.3, Proposition 8), it is not immediately clear how to extend this model to study allocation of resources in the general case of multiple co-existing blockchains. A critical observation is that these types of equilibria (both Nash and evolutionary stable) are derived in a model in which individual miners are assumed to influence aggregate market outcomes with their strategic decisions. However, despite the currently observed concentration of mining power, this assumption may not be satisfied in practice as mining networks continue to expand and is certainly not satisfied in the originally envisioned architecture in which (permissionless) mining networks were expected to function in a genuinely decentralized fashion [43]. Thus, the question that naturally

[1] The term *griefing* originated in multiplayer games [55] and was recently introduced in blockchain related settings by [13].

[2] An allocation has a griefing factor of $k$ if a miner can reduce others' payoffs by \$k at a cost of \$1 to themselves by deviating to some other allocation.

arises is whether we can reason about the stability of the ecosystem under the assumption of negligible individual influence.

To address this question, we extend the initial model to the multiple blockchain setting under the assumption that each miner has a finite capacity of resources that is negligible in comparison to collective network levels (large market assumption [21]). Under these conditions griefing becomes irrelevant. The ensuing model is mathematically equivalent to a *Fisher market* (or production economy [10]) in which miners correspond to buyers, goods to revenues from different cryptocurrencies and prices to aggregate allocated resources (Section 3). We endow this model with *quasi-constant elasticity of substitution (quasi-CES)* utilities (parameterized by a miner-specific substitution parameter $\rho_i$) to account for risk diversification and various degrees of resource mobility between different blockchain technologies.

Our main theoretical contribution in this part is the derivation of a *Proportional Response (PR)* protocol that converges to the market equilibria of the model for any quasi-CES utilities with substitution parameters $\rho_i \in [0, 1]$ (Theorem 9). The protocol requires as inputs only local (i.e., miner specific) and collective (total revenues and resources, e.g., estimated hashrate) information which make it particularly suitable for such distributed economies from a practical perspective (Algorithm 1).[3] By contrast, we show that learning protocols that are commonly used in game-theoretic settings, such as Gradient Ascent (GA) and Best Response (BR) dynamics, exhibit chaotic or highly irregular behavior (Section 3.3). This is true even for large number of miners and, in the case of GA, even for relative small step-size (as long as miners are assumed to have influence via non-binding capacities on collective outcomes). Interestingly, these findings establish another source of instability of the equilibria of the game-theoretic model that is different in nature from the previous ones (algorithmic versus incentive driven).

**Case Study:** We use the (PR) dynamics to study the equilibrium allocations of a representative miner in a blockchain economy with four popular cryptocurrencies: Bitcoin, Bitcoin Cash, Ethereum and Litecoin (Section 4). Our empirical results, that are based on empirical data (daily revenues and hashrates over a period of three years), suggest that the *Proportional Profitability Ratio (PPR)*, which is defined as the normalized ratio of revenue over expenses for each coin (Definition 10), is an important metric to understand miner's behavior in the blockchain economy. Specifically, risk neutral miners (equivalently, miners with full mobility of resources) allocate all their resources to the coin with the highest PPR. However, miners with intermediate values of risk neutrality (restricted mobility of resources), distributes their resources precisely in proportion to the PPR of the four available coins (Figure 5). Our findings suggest that restricted mobility of resources (as enforced by the use of different mining technologies in the various blockchains), risk diversification and growth of the mining networks, are all factors that contribute to the stability of the emerging blockchain ecosystem.

**Other Related Works** Our paper main contributes to the growing literature on miners' incentives in blockchain networks. The two derived sources of instabilities, griefing and fluctuating allocations derived by greedy update rules, complement existing results concerning inherent protocol instabilities [8, 15, 25], manipulation of the difficulty adjustment in PoW protocols [31, 34, 44] or adversarial behavior [37, 30, 11, 1]. Our findings in the case of a single blockchain support the accumulating evidence that decentralization is threatened in permissionless blockchains [3, 39, 40] and offer an (evolutionary) explanation for the increased dissipation of resources (above optimal levels) that is observed in the main PoW mining networks [22, 52, 23]. Our market model approach, provides the first (to our knowledge) modeling and equilibrium

[3]While our techniques to derive the (PR) protocol and establish its convergence are based on well-known approaches, the result is novel and may be of independent theoretical interest in the study of exchange [56, 19] or distributed production economies [10].

analysis of the blockchain mining economy as a whole (multiple co-existing blockchains) and contributes to the related literature that is still under early development [50, 7, 53].

Technically, our models mirror the model of single or multiple simultaneous Tullock contests (equivalently all-pay auctions) and the model of Fisher markets with quasi-CES utilities. Thus, some elements of the paper, in particular the notion of griefing factors and the convergence of the PR dynamics, may be of independent interest in the study of general evolutionary, game-theoretic models (in arbitrary non-homogeneous populations) for decentralized markets [41, 26, 36], and in distributed production economies, respectively [56, 18, 27].

**Outline** Section 2 presents the strategic model (in a single blockchain) and studies the notions of griefing and evolutionary stability. Section 3 comprises the market model (with multiple blockchains and negligible individual capacities), the proportional response protocol and a comparison between the two models (Section 3.3). Section 4 contains the empirical results and Section 5 concludes the paper. All proofs of Sections 2 and 3 are deferred to Appendices A and B, respectively.

# 2 Allocation of Mining Resources: Strategic Model

For the first part of our analysis, we will study mining in a single blockchain. We will introduce some additional notation in Section 3, when we will study the allocation of mining resources in multiple blockchains.

## 2.1 Model and Nash Equilibrium Allocations

We consider a network of $N = \{1, 2, \ldots, n\}$ miners who allocate their resources, $x_i \geq 0$, to mine a blockchain-based cryptocurrency. Each miner $i \in N$ has an individual per unit cost $c_i > 0$. For instance, in Proof of Work (PoW) mining, $x_i$ corresponds to TeraHashes per second (TH/s) and $c_i$ to the associated costs (energy, amortized cost of hardware etc.) of producing a TH/s. We will write $\mathbf{x} = (x_i)_{i \in N}$ to denote the vector of allocated resources of all miners, and $X = \sum_{i=1}^{n} x_i$ to denote their sum. We will also write $v$ to denote the total miners' revenue (coinbase transaction reward plus transaction fees) in a fixed time period (typically an epoch or a day in the current paper). The market share of each miner is proportional to their allocated resources (as is the case in most popular cryptocurrencies, see e.g., [43, 13]). Thus, the utility of each miner is equal to

$$u_i\left(x_i, \mathbf{x}_{-i}\right) = \frac{x_i}{x_i + X_{-i}} v - c_i x_i, \qquad \text{for all } i \in N, \tag{1}$$

where, following standard conventions, we write $\mathbf{x}_{-i} = (x_j)_{j \neq i}$ and $X_{-i} := \sum_{j \neq i} x_j$ to denote the vector and the sum, respectively, of the allocated resources of all miners other than $i$. In equation (1), we may normalize $v$ to 1 without loss of generality (by scaling each miner's utility by $v$). We will refer to the game, $\Gamma = (N, (u_i, c_i)_{i \in N})$, defined by the set of miners $N$, the utility functions $u_i, i \in N$ and the cost parameters $c_i, i \in N$ as the *mining game* $\Gamma$. As usual, a *Nash equilibrium* is a vector $\mathbf{x}^*$ of allocations $x_i^*, i \in N$, such that

$$u_i\left(\mathbf{x}^*\right) \geq u_i\left(x_i, \mathbf{x}_{-i}^*\right), \qquad \text{for all } x_i \neq x_i^*, \text{ for all miners } i \in N. \tag{2}$$

In terms of its Nash equilibrium, this game has been analyzed by [3]. To formulate the equilibrium result, let

$$c^* := \frac{1}{n-1} \sum_{i=1}^{n} c_i, \tag{3}$$

and assume for simplicity that $c^* > c_i$ for all $i \in N$. This is a *participation constraint* and implies that we consider only miners that are active in equilibrium. The unique Nash equilibrium of $\Gamma$ is given in Theorem 1.

**Theorem 1** ([3])**.** *At the unique pure strategy Nash equilibrium of the mining game $\Gamma$, miner $i \in N$ allocates resources $x_i^* = (1 - c_i/c^*)/c^*$. In particular, the total mining resources, $X^*$, allocated at equilibrium are equal to $X^* = 1/c^*$.*

Theorem 1 is our starting point. Our first task is to test the robustness of this Nash equilibrium in the context of decentralized and potentially adversarial networks. For instance, while the Nash equilibrium outcome is well-known to be incentive compatible, an adversary may decide to harm others by incurring a low(er) cost to himself. In decentralized networks, the (adversarial) practice of harming others at some lesser own loss is termed *griefing* [13]. As we show next, griefing is indeed possible in this case: a miner who increases their allocated resources above the Nash equilibrium prediction forgoes some of their own profits but incurs a (considerably) larger loss to the rest of the network. Our proof exploits a link between griefing and the fact that the Nash equilibrium is not evolutionary stable. To make these statements explicit, we first provide the relevant framework.

### 2.2 Evolutionary Stable Allocations and Griefing Factors

For this part, we restrict attention to homogeneous populations of miners, for which the notion of *evolutionary stability* is defined. Specifically, we consider a mining game $\Gamma = (N, (u_i, c_i)_{i\in N})$ such that all miners have equal costs, i.e., $c_i = c$ for some $c > 0$, for all $i \in N$. We will write $\Gamma = (N, c, u_{i\in N})$ and we will call this mining game *symmetric*. In this case, $c^* = \frac{n}{n-1}c$ and each miner allocates $x_i^* = \frac{n-1}{n^2 c}$ resources in the unique (symmetric) pure strategy Nash equilibrium of $\Gamma$. The symmetry assumption implies that $u_i(\mathbf{x}) = u_j(\mathbf{x})$ for all $i, j \in N$ and for any allocation $\mathbf{x} = (x_i)_{i\in N}$. The following definition of evolutionary stability due to [47, 35] requires the weaker condition that $u_i(\mathbf{x}) = u_j(\mathbf{x})$ for all $i, j \in N$ and for any *symmetric* allocation $\mathbf{x} = (x_i)_{i\in N}$. In the case of the utility functions in equation (1), these two conditions are equivalent.

**Definition 2** (Evolutionary Stable Allocation (ESA), [47, 35])**.** Let $\Gamma = (N, (u_i, c_i)_{i\in N})$ be a mining game such that $u_i \equiv u_j$ for all $i, j \in N$ for all symmetric allocation profiles $\mathbf{x} \geq 0$. Then, a symmetric vector $\mathbf{x}^{\text{ESA}} = \left(x^{\text{ESA}}\right)_{i\in N}$ is an *evolutionary stable allocation (ESA)* if

$$u_i\left(x_i, \mathbf{x}_{-\mathbf{i}}^{\text{ESA}}\right) < u_j\left(x_i, \mathbf{x}_{-\mathbf{i}}^{\text{ESA}}\right), \quad \text{for all } j \neq i \in N, x_i \neq x^{\text{ESA}}. \tag{4}$$

Definition 2 implies that an ESA, $\mathbf{x}^{\text{ESA}}$, maximizes the relative payoff function, $u_i(x_i, \mathbf{x}_{-\mathbf{i}}^{\text{ESA}}) - u_j(x_i, \mathbf{x}_{-\mathbf{i}}^{\text{ESA}})$ with $j \in N, j \neq i$, of any miner $i \in N$. Intuitively, if all miners select an ESA, then there is no other allocation that could give an individually deviating miner a higher *relative payoff*. In other words, if a symmetric allocation $x_i = x, i \in N$, is not ESA, then there exists a $x' \neq x$, so that a single miner who deviates to $x'$ has a strictly higher payoff (against $x$ of the other $n-1$ miners) than every other miner who allocates x (against $n-2$ other miners who allocate $x$ and the deviator who allocates $x'$) [35].

As mentioned above, evolutionary stability is defined for homogeneous populations and may be, thus, of limited applicability for practical purposes. To study non homogeneous populations, we will need a proper generalization of evolutionary stability. To achieve this, we introduce the notion of *griefing factors* which, as we show, can be used to formulate evolutionary stability and which is readily generalizable to arbitrary settings. This is done next.[4]

[4]In the current setting, the assumption of symmetric miners (miners with equal or at least almost equal cost) is less restrictive than it seems. The participation constraint $c_i < c^* = \frac{1}{n-1}\sum_{j=1}^{n} c_j$ implies that the costs, $c_i$'s, of the active miners in equilibrium cannot be *too different*. This is formalized in Observation 1 in Appendix A.

**Definition 3** (Griefing Factors (GF))**.** Let $\Gamma = (N, (u_i, c_i)_{i\in N})$ be a mining game (not necessarily symmetric) in which all miners are using the allocations $x_i^*, i \in N$, and suppose that a miner $i$ deviates to an allocation $x_i \neq x_i^*$. Then, the *griefing factor, (GF), of strategy $x_i$ with respect to strategy $x^*$* is defined by

$$\mathrm{GF}_i\left(\left(x_i, \mathbf{x}_{-i}^*\right); \mathbf{x}^*\right) := \frac{\text{loss incurred to the network}}{\text{deviator's own loss}} = \frac{\sum_{j\neq i}^{n}\left[u_j\left(\mathbf{x}^*\right) - u_j\left(x_i, \mathbf{x}_{-i}^*\right)\right]}{u_i\left(\mathbf{x}^*\right) - u_i\left(x_i, \mathbf{x}_{-i}^*\right)}, \quad (5)$$

for all $i \in N$, where *loss* is the same as *utility loss*. The GF with respect to an allocation $x^*$ can be then defined as the supremum over all possible deviations, i.e.,

$$\mathrm{GF}\left(\mathbf{x}^*\right) = \sup_{i\in N, x_i\geq 0}\left\{\mathrm{GF}_i\left(\left(x_i, \mathbf{x}_{-i}^*\right); \mathbf{x}^*\right)\right\}.$$

We can also define the *individual griefing factor of strategy $x_i$ with respect to strategy $x^*$ against a specific miner $j$*, as follows

$$\mathrm{GF}_{ij}\left(\left(x_i, \mathbf{x}_{-\mathbf{i}}^*\right); \mathbf{x}^*\right) := \frac{\text{loss incurred to miner } j}{\text{deviator's own loss}} = \frac{u_j\left(\mathbf{x}^*\right) - u_j\left(x_i, \mathbf{x}_{-i}^*\right)}{u_i\left(\mathbf{x}^*\right) - u_i\left(x_i, \mathbf{x}_{-i}^*\right)} \quad (6)$$

for all $j \neq i \in N$, where as in equation (5), *loss* is a shorthand for *utility loss*. It holds that $\mathrm{GF}_i\left(\left(x_i, \mathbf{x}_{-\mathbf{i}}^*\right); \mathbf{x}^*\right) = \sum_{j\neq i}\mathrm{GF}_{ij}\left(\left(x_i, \mathbf{x}_{-\mathbf{i}}^*\right); \mathbf{x}^*\right)$.

As mentioned in Definition 3, the numerator of GF corresponds to the loss of all miners other than $i$ incurred by $i$'s deviation to $x_i$, whereas the denominator corresponds to miner $i$'s own loss (cf. equation (5)). In decentralized mechanisms (e.g., blockchains), this metric captures an important *incentive compatibility* condition: namely, a mechanism is safe against manipulation if the costs of an attack exceed its potential benefits to the attacker [12, 4, 32]. This motivates to define an allocation as *griefable* if its GF is larger than 1.

**Definition 4** (Griefable and Individually Griefable Allocations)**.** An allocation $\mathbf{x}^* = (x_i^*)_{i\in N}$ is *griefable* if $\mathrm{GF}(\mathbf{x}^*) > 1$. An allocation $\mathbf{x}^* = (x_i^*)_{i\in N}$ is *individually griefable* if there exist $i, j \in N$ and $x_i \neq x_i^* \geq 0$, such that the individual griefing factor $\mathrm{GF}_{ij}\left(\left(x_i, \mathbf{x}_{-\mathbf{i}}^*\right); \mathbf{x}^*\right)$ is larger than 1.

An important observation is that the condition of evolutionary stability can be expressed in terms of the individual griefing factors. In particular, an allocation $\mathbf{x}^{\mathrm{ESA}}$ is evolutionary stable if and only if all *individual* griefing factors are less than 1, i.e., if and only if $\mathbf{x}^{\mathrm{ESA}}$ is not individually griefable. This is formalized in Lemma 5.

**Lemma 5.** *Let $\Gamma = (N, c, u_{i\in N})$ be a symmetric mining game. Then, an allocation $\mathbf{x}^{ESA} = \left(x^{ESA}\right)_{i\in N}$ is evolutionary stable if and only if $\mathbf{x}^{ESA}$ is not griefable, i.e., iff*

$$\mathrm{GF}_{ij}\left(\left(x_i, \mathbf{x}_{-\mathbf{i}}^{ESA}\right); \mathbf{x}^{ESA}\right) < 1, \quad \textit{for all } j \neq i \in N, x_i \neq x^{ESA}. \quad (7)$$

*Proof.* Since $u_i \equiv u_j$ for all symmetric $\mathbf{x}$ and all $i, j \in N$ by assumption, we may write equations (4) as

$$u_i\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right) - u_i\left(\mathbf{x}^{\mathrm{ESA}}\right) < u_j\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right) - u_j\left(\mathbf{x}^{\mathrm{ESA}}\right),$$

for all $j \neq i \in N$ and for all $x' \neq x^{\mathrm{ESA}}$. Since $u_i\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right) < u_i\left(\mathbf{x}^{\mathrm{ESA}}\right)$ for all $x \neq x^{\mathrm{ESA}}$ and for any miner $i \in N$, we may rewrite the previous equation as

$$1 > \frac{u_j\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right) - u_j\left(\mathbf{x}^{\mathrm{ESA}}\right)}{u_i\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right) - u_i\left(\mathbf{x}^{\mathrm{ESA}}\right)} = \mathrm{GF}_{ij}\left(\left(x', \mathbf{x}_{-\mathbf{i}}^{\mathrm{ESA}}\right); \mathbf{x}^{\mathrm{ESA}}\right),$$

for all $j \neq i \in N$ and for all $x' \neq x^{\mathrm{ESA}}$. This proves the claim.

Thus, Lemma 5 suggests that an allocation is evolutionary stable if and only if it is individually non-griefable. According to Definition 4, this is weaker than an allocation being non-griefable, which is satisfied if for all $i \in N$, the sum over $j \neq i \in N$ of all individual griefing factors $G_{ij}$ is less than 1.

### 2.3 Griefing in Mining Games

While immediate, Lemma 5 provides a handy way to generalize the notion of evolutionary stability. In particular, in general, non-homogeneous populations, we may impose the stability requirement that an allocation be individually non-griefable or, as mentioned above, the stronger requirement that an allocation be non-griefable. This brings us to the main result of this section, which suggests that the Nash equilibrium of Theorem 1 is griefable for both symmetric and asymmetric populations of miners. In particular, assuming that the network has stabilized at the $x^*$ equilibrium allocation, a strategic miner may attack other miners simply by increasing their own mining resources. Specifically, if a miner $i$ deviates to a resource allocation $x_i^* + \Delta$ for some $\Delta > 0$, then this creates a GF equal to $\mathcal{O}(n/\Delta)$. Such a deviation reduces the attacking miner's own payoff but, as we will see, it decreases the payoff of all other miners by a larger margin. This improves the attacking miner's *relative payoff* and hence their long-term survival chances in the blockchain mining network. This is formalized in Theorem 6. All proofs of Section 2 are presented in Appendix A.

**Theorem 6.** *Let $\Gamma = (N, (u_i, c_i)_{i\in N})$ be a mining game and let $\mathbf{x}^* = (x_i^*)_{i\in N}$ be its unique pure strategy Nash equilibrium.*

*(i) In a homogeneous population, i.e., when all miners have the same cost, $c_i = c > 0$ for all $i \in N$, the unique Nash equilibrium allocation $x^* = \frac{n-1}{n^2 c}$ is not evolutionary stable. In particular, there exists $x' \neq x^*$, so that an individually deviating miner $i$ increases their relative payoff $u_i\left(x', x_{-i}^*\right) - u_j\left(x', x_{-i}^*\right)$.*

*(ii) In a general, non-homogeneous population, the pure Nash equilibrium $x^*$ is griefable. In particular, assuming that all miners $j \in N$ are using their equilibrium allocations $x_j^*, j \in N$, the deviation $x_i^* + \Delta$, for some $\Delta > 0$, of miner $i \in N$, has a griefing factor*

$$\mathrm{GF}_i\left(\left(x_i^* + \Delta, \mathbf{x}_{-i}^*\right); \mathbf{x}^*\right) = \frac{n-1}{\Delta \cdot \sum_{j=1}^n c_j} = \mathcal{O}(n/\Delta).$$

*In particular, at the Nash equilibrium allocation, $x^*$, any single miner may increase their mining resources and improve their utility in relative terms.*

*(iii) In both the homogeneous and non-homogeneous populations, the unique individually non-griefable allocation, $\mathbf{y} = (y_i)_{i\in N}$, satisfies $y_i = \frac{n}{n-1} x_i^*$, where $x_i^*$ is the Nash equilibrium allocation of miner $i \in N$.*

*Remark.* Part (ii) of Theorem 6 reveals one shortcoming of the current definition of GF. Specifically, the GF may grow arbitrarily large as $\Delta \to 0$. However, as $\Delta \to 0$, the *absolute* total harm to the network is negligible (even if the relative loss is very large as expressed by the GF). One possibility to circumvent this problem is to consider discrete increments for $\Delta$, i.e., $\Delta \in \{1, 2, \ldots, 100, \ldots\}$ as in e.g., [17]. Alternatively, one may combine GF with the absolute loss of the network to obtain a more reliable measure. We do not go deeper into this question at the current moment since it seems to be better suited for a standalone discussion. We leave this analysis as an intriguing direction for future work.

*Remark.* Part (iii) of Theorem 6 allows us to reason about the overall expenditure at the unique individually non-griefable allocation $\mathbf{y} = (y_i)_{i\in N}$. In the general case, that of a non-homogeneous population, the total expenditure at an individually non-griefable allocation $\mathbf{y} =$

$(y_i)_{i\in N}$ is

$$E(\mathbf{y}) = \sum_{i\in N} c_i y_i = \frac{n-1}{n}\sum_{i\in N} c_i x_i^* = n\left[1-(n-1)\frac{\sum_i c_i^2}{\left(\sum_i c_i\right)^2}\right],$$

where we used that $x_i^* = (1-c_i/c^*)/c^*$ and $y_i = \frac{n}{n-1}x^*$ by Theorem 1 and part (iii) of Theorem 6, respectively. Cauchy-Schwarz inequality implies that $\left(\sum_i c_i\right)^2 \leq n\sum_i c_i^2$ which yields that $E(y)\leq 1$ with equality if and only if $c_i = c$ for all $i\in N$. Thus, the expenditure in the individually non-griefable allocation is always less than or equal to the aggregate revenue generated by mining, with equality only if the population is homogeneous. In that case, i.e., if all miners have the same cost $c_i = c$ for all $i\in N$, then the unique individually non-griefable allocation is also evolutionary stable (cf. Lemma 5), i.e., $\mathbf{y} = \mathbf{x}^{\text{ESA}}$ with $x^{\text{ESA}} = \frac{1}{nc}$ for all $i\in N$ (by part (iii) and symmetry). In all cases, the total expenditure $E(\mathbf{x}^*)$, at the unique Nash equilibrium $\mathbf{x}^*$ must be equal to $E(\mathbf{x}^*) = \frac{n-1}{n}E(\mathbf{y})$ and hence it less than the expenditure at the unique individually non-griefable allocation and strictly less than the generated revenue (which is equal to 1).

In the proof of Theorem 6, we have actually shown something slightly stronger. Namely, miner $i$'s individual loss due to its own deviation to $x_i^*+\Delta$ is less than the loss of each other miner $j$ provided that $\Delta$ is not too large. In other words, the individual griefing factors with respect to the Nash equilibrium allocation are all larger than 1 and hence, the Nash equilibrium is also individually griefable. This is formalized next.

**Corollary 7.** *For every miner $j\in N$ such that $\Delta < x_j^*$, it holds that $\mathrm{GF}_{ij}\left(\left(x_i^*+\Delta, \mathbf{x}_{-\mathbf{i}}^*\right); \mathbf{x}^*\right) > 1$, i.e., the loss of miner $j$ is larger than the individual loss of miner $i$.*

Theorem 6 and Corollary 7 imply that miners are incentivised to exert higher efforts than the Nash equilibrium predictions. The effect of this strategy is twofold: it increases their own relative market share (hence, their long-term payoffs) and harms other miners. The notable feature of this *over-mining* attack (or deviation from equilibrium) is that it does not undermine the protocol functionality directly. As miners increase their *constructive effort* to, security of the blockchain network also increases. This differentiates the blockchain paradigm from conventional contests in which griefing occurs via exclusively destructive effort or deliberate sabotage against others [38, 2].

However, the over-mining strategy has implicit undesirable effects. As we show next, it leads to consolidation of power by rendering mining unprofitable for miners who would otherwise remain active at the Nash equilibrium and by raising entry barriers for prospective miners. This undermines the (intended) decentralized nature of the blockchain networks and creates long-term risks for its sustainability as a distributed economy. Again, this is a distinctive feature of decentralized, blockchain-based economies: for the security of the blockchain to increase, it is necessary that the aggregate resources *and* their distribution among miners both increase (which is not the case in the over-mining scenario).

**Proposition 8.** *Let $\Gamma = (N, (u_i, c_i)_{i\in N})$ be a mining game with unique Nash equilibrium allocation $\mathbf{x}^* = (x_i^*)_{i\in N}$. Assume that all miners $j\neq i\in N$ are allocating their equilibrium resources $x_j^*$, and that miner $i$ allocates $x_i^*+\Delta$ resources for some $\Delta>0$. Then*

*(i) the maximum increase $\Delta_i$ of miner $i$ before miner $i$'s payoff becomes zero is $\Delta_i = \frac{1}{c_i} - \frac{1}{c^*}$.*

*(ii) the absolute losses of all other miners $j\neq i$ are maximized when $\Delta = \Delta_i$ and are equal to $c_i x_i^*$.*

Proposition 8 quantifies (i) the maximum possible increase, $\Delta_i$, in the mining resources of a single miner before their profits hit the break-even point (i.e., become zero), and (ii) the

absolute losses of all other miners when miner $i$ increases their resources by some $\Delta$ up to $\Delta_i$. As intuitively expected, more efficient miners can cause more harm to the network (part (i)) and in absolute terms, this loss can be up to the equilibrium spending $c_i x_i^*$ of miner $i$, assuming that miner $i$ does not mine at a loss (part (ii)). While not surprising these findings provide a formal argument that cost asymmetries can be severely punished by more efficient miners and that efficient miners can grow in size leading ultimately to a centralized mining network.

# 3 From Oligopoly to Market Equilibria

The previous analysis hinges on an important assumption: namely, that each individual miner has a significant effect on aggregate market outcomes. The utility function in equation (1)

$$u_i\left(x_i, \mathbf{x}_{-i}\right) = \frac{x_i}{X} v - c_i x_i, \qquad \text{for all } i \in N,$$

assumes that the allocation, $x_i$, of miner $i$ affects the aggregate market resources, since $X = x_i + X_{-i}$ (in the denominator of the proportional rewards of each miner $i \in N$). However, in large networks, individual resources are typically (or ideally) negligible in comparison to aggregate resources. With this in mind, the results that we derive with these utility functions can be interpreted as the existence of a positive feedback loop towards centralization: if miners are relative large to the size of the whole economy then, there are intrinsic motives for miners to cause griefing to their peers which leads to further concentration of resources in few miners.

This observation bring us to the next part of our analysis which concerns the study of same problem under the assumption that each miner has an individually insignificant influence on aggregate market outcomes. To study this setting in full generality, i.e., in the presence of multiple co-existing blockchain networks in which the miners may distribute their resources, we first introduce some additional notation.

## 3.1 Additional Notation: Large Market Assumption and Quasi-CES Utilities

As in Section 2.1, let $N = \{1, 2, \ldots, n\}$ denote the set of miners. In addition, let $M = \{1, 2, \ldots, m\}$ denote a set of $m$ mineable cryptocurrencies. Here the word *mineable* refers to various possible mechanisms, such as Proof of Work, Proof of Stake or any other mining mechanism that requires proof (expense) of scarce resources. Let $c_{ik}, i \in N, k \in M$ denote the cost of miner $i$ to allocate one unit of resource in cryptocurrency $k$. Finally, let $v_k$ denote the aggregate revenue generated by cryptocurrency $k \in M$. Typically, $v_k$ refers to the newly minted coins and total transaction fees paid to miners within the study period. In the case of multiple blockchains, miner $i$'s utility in equation (1) can be generalized in a straightforward way to the following *quasi-linear* utility

$$u_i\left(\mathbf{x}_i, \mathbf{x}_{-i}\right) = \sum_{k=1}^{m} \frac{x_{ik}}{x_{ik} + \sum_{j \neq i} x_{jk}} v_k - \sum_{k=1}^{m} c_{ik} x_{ik}. \tag{8}$$

We will write $X_k := \sum_{i \in N} x_{ik}$ to denote the aggregate allocated resources in blockchain $k \in M$. To make comparisons among different cryptocurrencies, it will be convenient to express all allocations in common monetary units that denote *spending* rather than individual (and potential different) physical resources. Accordingly, let $b_{ik} := c_{ik} x_{ik}$ denote the *spending* of miner $i$ for cryptocurrency $k \in M$. A strategy of miner $i$ will be described by a non-negative vector $\mathbf{b}_i = (b_{ik})_{k \in M}$. Using this notation, we can write equation (8) as

$$u_i\left(\mathbf{b}_i, \mathbf{b}_{-i}\right) = \sum_{k=1}^{m} \frac{v_k}{c_{ik} X_k} \cdot c_{ik} x_{ik} - \sum_{k=1}^{m} c_{ik} x_{ik} = \sum_{k=1}^{m} v_{ik} b_{ik} - \sum_{k=1}^{m} b_{ik}, \tag{9}$$

where $v_{ik} := v_k / X_k c_{ik}$ for any $i \in N$ and $k \in M$. Equivalently, if $\bar{c}_k$ is such that $b_k := \bar{c}_k X_k$ is the total spending of the network of cryptocurrency $k$, then $v_{ik} := (v_k/b_k) \cdot (\bar{c}_k/c_{ik})$ for any $i \in N, k \in M$.

The utility function in equation (9) assumes that miners are risk-neutral and that resources can be reallocated effectively in all networks. However, in practice this is not always the case. First, mining is largely an act of investment and as such it is subject to (considerable) risk. Each individual cryptocurrency market is subject to both volatile returns (fluctuations in the $v_{ik}$'s) and uncertainty concerning its future development and success. Thus, it is reasonable for individual miners to hedge their risks by diversifying their resources. Second, mining of a specific cryptocurrency typically requires a commitment in the invested resources (in form of mining equipment or staked capital). While in some cases, mobility of these resources can be assumed to be frictionless between different blockchains (e.g., when they use the same mining algorithm and technology), in general, this is not always the case.

To address these considerations, we introduce (as is standard in economics) *diminishing marginal returns* from the mining revenues of each individual coin. This is captured via concave utility functions of the form $u_i(x) = x^{\rho_i}$, for some $0 < \rho_i \leq 1$, for each miner $i \in N$ which when aggregated, amount to a *quasi Constant Elasticity of Substitution (quasi-CES)* utility function. Using this abstraction, miner $i$'s utility of equation (9) becomes

$$u_i(\mathbf{b}_i, \mathbf{b}_{-i}) = \left( \sum_{k=1}^{m} (v_{ik} b_{ik})^{\rho_i} \right)^{1/\rho_i} - \sum_{k=1}^{m} b_{ik}, \tag{10}$$

Note that for $\rho_i = 1$, we recover the quasi-linear utility of equation (9). The parameters $\rho_i$ can be interpreted both as the risk profile of the miner and the mobility of their resources (depending on whether we view it as utility from consumption or utility from production). For instance, for $\rho_i \to 0$, the utility (10) becomes a Cobb-Douglas utility which corresponds to maximum risk diversification (or equivalently minimal mobility of resources). In the other extreme, $q = 1$ implies that the miner is risk neutral and can freely move their resources to the most profitable (in some correct sense) cryptocurrency. Intermediate values $0 < \rho_i < 1$ yield intermediate risk profiles and degrees of mobility of resources between different blockchains. We further discuss this topic in our case study in Section 4.

Finally, we assume that each miner $i \in N$ has a total monetary capacity, $K_i > 0$, of resources and make the following important assumption. If the total capacity, $K_i$, of each individual miner $i \in N$ is not very large compared to the total allocated resources in each cryptocurrency, $X_k := \sum_{i=1}^{n} x_{ik}$, in each cryptocurrency, then miner $i$ may neglect the effect of her own allocation, $x_{ik}$, in the total mining resources. In other words, each miner $i \in N$ takes the total mining capacity, $X_k$ of each cryptocurrency $k \in M$, as given in her strategic decision making. This implies that $v_{ik}$ does not depend on the decision of miner $i$ (nor on the decision of any other miner $j \in N$) and hence, the utility function in equation (10) is only a function of the $b_i$'s. We will denote the *blockchain mining economy* defined by the utilities in equation (10) with $\Gamma = \big(N, M, (u_i, v_{ik}, \rho_i, K_i)_{i \in N}\big)$.

### 3.2 Proportional Response Dynamics and Equilibrium Allocations

The assumption that each individual miner has negligible influence in aggregate market outcomes has far-reaching implications in the equilibrium analysis of the blockchain mining economy $\Gamma$. Under this assumption, $\Gamma$ can be abstractly seen as a *Fisher market with quasi-CES utilities*. This provides an alternative approach to determine its equilibria via the convex optimization tools that have been developed for the analysis of such markets [24, 6, 20, 19].

Based on this framework, we derive a *Proportional Response (PR)* update rule that converges to the equilibrium of this economy for any selection of the $\rho_i's \in (0, 1]$. Since the utilities in our

case are quasi-CES, we need to adapt existing techniques (which are available only for linear or quasi-linear cases). This is topic of this section which leads to the main result that is stated in Theorem 9. To focus on the interpretation of the results in the blockchain context rather than on the techniques, we defer all proofs to Appendix B. However, we note that the convergence result of the PR dynamics applies to *any* Fisher markets with quasi-CES utilities and may be thus, of independent interest.

To formulate the proportional response dynamics, we first introduce some minimal additional notation. At time step $t \geq 0$, let $u_{ik}(t) := (v_{ik} b_{ik}(t))^{\rho_i}$ and $u_i(t) := \sum_{k=1}^{m} u_{ik}(t)$ denote miner $i$'s utility from cryptocurrency $k$ and aggregate utility (before accounting for expenses), respectively. Let also $w_i(t) := K_i - \sum_{k=1}^{m} b_{ik}(t)$ denote miner $i$'s unspent budget at time $t \geq 0$ and let $\tilde{K}_i(t) := K_i \cdot (K_i - w_i(t))^{\rho_i - 1}$ for each $i \in N$. Then, for the utility function in (10), we define the *Proportional Response (PR) Dynamics* as follows

$$b_{ik}(t+1) := K_i \cdot \frac{u_{ik}(t)}{\max\{u_i(t), \tilde{K}_i(t)\}}. \tag{PR}$$

A pseudocode implementation for the (PR) dynamics is provided in Algorithm 1.

**Algorithm 1** PR-QCES Protocol

**Input (network):** network hashrate, $X_k$, and revenue, $v_k$, of each cryptocurrency $k \in M$.
**Input (miner):** miner $i$'s unit cost, $c_{ik}$, budget capacity, $K_i$, and utility parameter, $\rho_i$.
**Output:** equilibrium spending (allocation) $b_{ik}, k \in M$ for each miner $i \in N$.

**Initialize:** spending (allocation) $b_{ik} > 0$ for all $k \in M$.
**loop**over $t \geq 0$ till convergence
  **for** each miner $i \in N$ **do**
  **procedure** AUXILIARY($(X_k, v_k, c_{ik})_{k \in M}, K_i, \rho_i$)
    $v_{ik} \leftarrow v_k / X_k c_{ik}$
    $w_i \leftarrow K_i - \sum_{k \in M} b_{ik}$ (▷) not invested capital
    $\tilde{K}_i \leftarrow K_i (K_i - w_i)^{\rho_i - 1}$
    $u_{ik} \leftarrow (v_{ik} b_{ik})^{\rho_i}$ and $u_i \leftarrow \sum_{k \in M} u_{ik}$ (▷) utilities before subtracting costs
  **procedure** PR-DYNAMICS($(u_{ik})_{k \in M}, u_i, K_i, \tilde{K}_i$)
    **if** $u_i > \tilde{K}_i$ **then**
      $b_{ik} \leftarrow u_{ik} K_i / u_i$
    **else**
      $b_{ik} \leftarrow u_{ik} K_i / \tilde{K}_i$
  $X_k \leftarrow \sum_{j \in N} b_{jk}$ (▷) update network hashrate and repeat

An important feature of the PR update rule is that it has low informational requirements. It uses as inputs only observable information at network level (aggregate revenue and hashrate) and local information at a miner's level (individual capacity and mining cost). Thus, it provides a protocol that is both feasible to implement in practice and relevant for this particular type of large, distributed economics.

Intuitively, the update rule PR suggests the following. If the revenue of miner $i$ is high enough at round $t$, i.e., if $u_i \geq \tilde{K}_i$, then miner $i$ will reallocate all their resources in round $t+1$ in proportion to the generated revenues, $u_{ik}/u_i$, in round $t$. By contrast, if $u_i < \tilde{K}_i$, then miner $i$ will behave cautiously and allocate only a fraction of their resources. This fraction is precisely equal to the generated revenue at round $t$, i.e., $u_i(t)$ again in proportion to the revenue generated by each cryptocurrency $k \in M$. The important property of the PR dynamics is that they converge to the set of equilibrium allocations for any initial strictly positive allocation vector. This is statement of Theorem 9 which is our main theoretical result.

**Theorem 9** (Mining Resources Equilibrium Allocation)**.** *For any positive initial allocation,* $\mathbf{b}^0 > 0$*, the* (PR)*-dynamics converge to the set of equilibrium allocations,* $\mathbf{b}^*$*, of the blockchain mining economy* $\Gamma$*.*

Theorem 9 will be our main tool to study equilibria in the blockchain mining economy. Before we proceed with our empirical results in Section 4, a comparison between the oligopoly model of Section 2.3 and the market model of Section 3 is due.

### 3.3 Comparing the two Models: Nash vs Market equilibria

When comparing the two models that we considered thus far, the oligopoly model in Section 2.3 and the market model in Section 3, we make the following two main observations.

**Bounded versus Unbounded Capacities** The first observation concerns the capacities of individual miners and the influence that they have on aggregate outcomes. In the former case, that of the oligopoly model, miners are assumed to have large capacities of resources which if used strategically, affect the welfare of other miners. This generates adversarial incentives that lead to griefing and destabilize the Nash equilibrium outcome. At the unique evolutionary stable equilibrium, griefing is not possible, however, at that equilibrium, miners fully dissipate the reward and cause further consolidation of power that raises entry barriers to prospective entrants. Thus, the system enters a positive feedback loop towards market concentration.

By contrast, in the latter case, that of the market model, miners are assumed to have individually negligible resources in comparison to aggregate market levels. Moreover, the comparison of instances with few large miners to instances with many small miners, necessitates the introduction of capacity limits to the model. Thus, miners cannot arbitrarily increase their allocated resources to harm others (and benefit themselves in relative terms). This renders griefing irrelevant and is the decisive factor that ultimately leads to stabilization (see [45] for a related argument). One may argue that the oligopoly model is closer to what we observe in practice, whereas the market model is the ideal model that was envisioned in the paper by Nakamoto that sparked the interest in the blockchain-based economies [43].

**Equilibrium versus Learning Dynamics** The second observation concerns the discrepancy between the static approach in the oligopoly model and the dynamic approach in the market model. The question that naturally arises is whether typical learning dynamics converge to the equilibrium of the oligopoly model. The answer to this question is negative and highlights the necessity of the market assumption (individually negligible resource capacities) to obtain a stable update rule that converges to equilibrium.

To see this, we consider two greedy update rules, *Gradient Ascent* and *Best Response* dynamics that are frequently used in such strategic interactions. Recall that the utility of miner $i$ in the strategic (single blockchain) model is given by

$$u_i\left(x_i, X_{-i}\right) = \frac{x_i}{x_1 + X_{-i}} - c_i x_i, \text{ for all } x_i \geq 0$$

and $i = 1, 2, \ldots, n$, where $X_{-i} = \sum_{j \neq i} x_j$ (cf. equation (1)). Thus, the *Gradient Ascent (GA)* update rule is given by

$$x_i^{t+1} = x_i^t + \theta_i \frac{\partial}{\partial x_i^t} u_i\left(x_i^t\right) = x_i^t + \theta_i \left[\frac{X_{-i}^t}{\left(x_1^t + X_{-i}^t\right)^2} - c_i\right], \tag{GA}$$

for all $i = 1, 2, \ldots, n$, where $\theta_i$ is the learning rate of miner $i = 1, 2$. The bifurcation diagrams in Figure 1 show the attractor of the dynamics for different values of the step-size (assumed here

to be equal for all miners for expositional purposes) and for different numbers of active miners, $n = 2, 5$ and 10, with $c_i = 1$ for all $i$. The blue dots show the aggregate allocated resources for 400 iterations after a burn-in period of 50 iterations (to ensure that the dynamics have reached the attractor).

All three plots indicate that the GA dynamics transition from convergence to chaos for relative small values of the step-size. Interestingly, as the number of miners increases, the instabilities emerge for increasingly smaller step-size. This is in sharp contrast to the (PR) dynamics and their convergence to equilibrium under the large market assumption. The reason that a growing number of miners does not convey stability to the system is precisely because the miners are not assumed to have binding capacities. As miners act greedily, their joint actions drive the system to extreme fluctuations and the larger their number, the easier it is for these fluctuations to emerge. Finally, while convergence is theoretically established for small step-sizes in all cases, such step-sizes correspond to very slow adaption and are of lesser practical relevance.

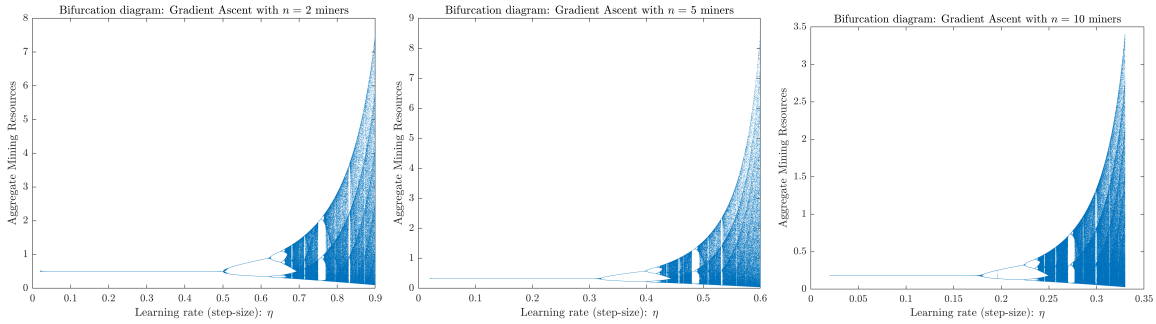



Figure 1: Bifurcation diagrams for the Gradient Ascent dynamics with $n = 2, 5, 10$ miners with respect to the learning parameter $\theta$. As the number of miners grows, the dynamics become chaotic for even lower step-sizes.

We obtain a qualitatively similar result for the best response dynamics. The *Best Response (BR)* update rule is given by

$$x_i^{t+1} = \sqrt{X_{-i}^t / c_i} - X_{-i}^t, \quad \text{for all } i = 1, 2, \ldots, n. \tag{BR}$$

As above, the bifurcation diagrams in Figure 2 show the aggregate allocated mining resources for $n = 2, 5$ and 10 miners. The horizontal axis (i.e., the bifurcation parameter) is now the cost asymmetry between the representative miner and all other miners which are assumed to have the same cost (again only for expositional purposes). The plots suggest that the stability of the dynamics critically depend on the parameters of the system with chaos emerging for various configurations.

In sum, the above results indicate the importance of the large market assumption, i.e., that miners' individual allocations do not affect aggregate network levels, in the stability of the blockchain ecosystem. As showcased by the GA and BR dynamics, if miners' decisions affect the decisions of other miners and if miners can adjust (increase or decrease) their capacities to optimize their profits, then common learning dynamics can exhibit arbitrary behavior. Instead of converging to the Nash equilibrium (or to some other stable outcome), the aggregate allocations may oscillate between extreme values or exhibit chaotic trajectories, with adverse effects on the reliability of the supported applications and the value of the blockchain-based cryptocurrency. Along with our earlier findings about griefing, these results paint a more complete picture about the various reasons that can destabilize permissionless blockchain networks when there is concentration of mining power.

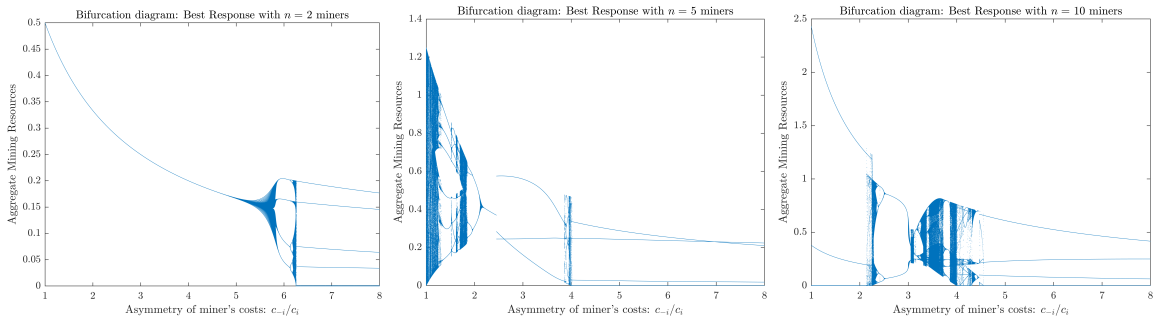



Figure 2: Bifurcation diagrams for the Best Response dynamics with $n = 2, 5, 10$ miners with respect to the miners cost asymmetry. The dynamics become chaotic typically for intermediate values of cost asymmetry.

# 4 Case Study: Allocation of Mining Resources in the Wild

Due to its low informational requirements, the PR protocol allows us to reduce the degrees of freedom that accompany synthetic data (such as estimates about the numbers of active miners, their individual capacities, mining costs etc.), and adopt a "single miner's" perspective against real data when we study equilibrium allocations in the actual blockchain mining economy. Since the PR protocol converges to the equilibrium allocations for a wide range of quasi-CES utilities (as defined by parameters $\rho_i \in (0, 1]$), we can reason about the effects of risk diversification and resource mobility on miners' equilibrium allocations. This allows us to extend existing results [53, 44].

## 4.1 Data Set and Experimental Setting

We apply the above theoretical framework in the following case study in which we consider four Proof of Work blockchains (cryptocurrencies): Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH) and Litecoin (LTC). Our data set consists of the total daily network hashrate in Tera-Hashes per second (TH/s) and the aggregate daily miners' revenue in USD (newly minted coins and transaction fees) the for the four selected cryptocurrencies in the period between 1/1/2018 and 10/18/2020. The data are visualized in Figures 3 and 4.

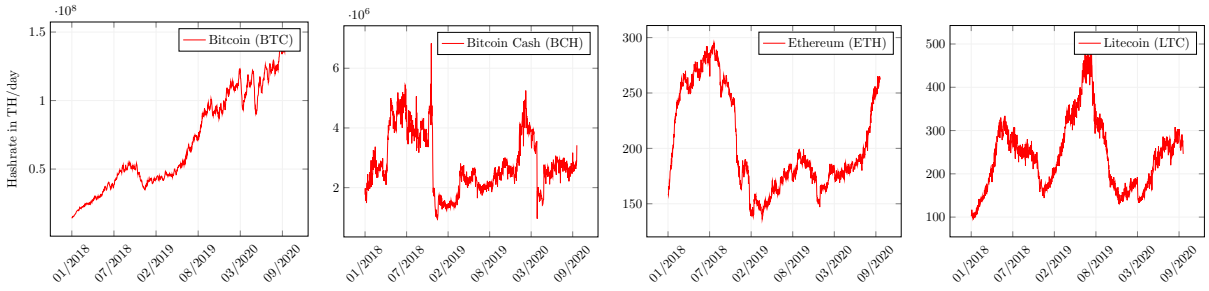



Figure 3: Daily estimated hashrate (measured in TeraHashes per day (TH/day)) in the four cryptocurrencies: Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH) and Litecoin (LTC). Source: glassnode.com.

To apply the PR-QCES protocol, we need to derive an estimation for the cost of a representative miner to produce one unit of resource, i.e., one TH/s for a whole day, in each network. This is done as follows. For each cryptocurrency, we collect data regarding the state of the art (or most popular) mining equipment for each calendar year in the considered time period. The data (and their sources) are presented in Table 1.

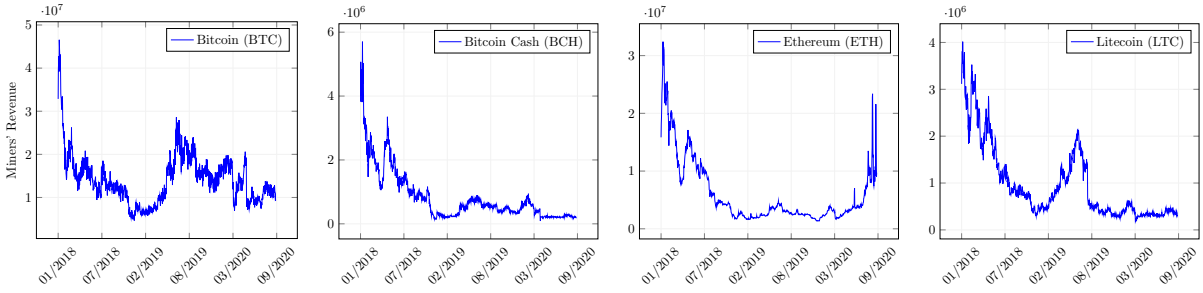



Figure 4: Daily miners' revenue (aggregate value in USD of newly minted coins and transaction fees) in the four cryptocurrencies: Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH) and Litecoin (LTC). Source: glassnode.com.

| | **Year** | **Model** | **Price** ($P$) | **Hashrate** ($H_s$) | **Power** ($W$) |
|---|---|---|---|---|---|
| Bitcoin/ | 2018 | Ebang Ebit E11+ | \$2,494 | 37 TH/s | 2035W |
| Bitcoin | 2019 | Antminer s17 | \$2,100 | 56 TH/s | 2520W |
| Cash | 2020 | Antminer s19 Pro | \$2,507 | 110 TH/s | 3250W |
| | 2018 | PandaMiner B5+ | \$2,916 | 110 MH/s | 800W |
| Ethereum | 2019 | PandaMiner B7 | \$2,035 | 230 MH/s | 1150W |
| | 2020 | PandaMiner B9 | \$3,280 | 330 MH/s | 950W |
| | 2018 | Moonlander 2 L3++ | \$65 | 5 MH/s | 10W |
| Litecoin | 2019 | FutureBit Apollo LTC | \$500 | 120 MH/s | 200W |
| | 2020 | Antminer s19 Pro | \$300 | 580 MH/s | 1200W |

Table 1: Mining equipment. The selected models correspond to the state of the art or most popular mining rigs for each cryptocurrency. The lifespan, $L_s$, of all model is assumed to be 2 years. Sources: (asicminervalue.com) for Bitcoin and Bitcoin Cash, (pandaminer.com) for Ethereum, and (exodus.io) for Litecoin.

The hardest part in the data collection process is the estimation of a single average value for the average network cost per kWh. According to [22, 23] prices per kWh follow a seasonal trend (due to weather dependent fluctuations, e.g., in China) and a constant to slightly decreasing overall trend between 2018 and 2020. The exact values that we used in the experiments are in Table 2. However, as argued by the referenced papers, these estimates should be accepted with caution.

Using the above figures, the cost, $c$, to produce one TH/s for a whole day is given by the following formula

$$c = \frac{P}{365 \cdot L_s \cdot H_s} + \frac{(W/1000) \cdot c(kWh) \cdot 24}{H_s},$$

where, as in Tables 1 and 2, $P$ denotes the acquisition price of the model in USD, $L_s$ the useful lifespan (assumed to be 2 years for all models), $H_s$ the effective hashrate of the model (in TH/s), $W$ its power consumption (in Watt) and $c(kWh)$ the average cost per kWh in USD.

The above estimations provide the necessary inputs to run the PR-QCES protocol (cf. Inputs in Algorithm 1) for a single miner with cost $c$ per kWh and obtain their equilibrium allocations given the network hashrates and aggregate revenue for each coin. Throughout, we assume that the miner has a fixed capacity, $K_i$, which is a small percentage of the aggregate mining resources in all networks. Different values of $K_i$ yield the same equilibrium allocations and are hence not presented here. In each experiment, we use a different parameter, $\rho_i$, in the quasi-CES utility of miner $i$. This allows us to reason about the effects of a miner's risk profile or under a different

| Average price per kWh ($c(kWh)$) | | | | | |
|---|---|---|---|---|---|
| 01-06/2018 | 07-12/2018 | 01-06/2019 | 07-12/2019 | 01-06/2020 | 07-12/2020 |
| \$0.06 | \$0.05 | \$0.04 | \$0.05 | \$0.03 | \$0.02 |

Table 2: Average prices per kWh. The figures are updated every six months (i.e., 01-06 and 07-12 in each year) and concern a global estimated average. They are mainly based on [22, 23]. Scattered online resources offer similar estimates but we refrain from recommending these figures as precise. As cautioned by the referenced papers, there are several practical reasons for which these figures may have limited accuracy, e.g., different bargains achieved by individual (large) miners, lack of transparency in the exact energy source (renewable or electricity), spatial and seasonal fluctuations in prices (even within the same country as in the USA or China) etc. In the context of the current empirical study, the exact trend and values of electricity prices do not affect the interpretation of the results.

interpretation, of the degree of mobility of their resources, against real data.

### 4.2 Empirical Results

Our results are summarized in Figure 5. Each row of Figure 5 corresponds to a different parameter $\rho_i$ and each panel corresponds to each of the four considered coins: Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH) and Litecoin (LTC). In each panel, the blue dotted lines depict the equilibrium allocations of the miner for each day (derived by running the PR-QCES dynamics) for that coin and the red lines depict the *proportional profitability ratio* of the coin which turns out to play an important role in the interpretation of the results. Formally, the proportional profitability ratio of a coin is defined as follows.

**Definition 10** (Profitability and Proportional Profitability Ratios)**.** Let $v_k$ denote the aggregate network revenue and $b_k$ the aggregate network spending (e.g., hashrate times cost to produce this hashrate) for mining cryptocurrency $k = 1, 2, \ldots, n$ in a specific time period (e.g., one day). The *profitability ratio*, $(PFR_k)$, of cryptocurrency $k$ is defined by

$$PFR_k := \frac{\text{total network revenue from mining coin } k}{\text{total network spending for mining coin } k} = \frac{v_k}{b_k}\,. \tag{11}$$

The *proportional profitability ratio*, $(PPR_k)$, of cryptocurrency $k$ is defined as the ratio of $PFR_k$ over the sum of the $PFR_k$'s of all considered cryptocurrencies, i.e.,

$$PPR_k := \frac{PFR_k}{\sum_{j=1}^{n} PFR_j} = \frac{v_k/b_k}{\sum_{j\in M} v_j/b_j}\,. \tag{12}$$

We this definition at hand, we return to the interpretation of the results in Figure 5. The first row shows the equilibrium allocations of a risk averse miner with $\rho_i = 0.01$. Such a miner essentially ignores the input data and distributes (approximately) evenly their resources among the available coins (for $\rho_i = 0$, the distribution would be exactly uniform, i.e., 1/4 for each coin). The second row shows the equilibrium allocations of a miner with $\rho_i = 0.5$. This value of parameter $\rho_i$ suggests that the miner is still willing to diversify their risks, albeit to a lesser extent. From a production perspective, $\rho_i = 0.5$ implies an intermediate degree in the mobility of resources. Such a degree may be viewed as realistic in practical applications since there exist some blockchains that use compatible technology (e.g., Bitcoin and Bitcoin Cash) and certain mining models which are easily switchable between different mining algorithms. Interestingly, this case reveals the empirical finding that the a miner with parameter $\rho_i = 0.5$ allocates their resources precisely according to the $PPR_k$ of each coin $k = 1, 2, 3, 4$ (cf. Definition 10). Thus,

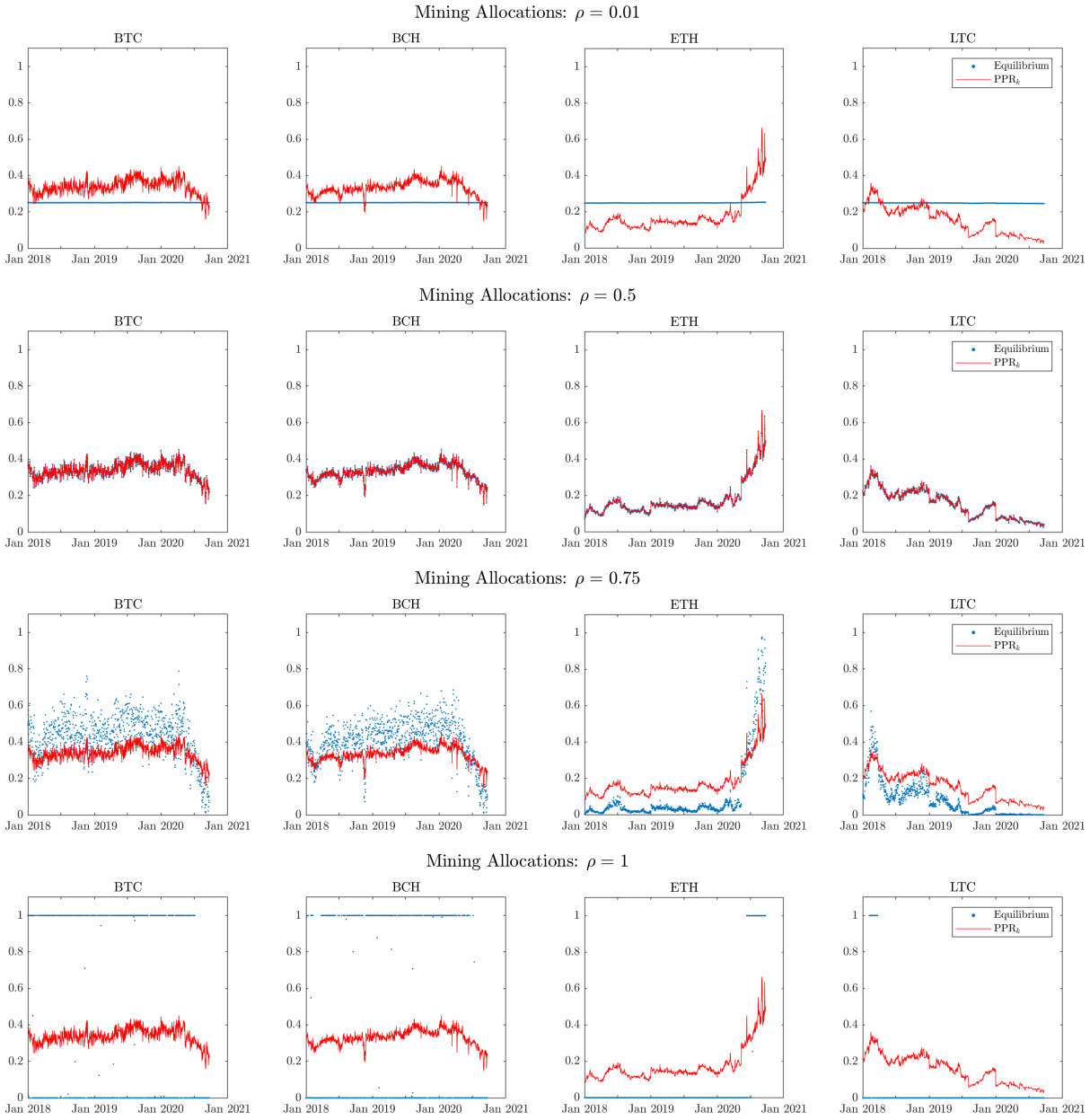



Figure 5: Equilibrium allocations (blue dotted lines) and proportional profitability ratios ($PPR_k$'s) (red lines) for the four coins of the case study. Each row corresponds to a different parameter $\rho_i$ of the miner's quasi-CES utility. When $\rho_i = 0.01$, the miner distributes equally their resources among the available networks (risk aversion). For $\rho_i = 0.5$, the equilibrium allocations exactly match the $PPR_k$'s (cf. Definition 10). For $\rho = 1$, which corresponds to risk neutrality (with full mobility of resources), the miner allocates all their resources to the cryptocurrency with the highest $PPR_k$.

such a miner can fully determine their allocations from observable network data (aggregate revenues and hashrate) and local information (their own mining cost and capacity).

The importance of the $PPR_k$ is further highlighted in the last row of the matrix which shows the equilibrium allocations for a risk neutral miner with $\rho_i = 1$. Such a miner allocates on each day (or period) the entirety of their resources to the cryptocurrency with the highest $PPR_k$. This approach is consistent with full or instant mobility of resources and can be, thus, observed in practice only between cryptocurrencies that use the same mining technology such as Bitcoin

and Bitcoin Cash. From a modeling perspective, it highlights the importance of considering quasi-CES utilities instead of quasi-linear utilities in the case of multiple co-existing blockchains. From an analytical perspective, it also highlights how the use of different mining technologies by different blockchains conveys stability to the blockchain ecosystem as a whole by acting as a barrier in arbitrary reallocations of resources. Finally, the fourth row includes an intermediate case with $\rho_i = 0.75$.

# 5 Conclusions

In this paper, we studied resource allocation in blockchain mining networks. We identified two very different reasons for instabilities in the mining networks when mining power is consolidated in few miners: griefing (which generalizes the notion of evolutionary stability to non-homogeneous populations) and instability of dynamic allocation rules (such as gradient ascent or best response). Along with existing in-protocol attacks, such as selfish mining or manipulation of the difficulty adjustment in Proof of Work blockchains ([33, 30, 14] and [31, 34, 44]), these results paint a more complete picture of the inherent instabilities of these decentralized networks in practice. By contrast, under a large market assumption, which can be met in practice as more miners enter the blockchain ecosystem, we show that these problems disappear and we establish convergence of a natural proportional response protocol to non-griefable market equilibria. The protocol has low informational requirements which make it suitable for such decentralized settings and converges to the market equilibria for a wide range of miners' risk diversification and various degrees of resource mobility between different blockchain networks. Our theoretical and empirical results suggest that decentralization, risk diversification among different blockchains and restricted mobility of resources (as enforced by the use of different mining technologies among different blockchains) are all factors that contribute to the stabilization of this otherwise volatile and unpredictable ecosystem.

# Acknowledgments

This research is supported in part by NRF2019-NRF-ANR095 ALIAS grant, grant PIE-SGP-AI-2018-01, NRF 2018 Fellowship NRF-NRFF2018-07, AME Programmatic Fund (Grant No. A20H6b0151) from the Agency for Science, Technology and Research (A*STAR) and the National Research Foundation, Singapore under its AI Singapore Program (AISG Award No: AISG2-RP-2020-016).

# References

[1] C. Alkalay-Houlihan and N. Shah. The Pure Price of Anarchy of Pool Block Withholding Attacks in Bitcoin Mining. *AAAI Conference on Artificial Intelligence, AAAI-19*, 33(1), 2019.

[2] J.A. Amegashie. Productive versus destructive efforts in contests. *European Journal of Political Economy*, 28(4):461–468, 2012.

[3] N. Arnosti and S. M. Weinberg. Bitcoin: A Natural Oligopoly. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124, pages 5:1–5:1, 2018.

[4] R. Auer. Beyond the Doomsday Economics of Proof-of-Work in Cryptocurrencies. Discussion Paper DP13506, London, Centre for Economic Policy Research, February 2019.

[5] I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies without proof of work. In Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, editors, *Financial Cryptography and Data Security*, pages 142–157, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[6] B. Birnbaum, N. R. Devanur, and L. Xiao. Distributed Algorithms via Gradient Descent for Fisher Markets. In *EC'11*, pages 127–136. ACM, 2011.

[7] G. Bissias, B. N. Levine, and D. Thibodeau. Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium, 2019.

[8] J. Bonneau. Why Buy When You Can Rent? Financial Cryptography and Data Security, pages 19–26, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[9] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy, pages 104–121, 2015.

[10] S. Brânzei, R. Mehta, and N. Nisan. Universal Growth in Production Economies. In *NeurIPS 2018*, volume 31, pages 1973–1973, 2018.

[11] J. Brown-Cohen, A. Narayanan, A. Psomas, and S. M. Weinberg. Formal Barriers to Longest-Chain Proof-of-Stake Protocols. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, EC '19, page 459–473, New York, NY, USA, 2019. ACM.

[12] E. Budish. The Economic Limits of Bitcoin and the Blockchain. Working Paper 24717, National Bureau of Economic Research, June 2018.

[13] V. Buterin. A griefing factor analysis model, 2018. ethresear.ch [Online; accessed: 11-February-2021].

[14] V. Buterin, D. Reijsbergen, S. Leonardos, and G. Piliouras. Incentives in ethereum's hybrid casper protocol. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 236–244. IEEE, USA, May 2019.

[15] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan. On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 154–167. ACM, 2016.

[16] G. Chen and M. Teboulle. Convergence Analysis of a Proximal-Like Minimization Algorithm Using Bregman Functions. *SIAM J. Optim.*, 3(3):538–543, 1993.

[17] X. Chen, C. Papadimitriou, and T. Roughgarden. An Axiomatic Approach to Block Rewards. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, AFT '19, pages 124–131, New York, NY, USA, 2019. ACM.

[18] Y. K. Cheung, R. Cole, and N. R. Devanur. Tatonnement beyond gross substitutes? Gradient descent to the rescue. *Games and Economic Behavior*, 123:295–326, 2020.

[19] Y. K. Cheung, R. Cole, and Y. Tao. Dynamics of Distributed Updating in Fisher Markets. In *EC'18*, pages 351–368, New York, NY, USA, 2018. ACM.

[20] R. Cole, N. R. Devanur, V. Gkatzelis, K. Jain, T. Mai, V. V. Vazirani, and S. Yazdanbod. Convex Program Duality, Fisher Markets, and Nash Social Welfare. In *EC'17*, pages 459–460, 2017.

[21] R. Cole and Y. Tao. Large Market Games with Near Optimal Efficiency. In *EC'16*, pages 791–808, New York, NY, USA, 2016. ACM.

[22] A. De Vries. Bitcoin's Growing Energy Problem. *Joule*, 2(5):801–805, 2018.

[23] A. De Vries. Bitcoin's energy consumption is underestimated: A market dynamics approach. *Energy Research & Social Science*, 70:101721, 2020.

[24] N. R. Devanur. Fisher Markets and Convex Programs. Unpublished manuscript, 2009.

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

[26] D. DiPalantino and M. Vojnovic. Crowdsourcing and All-Pay Auctions. In *EC '09*, pages 119–128, 2009.

[27] K. Dvijotham, Y. Rabani, and L. J. Schulman. Convergence of incentive-driven dynamics in Fisher markets. *Games and Economic Behavior*, 2020.

[28] D. Easley, M. O'Hara, and S. Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109, 2019.

[29] E. Eisenberg and D. Gale. Consensus of Subjective Probabilities: The Pari-Mutuel Method. *Ann. Math. Statist.*, 30(1):165–168, 1959.

[30] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Commun. ACM*, 61(7):95–102, 2018.

[31] A. Fiat, A. Karlin, E. Koutsoupias, and C. Papadimitriou. Energy Equilibria in Proof-of-Work Mining. In *EC'19*, pages 489–502, New York, NY, USA, 2019. ACM.

[32] N Gandal and J. Gans. More (or Less) Economic Limits of the Blockchain. Discussion Paper DP14154, London, Centre for Economic Policy Research, November 2019.

[33] J. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[34] G. Goren and A. Spiegelman. Mind the Mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, EC '19, pages 475–487, New York, NY, USA, 2019. ACM.

[35] B. Hehenkamp, W. Leininger, and A. Possajennikov. Evolutionary equilibrium in Tullock contests: spite and overdissipation. *European Journal of Political Economy*, 20(4):1045–1057, 2004.

[36] J. J. Horton and L. B. Chilton. The Labor Economics of Paid Crowdsourcing. In *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pages 209–218, 2010.

[37] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. Blockchain Mining Games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, page 365–382, New York, NY, USA, 2016. ACM.

[38] K. A. Konrad. Sabotage in Rent-Seeking Contests. *Journal of Law, Economics, & Organization*, 16(1):155–165, 2000.

[39] Y. Kwon, J. Liu, M. Kim, D. Song, and Y. Kim. Impossibility of Full Decentralization in Permissionless Blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, AFT '19, pages 110–123, New York, NY, USA, 2019. Association for Computing Machinery.

[40] N. Leonardos, S. Leonardos, and G. Piliouras. Oceanic Games: Centralization Risks and Incentives in Blockchain Mining. In P. Pardalos, I. Kotsireas, Y. Guo, and W. Knottenbelt, editors, *Mathematical Research for Blockchain Economy*, pages 183–199, Cham, 2020. Springer International Publishing.

[41] D. Levin, K. LaCurts, N. Spring, and B. Bhattacharjee. Bittorrent is an Auction: Analyzing and Improving Bittorrent's Incentives. *SIGCOMM Comput. Commun. Rev.*, 38(4):243–254, 2008.

[42] M. Shen. Crypto Investors Have Ignored Three Straight 51% Attacks on ETC, 2020. coindesk.com [Online; accessed 11-February-2021].

[43] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [Accessed: 31-08-2020].

[44] S. Noda, K. Okumura, and Y. Hashimoto. An Economic Analysis of Difficulty Adjustment Algorithms in Proof-of-Work Blockchain Systems. In *Proceedings of the 21st ACM Conference on Economics and Computation*, EC '20, page 611, New York, NY, USA, 2020. Association for Computing Machinery.

[45] T. Puu. On the stability of Cournot equilibrium when the number of competitors increases. *Journal of Economic Behavior & Organization*, 66(3):445–456, 2008.

[46] Reuters Staff. Crypto market cap surges above $1 trillion for first time, 2021. reuters.com [Online; accessed 11-February-2021].

[47] Mark E. Schaffer. Evolutionarily stable strategies for a finite population and a variable contest size. *Journal of Theoretical Biology*, 132(4):469–478, 1988.

[48] V. I. Shmyrev. An algorithm for finding equilibrium in the linear exchange model with fixed budgets. *Journal of Applied and Industrial Mathematics*, 3(4):505, Dec 2009.

[49] R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng. A game theoretic analysis of resource mining in blockchain. *Cluster Computing*, 23(3):2035–2046, Sep 2020.

[50] A. Spiegelman, I. Keidar, and M. Tennenholtz. Game of Coins, 2018.

[51] State of the Dapps. Explore Decentralized Applications, 2021. stateofthedapps.com [Online; accessed 11-February-2021].

[52] C. Stoll, L. Klaaßen, and U. Gallersdörfer. The Carbon Footprint of Bitcoin. *Joule*, 3(7):1647–1661, 2019.

[53] J. Sun, P. Tang, and Y. Zeng. Games of Miners. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems*, AAMAS '20, pages 1323–1331, Richland, SC, 2020. International Foundation for Autonomous Agents and Multiagent Systems.

[54] Wave Financial LLC. Ethereum 2.0 staking, a worthwhile investment?, 2021. cityam.com [Online; accessed 11-February-2021].

[55] Wikipedia contributors. Griefer — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Griefer&oldid=1006081077, 2021. [Online; accessed 11-February-2021].

[56] L. Zhang. Proportional response dynamics in the Fisher market. *Theoretical Computer Science*, 412(24):2691–2698, 2011. Selected Papers from 36th International Colloquium on Automata, Languages and Programming (ICALP 2009).

# A Omitted Proofs and Materials from Section 2.3

**Observation 1.** *Let* $c_{\max} := \max_{i \in N} \{c_i\}$ *denote the maximum mining cost among all active miners and let* $\bar{c} = \frac{1}{n} \sum_{i=1}^{n} c_i$ *denote the average mining cost. Then, the variance* $\sigma_c^2 := \sum_{i=1}^{n} (c_i - \bar{c})$ *of the per unit mining costs of all active miners in equilibrium satisfies*

$$\sigma_c^2 < c_{\max} \left( \frac{n}{n-1} - c_{\max} \right).$$

*Proof.* Since $c_i < 1$ for all $i \in N$ (recall that this equivalent to $c_i < v$ prior to normalization which is naturally satisfied), it holds that $\sum_{i=1}^{n} c_i^2 < \sum_{i=1}^{n} c_i$. Along with the definition of $c^*$,

cf. (3), this yields

$$\sigma_c^2 = \frac{1}{n-1}\sum_{i=1}^{n}(c_i-\bar{c})^2 = \frac{1}{n-1}\sum_{i=1}^{n}c_i^2 - \frac{1}{n(n-1)}\left(\sum_{i=1}^{n}c_i\right)^2$$
$$\leq \frac{1}{n-1}\sum_{i=1}^{n}c_i - \frac{n-1}{n}\left(\frac{1}{n-1}\sum_{i=1}^{n}c_i\right)^2 = c^*\left(1-\frac{n-1}{n}c^*\right).$$

The participation constraint, $c_i < c^*$ for all $i \in N$, implies, in particular, that $c_{\max} < c^*$. Moreover, $c^* = \frac{1}{n-1}\sum_{i=1}^{n} c_i < \frac{n}{n-1}c_{\max}$. Substituting these in the last expression of the above inequality, we obtain that

$$\sigma_c^2 < c^*\left(1-\frac{n-1}{n}c^*\right) < \frac{n}{n-1}c_{\max}\left(1-\frac{n-1}{n}c_{\max}\right) = c_{\max}\left(\frac{n}{n-1}-c_{\max}\right).$$

To gain some intuition about the order of magnitude of the bound derived in Observation 1 in real applications, we consider the BTC network. Currently, the cost to produce 1 TH/s consistently for a whole day is approximately equal to \$0.08. On the other hand, the total miners' revenue per day is in the order of magnitude of \$10million. Thus, in normalized units (as the ones that we work here), $c_i$ would be equal to $c_i = 0.08/10m = \$8e-09$.

*Proof of Theorem 6.* Part (i). For $\Delta < x^*$, Corollary 7 implies that

$$u_j(x^*) - u_j\left(x^*+\Delta, x^*_{-i}\right) > u_i(x^*) - u_i\left(x^*_i+\Delta, x^*_{-i}\right).$$

Since $u_i(x^*) = u_j(x^*)$ for all $i,j \in N$ by the symmetry assumption, $c_i = c > 0$ for all $i \in N$, it follows that $u_i\left(x^*_i+\Delta, x^*_{-i}\right) - u_j\left(x^*+\Delta, x^*_{-i}\right) > 0$ as claimed.
Part (ii). The own loss of miner $i$ by deviating to allocation $x^*_i+\Delta$ when all other miners use their equilibrium allocations $x^*_{-i}$ is equal to

$$u_i(\mathbf{x}^*) - u_i\left(x^*_i+\Delta, \mathbf{x}^*_{-i}\right) = \frac{x_i*}{X^*} - c_i x^*_i - \left[\frac{x^*_i+\Delta}{X^*+\Delta} - c_i\left(x^*_i+\Delta\right)\right] = \Delta\left[c_i - \frac{X^*_{-i}}{X^*\left(X^*+\Delta\right)}\right].$$

By Theorem 1, $X^* = 1/c^*$, and $x^*_i = \left(1-c_i/c^*\right)/c^*$, which implies that $X^*_{-i} = X^* - x^*_i = c_i/\left(c^*\right)^2$. Substituting in the right hand side of the above equality yields

$$u_i(\mathbf{x}^*) - u_i\left(x^*_i+\Delta, \mathbf{x}^*_{-i}\right) = \Delta\left[c_i - \frac{c_i/\left(c^*\right)^2}{\left(1/c^*+\Delta\right)/c^*}\right] = \frac{\Delta^2 c_i c^*}{1+c^*\Delta}. \tag{13}$$

Similarly, the loss incurred to any miner $j \neq i$ by miner $i$'s deviation is equal to

$$u_j(\mathbf{x}^*) - u_j\left(x^*_i+\Delta, \mathbf{x}^*_{-i}\right) = \frac{x^*_j}{X^*} - c_j x^*_j - \left[\frac{x^*_j}{X^*+\Delta} - c_j x^*_j\right] = \frac{x^*_j\Delta}{X^*\left(X^*+\Delta\right)}$$
$$= \frac{1}{c^*}\left(1-\frac{c_j}{c^*}\right)\cdot\frac{\Delta}{\left(1/c^*+\Delta\right)/c^*} = \frac{\Delta\left(c^*-c_j\right)}{1+c^*\Delta}. \tag{14}$$

Since $c_j < c^*$ for all miners $j \in N$, the last expression is always positive (i.e., all miners incur a strictly positive loss). Summing over all $j \in N$ with $j \neq i$, equation (14) yields

$$\sum_{j\neq i}^{n}\left[u_j(\mathbf{x}^*) - u_j\left(x^*_i+\Delta, \mathbf{x}^*_{-i}\right)\right] = \frac{\Delta}{1+c^*\Delta}\left[(n-1)c^* - \sum_{j\neq i}c_j\right]$$
$$= \frac{\Delta}{1+c^*\Delta}\left[(n-1)c^* - \sum_{j=1}^{n}c_j + c_i\right] = \frac{\Delta c_i}{1+c^*\Delta}, \tag{15}$$

where the last equality holds by definition of $c^*$, cf. (3). Combining equations (13) and (15), we obtain

$$\mathrm{GF}\left(\mathbf{x}^*; \left(x_i^* + \Delta, \mathbf{x}_{-i}^*\right)\right) = \left(\frac{\Delta c_i}{1 + c^*\Delta}\right) \Big/ \left(\frac{\Delta^2 c_i c^*}{1 + c^*\Delta}\right) = \frac{1}{c^*\Delta},$$

which concludes the proof of part (ii).
Part (iii). For an allocation $\mathbf{y} = (y_i)_{i \in N}$ to be individually non-griefable it must hold that

$$u_j(\mathbf{y}) - u_j(y_i + \Delta, \mathbf{y}_{-i}) < u_i(\mathbf{y}) - u_i(y_i + \Delta, \mathbf{y}_{-i}),$$

for all $i, j \in N$ with $i \neq j$ and for all $\Delta > 0$. This yields the inequality (cf. equation (14) in the proof of part (ii))

$$\frac{y_j \Delta}{Y(Y + \Delta)} < \Delta \left[c_i - \frac{Y - y_i}{Y(Y + \Delta)}\right], \quad \text{for each } i, j \in N, \Delta > 0,$$

which after some trivial algebra can be equivalently written as

$$c_i (Y + \Delta) Y > Y + y_j - y_i, \quad \text{for each } i, j \in N, \Delta > 0.$$

Since the left hand side is increasing in $\Delta$ and since the above must hold for each $\Delta > 0$, it suffices to prove the inequality for $\Delta = 0$ in which case it must hold with equality. This gives the condition

$$c_i Y^2 = Y + y_j - y_i, \quad \text{for each } i, j \in N,$$

which can be now solved for the individually non-griefable allocation $\mathbf{y} = (y_i)_{i \in N}$. Summing over $j \neq i \in N$ yields

$$(n-1) c_i Y^2 = (n-1) Y + Y - y_i - (n-1) y_i, \quad \text{for each } i \in N,$$

or equivalently

$$y_i = Y \left[1 - \frac{n-1}{n} c_i Y\right], \quad \text{for each } i \in N. \tag{16}$$

Summing equation (16) over all $i$ yields

$$Y = Y \left[n - \frac{n-1}{n} Y \sum_{i \in N} c_i\right]$$

which we can solve for $Y$ to obtain that $Y = \frac{n}{\sum_{i \in N} c_i}$. Using the notation of equation (3), this can be written as

$$Y = \frac{n}{n-1} \cdot \frac{n-1}{\sum_{i \in N} c_i} = \frac{n}{n-1} \cdot \frac{1}{c^*}.$$

Substituting back in equation (16) yields the unique allocations $y_i$

$$y_i = \frac{n}{(n-1)c^*} \left[1 - \frac{(n-1)c_i}{n} \frac{n}{(n-1)c^*}\right] = \frac{n}{n-1} \left(1 - c_i/c^*\right)/c^* = \frac{n}{n-1} x_i^*,$$

where $x_i^* = \left(1 - c_i/c^*\right)/c^*$ is the Nash equilibrium allocation for each $i \in N$ (cf. Theorem 1). This concludes the proof of part (iii).

*Proof of Corollary 7.* By equations (13) and (14), the inequality

$$u_j(\mathbf{x}^*) - u_j\left(x_i^* + \Delta, \mathbf{x}_{-i}^*\right) > u_i(\mathbf{x}^*) - u_i\left(x_i^* + \Delta, \mathbf{x}_{-i}^*\right)$$

is equivalent to

$$\frac{\Delta (c^* - c_j)}{1 + c^*\Delta} > \frac{\Delta^2 c_i c^*}{1 + c^*\Delta} \iff c^* - c_j > \Delta c_i c^*$$

$$\iff \Delta < \frac{1}{c_i}\left(1 - \frac{c_j}{c^*}\right).$$

Since $c_i < c^*$ by assumption, and $x_j^* = \frac{1}{c^*}\left(1 - \frac{c_j}{c^*}\right)$ by Theorem 1, the right hand side of the last inequality satisfies

$$\frac{1}{c_i}\left(1 - \frac{c_j}{c^*}\right) > \frac{1}{c^*}\left(1 - \frac{c_j}{c^*}\right) = x_j^*.$$

This implies that $\Delta < x_j^*$ is sufficient for the initial inequality to hold which concludes the proof.

*Proof of Proposition 8.* Part (i). Let $\Delta_i > 0$ be such that $u_j\left(x_i^* + \Delta_1, \mathbf{x}_{-i}^*\right) = 0$. Then

$$\begin{aligned} u_j\left(x_i^* + \Delta_1, \mathbf{x}_{-i}^*\right) = 0 &\implies \frac{x_j^*}{X^* + \Delta_1} - c_j x_j^* = 0 \\ &\implies \frac{1}{X^* + \Delta_1} = c_j \\ &\implies \Delta_1 = \frac{v}{c_j} - X^* \end{aligned}$$

Since $X^* = \frac{1}{c^*}$ by Theorem 1, it follows that

$$\Delta_i = \frac{(c^* - c_i)}{(c_i c^*)} = \frac{1}{c_i} - \frac{1}{c^*}. \tag{17}$$

The previous equation implies in particular that $\Delta_i < \Delta_j$ if and only if $c_i > c_j$ for any $i \neq j \in N$. Part (ii). From equation (15) in the proof of Theorem 6, we know that the absolute losses, $L(\Delta)$, of the network when miner $i$ deviates to $x_i^* + \Delta$ are equal to

$$L(\Delta) = \sum_{j \neq i}^{n} u_j(x^*) - u_j\left(x_i^* + \Delta, \mathbf{x}_{-i}^*\right) = \frac{\Delta c_i}{1 + c^* \Delta}.$$

Taking the derivative of the right hand side expression with respect to $\Delta$, we find that

$$\frac{\partial}{\partial \Delta} L(\Delta) = \frac{\partial}{\partial \Delta} \frac{\Delta c_i}{1 + c^* \Delta} = \frac{c_i}{(1 + c^* \Delta)^2} > 0.$$

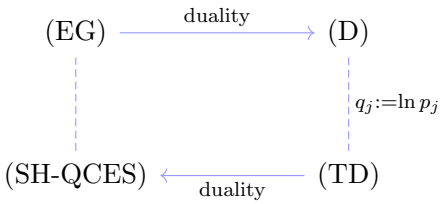
This implies that the absolute losses of the network are increasing in $\Delta$. Thus, for $\Delta \in (0, \Delta_i]$, they are maximized at $\Delta = \Delta_i$ where they are equal to

$$L(\Delta_i) = \frac{\left(\frac{1}{c_i} - \frac{1}{c^*}\right) c_i}{1 + c^*\left(\frac{1}{c_i} - \frac{1}{c^*}\right)} = c_i \cdot (1 - c_i/c^*)/c^* = c_i x_i^*,$$

where the last equality follows from Theorem 1.

# B Omitted Proofs from Section 3: Proportional Response Dynamics with Quasi-CES Utilities

Our proof of Theorem 9 consists of two parts. The first involves the derivation of a convex program that captures the market equilibrium (ME) spending of quasi-CES Fisher markets. To obtain this part, we utilize the approach of [6, 20, 19]. The second concerns the derivation of a general Mirror Descent (MD) algorithm which converges to the optimal solution of this convex program. Then, the last step is to show that the PR-QCES is an instantiation of this MD algorithm which concludes the proof.




| Program | Description | Variables |
|---|---|---|
| (EG) | Eisenberg-Gale | $x_{ij}$ = allocations $i \in N, j \in M$ |
| (D) | Dual | $p_j$ = prices $j \in M$ |
| (TD) | Transformed dual | $q_j = \ln(p_j)$ $j \in M$ |
| (SH-QCES) | Shmyrev-type | $b_{ij}$ = spending $i \in N, j \in M$ |

Figure 6: Convex programs in the derivation of the PR-QCES protocol via the Mirror Descent (MD) protocol. Starting from the dual (D) of a generalized Eisenberg-Gale convex program (EG), we go to the transformed dual (TD) and by convex duality to a Shmyrev-type primal program (SH-QCES) which is hence, equivalent to the initial program (EG). The objective function of (SH-QCES) for quasi-CES utilities is 1-Bregman convex which implies convergence of the MD protocol.

**Convex Program Framework.** The convex optimization framework that we use to capture the ME spendings in quasi-CES FM is summarized in Figure 6. Our starting point is a convex program proposed by [24] that captures ME prices of quasi-linear (a sub-case of quasi-CES) Fisher markets which belongs to type (D) in Figure 6 [29]. From this, we derive a new convex program with captures the ME spending of the market which belongs to type (SH) [48]. After obtaining this new convex program, we follow the approach of [19] to modify it so that it captures the ME spending of a quasi-CES FM. The convex program is

$$\begin{aligned} \min_{\mathbf{b},\mathbf{w},\mathbf{p}} \quad F(\mathbf{b},\mathbf{w},\mathbf{p}) \quad \text{s.t.} \quad & \sum_{i=1}^{n} b_{ij} = p_j, && \forall j \in M, \\ & \sum_{j=1}^{m} b_{ij} + w_i = K_i, && \forall i \in N, \\ & b_{ij}, w_i \geq 0, && \forall i \in N, j \in M, \end{aligned} \tag{SH-QCES}$$

where $F(\mathbf{b},\mathbf{w},\mathbf{p})$ is the following function:

$$F(\mathbf{b},\mathbf{w},\mathbf{p}) := -\sum_{i=1}^{n} \frac{1}{\rho_i} \sum_{j=1}^{m} b_{ij} \ln[v_{ij}(b_{ij})^{\rho_i - 1}] + \sum_{j=1}^{m} p_j \ln p_j + \sum_{i=1}^{n} \left[ w_i + \frac{\rho_i - 1}{\rho_i} \cdot (K_i - w_i) \ln(K_i - w_i) \right].$$

Recall that $b_{ij}$ is the spending of agent $i$ on good $j$, $p_j := \sum_i b_{ij}$, and $w_i$ is the amount of budget/capital of agent $i$ left not spent/invested. We start by showing that the solutions of (SH-QCES) are solutions to our initial problem, i.e., to find the market equilibrium spending.

**Lemma 11.** *Each minimum point of* (SH-QCES) *corresponds to a market equilibrium spending.*

*Proof.* We verify that the optimality condition of the convex program is the same as the market equilibrium condition.

**Optimality Condition.** The partial derivatives of $F$ are

$$\begin{aligned} \frac{\partial}{\partial b_{ij}} F(b,w) &= \frac{1}{\rho_i} \left( 1 - \ln \frac{v_{ij}(b_{ij})^{\rho_i - 1}}{(p_j)^{\rho_i}} \right) = \frac{1}{\rho_i} (1 - \ln v_{ij}) + \frac{1 - \rho_i}{\rho_i} \cdot \ln b_{ij} + \ln p_j \\ \frac{\partial}{\partial w_i} F(b,w) &= \frac{1}{\rho_i} \left[ 1 - (\rho_i - 1) \ln(K_i - w_i) \right]. \end{aligned}$$

Since $(1 - \rho_i)/\rho_i > 0$, $\lim_{b_{ij} \searrow 0} \frac{1-\rho_i}{\rho_i} \cdot \ln b_{ij} = -\infty$. Hence, at each minimum point, $b_{ij}$ must be strictly positive. In turn, since $b_{ij}$ is in the relative interior of the domain at each minimum point, and we have the constraint $\sum_{j=1}^{m} b_{ij} \leq K_i$, it must hold that all $\frac{\partial}{\partial b_{ij}} F(b,w)$ are identical for all $j$, for each buyer $i$. Equivalently, $\frac{v_{ij}(b_{ij})^{\rho_i - 1}}{(p_j)^{\rho_i}}$ are identical for all $j$. Moreover,

- if $K_i > w_i > 0$, then $\frac{\partial}{\partial b_{ij}} F(b, w) = \frac{\partial}{\partial w_i} F(b, w)$, i.e., $\frac{v_{ij}(b_{ij})^{\rho_i - 1}}{(p_j)^{\rho_i}} = (K_i - w_i)^{\rho_i - 1}$ for all $j$;
- if $w_i = 0$, then $\frac{\partial}{\partial b_{ij}} F(b, w) \leq \frac{\partial}{\partial w_i} F(b, w)$, i.e., $\frac{v_{ij}(b_{ij})^{\rho_i - 1}}{(p_j)^{\rho_i}} \geq (K_i - w_i)^{\rho_i - 1}$ for all $j$.

**Market Equilibrium Condition.** We are interested in the rate the utility changes w.r.t. changes in spending on good $j$. Since prices are considered as independent signals in market, the rate is $\frac{1}{p_j} \cdot \frac{\partial}{\partial x_{ij}} u_i(x_i; p) = \left( \sum_{j=1}^{m} v_{ij}(x_{ij})^{\rho_i} \right)^{1/\rho_i - 1} \cdot \frac{v_{ij}(x_{ij})^{\rho_i - 1}}{p_j} - 1$. Since $\rho_i - 1 < 0$ and, hence, $\lim_{x_{ij} \searrow 0} (x_{ij})^{\rho_i - 1} = +\infty$, at the market equilibrium, $x_{ij}$ must be strictly positive, and hence $b_{ij}$ too.

Thus, at the market equilibrium, each $b_{ij}$ is in the relative interior of the domain, and we have the constraint $\sum_j b_{ij} \leq K_i$, it must be the case that $\frac{1}{p_j} \cdot \frac{\partial}{\partial x_{ij}} u_i(x_i; p)$ are identical for all $j$. Thus,

$$\frac{v_{ij}(x_{ij})^{\rho_i - 1}}{p_j} = \frac{v_{ij}(b_{ij})^{\rho_i - 1}}{(p_j)^{\rho_i}}$$

are identical for all $j$. We denote this (common) value by $z_i$. Then

$$\begin{aligned} \frac{1}{p_j} \cdot \frac{\partial}{\partial x_{ij}} u_i(x_i; p) &= \left( \sum_{j=1}^{m} z_i x_{ij} p_j \right)^{1/\rho_i - 1} \cdot z_i - 1 \\ &= (z_i)^{1/\rho_i} \left( \sum_{j=1}^{m} b_{ij} \right)^{1/\rho_i - 1} - 1 \\ &= (z_i)^{1/\rho_i} (K_i - w_i)^{1/\rho_i - 1} - 1. \end{aligned}$$

There are two cases:

- If $K_i > w_i > 0$, which means $w_i$ is in the relative interior of its domain too, then the above derivative has to be zero, i.e., $z_i = (K_i - w_i)^{\rho_i - 1}$ for all $i$;
- If $w_i = 0$, then the above derivative at market equilibrium is positive or zero, i.e., $z_i \geq (K_i - w_i)^{\rho_i - 1}$ for all $i$.

**From Mirror Descent to Proportional Response.** A useful observation in (SH-QCES) is that the first and second constraints determine the values of $p_j, w_i$ in terms of $b_{ij}$'s. Thus, we may rewrite $F(\mathbf{b}, \mathbf{w}, \mathbf{p})$ as a function of $\mathbf{b}$ only. Then the convex program has variables $\mathbf{b}$ only, and the only constraints on $\mathbf{b}$ are $b_{ij} \geq 0$ and $\sum_{j=1}^{m} b_{ij} \leq K_i$.

After deriving the convex program with variables $\mathbf{b}$ only, we can compute a ME spending by using standard optimization method like Mirror Descent (MD). To begin, we introduce some additional notation and recap a general result about MD [16, 6] below.

Let $C$ be a compact and convex set. The *Bregman divergence* generated by a convex regularizer function $h$ is denoted by $d_h$, defined as: for any $\mathbf{b} \in C, \mathbf{a} \in \mathsf{rint}(C)$ where $\mathsf{rint}(C)$ is the relative interior of $C$,

$$d_h(\mathbf{b}, \mathbf{a}) := h(\mathbf{b}) - [h(\mathbf{a}) + \langle \nabla h(\mathbf{a}), \mathbf{b} - \mathbf{a} \rangle] .$$

Due to convexity of the function $h$, $d_h(\mathbf{b}, \mathbf{a})$ is convex in $\mathbf{b}$, and its value is always non-negative. The *Kullback-Leibler divergence* (KL-divergence) between $\mathbf{b}$ and $\mathbf{a}$ is $\mathrm{KL}(\mathbf{b} \| \mathbf{a}) :=$

$\sum_j b_j \cdot \ln \frac{b_j}{a_j} - \sum_j b_j + \sum_j a_j$, which is same as the Bregman divergence $d_h$ with regularizer $h(\mathbf{b}) := \sum_j (b_j \cdot \ln b_j - b_j)$. For the problem of minimizing a convex function $f(\mathbf{b})$ subject to $\mathbf{b} \in C$, the Mirror Descent (MD) method w.r.t. Bregman divergence $d_h$ is given by the update rule in Algorithm 2.

**Algorithm 2** MD w.r.t. Bregman-divergence $d_h$

1: **procedure** MIRRORDESCENT($f, C, \Gamma, d_h$)
2: **Initialize:** $\mathbf{b}^\circ \in C$
3: **while** $t > 0, \mathbf{b}^t, \mathbf{b} \in C$ **do**
4: $g\left(\mathbf{b}, \mathbf{b}^t\right) \leftarrow \left\langle \nabla f(\mathbf{b}^t), \mathbf{b} - \mathbf{b}^t \right\rangle + d_h(\mathbf{b}, \mathbf{b}^t)/\Gamma$
5: $\mathbf{b}^{t+1} \leftarrow \arg\min_{\mathbf{b} \in C} \{ g\left(\mathbf{b}, \mathbf{b}^t\right) \}$

In the MD update rule, $1/\Gamma > 0$ is the step-size, which may vary with $t$ (and typically diminishes with $t$). However, in the current application of distributed dynamics, time-varying step-size and thus, update rule is *undesirable* or even *impracticable*, since this will require from the agents/firms to keep track with a global clock.

A function $f$ is *L-Bregman convex* w.r.t. Bregman divergence $d_h$ if for any $\mathbf{b} \in C$ and $\mathbf{a} \in \mathsf{rint}(C)$, $f(\mathbf{a}) + \langle \nabla f(\mathbf{a}), \mathbf{b} - \mathbf{a} \rangle \leq f(\mathbf{b}) \leq f(\mathbf{a}) + \langle \nabla f(\mathbf{a}), \mathbf{b} - \mathbf{a} \rangle + L \cdot d_h(\mathbf{b}, \mathbf{a})$.

**Theorem 12.** *Suppose $f$ is an $L$-Bregman convex function w.r.t. Bregman divergence $d_h$, and $\mathbf{b}^T$ is the point reached after $T$ applications of the mirror descent update rule in Algorithm 2 with parameter $\Gamma = 1/L$. Then*

$$f(\mathbf{b}^T) - f(\mathbf{b}^*) \;\leq\; L \cdot d(\mathbf{b}^*, \mathbf{b}^0)/T.$$

Using the above, we can now show that the objective function of the (SH-QCES) is a 1-Bregman convex function w.r.t. the KL-divergence (Lemma 13). Subsequently, we show that PR-QCES can be *derived* from Algorithm 2 with a suitable choice of $\Gamma$. Then, Theorem 12 guarantees that the updates of PR-QCES converge to an optimal solution of the convex program (SH-QCES) and Theorem 9 follows.

**Lemma 13.** *The objective function $F$ of* (SH-QCES) *is a* 1*-Bregman convex function w.r.t. the divergence $\sum_{i=1}^n \frac{1}{\rho_i} \cdot \mathrm{KL}(x_i' || x_i)$.*

To prove Lemma 13, we need the following technical result.

**Lemma 14.** *Let $d = (d_i)_{i=1}^N$, $d' = (d_i')_{i=1}^N$ be two vectors with non-negative entries, and let $e = (e_{11}, \ldots, e_{1M_1}, \ldots, e_{N1}, \ldots, e_{NM_N})$, $e' = (e'_{11}, \ldots, e'_{1M_1}, \ldots, e'_{N1}, \ldots, e'_{NM_N})$ be two vectors with non-negative entries, such that for each $1 \leq i \leq N$, $\sum_{k=1}^{M_i} e_{ik} = d_i$ and $\sum_{k=1}^{M_i} e'_{ik} = d_i'$. Then $\mathrm{KL}(d' \| d) \leq \mathrm{KL}(e' \| e)$.*

*Proof.* Note that $g(q, r) = q \ln(q/r)$ is a a convex function in $q, r$ when $q, r > 0$. Thus,

$$\begin{aligned}
\mathrm{KL}(d' \| d) &= \sum_{i=1}^N \left( d_i' \ln \frac{d_i'}{d_i} - d_i' + d_i \right) \\
&= \sum_{i=1}^N M_i \cdot g\left( \frac{1}{M_i} \sum_{k=1}^{M_i} e'_{ik}, \frac{1}{M_i} \sum_{k=1}^{M_i} e_{ik} \right) - \sum_{i=1}^N \sum_{k=1}^{M_i} e'_{ik} + \sum_{i=1}^N \sum_{k=1}^{M_i} e_{ik} \\
&\leq \sum_{i=1}^N M_i \cdot \frac{1}{M_i} \sum_{k=1}^{M_i} g\left(e'_{ik}, e_{ik}\right) - \sum_{i=1}^N \sum_{k=1}^{M_i} e'_{ik} + \sum_{i=1}^N \sum_{k=1}^{M_i} e_{ik}
\end{aligned}$$

$$= \sum_{i=1}^{N}\sum_{k=1}^{M_i} e'_{ik} \ln \frac{e'_{ik}}{e_{ik}} - \sum_{i=1}^{N}\sum_{k=1}^{M_i} e'_{ik} + \sum_{i=1}^{N}\sum_{k=1}^{M_i} e_{ik}$$
$$= \mathrm{KL}(e' \| e),$$

where the inequality follows from the convexity of $g$.

We can now prove Lemma 13. For convenience, we will use the notation $\mathbf{z} := (\mathbf{b}, \mathbf{w}, \mathbf{p})$ and

$$d_F\left(\mathbf{z}', \mathbf{z}\right) := F(\mathbf{b}', \mathbf{w}', \mathbf{p}') - F(\mathbf{b}, \mathbf{w}, \mathbf{p}) - \left\langle \nabla F(\mathbf{b}, \mathbf{w}, \mathbf{p}), (\mathbf{b}' - \mathbf{b}, \mathbf{w}' - \mathbf{w}, \mathbf{p}' - \mathbf{p}) \right\rangle$$

*Proof of Lemma 13.* We begin with the following calculations:

$$\begin{aligned}
d_F\left(\mathbf{z}', \mathbf{z}\right) = &- \sum_{i=1}^{n} \frac{1}{\rho_i} \sum_{j=1}^{m} \left( b'_{ij} \ln[v_{ij}(b'_{ij})^{\rho_i - 1}] - b_{ij} \ln[v_{ij}(b_{ij})^{\rho_i - 1}] \right) + \sum_{j=1}^{m} \left( p'_j \ln p'_j - p_j \ln p_j \right) \\
&+ \sum_{i=1}^{n} \left[ (w'_i - w_i) + \frac{\rho_i - 1}{\rho_i} \cdot \left[ (K_i - w'_i) \cdot \ln(K_i - w'_i) - (K_i - w_i) \ln(K_i - w_i) \right] \right] \\
&- \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{(b'_{ij} - b_{ij})}{\rho_i} \left( 1 - \ln[v_{ij}(b_{ij})^{\rho_i - 1}] + \rho_i \ln p_j \right) \\
&- \sum_{i=1}^{n} \frac{(w'_i - w_i)}{\rho_i} \left( 1 - (\rho_i - 1) \cdot \ln(K_i - w_i) \right) \qquad (18) \\
= &- \sum_{i=1}^{n} \frac{\rho_i - 1}{\rho_i} \sum_{j=1}^{m} b'_{ij} \ln \frac{b'_{ij}}{b_{ij}} + \sum_{j=1}^{m} p'_j \ln \frac{p'_j}{p_j} - \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{1}{\rho_i} \cdot (b'_{ij} - b_{ij}) \\
&+ \sum_{i=1}^{n} \left[ \frac{\rho_i - 1}{\rho_i} (w'_i - w_i) \frac{\rho_i - 1}{\rho_i} \cdot (K_i - w'_i) \ln \frac{K_i - w'_i}{K_i - w_i} \right]. \qquad (19)
\end{aligned}$$

Let $q_i = K_i - w_i$ and $q'_i = K_i - w'_i$. Then (19) can be rewritten as

$$\sum_{i=1}^{n} \frac{\rho_i - 1}{\rho_i} \cdot \left( q'_i \ln \frac{q'_i}{q_i} - q'_i + q_i \right),$$

which equals to $\sum_{i=1}^{n} \frac{\rho_i - 1}{\rho_i} \cdot \mathrm{KL}(q'_i \| q_i)$. Recall that $q_i = \sum_{j=1}^{m} b_{ij}$ and $q'_i = \sum_{j=1}^{m} b'_{ij}$, and observe that $\frac{\rho_i - 1}{\rho_i} < 0$. By Proposition 14, we have

$$0 \geq \sum_{i=1}^{n} \frac{\rho_i - 1}{\rho_i} \cdot \mathrm{KL}(q'_i \| q_i) \geq \sum_{i=1}^{n} \frac{\rho_i - 1}{\rho_i} \cdot \mathrm{KL}(x'_i \| x_i).$$

For (18), there are two ways to rewrite it. Firstly, it can be rewritten as

$$\begin{aligned}
(18) = &- \sum_{i=1}^{n} \sum_{j=1}^{m} b'_{ij} \ln \frac{b'_{ij}}{b_{ij}} + \sum_{j=1}^{m} p'_j \ln \frac{p'_j}{p_j} + \sum_{i=1}^{n} \frac{1}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i) \\
= &- \mathrm{KL}(b' \| b) + \mathrm{KL}(p' \| p) + \sum_{i=1}^{n} \frac{1}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i) \\
\leq &\sum_{i=1}^{n} \frac{1}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i)
\end{aligned}$$

where the inequality holds due to Proposition 14. Secondly, it can be rewritten as

$$\begin{aligned}(18) &= \sum_{i=1}^{n} \frac{1-\rho_i}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i) - \sum_{i=1}^{n}\sum_{j=1}^{m}(b'_{ij} - b_{ij}) + \sum_{j=1}^{m} p'_j \ln \frac{p'_j}{p_j} \\ &= \sum_{i=1}^{n} \frac{1-\rho_i}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i) - \sum_{j=1}^{m}(p'_j - p_j) + \sum_{j=1}^{m} p'_j \ln \frac{p'_j}{p_j} \\ &= \sum_{i=1}^{n} \frac{1-\rho_i}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i) + \mathrm{KL}(p' \| p) \\ &\geq \sum_{i=1}^{n} \frac{1-\rho_i}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i).\end{aligned}$$

Combining all the above inequalities yields

$$0 \leq d_F\left(\mathbf{z}', \mathbf{z}\right) \leq \sum_{i=1}^{n} \frac{1}{\rho_i} \cdot \mathrm{KL}(b'_i \| b_i),$$

as claimed.

We now turn to the derivation of the PR-QCES protocol from Mirror Descent algorithm. For the convex program (SH-QCES), the Mirror Descent rule (Algorithm 2) is

$$\begin{aligned}(b^{t+1}, w^{t+1}) = \arg\min_{(b,w)\in C} \Bigg\{ &\sum_{i=1}^{n}\sum_{j=1}^{m} \frac{(b_{ij} - b_{ij}^t)}{\rho_i} \cdot \left(1 - \ln \frac{v_{ij}(b_{ij}^t)^{\rho_i - 1}}{(p_j^t)^{\rho_i}}\right) \\ &+ \sum_{i=1}^{n} \frac{1}{\rho_i}\left[1 - (\rho_i - 1)\cdot \ln(K_i - w_i^t)\right] \cdot (w_i - w_i^t) + \sum_{i=1}^{n} \frac{1}{\rho_i} \cdot \mathrm{KL}(b_i \| b_i^t) \Bigg\}.\end{aligned}$$

Since $\sum_{j=1}^{m} b_{ij} + w_i$ is a constant in the domain $C$, we may ignore any term that does not depend on $b$ and $w$, and any positive constant factor in the objective function and simplify the above update rule to

$$\begin{aligned}(b^{t+1}, w^{t+1}) &= \arg\min_{(b,w)\in C} \left\{ -\sum_{i=1}^{n}\sum_{j=1}^{m} \left( \ln \frac{v_{ij}(b_{ij}^t)^{\rho_i - 1}}{(p_j^t)^{\rho_i}} \cdot b_{ij} - b_{ij} \ln \frac{b_{ij}}{b_{ij}^t} + b_{ij} \right) + \sum_{i=1}^{n} (1-\rho_i) \ln(K_i - w_i^t) \cdot w_i \right\} \\ &\triangleq \arg\min_{(b,w)\in C} \overline{F}(b, w).\end{aligned}$$

We have

$$\begin{aligned}\frac{\partial}{\partial b_{ij}} \overline{F}(b,w) &= -\ln \frac{v_{ij}(b_{ij}^t)^{\rho_i - 1}}{(p_j^t)^{\rho_i}} + \ln \frac{b_{ij}}{b_{ij}^t} = \ln b_{ij} - \ln \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}} \\ \frac{\partial}{\partial w_i} \overline{F}(b,w) &= (1-\rho_i)\ln(K_i - w_i^t).\end{aligned}$$

As before, for each fixed $i$, the values of $\ln b_{ij} - \ln \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}}$ for all $j$ are identical. In other words, there exists $c_i > 0$ such that

$$b_{ij} \;=\; c_i \cdot \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}}.$$

As before, there are two cases which depend on $S_i \triangleq \sum_{j=1}^{m} \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}}$.

- If $S_i \geq K_i \cdot (K_i - w_i^t)^{\rho_i - 1}$, then for each $j$ we set $b_{ij}^{t+1} = K_i \cdot \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}} / S_i$, and $w_i^{t+1} = 0$. At this point, we have $\frac{\partial}{\partial b_{ij}} \overline{F}(b, w) = \ln \frac{K_i}{S_i} \leq \frac{\partial}{\partial w_i} \overline{F}(b, w)$, so the optimality condition is satisfied.
- if $S_i < K_i \cdot (K_i - w_i^t)^{\rho_i - 1}$, then for each $j$, we set $b_{ij}^{t+1} = (K_i - w_i^t)^{1-\rho_i} \cdot \frac{v_{ij}(b_{ij}^t)^{\rho_i}}{(p_j^t)^{\rho_i}}$, and $w^{t+1} = K_i - \sum_{j=1}^m b_{ij}^{t+1} > 0$. At this point, $\frac{\partial}{\partial b_{ij}} \overline{F}(b, w) = \frac{\partial}{\partial w_i} \overline{F}(b, w)$, so the optimality condition is satisfied.

This concludes the proof of Theorem 9 which shows that the (PR) dynamics converge to the market equilibrium of a Fisher market with quasi-CES utilities. The result holds for any $0 < \rho_i \leq 1$. However, the proof cannot be extended in a straightforward way to values of $\rho_i < 0$. To see this, we rewrite (18) and (19) as:

$$d_F\left(\mathbf{z}', \mathbf{z}\right) = \sum_{i=1}^{n} \frac{1 - \rho_i}{\rho_i} \cdot \left[\mathrm{KL}(b_i' \| b_i) - \mathrm{KL}(q_i' \| q_i)\right] + \mathrm{KL}(p' \| p). \tag{20}$$

As it happens, the RHS of (20) can be either positive or negative. By Proposition 14,

$$\mathrm{KL}(b_i' \| b_i) \geq \mathrm{KL}(q_i' \| q_i),$$

and there are situations where the equality holds, and thus the RHS of (20) is positive. On the other hand, it is not hard to find two points $b' \neq b$ such that $p' = p$ and $q_i' = q_i$ for all $i$ [5], then the RHS of (20) is negative as $\frac{1-\rho_i}{\rho_i} < 0$. Thus, $F$ is neither convex nor concave function.

[5] For instance, consider $b', b$ such that there exists two goods $j, k$ satisfying $p_j = p_k$, but there exists $i$ such that $b_{ij} \neq b_{ik}$. Then set $b'$ same as $b$, except that $b_{ij}' = b_{ik}$ and $b_{ik}' = b_{ij}$. A sanity check verifies $p' = p$ and $q_i' = q_i$ for all $i$.