Blockchain competition between miners: a game theoretic perspective

Eitan Altman, Daniel Menasché, Alexandre Reiffers, Mandar Datar, Swapnil Dhamal, Corinne Touati, Rachid El-Azouzi

Blockchain competition between miners: a game theoretic perspective

EITAN ALTMAN, INRIA, France
DANIEL SADOC MENASCHÉ, UFRJ, Brazil
ALEXANDRE REIFFERS-MASSON, Indian Institute of Science, India
MANDAR DATAR, SWAPNIL DHAMAL, and CORINNE TOUATI, INRIA, France
RACHID EL-AZOUZI, Unviersity of Avignon, France

We model the competition over mining resources and over several cryptocurrencies as a non-cooperative game. Leveraging results about congestion games, we establish conditions for the existence of pure Nash equilibria and provide efficient algorithms for finding such equilibria. We account for multiple system models, varying according to the way that mining resources are allocated and shared and according to the granularity at which mining puzzle complexity is adjusted. When constraints on resources are included, the resulting game is a constrained resource allocation game for which we characterize a normalized Nash equilibrium. Under the proposed models, we provide structural properties of the corresponding types of equilibrium, e.g., establishing conditions under which at most two mining infrastructures will be active or under which no miners will have incentives to mine a given cryptocurrency.

Additional Key Words and Phrases: Bitcoin, game theory, competition, miners

ACM Reference Format:
Eitan Altman, Daniel Sadoc Menasché, Alexandre Reiffers-Masson, Mandar Datar, Swapnil Dhamal, Corinne Touati, and Rachid El-Azouzi. 2020. Blockchain competition between miners: a game theoretic perspective. 1, 1 (January 2020), 29 pages. https://doi.org/10.3389/fbloc.2019.00026

1 INTRODUCTION

The blockchain is a distributed synchronized secure database containing validated blocks of transactions. A block is validated by special nodes called miners and the validation of each new block is done via the solution of a computationally difficult problem, which is called the proof-of-work puzzle. The miners compete against each other and the first to solve the problem announces it, the block is then verified by the majority of miners in this network, trying to reach consensus. After the propagated block reaches the consensus, it is successfully added to the distributed database. The miner who found the solution receives a reward either in the form of cryptocurrencies or in the form of a transaction reward.

Due to the huge energy requirement necessary to be the first to solve a puzzle, blockchain mining is typically executed in specialized hardware. In [55] an Edge computing Service Provider (ESP) is introduced to support proof-of-work puzzle offloading by using its edge computing nodes. In [54] a game is formulated between the miners in the presence of a single ESP and then a Stackelberg game is used to compute the pricing that maximizes the revenue of the ESP.

Authors' addresses: Eitan Altman, eitan.altman@inria.fr, INRIA, France; Daniel Sadoc Menasché, UFRJ, Brazil; Alexandre Reiffers-Masson, Indian Institute of Science, India; Mandar Datar; Swapnil Dhamal; Corinne Touati, INRIA, France; Rachid El-Azouzi, Unviersity of Avignon, France.

XXXX-XXXX/2020/1-ART
https://doi.org/10.3389/fbloc.2019.00026

Our work addresses the following two questions:

1) given a single blockchain, how should rational users contribute to the mining process, possibly counting on third-party ESPs or mining pools to offload infrastructure costs?

2) given multiple blockchains, e.g., in a multi-cryptocurrency ecosystem, how should rational users distribute their monetary and/or computational budget towards mining?

In this paper, we focus on the competition between miners while addressing the two questions above. We model the competition between miners, who have to choose which ESP to use and which blockchains to mine, as a non-cooperative game. Note that each ESP corresponds to a separate mining infrastructure, and each blockchain corresponds to a different cryptocurrency. Then, we specialize our results to two instances of the general game, showing properties of the Nash equilibrium.

In the first game, there is a single blockchain (e.g., cryptocurrency) and any of the M ESPs (or mining pools) can be used by the miners to solve the puzzle. In the second game, we consider K opportunities, each of which corresponding to another blockchain. At each time slot of duration T (which corresponds to a new puzzle to be solved) each of the miners decides which of K puzzles to solve. We formulate both games and establish conditions for the existence of a pure Nash equilibrium for the association problem between miners and ESPs, providing an efficient algorithm for solving it. We summarize our contributions as follows:

Congestion game for mining competition: we model the competition among users searching for a solution to the mining puzzle as a game (Section 3). In essence, as the number of users willing to mine increases, the chances that a given user is the first to succeed in solving the mining puzzle and wins a reward decreases (i.e., the system becomes *congested*). In particular, we assume that users can count on third-parties to offload infrastructure costs, and can mine multiple cryptocurrencies. Under the assumption that such third-parties are roughly indistinguishable, we further show that when there is one single cryptocurrency of interest the *congestion game* admits a simple equilibrium accounting for users that must decide whether to mine or otherwise not join the system (Section 4).

Analysis of multi-cryptocurrency ecosystem: we analyze the congestion game involving multiple cryptocurrencies. In that case, miners compete against those that decide to mine the same cryptocurrency (Section 5) and we show that the proposed game admits a potential.

Continuous actions and physical bounds on resources: we consider two extensions of the proposed games. First, we consider continuous actions, wherein miners can split their budget across multiple ESPs and multiple cryptocurrencies (Section 7.1). Second, we allow for physical bounds on resources, such as energy, which can be consumed by the whole system (Section 7.2).

Paper outline The remainder of this paper is organized as follows. Sections 2 and 3 present background on mining competition and the general game framework considered in this paper to characterize such competition. Then, Section 4 specializes to the setup wherein there is only one single cryptocurrency, and Section 5 accounts for multiple cryptocurrencies. The general game accounting for multiple ESPs and multiple cryptocurrencies is considered in Section 6. Extensions to account for continuous actions and physical bounds on resources are introduced in Section 7. Discussion and related work follow in Sections 8 and 9, and Section 10 concludes. Appendices contain supplementary material, including a discussion on positive and negative mining externalities (Appendix A), a technical proof (Appendix B) and the analysis of the setup wherein ESPs continuously use their resources at maximum capacity (Appendix C).

2 MINING COMPETITION

In this section we discuss two key aspects pertaining mining competition. First, we indicate how the granularity of the adjustment of mining difficulty impacts the nature of the competition (Section 2.1). Then, we relate the granularity of the mining difficulty adjustment to the horizon at which competition takes place (Section 2.2).

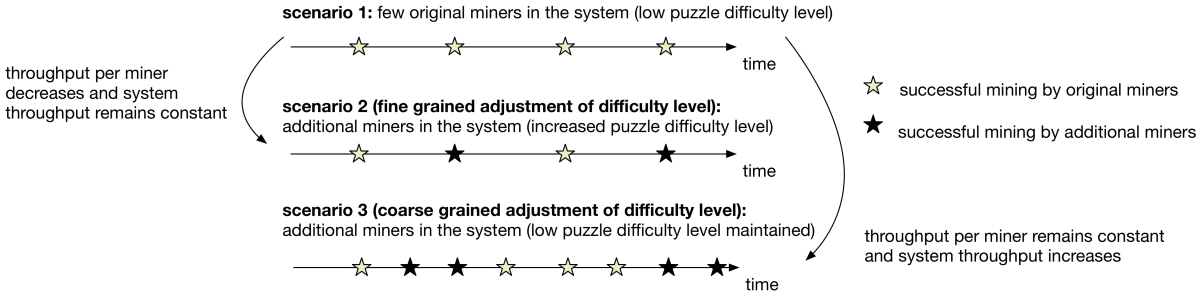

Fig. 1. The difficulty of the puzzle varies as a function of the number of users in the system. Under the fine grained adjustment of difficulty level, the aggregate rate at which the population solves puzzles remains constant over time. A larger number of users in the system leads to competition and smaller rate reward per user. In scenario 1, we have a few miners in the system and low puzzle difficulty level. In scenario 2, we have additional miners in the system and increased puzzle difficulty level (smaller rate reward per user). Under the coarse grained adjustment of difficulty level, the increase in the number of miners may not immediately reflect in adjustment of difficulty level. In scenario 3, miners still compete in the short term, to determine who will be the next to mine the upcoming block.

In the appendix we further indicate more broadly how competition and cooperation play important roles in blockchain systems.

2.1 Granularity of adjustment of mining complexity

The goal of adjusting the mining complexity is to find a difficulty point at which the network mines a block containing outstanding transactions every x minutes. In Bitcoin, we have $x = 10$ minutes. By decreasing (resp., increasing) difficulty, the Bitcoin protocol also decreases (resp., increases) the amount of time, processing power, and electricity required to solve a block.

Next, we discuss the implications of the granularity at which mining complexity is adjusted. Bitcoin's difficulty adjustment, for instance, is naturally adjusted by the system every 2016 blocks. This adjustment probabilistically averages to two week intervals between adjustments.

In this paper, we consider two extreme cases with respect to the granularity of adjustment of mining complexity:

Fine grained adjustment of mining complexity: under the fine grained adjustment of complexity, every time a miner joins or leaves the network the mining complexity is correspondingly adjusted. In this case, the mean time to solve a puzzle by the network is independent of the number of miners. From the perspective of each miner, however, the mean time to solve a puzzle increases as the number of miners grows.

Coarse grained adjustment of mining complexity: under the coarse grained adjustment of complexity, the number of miners may vary inbetween the adjustment of mining complexity. In that case, the mean time to solve a puzzle decreases as the number of miners grows.

In Section 3 we introduce the general game, accounting for the two scenarios described above. Then, we present specialized results to the two instances in the upcoming sections.

2.2 Horizon of competition

The horizon of competition among miners depends on the granularity at which the adjustment of mining complexity takes place. Under the fine grained adjustment of mining complexity, competition occurs both at a short term and long term horizon. This is because as the number of miners increases, the difficulty of the puzzle grows and the competition becomes more aggressive. Under the coarse grained adjustment of mining complexity,

in contrast, competition occurs only at the short term horizon. In essence, miners still compete to decide who will be the next to mine the upcoming block (see Figure 1).

3 BLOCKCHAIN COMPETITION GAME

3.1 Basic concepts

Miners, mining servers and puzzles. We consider a population of M ESPs and a set of K cryptocurrencies, where each cryptocurrency is associated to its blockchain. We denote by $\mathcal{N} = \{1, 2, \ldots, N\}$ the set of miners, also referred to as users. There is a finite population of miners, and if a miner changes his strategy this will cause a change in the utilities of other miners. Let $\mathcal{K} = \{1, 2, \ldots, K\}$ be the set of puzzles, each of which associated with a different cryptocurrency that the miners are trying to solve. We assume that each cryptocurrency corresponds to exactly one puzzle. Let $\mathcal{M} = \{1, 2, \ldots, M\}$ denote the ESPs, also referred to as mining servers, that miners can rely on. A special virtual ESP with index 0 corresponds to an always idle ESP, whose service rate is zero. Miners join ESP 0 when they decide not to join the mining game. Notation is summarized in Table 2.

Strategies. Set $\mathcal{S}_i \subset \mathcal{K} \times \mathcal{M}$ denotes the set of ordered pairs (puzzle, ESP), corresponding to ESPs that miner i can rely on to solve puzzles of a given type. The set $\mathcal{S}_i$ can differ across miners due to political or economic restrictions. For instance, certain countries do not allow investment in certain cryptocurrencies. Alternatively, the set of available ESPs for two different miners may not be the same. A strategy for miner i is denoted by $s_i \in \mathcal{S}_i$, corresponding to the puzzle (cryptocurrency) which the miner intends to solve using a given infrastructure. Strategy $s_i = (k, m)$ corresponds to user i using ESP infrastructure m to mine cryptocurrency k. A strategy vector $s = (s_i)_{i \in \mathcal{N}}$ produces a load vector $\ell = (\ell_{k,m})_{k,m}$, where $\ell_{k,m}$ denotes the number of miners using ESP m to mine cryptocurrency k.

Mining complexity. We denote by $\mu_{k,m,i}$ the service rate from ESP m requested by miner i to solve puzzle k. We assume $\mu_{k,m,i} > 0$ when $m \neq 0$, and $\mu_{k,0,i} = 0$, for $k = 1, \ldots, K$ and $i = 1, \ldots, N$. For convenience, the service rate is measured

- in rate of hashes computed per time unit (trials to solve the puzzle per time unit), when accounting for the fine grained adjustment of mining complexity, wherein the average number of puzzles solved per time unit for the whole population is fixed and given, and
- in rate of puzzles successfully solved per time unit, when accounting for the coarse grained adjustment, so as to simplify notation.[1]

Let η_k be the load of miners across all ESPs towards cryptocurrency k. Then,

$$\eta_k = \sum_{m' \in \mathcal{M}} \sum_{i' \in \mathcal{N}} \mu_{k,m',i'}. \tag{1}$$

In the remainder of this paper, except otherwise noted, we assume that a user who selects a given (ESP, cryptocurrency) pair is allocated a given hash power by the ESP.[2] Figure 2 illustrates the considered setup. Then, (1) simplifies to

$$\eta_k = \sum_{m' \in \mathcal{M}} \ell_{k,m'} \mu_{k,m'}. \tag{2}$$

Note that (2) is obtained from (1) by lumping the state space: for symmetric users it suffices to track the *number* of users selecting each of the available (ESP, cryptocurrency) pairs rather than their identities.

[1] Alternatively, the service rate could be uniformly set in units of hashes per time unit, but in that case one would need to introduce and additional parameter to relate the number of hashes computed per time unit and the fraction of those that translate into successful mining.
[2] To account for non-symmetric users, one may add additional virtual users and/or virtual (ESP, cryptocurrency) pairs representing different service level agreements offered by a given ESP to users.

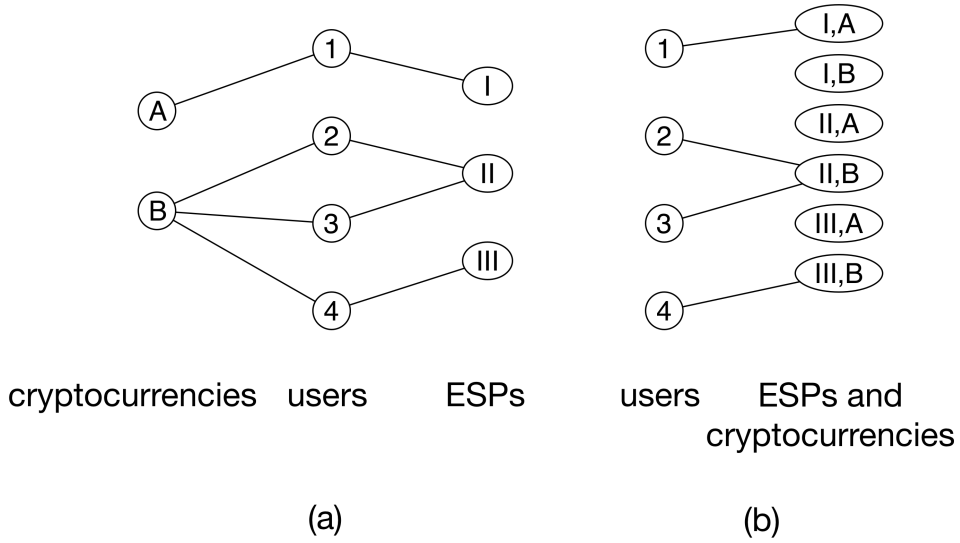

Fig. 2. Graph characterizing the selection of cryptocurrencies and ESPs by users: (*a*) general system representation; (*b*) bipartite graph representing the system accounting for symmetries considered throughout this work.

Let $\mathcal{T}_k$ be the time it takes for the first miner, across all ESPs, to solve puzzle k. Let q_k be the probability that puzzle k is solved by time T since the last puzzle of cryptocurrency k was solved. Note that under the fine grained adjustment of mining complexity, $\mathcal{T}_k$ and q_k are functionally independent of η_k, as far as the number of miners of cryptocurrency k is positive. Without loss of generality, we assume that the time horizon of interest, T, is set to a large enough value, independent of η_k, so that $q_k \approx 1$. Under the coarse grained adjustment of mining complexity, in contrast, $\mathcal{T}_k$ and q_k depend on η_k as the time it takes for a block of cryptocurrency k to be successfully mined is a function of the load of miners towards k (Table 1).

Under the coarse grained adjustment of mining complexity, $\mathcal{T}_k$ depends on the number of miners in the system. In that case, we denote by $R_{k,m,i}$ the amount of service time from ESP m required by miner i to solve puzzle k. As we assume that users are symmetric, the random variables $R_{k,m,i}$ are independent and identically distributed, for $i = 1, \ldots, N$, with each $R_{k,m,i}$ being exponentially distributed with rate $\mu_{k,m}$. Thus, if there are $\ell_{k,m}$ miners associated to ESP m mining currency k, the time it takes for the fastest of them to solve the puzzle corresponding to currency k is exponentially distributed with rate $\eta_k = \sum_m \mu_{k,m}\ell_{k,m}$. Then,

$$\mathcal{T}_k \sim \text{Exp}(\sum_m \mu_{k,m}\ell_{k,m}) \tag{3}$$

$$q_k = 1 - \exp(-T\eta_k). \tag{4}$$

Note that in this case if T is set to a large enough value, dependent on η_k, we also have $q_k \approx 1$ as in the previous paragraph.

Rewards and costs. Let $\tilde{p}_{k,m}$ denote the probability that a miner using ESP m is the first to solve puzzle k at state ℓ. Then,

$$\tilde{p}_{k,m}(\ell) = q_k \frac{\ell_{k,m}\mu_{k,m}}{\eta_k}. \tag{5}$$

Throughout this paper, $0/0 = 0$. In the expression of $\tilde{p}_{k,m}$, for instance, if $\eta_k = 0$ and $\ell_{k,m} = 0$, then $\tilde{p}_{k,m} = 0/0 = 0$.

Table 1. Granularity of difficulty adjustment

	average time between two blocks mined, for whole population ($\mathcal{T}_k$)	average time between two blocks mined, per miner	probability of success by time T (q_k)	time horizon to grant rewards to given player (T)
Fine grained adjustment of mining complexity	fixed and given	variable, depends on η_k, for fixed $\mu_{k,m}$	≈ 1	large, compared against puzzle complexity adjustment
Coarse grained adjustment of mining complexity	variable, depends on η_k, for fixed $\mu_{k,m}$	fixed and given, for fixed $\mu_{k,m}$	$1-\exp(-T\eta_k)$	small, compared against puzzle complexity adjustment

Under strategy profile ℓ, the probability that a given miner using ESP m is the first to solve puzzle k is

$$p_{k,m}(\ell) = 1_{\ell_{k,m}>0}\frac{q_k\mu_{k,m}}{\eta_k}, \tag{6}$$

where 1_c equals 1 if condition c holds and 0 otherwise.

We denote by $\gamma_{k,m}$ the cost of mining blockchain k at ESP m. Under the fine grained adjustment of puzzle complexity, $\gamma_{k,m}$ is measured in cost per time unit. Under the coarse grained adjustment of puzzle complexity, $\gamma_{k,m}$ is the cost incurred by users to reserve mining resources during the time horizon T of interest.

Utilities. Let $U_{k,m}(\ell)$ denote the utility to a miner who tries to find the solution of puzzles associated to cryptocurrency k, using ESP m. The utility is given by rewards minus costs. Thus,

$$U_{k,m}(\ell) = \begin{cases} p_{k,m}\rho - \gamma_{k,m} & \text{if } m > 0, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

Under the fine grained adjustment of puzzle complexity, ρ is the rate reward granted to successful miners, which is fixed and given. Therefore, to simplify presentation we let $\rho = 1$, and $\gamma_{k,m}$ is adjusted accordingly. Under the coarse grained adjustment of puzzle complexity, in contrast, if users are still interested in the long term rewards they need to account for a rate reward that is a function of the users actions. This is because under the coarse grained adjustment of puzzle complexity, the larger the number of users mining a given cryptocurrency, the larger the rate at which blocks are mined. Alternatively, motivated by [11] we assume that users under the coarse grained adjustment of puzzle complexity are greedy and myopic, as detailed next.

Whereas under the fine grained adjustment of puzzle complexity users are interested in maximizing a long term average rate reward, under the coarse grained adjustment they are interested in maximizing the reward collected by time T, assuming that during that time horizon the chances that more than one user collects rewards are negligible. In that case, users are granted a reward if and only if they are the first to successfully mine by the time horizon of interest, T. We let $\rho = 1$ and $\gamma_{k,m}$ characterizes the cost of reserving mining resources to mine during slot T.

Note that under the fine grained adjustment of puzzle complexity, a new mining interval starts immediately after a successful mining event occurs. Under the coarse grained adjustment of puzzle complexity, in constrast, we assume that mining resources are reserved for a mining interval T, and even if a success occurs before T

miners pay for resources allocated up until T. In both cases, the utility reduces to

$$U_{k,m}(\ell) = \begin{cases} p_{k,m} - \gamma_{k,m} & \text{if } m > 0, \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

User i utility is $\tilde{U}_i(s_i, s_{-i}) = \sum_{(k,m)\in\mathcal{S}_i} 1_{s_i=(k,m)} U_{k,m}(\ell)$, where $s_{-i} = (s_1, s_2, \ldots, s_{i-1}, s_{i+1}, \ldots, s_N)$ is the vector of strategies of all miners except miner i. Given the ingredients above, the blockchain competition game is characterized by $C = \langle \mathcal{N}, \mathcal{K} \times \mathcal{M}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (U_{k,m})_{(k,m)\in\mathcal{K}\times\mathcal{M}} \rangle$. In Sections 4 and 5 we analyze two special instances of this game.

3.2 Summary of terminology

We summarize the basic terminology used throughout this paper.

Edge Service Providers (ESPs) continuously try to solve blockchain puzzles, by allocating hash power for that purpose.

Hash power dedicated to a given blockchain by a given ESP is the number of hashes computed per time unit by that ESP to solve puzzles from the corresponding blockchain.

Service rate dedicated to a given blockchain by a given ESP equals the corresponding hash power. Under the coarse grained adjustment of puzzle complexity, it is more convenient to measure the service rate in number of successful puzzles solved per time unit, noting that in this case the number of successful puzzles solved per time unit equals the hash power times a constant multiplicative factor smaller than one.

Miners pay to ESPs in order to solve blockchain puzzles.

Active miners participate in the mining game, by paying a strictly positive amount to ESPs in order to solve blockchain puzzles. **Inactive miners** decide not to actively join the mining game. They receive no rewards, and incur zero costs.

Rewards are granted to miners once the contracted ESP solves the corresponding puzzle.

Costs are incurred by miners to contract ESPs.

Revenue corresponds to rewards minus costs incurred by each miner.

3.3 Congestion games and potentials

Next, we briefly introduce some basic background on congestion games, crowding games and potentials. Such background is instrumental in the analysis of the blockchain competition game that follows.

Congestion games were introduced by [36] and are equivalent to routing over an arbitrary graph, when all routed objects have the same size, and are non splittable. The cost of using an edge is the same for all players. Crowding games proposed by [34] are congestion games with more restricted topology (parallel links) but more general costs (user dependent).

In our setup, the routed object is the mining power. The network has a bipartite topology, where one side consists of mining users (end users) and the other side consists of ESPs that mine according to mining users requests. A virtual ESP corresponds to the option of not mining. The cost incurred by a user who decides to mine through a given ESP is the cost of an edge between the user and the ESP (see Figure 3).

A congestion game without player specific payoff functions is guaranteed to admit a standard potential and a pure equilibrium (see [36]). A game that does not admit a standard potential may still admit an ordinal potential. A game with an ordinal potential can have any finite subset of actions available to a player, still admitting a pure equilibrium.

[34] proves the existence of a pure Nash equilibrium given user dependent costs in crowding games. In this paper, we are interested in user dependent strategy sets. Nonetheless, one can show an equivalence between user dependent costs and user dependent strategy sets, and henceforth we use interchangeably the two notions.

4 ESP CONNECTION GAME

In this section, we introduce the ESP connection game and analyze some properties of its equilibria. We consider the special case where we have only one cryptocurrency, which we denote by $\star$.

4.1 Coarse grained adjustment of mining difficulty

In this section we consider the coarse grained adjustment of mining complexity under a scenario wherein there is a single cryptocurrency. First, we consider the simplest setting wherein all miners are symmetric (Section 4.1.1). Then, we relax our assumptions and show conditions under which the mapping between ESP connection games and potential games still holds, posing a conjecture on the extent at which the assumptions can be further relaxed (Section 4.1.2).

4.1.1 To mine or not to mine? A simple congestion game accounting for symmetric ESPs. In this section, our goal is to illustrate the relationship between the games considered in this work and congestion games. To that aim, we assume ESPs are symmetric, i.e., $\mu_{\star,m} = \mu_\star$ and $\gamma_{\star,m} = \gamma_\star$ for all m. Although the scenario is very simple, it already serves to appreciate the sort of analysis considered in the remainder of this work. In the following section, we relax those assumptions.

Let $\ell_\star$ be the number of miners that decide to associate to an ESP,

$$\ell_\star = \sum_{m=1}^{M} \sum_{i \in \mathcal{N}} 1_{s_i^*=(\star,m)}. \tag{9}$$

Then, $N - \ell_\star$ is the number of users that decide not to mine.

When all $\mu_{\star,m}$ are equal we denote them by $\mu_\star$. Then, equation (6) reduces to

$$p_\star(\ell_\star) = 1_{\ell_\star > 0} \frac{1 - \exp(-T\mu_\star \ell_\star)}{\ell_\star}, \tag{10}$$

where $p_\star$ is the probability that a user that decides to connect to an ESP is the first to solve the puzzle. The utility for a miner associating to ESP m is given by (8).

Theorem 4.1 (no player-specific strategies). *If for all i and j, $\mathcal{S}_i = \mathcal{S}_j$, the Nash equilibrium is given by the solution of the following optimization problem,*

$$argmax_{\ell_\star} \quad \sum_{l=1}^{\ell_\star} (p_\star(l) - \gamma_\star) \tag{11}$$

$$\text{subject to:} \quad \ell_\star \leq N, \quad \ell_\star \geq 0, \tag{12}$$

where $\ell_\star$ solution of (11)-(12) *is the number of users that decide to mine. Equation* (11) *is the game* potential function. *The optimization problem* (11)-(12) *is equivalent to a bin-packing problem with concave costs. Therefore existence and uniqueness is guaranteed.*

Proof. This is a congestion game in the sense of [45] and therefore has a potential. Indeed, in this game each player can decide to associate or not with an ESP. Thus all connections to the M ESPs can be aggregated to a single route that represents the choice of mining and the option of not associating represents the second route (see Figure 3). □ □

Theorem 4.2 (player-specific strategies). *If $\mathcal{S}_i$ depends on the identity of user i, the game may not admit a standard potential, but still admits pure Nash equilibria.*

Proof. The game is a crowding game, and the result follows from [34, 35]. □ □

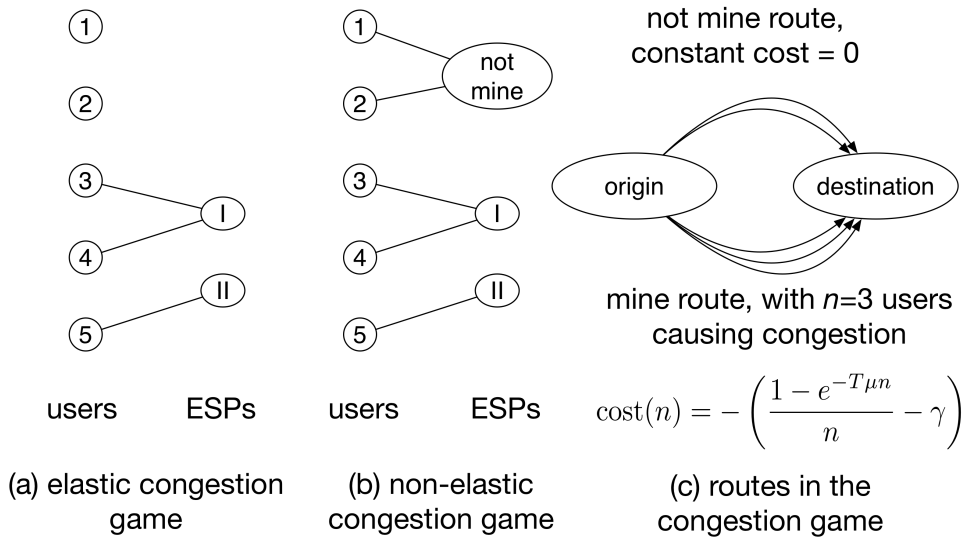

Fig. 3. Graph characterizing the selection of ESPs by users: (*a*) bipartite graph representation; (*b*) alternative representation wherein the option of not mining is represented through a separate node and (*c*) simplified representation where M ESPs are aggregated into a single route that represents the choice of mining and the option of not mining is represented by a second route.

4.1.2 Existence of equilibrium under general conditions. Next, our goal is to illustrate results on the existence of equilibria. To that aim, we generalize the conditions considered in the previous section, allowing for multiple non-symmetric ESPs, and indicate how the considered game still relates to congestion games.

Theorem 4.3 (existence). *If $\gamma_{\star,m} = \gamma_{\star,m'}$ for all m' and m, $\mu_{\star,m} \neq \mu_{\star,m'}$ for all m and m' such that $m \neq m'$, and $\mathcal{S}_i = \mathcal{S}_j$ then:*

(1) *a pure Nash equilibrium exists*
(2) *miners will only rely on ESP m^*, with $m^* = \max\{m : \ \mu_{\star,m} \geq \mu_{\star,m'} \ \forall m'\}$ and*
(3) *the Nash equilibrium is given by the solution of the following optimization problem,*

$$argmax_{\ell_{\star,m^*}} \quad \sum_{l=1}^{\ell_{\star,m^*}} (p_{\star,m^*}(l) - \gamma) \tag{13}$$

$$\text{subject to:} \quad \ell_{\star,m^*} \leq N, \quad \ell_{\star,m^*} \geq 0. \tag{14}$$

Proof. Let $l'_{\star,m}$ be the number of users, except one, mining the unique cryptocurrency using ESP m. $l'_{\star,m}$ needs not to be at Nash Equilibrium. The player that did not take his decision is facing the following optimization problem:

$$\max\left\{\max_m\left\{\frac{\mu_{\star,m}(1-\exp(-T(\mu_{\star,m}+\sum_{m'} l'_{\star,m'}\mu_{\star,m'})))}{\mu_{\star,m}+\sum_{m'} l'_{\star,m'}\mu_{\star,m'}}\right\}, \gamma\right\}. \tag{15}$$

Let us define the function f such that:

$$f(x) = \frac{x(1-\exp(-T(x+\sum_{m'} l'_{\star,m'}\mu_{\star,m'})))}{x+\sum_{m'} l'_{\star,m'}\mu_{\star,m'}}. \tag{16}$$

Table 2. Table of notation

variable	description
K	number of blockchains (cryptocurrencies)
M	number of edge service providers (ESPs)
N	number of miners (willing to mine using ESPs)
$U_{k,m}(\ell)$	utility of user mining blockchain k at ESP m
$\gamma_{k,m}$	mining cost associated to blockchain k at ESP m
$\mu_{k,m}$	service rate from ESP m requested by each miner to solve puzzle k
	action space and corresponding variables
$\mathcal{S}_i \subset \mathcal{K} \times \mathcal{M}$	set of ordered pairs (puzzle, ESP), corresponding to ESPs that miner i can use to mine k
$\ell_{k,m}$	number of users mining blockchain k at ESP m
ℓ	strategy profile, $\ell = (\ell_{1,1}, \ell_{1,2}, \ldots, \ell_{k,m}, \ldots, \ell_{K,M})$ (discrete action space, all sections except Section 7)
	control variables
s_i	$s_i = (k, m)$ if user i mines blockchain k at ESP m (discrete action space, all sections except Section 7)
x_m	amount bid by ESP m, proportional to the load invested by ESP m for mining (continuous action space, Section 7)
	metrics
$p_{k,m}(\ell)$	probability that user is first to mine a block

$f(x)$ is strictly increasing for $x > 0$. Therefore, for all $\sum_{m'} l'_{\star,m'}\mu_{\star,m'}$:

$$\max_x f(x) = f(\mu_{\star,m^*}) = \frac{\mu_{\star,m^*}(1 - \exp(-T(\mu_{\star,m^*} + \sum_{m'} l'_{\star,m'}\mu_{\star,m'})))}{\mu_{\star,m^*} + \sum_{m'} l'_{\star,m'}\mu_{\star,m'}}, \tag{17}$$

with $m^* = \max\{m : \ \mu_{\star,m} \geq \mu_{\star,m'} \ \forall m'\}$. It follows that the utility of a player at equilibrium will be:

$$\max\left\{\frac{\mu_{\star,m^*}(1 - \exp(-T(\mu_{\star,m^*} + l'_{\star,m^*}\mu_{\star,m^*})))}{\mu_{\star,m^*} + l'_{\star,m^*}\mu_{\star,m^*}} - \gamma, 0\right\}. \tag{18}$$

To summarize, the best-response of any player to any $l'_{\star,m}$ is such that miners will only rely on ESP m^*, with $m^* = \max\{m : \ \mu_{\star,m} \geq \mu_{\star,m'} \ \forall m'\}$. Moreover, let us assume that each player is now only focusing on the ESP m^*. In this case, the ESP connection game is a congestion game, in the sense of [45]. The rest of the proof follows as a special case of Theorem 4.1. In a network congestion game, the time it takes to travel (expected number of trials to be the first to mine) on any road (ESP) is an increasing (payoff decreasing) function of the number of people (miners) selecting that road (ESP). Then, by the theorem 1 from [45] there exists pure Nash equilibrium. □ □

Illustrative examples. Consider 4 miners and 3 ESPs, $N = 4$ and $M = 3$. Let $\mu_{\star,m}$ equal 0, 0.2, 0.4 and 0.6 for $m = 0, 1, 2, 3$, respectively. Let $T = 1$ and $\gamma = 0.3$. Then, the game admits 6 pure equilibria, where $6 = \binom{4}{2}$. In each equilibrium, two of the players adopt strategy 0 and the other two players adopt strategy 3. The players adopting strategies 3 and 0 have corresponding utilities of 0.049 and 0, respectively, where $m^* = 3$. In addition, $p_{\star,m^*}(l) - \gamma$ equals 0.15, 0.049, -0.02 and -0.09 for $l = 1, 2, 3, 4$, indicating that $\sum_{m=1}^{\ell_{\star,m^*}}(p_{\star,m^*}(l) - \gamma)$ is maximized for $\ell_{\star,m^*} = 2$ which is in agreement with the fact that 2 users are active in equilibrium (see (11)).

Table 3. Assumptions throughout sections

Section	ESPs	Symmetric ESPs	Users can decide not to mine	Puzzle complexity adjustment	Multiple ESPs	Multiple crypto	Atomic miners	Continuous actions
4.1.1	one or more	yes	yes	coarse	yes	no	yes	no
4.1.2	one or more	no	yes	coarse	yes	no	yes	no
4.2	one or more	no	yes	fine	yes	no	yes	no
5	one	no	yes	coarse	no	yes	yes	no
6	one or more	no	yes	fine or coarse	yes	yes	no	no
7	one or more	no	yes	fine	yes	no	yes	yes

Consider now the following additional example, which is out of the scope of Theorem 4.3, wherein 4 miners compete over 3 ESPs, $N = 4$ and $M = 3$. Let $\mu_{\star,m}$ equal 0, 0.24, 0.45 and 0.6 for $m = 0, 1, 2, 3$, respectively. Let $\gamma_{\star,m}$ equal 0, 0.147, 0.26 and 0.46 for $m = 0, 1, 2, 3$, respectively. Note that Theorem 4.3 assumes $\gamma_{\star,m}$ to be the same across all ESPs, which is not the case in the current setup. This game admits 19 pure Nash equilibria: 12 equilibria correspond to permutations of the strategy profile (0,1,1,2), 6 equilibria correspond to permutations of the strategy profile (0,0,2,2) and the last equilibrium equals (1,1,1,1). Note that strategy 3, which corresponds to the highest rate, does not appear in any of the equilibrium profiles. This is in stark contrast with the previous setup, wherein the strategy with highest rate was the only candidate to be an element in the equilibrium. In addition, note that users adopting different strictly positive rates may together comprise the equilibrium. This motivates the following conjecture.

Conjecture 4.4. *If (i) $\mu_{\star,m} \neq \mu_{\star,m'}$ whenever $m \neq m'$, (ii) $\gamma_{\star,m} \geq \gamma_{\star,m'}$ implies that $\mu_{\star,m} \geq \mu_{\star,m'}$, and (iii) $\mathcal{S}_i = \mathcal{S}_j$ then:*

(1) *a pure Nash equilibrium exists*
(2) *at equilibrium, across the set of active miners there will be connections to at most two ESPs, denoted by m' and m'' and*
(3) *when $m' \neq m''$, the Nash equilibrium is given by the solution to the following optimization problem,*

$$\underset{(\ell_{\star,m'},\ell_{\star,m''})}{argmax} \quad \sum_{l'=1}^{\ell_{\star,m'}} \sum_{l''=1}^{\ell_{\star,m''}} p_{\star,m'}(\ell) - \gamma_{\star,m'} + p_{\star,m''}(\ell) - \gamma_{\star,m''} \tag{19}$$

$$\text{subject to:} \qquad \ell_{\star,m'} + \ell_{\star,m''} \leq N, \quad \ell_{\star,m'} \geq 1, \qquad \ell_{\star,m''} \geq 1, \tag{20}$$

where $\ell = (N - l' - l'', l', l'')$ denotes a strategy profile wherein $N - l' - l''$ miners are inactive, l' miners adopt ESP m' and l'' miners adopt ESP m''.

To illustrate the last part of the conjecture above, consider again the previous numerical result. Let $m' = 1$ and $m'' = 2$, and let the lumped strategy profile be a vector (n_0, n_1, n_2, n_3) which corresponds to a profile wherein n_i users adopt ESP i. Then, the lumped strategy profiles $(2, 1, 1, 0)$, $(1, 1, 2, 0)$, $(0, 1, 3, 0)$, $(1, 2, 1, 0)$, $(0, 2, 2, 0)$ and $(0, 3, 1, 0)$ evaluate the objective function (19) to 0.0914, 0.0961, 0.0345, 0.1336, 0.1055 and 0.1333 indicating that the equilibrium with strategy profile $(0, 1, 1, 2)$ found in the previous paragraph, which corresponds to the lumped strategy profile $(1, 2, 1, 0)$, is in agreement with the conjecture. In Section 6.2 we prove a result inspired by the conjecture above, under the setup of non-atomic games.

4.2 Fine grained adjustment of mining difficulty

Next, we consider the fine grained adjustment of mining difficulty. To that aim, we assume $q_k = 1$, i.e., we do not include the exponential term in the definition of q_k (eq. (4)). Recall that the exponential term captures the probability that the puzzle is not solved by time T, which we assume to be negligible (i.e., much smaller than 1), for large enough T (see Table 3).

4.2.1 Best response dynamics and convergence under M-concave potential. Consider any better response learning scheme. In particular, the best response learning scheme is one of such schemes. Note that for a player to update its response it only needs to have access to the total load across all ESPs. Note also that for a player to compute its response, without previous knowledge of historical responses, it needs to know the overall load generated by all the miners over each ESP.

Since the utility is concave we may expect the potential to converge to a global optimum in finite time under any standard best response strategy or better response policy. However, the concave function is defined only on integers, which is not a convex compact set. In this case, some modifications of the definition of concavity and convex sets are needed in order to guarantee that any local extremal point of the function is a global extremal point. These modifications are called M-concavity and M-convex set, respectively (see [27] and references therein). Then, the key result of this section follows.

Theorem 4.5. *The ESP competition game under fine grained adjustment of mining difficulty admits a potential.*

Proof. It is shown in [27] that the social medium selection game is a congestion game. We have already shown that the ESP selection game is a congestion game and that there exists a potential. The potential function for the social medium selection game is also a potential function for the ESP selection game. Moreover, Theorem 2 from [27] shows that the potentials are M-concave functions defined over an M-convex set. □ □

5 CRYPTOCURRENCY ASSOCIATION GAME

In this section, we introduce the multiple cryptocurrencies game and derive structural properties of the associated set of equilibria. As in Section 4.1, we assume a coarse grained adjustment of difficulty level. In addition, we assume that there are K cryptocurrencies. We consider a single ESP, and drop subscript m from all variables.

For a given load vector ℓ, the time it takes till the fastest puzzle to be solved is exponentially distributed with expectation $1/(\mu_k \ell_k)$. Thus, the probability that a miner is the first to solve the puzzle is

$$p_k(\ell_k) = \frac{1 - \exp(-T\mu_k \ell_k)}{\ell_k}. \tag{21}$$

Note that $p_k = 0$ if $\ell_k = 0$ (recall that we assume $0/0 = 0$ throughout this paper). The utility of a tagged miner to mine a cryptocurrency k when there are ℓ_k miners associated with the same cryptocurrency (including the tagged miner) is given by (8), where

$$U_k(\ell_k) = p_k - \gamma_k. \tag{22}$$

We add to it the constraint that a miner does not participate in solving the puzzle if its utility is negative. In that case the equilibrium is characterized by the condition $\sum_k \ell_k^* \le N$, with $\ell_k^* \ge 0$, for $k = 1, \ldots, K$. This game is referred to as an *elastic game*. Alternatively, we can consider an additional cryptocurrency, indexed by 0, with corresponding utility being constant equal to 0. Then,

$$U_k(\ell_k) = \begin{cases} p_k - \gamma_k, & \text{if } k > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{23}$$

This game is referred to as the *non-elastic game* equivalent to the elastic game above (Figure 3 illustrates the elastic and non-elastic instances of the ESP connection game). If the equilibrium vector ℓ^* saturates the constraint

in the elastic game ($\sum_k \ell_k^* = N, \ell_k^* \geq 0, k = 1, ..., K$) or, alternatively, if $\ell_0^* = 0$ in the non-elastic game, then for each k for which $\ell_k^* > 0$, and each k', $U_k(\ell_k^* - 1) \geq U_{k'}(\ell_{k'}^* + 1)$.

Similar theorems as those presented in the previous section establishing the existence of pure Nash equilibria and characterizing the equilibria still hold under the blockchain association game. The statements of the theorems and the proofs are similar to those in the previous section, and are omitted for conciseness. Recall that in Theorem 4.1 for all i and j, $\mathcal{S}_i = \mathcal{S}_j$. Then, in this case the number of miners associated to each cryptocurrency $\ell_k^* = \sum_{i \in \mathcal{N}} 1_{s_i^* = k}$ is now the solution of the following optimization problem,

$$\text{argmax}_{\ell} \quad \sum_{k \in \mathcal{K}} \sum_{l=1}^{\ell_k} (p_k(l) - \gamma_k) \tag{24}$$

$$\text{subject to:} \quad \sum_{k \in \mathcal{K}} \ell_k \leq N, \quad \ell_k \geq 0. \tag{25}$$

Theorem 4.1 holds replacing (11)-(12) by the equations above.

6 NON-ATOMIC MINERS FOR THE MULTIPLE ESP'S AND MULTIPLE CRYPTOCURRENCIES GAME

We will now study a mean-field approximation of the cryptocurrencies game. This approximation is instrumental to provide additional insight concerning the multiple ESPs/multiple cryptocurrencies game.

6.1 Wardrop equilibrium basics

6.1.1 Problem formulation. We assume that the miners are non-atomic. In this case, for a given load vector ℓ, a miner solves the following optimization problem:

$$\max \left\{ \max_{k,m} \left\{ \mathcal{U}_{k,m}(\ell) \right\}, 0 \right\}, \tag{26}$$

where

$$\mathcal{U}_{k,m}(\ell) = \frac{\mu_{k,m}}{\sum_{m'} \mu_{k,m'} \ell_{k,m'}} q_k \left(\sum_{m'} \mu_{k,m'} \ell_{k,m'} \right) - \gamma_{k,m}. \tag{27}$$

If the miners were atomic, the mining decision of a given miner (assuming that the rest of the miners will not modify their strategies) would impact the load vector ℓ. However, under the assumption that the miners are non-atomic, the deviation of one miner will not modify the load vector ℓ and therefore the miner's best-response to a given load ℓ is given by the arg max of (26).

This assumption is valid in two cases: (1) when miners do not realize that their mining decisions will impact utilities $\mathcal{U}_{k,m}(\ell)$ for all k and all m or (2) when the number of miners is large and $\gamma_{k,m}$ and $\mu_{k,m}$ are small. [23] were the first to prove that the non-atomic equilibrium (also known as Wardrop equilibrium) is the limit of many players of Nash equilibrium, under strict diagonal concavity conditions established by [44]. [2, 3] showed that for a game equivalent to the one considered in the section, under the fine grained adjustment of puzzle complexity, i.e., when $q_k = 1$, the strict diagonal concavity conditions hold. In this case, the assumption that miners do not account for the impact of their decisions on the actions of the others is referred to as a *mean-field* approximation.

6.1.2 Equilibrium characterization. A non-atomic equilibrium load vector ℓ^* satisfies:

$$\mathcal{U}_{k,m}(\ell^\star) = \mathcal{U}_{k'',m''}(\ell^\star), \quad \text{if } \ell^*_{k,m} > 0, \quad \ell^*_{k'',m''} > 0, \quad \forall m, m'', k, k'', \tag{28a}$$

$$\mathcal{U}_{k,m}(\ell^\star) \geq \mathcal{U}_{k'',m''}(\ell^\star), \quad \text{if } \ell^*_{k,m} > 0, \quad \ell^*_{k'',m''} = 0, \quad \forall m, m'', k, k'', \tag{28b}$$

$$\mathcal{U}_{k,m}(\ell^\star) \leq 0, \quad \text{if } \ell^*_{k,m} = 0, \quad \forall m, k, \tag{28c}$$

$$\sum_{k,m} \ell^\star_{k,m} \leq N. \tag{28d}$$

Before studying the properties of such equilibria, we provide some intuition for the rationale behind equations (28a)-(28d). For an in depth analysis of non-atomic equilibria, we refer the reader to [46] and [51].

Can a miner be interested in deviating from ℓ^*? To answer that question, let $S_A(\ell^*)$ be the set of all pairs (k, m) corresponding to active miners under equilibrium ℓ^*,

$$S_A(\ell^*) := \{(k, m) \mid \ell^*_{k,m} > 0,\ \ell^*_{k,m} \text{ solution of (28a) – (28d)}\}. \tag{29}$$

Equation (28a) implies that for all pairs in $S_A(\ell^*)$ the utility is the same. Therefore, if a miner is interested in deviating from ℓ^*, arg max of (26) must be a pair $(k'', m'') \notin S_A(\ell^*)$. However, an investment, say, in $(k'', m'') \notin S_A(\ell^*)$, must be suboptimal according to (28b). Therefore, a miner will always choose $(k, m) \in S_A(\ell^*)$, which naturally implies that ℓ^* satisfying (28a)-(28d) is an equilibrium strategy.

By studying (28a)-(28d), we will give some basic insights about the structure of any equilibrium. For now, we will assume that an equilibrium ℓ^* always exists. Later in this section, we will study the existence and uniqueness of ℓ^*.

6.2 Miners invest at maximum in two ESPs for a given cryptocurrency

Next, we show that under equilibrium miners invest at maximum in two ESPs for a given cryptocurrency. To that aim, we start with the following definition.

Definition 6.1. Two pairs of ESPs (m, m') and (m'', m'''), such that $\mu_{k,m} < \mu_{k,m'}$ and $\mu_{k,m''} < \mu_{k,m'''}$, are said to be colinear with respect to cryptocurrency k if

$$\frac{\mu_{k,m} - \mu_{k,m'}}{\gamma_{k,m} - \gamma_{k,m'}} = \frac{\mu_{k,m''} - \mu_{k,m'''}}{\gamma_{k,m''} - \gamma_{k,m'''}}. \tag{30}$$

Intuitively, two pairs of ESPs are colinear when their difference in capacities and costs can be linearly aligned. The following theorem establishes our main structural result for this section.

Theorem 6.2. *If no two pairs of ESPs are colinear with respect to cryptocurrency k, then at equilibrium miners invest at maximum in two ESPs for that cryptocurrency.*

Proof. The proof of this statement is based on a contradiction argument. Let us assume, without loss of generality, that $\ell_{k,m}, \ell_{k,m'}, \ell_{k,m''} > 0$. Then we have the following system:

$$\frac{\mu_{k,m} - \mu_{k,m'}}{\sum_n \mu_{k,n}\ell^*_{k,n}} q_k\Big(\sum_n \mu_{k,n}\ell^*_{k,n}\Big) = \gamma_{k,m} - \gamma_{k,m'} \tag{31}$$

$$\frac{\mu_{k,m} - \mu_{k,m''}}{\sum_n \mu_{k,n}\ell^*_{k,n}} q_k\Big(\sum_{m'} \mu_{k,n}\ell^*_{k,n}\Big) = \gamma_{k,m} - \gamma_{k,m''} \tag{32}$$

which leads to the following contradiction $\frac{\mu_{k,m}-\mu_{k,m''}}{\gamma_{k,m}-\gamma_{k,m''}} = \frac{\mu_{k,m}-\mu_{k,m'}}{\gamma_{k,m}-\gamma_{k',m'}}$, concluding the proof. □ □

6.2.1 When will miners invest in only one ESP for a given cryptocurrency? Next, we further establish sufficient conditions for miners to invest in only one ESP for a given cryptocurrency.

Theorem 6.3. *If, for a given cryptocurrency, the costs are the same across all ESPs ($\gamma_{k,m} = \gamma_{k,m'}$ for all m, m'), and service rates are different from each other ($\mu_{k,m} \neq \mu_{k,m'}$ for any $m \neq m'$), then: (1) only one ESP will be used, and (2) the ESP that will be used will be the one with the highest service rate.*

Proof. Let us assume that for a given cryptocurrency, say k, the cost for using each ESP is the same ($\gamma_{k,m} = \gamma_{k,m'}$ for all m, m'), and the service rate associated to each ESP is different ($\mu_{k,m} \neq \mu_{k,m'}$ for all m, m'). Let us assume that there exists at equilibrium ℓ^* two elements $\ell_{k,m}$ and $\ell_{k,m'}$ such that $\ell^*_{k,m} > 0$ and $\ell^*_{k,m'} > 0$, for a pair of ESPs (m, m'), with $m \neq m'$. Then, according to (28a) $\mu_{k,m} = \mu_{k,m'}$, which by a contradiction argument implies (1). Moreover, if miners invest only in one ESP, then according to (28b), that ESP will be the one with the highest $\mu_{k,m}$, establishing (2). □ □

Note that Theorems 6.2 and 6.3 are the mean field results equivalent to Conjecture 4.4 and Theorem 4.3. It is often the case that structural results are easier to be derived under the mean field approximation, as further illustrated through the following additional structural results.

6.3 Blockchain mining collapse

Next, we characterize conditions under which the mining costs preclude miners from investing their computational resources into the mining game.

Definition 6.4. A given cryptocurrency k dies under equilibrium ℓ^* if $\ell^*_{k,m} = 0$ for $1 \leq m \leq M$.

Theorem 6.5. *If no two pairs of ESPs are colinear with respect to cryptocurrency k, and*

$$\max_{m:1\leq m\leq M} \left\{ \frac{q_k\left(\mu_{k,m}N\right)}{N} - \gamma_{k,m} \right\} < 0 \tag{33}$$

then cryptocurrency k dies under all equilibria.

Proof. Equations (28a)-(28d) imply that if

$$\mathcal{U}_{k,m}(\ell) < 0, \text{for all } m \in \{1, \ldots, M\} \text{ and } \ell \text{ such that } \sum_m \ell_{k,m} \leq N \tag{34}$$

then cryptocurrency k dies. Condition (34) is satisfied if:

$$\max_m \left\{ \max_{\sum_{m'} \ell_{k,m'} \leq N} \mathcal{U}_{k,m}(\ell) \right\} < 0. \tag{35}$$

Next, we further characterize the solution of the fractional pseudo-concave optimization problem

$$\max_{\sum_{m'} \ell_{k,m'} \leq N} \mathcal{U}_{k,m}(\ell) \tag{36}$$

We denote by $\ell^\star(k, m')$ the optimal load vector for the previously defined optimization problem, for a given pair (k, m'), where $1 \leq m' \leq M$. The first order optimality conditions that must be satisfied by the solution $\ell^\star(k, m')$ of the problem above entail the existence of $\lambda(k, m') \in \mathbb{R}$ such that:

$$\mu_{k,m'} q_k \left(\sum_{m''} \mu_{k,m''} \ell^\star_{k,m''}(k, m') \right) = \lambda(k, m'), \text{ if } \ell^\star_{k,m''}(k, m') > 0, \tag{37}$$

$$\mu_{k,m} q_k \left(\sum_{m''} \mu_{k,m''} \ell^\star_{k,m''}(k, m') \right) \leq \lambda(k, m'), \text{ if } \ell^\star_{k,m''}(k, m') = 0. \tag{38}$$

Equations (37)-(38) together with the fact that no two pairs of ESPs are colinear with respect to cryptocurrency k imply that the optimal load is given by,

$$\ell^{\star}_{k,m''}(k,m') = \begin{cases} N, & \text{if } m'' = m' \\ 0, & \text{otherwise.} \end{cases} \tag{39}$$

Therefore, $\mathcal{U}_{k,m'}(\ell^{\star}(k,m')) = \frac{q_k(\mu_{k,m'}N)}{N} - \gamma_{k,m'}$, which together with (35) concludes the proof. □ □

Then, we consider the most extreme scenario, wherein miners have no incentives to mine any of the existing cryptocurrencies.

Definition 6.6. Blockchain mining collapses if there is an equilibrium under which all cryptocurrencies die.

Corollary 6.7. *If, for each k, there are no two pairs of ESPs that are colinear with respect to cryptocurrency k, and if for all m and k,*

$$1 - \exp(-T_k\mu_{k,m}N)) - N\gamma_{k,m} < 0, \tag{40}$$

then blockchain mining collapses. Note that there exists an $\overline{N}$ such that for every $N > \overline{N}$ the condition above is satisfied. Morevover, if $N\gamma_{k,m} > 1$ for all k and m, the condition above also holds.

Proof. The proof follows directly from Theorem 6.5. Indeed, blockchain mining collapses if

$$\max_m \left\{ \frac{q_k\left(\mu_{k,m}N\right)}{N} - \gamma_{k,m} \right\} < 0, \forall k. \tag{41}$$

The condition above is equivalent to

$$\frac{q_k\left(\mu_{k,m}N\right)}{N} - \gamma_{k,m} < 0, \forall (m,k), \tag{42}$$

which concludes the proof. □ □

6.4 Existence and uniqueness of equilibrium

Concerning the existence and the uniqueness of the equilibrium, we will restrict to the scenario wherein for each cryptocurrency k, the cost across all ESPs are the same ($\gamma_{k,m} = \gamma_{k,m'}$ for all m, m'), and the service rate associated to each ESP is different ($\mu_{k,m} \neq \mu_{k,m'}$ for all m, m'). As shown in Theorem 6.3, under equilibrium, for each cryptocurrency, at most one ESP will be used to actively mine. Let $m(k) := \max_{m'} \mu_{k,m'}$. ESP $m(k)$ is the only candidate to be actively used for mining cryptocurrency k. Therefore, the equilibrium conditions (28a)-(28d) simplify to:

$$\mathcal{U}_{k,m(k)}(\ell^{\star}) = \mathcal{U}_{k'',m(k'')}(\ell^{\star}), \quad \text{if } \ell^{*}_{k,m(k)} > 0, \quad \ell^{*}_{k'',m(k'')} > 0, \quad \forall k, k'', \tag{43a}$$

$$\mathcal{U}_{k,m(k)}(\ell^{\star}) \geq \mathcal{U}_{k'',m(k'')}(\ell^{\star}), \quad \text{if } \ell^{*}_{k,m(k)} > 0, \quad \ell^{*}_{k'',m(k'')} = 0, \quad \forall k, k'', \tag{43b}$$

$$\mathcal{U}_{k,m(k)}(\ell^{\star}) \leq 0, \quad \text{if } \ell^{*}_{k,m(k)} = 0, \quad \forall k, \tag{43c}$$

$$\sum_k \ell^{\star}_{k,m(k)} \leq N. \tag{43d}$$

Theorem 6.8. *The non-atomic game under symmetric costs considered in this section admits at most one interior equilibrium, which is the solution to the following optimization problem*

$$argmax \sum_{k=1}^{K} \int_{\epsilon}^{\ell_{k,m(k)}} \frac{q_k(\mu_{k,m(k)}x)}{x} dx - \gamma_{k'}\ell_{k,m(k)}, \tag{44}$$

$$subject\ to \sum_{k} \ell_{k,m(k)} \leq N, \quad \ell_{k,m(k)} \geq \epsilon \tag{45}$$

Proof. First, note that if there exists an interior solution to the optimization problem (44)-(45), i.e., if each load is strictly greater than ϵ, then the first-order optimality conditions of the posed optimization problem are given by (43a)-(43d), which implies a one-to-one correspondence between the solution to the optimization problem and an equilibrium of the non-atomic game. In addition, note that for all k and m, $\frac{q_k(\mu_{k,m(k)}\ell_{k,m(k)})}{\ell_{k,m(k)}}$ is a decreasing function in $\ell_{k,m(k)} > 0$. Therefore the function $\int_{\epsilon}^{\ell_{k,m(k)}} \frac{q_k(\mu_{k,m(k)}x)}{x} dx - \gamma_{k'}\ell_{k,m(k)}$ is stricly concave and the optimization problem posed above has a unique solution, as all the functions are strictly concave. □ □

7 PARALLEL COMPUTATIONS: AUCTIONS AND CONTINUOUS ACTIONS

The models studied so far assumed that a puzzle to be solved by a miner is sent entirely to a single ESP both in the context of competition over ESPs (Section 4) as well as for the competition over cryptocurrencies (Section 5). In this section we consider a game in which each miner can decide how much to bid for the computation power proposed by the ESP. The load on an ESP need not be a multiple of its service rate anymore.

Assumptions In this section we assume $q_k = 1$. This corresponds to a fine grained adjustment of puzzle complexity (see Section 2.1 and Table 1). In addition, we consider a one-to-one correspondence between miners and ESPs and a single cryptocurrency, i.e., $K = 1$. Then, $\ell_{\star,m} = 1$ for $m = 1, \ldots, M$.

Let x_m denote the value bid by the miner corresponding to ESP m. We have a minimum constraint $x_m \geq \epsilon$ for all m. We also assume that the service rate from ESP m requested by miner m, $\mu_{\star,m}$, equals the value bid by miner m, x_m, i.e., $\mu_{\star,m} = x_m$. Then, (2) reduces to

$$\eta = \sum_{j=1}^{M} x_j. \tag{46}$$

7.1 Basic model

The probability that miner m is the first to solve the puzzle is

$$P_m = \frac{x_m}{\eta} = \frac{x_m}{\sum_{j=1}^{M} x_j}, \tag{47}$$

which is the miner *expected gain* that can be contrasted against (6). The total cost for miner m is $x_m\gamma$, where γ is a constant. The utility for player m is thus

$$U_m(x) = \frac{x_m}{\sum_{j=1}^{M} x_j} - x_m\gamma. \tag{48}$$

The utility above gives rise to the following Unconstrained Game,

$$\text{Unconstrained Game: } \max_{x_m} \frac{x_m}{\sum_{i=1}^{M} x_i} - x_m\gamma \tag{49}$$

The main result of this section establishes the uniqueness of the Nash equilibrium of the Unconstrained Game.

Theorem 7.1 (continuous actions). *(i) For any strictly positive value of γ, the above game has a unique Nash equilibrium and (ii) U_m is concave in x_m.*

Proof. This was etablished in [4] using a modification of the diagonal strict concavity property. □ □

The game presented above was introduced and studied in [13]. In what follows, we extend the results from [13] to account for physical constraints on the resources consumed by the population of miners.

7.2 Normalized equilibrium: physical bounds on resources and shadow prices

The games we have seen so far involved orthogonal constraints. By that we mean that the actions that a miner can use do not depend on the actions of other miners. We next introduce a capacity constraint. Formally, for some constant V which bounds the total service rate from all ESPs, we introduce the following game with capacity constraints. For each player m,

$$\text{Constrained Game: } \max_{x_m} \frac{x_m}{\sum_{i=1}^{M} x_i} \tag{50}$$

$$\sum_{j=1}^{M} x_j \leq V \tag{51}$$

Note that in the game above we assume that each player maximizes the probability of being the first to successfully solve the puzzle, P_m, under constraints on the total amount bid by all players. Recall that the amount bid by a player is proportional to the amount of resources invested by that player to mine.

Capacity constraints may represent physical bounds on resources, such as bounded power, or resources that are bounded by regulation. For example, legislation may impose bounds on the power consumption. With the additional capacity constraints, the Nash equilibrium is no more unique and there may in fact be an infinite number of equilibria. We call this the *game with capacity constraints*.

Let y be an equilibrium of the Constrained Game and let $y_{[-m]}$ denote the action vectors of all miners other than m. Note that for each m, U_m is concave in y_m. Then, by the KKT theorem, there is a Lagrange multiplier $\lambda_m(y_{[-m]})$ such that y_m maximizes the Lagrangian

$$\mathcal{L}_m(y_m) = \frac{y_m}{\sum_{j=1}^{M} y_j} - \lambda_m(y_{[-m]}) \left(\sum_{j=1}^{M} y_j - V \right) \tag{52}$$

and

$$\lambda_m(y_{[-m]}) \left(\sum_{j=1}^{M} y_j - V \right) = 0. \tag{53}$$

The last condition is referred to as *complementarity property*. We call the game with utilities given by Lagrangians $\mathcal{L}_m$ as the *relaxed game* or *Lagrangian game*.

$$\text{General Relaxed Game:} \tag{54}$$

$$\max_{x_m} \quad \mathcal{L}_m(x_m) = \frac{x_m}{x_m + \sum_{j=1, j\neq m}^{M} y_j} - \lambda_m(y_{[-m]}) \left(x_m + \sum_{j=1, j\neq m}^{M} y_j - V \right) \tag{55}$$

A simplified version of the General Relaxed Game will be instrumental in the upcoming section to prove properties about the Constrained Game.

7.2.1 Shadow prices and normalized equilibrium. The Lagrange multipliers can be interpreted as shadow prices: if a price is set on miner m such that when other players are at equilibrium, the miner pays $y_m \lambda_m(y_{[-m]})$ for its use of cryptocurrency, then y is an equillibrium in the game with capacity constraints. Yet this pricing is not scalable since for the same use of the resources the price may vary from user to user and it further depends on the the chosen equilibrium. For billing purposes one would prefer λ_m not to depend on y nor on m, but to be a constant.

Does there exist a constant Lagrange multiplier λ independent of strategies of the payers and of the idendity m of the player, along with an associated equilibrium y for the corresponding relaxed game? If the answer is positive then y is called a *normalized equilibrium* [3, 19, 44]. Then, λ is the Lagrange multiplier corresponding to the normalized equilibrium.

The Constrained Game admits an infinite number of equilibria. Nonetheless, as will be shown in the sequel, it admits a unique normalized equilibrium. To prove that claim, we translate global constraints from the Constrained Game into local penalties (associated to the Lagrange multipliers) in a simpler version of the General Relaxed Game, referred to as the Relaxed Game.

$$\text{Relaxed Game: } \max_{x_m} \quad \mathcal{L}_m(x_m) = \frac{x_m}{x_m + \sum_{j=1, j\neq m}^{M} y_j} - \lambda \left(x_m + \sum_{j=1, j\neq m}^{M} y_j - V \right) \tag{56}$$

Whereas the actions of the players are coupled through hard constraints in the Constrained Game, the local penalties (and corresponding Lagrange multipliers) allow us to decouple the actions of the players in the Relaxed Game.

Definition 7.2. A symmetric game is a game wherein the functional dependency of the utility with respect to the actions is the same for all players.

Note that the Relaxed Game is a symmetric game, whereas the General Relaxed Game is not. In the former, the constant λ that appears in the utility function is fixed and given, whereas in the latter it is player-dependent.

Let $\mathcal{E}_0$ and $\mathcal{E}_1$ be the set of equilibria of the General Relaxed Game and of the Relaxed Game, respectively (see Table 4 and Figure 5). As mentioned earlier, $\mathcal{E}_0$ in general contains multiple elements, i.e., the Constrained Game admits multiple equilibria. Then, our initial aim was to establish necessary and sufficient conditions for $\mathcal{E}_1$ to be a singleton, i.e., for the Constrained Game to admit a single normalized equilibrium. However, we were only able to establish those conditions for a symmetric normalized equilibrium to the Constrained Game. For this reason, in the upcoming section we restrict to symmetric equilibria of the Relaxed Game and the corresponding symmetric normalized equilibria of the Constrained Game, and refer to the corresponding set as $\mathcal{E}_2$. We will show that $\mathcal{E}_2$ is a singleton, and we leave the necessary and sufficient conditions for $\mathcal{E}_1$ to be a singleton as subject for future work.

7.2.2 Existence and uniqueness of symmetric normalized equilibrium. Next, we establish the existence and uniquenesss of the normalized equilibrium. We start by showing a condition under which the game admits a symmetric equilibrium.

Definition 7.3. A symmetric equilibrium $\tilde{y}^\star$ is an equilibrium wherein $y_i = \tilde{y}^\star$ for all i, $i = 1, \ldots, M$.

Theorem 7.4 (symmetric equilibrium). *If*

$$\gamma = \frac{M-1}{MV} \tag{57}$$

where V is a constant, fixed and given, then

$$\tilde{y}^\star = \frac{V}{M} = \frac{M-1}{M^2 \gamma} \tag{58}$$

is the unique symmetric equilibrium to the Unconstrained Game.

Proof. We replace x_m by $\tilde{y}^\star$ in equation (48) to obtain

$$U_m(\tilde{y}^\star) = \frac{\tilde{y}^\star}{\tilde{y}^\star + \sum_{j=1, j\neq m}^{M} x_j} - \tilde{y}^\star \gamma. \tag{59}$$

The symmetric equilibrium is obtained by differentiating (59) with respect to $\tilde{y}^\star$ and equating the resulting expression to 0,

$$\frac{1}{\tilde{y}^\star + \sum_{j=1, j\neq m}^{M} x_j} - \frac{\tilde{y}^\star}{\left(\tilde{y}^\star + \sum_{j=1, j\neq m}^{M} x_j\right)^2} - \frac{M-1}{MV} = 0 \tag{60}$$

$$\left(\sum_{j=1, j\neq m}^{M} x_j\right) - \frac{M-1}{MV}\left(\tilde{y}^\star + \sum_{j=1, j\neq m}^{M} x_j\right)^2 = 0 \tag{61}$$

Noting that the same argument holds for all players, we conclude that $\tilde{y}^\star = V/M$ is a symmetric equilibrium. Indeed, setting $x_m = V/M$ for $m = 1, \ldots, M$ equation (61) is satisfied. □ □

It is worth noting that (58) corresponds to a special case of equation (4) in [13], and the proposition above follows from the main proposition in [13]. Indeed, starting from equation (4) in [13] and replacing R, n, $c_{(n)}$ and c_i by 1, M, γM and γ we obtain (58). In what follows, we extend the analysis of [13], which encompasses unconstrained games, to the setup wherein constraints are active.

Corollary 7.5 (normalized equilibrium). *If*

$$\lambda = \frac{M-1}{MV} \tag{62}$$

where V is a constant, fixed and given, determining the system constraints, then

$$\tilde{y}^\star = \frac{V}{M} = \frac{M-1}{M^2\lambda} \tag{63}$$

is an equilibrium to the Relaxed Game *and a normalized equilibrium to the* Constrained Game.

Proof. The proof follows by noting that the equilibrium corresponding to (59) in the proof of Theorem 7.4 is also an equilibrium corresponding to the utility function (52) of the Relaxed Game. This is because the utility of the Relaxed Game can be obtained from (59) replacing γ, $\tilde{y}^\star$ and x_j by λ, y_m and y_j, respectively, for $j \neq m$, and adding a term $-\lambda(\sum_{j\neq m} y_j - V)$. Note that after adding this term, the equilibrium of the original Unconstrained Game is also an equilibrium of the modified game since the new utility differs from the previous one by terms that do not depend on $y^\star = y_m$, the action of player m. □ □

Next, we establish the main result of this section. Figure 4 summarizes the proof strategy. The proof follows by relating the symmetric equilibrium to the Unconstrained Game into an equilibrium to the Relaxed Game and a normalized equilibrium to the Constrained Game.

Theorem 7.6 (normalized equilibrium). *There exists a unique symmetric normalized equilibrium to the* Constrained Game*, i.e., the set $\mathcal{E}_2$ is a singleton.*

Proof idea. The proof is presented in Appendix B, and the proof idea is summarized in Figure 4. We know that for any γ there is a unique Nash equilibrium $y(\gamma)$ to the Unconstrained Game (Theorem 7.1). We show that this defines a unique symmetric equilibrium to the Relaxed Game with Lagrange multiplier $\lambda(\gamma)$. We further

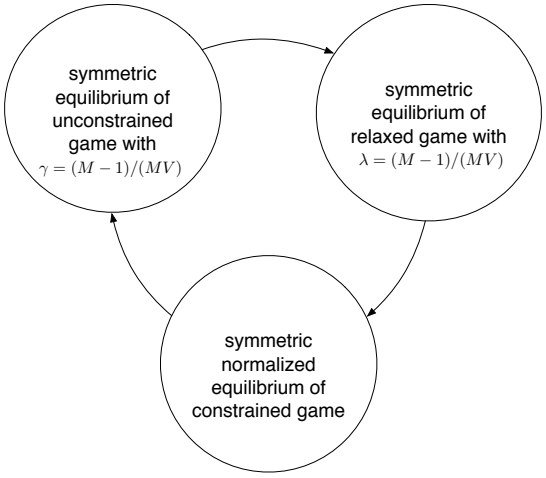

Fig. 4. Relationship between Unconstrained Game, Relaxed Game and Constrained Game. Arrows indicate that equilibrium of a game implies equilibrium of the other. Theorem 7.6 establishes that the uniqueness of the equilibrium to the Unconstrained Game implies the uniqueness of the symmetric equilibrium to the Relaxed Game and uniqueness of the symmetric normalized equilibrium to the Constrained Game.

Table 4. Normalized and symmetric equilibria

Set of equilibria	Description	Specific description
$\mathcal{E}_0$	general equilibria to general game	general equilibria to General Relaxed Game, satisfying complementarity conditions, i.e., general equilibria to Constrained Game
$\mathcal{E}_1$	general equilibria to symmetric game	general equilibria to Relaxed Game, satisfying complementarity conditions, i.e., normalized equilibria to Constrained Game
$\mathcal{E}_2$	symmetric equilibria to symmetric game	symmetric equilibria to Relaxed Game, satisfying complementarity conditions, i.e., symmetric normalized equilibria to Constrained Game

show that there is a unique $\gamma^\star$ for which the capacity constraints hold with equality. This implies that $y(\gamma^\star)$ is a normalized equilibrium to the Constrained Game where $\lambda(\gamma^\star)$ is the corresponding Lagrange multiplier. □

We have just shown that the symmetric equilibrium to the Constrained Game is unique, i.e., $\mathcal{E}_2$ is a singleton. It remains to show the conditions under which the general equilibrium (symmetric or asymmetric) to the Constrained Game is unique. *What are the necessary and sufficient conditions under which $\mathcal{E}_1$ is also a singleton?*

The fact that there does not exist asymmetric equilibria to certain class of symmetric games was shown in [38]. If we were able to establish conditions under which the symmetric Constrained Game admits only symmetric equilibrium, we would also be able to guarantee uniqueness across general equilibra. However, the conditions of [38] to show that certain symmetric games admit only symmetric equilibria do not hold in our games. In particular, the sufficient conditions established by [38] state that the utility must be decreasing in the aggregated actions of all players and in the action of each of the players. In the Constrained Game, in contrast, given

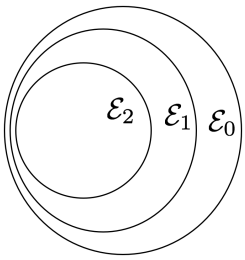

Fig. 5. In this paper, we focus on symmetric equilibria to a symmetric game (set $\mathcal{E}_2$ above). General equilibria to symmetric or general games (sets $\mathcal{E}_1$ and $\mathcal{E}_0$, respectively) may not be unique, whereas $\mathcal{E}_2$ is a singleton.

player j, the utility is decreasing in the actions of the others players, but increasing in the action of player j. The probability that j is the first to solve the puzzle is given by,

$$P_j = \frac{y_j}{y_j + \sum_{i \neq j} y_i} \tag{64}$$

As y_j increases, the probability that j is the first to solve the puzzle increases, as the numerator increases, and the utility of player j correspondingly increases. Correspondingly, the probability that any other player i is the first to solve the puzzle decreases, as the denominator in P_i increases as y_j grows.

The analysis in this section implies that players have less incentives to invest in blockchain mining when constraints are more stringent [9]. Indeed, as V decreases, i.e., as constraints are more stringent, shadow prices $\gamma^\star$ grow and the investments in blockchain mining, reflected by $y^\star$, decrease (see eq. (58)). We further discuss general aspects related to the blockchain ecosystem in Section 8.

7.2.3 Global constraints and local costs. In Section 7.2.2 we considered the setup wherein each player m maximized a utility whose value increases as its bid, x_m, increases. The players were restricted by global constraints.

Next, we consider the general setup wherein players are constrained both by global constraints, as in the previous section, as well as local constraints. Then, players face the Constrained Game with Local Costs. The constrained game with local costs accounts for both global constraints (through a hard constraint) and local costs (through a term that penalizes large values of x_m in the utility function),

$$\text{Constrained Game with Local Costs: } \max_{x_m} \frac{x_m}{\sum_{i=1}^M x_i} - \gamma x_m \tag{65}$$

$$\sum_{j=1}^M x_j \leq V \tag{66}$$

The Lagrangian of the Constrained Game with Local Costs is given by

$$\mathcal{L}_m(x_m) = \frac{x_m}{\sum_{j=1}^M x_j} - \gamma x_m - \lambda \left(\sum_k x_k - V \right) \tag{67}$$

In particular, note that if $\gamma = (M-1)/(MV)$ the equilibrium presented in Corollary 7.5 is also a normalized equilibrium to the Constrained Game with Local Costs. Nonetheless, for arbitrary values of γ the conditions for existence and uniqueness of the normalized equilibrium to the Constrained Game with Local Costs remain open. We envision that the argument presented in the previous section regarding existence and uniqueness of normalized equilibrium can be adapted to this setup, but leave the proof as subject for future work.

8 DISCUSSION

Positive and negative externalities. In the models proposed in this paper, we assumed that users who contribute to the system by mining cryptocurrencies generate negative externalities towards their mining peers. Indeed, the competition among miners is a very fundamental aspect of the mining process [13]. Nonetheless, by incorporating more miners, the blockchain becomes more robust [16]. Such robustness, in turn, may translate into an increase in the real value of the cryptocurrency under consideration [10, 41, 43, 48]. Therefore, by increasing the pool of miners, each miner is also contributing with positive externalities towards the system, and we leave such aspect as subject for future work.

Mining pools. Mining pools play a key role in todays' public blockchain systems [14, 52].[3] The competition analyzed in this paper applies to mining pools under two scenarios. First, from the perspective of the mining pool, it can use cloud resources for mining purposes. Therefore, the mining pools assume the role of players as considered in this work. Alternatively, the players are the end users, who contract mining pool services. Then, mining pools assume the role of ESPs. In the first case, we consider competition among mining pools, at the macro level, and in the latter case, we consider the micro-competition among end-users.

Figure 6 illustrates the hashrate distribution over Bitcoin, as of 24 October 2019.[4] Note that a significant portion of the hashrate is originated from four mining pools. According to Conjecture 4.4 and Theorem 6.2, the proposed model suggests that only two major mining pools would have a role in the network. A discrepancy between model predictions and hashrate distribution over Bitcoin may occur if the market is not stabilized or agents are not fully rational. In addition, note that the proposed model only accounts for the competition among miners, and does not take into consideration the positive externalities produced by the miners (see Appendix A). Such positive externalities may motivate a longlasting equilibrium wherein four mining pools take place, as positive externalities naturally serve as incentives for multiple pools to coexist. Our work serves as a plausible model to justify the relatively small number of mining pools, which we posit as being due to the competition among those [6, 8, 12, 17, 18, 28].

Multi-cryptocurrency ecosystem. In the cryptocurrency ecosystem, large mining pools typically decide, dynamically, which blockchain to mine. Such decisions are made based on different thresholds related to the value of the cryptocurrencies and the costs for mining (mining complexity). The churn of computational power across blockchains is a well-known source of price volatility, and different mechanisms have been developed to counteract migrations of miners across platforms [50]. One of those mechanisms is referred to as emergency difficulty adjustment (EDA), which reduces the difficulty of the puzzle when there are not many miners in the system, preventing the blockchain from dying.

Puzzle complexity. In Bitcoin, puzzle difficulty (complexity) is dynamically adjusted so that the time to mine a block varies between certain pre-established time bounds. Bitcoin target block generation rate is of 10 minutes. In theory, due to the dynamic adjustment of puzzle complexity, Bitcoin throughput (number of blocks generated per time unit) does not depend on the number of miners. An increase in the number of miners increases the time between generation of blocks per miner [33, 53]. In [24], the authors argue in favor of adjusting the frequency at which blocks are generated as a function of the congestion in the network.

Users fees. Users pay fees to have their blocks mined. Such fees impact the competition among miners, as they serve as incentives for mining. The higher the fees offered by users, the larger the expected number of miners. In this paper, we have not accounted for the role of blockchain users in the competition among miners. We envision that the interplay between users and miners leads to complex dynamics, which should be studied in light of the tension between positive and negative externalities discussed in Appendix A.

[3] For instance, https://miningpoolhub.com/.
[4] https://www.blockchain.com/pools

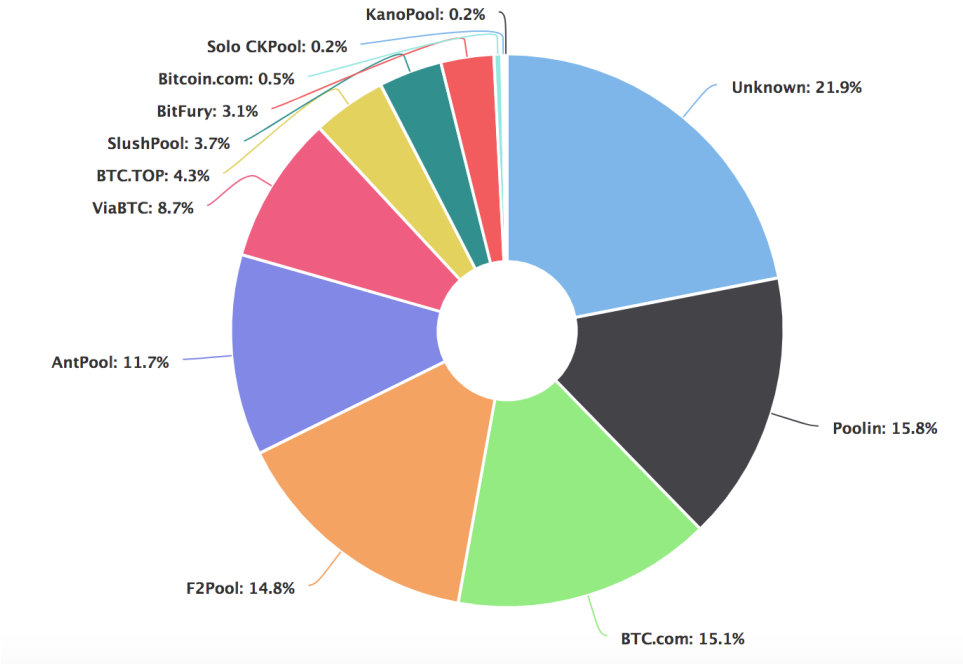

Fig. 6. Bitcoin hashrate distribution as of 24 October, 2019.

9 RELATED WORK

There is a vast literature investigating game theoretical aspects of blockchain systems [1, 7, 20, 24, 26, 29–31, 39, 49, 52]. Nonetheless, the literature on congestion games applied to such systems is scarce. In particular, to the best of our knowledge, there is no prior work investigating the competition at the network edge among miners as a congestion game, and its connection to multi-cryptocurrency markets.

Congestion games have been applied in the field of networking to account for security aspects [32], link congestion [25] and pricing of infrastructures and users [21]. In [24], the authors study Bitcoin as a congestion game, where the congestion occurs due to an increase in the number of transaction requests from users. In particular, the authors abstract away from several aspects of the competition between miners. In this paper, in contrast, we focus on the competition between miners.

[49] adopted the framework of congestion games to model competition between miners of multiples cryptocurrencies who try to maximize utilities by choosing which puzzle (cryptocurrency) to mine (the work was then extended at [20]). The authors prove that there is no standard potential function for the game they propose, but that an ordinal potential always exists, implying that best response converges to a pure Nash equilibrium. Our work captures different aspects of the problem, and is complementary to [49]. An important similarity between the two works consists of establishing conditions under which pure Nash equilibria exist even when the game does not admit a standard potential function. The major differences between our work and [49] are: 1) in the modeling of the probability to succeed in solving a puzzle (see Section 8); 2) in the ESP decision, which is out of the scope of [49]; 3) in the action space (mining power), which is continuous in [49], precluding the use of crowding game results, and discrete in this paper (except in Section 7), allowing us to rely on [34] to prove existence of pure

Nash equilibria. We refer the reader to [49, 50] for additional references on the multi-cryptocurrency ecosystem and its security challenges.

m[47] initiates a preliminary study on the so-called price of crypto-anarchy based on the models introduced here. In this paper, in contrast, we focused on the distributed competition among miners, and have not assessed the loss of efficiency due to the absence of a central controller to perturb the competition. We envision that a more in-depth study of the loss of efficiency due to the lack of controllers, and a study of the role of authorities in regulating the crypto-market, e.g., as indicated in Section 7.2 (see also [9] and [15]), is an important open aspect, and leave that topic as subject for future work.

10 CONCLUSION

Competition among miners is at the core of public blockchain systems. Competition is one of the most fundamental elements ensuring that miners will strive to reach a consensus about the current state of the blockchain. We modeled the competition over several ESPs and over several blockchains characterizing multiple cryptocurrencies as a non-cooperative game. Then, we specialized our game to two cases: the ESP connection game and the cryptocurrency selection game. For each game, we showed properties of the Nash equilibrium. In particular, leveraging results about congestion games, we establish the existence of pure Nash equilibria and characterize such equilibria through problems that admit efficient algorithmic solutions.

We believe that this work opens up a number of interesting directions for future work. In particular, we did not account for strategic decisions related to punishment and cooperation between miners over repeated games. Those games naturally emerge in the sequential solution of multiple puzzles. The study of those is left as subject for future work.

Acknowledgment Research conducted within the joint Lab between INRIA and Nokia Bell Labs. Part of the work was performed within the THANES Associate Team, jointly supported by Inria (France) and FAPERJ (Brazil). DSM was partially supported by CAPES and CNPq. This paper extends our conference version of the paper whhich appeared in [5]. In particular, Section 7 is novel as well as the background discussion on mining competition, accounting for dynamic puzzle complexity (Section 2).

REFERENCES

[1] Kobbane Abdellatif and Charkaoui Abdelmouttalib. 2018. Graph-Based Computing Resource Allocation for Mobile Blockchain. In *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 1–4.

[2] Eitan Altman, Richard Combes, Zwi Altman, and Sylvain Sorin. 2011. Routing games in the many players regime.. In *VALUETOOLS*. 525–527.

[3] Eitan Altman, Mandar Datar, Gerard Burnside, and Corinne Touati. 2019. Normalized Equilibrium in Tullock Rent Seeking Game. In *International Conference on Game Theory for Networks*. Springer, 109–116.

[4] Eitan Altman, Manjesh Kumar Hanawal Hanawal, and Rajesh Sundaresan. 2016. Generalising diagonal strict concavity property for uniqueness of Nash equilibrium. *Indian Journal of Pure and Applied Mathematics* 47, 2 (2016), 213–228. https://doi.org/10.1007/s13226-016-0185-4

[5] Eitan Altman, Alexandre Reiffers-Masson, Daniel Sadoc Menasché, Mandar Datar, Swapnil Dhamal, and Corinne Touati. 2018. Mining competition in a multi-cryptocurrency ecosystem at the network edge: A congestion game approach. In *SOCCA 2018 - 1st Symposium on Cryptocurrency Analysis*, IFIP (Ed.). Toulouse, France, 1–4. https://hal.inria.fr/hal-01906954

[6] Nick Arnosti and S Matthew Weinberg. 2018. Bitcoin: A Natural Oligopoly. In *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. https://par.nsf.gov/biblio/10097713.

[7] Sarah Azouvi and Alexander Hicks. 2019. SoK: Tools for Game Theoretic Models of Security for Cryptocurrencies. *arXiv preprint arXiv:1905.08595* (2019).

[8] Qianlan Bai, Xinyan Zhou, Xing Wang, Yuedong Xu, Xin Wang, and Qingsheng Kong. 2019. A deep dive into blockchain selfish mining. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[9] BBC News. 2019. Bitcoin mining ban considered by China's economic planner. *BBC News* (April 2019). https://www.bbc.com/news/technology-47867031.

[10] Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. 2019. The blockchain folk theorem. *The Review of Financial Studies* 32, 5 (2019), 1662–1715.
[11] George Bissias, Brian N Levine, and David Thibodeau. 2019. Greedy but Cautious: Conditions for Miner Convergence to Resource Allocation Equilibrium. *arXiv preprint arXiv:1907.09883* (2019).
[12] Lin William Cong, Zhiguo He, and Jiasun Li. 2019. *Decentralized mining in centralized pools.* Technical Report. National Bureau of Economic Research.
[13] Nicola Dimitri. 2017. Bitcoin mining as a contest. *Ledger* 2 (2017), 31–37.
[14] Ittay Eyal. 2015. The miner's dilemma. In *Security and Privacy*. IEEE, 89–103.
[15] Jesús Fernández-Villaverde and Daniel Sanches. 2016. Can currency competition work? *Journal of Monetary Economics* 106 (2016), 1–15.
[16] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin backbone protocol. In *Theory and Applications of Crypto Techniques*. Springer, 281–310.
[17] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer. 2018. Decentralization in Bitcoin and Ethereum Networks. In *Proc. of the Financial Cryptography and Data Security Conference*.
[18] Arthur Gervais, Ghassan O Karame, Vedran Capkun, and Srdjan Capkun. 2014. Is bitcoin a decentralized currency? *IEEE security & privacy* 12, 3 (2014), 54–60.
[19] Arnob Ghosh, Laura Cottatellucci, and Eitan Altman. 2015. Normalized Nash equilibrium for power allocation in cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking* 1, 1 (2015), 86–99.
[20] Guy Goren and Alexander Spiegelman. 2019. Mind the Mining. *arXiv preprint arXiv:1902.03899* (2019).
[21] Refael Hassin and Moshe Haviv. 1997. Equilibrium threshold strategies: The case of queues with priorities. *Operations Research* 45, 6 (1997), 966–973.
[22] Refael Hassin and Moshe Haviv. 2003. *To queue or not to queue: Equilibrium behavior in queueing systems*. Vol. 59. Springer Science & Business Media.
[23] Alain Haurie and Patrice Marcotte. 1985. On the relationship between Nash—Cournot and Wardrop equilibria. *Networks* 15, 3 (1985), 295–308.
[24] Gur Huberman, Jacob D Leshno, and Ciamac C Moallemi. 2017. Monopoly without a monopolist. *SSRN* (2017).
[25] Ramesh Johari and John N Tsitsiklis. 2003. Network resource allocation and a congestion game. In *Allerton*.
[26] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain mining games. In *Conf. Economics and Computation*. ACM.
[27] Fabrice Lebeau, Corinne Touati, Eitan Altman, and Nof Abuzainab. 2019. The Social Medium Selection Game. In *Network Games, Control, and Optimization*. Springer, 249–269. https://hal.inria.fr/hal-01249195/file/social-infocom.pdf.
[28] Jacob Leshno and Philipp Strack. 2019. Bitcoin: An Impossibility Theorem for Proof-of-Work based Protocols. *SSRN* (2019).
[29] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A Survey on Applications of Game Theory in Blockchain. *arXiv preprint arXiv:1902.10865* (2019).
[30] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A Survey on Blockchain: A Game Theoretical Perspective. *IEEE Access* 7 (2019), 47615–47643.
[31] June Ma, Joshua S Gans, and Rabee Tourky. 2018. *Market structure in bitcoin mining*. Technical Report. National Bureau of Economic Research.
[32] Patrick Maillé, Peter Reichl, and Bruno Tuffin. 2011. Interplay between security providers, consumers, and attackers: a weighted congestion game approach. In *Conf. Decision Game Theory for Security*. Springer.
[33] Dmitry Meshkov, Alexander Chepurnoy, and Marc Jansen. 2017. Revisiting Difficulty Control for Blockchain Systems. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 429–436.
[34] Igal Milchtaich. 1996. Congestion games with player-specific payoff functions. *Games and economic behavior* 13, 1 (1996), 111–124.
[35] Igal Milchtaich. 1998. Crowding games are sequentially solvable. *Intl. Journal Game Theory* 27, 4 (1998), 501.
[36] Dov Monderer and Lloyd S Shapley. 1996. Potential games. *Games and economic behavior* 14, 1 (1996), 124–143.
[37] David Morris. 2018. Difficulty adjustment is why Bitcoin will never die. *https://breakermag.com/difficulty-adjustment-is-why-bitcoin-will-never-die/* (2018).
[38] A Orda, R Rom, and N Shimkin. 1993. Competitive routing in multi-user environments. *IEEE/ACM Transactions on Networking* 1, 5 (1993), 510–521.
[39] Nikolaos Papadis, Sem Borst, Anwar Walid, Mohamed Grissa, and Leandros Tassiulas. 2018. Stochastic models and wide-area network measurements for blockchain design and analysis. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2546–2554.
[40] B Peter Pashigian and Eric D Gould. 1998. Internalizing externalities: the pricing of space in shopping malls. *The Journal of Law and Economics* 41, 1 (1998), 115–142.
[41] Julien Prat and Benjamin Walter. 2018. An equilibrium model of the market for bitcoin mining. *SSRN* (2018). CESifo Working Paper Series No. 6865.

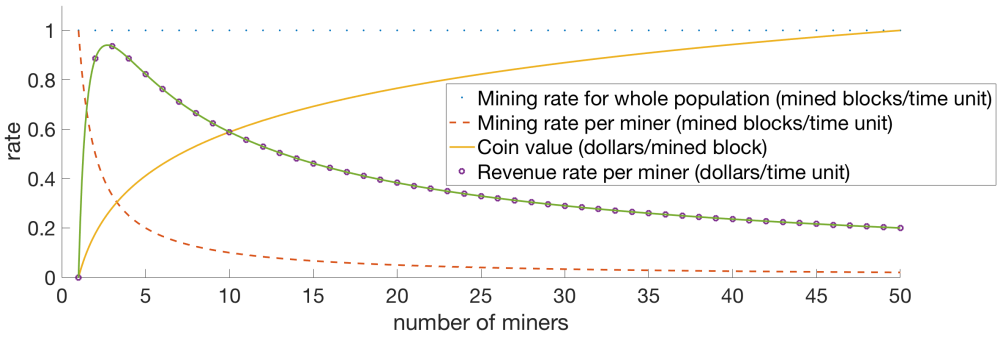

Fig. 7. Under the fine grained adjustment of difficulty level, the difficulty of the puzzle constantly varies as a function of the number of users in the system. The larger the number of miners, the smaller the rate reward per miner due to competition (dashed line) but the larger the value of the mined coin in dollars (full line). Taken together, the product of rate reward times value of mined coin yields the utility in dollars per time unit (line with circles). In this paper, we consider the competition effects (dashed line) and in [10] the authors consider the gains due to increased interest in the mined coin (full line). An integrated approach accounting for competition and increased interest in the mined coin (line with circles) is out of the scope of [10] and of this paper, and is subject for future work.

[42] Jules Pretty, Craig Brett, David Gee, Rachel Hine, Chris Mason, James Morison, Matthew Rayment, Gert Van Der Bijl, and Thomas Dobbs. 2001. Policy challenges and priorities for internalizing the externalities of modern agriculture. *Journal of environmental planning and management* 44, 2 (2001), 263–283.
[43] S. Raval. 2018. Ethereum Price Prediction. *https://tinyurl.com/ethereumpred* (2018).
[44] J. B. Rosen. 1965. Existence and uniqueness of equilibrium points for concave N-person games. *Econometrica* 33 (1965), 520–534. Issue 3.
[45] Robert W Rosenthal. 1973. A class of games possessing pure-strategy Nash equilibria. *International Journal of Game Theory* 2, 1 (1973), 65–67.
[46] Tim Roughgarden. 2005. *Selfish routing and the price of anarchy*. Vol. 174. MIT press Cambridge.
[47] David Cerezo Sánchez. 2019. Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies. *arXiv preprint arXiv:1905.09093* (2019).
[48] Devavrat Shah and Kang Zhang. 2014. Bayesian regression and Bitcoin. In *Allerton*. IEEE, 409–414.
[49] Alexander Spiegelman, Idit Keidar, and Moshe Tennenholtz. 2018. Game of Coins. *arXiv:1805.08979* (2018).
[50] F. Ulrich. 2017. Attacking Bitcoin. *https://tinyurl.com/fulrich* (2017).
[51] Cheng Wan. 2012. *Contributions to evolutionary and congestion game theory*. Ph.D. Dissertation. Université Pierre et Marie Curie-Paris VI.
[52] Canhui Wang, Xiaowen Chu, and Qin Yang. 2019. Measurement and Analysis of the Bitcoin Networks: A View from Mining Pools. *arXiv preprint arXiv:1902.07549* (2019).
[53] Bitcoin Wisdom. 2018. Bitcoin Difficulty. *https://bitcoinwisdom.com/bitcoin/difficulty* (2018).
[54] Zehui Xiong, Shaohan Feng, Dusit Niyato, and Ping Wang. 2017. Edge computing resource management and pricing for mobile blockchain. *arXiv:1710.01567* (2017).
[55] Yanru Zhang, Lanchao Liu, Yunan Gu, Dusit Niyato, Miao Pan, and Zhu Han. 2016. Offloading in software defined network at edge with information asymmetry. *Journal of Signal Processing Systems* 83, 2 (2016), 241–253.

APPENDIX A: FOLLOWING THE CROWD OR AVOIDING IT? POSITIVE AND NEGATIVE MINING EXTERNALITIES

Next, we discuss two contending aspects involved in the value of mining. *First,* the payoff for a miner from solving a mining puzzle increases as the number of active miners grows. This is because the market value of a coin (or of a chain of a coin) is proportional to the interest towards that coin (or towards that chain) (see [48]). This effect has been captured and studied in [10, 41], and corresponds to a *positive externality* due to mining. *Second,* the

competition among miners implies that the probability that a miner succeeds in solving a puzzle decreases as the number of active miners grows. This is because the puzzle complexity is dynamically adjusted so that the system throughput in terms of total blocks mined for the whole population per time unit remains constant [37]. This effect corresponds to a *negative externality* due to mining (Figure 1, scenarios 1 and 2). It has been studied in [13], where the author assumes a fixed exchange rate between the virtual currency and fiat currency, and the exchange rate does not depend on the number of miners or on the total investment in computational power for mining.

The first effect is an incentive for miners to mine where they expect the others to mine as well ("crowding in" or "following the crowd"). The second effect ("crowding out" or "avoiding the crowd") is the subject of this paper, and makes it less attractive to mine a coin or a branch where many others mine. Whereas the first effect is out of the scope of this paper, the second one is beyond the scope of [10]. Following the crowd and avoiding the crowd behavior has been investigated in queueing systems by [22]. An integrated approach accounting for both effects in the realm of blockchain systems is subject for future work (Figure 7).

APPENDIX B: PROOF OF THEOREM 7.6

The existence of the equilibrium follows from Theorem 1 in [44] as well as from Corollary 7.5. Next, we establish the uniqueness.

Fix an arbitrary constant γ. Theorem 7.1 implies that the Unconstrained Game with utilities given by 48 has a unique equilibrium $y(\gamma)$, where we make the dependence of y on γ explicit. Then, $y(\gamma)$ is also the unique equilibrium of the game with utilities (48) but with $-x_m\gamma$ replaced by $-\gamma(\sum_k x_k - V)$. The replacement corresponds to adding a term $-\gamma(\sum_{k\neq m} x_k - V)$ to the utility (48). Note that after adding this term, $y(\gamma)$ is still an equilibrium of the modified game since the new utilities differ from the previous ones by terms that do not depend on, x_m, the action of player m. The new utility is given by

$$U_m(x) = \frac{x_m}{\sum_{j=1}^M x_j} - x_m\gamma - \gamma\left(\sum_{k\neq m} x_k - V\right) = \frac{x_m}{\sum_{j=1}^M x_j} - \gamma\left(\sum_{k} x_k - V\right) \tag{68}$$

The new utility corresponds to internalizing externalities in the game given by (50)-(51), as the global constraints are now part of the utilities of each player [40, 42].

Recall that the Lagrangian of the Constrained Game is given by,

$$\mathcal{L}_m(x_m) = \frac{x_m}{\sum_{j=1}^M x_j} - \lambda\left(\sum_{k} x_k - V\right) \tag{69}$$

Comparing (68) against (69) we note that the two have the same shape. Replacing γ by λ, we also establish a mapping between equilibria of the Unconstrained Game and the Relaxed Game, allowing us to leverage Theorem 7.1 (about the Unconstrained Game) and Corollary 7.5 (about the Relaxed Game) to complete our proof. Indeed, since the argument above holds for any γ, then it holds in particular for γ for which the complementarity condition (53) holds. We shall next show that such a γ exists. Let us denote it by $\gamma^\star$.

The Nash equilibrium $y^\star$ induced by $\gamma^\star$ in the Unconstrained Game, with utilities (48), is a symmetric equilibrium to the Relaxed Game (50)-(51) and a normalized equilibrium to the Constrained Game. For every γ, the Unconstrained Game has a unique equilibrium by Theorem 7.1.

Recall that the complementarity conditions are given by (53). With λ replaced by γ, the complementarity conditions are given by

$$\gamma\left(\sum_{j=1}^M y_j - V\right) = 0. \tag{70}$$

We are interested in the case $\gamma \neq 0$, hence

$$\sum_{j=1}^{M} y_j - V = 0. \tag{71}$$

Focusing on the symmetric equilibrium, we must have $y^\star = y_j$, for $j = 1, \ldots, M$, and

$$y^\star = \frac{V}{M}. \tag{72}$$

Thus, it follows from Corollary 7.5 that the required $\gamma^\star$ is $\gamma^\star = (M-1)/(MV)$.

We conclude that there is a unique symmetric equilibrium to the Unconstrained Game game, which is also the unique symmetric equilibrium to the Relaxed Game and the unique symmetric normalized equilibrium to the Constrained Game. □

APPENDIX C: ESP CONNECTION GAME UNDER PROCESSOR SHARING SCHEME

In this section, we consider the ESP connection game under a processor sharing scheme. Whereas in the remainder of this work we assumed that the hash power of an ESP is proportional to the number of users that decide to count on that ESP, in this section we assume that all ESPs continuously operate at their capacity. In that case, $\mu_{\star,m}$ refers to the capacity of ESP m.

Connection to queueing theory literature. Under the schemes considered in the remainder of this paper, the hash power of each ESP linearly increases with respect to the number of miners that rely on that ESP, corresponding to the infinite server queuing model in the queueing theory literature. In this section, in contrast, each ESP m has a fixed hash power $\mu_{\star,m}$, which is equally shared among miners who join that ESP, corresponding to the processor sharing scheme in queueing theory.

Model. We consider a time slotted system, where each time slot has duration given by an exponentially distributed random variable with rate $\sum_{m=1}^{M} \mu_{\star,m'}$. Rewards and costs are then computed per time slot. Note that in a given time slot it may be the case that a block is successfully mined by an ESP to which no miner is associated to. The latter occurs with probability $\sum_{m':\ell_{\star,m'}=0} \mu_{\star,m'} / \sum_{m'=1}^{M} \mu_{\star,m'}$.

The probability that a reward is granted to a tagged miner who joined ESP m, per time slot, is given by

$$p_{\star,m} = \begin{cases} \frac{\mu_{\star,m}}{\sum_{m'} \mu_{\star,m'}} \times \frac{1}{\ell_{\star,m}}, & \text{if } \ell_{\star,m} > 0 \\ 0, & \text{otherwise} \end{cases} \tag{73}$$

Every miner who joins ESP m pays a cost $\gamma_{\star,m}$, per time slot. Thus,

$$U_{\star,m}(\ell) = \begin{cases} p_{\star,m} - \gamma_{\star,m}, & \text{if } m > 0 \\ 0, & \text{otherwise.} \end{cases} \tag{74}$$

In that setting, the payoff to a miner who joins ESP m is decreasing in the number of miners using that ESP. This is a congestion game in the sense of [45] and thus the game admits a pure Nash equilibrium.