


Pool Formation in Oceanic Games: Shapley Value and Proportional Sharing

Aggelos Kiayias 

University of Edinburgh, UK

Input Output Global (IOG), Edinburgh, UK

Elias Koutsoupas 

University of Oxford, UK

Evangelos Markakis 

Athens University of Economics and Business, Greece

Input Output Global (IOG), Athens, Greece

Panagiotis Tsamopoulos 

Athens University of Economics and Business, Greece

Abstract

We study a game-theoretic model for pool formation in Proof of Stake blockchain protocols. In such systems, stakeholders can form pools as a means of obtaining regular rewards from participation in ledger maintenance, with the power of each pool being dependent on its collective stake. The question we are interested in is the design of mechanisms, i.e., “reward sharing schemes,” that suitably split rewards among pool members and achieve favorable properties in the resulting pool configuration. With this in mind, we initiate a non-cooperative game-theoretic analysis of the well known Shapley value scheme from cooperative game theory into the context of blockchains. In particular, we focus on the *oceanic* model of games, proposed by Milnor and Shapley (1978), which is suitable for populations where a small set of large players coexists with a big mass of rather small, negligible players. This provides an appropriate level of abstraction for pool formation processes that occur among the stakeholders of a blockchain. We provide comparisons between the Shapley mechanism and the more standard proportional scheme, in terms of attained decentralization, via a Price of Stability analysis and in terms of susceptibility to Sybil attacks, i.e., the strategic splitting of a players’ stake with the intention of participating in multiple pools for increased profit. Interestingly, while the widely deployed proportional scheme appears to have certain advantages, the Shapley value scheme, which rewards higher the most pivotal players, emerges as a competitive alternative, by being able to bypass some of the downsides of proportional sharing in terms of Sybil attack susceptibility, while also not being far from optimal guarantees w.r.t. decentralization. Finally, we also complement our study with some variations of proportional sharing, where the profit is split in proportion to a superadditive or a subadditive function of the stake, showing that our results for the Shapley value scheme are maintained in comparison to these functions as well.

2012 ACM Subject Classification Theory of computation → Algorithmic game theory and mechanism design

Keywords and phrases Shapley value, Nash equilibria, Price of Stability, Reward sharing schemes, Proof of Stake blockchains

Digital Object Identifier 10.4230/LIPIcs.AFT.2025.21

Related Version *Full Version:* <https://arxiv.org/pdf/2505.04422> [19]

Funding This work has been supported by the H.F.R.I call “Basic research Financing (Horizontal support of all Sciences)” under the National Recovery and Resilience Plan “Greece 2.0” funded by the European Union – NextGenerationEU (H.F.R.I. Project Number: 15877).

Acknowledgements Part of this work was done while the 4th author was a research intern at IOG. The authors would also like to acknowledge the use of resources of the “Theory, Economics and Systems Lab” at the Athens University of Economics and Business.



© Aggelos Kiayias, Elias Koutsoupas, Evangelos Markakis, and Panagiotis Tsamopoulos;
licensed under Creative Commons License CC-BY 4.0

7th Conference on Advances in Financial Technologies (AFT 2025).

Editors: Zeta Avarikioti and Nicolas Christin; Article No. 21; pp. 21:1–21:24

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Permissionless blockchain protocols base participation on the resources that parties possess such as their *computational power* (as in Bitcoin, [26]), or their *stake* in the system, measured by the number of digital coins they own (as in Ethereum [8], see e.g., [9]). This resource-based operation opens up the possibility for pooling resources together and having multiple resource holders engage as a single entity in protocol operation. Pooling resources can have both positive effects for the system, such as reducing the variance of rewards awarded to participants, as well as negative ones, leading to centralization with a handful of large pools controlling the protocol. Importantly, viewing the blockchain protocol as a mechanism, the question that arises is what are the objectives of this mechanism design problem and how it is possible to realize them.

As a running paradigm, we will use throughout our work the pool formation process in Proof of Stake blockchains. In such systems, stakeholders are attracted to coalitions as a means of obtaining rewards from participation in block production. The power of such a (stake) pool is then dependent on the collective stake (up to some threshold) that its members possess, which affects the probability that a pool operator is selected as a validator or block producer. Creating or joining a pool can be done either explicitly via options that the protocol itself provides (referred to as *onchain pooling*, for example, in the Cardano blockchain) or by agreements among the stakeholders via smart contracts or even via informal agreements. In fact, for the Ethereum protocol, there even exist platforms¹ (e.g. Rocketpool or Lido) that facilitate the grouping of stakeholders into pools. Essentially these platforms match smaller stakeholders to larger ones, so as to collectively accrue the amount of 32 ETH, required for a block validator.

Once a pool forms, the central question of interest, which is the focus of our work as well, is how should the pool members split the received rewards among themselves. This has led to an interesting and currently active research agenda, with several (and sometimes conflicting) desiderata that one would like to satisfy. Among these, a significant desideratum in blockchain communities is to promote decentralization. Viewed as a game, this means that we would like the reward scheme to induce equilibria with a relatively high number of pools. At the same time, we would also like to achieve resilience to Sybil attacks [15], since the pseudonymity of blockchain systems may allow seemingly independent pools controlled by the same entity. Although completely eliminating this may be too much to hope for, cf. [21], one could aim for mechanisms that attempt to discourage Sybil behavior.

If we look at current implementations, both in onchain pooling and in mediating platforms, the deployed reward scheme is typically very simple: the pool operator may keep a certain amount (accounting for a profit margin and/or operational costs) and the remaining amount is split in a proportional manner, based on stake contribution. This puts forth the natural question of whether the proportional scheme is the best thing to do. To answer this, it seems reasonable to also consider alternative candidate solutions from economic theory. Concepts from cooperative game theory, like the core [18] or the Shapley value [30], to name a few, have been extensively studied in almost any setting that involves cost or profit sharing. Despite however the popularity of such notions within game theory and economics, there have been surprisingly very few attempts to incorporate them in models tailored to blockchain protocols, such as [23, 13] (discussed further in our related work section). More generally, there is only a limited number of works that provide comparisons among different reward schemes, with some notable exceptions being [7, 12, 10].

¹ To give an idea of their volume and popularity, their total market capitalization is currently over 30 billion USD.

1.1 Our contribution

The main question we are interested in is: *How does the choice of a reward sharing scheme within a pool affect performance w.r.t. decentralization, and w.r.t. resilience to Sybil attacks?*

To study this question, we consider the model of *oceanic games*, originally introduced by Milnor and Shapley [24] in the context of cooperative games. This model captures populations where (atomic) players with moderate or large stake coexist with smaller non-atomic players of negligible stake (the ocean). We believe this model is particularly suitable for certain blockchain environments, as also advocated in [22]. Empirical studies have shown that the stake distribution in many blockchain systems follows a power-law distribution. Therefore, the majority of users control only a small fraction of the total stake, and this aligns well with the oceanic game framework.

Within this model, we initiate a comparison between two reward schemes; the first one is based on the *Shapley value*, as one of the most prominent concepts of profit sharing from game theory. The second one is *proportional sharing*, used extensively in practice.

We analyze the corresponding *non-cooperative games*, induced by these reward schemes, where each player chooses which pool to join. We quantify the attained decentralization through a *Price of Stability* analysis on the set of Nash equilibria. The Price of Stability measures the quality of the *best* Nash equilibrium by comparing it to the ideal non-selfish solution. We employ the Price of Stability rather than the more pessimistic Price of Anarchy, as it is a more appropriate measure in our setting (where, as we will exhibit, some bad but quite unnatural equilibria may arise). The Price of Stability corresponds to an equilibrium that maximizes social welfare, and players will likely attempt to converge to it (or near it). Conversely, the Price of Anarchy corresponds to an equilibrium that minimizes welfare, and it is improbable that players would stabilize at such an equilibrium. With this in mind, we show that the proportional scheme always has an optimal equilibrium (i.e. the Price of Stability equals 1). Not far from this, the Shapley value scheme attains a constant Price of Stability bounded by $4/3$. We complement this with an analysis for the purely atomic model, where the Shapley scheme deteriorates, albeit not by a lot, achieving a bound of 2.

We also consider the resiliency of such schemes against *Sybil attacks*, where the players can split their stake and contribute to multiple pools. Although none of the schemes can completely avoid Sybil attacks, we highlight a potential drawback of the proportional scheme, which can be avoided by the use of the Shapley value. In particular, we prove that under the equilibria of the Shapley scheme identified in the previous sections, the players have no incentive to perform Sybil attacks. On the contrary this is not true for proportional sharing, which is demonstrated with rather simple examples.

Finally, we include a study of some non-linear variations of the proportional scheme. Specifically, we consider the *proportional to square roots* and *proportional to squares* mechanisms, which use subadditive and superadditive reward functions, respectively. We exhibit that both have their drawbacks, regarding our desiderata. Namely the proportional to squares scheme has unbounded Price of Stability whereas the proportional to square roots scheme is more vulnerable to Sybil attacks.

Overall, while our results reveal certain advantages of the proportional scheme, they also discover important drawbacks (cf. Sybil attacks above). At the same time, the Shapley value emerges as a competitive alternative, that can bypass some of the negative aspects of proportional splitting, while maintaining comparable guarantees w.r.t. the Price of Stability for decentralization.

1.2 Related Work

In terms of the model we use, oceanic games were introduced by Milnor and Shapley [24]. In their work, they define the Shapley value and study its properties for a class of cooperative games, namely weighted voting games, when the set of players contains both atomic and non-atomic players. Especially for blockchain systems, the work of [22] revisited and advocated the use of oceanic games for mining. They also studied further aspects concerning the stability of the grand coalition of all players. In our work we consider a non-cooperative model of oceanic games, where we care to evaluate the Nash equilibrium outcomes (i.e., partitions into pools).

Our work is also related to the literature of weighted voting games in social choice theory. This is a class of cooperative games, where the value of a coalition is threshold-based, and reward sharing is viewed as determining the voting power of each player. The main solutions that have been proposed for such games are the core, the Shapley value and the Banzhaf index, and we refer to [11] for an overview of results. The main difference from our model is that we have a non-cooperative game where each strategy profile essentially induces a collection of weighted voting games, one per pool.

The use of solution concepts from cooperative game theory in blockchain applications has been limited so far. In [23] the notion of the core was studied for a model of mining in Bitcoin. They obtained a negative result that the core is empty and hence there is always a motive for some players to deviate. The Shapley value as a reward scheme in mining pool games has also been proposed in [13]. The focus of that work was however on its computational aspects and no game-theoretic analysis was given.

Some closely related works, along a similar spirit are [7] and [20], which present different reward sharing schemes for the Proof of Stake setting. Our difference is that they focus on how the system should allocate rewards to the pools, which are then split in a proportional manner among pool members (after the operator takes a cut). In our case we study an orthogonal question of how the pool should allocate the received rewards among its members. Hence it can be seen as complementary direction to [7].

There are also several papers discussing decentralization from various angles. The work of [4] introduces a model where the utility function of the players is decentralization conscious, in terms of effort exerted. In [6] a different model is analyzed where effort corresponds to committed stake, and is related to Tullock contests. Another attempt more tailored to Proof of Work systems is presented in [1], which highlights the heterogeneity of the costs invested in hardware. Finally, reward schemes are also studied in [16] under a dynamic model focusing on the “rich-get-richer” phenomenon in the long run over blockchain systems. The main difference of all these papers with our work is that they do not study explicitly any pool formation process, as they focus more on the individual effort or possessed resources in their proposed models.

One of the few works that formally studies the properties of proportional sharing for blockchain protocols is by [12]. This is an axiomatic study, tailored to Proof of Work protocols, and demonstrates why the proportional rule can have favorable performance (but in a model without pool formation). Other variants that are studied include the proportional to square roots and the proportional to squares schemes that we also consider. A follow up work with a further axiomatic study is provided in [10]. These models however do not consider any pool formation aspects, and there is no discussion on the performance of these schemes w.r.t. decentralization.

Finally, Sybil attacks have been a major concern for any environment where identity cannot be traced effectively [15]. In the context of auctions, it is often referred to as “false-name” bidding [3]. It is natural that blockchains also offer opportunities for such

manipulations, and general resilience against Sybil attacks seems a utopia [21]. Nevertheless some positive results have also been obtained towards having reward schemes that can potentially deter such behaviors, see e.g., [7].

2 Model and definitions

2.1 The oceanic model with atomic and non-atomic players

We consider a population of stakeholders, say N , in a Proof of Stake protocol, who will be referred to from now on as the players of the underlying game. We will mostly focus on the model of oceanic games, as defined by [24], where the population is split into two types of players. Namely, $N = N_a \cup N_s$, where $N_a = \{1, \dots, n\}$ is a set of n atomic players. Each $i \in N_a$, possesses stake equal to a_i . The remaining players are *small* players, each with a tiny stake $\epsilon > 0$. We let $\epsilon \rightarrow 0$, and we can view N_s as a continuum of infinitesimally small, non-atomic players (i.e., the ocean). We denote by L the total stake possessed by the ocean, which equals the measure of N_s . For convenience we imagine N_s as arranged in the interval $[0, L]$. With this in mind, any subinterval $I \subseteq [0, L]$ corresponds to a mass of players possessing stake equal to the length of I . This model shares some characteristics with the atomic and non-atomic models in congestion/routing games [28].

Available strategies. Every player is considering either to operate a pool or join the pool of some other player. The corresponding game is as follows: every player i needs to choose some index $j \in N$. If she chooses herself, i.e., $j = i$, it means that she is starting her own pool, otherwise she joins someone else's pool. A strategy profile \mathbf{x} specifies a choice of strategy x_i for each player $i \in N$. We say that a strategy profile is *valid* if whenever some player i chooses $x_i = j$, with $i \neq j$, we also have $x_j = j$, i.e., users who do not operate a pool do choose a valid pool to join. Technically, non-valid profiles could also arise in this model, but we will exclude them from our equilibrium analysis, as they lack a natural real life interpretation.

Pool rewards. A valid strategy profile induces a partition of the players into disjoint sets (pools), $\Pi = (S_1, \dots, S_k)$, for some k , so that $\cup_j S_j = N$. Given such a partition, each pool S_j receives a reward $\rho(S_j)$, determined by the execution of the blockchain protocol. In this work, we consider a simple reward function, as an attempt to model the rationale behind the operation of Ethereum or other protocols with a similar design. In Ethereum, a stake holder needs to have 32 ETH in order to register as a validator and claim rewards. This gives rise to a threshold-based scheme, where a pool can obtain rewards when its total stake exceeds a given threshold h . To define this formally, for a given pool $S \subseteq N$, let $m(S)$ be the total stake that it possesses. This consists of two terms; the total mass of stake by the non-atomic players, which equals $|S \cap N_s|$, and the stake of the atomic players, which is equal to $\sum_{i \in S \cap N_a} a_i$. Then, given the threshold h , the reward is equal to:

$$\rho(S) = \begin{cases} 1, & \text{if } |S \cap N_s| + \sum_{i \in S \cap N_a} a_i \geq h \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

We say that a pool $S \subseteq N$ is a winning pool if $\rho(S) = 1$.

► **Remark 1.** For the remainder of the paper, we make the assumption that $a_i < h$, for any atomic player $i \in N_a$. The main reason is that, as also considered in the initial model of oceanic games by [24], we want to focus on players who need to collaborate with other people in order to form a successful pool. If there exist players with $a_i > h$, given our

threshold-based reward function ρ , intuitively it makes sense for them to break their stake and run their own pools with avatars of size h each, and participate in our game with the remainder $a_i \bmod h$. For a further discussion on this, see the full version of this paper [19].

Reward sharing scheme within a pool. Once the pools are formed, the pool members need to split the obtained reward according to some agreed upon scheme.

► **Definition 2** (Reward sharing schemes). *Given a pool $S \subseteq N$ and its reward $\rho(S)$, a reward sharing scheme² specifies a payment allocation $p_i(S)$ to each pool member $i \in S$, dependent on the stake that i contributes to S , so that all the payments sum up to $\rho(S)$.*

► **Remark 3.** We focus on scenarios where the same reward scheme is applied to all formed pools. This is the case for example in protocols with onchain pooling (e.g., Cardano) but also in many of the platforms that facilitate pooling (e.g., for Ethereum). We do not consider secondary effects where pool members may re-negotiate their payments later on, among themselves.

In our model, we have not explicitly defined the cost that a pool may bear towards participating in the protocol. We essentially assume that $\rho(S)$ is the reward that is left for being shared, after subtracting the amount that the pool operator may claim to cover her operational costs.

2.2 Equilibria, Decentralization and Price of Stability

Under any strategy profile, we define the utility of each player to be the reward that she receives. For a non-valid profile, the reward of a player who does not end up in a pool is simply equal to 0. We are interested in profiles that induce a partition into winning pools, and we will denote by $u_i(\Pi)$ the utility of a player under a formed partition $\Pi = (S_1, \dots, S_k)$.

► **Definition 4.** *Given a game G , a partition Π into winning pools is a Nash equilibrium if for every player $i \in N$, $u_i(\Pi) \geq u_i(\Pi')$, for any partition Π' that arises from Π if i moves to a different pool or opens a new pool on her own.*

A major concern in blockchain design is whether the actual execution of the protocol by selfish entities can result in a decentralized configuration. As a metric for this, we use the number of winning pools that are formed at an equilibrium. Given a game, the ideal scenario is that the players split into pools of size exactly h . Since this may not always be possible, we let $OPT(G)$, for a game G , be the maximum number of winning pools that can form over all possible partitions, i.e.,

$$OPT(G) = \max\{t : \exists \Pi = (S_1, \dots, S_t) \text{ s.t. } m(S_i) \geq h \ \forall i \in [t]\} \quad (2)$$

In the purely atomic case, when $N_s = \emptyset$, finding $OPT(G)$ is the dual version of the well known Bin Packing problem, referred to as dual Bin Packing in [2], and is easily seen to be intractable. An interesting question that arises is whether equilibria can lead to an approximate solution. In order to evaluate Nash equilibria, the usual metrics are the Price of Anarchy (PoA) and the Price of Stability (PoS). The Price of Anarchy is not an appropriate metric here as it is unavoidable to have completely centralized equilibria, which are however rather unrealistic. This is captured below.

² Given the form of $\rho(S)$, each pool can be seen as a weighted voting game [11] and the reward to each pool member can be also interpreted as her power within the pool.

▷ **Claim 5.** When $a_i < h$ for all $i \in N_a$, the grand coalition consisting of all players is an equilibrium under any reward scheme, and hence the Price of Anarchy is $\Omega(n)$.

We will therefore turn our attention to the Price of Stability, defined as the ratio between the quality of the optimal solution and the quality of the best Nash equilibrium. Given a partition Π , let $W(\Pi)$ be the number of winning pools that are formed under Π .

► **Definition 6.** *The Price of Stability (PoS) of a game G is computed as $\min_{\Pi \in NE} \frac{OPT(G)}{W(\Pi)}$, where NE is the set of all equilibrium partitions.*

The Price of Stability appears to be an appropriate quality benchmark for the equilibria of the games we consider. As the Price of Stability aligns with maximizing social welfare, the dynamics of threshold-based mechanisms would likely guide players towards more decentralized outcomes.

Finally, we note that all missing proofs in the remainder of the paper can be found in the full version of our work [19].

3 Analysis of the Shapley value reward sharing scheme

In this section, we study the scheme, where the reward in each winning pool is distributed using the Shapley value of each player. The Shapley value was introduced in [30] as the unique reward allocation rule that satisfies a particular set of axioms. Ever since, there is hardly any economic setting involving the sharing of costs or payoffs where the Shapley value has not been considered. Prominent examples are the design of truthful cost-sharing mechanisms [25] and the study of power indices in voting games [11]. Furthermore, despite the fact that the exact computation of the Shapley value is a #P-hard problem [14], there are very efficient sampling-based approximations that work quite well [5, 17]. Even further, the Shapley value has been deployed successfully in practice, in machine learning applications, as a way to identify important parameters in the training of neural networks [29].

3.1 Definition of the Shapley value in the oceanic model

The standard definition and use of the Shapley value is for the purely atomic model, when $N_s = \emptyset$. It is very instructive to recall first how the scheme works there, without any small players.

The atomic model. The rationale for the Shapley value is that within each pool, *each stakeholder gets their expected marginal contribution* if the members of the pool would arrive in a random order. Hence, one needs to take the average over all permutations. The Shapley value for a player i , when she belongs to a pool S is therefore given by the following formula:

$$\phi_i(S) = \sum_{T \subseteq S \setminus \{i\}} \frac{|T|!(|S| - |T| - 1)!}{|S|!} (\rho(T \cup \{i\}) - \rho(T)) \quad (3)$$

This is a valid scheme since it is shown already in Shapley's original work that $\sum_{i \in S} \phi_i(S) = \rho(S)$.

► **Example 7.** Consider a game G with atomic players and stake distribution $\mathbf{s} = (3, 1, 1, 1, 1, 1)$, and let the threshold be $h = 4$. The optimal pool formation is to have two pools, each with total weight 4. Thus $OPT(G) = 2$. However, this is not a Nash equilibrium, because the large player prefers to switch to the other pool: the reward of the

large player in the pool with one small player (with stake vector $(3, 1)$) is $1/2$, while if she joins the other pool with the 4 small players, so that the pool becomes $(3, 1, 1, 1, 1)$, it is $3/5$. Therefore, only the grand coalition can be a Nash equilibrium (which is a rather extreme case, since we will see that in bigger games other equilibria also arise). ◀

Extension to the oceanic model. We discuss now how to compute the Shapley value, when we include non-atomic players. Consider a pool with non-atomic players of total mass k and t atomic players with stakes (a_1, \dots, a_t) ; the total stake of the pool is $k + a_1 + \dots + a_t$. For convenience, we will often refer to the atomic players as *large* players and the non-atomic ones as *small* players. Imagine that the small players are arranged in the interval $[0, k]$. Then a random arrival of the players corresponds to placing arrival times $L_{i_1}, L_{i_2}, \dots, L_{i_t}$ for the atomic players on the interval $[0, k]$. The arrivals can be viewed as filling in the stake $k + a_1 + \dots + a_t$, say starting at 0, from left to right, as follows: first, a mass of small players (possibly empty) arrives, filling in the interval $[0, L_{i_1}]$; then the first large player arrives, so that the stake of the current subset of players accrues to $L_{i_1} + a_{i_1}$. This is followed by another mass of small players; then a second large player arrives at L_{i_2} , accumulating now a total stake of $L_{i_2} + a_{i_1} + a_{i_2}$; and so on. For random arrivals, the points $L_{i_1}, L_{i_2}, \dots, L_{i_t}$ are *uniformly distributed within the interval of length k* . The reward of each large player i is then the probability that the threshold h falls within the interval that makes player i pivotal. To be more precise, for a given arrival order, and for an atomic player i , let $P(i)$ be the set of other atomic players preceding i in the order. Then, if L_i is the random arrival time of player i , the Shapley value is given as follows:

$$\phi_i(S) = Pr \left[\sum_{j \in P(i)} a_j + L_i < h \leq \sum_{j \in P(i)} a_j + L_i + a_i \right] \quad (4)$$

After computing the reward of all large players, the remaining reward is distributed evenly among the small players. Hence, for the small players, all that matters is the reward per unit of stake, which is what we will consider in the game-theoretic analysis that will follow.

3.2 The Price of Stability in the oceanic model

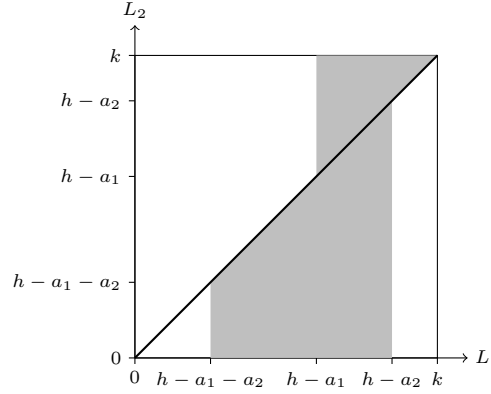
For a pool with many large players along with a mass of small players, the exact formula for the Shapley reward might be too complex to derive analytically. For our study on the Price of Stability however, it will suffice to only consider equilibria in which every pool has at most one large player. Hence, when arguing about equilibria and deviations to other pools, it is sufficient to be able to compute the rewards of pools with at most 2 large players. This is done in the following lemma, which we will use repeatedly.

► **Lemma 8.** *Consider a pool with a mass of non-atomic players equal to k and total stake at least h .*

- *If $k \leq h$ and the pool has a single large player with stake a , the Shapley value of this player is $(k + a - h)/k$.*
- *If $k > h$ and the pool has a single large player with stake a , the Shapley value of this player is a/k .*
- *If $k \leq h$ and the pool has two large players with stakes a_1, a_2 , respectively, the Shapley value of the player with stake a_1 is equal to (with an analogous formula for the second player)*

$$\frac{(h - a_2)^2 - (\max(0, h - a_1 - a_2))^2 + (\max(0, a_1 - h + k))^2}{2k^2}.$$

In all 3 cases above, the remaining reward is distributed equally to the non-atomic players.



■ **Figure 1** Calculation of the Shapley value for the first player in a winning pool of two large players with stakes a_1, a_2 and non-atomic mass of $k \leq h$. It is easy to verify that player 1 is pivotal when (L_1, L_2) is in the gray areas. The gray triangle shows the pivotal cases when $L_1 \leq L_2$, whereas the trapezoid corresponds to the cases with $L_1 \geq L_2$. The reward of player 1 is then the gray area (equal to $((h-a_2)^2 - \max(0, h-a_1-a_2)^2 + \max(0, a_1-h+k)^2)/2$) divided by the total area (equal to k^2). When $h-a_1 > k$, the gray triangle disappears. Similarly, when $h-a_1-a_2 < 0$, the gray trapezoid becomes a triangle.

Proof. Consider a pool with a single large player and with $k \leq h$. We apply the procedure described in Section 3.1 on how to determine the reward of the large players. If L_1 is the random arrival of the single player within the interval $[0, k]$, then the player is pivotal, only when $L_1 \in [h-a, k]$. The probability of this event is $(k - (h-a))/k$, which proves the first part of the lemma.

Suppose now that $k > h$. In that case, the large player is pivotal, only when $L_1 \in [h-a, h]$, and this event occurs with probability a/k .

Finally, for the last part of the lemma, the formula for a pool of two large players, is a bit more complicated. If L_1, L_2 are their random arrival times, we distinguish two cases: $L_1 \leq L_2$ and $L_2 < L_1$. In the first case, player 1 arrives before the second player, and hence she receives a reward when $L_1 \in [h-a_1, k]$. In the second case, player 2 arrives before player 1, which means that for player 1 to be pivotal, it should hold that $L_1 + a_2 \in [h-a_1, h]$. This implies that $L_1 \in [h-a_1-a_2, h-a_2] \cap [0, k]$. The ranges for the values of L_1, L_2 , under which player 1 is pivotal, are depicted in Figure 1. The probability that a random point (L_1, L_2) falls into these areas gives the reward of player 1. ◀

We exhibit below an example to demonstrate how we can construct relatively good equilibria in this game.

► **Example 9.** Fix the threshold at $h = 3$ and consider a population where all large players have stake $a = 2$. Suppose also that there is enough mass of small players, so that we can create a partition into two types of pools. The first type has a single large player and non-atomic players with total mass $k = 2$ (hence each such pool has total stake equal to 4). The second type has only non-atomic players with mass $l = 4$. Let us argue that this partition is a Nash equilibrium.

The reward of each large player, as given by Lemma 8, is $(a-h+k)/k = 1/2$. If the player switches to a pool with only non-atomic players, her reward (by applying now the second part of Lemma 8) will be $a/l = 1/2$, so the player has no reason to switch. Also, if the player switches to a pool with another large player, her rewards will be at most $1/2$, since she will share the reward with another identical large player, and there is also a mass

21:10 Pool Formation in Oceanic Games: Shapley Value and Proportional Sharing

of non-atomic players, who also receive some part of the profit. Furthermore, we can verify that for the non-atomic players, the reward per unit of stake is the same, and equal to $1/4$, in both types of pools. Therefore this partition is a Nash equilibrium. Every pool at this equilibrium has a total stake equal to 4, which shows that for this instance the PoS is at most $4/h = 4/3$. ◀

The previous example also leads to a lower bound on the Price of Stability.

▷ **Claim 10.** The Price of Stability in the oceanic model, is at least $\frac{4}{3}$.

Proof. We consider a special case of Example 9, with $h = 3$. The set of players consists of only one atomic player with stake $a = 2$ and a mass of small players, equal to $m = 4t + 2$, where t is a large integer. The optimal partition for this game would be to have one pool including the atomic player and one unit of non-atomic players, and then have the remaining players form pools of size 3, except the last pool which will have one additional unit. Hence $OPT(G) = 1 + 4t/3$ (assuming that $4t$ is divisible by 3). By the construction of Example 9 above, we know that there exists an equilibrium in which a mass of size 2 forms a pool with the large player, and the remainder $4t$ units of small players form t pools of size 4 each.

For the sake of contradiction, assume that there is a better equilibrium formation that achieves a ratio better than $\frac{4}{3}$, compared to the optimal partition. In this equilibrium, the large player has to be paired with some mass, say of size k , of small players and all other pools have to consist only of small players of mass $l \geq h = 3$. The latter pools have to be of the exact same size otherwise the small players would have an incentive to move. In order for this formation to achieve a better than $4/3$ Price of Stability, it has to be the case that $3 \leq l < 4$. Since, it is an equilibrium it must hold that the large player should not have a motive to move to a pool consisting only of small players, hence by Lemma 8, we have that $\frac{k-h+a}{k} \geq \frac{a}{l} \Leftrightarrow l(k-h+a) \geq a \cdot k \Rightarrow l(k-1) \geq 2k \Rightarrow k > 2$, where the implication holds from the fact that $l < 4$, $a = 2$ and $h = 3$. Moreover, no small agent who has been paired with the large player should want to move to a pool of only small players, and vice versa, so that $\frac{1-\frac{a-h+k}{k}}{k} = \frac{1}{l} \Rightarrow \frac{1}{k^2} = \frac{1}{l} \Leftrightarrow l = k^2$. Combining the facts that $k > 2$ and $l = k^2$, we obtain that $l > 4$ and thus we arrive to the desired contradiction.

Therefore, the Price of Stability is lower bounded by $\frac{4t/3+1}{t+1}$, which tends to $4/3$ as $t \rightarrow \infty$. ◀

Our main result in this section is a matching upper bound, provided that all atomic players have a sufficiently large stake³ and that the total population of small players is sufficiently large.

► **Theorem 11.** *In the oceanic model, and given any constant $\epsilon > 0$, the Price of Stability for the Shapley scheme, is at most $4/3 + \epsilon$, when all large players have stake in $(h/4, h)$ and there is a sufficiently large mass of non-atomic players (dependent on ϵ and the total stake of the large players).*

The remainder of this subsection is devoted to the proof of Theorem 11. Before we proceed, we comment on the type of equilibria that we construct to establish the proof. Following Example 9, we show that such games always possess equilibria where each large player forms a pool together with some mass of non-atomic players and with no other large

³ The theorem requires large players to hold at least $h/4$ stake, which, coincidentally, is also the minimum stake requirement for validators in the Rocketpool platform.

players. We find such equilibria to be natural for the blockchain scenarios that we study (certainly more natural than the grand coalition equilibrium from Claim 5), in the sense that bigger players tend to avoid each other and form pools with less important users. They provide each big player with *skin in the game*, as each of them is the only entity with high enough stake in their pool. Furthermore, they reduce the question on the Price of Stability to upper bounding the mass of non-atomic players in each pool, as demonstrated in the sequel. Finally, we note that some games may also have other equilibria, with more than one large player in some pools, but the existence of more equilibria could only positively (if at all) affect the Price of Stability.

To prove Theorem 11, we start with the following lemma, that provides a characterization for the particular type of equilibria we are after.

► **Lemma 12** (Equilibrium conditions). *Consider a partition of the players into winning pools, where every large player $i \in N_a$ is in a pool with only small players of mass $k_i \leq h$, with $a_i + k_i \geq h$, and all remaining small players are in pools of total mass equal to l , with $l \geq h$. Such a partition is at a Nash equilibrium if and only if the following conditions are satisfied for any large players i, j :*

$$\frac{h - a_i}{k_i^2} = \frac{1}{l} \quad (5)$$

$$\frac{k_i + a_i - h}{k_i} \geq \frac{a_i}{l} \quad (6)$$

$$\frac{k_i + a_i - h}{k_i} \geq \frac{(h - a_j)^2 - (\max(0, h - a_i - a_j))^2 + (\max(0, a_i - h + k_j))^2}{2k_j^2} \quad (7)$$

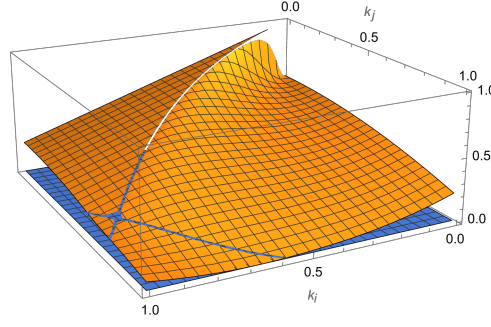
Proof. We focus first on the non-atomic players. Since these players are infinitesimally small, a unilateral deviation of any such player to a different pool does not have any effect on the reward per unit of stake in the pool that she moves to. Therefore, at a Nash equilibrium, all pools with no large player must have the same stake, equal to l in the pools we consider, otherwise the non-atomic players will have an incentive to move to the smallest of these pools.

We consider now deviations of small players either from a pool with no large players to a pool with a large player or the opposite. Constraint (5) rules out such deviations. Indeed, by Lemma 8 the reward that is left over for the non-atomic players in the pool of player $i \in N_a$ is $1 - \frac{a_i - h + k_i}{k_i}$. Since the pool has a mass of size k_i of non-atomic players, the reward per unit of stake for them is equal to $(h - a_i)/k_i^2$. In pools with no large players, the corresponding reward per unit of stake is $1/l$. These two rewards must be equal for non-atomic players in either pool to have no incentive to switch.

Constraints (6) and (7) express the fact that an atomic player i has no reason to switch neither to a pool of non-atomic players nor to the pool of any other atomic player j , respectively. These follow directly by Lemma 8. ◀

We can now show that it is possible to construct such equilibria for a sufficiently large population of non-atomic players.

Proof of Theorem 11. Consider a game that satisfies the premises of the theorem. We will show that there exists a partition into winning pools that is a Nash equilibrium and in which every pool has at most one large player. We will establish that this equilibrium achieves $PoS \leq 4/3$.



■ **Figure 2** The function $f(k_i, k_j)$ of Equation (8). For $k_i, k_j \in [0, 1]$, the minimum value is 0 and it is achieved when $k_i = 2/3$ and $k_j = 1$.

Without loss of generality (simply by scaling), from now on we assume that $h = 1$. We will show that we can find numbers k_1, \dots, k_n , so that we can fill in the pool of each large player $i \in N_a$, with a mass of non-atomic players, equal to k_i , and ensure that the equilibrium constraints of Lemma 12 are satisfied. Let us also make the simplifying assumption that the mass of small players is such that after allocating a mass of size k_i to the pool of each large player i , the remaining mass can be partitioned into pools without large players and with stake of exactly $l = 4/3$. We will revisit this assumption at the end of the proof.

Note that we need $k_i \leq h$ to be able to use Lemma 12. The first constraint (Constraint (5)) is an equality and tells us precisely how much k_i should be in terms of a_i . By solving for a_i , for each i , it should necessarily hold that: $a_i = h - k_i^2/l = 1 - 3k_i^2/4$. Since by the premises of the theorem, $a_i \in (1/4, 1)$, we get that $k_i \in (0, 1)$, i.e., $k_i \leq h$. An immediate implication of the assumption that $l \geq 4/3$ is that Constraint (6) is satisfied for every k_i because it reduces to $(3k_i/4 - 1/2)^2 \geq 0$.

It remains to show that Constraint (7) is also satisfied. By substituting a_i and a_j from Constraint (5), we can see that this last constraint becomes equivalent to $f(k_i, k_j) \geq 0$, where

$$f(k_i, k_j) = 1 - \frac{3}{4}k_i - \frac{9}{32}k_j^2 + \begin{cases} \frac{(3k_i^2 + 3k_j^2 - 4)^2}{32k_j^2} & \text{if } 3k_i^2 + 3k_j^2 \geq 4 \\ 0 & \text{otherwise} \end{cases} - \begin{cases} \frac{(3k_i^2 - 4k_j)^2}{32k_j^2} & \text{if } 3k_i^2 \leq 4k_j \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

The following technical claim can then be established.

▷ **Claim 13.** For any $k_i, k_j \in (0, 1]$, we have $f(k_i, k_j) \geq 0$.

Figure 2 shows a plot of $f(k_i, k_j)$, which demonstrates that it is non-negative for all $k_i, k_j \in [0, 1]$. One can prove analytically Claim 13, using standard arguments and an exhaustive case analysis.

So far, we have established that we can have a Nash equilibrium, with the values of k_i set by (5). Under such a partition, the pools without a large player have size $l = 4/3$, while pools with one large player have size $k_i + a_i = 4/3 - (2 - 3k_i)^2/12 \leq 4/3$. Since the optimal partition, at its best would split the players into pools of total stake equal to $h = 1$, the Price of Stability is at most $4/3$. A matching lower bound is given by Example 9 and Claim 10.

This completes the proof of the theorem when all pools of non-atomic players have stake of exactly $l = 4/3$. If the total stake is such that this is not possible, we can construct a Nash equilibrium with pools of stake $l = 4/3 + \epsilon$, where ϵ can be made arbitrarily small, provided there is a sufficiently large mass of non-atomic players. The preceding argument applies almost identically to this case as well. This complicates some expressions, regarding the function $f(k_i, k_j)$, but it does not affect the core logic of the proof. ◀

An interesting consequence of the theorem's proof is that large players receive more reward at the Nash equilibrium than their proportional share. Specifically, their reward is $(a_i - h + k_i)/k_i$, while their proportional share is $a_i/(a_i + k_i)$. Given that $a_i = 1 - 3k_i^2/4$, we get the following.

► **Fact 1.** *In the Nash equilibria of Theorem 11, when $h = 1$, the reward of a large player in a pool of mass of non-atomic players k_i is more than its proportional sharing by*

$$\frac{k_i(3k_i - 2)^2}{4(2 - k_i)(3k_i + 2)} \geq 0,$$

The extra reward varies between 0 (when $a_i = 2/3$) and 0.05 (when $a_i \approx 1/4$).

3.3 The Price of Stability in the atomic model

In this subsection, we provide an analogous analysis for the atomic case, where we could have again large and small players, but not infinitesimally small, i.e., $N_s = \emptyset$, and therefore $N = N_a$. We believe it is valuable to understand the performance under the purely atomic model as well. This provides a more complete picture for these games and intends to answer the question of whether a low Price of Stability is maintained even without infinitesimally small players. When there are only atomic players, the discrete nature of the problem makes the Price of Stability go up, albeit not by a lot in the cases we consider below. This is consistent with the analogous flavor of results in the analysis of congestion games with atomic and non-atomic players [28].

We start with the following easy observation, showing that we have a worse lower bound when there is no mass of non-atomic players.

▷ **Claim 14.** The analysis of Example 7 yields that in the atomic model, $PoS \geq 2$.

Assumption on the stake distribution. The analysis for the atomic model quickly becomes much more technical and challenging for an arbitrary stake distribution, due to the expression for the Shapley formula. But following the same spirit as with the oceanic model, we have managed to analyze a class of games that follow a separation of N into large and small players. In particular, we will consider a 2-valued stake distribution, so that for every player $i \in N$, either $a_i = 1$ modeling a small player or $a_i = a > 1$, with $a < h$, modeling a large player. We leave as an open problem the analysis for the case where the large players can have different stakes.

Let n_b, n_s be the number of large and small players respectively, so that $n = n_s + n_b$. Our main result of this subsection is the following theorem, where we give a matching upper bound to Claim 14, as long as the number of small players is sufficiently large, so that again the Price of Stability is bounded by a small constant.

► **Theorem 15.** *For instances on $n = n_s + n_b$ players, with $n_s \geq (2h - 1)^2 + n_b \cdot (h + 1)$, it holds that $PoS \leq 2$.*

To prove this, we will construct an equilibrium, with a similar pattern as in the proof of Theorem 11, where each large player forms a pool with only small players. In the atomic model, such partitions are captured by the following definition.

► **Definition 16.** *For 2 integers k, l , with $k + a \geq h$ and $l \geq h + 1$, we say that a partition of N is a (k, l) -partition if it consists only of pools of the following form (without necessarily having pools from all the three types below)*

- Pools with exactly one big player and k small players (Type A pools),
- Pools with l small players (Type B pools),
- Pools with $l - 1$ small players (Type C pools).

A (k, l) -partition that is also a Nash equilibrium is referred to as a (k, l) -equilibrium. The reason we may need both Type B and Type C pools is that the total number of agents assigned to these pools may not be divisible by l or $l - 1$. Furthermore, if we find equilibria where k and l are upper bounded by a small multiple of h , this yields directly a bound on the Price of Stability.

3.3.1 Games with one large player

For the atomic model, it is very instructive (and essentially the core of the proof) to provide first the analysis when we have only one large player with stake a (we fix this to be player 1). All the other players have stake equal to 1. As we will see, this is already a non-trivial case.

We first provide some useful properties that help us understand the Shapley value scheme as well as the structure of its equilibria. The next lemma is the analog of Lemma 8 and is derived by applying the Shapley formula (3).

- **Lemma 17.** *Consider a winning pool S , containing the large player and k small players.*
- *If $k < h$, then the Shapley scheme provides to player 1 a payoff of $\phi_1(S) = \frac{k-h+a+1}{k+1}$. Each of the other players receives a payoff of $\frac{h-a}{k \cdot (k+1)}$.*
 - *If $k \geq h$, then player 1 has a payoff of $\phi_1(S) = \frac{a}{k+1}$. Each of the other players receives a payoff of $\frac{k+1-a}{k \cdot (k+1)}$.*

The following is straightforward by applying (3).

- **Fact 2** (Pools of Type B or C). *Consider a winning pool S consisting of only small players, with $|S| = t$, for some $t \geq h$. Then for every $i \in S$, $\phi_i(S) = 1/t$.*

The next lemma justifies why in Definition 16, it suffices to consider pools of Type B and Type C, regarding the pools containing only small players, in the construction of equilibria.

- **Lemma 18.** *Suppose there exists a Nash equilibrium containing in its partition 2 pools S_1, S_2 , that consist only of small players. Then, it must hold that*

$$||S_1| - |S_2|| \leq 1$$

Therefore, for games with a single large player, when $a < h$, the equilibria of the game must have the format of a (k, l) -partition, for appropriate values of k and l . Each of the pools should have total stake that exceeds the threshold h , so that they are winning pools, and this is why in Definition 16, we enforced that $k + a \geq h$ and $l - 1 \geq h$ ($l \geq h$ some times also suffices if there are no pools of Type C). The next step is to understand how to set the parameters k and l so that a (k, l) -partition is a Nash equilibrium. The following lemma describes a set of sufficient conditions, which are also necessary when the partition has pools of all types (A, B and C). For our purposes, we will stick below to the case that $k \leq h - 1$.

- **Lemma 19** (Sufficient conditions). *Consider a (k, l) -partition with $k < h$. When $k \leq h - 2$, the partition is a Nash equilibrium, if the following conditions hold:*

1. $\frac{k(k+1)}{h-a} \leq l \leq \frac{(k+1)(k+2)}{h-a}$
2. $l \geq \frac{a(k+1)}{k-h+a+1}$

When $k = h - 1$, the only change is that the upper bound in the first condition needs to be replaced by: $l \leq \frac{(k+1)(k+2)}{h+1-a} = \frac{h(h+1)}{h+1-a}$.

Based on the above, we prove below that for large enough games, there always exist Nash equilibria (characterized by the values of k and l), which are relatively good compared to the optimal formation.

► **Theorem 20.** *For instances with a single large player and with $n \geq (2h - 1)^2 + h$, $PoS \leq 2$.*

Proof. We only provide an outline here and omit the proofs of Lemmas 21 and 22, that are stated below, which are the most technical parts of the entire proof. We show that there exists a (k, l) -equilibrium profile, with $l \leq 2h$ and $k + a \leq 2h$. This would mean that all the pools at the equilibrium have stake at most $2h$. Since the optimal formation has pools with stake at least h , the Price of Stability is at most 2.

To ensure the existence of such an equilibrium, we exploit the sufficient conditions of Lemma 19, and we distinguish 2 cases, based on whether we will search for $k \leq h - 2$ or for $k = h - 1$.

Case 1: $h \leq a^2 - 2a + 2$. In this case we will identify a value for k so that $k \leq h - 2$. The first condition of Lemma 19 defines an interval Δ for the possible values of l , which contains at least two integers. This is true since $\frac{(k+1)(k+2)}{h-a} - \frac{k(k+1)}{h-a} = \frac{2(k+1)}{h-a} \geq 2$, for any feasible k , since we are only looking for values of k with $k + a \geq h$. Hence, if the interval Δ belongs entirely to the region for l defined by the second condition of Lemma 19, there exists an equilibrium where both $l - 1$ and l can take an integer value belonging to Δ . In order for this to happen, it must hold that: $\frac{k(k+1)}{h-a} \geq \frac{a(k+1)}{k-h+a+1} \Leftrightarrow k^2 + k(a - h + 1) - a(h - a) \geq 0$.

We can proceed with solving the inequality of degree two, with respect to k . It is easy to check that the discriminant is positive. Hence, by carrying out the calculations, we eventually get that the inequality holds for the integer values that satisfy

$$k \geq k^* = \frac{1}{2}(\sqrt{-3a^2 + h^2 + 2ah - 2h + 2a + 1} - a + h - 1). \quad (9)$$

The remainder of the proof for this case now is to show how to set k and l appropriately.

► **Lemma 21.** *For any pair of integer values of a and h for which $2 \leq a \leq h - 1$, and $h \leq a^2 - 2a + 2$, there are integer values k, l such that: $k \geq k^*$, $h - a \leq k \leq h - 2$ and $h + 1 \leq l \leq 2h$.*

Case 2: $h > a^2 - 2a + 2$. Now we cannot guarantee that $k \leq h - 2$ and we need to follow a different (and in fact simpler) approach. We have again an interval Δ for the values of l , but as we will be looking for $k = h - 1$, we need to use the analogous conditions from Lemma 19. The remaining part for handling Case 2 is by the lemma below.

► **Lemma 22.** *For any pair of integer values of a and h for which it holds that $2 \leq a \leq h - 1$, $h > a^2 - 2a + 2$, there are integer values k, l such that: $h - a \leq k \leq h - 1$ and $h + 1 \leq l \leq 2h$.*

Given Lemmas 21 and 22, we can now describe the equilibrium construction for any $n \geq l^2 + k + 1$ (for the integer values k, l that were determined in Lemmas 21 and 22), and thus for any $n \geq (2h - 1)^2 + 2h$. Since the values for k and l that we found satisfy the equilibrium conditions, all that remains to show is that we can actually partition the n players into such a (k, l) -partition. To do this, we will have $k + 1$ players, including the large player, form one Type A pool. For the remaining $n - k - 1 \geq (l - 1)^2$ players, we first create as many Type C pools with exactly $l - 1$ players as possible. And then, each of the remaining $(n - k - 1) \bmod (l - 1)$ players is added to a different Type C pool, converting it to a Type B pool. This completes the proof of Theorem 20. ◀

3.3.2 Games with more large players

Building upon the results of the previous subsection, we can address the more general case, where there are more large players. Suppose we have n_b large players and n_s small players so that $n = n_b + n_s$. As before, we show that there is again a (k, l) -partition that is an equilibrium and so that each pool has stake at most $2h$. To prove this, we need again to identify sufficient equilibrium conditions. But for this we can still utilize Lemma 19 with one additional condition: that large players have no incentive to deviate to another Type A pool.

3.3.3 Lower bounds for the atomic model with enough small players

For the atomic model, Claim 14 shows that Example 7 provides a lower bound of 2. However the example does not satisfy the premises of Theorem 15, that we have sufficiently many small players of stake 1. Under this assumption the best lower bound we have established is 1.5, as stated below. Therefore, for the atomic model, it remains an open problem whether the Price of Stability is lower than 2 when there is a sufficiently high population of small players or whether Theorem 15 is tight.

► **Theorem 23.** *There exist instances where the number of small players satisfies the assumption of Theorem 15, and where $PoS \geq 1.5$.*

Proof. In order to prove this lower bound of $\frac{3}{2}$ we will consider a simple instance, where there is only one large player with stake $a = 2$, the threshold is equal to $h = 4$, and there is a large amount of small players with stake 1. In this instance, since there is only one “big” player and many small players, the best equilibrium is necessarily in the form of a (k, l) -equilibrium, with the lowest possible value for l . From the conditions of Lemma 19, we have that in a (k, l) -equilibrium it must hold that $\frac{k(k+1)}{h-a} \leq l \leq \frac{(k+1)(k+2)}{h-a}$ and $l \geq \frac{a(k+1)}{k-h+a+1}$. In order to find the best equilibrium, it suffices to find the smallest value of k , for which the two above conditions overlap. This happens for $k = 2$ and the two conditions above become $3 \leq l \leq 6$ and $l \geq 6$. Hence, the only feasible value for l to have a (k, l) -equilibrium is $l = 6 = \frac{3h}{2}$. Given that the optimal formation consists of pools with total stake at least equal to h , this leads us to the lower bound of $\frac{3}{2}$ for the Price of Stability. ◀

4 Optimality of the proportional sharing scheme

We come now to compare the Shapley scheme with the simplest possible scheme that one could apply in this setting, namely proportional sharing.

Recall that for a pool C , we have denoted by $m(C)$ the total stake of the pool, including atomic and non-atomic stake. For atomic players, the proportional share of an agent i is the percentage of her contribution over $m(C)$, where C is the pool that she belongs to. For the non-atomic players, the reward per unit of stake is equal to the profit divided by the total stake of the pool. This is a quite standard and popular rule, that is being used widely in several off-chain and on-chain agreements.

► **Definition 24.** *For a player $i \in N_a$, with stake a_i belonging to a pool C , the reward she receives by the proportional reward sharing scheme is $p_i(a_i, C) = \frac{a_i}{m(C)} \cdot \rho(C)$. For non-atomic players, the reward per unit of stake is $\rho(C)/m(C)$.*

For this scheme, there is always an equilibrium that induces an optimal formation, and this holds for any stake distribution, without the premises of Theorem 11.

► **Theorem 25.** *In the oceanic model, the proportional sharing scheme has Price of Stability equal to 1. This holds independently of the volume of non-atomic players (and hence it holds for the purely atomic model as well).*

Proof. Consider an optimal partition of the players into pools, as defined in (2). If there are multiple optimal partitions, consider the one that is as balanced as possible, i.e., a lexicographically optimal (leximin) one, where the stake of the smallest pool is maximized, and subject to that, the stake of the second smallest pool is maximum, and so on. Let C_1, \dots, C_t be the pools of this partition. It holds that $m(C_j) \geq h$ for any $j \in [t]$.

We note first that all the non-atomic players must belong to the pool (or pools) of minimum stake. If not, we could transfer some stake to the smallest pools and arrive at a lexicographically better one. Hence, for all non-atomic players, the reward per unit of stake is $\frac{1}{\min_j m(C_j)}$. This means that they have no incentive to switch to any other pool, where the reward per unit of stake is lower. Let us consider now the atomic players. If the partition is not an equilibrium, then there exists a player $i \in N_a$, belonging to some pool C_k , who becomes better off by moving to a pool C_r . But then this means that $\frac{s_i}{m(C_k)} < \frac{s_i}{s_i + m(C_r)}$. This implies that $m(C_k) > s_i + m(C_r)$, i.e., that $m(C_k \setminus \{i\}) > m(C_r)$. But then i is included in a pool C_k in the optimal partition that we considered, where even without i , C_k has more stake than C_r . This means that the partition we started with was not a lexicographically optimal partition, a contradiction. ◀

5 Sybil resilience

So far, it may appear that the proportional scheme is a dominating solution within the space of candidate reward schemes. In this section, we highlight one drawback of proportional sharing, which provides an advantage of Shapley, related to the resilience to Sybil strategies. By a Sybil strategy we refer to the act of an atomic player to split her stake into smaller portions so as to participate in different pools, disguised as a set of different players (which can be feasible, given the anonymity in blockchain environments).

5.1 Sybil resilience of equilibria

There are different ways to define Sybil attacks in the literature, depending on the model at hand and on the allowed or feasible behaviors from the players. For our model, we consider Sybil attacks with respect to some given configuration (which may have formed from previous actions that the players took). We also consider that only the atomic players are eligible to perform a Sybil attack.

► **Definition 26.** *Fix a strategy profile inducing a partition Π , of the players into pools. Given Π , a Sybil strategy for a player $i \in N_a$ with stake a_i is a strategy where the player splits her stake into s_{i_1}, \dots, s_{i_t} for some t , with $\sum_{j=1}^t s_{i_j} = a_i$ and chooses t pools to join among the ones formed by Π , contributing stake s_{i_j} to pool j , for $j \in [t]$. The payoff under such a strategy for player i is the sum of the payoffs from all the t pools.*

Based on the above definition of a Sybil attack, below we define the notion of Sybil-proofness (alternatively Sybil-resiliency).

► **Definition 27.** *Fix a partition Π . We say that a reward sharing scheme is Sybil-proof w.r.t. the partition Π if no player i can become strictly better off by switching to a Sybil strategy.*

Ideally, we would like to have reward schemes where no player has an incentive for Sybil attacks regardless of the configuration the game might be at. This is too much to ask for, but we start here with a positive result, that concerns Sybil resilience w.r.t. the equilibrium formations of Section 3. In particular, for the Shapley scheme, we show that even after enlarging the strategy space with Sybil strategies, the equilibrium partitions described in Section 3, continue to be at equilibrium.

► **Theorem 28.** *In the oceanic model, the Shapley value reward sharing scheme is Sybil-proof w.r.t. the equilibria identified in Theorem 11, and more generally w.r.t. any equilibrium as described by the conditions of Lemma 12.*

Proof. Consider an equilibrium formation satisfying the conditions of Lemma 12, with d pools C_1, \dots, C_d . Each pool contains either an atomic player j with stake a_j with a mass of k_j small players (such that $a_j + k_j \geq h$), or a mass of $l > h$ small players.

Suppose that an atomic player i with stake a_i decides to split her stake into m different portions, $s_{i_1}, s_{i_2}, \dots, s_{i_m}$ and commit s_{i_t} to pool C_t , where $\sum_{t \in [m]} s_{i_t} = a_i$. We distinguish the following cases.

Case 1. C_t is the pool that i belonged to initially. Then by Lemma 8, her reward is $\frac{k_i - h + s_{i_t}}{k_i}$.

Case 2. C_t is a pool, with a mass of $l \geq h$ small players. By contributing s_{i_t} to such a pool, Lemma 8 shows that player i receives a reward equal to $\frac{s_{i_t}}{l}$. This is at most $\frac{s_{i_t}}{k_i}$, due to the fact that $k_i < h = 1 \leq l$.

Case 3. C_t is a pool with another atomic player j with stake a_j and a mass of small players k_j . For ease of notation in this case, let $s_{i_t} = b$ and without loss of generality, let $h = 1$. We will establish that the reward player i gets is at most $\frac{b}{k_i}$. After the Sybil attack of player i , C_t contains player j with stake a_j , player i with stake b , and a mass of size k_j of small players. We need to discriminate between some subcases here, since the formula of the reward agent i receives varies. The reward agent i receives, by Lemma 8 is $\frac{(1-a_j)^2 - \max(0, 1-b-a_j)^2 + \max(0, b-1+k_j)^2}{2k_j^2}$.

Since we are in an equilibrium formation, from the conditions in Lemma 12 it holds that $k_i = \sqrt{l \cdot (1-a_i)}$ and $k_j = \sqrt{l \cdot (1-a_j)}$. Also, since $k_i, k_j \leq h$, it holds that $a_i, a_j \in [1-\frac{1}{l}, 1)$. Note also that the function $\frac{b}{k_i} = \frac{b}{\sqrt{l \cdot (1-a_i)}}$, is increasing with respect to a_i . At the same time, for the reward function of player i within pool C_t , we have the following property, which can be easily verified:

▷ **Claim 29.** The function $\frac{(1-a_j)^2 - \max(0, 1-b-a_j)^2 + \max(0, b-1+k_j)^2}{2k_j^2}$, is decreasing with respect to a_j , for $a_j \in [0, 1)$.

So in order to show that $\frac{b}{k_i} \geq \frac{(1-a_j)^2 - \max(0, 1-b-a_j)^2 + \max(0, b-1+k_j)^2}{2k_j^2}$, it suffices to show that this holds for the lowest values that a_i and a_j can take, which is $1 - \frac{1}{l}$.

When $a_i = a_j = 1 - \frac{1}{l}$, it holds that $k_i = k_j = 1$. Given the form of the right hand side, we consider first the subcase that $1 - b - a_j < 0 \Rightarrow b > 1 - a_j = 1 - (1 - \frac{1}{l}) = \frac{1}{l}$. Also note that $b - 1 + k_j \geq 0$, since $k_j = 1$. In this scenario, the Sybil attacker gets reward from C_t equal to $\frac{(1-a_j)^2 + (b-1+k_j)^2}{2k_j^2}$. The desired inequality is equivalent to showing that $2b \geq (1 - (1 - \frac{1}{l}))^2 + b^2 = \frac{1}{l^2} + b^2$, which holds due to the fact that $b > \frac{1}{l} \Rightarrow b > \frac{1}{l^2}$, for any $l \geq 1$ and also $b \geq b^2$, since $b \leq a_i < 1$.

Next, we move to the subcase where $1 - b - a_j \geq 0 \Rightarrow b \leq 1 - a_j = \frac{1}{l}$. Again, $k_i = k_j = 1$, so the desired inequality becomes $2b \geq (1 - (1 - \frac{1}{l}))^2 - (\frac{1}{l} - b)^2 + b^2 = \frac{2b}{l} \Rightarrow 2b \geq \frac{2b}{l}$, which holds for any $l \geq 1$.

Putting everything together, the initial reward player i receives is $\frac{k_i - h + a_i}{k_i}$. Let C_1 be the pool where i belonged to initially, before the Sybil attack. We can then rewrite this as follows

$$\frac{k_i - h + a_i}{k_i} = \frac{k_i - h + (\sum_{t=1}^m s_{i_t})}{k_i} = \frac{k_i - h + s_{i_1}}{k_i} + \sum_{t=2}^m \frac{s_{i_t}}{k_i}$$

But now we can see that each term in the summation is at least as big as the reward received by each pool C_t analyzed in Cases 2 and 3. Also the leftmost term is at least as good as the reward received at Case 1. Hence player i earns more rewards by staking all her stake in her original pool. ◀

Next, we analyze the proportional scheme. In contrast to the Shapley value, and to our surprise, the proportional scheme has a disadvantage here. We show that the optimal equilibrium formation identified in Theorem 25 is not always Sybil-proof.

► **Theorem 30.** *There exist instances where the proportional reward sharing scheme is not Sybil-proof w.r.t. the optimal equilibrium of Theorem 25.*

Proof. We show first a simple example when there is no ocean of small players. Consider an instance with 3 large players, who all have stake $a = h/2 + 1$, and with $h/2 - 1$ additional players, with stake equal to 1. Obviously $OPT(G) = 2$, where the optimal formation is to have 2 pools C_1, C_2 , with C_1 containing two large players together and C_2 containing the remaining players. This is an equilibrium, as follows by Theorem 25, and the payoff for each player in C_1 is $1/2$. Suppose now that one of the large players in C_1 decides to allocate 1 unit of stake to C_2 and keep the remaining stake in C_1 . Her total payoff from this Sybil attack will be equal to $\frac{h/2}{h+1} + \frac{1}{h+1} > 1/2$.

Even when we have a large mass of non-atomic players, one can still have analogous constructions. The reason is that when the total stake of the game is not a multiple of h , the scheme then becomes vulnerable to Sybil attacks. To illustrate this, consider an instance with n atomic players and a mass of small players, such that the total stake is not a multiple of h . This means that in the optimal equilibrium formation of Theorem 25, the pool of maximum stake, say C_1 will have total stake $\ell_1 > h$. Suppose that C_2 is the pool of minimum stake, equal to ℓ_2 , with $h \leq \ell_2 \leq \ell_1$. Let i be an atomic player in C_1 with stake a_i . There exists such a player, since by the proof of Theorem 25, we know that when $\ell_1 > \ell_2$, then C_1 has to contain atomic players (if $\ell_1 = \ell_2$, then we pick as C_1 any pool that contains an atomic player). We argue that agent i can gain more total reward by splitting her stake into two portions, specifically $a_i - x$ which she will commit to her initial pool C_1 and x (s.t. $\ell_1 - x \geq h$, which is feasible if x is small enough), which she will commit to pool C_2 . By this splitting, agent i will receive a total reward of $\frac{a_i - x}{\ell_1 - x} + \frac{x}{\ell_2 + x}$, based on the proportional reward sharing scheme. Suppose now that $\ell_1 = \ell_2 + \delta$, for some $\delta \geq 0$. By simple calculations, we can see that the reward of i under this Sybil attack is greater than her initial reward of $\frac{a_i}{\ell_1}$, as long as

$$x \leq \frac{\ell_2(a_i + \delta) + \delta^2}{2\ell_2 + 2\delta - a_i}. \quad \blacktriangleleft$$

The next definition captures the stronger property that one could envision, i.e., Sybil resilience no matter what is the initial configuration at hand (equilibrium or not).

► **Definition 31.** *A reward sharing scheme is Sybil-proof if it is Sybil-proof w.r.t. any partition Π .*

This is obviously a quite demanding requirement, especially since some partitions may be very unlikely to form in practice. Theorem 30 shows already that proportional sharing does not satisfy it. For the Shapley scheme we can also construct non-equilibrium profiles where Definition 31 fails. To see this consider a partition (C_1, C_2) , where C_1 contains 2 atomic players with stake $a > h/2$ and C_2 contains non-atomic players of mass $l = h$. Then it is easy to verify, using Lemma 8, that a large player from C_1 can keep a stake of $h/2$ in the first pool and contribute the remaining to C_2 resulting in a higher payoff for her.

Hence, when there is no significant cost of carrying out a Sybil attack, we cannot expect to avoid such strategies from any configuration Π , except with trivial schemes (e.g., zero payments). In fact such impossibilities have already been pointed out under a quite different model in [21]. We exhibit below that for our model, this holds beyond the Shapley and the proportional scheme, for a wide class of reward schemes.

► **Observation 32.** *Consider a reward scheme where the payment $p_i(a_i, S)$ of a player with stake a_i in a pool S , depends on a_i and on the stake distribution of S_{-i} but in an anonymous way. Suppose further that the payment is concave w.r.t. a_i , even in a subset of the entire range of $(0, h)$ (with at least one value of a_i where concavity holds with strict inequality). Then the scheme is not Sybil-proof.*

Proof. Consider a partition where player i ends up in a pool S , and where two other pools have formed S_1, S_2 , such that $m(S_1) = m(S_2) = m(S \setminus \{i\})$ and the stake distribution of S_1 and S_2 is the same with the distribution of $S \setminus \{i\}$ (meaning that the composition in terms of the stakes of the atomic players and the volume of the non-atomic players is the same). Then suppose that player i splits her stake a_i into 2 portions of $a_i/2$ and commits it to S_1 and S_2 . Then by the assumption of the theorem, regarding strict concavity, we would have that $p_i(a_i, S) < p_i(a_i/2, S_1) + p_i(a_i/2, S_2)$. ◀

5.2 Computation of Sybil strategies

We conclude this section by commenting on the computational problem of actually finding a good Sybil strategy. For this, fix a player i with stake a_i , and an arbitrary strategy profile of the other players \mathbf{x}_{-i} . Imagine that player i enters the game at a time where the strategies of the other players induce a partition $\Pi_{-i} = (C_1, \dots, C_m)$, where each C_j is a winning pool (we ignore non-winning pools, if there are any, under the current partition). If player i wishes to maximize her utility, the problem that she has to solve is to compute how to split her stake and commit it to different pools in order to receive the maximum possible amount of reward. More formally, let $s_{i_1}, s_{i_2}, \dots, s_{i_m}$, be the variables representing the portions of stake of a_i , that agent i will assign to each of the m pools. Then player i faces the following optimization problem:

$$\begin{aligned} & \text{maximize} && \sum_{j=1}^m p_i(s_{i_j}, C_j \cup \{i\}) \\ & \text{subject to} && \sum_{j=1}^m s_{i_j} \leq a_i \\ & && s_{i_j} \geq 0 \quad \forall j \in [m] \end{aligned}$$

The constraints above are linear but this is not always an easy problem to solve, and its complexity is dependent on the reward scheme, since this affects the form of the objective function. For simpler schemes, such as the proportional one, we can have a polynomial

algorithm. In particular, under the proportional scheme, the objective function is a sum of concave functions (and hence a concave function itself), equal to $\sum_{j=1}^m \frac{s_{ij}}{m(C_j) + s_{ij}}$. This means that the optimization problem is equivalent to minimizing a convex function subject to linear constraints, which can be done efficiently. In fact, for the proportional scheme, we can have an even simpler, greedy algorithm, based on a water-filling argument. Hence, we can conclude with the following.

► **Theorem 33.** *Under the proportional scheme, the optimal solution of the above problem, can be computed in polynomial time.*

Proportional vs Shapley w.r.t. complexity of Sybil attacks. The above algorithm shows that for the proportional scheme, it is relatively easy to find a profitable Sybil attack (whenever one exists). On the other hand, this is not known to be applicable for the Shapley scheme. For the restriction to integer stakes, solving the aforementioned optimization problem is PP-hard [27]. Without integrality constraints, we are not aware of any efficient algorithm. Even if we have access to an approximation algorithm for the Shapley value of a pool, it does not seem obvious how to find an approximately optimal Sybil strategy. Hence the overall computational difficulty of the Shapley value could serve as a deterrent for potential manipulators.

6 Alternative variations of proportional schemes

We conclude our study with some further ideas that have been proposed in the literature. In [12], some alternative schemes are considered, based on variations of proportional sharing. This involves functions that are superadditive in a player's stake. For illustration, we examine the proportional-to-squares reward sharing scheme. Qualitatively, similar results hold if we use other functions of the stake in the form a_i^β with $\beta > 1$.

► **Definition 34.** *For a player i , with stake a_i belonging to a pool C , the reward by the proportional-to-squares reward sharing scheme is $p_i(a_i, C) = \frac{a_i^2}{\sum_{j \in C} a_j^2} \cdot \rho(C)$.*

On the opposite direction, we could have a subadditive function of each player's stake.

► **Definition 35.** *For a player i , with stake a_i belonging to a pool C , the reward she receives by the proportional-to-square-roots scheme is $p_i(a_i, C) = \frac{\sqrt{a_i}}{\sum_{j \in C} \sqrt{a_j}} \cdot \rho(C)$.*

We note that we have presented the definition above only for the purely atomic model, as taking the square or the square root of infinitesimally small quantities leads to uninteresting or trivialized payment rules in the limit. E.g., for a pool with one atomic player and a mass of non-atomic players, the proportional to squares rule would allocate the entire reward to the atomic player.

Even though such schemes can have their merits, we argue here that in our context they also have their drawbacks related to the metrics of the previous sections. We first exhibit that the proportional-to-squares scheme can lead to very bad equilibria, attaining very high Price of Stability.

► **Theorem 36.** *For any h , there exist instances where the proportional-to-squares scheme has Price of Stability at least $\frac{h-1}{2} = \Omega(h)$, and thus unbounded.*

When it comes to the proportional-to-square-roots scheme, the picture is quite different. We can show that the Price of Stability is comparable to the Shapley scheme.

► **Theorem 37.** *Consider instances with n players ($n = n_s + n_b$), so that $n_s \geq h^2 + n_b(\lceil h - \sqrt{a} + 1 \rceil)$. Then, for the proportional-to-square-roots reward sharing scheme, we have that $PoS = 2$.*

However, the proportional-to-square-roots scheme is not Sybil-proof w.r.t. its equilibria, in contrast to the Shapley value.

► **Theorem 38.** *There exist instances where the proportional-to-square-roots scheme is not Sybil-proof w.r.t. (k, l) -equilibria, as given in Definition 16.*

Hence we can conclude that for the family of all considered variants of proportional sharing, we either have vulnerability to Sybil attacks or high Price of Stability.

7 Conclusions

We have studied a model of pool formation over blockchains with large, influential players and players with negligible stake. The conclusions regarding the schemes we considered are as follows.

1. The Shapley scheme has constant Price of Stability bounded by $4/3$ in the oceanic model and by 2 in the atomic model. It is also Sybil-proof w.r.t. the constructed equilibria. Furthermore it is not always easy to find the best possible Sybil strategy.
2. The proportional scheme always has an optimal equilibrium ($PoS = 1$). But it is not Sybil-proof w.r.t. its equilibria. Moreover, Sybil attacks can be computed relatively easily.
3. The proportional to squares scheme has unbounded Price of Stability.
4. The proportional to square roots scheme has constant Price of Stability bounded by 2 . But it is not Sybil-proof w.r.t. its equilibria.

We view this work as a promising initial step towards demonstrating the applicability of cooperative game theory concepts, such as the Shapley scheme, in the context of reward sharing for blockchain protocols. While not exhaustive, our findings provide a foundation for further exploration and development in this area.

7.1 Future work

There are several interesting avenues for future research. An immediate direction is to consider a different function $\rho(S)$ for the pool rewards so as to capture other scenarios or protocols. Our focus for $\rho(\cdot)$ in this paper was a threshold function inspired of validator rewards in Ethereum. However, other schemes are possible for instance, we can consider a model where $\rho(S)$ is a linear (up to a threshold) function of $\sum_{i \in S} a_i$, or other variants that provide additional reward to pools with large pool operators so that some “skin in the game” is present in pool formation, cf. [7]. With respect to this latter property, it would be also interesting to identify skin in the game as a separate or alternative objective (i.e., separate from welfare and the number of independent pools involved at equilibrium). For instance, having skin in the game is reflected in design choices of pool formation contracts like Rocketpool to impose a minimum threshold of 8 ETH to the operator for each pool spun by the system. It is easy to capture such considerations in the oceanic model by observing that skin in the game is not provided by non-atomic players and hence a pool configuration can

only derive skin in the game from the atomic players. Comparing equilibria and the Price of Stability under this objective would be an interesting parallel to the results presented herein, while considering both objectives simultaneously (equilibria exhibiting high decentralization and high skin in the game at the same time) points to an interesting Pareto optimization question.

Another direction is to consider further concepts from game theory, such as the Banzhaf index [11]. This has played a prominent role in weighted voting games, and it would be interesting to explore if it would lead to a performance comparable to the Shapley scheme. Finally, it is also important to investigate the dynamics for the iterated version of pool formation games and the speed of convergence to good equilibria.

References

- 1 Nick Arnosti and S. Matthew Weinberg. Bitcoin: A natural oligopoly. *Management Science*, 68(7):4755–4771, 2022. doi:10.1287/mnsc.2021.4095.
- 2 S. F. Assmann, D. S. Johnson, D. J. Kleitman, and J. Y. Leung. On a dual version of the one-dimensional bin packing problem. *Journal of Algorithms*, 5:502–525, 1984. doi:10.1016/0196-6774(84)90004-X.
- 3 L. M. Ausubel and P. Milgrom. The lovely but lonely vickrey auction. In Peter Cramton, Yoav Shoham, and Richard Steinberg, editors, *Combinatorial Auctions*, pages 18–40. MIT Press, 2006.
- 4 Sarah Azouvi and Alexander Hicks. Decentralisation conscious players and system reliability. In *26th International Conference on Financial Cryptography and Data Security, FC 2022*, pages 426–443. Springer, 2022. doi:10.1007/978-3-031-18283-9_21.
- 5 Yoram Bachrach, Evangelos Markakis, Ezra Resnick, Ariel D. Procaccia, Jeffrey S. Rosenschein, and Amin Saberi. Approximating power indices: theoretical and empirical analysis. *Auton. Agents Multi Agent Syst.*, 20(2):105–122, 2010. doi:10.1007/s10458-009-9078-9.
- 6 Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. Centralization in block building and proposer-builder separation, 2024. arXiv:2401.12120. doi:10.48550/arXiv.2401.12120.
- 7 Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. Reward sharing schemes for stake pools. In *2020 IEEE european symposium on security and privacy (EuroSec)*, pages 256–275. IEEE, 2020. doi:10.1109/EuroSP48549.2020.00024.
- 8 Vitalik Buterin. A next-generation smart contract and decentralized application platform, 2013. URL: <https://github.com/ethereum/wiki/wiki/White-Paper>.
- 9 Vitalik Buterin, Daniël Reijnders, Stefanos Leonardos, and Georgios Piliouras. Incentives in ethereum’s hybrid casper protocol. In *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2019, Seoul, Korea (South), May 14-17, 2019*, pages 236–244. IEEE, 2019. doi:10.1109/BLCC.2019.8751241.
- 10 Burak Can, Jens Leth Hougaard, and Mohsen Pourpouneh. On reward sharing in blockchain mining pools. *Games Econ. Behav.*, 136:274–298, 2022. doi:10.1016/j.geb.2022.10.002.
- 11 G. Chalkiadakis and M. Woolridge. Weighted voting games. In Felix Brandt, Vincent Conitzer, Ulle Endriss, Jérôme Lang, and Ariel D. Procaccia, editors, *Handbook of Computational Social Choice*, pages 377–396. Cambridge University Press, 2016. doi:10.1017/CB09781107446984.017.
- 12 Xi Chen, Christos Papadimitriou, and Tim Roughgarden. An axiomatic approach to block rewards. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 124–131, 2019. doi:10.1145/3318041.3355470.
- 13 Zhihuai Chen, Xiaoming Sun, Xiaohan Shan, and Jialin Zhang. Decentralized mining pool games in blockchain. In *IEEE International Conference on Knowledge Graph, ICKG 2020*, pages 426–432, 2020. doi:10.1109/ICKG50248.2020.00067.
- 14 Xiaotie Deng and Christos Papadimitriou. On the complexity of cooperative solution concepts. *Mathematics of Operations Research*, 19(2):257–266, 1994. doi:10.1287/moor.19.2.257.

- 15 John R. Douceur. The sybil attack. In *Peer-to-Peer Systems, First International Workshop, IPTPS 2002*, pages 251–260, 2002. doi:10.1007/3-540-45748-8_24.
- 16 Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. Compounding of wealth in proof-of-stake cryptocurrencies. In *23rd International Conference on Financial Cryptography and Data Security, FC 2019*, pages 42–61. Springer, 2019. doi:10.1007/978-3-030-32101-7_3.
- 17 Shaheen S Fatima, Michael Wooldridge, and Nicholas R Jennings. A linear approximation method for the Shapley value. *Artificial Intelligence*, 172(14):1673–1699, 2008. doi:10.1016/j.artint.2008.05.003.
- 18 Donald Bruce Gillies. *Some theorems on n-person games*. Princeton University, 1953.
- 19 Aggelos Kiayias, Elias Koutsoupias, Evangelos Markakis, and Panagiotis Tsamopoulos. Pool formation in oceanic games: Shapley value and proportional sharing, 2025. doi:10.48550/arXiv.2505.04422.
- 20 Aggelos Kiayias, Elias Koutsoupias, Francisco Marmolejo-Cossio, and Aikaterini-Panagiota Stouka. Balancing participation and decentralization in proof-of-stake cryptocurrencies. In *17th International Conference on Algorithmic Game Theory, SAGT 2024*, pages 333–350, 2024. doi:10.1007/978-3-031-71033-9_19.
- 21 Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim. Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 110–123, 2019. doi:10.1145/3318041.3355463.
- 22 Nikos Leonardos, Stefanos Leonardos, and Georgios Piliouras. Oceanic games: Centralization risks and incentives in blockchain mining. In *1st International Conference on Mathematical Research for Blockchain Economy, MARBLE 2019*, Springer Proceedings in Business and Economics, pages 183–199. Springer, 2019. doi:10.1007/978-3-030-37110-4_13.
- 23 Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolsky, Aviv Zohar, and Jeffrey S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2015*, pages 919–927. ACM, 2015. URL: <http://dl.acm.org/citation.cfm?id=2773270>.
- 24 J. W. Milnor and L. S. Shapley. Values of large games ii: Oceanic games. *Mathematics of Operations Research*, 3(4):290–307, 1978. doi:10.1287/moor.3.4.290.
- 25 Herve Moulin and Scott Shenker. Strategyproof sharing of submodular costs: Budget balance vs efficiency. *Economic Theory*, 18:511–533, 2001.
- 26 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. URL: <https://bitcoin.org/bitcoin.pdf>.
- 27 Anja Rey and Joerg Rothe. False-name manipulation in weighted voting games is hard for probabilistic polynomial time. *Journal of Artificial Intelligence Research*, 50:573–601, 2014. doi:10.1613/jair.4293.
- 28 Tim Roughgarden. *Twenty Lectures on Algorithmic Game Theory*. Cambridge University Press, 2016.
- 29 Benedek Rozemberczki, Lauren Watson, Péter Bayer, Hao-Tsung Yang, Oliver Kiss, Sebastian Nilsson, and Rik Sarkar. The Shapley value in machine learning. In *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI 2022*, pages 5572–5579, 2022. doi:10.24963/ijcai.2022/778.
- 30 Lloyd Shapley. A value for n -person games. In H. Kuhn and A. W. Tucker, editors, *Contributions to the Theory of Games*, volume 2, pages 307–317. Princeton University Press, 1953.