DOI:
10.1007/978-3-030-37110-4_13

Document Version
Publisher's PDF, also known as Version of record

Oceanic Games: Centralization Risks and Incentives in Blockchain Mining

Nikos Leonardos, Stefanos Leonardos and Georgios Piliouras

Abstract To participate in the distributed consensus of permissionless blockchains, prospective nodes—or *miners*—provide proof of designated, costly resources. However, in contrast to the intended decentralization, current data on blockchain mining unveils increased concentration of these resources in a few major entities, typically *mining pools*. To study strategic considerations in this setting, we employ the concept of *Oceanic Games* [27]. Oceanic Games have been used to analyze decision making in corporate settings with small numbers of dominant players (shareholders) and large numbers of individually insignificant players, *the ocean*. Unlike standard equilibrium models, they focus on *measuring the value (or power) per entity and per unit of resource* in a given distribution of resources. These values are viewed as strategic components in coalition formations, mergers and resource acquisitions. Considering such issues relevant to blockchain governance and long-term sustainability, we adapt oceanic games to blockchain mining and illustrate the defined concepts via examples. The application of existing results reveals incentives for individual miners to merge in order to increase the value of their resources. This offers an alternative

Stefanos Leonardos and Georgios Piliouras acknowledge that this work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2016NCR-NCR002-028) and administered by the National Cybersecurity R&D Directorate. Georgios Piliouras acknowledges SUTD grant SRG ESD 2015 097, MOE AcRF Tier 2 Grant 2016-T2-1-170 and NRF 2018 Fellowship NRF-NRFF2018-07.

N. Leonardos
National and Kapodistrian University of Athens, Panepistimioupolis, 161 22 Zografou, Greece
e-mail: nleon@di.uoa.gr

S. Leonardos (✉) · G. Piliouras
Singapore University of Technology and Design, 8 Somapah Rd, Singapore 487372, Singapore
e-mail: stefanos_leonardos@sutd.edu.sg

G. Piliouras
e-mail: georgios@sutd.edu.sg

P. Pardalos et al. (eds.), *Mathematical Research for Blockchain Economy*,
Springer Proceedings in Business and Economics,
https://doi.org/10.1007/978-3-030-37110-4_13

perspective to the observed centralization and concentration of mining power. Beyond numerical simulations, we use the model to identify issues relevant to the design of future cryptocurrencies and formulate prospective research questions.

Keywords Blockchain · Cryptocurrencies · Resources · Mining pools · Oceanic games · Values

1 Introduction

Decentralization is a core element in the design of permissionless blockchains. To participate in the blockchain consensus mechanisms, prospective network nodes—also called *miners*—need to provide proof of some costly resource. This resource may be computational power in protocols with Proof of Work (PoW) selection mechanisms, [15, 28], or coins of the native cryptocurrency in Proof of Stake (PoS) selection mechanisms, [5, 8]. Under default conditions, the selection is proportional to miners' resources and hence, it depends on their actual distribution. An integral assumption in the security philosophy of permissionless blockchains is that the network of mining nodes remains "sufficiently" decentralized and distributed. In the extreme case, *sufficiently* means that no single entity holds 50% or more of the resources but in practice much more fragmentation may be desired to safeguard the safety properties of the underlying protocol [3, 11, 22].

With this in mind, the picture illustrated in Table 1 is disconcerting. Table 1 shows the distribution of blocks among miners in the two largest[1] cryptocurrencies, Bitcoin and Ethereum, and indicates that the desired assumption of a highly decentralized (and distributed) network is currently not satisfied. As can be seen, the vast majority of mining resources is concentrated in a small number of "major" nodes or *mining pools* in which individual miners join forces to reduce the variance of their payments [14, 34]. The rest is scattered among a large number of minor and individually insignificant miners. The discrepancy between the intended distribution and the concentration of resources that is observed in practice raises some questions. What is the actual power of such pools or major miners to influence the evolution of the blockchain? Does this distribution create incentives for mergers and formation of coalitions (cartels) that will seize control of the majority of resources and manipulate the blockchain [24, 26]? What strategic considerations arise and what are their implications on blockchain governance and long-term sustainability?

Similar questions have been examined by conventional economics in the context of corporate governance. To study interactions between shareholders with various degrees of power in particular, [27] developed the model of *Oceanic Games*. These are games featuring a mixture of few large players (shareholders) and a continuum of infinitesimal players, called the *ocean*, each of which holds an insignificant fraction of corporate shares. The resemblance with blockchain mining—with

[1] In terms of market capitalization, cf. coinmarketcap.com.

Table 1 Distribution of the blocks mined in the Bitcoin and Ethereum blockchains. Mining is dominated by few major miners, typically mining pools, numbered from 1 to 10 and a great number of minor players in the "Unkown/other" category. *Source* blockchain.com and etherscan.io, 5 March 2019

	Bitcoin		Ethereum	
	Entity (Pool)	Blocks (%)	Entity (Pool)	Blocks (%)
1.	BTC.com	18.2	Ethermine	28.2
2.	AntPool	14.7	Sparkpool	21.4
3.	F2Pool	12.6	Nanopool	12.6
4.	SlushPool	10.1	F2Pool_2	12.4
5.	BTC.TOP	7.9	MiningPoolHub_1	5.6
6.	ViaBTC	7.9	DwarfPool_1	1.9
7.	DPOOL	4.1	PandaMiner	1.8
8.	BitFury	2.3	firepool	1.6
9.	BitClub Network	2.3	Address_1	1.4
10.	Bitcoin.com	1	MinerallPool	1.1
	Unknown/other	**18.9**	**Unknown/other**	**12.0**

shares corresponding to units of mining resources—is apparent. Our goal in this paper is to explore incentives in blockchain mining from the perspective of Oceanic Games and complement existing studies that focus on safety and security related issues [9, 13, 29].

The central idea in the literature of Oceanic Games is the measurement of a *value* for each entity and for each *unit of resource* given the distribution of resources among shareholders. The concept of *value* is considered as a powerful tool in the theory of decision making [2, 31, 33] and [32]. For instance, if a miner holds 51% of the total resources, then each of her units is worth much more than if she holds only 49% of the total resources, since in the former case, the entirety of her shares gives her absolute control over the blockchain. Similar, but maybe less obvious considerations, arise also in intermediate cases. If a miner holds 49% of the resources and a second miner holds 2% of the resources, then both miner's resources value higher than in the case in which the first miner only holds 47% of the resources, since in the former case, the two miners may collude and jointly seize control of the blockchain.

Motivated by these considerations, we adapt the model of Oceanic Games from [27] on blockchain mining. Our aim is to measure the *value of mining resources per miner and per unit of resource* as a strategic component in the process of power gain and coalition formation between mining nodes. With this approach, we shift our attention from safety attacks and equilibration models, [12, 20], to the understanding of incentives related to the distribution and acquisition of protocol resources. The analysis of these issues is relevant to the broader subjects of long term sustainability and blockchain governance [7].

Based on the above, our contribution in the present paper can be summarized in the following points

- We model instances of blockchain mining as Oceanic Games: the discrete set of large players corresponds to the large mining nodes, typically mining pools, and the continuum of infinitesimal oceanic players to the remaining, individual miners, cf. Fig. 1. Conveniently, the resulting model does not depend on the underlying selection mechanism (PoW, PoS or similar) or consensus protocol and hence can be used for the study of resource acquisition, strategic interactions, coalition formations (mergers) and governance related issues in a broad spectrum of permissionless blockchains [4, 9, 10, 16, 18, 21, 30]. We extend an example of [27] to illustrate the defined concepts in blockchain context.
- The application of existing results uncovers incentives for the formation of mergers between miners. Starting from an initial distribution in which the oceanic players control the majority of resources, we use simulations to show that this holds in two instances: first, in the formation—crystallization—of a coalition out of the ocean and second, in the exogenous acquisition of additional resources by a group of individual miners who, nevertheless, have the ability to coordinate their actions (collude). In both cases, the value of the miners' resources is higher when they act as a single entity rather than individual, oceanic players. This result provides an alternative perspective to the observed centralization in cryptocurrency mining, cf. Table 1.
- Further numerical simulations demonstrate that the above conclusions do not hold in the whole range of parameters. Instead, the dynamics of coalition formations and entry barriers are shown to depend on the current distribution of mining resources among major miners and the ocean.
- Finally, we use this model to raise issues relevant to the design of future cryptocurrencies and formulate prospective research questions.

In general, the present paper can be seen as a first step towards the application of the Oceanic Game concept in blockchain mining. Beyond some first insight, the extent to which this model can provide further results in the issues of (de)centralization, blockchain governance and long-term sustainability is yet to be fully understood.

1.1 Outline

The rest of the paper is structured as follows. In Sect. 2 we present the model of Oceanic Games and give an example to illustrate the defined notions. Revelant results from [27] and their application in blockchain settings are shown in Sect. 3 along with numerical simulations. In Sect. 4, we raise related issues and research questions and discuss limitations of the current approach. Section 5 concludes the paper.

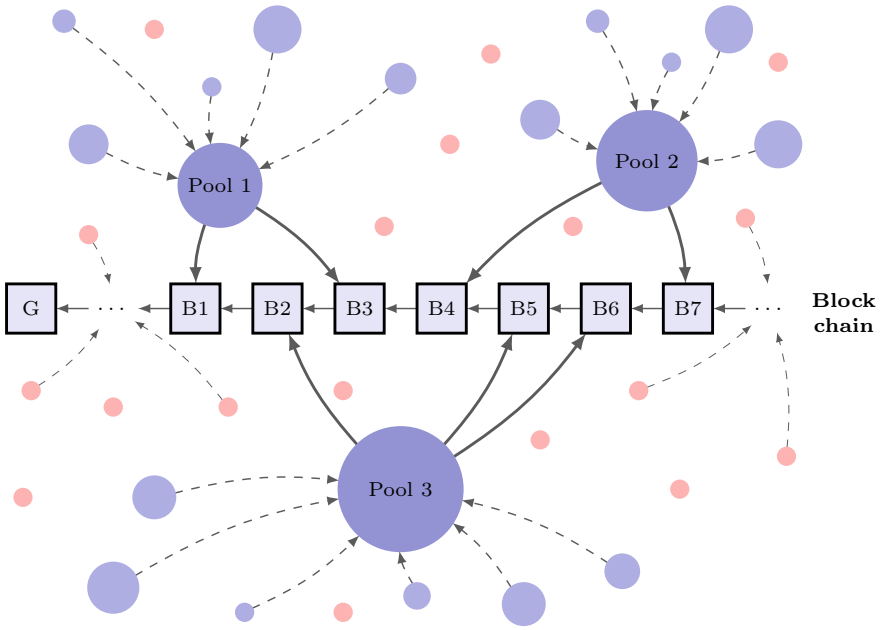

Fig. 1 Illustration of centralization in blockchain mining. Miners join forces in few major mining pools (blue), $M = \{1, 2, \ldots, m\}$, which dominate the mining process. The remaining small miners (light red)—or the ocean, I—mine individually

2 The Model: Oceanic Games on the Blockchain

The current model adjusts the notation and terminology of [27] in a standard blockchain setting.

Miners: The *miners* are the physical entities that participate in the block proposal and creation process. The term is used here in the broadest sense and depending on the underlying protocol and selection mechanism, it may refer to "conventional" miners as in PoW, [28], or to *virtual miners* as in PoS or other alternative forms [8]. The set of miners consists of two distinctive components

- A finite, discrete set $M = \{1, 2, \ldots, m\}$ of major miners or mining pools.
- An interval $I = [0, 1]$ of infinitesimal miners. We refer to I as the *ocean* and to miners in I, as *oceanic players*. We only consider subsets $U = [u_1, u_2] \subseteq I$ of the ocean I, e.g. $U = [0.1, 0.5]$, and not individual oceanic players.

Resources: To participate in the distributed consensus, each miner needs to provide proof of some designated, costly resource. This may be a physical or digital asset such as computational power in PoW or native coins in PoS mechanisms, respectively. To describe these resources, we use following notation

– A set of real numbers $r_1, r_2, \ldots, r_m \geq 0$, where r_i denotes the amount of resources of miner $i \in M$. For any subset $S \subseteq M$, we will write $r(S) = \sum_{i \in S} r_i$ to denote the total resources of miners in S.
– A positive constant $\alpha > 0$ which denotes the total resources of the ocean I. Accordingly, any subset $U = [u_1, u_2] \subseteq I$ controls $\alpha \cdot |U|$ of resources where $|U| = u_2 - u_1$.

Based on the above, the total protocol resources R are equal to $R := \alpha + \sum_{i \in M} r_i$. While resources change over time, in the present analysis, we will focus on a single period or a static setting and hence, unless indicated otherwise, our notation is independent of the time t. Resources may be expressed as absolute numbers or percentages but this will be made explicitly clear from the context.

Blockhain Oceanic Games: Given the above, a *blockchain oceanic game* Γ is defined by a *majority quota*, $q \geq 0$, using the symbol[2]

$$\Gamma := [q; r_1, r_2, \ldots, r_m; \alpha]$$

with the following interpretation: a coalition of miners $C := S \cup U$ with $S \subseteq M$ and $U \subseteq I$ wins in the game Γ, if and only if its total resources are larger than or equal to q, i.e., if

$$r(C) := r(S) + \alpha \cdot |U| \geq q$$

Addition of resources: Given an oceanic game Γ, we want to study the situation in which new entities acquire resources and enter the protocol. For this, we will use the notation Γ^+ with

$$\Gamma^+ := \left[q; r_1, r_2, \ldots, r_m, r_{m+1}; \alpha\right]$$

and $M^+ = \{1, 2, \ldots, m, m+1\}$. In words, Γ^+ results from Γ by the addition of a new major player $m+1$ with exogenous resources $r_{m+1} > 0$. Similar notation can be used to denote the formation of a new entity *crystallizing* out of the ocean. In this case, $\Gamma^+ := \left[q; r_1, r_2, \ldots, r_m, r_{m+1}; \alpha - r_{m+1}\right]$ for some $r_{m+1} > 0$, and $M = \{1, 2, 3, \ldots, m+1\}$.

Values: The first core functionality of the present model is to calculate a *value* φ_i for each major miner $i \in M$ and one value Φ for the entirety of the oceanic players, also referred to as the *oceanic value*. Each miner's value depends on that miner's share of resources *and* on the total distribution of the remaining resources among the rest of major and oceanic miners. To define the miner's values $\varphi_i, i \in M$ and the oceanic value Φ, let $X_1, X_2, \ldots, X_m$ be independent random variables uniformly distributed on $I = [0, 1]$. For each $x \in I$, let $r(x) := \sum_{j \in M} r_j \cdot \mathbf{1}\{X_j < x\}$, where $\mathbf{1}\{X_j < x\} = 1$ if $X_j < x$ and 0 otherwise (indicator

[2]The notation is common in the literature of *weighted voting games*, see [25, 31, 32] for a more related application. Also, in most cases, we will be interested in $q = 0.5$ or 50% but the current model applies to any q of interest.

function). Then, the *value* of miner $i \in M$ is defined by

$$\varphi_i := \mathbb{P}\text{rob}\left[r\left(X_i\right) + \alpha X_i < q \leq r\left(X_i\right) + \alpha X_i + r_i\right] \tag{1}$$

and the oceanic value by $\Phi := 1 - \sum_{i \in M} \varphi_i$. Intuitively, the value φ_i is the probability that miner i will be the crucial entity to turn a random coalition of miners from losing (total resources of the coalition without i are less than q) to winning (total resources of the coalition with i are equal to or greater than q).[3]

Value-per-unit of resource: The second functionality of this model is to determine the *value per-unit of resource* or power ratio, v_i, for each player $i \in M$, which is defined by

$$v_i := \varphi_i / r_i \tag{2}$$

Similarly, the *value per oceanic unit of resource* or oceanic power ratio, v_{oc}, is equal to $v_{\text{oc}} := \Phi/\alpha$.

2.1 An Example: Why Values and Not Shares?

We illustrate the above with the help of an example adapted from [27, Section 6]. We consider a mining situation with two major mining entities or pools, $M = \{1, 2\}$, and the simple majority quota $q = 0.5$ represented by the following game $\Gamma = [0.5; r_1, r_2; \alpha]$, where $\alpha = 1 - r_1 - r_2$. The 0.5 or 50% quota corresponds to cntrol of the majority of protocol resources and hence, of the blockchain as a whole. In this game a coalition S wins, if $r\left(S\right) \geq 0.5$, i.e., if it occupies 50% or more of the protocol resources.[4]

All possible resource configurations (r_1, r_2, α) are illustrated in Fig. 2. The horizontal and vertical axes represent miner 1's and miner 2's fraction of the resources, respectively. Their possible combinations are divided in 4 inner regions, $\Delta_i, i = 1, 2, 3, 4$. Region Δ_1 contains all configurations for which the combined resources of both major miner are less than 50%, i.e., $r_1 + r_2 \leq 0.5$. In this case, the majority of resources is controlled by oceanic players. However, the ocean is not actually "in control", since, by assumption, there is no coherence nor organizational structure between oceanic players. The explanation of regions Δ_2, Δ_3 and Δ_4 is similar and is briefly given in the legend of Fig. 2.

Using (1), the value φ_1 of the first major miner is given by

[3] For more details and the probabilistic derivation of these values, we refer to [27].

[4] Due to continuity properties, there is no difference between using the q = 50% quota or symbolically, the q = 51% quota, as is common in the related literature [11, 22, 28].

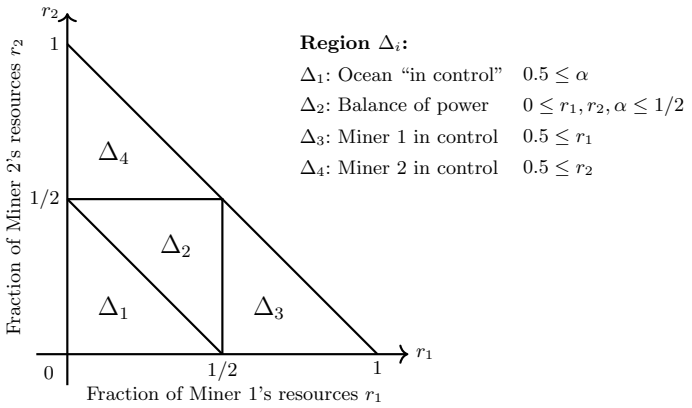

Fig. 2 All possible configurations in the distribution of resources (r_1, r_2) between 2 major miners and the ocean, α

$$\varphi_1 = \begin{cases} \frac{r_1 \bar{r}_2}{\alpha^2}, & \text{if } (r_1, r_2) \in \Delta_1 \\ \left(\frac{1-2r_2}{2\alpha}\right)^2, & \text{if } (r_1, r_2) \in \Delta_2 \\ 1, & \text{if } (r_1, r_2) \in \Delta_3 \\ 0, & \text{if } (r_1, r_2) \in \Delta_4 \end{cases} \tag{3}$$

with $\bar{r}_i := \alpha - r_j$ for $i = 1, 2$ and $j = 3 - i$. The value φ_2 of Miner 2 is analogous and the oceanic value Φ is simply equal to $\Phi = 1 - \varphi_1 - \varphi_2$.

The interpretation of the values in the extreme regions Δ_3 and Δ_4 is straightforward. In Δ_3, miner 1 controls more than 50% of the resources and hence, has absolute power over the blockchain. This implies that her value is equal to 1 and consequently, the value for both miner 2 and the oceanic miners is 0. Region Δ_4 is similar. The interesting cases arise whenever $(r_1, r_2) \in \Delta_2$, i.e., when the major miners and the ocean, each control less than 50% of the resources, or $(r_1, r_2) \in \Delta_1$, i.e., when the resources controlled by the ocean account for more than half of the total resources. This case is also referred to as the *interior case* in the original paper. Some instantiations in regions Δ_1 and Δ_2 are presented in Table 2.

An indicative observation—which does not aim to an exhaustive analysis of the above measurements—is that the values and the ratios unveil disparities between *shares* and actual *influence* or *power* of the participating entities. For example, there are instances, as in the (40, 9, 51)-configuration (first row in Δ_1), in which a major miners' ratio is larger than the ratio of oceanic players. This imbalance generates a motive for oceanic players to merge with that miner to increase the power of their individual resources. Equivalently, the large miner has an increased influence to attract resources from the ocean. The picture is totally different in the (40, 40, 20)-configuration (third row of Δ_2), in which the competition between the major miners raises the value of resources owned by the ocenic players. Both cases can be con-

Table 2 Resources, values and values per unit of resource for various configurations in the Δ_1 and Δ_2 regions. The resources $r_i, i = 1, 2$ are selected arbitrarily, $\alpha = 1 - r_1 - r_2$, the values $\varphi, i = 1, 2$ and Φ are given by (3) and the ratios $v_i, i = 1, 2$ and v_{oc} by (2)

	Resources %			Values %			Ratios		
	r_1	r_2	α	φ_1	φ_2	Φ	v_1	v_2	v_{oc}
Δ_1: Interior game	40	9	51	65	4	31	1.62	0.42	0.62
	30	19	51	37	15	48	1.23	0.81	0.94
	25	24	51	26	24	50	1.04	1.00	0.98
Δ_2: Balance of power	35	20	45	44	11	44	1.27	0.56	0.99
	40	30	30	44	11	44	1.11	0.37	1.48
	40	40	20	25	25	50	0.63	0.63	2.5

trasted to the stability in the $(25, 24, 51)$-configuration, in which all 3 ratios are approximately equal to 1.

Yet, as argued in [27], the interpretation of values should be done with caution and only in addition to complementary analytical tools. This is because values do not take into account qualitative factors such as ethical commitments, operational constraints or other kinds of incentives.

3 Individual Mining Is Not Stable

A direct outcome of applying the model of Oceanic Games in the blockchain context is the next result due to [27]. Both parts of Theorem 1 make critical use of the assumption that the majority of mining resources is controlled by oceanic players. Their proof relies on a recursion in the number m of major miners and can be found in [27]. Here, we will focus on the interpretation of Theorem 1 and its application in blockchain context.

Theorem 1 ([27]) *Let $\Gamma = [0.5; r_1, r_2, \ldots, r_m; \alpha]$ with $M = \{1, 2, \ldots, m\}$ be a blockchain oceanic game, such that $r(M) < 0.5 \leq \alpha$, i.e., such that the majority of mining resources is controlled by individual (oceanic) miners. Then*

(a) The value φ_i of any major player $i \in M$ in Γ is given by

$$\varphi_i = \frac{r_i}{\alpha^m} \sum_{S \subseteq M - \{i\}} \left[c_s \prod_{j \in S} r_j \prod_{k \notin S} (\alpha - r_k) \right]$$

where $c_s := s! \left[\frac{1}{s!} - \frac{1}{(s-1)!} + \cdots + (-1)^s \right]$ and $s := |S|$ is the number of major miners in S. The oceanic value Φ is equal to $\Phi = 1 - \sum_{i \in M} \varphi_i$.

(b) If $\Gamma^+ = [0.5; r_1, r_2, \ldots, r_m, r_{m+1}; \alpha]$ *for some* $r_{m+1} > 0$*, and* $\Phi^+, \varphi_i^+, i = 1, \ldots, m+1$ *are the values in* Γ^+*, then*

$$\varphi_{m+1}^+ / r_{m+1} = \Phi / \alpha$$

or equivalently, $v_{m+1}^+ = v_{oc}$.

Interpretation of Theorem 1. Statement (a) of Theorem 1 is an analytical result which yields the exact formula to compute the values of the major miners and the ocean. Its usefulness will become aparent in the applications. Statement (b) carries more intuition. It states that the value-per-unit of resource of a miner entering Γ is equal to the oceanic value-per-unit of resource in Γ. One possible interpretation, also supported by [27], is that this provides a stability argument in favor of decentralization, in the sense that there is no incentive for the formation of a "cartel" or a mining pool, *provided that* the size of the ocean is big enough, i.e., provided that the ocean controls the majority of the resources.[5]

However, as we will see in the following applications, this picture is misleading and decentralization is actually not stable. In practice, the oceanic value per unit of resource in Γ^+ can go below the value per unit of resource of the crystallizing or newly entering entity. Hence, *given that* a set of miners can coordinate their actions, then it may be beneficial for them to either crystallize out of the ocean or to acquire exogenous resources and form in both cases a single mining entity.

3.1 Applications of Theorem 1

The above interpretations of Theorem 1 are illustrated via the simulation of two representative scenarios. In both cases, we assess the stability of initial distributions of mining resources, in which the majority of resources is controlled by the ocean. This is achieved by comparing the oceanic value per unit of resource to the value per unit of resource of the same miners when acting as single entity.

I. Crystallization out of the ocean: In the first scenario, we consider an instance of the blockchain oceanic game in which all resources are initially controlled by oceanic players. This is described by the game $\Gamma = [50\%; \alpha = 100]$ and $M = \emptyset$. Then, we simulate a gradual formation of a single mining entity by the process of *crystallization* out of the ocean. This is captured by a sequence of games (instances) $\Gamma^+ = [50\%; r_1; \alpha]$ with $0 < r_1 < 50$ and $\alpha = 100 - r_1$. For each instance, we calculate the value per unit of resource of the single entity that is forming out of the ocean and compare it with the value per unit of oceanic resource. The results are shown in Fig. 3.

It is apparent that v_1 is higher than v_{oc} even for arbitrarily low values of r_1 and that the difference is increasing in the percentage of crystallized resources. This

[5] This statement actually holds for any quota $q \in (0, 1)$ and not only for $q = 0.5$ as formulated here.

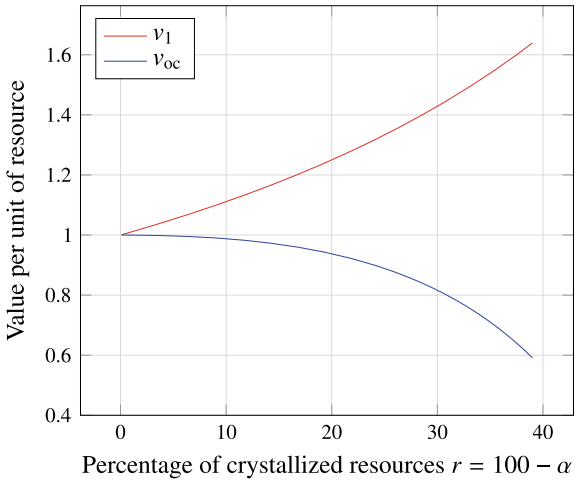

Fig. 3 The value per unit of resource of a single entity, $m = 1$, that is forming by mergers (crystallization) out of the ocean (red line) and the value per unit of oceanic resource (blue line). The total percentage of resources that is controlled by the crystallizing entity is shown in the horizontal axis

uncovers a motive for coalition formations and merging between miners, even if the initial distribution is perfectly decentralized. Further simulations (not shown here) demonstrate that the same picture continues to hold even if $M \neq \emptyset$, as long as $\alpha > 50\%$ and no single miner in M holds a percentage close to 50%. If there exists a "large" miner $i \in M$ with, e.g., $r_i > 40\%$, then the oceanic players may be disincentivized to collude. However, this is only a semblance of stability, since in this case, oceanic miners have an incentive to merge with the "large" miner.

II. Acquisition of exogenous resources: In the second scenario, we consider miners who are acquiring exogenous resources to enter the mining process. We assume that these miners can either enter the ocean and mine individually or collude and form a single mining entity. We want to compare the value per unit of resource in these two cases. Formally, we denote the current distribution of resources by $\Gamma = [50\%; r_1, r_2, \ldots, r_m; \alpha]$ with $\alpha > 50\%$ and the total mining resources of the new entities by w. We want to compare

- $v^+_{m+1} := \varphi^+_{m+1}/w$ in the game $\Gamma^+ := [50\%; r_1, r_2, \ldots, r_m, w; \alpha]$ to
- $v^{\mathrm{o}}_{\mathrm{oc}} := \Phi^{\mathrm{o}}/(\alpha + w)$ in the game $\Gamma^{\mathrm{o}} := [50\%; r_1, r_2, \ldots, r_m; \alpha + w]$.

The game Γ^+ describes the instance in which the entering miners merge in a single mining entity and the game Γ^{o} the instance in which the entering miners become part of the ocean and mine individually. We assume that initially, the majority of resources is controlled by oceanic players and that there exist two other major mining entities. It turns out that the share of mining resources of the other major entities influences the incentives of the entering miners. To see this, we consider two cases.

Case 1: Let $\Gamma = [50\%; 6, 4; 90]$, so that $\Gamma^+ = [50\%; 6, 4, w; 90]$ and $\Gamma^{\mathrm{o}} = [50\%; 6, 4; 90 + w]$ for any $w > 0$. As shown in Fig. 4, in this case, both major miners are not large enough to create entry barriers for the third entity and $v^+_{m+1} > v^{\mathrm{o}}_{\mathrm{oc}}$

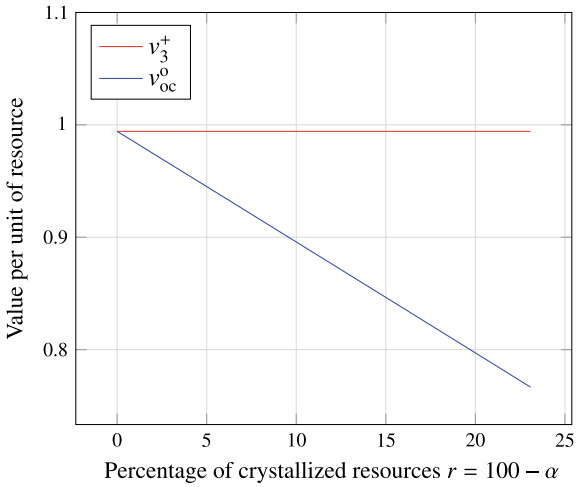

Fig. 4 The value per unit of resource of the entering miners when they enter as a single entity (red line) and their value per unit of resource when they enter as individual oceanic miners (blue line). The additional resources are shown as a percentage of the total resources in the horizontal axis

for any $w > 0$. In agreement with Theorem 1(b), the value per unit of resource, v_3^+, of the new miners when they enter as a single entity is equal to the oceanic value v_{oc} in the initial game Γ (red line). According to [27] this implies that "there is no incentive for a new entity to form". However, this only says half the truth. As we can see by the blue line, if the newly entering miners enter the ocean as individual miners, then their value per unit of resource will be lower compared to the case in which they collude. Hence, *given that* a group of entering miners are capable to coordinate their actions, then they are better off if they enter as a single entity than as oceanic players.

Case 2: Let $\Gamma = [50\%; 55, 5; 90]$, so that $\Gamma^+ = [50\%; 55, 5, w; 90]$ and $\Gamma^o = [50\%; 55, 5; 90 + w]$ for any $w > 0$. As shown in Fig. 5, in this case, the presence of major miner 1 seems to create a disincentive for a forming coalition and $v_{m+1}^+ < v_{oc}^o$ for any $w > 0$ such that $w + 90 < 50\%$. The resulting picture shows that we cannot generalize the outcome of the previous case. In particular, we conclude that whether the entering miners have an incentive to form a single entity or to join the ocean as individual miners, may depend on the actual distribution of resources among the existing major miners and the ocean. However, this is only a semblance of stability, stemming from an already centralized initial distribution ($r_1 > 33\%$). In this case, oceanic miners actually have a stronger incentive to merge with miner 1 instead of forming a new entity.

The previous simulations create an inconclusive picture. In general, the incentives for miners to merge seem to depend on the current distribution of resources. Since blockchain mining is a dynamical system that evolves over time, they suggest that even if the blockchain starts from a sufficiently decentralized point, then it is unlikely to remain decentralized also in the future or equivalently that decentralization creates a *negative feedback loop*, [19, 36]. The dynamics of the coalition formation process and the entry barriers resemble these of conventional economic markets of either

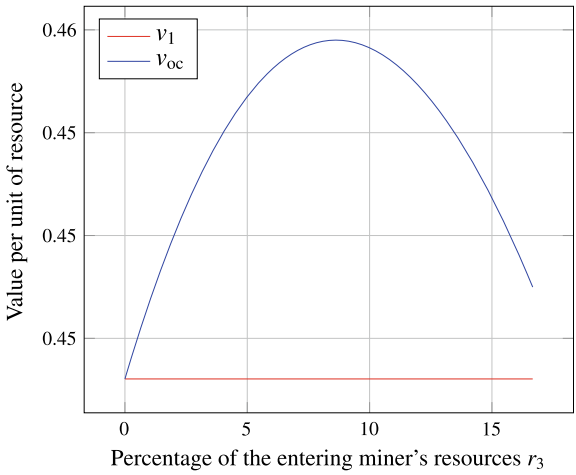

Fig. 5 The value per unit of resource of the entering miners when they enter as a single entity (red line) and their value per unit of resource when they enter as individual oceanic miners (blue line). The additional resources are shown as a percentage of the total resources in the horizontal axis

perfect or oligopolistic competition. These findings provide an alternative perspective to cryptocurrency mining along with [1], and suggest the need for further research in this direction.

4 General Issues, Research Perspectives and Limitations

The application of the oceanic-game model in blockchain mining opens new research perspectives but also has its own limitations. Beyond the insight from existing results, a complete model needs to account for the additional challenges and address the questions that are specific to the blockchain context. In the following discussion, we raise such relevant issues, discuss their connection and research possibilities via the current model and identify potential limitations.

Cryptocurrencies as Resources: The difference between PoW and PoS in terms of their resources—computational power versus native coins—has a direct impact on both the mining process and the value of the underlying cryptocurrency. When coins are used as mining resources (PoS protocols), their value depends on their distribution among existing miners, their availability for prospective miners and the returns (profits) from mining. This in contrast to PoW protocols, in which the price of the resources—e.g., hardware and electricity—is not tied to the price of the underlying cryptocurrency.

Resource Acquisition & Entry Barriers: The above suggest that the nature of protocol resources may also generate different entry barriers. In PoS, the acquisition of protocol resources, i.e., coins, by prospective nodes depends on the willingness of current owners to exchange their coins and the way that new coins are minted. Different configurations may lead to high entry barriers and centralization. In

PoW, computational power is essentially unlimited and acquisition of additional resources is independent of the underlying cryptocurrency. This implies lower entry barriers but also more frequent changes in the configuration (distribution) of resources among miners.
In particular, the current cost of acquiring enough computational power to control the majority in the Bitcoin and Ethereum PoW-blockchains is estimated at 1.5 billion US Dollars [6]. This amount is well within the budget of several physical or legal entities worldwide. Moreover, it is *independent* of the value of the underlying cryptocurrency and depends only on the size of the network and the hardware and electricity costs. With this in mind, it is natural to ask: how stable are PoW blockchains against arbitrary authorities able to acquire the majority of resources? How relevant are these questions to the current distribution of resources and how do they translate in the PoS setting?
In this context, further work on blockchain oceanic games can aid the community to raise and study questions about investment in cryptocurrencies. When viewed not only as assets but also as means to gain power in the mining process and the governance of a blockchain, cryptocurrencies fit to the current perspective and their mechanics can be better understood.

Mathematical Modelling: From a mathematical perspective, oceanic games bridge the gap between atomic and non-atomic congestion games [23]. Yet, the use of *values* instead of equlibria to study real settings has its own limitations [27, 32]. This is mainly due to the probabilistic derivation of values, which ignores qualitative aspects such as ethical commitments, preferences or any other motives of the participating agents. However, despite these limitations, if properly interpreted, values can become a powerful tool in the analysis of strategic interactions. In an immediate direction, they can be used to rethink the notion of *blockchain fairness* or *equitability*, which is currently based on the theoretically tentative premise that *one unit of resource—one vote* also implies fairness [13, 35].

5 Conclusions

In this paper, we employed the concept of Oceanic Games [27], to model and study strategic interactions in blockchain mining. Oceanic Games have been used in conventional economics to analyze decision making in corporate settings with a small number of major players—shareholders or here, mining pools—and a continuum of minor, individually insignificant players, called the *ocean*. This stream of literature focuses on the measurement of the value per miner and per unit of resource for each miner given a distribution of resources. Values are then interpreted as strategic components in decisions related to resource acquisition, mergers and coalition formations and offer an alternative perspective to the common equilibration models.

An immediate implication of existing results was that given a sufficiently large initial distribution of resources, there are *incentives* both for active and for newly

entering miners to merge (form cartels or coalitions) and act as single entities. These observations provide an alternative justification of the observed centralization and concentration of power in the mining process of the major cryptocurrencies. Contrary to common perceptions, they amount to the existence of a negative feedback loop in terms of decentralization as a core ingredient in permissionless blockchain philosophy, [17], and reveal the need for futher research in this direction. In a general discussion, we identified critical issues related to resource acquisition, entry barriers and centralization risks in blockchain mining and formulated relevant questions that may be answered by further exploration of the present model. These findings can be placed in the broader context of governance and long-term sustainability for pemissionless blockchains.

References

1. Arnosti, N., Weinberg, S.M.: Bitcoin: A natural oligopoly. In: 10th Innovations in Theoretical Computer Science Conference, ITCS 2019, pp. 5:1–5:1. San Diego, USA (2019). https://doi.org/10.4230/LIPIcs.ITCS.2019.5
2. Aumann, R.J.: Markets with a continuum of traders. Econometrica **32**(1/2), 39–50 (1964)
3. Badertscher, C., Garay, J., Maurer, U., Tschudi, D., Zikas, V.: But why does it work? a rational protocol design treatment of bitcoin. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology—EUROCRYPT 2018, pp. 34–65. Springer International Publishing, Cham (2018)
4. Badertscher, C., Gaži, P., Kiayias, A., Russell, A., Zikas, V.: Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 913–930. CCS '18, ACM, USA (2018). https://doi.org/10.1145/3243734.3243848
5. Bentov, I., Gabizon, A., Mizrahi, A.: Cryptocurrencies Without Proof of Work. In: Clark, J., Meiklejohn, S., Ryan, P.Y., Wallach, D., Brenner, M., Rohloff, K. (eds.) Financial Cryptography and Data Security, pp. 142–157. Springer, Heidelberg (2016)
6. Bonneau, J.: Hostile blockchain takeovers (short paper). In: Proceedings of the 5th IFCA Workshop on Bitcoin and Blockchain Research (2018)
7. Bonneau, J., Felten, E., Goldfeder, S., Kroll, J., Narayanan, A.: Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus. In: Financial Cryptography Workshops (2016)
8. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy, pp. 104–121 (2015). https://doi.org/10.1109/SP.2015.14
9. Brünjes, L., Kiayias, A., Koutsoupias, E., Stouka, A.P.: Reward Sharing Schemes for Stake Pools (2018). arXiv:1807.11218
10. Buterin, V., Reijsbergen, D., Leonardos, S., Piliouras, G.: Incentives in Ethereum's hybrid casper protocol. In: ICBC 2019. Seoul, Korea (2019). https://doi.org/10.1109/BLOC.2019.8751241
11. Eyal, I., Sirer, E.: Majority is not enough: bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) Financial Cryptography and Data Security, pp. 436–454. Springer, Heidelberg (2014)
12. Eyal, I.: The Miner's Dilemma. In: Proceedings of the 2015 IEEE Symposium on Security and Privacy. SP '15, pp. 89–103. IEEE Computer Society, USA (2015). https://doi.org/10.1109/SP.2015.13
13. Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., Wang, G.: Compounding of Wealth in Proof-of-Stake Cryptocurrencies (2018). ArXiv e-prints

14. Fisch, B., Pass, R., Shelat, A.: Socially optimal mining pools. In: R. Devanur, N., Lu, P. (eds.) Web and Internet Economics, pp. 205–218. Springer International Publishing, Cham (2017)
15. Garay, J., Kiayias, A., Leonardos, N.: The Bitcoin backbone protocol: analysis and applications. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 281–310. Springer, Berlin (2015)
16. Garay, J., Kiayias, A., Leonardos, N.: The Bitcoin backbone protocol with chains of variable difficulty. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017, pp. 291–323. Springer International Publishing, Cham (2017)
17. Garay, J.A., Kiayias, A., Leonardos, N., Panagiotakos, G.: Bootstrapping the blockchain, with applications to consensus and fast PKI setup. In: Public Key Cryptography (2018). https://eprint.iacr.org/2016/991
18. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N.: Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles. SOSP '17, pp. 51–68. ACM, USA (2017). https://doi.org/10.1145/3132747.3132757
19. Hauert, C., De Monte, S., Hofbauer, J., Sigmund, K.: Volunteering as Red Queen Mechanism for Cooperation in Public Goods Games. Science **296**(5570), 1129–1132 (2002). https://doi.org/10.1126/science.1070582
20. Johnson, B., Laszka, A., Grossklags, J., Vasek, M., Moore, T.: Game-theoretic analysis of DDoS attacks against bitcoin mining pools. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) Financial Cryptography and Data Security, pp. 72–86. Springer, Heidelberg (2014)
21. Kiayias, A., Russell, A., David, B., Oliynykov, R.: ouroboros: A provably secure proof-of-stake blockchain protocol. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology –CRYPTO 2017. pp. 357–388. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_12
22. Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y.: Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation, pp. 365–382. ACM, USA (2016)
23. Kleinberg, R., Piliouras, G., Tardos, E.: Multiplicative updates outperform generic no-regret learning in congestion games: extended abstract. In: Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. STOC '09, pp. 533–542. ACM, USA (2009). https://doi.org/10.1145/1536414.1536487
24. Laszka, A., Johnson, B., Grossklags, J.: When Bitcoin mining pools run dry. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) Financial Cryptography and Data Security, pp. 63–77. Springer, Heidelberg (2015)
25. Leonardos, S., Reijsbergen, D., Piliouras, G.: Weighted voting on the blockchain: Improving consensus in proof of stake protocols. In: ICBC 2019. Seoul, Korea (2019). https://doi.org/10.1109/BLOC.2019.8751290
26. Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., Rosenschein, J.S.: Bitcoin mining pools: a cooperative game theoretic analysis. In: Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. AAMAS '15, pp. 919–927. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC (2015)
27. Milnor, J.W., Shapley, L.S.: Values of Large Games II: Oceanic Games. Mathematics of Operations Research **3**(4), 290–307 (1978). https://doi.org/10.1287/moor.3.4.290
28. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). https://bitcoin.org/bitcoin.pdf. [Accessed: 14 Nov 2018]
29. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS P), pp. 305–320 (2016). https://doi.org/10.1109/EuroSP.2016.32
30. Pass, R., Shi, E.: Thunderella: blockchains with optimistic instant confirmation. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology—EUROCRYPT 2018, pp. 3–33. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_1
31. Shapiro, N.Z., Shapley, L.S.: Values of large games, I: a limit theorem. Math. Oper. Res. **3**(1), 1–9 (1978). https://doi.org/10.1287/moor.3.1.1

32. Shapley, L.S.: A value for n-person games. In: Roth, A.E. (ed.) The shapley value: essays in Honor of Lloyd S. Shapley, pp. 31–40. Cambridge University Press, Cambridge (1988). https://doi.org/10.1017/CBO9780511528446.003
33. Shitovitz, B.: Oligopoly in markets with a continuum of traders. Econometrica **41**(3), 467–501 (1973)
34. Sompolinsky, Y., Zohar, A.: Bitcoin's Underlying Incentives. Commun. ACM **61**(3), 46–53 (2018). https://doi.org/10.1145/3152481
35. Wong, T.: An application of game theory to corporate governance. Omega **17**(1), 59–67 (1989). https://doi.org/10.1016/0305-0483(89)90021-2
36. Zeigler, B., Praehofer, H., Kim, T.: Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems, 2nd edn. Academic Press (2000)