On the optimality of Shapley value mechanism for funding public excludable goods under Sybil strategies

Bruno Mazorra
Universitat Pompeu Fabra
brunomazorra@gmail.com

February 13, 2024

Abstract

In the realm of cost-sharing mechanisms, the vulnerability to Sybil strategies —also known as false-name strategies, where agents create fake identities to manipulate outcomes— has not yet been studied. In this paper, we delve into the details of different cost-sharing mechanisms proposed in the literature, highlighting their non-Sybil-resistant nature. Furthermore, we prove that a Sybil-proof cost-sharing mechanism for public excludable goods under mild conditions is at least $(n+1)/2-$approximate. This finding reveals an exponential increase in the worst-case social cost in environments where agents are restricted from using Sybil strategies. To circumvent these negative results, we introduce the concept of *Sybil Welfare Invariant* mechanisms, where a mechanism does not decrease its welfare under Sybil-strategies when agents choose weak dominant strategies and have subjective prior beliefs over other players' actions. Finally, we prove that the Shapley value mechanism for symmetric and submodular cost functions holds this property, and so deduce that the worst-case social cost of this mechanism is the nth harmonic number $\mathcal{H}_n$ under equilibrium with Sybil strategies, matching the worst-case social cost bound for cost-sharing mechanisms. This finding suggests that any group of agents, each with private valuations, can fund public excludable goods both permissionless and anonymously, achieving efficiency comparable to that of permissioned and non-anonymous domains, even when the total number of participants is unknown.

Keywords: Permisionless Mechanism design, Cost sharing, Sybil-proof, DAOs

Contents

1 Introduction

Imagine a scenario where a set of agents, want to fund a public excludable good, usually known as a club good. This could be anything from a community-funded park with an entrance fee, a digital platform available only to subscribers, a network-attached storage, or deploying and maintaining a smart contract in a Blockchain where state rental is implemented. The central question is: how do these individuals, or agents with private valuations, collaboratively finance such a good in a setting that is permissionless (maintaining the anonymity of the participants) and also recovers the cost of funding the public good? This paper explores suitable mechanisms for this task. In more permissioned settings, existing mechanisms are studied in the cost-sharing mechanisms literature, like the Shapley value mechanism that offers a solution that recovers the cost of the public good, and is approximately efficient in terms of social cost. But, how do these mechanisms fare in environments where agents operate under pseudonyms? Here, the challenge intensifies as agents might exploit this anonymity to create multiple false identities (known as Sybil or false-name strategies), influencing the outcome to their advantage. This raises two critical questions that we will answer in this paper:

1. Are there mechanisms robust against such strategies while still maintaining efficiency?
2. What are the implications in terms of efficiency when agents use Sybil strategies in equilibrium?

Formally, a mechanism for public excludable goods, usually named cost-sharing mechanism can be conceptualized as involving a set $[n] = \{1, ..., n\}$ of players and a cost function $C : 2^{[n]} \to \mathbb{R}_+$. This function models the cost incurred by deploying the public good as a function of the set of agents that have access to it. Each player i in this set has a private, non-negative value v_i for winning, reflecting their valuation for having access to the good or service in question. In the realm of public excludable goods, the problem is two-fold: determining whether to finance a public good and, if so, identifying the users who are granted access and how much the users have to pay. In the first part of this work, we will focus on the public excludable good problem that is represented by a cost function C where $C(\emptyset) = 0$ and $C(S) = 1$ for every non-empty subset S of players, and in the second part of the paper, we will focus on monotone symmetric submodular cost functions.

The problem of finding, individually rational, truthful, and optimal worst-case social cost is solved in the literature for public excludable goods. However, the advent of the digital age introduces additional complexities, notably the issue of identity misrepresentation. Players capable of creating fake identities or bids can potentially exploit these mechanisms. This phenomenon has been explored in two primary strands of literature: "Sybil attacks" and false-name proof mechanisms.

Our research addresses the intersection of these identity dynamics with cost-sharing mechanisms for public excludable goods. We reveal the susceptibility of conventional mechanisms, such as the Shapley value mechanism, to Sybil attacks and establish constraints on social costs for mechanisms satisfying properties like Sybil-proofness.

Building upon these insights, we introduce a comprehensive framework for analyzing cost-sharing mechanisms in the context of public excludable goods, particularly focusing on Sybil strategies and scenarios with an indeterminate number of agents. We introduce the novel concept of Sybil Welfare Invariant mechanisms, distinguishing them from Sybil-proof mechanisms. These mechanisms maintain economic efficiency outcomes, even when agents deploy Sybil or false-name strategies, ensuring robustness against deceptive behaviors by preserving welfare outcomes, irrespective of the number of participants, real or fictitious.

As we delve deeper into our analysis, a notable finding is that the Shapley value cost-sharing mechanism, despite its vulnerabilities, adheres to this property, ensuring that its welfare outcomes are $\mathcal{H}_n$-approximated, thus establishing an upper bound on the worst-case social cost.

We make several key contributions to the field:

- We introduce a framework to analyse cost-sharing mechanisms for public excludable goods with an unknown number of agents and Sybil strategies.
- We prove that the cost-sharing mechanism for public excludable goods with constant cost functions such as the Shapley value mechanism, the VCG mechanism for public excludable goods, and the potential mechanism are not truthful under Sybil strategies (i.e. are not Sybil-proof).
- Moreover, in theorem 3.6 we prove that cost-sharing mechanisms with constant cost functions that are strong-monotonic, anonymous, individually rational, and Sybil-proof have worst-case welfare social cost lower bounded by $(n + 1)/2$.
- Finally, we introduce Sybil welfare invariant mechanisms, and we prove that the Shapley value mechanism for non-decreasing symmetric and submodular cost-functions holds this property.

Conclusively, our research highlights a significant application of the Shapley value mechanism in the context of decentralized systems like Peer-to-Peer (P2P) Networks and Decentralized Finance (DeFi) platforms. We establish that, despite uncertainties in the number of participating agents, the Shapley value mechanism demonstrates consistent worst-case welfare outcomes. This finding is particularly relevant for decentralized autonomous organizations (DAOs) considering the deployment of public excludable goods.

1.1 Organization of the paper

The paper will be organized as follows. In Section 2, we will introduce tools from mechanism design, cost-sharing mechanism, weak dominant strategy sets and, Bayesian games with private beliefs. In Section 3, we will define an anonymous mechanism and the Sybil extension of single-parameter mechanisms. Moreover, we will prove that some of the most important cost-sharing mechanisms for public goods are not Sybil-proof. Moreover, we generalize it by computing the worst-case welfare of Sybil-Proof mechanism for public excludable goods under some mild conditions. In Section 4, we introduce the concept of Sybil welfare invariant mechanisms, and we prove that the Shapley value mechanism holds this property. Section 5, we present the conclusions of our study and propose directions for future work. Finally, the appendix contains some proofs the results stated in the paper and the notation used.

1.2 Related work

This paper explores the nuanced domain of cost-sharing mechanisms of public excludable goods, particularly emphasizing their non-Sybil proofness guarantees, also known in the literature as false-name proofness. The exploration into this area is rooted in the fundamental work on cost-sharing for public goods and services, where the objective is to allocate costs efficiently among participants. A landmark contribution in this field was made by Moulin and Shenker [6], who discussed the strategy-proof sharing of submodular costs, with budget-balance constraints. This work, alongside Myerson's seminal study [2] on optimal auction design, forms the bedrock of our understanding of mechanisms that incentivize truthful behavior in cost-sharing scenarios. The seminal work of Moulin and Shenker through the Shapley value mechanism [5, 6] initiated a rich vein of research into the efficiency loss of budget-balanced cost-sharing mechanisms. Subsequent studies by Feigenbaum et al. [10] and Roughgarden et al. [21], along with others [16, 15, 12, 28], expanded the understanding of these mechanisms under various constraints and objectives. More aligned with our paper, in [17], the authors proved that no deterministic and budget-balanced cost-sharing mechanism for public excludable good problems that satisfies equal treatment is better than $\mathcal{H}_n$-approximate.

Regarding Sybil attacks [8], where a single malicious entity creates multiple fake identities, pose a significant threat across different domains, from peer-to-peer networks [13, 25] and online social networks [14, 19] to blockchain systems [32], each facing unique challenges due to these attacks.

In the realm of game theory and auction theory, these attacks translate into false-name strategies or shill bids, a concept thoroughly explored in literature. Pioneering work by Yokoo et al. [7, 11] exposed the vulnerability of Vickrey–Clarke–Groves (VCG) mechanisms to such strategies, marking a significant milestone in understanding the intricacies of auction systems under false-name bids. This line of research was furthered by studies on the efficiency of Sybil-proof combinatorial auction mechanisms [24] and the strategic dynamics of shill bidding [27].

Parallel to these advancements, research in non-monetary mechanisms and voting systems, such as the facility location problem [26] and voting rules with costs [18, 35], has been instrumental in characterizing and tackling Sybil-proof mechanisms. These studies highlight the pervasive nature of Sybil strategies across various decision-making and resource allocation systems.

In their exploration of Sybil-proof mechanisms, the authors in [38] have developed a comprehensive framework that is notably adaptable for analyzing Sybil extensions in cost-sharing mechanisms.

2 Preliminaries

In the upcoming section, we delve into the fundamental concepts of mechanism design, focusing on private valuations, the public excludable goods problem, and Bayesian games with private beliefs. These foundational topics lay the groundwork for our more advanced discussions in subsequent sections. Specifically, the insights gained from private valuations and the public excludable goods problem will be crucial for understanding the complexities presented in Section 3. Additionally, the concept of Bayesian games with private beliefs will be pivotal in Section 4, where we examine the Shapley value mechanism under Sybil strategies. It's important to note that this mechanism is not Sybil-proof, and so we use an alternative approach to equilibrium. This preliminary section is designed to equip readers with the necessary theoretical tools to fully grasp the intricacies and challenges of mechanism design in the context of Sybil strategies and non-Sybil-proof environments.

2.1 Mechanism Design Basics

Mechanism design [4], often referred to as the reverse game theory, is a subfield of economics and game theory that focuses on the design of rules and procedures for making collective decisions. While traditional game theory studies how agents make decisions within given rules, mechanism design is concerned with creating the rules themselves to achieve desired outcomes. The central challenge in mechanism design is to ensure that when each participant acts in their own best interest, the collective outcome is still desirable. This is typically achieved by designing mechanisms that align individual incentives with the desired collective outcome.

A particularly important class of problems in mechanism design pertains to situations where agents have private information and/or valuations, and the mechanism designer wants to elicit this information in a truthful manner. This leads to the study of truthful mechanisms. In such mechanisms, agents find in their best interest to report their private information truthfully, rather than misreporting to manipulate the outcome.

One of the most fundamental settings in this context is the single-parameter domain. In these settings, each agent has a single private value (or parameter) that captures its valuation or cost for some service or good. The mechanism designer's task is to determine which agents receive the service (or goods) and at what prices, based on the reported valuations.

A mechanism in this setting can be formally represented as $\mathcal{M} = (\mathbf{x}, \mathbf{p})$, where:

- $\mathbf{x}$ is the allocation rule that determines which agents receive the service based on their reported valuations.
- $\mathbf{p}$ is the payment rule that specifies how much each agent pays or receives based on their reported valuations.

In mechanism design, especially in the context of auctions and allocation problems [3, 20], it is common to assume that agents have private valuations and quasilinear utilities [34, 17] (this is not always the case, but in this paper, we will restrict to this model). This means that the agent's utility depends linearly on the money plus the agent's valuation times the probability of being allocated. We will use the following notation:

- $v_i \in \mathbb{R}$ as agent i's valuation for the item or service.
- $x_i(b_i, b_{-i})$ as the allocation rule which determines the probability that agent i receives the item or service when they report b_i and the other agents report b_{-i}. In this paper, we will focus on deterministic mechanisms, and so we will assume that $x_i(b) \in \{0, 1\}$.
- $p_i(b_i, b_{-i})$ as the payment rule which determines how much agent i has to pay (or receives) when they report b_i and the other agents report b_{-i}.

Then, the quasi-linear utility of agent i when they report b_i is given by:

$$u_i(b_i, b_{-i}) = v_i \cdot x_i(b_i, b_{-i}) - p_i(b_i, b_{-i})$$

For mechanisms to be effective in single-parameter domains, they must satisfy certain properties. One of the most crucial properties is truthfulness, which ensures that agents have no incentive to misreport their valuations. More formally, a mechanism is said to be *truthful* if and only if every agent maximizes their utility by reporting their true type (or valuation) regardless of what the other agents report. That is, for all agents i and for any valuation v_i and reports b_i, and for all possible reports b_{-i} of the other agents:

$$u_i(v_i, b_{-i}) \geq u_i(b_i, b_{-i})$$

The characterization of truthful mechanisms in single-parameter domains is elegantly captured by the following theorem.

Theorem 2.1 (Myerson's Lemma, see [2])**.** In single parameter domains a normalized mechanism $\mathcal{M} = (\mathbf{x}, \mathbf{p})$ is truthful if and only if:

- $\mathbf{x}$ is *monotone*: For all $i = 1, ..., n$, if $b_i' \geq b_i$ and $\mathbf{x}(b_i, b_{-i}) = 1$ implies $\mathbf{x}(b_i', b_{-i}) = 1$.
- *Winners pay threshold payments*: payment of each winning bidder is $p_i = \inf\{b_i | \mathbf{x}(b_i, b_{-i}) = 1 \text{ and } b_i \geq 0\}$.

Myerson's Lemma provides a foundational result for the design of truthful mechanisms in single-parameter domains. It offers a clear characterization of the allocation and payment rules that ensure truthfulness, paving the way for the design of efficient and optimal mechanisms in various applications.

2.2 Weak dominant strategy sets & Private beliefs

Not all mechanisms studied in this paper will be truthful. When the mechanism is not truthful, the agents' information about the number of other players, their valuation, and their potential strategies have a strong implication in agents strategies and the outcome of the mechanism. This is the case in many real-world situations, where players might not have complete information about the game or about other players' types, preferences, or payoffs. Bayesian games, introduced by John C. Harsanyi [1], are a class of games that model such situations of incomplete information. In some cases however, seems unrealistic to exists common knowledge on people preferences, so players might not only have private information about their own types but also hold private beliefs about the distributions of other players' types and strategies. This contrasts with the standard Bayesian games where players share a common prior over types. Games in which players do not share common priors and instead have their own subjective beliefs are referred to as games with *heterogeneous beliefs* or *subjective priors*.

In this setting, there is a set of players $\mathcal{I}$ that is not common knowledge with types $t_i \in T_i$ that can take actions in a topological space A_i for $i \in \mathcal{I}$. Players have utility function $u_i : T_i \times \prod_{i\in\mathcal{I}} A_i \to \mathbb{R}$ unknown to other players such that $u_i(t_i, \cdot)$ is upper-semicontinuous for every $t_i \in T_i$. Every player has a private belief distribution $\mathcal{D}_i$ that models the i-th players' belief of other players taking a vector of actions $(a_i)_{i\in\mathcal{I}}$. More formally, given a set $B \subseteq A_{-i} := \prod_{j\in\mathcal{I}\setminus i} A_j$, the i-th player believes that the probability that the vector of action a_{-i} is in the set B is $\Pr_{\mathcal{D}_i}[B]$. In this setting, we say that a player is *rational with respect to its private beliefs* $\mathcal{D}_i$ and type t_i if they choose strategies in

$$\underset{a_i\in A_i}{\text{argmax}} \quad \mathbb{E}_{a_{-i}\sim\mathcal{D}_i}[u_i(t_i, a_i, a_{-i})].$$

In other words, every player best responds to his/her type and information about the behaviour of the remaining players, while this information can be partial, distorted, or ambiguous [29, 9]. Under some conditions, if the player has type t_i, we can restrict that maximization problem to a subset $\emptyset \neq B_i \subsetneq A_i$. When $B_i(t_i)$ holds the following property, for every action $a_i \in A_i$, there is an action $a_i' \in B_i(t_i)$ such that $u_i(t_i, a_i', a_{-i}) \geq u_i(t_i, a_i, a_{-i})$ for every action profile $a_{-i} \in A_{-i}$. In this scenario, we say that $B_i(t_i)$ is a *subweak dominant strategy set.* Moreover, if

1. for every $a_i \in A_i \setminus B_i(t_i)$, there is an $a_i' \in B_i(t_i)$ such that $u_i(t_i, a_i', a_{-i}) \geq u_i(t_i, a_i, a_{-i})$ for every action profile $a_{-i} \in A_{-i}$ and the inequality is strict for some $a_{-i} \in A_{-i}$, i.e. there exists $a_i' \in B_i(t_i)$ that weakly dominates a_i,

2. for every $a_i \in B_i(t_i)$, there is no a_i' such that weakly dominates a_i.

we say that $B_i(t_i)$ is a *weak dominant strategy set.* An example of (strictly) dominant strategy set on a mechanism is the set $B_i(v_i) = \{v_i\}$ in a second price auction with private valuations where v_i is the valuation of the item of player i.

Lemma 2.2. Given a game $([n], A_i, u_i)$ that for every type t_i has a subweak dominant strategy set B_i such that there exists a chain sets $C_1 \subseteq C_2 \subseteq ...$ such that:

1. $C_j \cap B_i(t_i)$ is sequentially compact for all $j \in \mathbb{N}$ and,

2. $\cup_{i\in\mathbb{N}} C_i = A_i$,

then there exists a unique weak dominant strategy set noted by $\overline{B_i(t_i)}$.

The proof of the lemma utilizes various technical details from elementary topology, and the reader can verify the proof of the lemma in the appendix.

Definition 2.3. A mixed Nash equilibrium with private beliefs for short, NEPB is a tuple of distributions $(d_1, ..., d_n)$ that depends on the tuple of types $(t_1, ..., t_n)$ over the set of strategies such that there exists a tuple of distributions $(\mathcal{D}_1, ..., \mathcal{D}_n)$ that hold:

$$\mathbb{E}_{(a_i,a_{-i})\sim d_i\times\mathcal{D}_i}[u_i(t_i, a_i, a_{-i})] = \max_{a_i\in A_i} \quad \mathbb{E}_{a_{-i}\sim\mathcal{D}_i}[u_i(t_i, a_i, a_{-i})].$$

If the distributions $\mathcal{D}_1, ..., \mathcal{D}_n$ have full support, we say the tuple of distributions $(d_1, ..., d_n)$ is mixed *Nash equilibrium with full support private beliefs* (NESPB).When all elements $(d_1, ..., d_n)$ are atomic with one element (i.e. $\Pr_{d_i}[a_i] = 1$ for some $a_i \in A_i$), we say that the equilibrium is *pure*.

Note that the tuple $(d_1, ..., d_n)$ is a NESPB, and player i has a weak dominant strategy set $B_i(t_i)$ then $\Pr_{d_i}[B_i(t_i)] = 1$. Also, the reader should note that this notion of equilibrium is very weak. Every mixed Nash equilibrium and Bayes Nash equilibrium with common priors are mixed Nash equilibrium with private beliefs. When restricting to the set of NESPB, fundamentally, the only thing that we are imposing for a set of strategies to be a subjective equilibrium is that rational agents take actions from the weak dominant strategy set. This is implicitly done in the literature. This condition is also known as the *no-overbidding* assumption [31]. For example, when a mechanism is truthful, even if reporting truthful valuations to the mechanism is not strictly dominant, but just weakly dominant, it is assumed that agents report their valuations truthfully to the mechanism. Analogously, we extend this idea to non-truthful mechanisms with weak dominant strategy sets. These concepts will be central for the definition of Sybil welfare invariant mechanisms in section 4.

2.3 Public excludable goods

In this section we introduce the notation and key concepts proposed in [17] within the context of cost-sharing mechanism design.

In a cost-sharing mechanism design problem [17, 22], several participants with unknown preferences vie to receive some goods or services, and each possible outcome has a known cost. Formally, we have a service and every player $i \in [n]$ has a valuation function $v_i \in \mathbb{R}_+$. The assumption here is that there are no externalities; each player's value is purely determined by the goods they receive, irrespective of other players accessing the same services. There is a cost function $C : 2^{[n]} \to \mathbb{R}_+$ that specifies the costs of every possible allocation of services.

The section 3 focuses on the study of the *public excludable good* problem, which involves determining whether to finance a public good and, if so, identifying who is allowed to use it. The public excludable good problem has cost function $C(S) = c \in \mathbb{R}_+$ (wlog in this paper we will assume that $c = 1$), for every $S \neq \emptyset$ and $C(\emptyset) = 0$. In section 4 we will study cost-sharing mechanisms with monotone, symmetric and submodular functions C. That is, we assume that there exists a non-decreasing concave function $f : \mathbb{R}_+ \to \mathbb{R}_+$ such that $f(0) = 0$ and $C([n]) = f(n)$ for all $n \in \mathbb{N}$.

A (deterministic) *cost-sharing mechanism* consists of an allocation rule $\mathbf{x} : \mathbb{R}^n_+ \to \{0, 1\}^n$ and a payment rule $\mathbf{p} : \mathbb{R}^n_+ \to \mathbb{R}^n$ that for a reported bid vector profile $\mathbf{b} = (b_1, ..., b_n)$ will determine the set of allocated agents $S = \{i \in [n] : x_i(\mathbf{b}) = 1\}$, and $p_i \geq 0$ is player i's payment. We assume that players have quasi-linear utilities, meaning that each player i aims to maximize $u_i(\mathbf{b}, p) = x_i(\mathbf{b})v_i - p_i(\mathbf{b})$.

In this paper, we will always require the following standard axiomatic properties:

- *No positive transfers* (NPT): Players never get paid, i.e., $p_i(\mathbf{b}) \geq 0$.
- *Individual rationality* (IR): If the allocation is (S, p), players never pay more than they bid, otherwise, they are charged nothing, i.e., $p_i(\mathbf{b}) \leq x_i(\mathbf{b})b_i$.

- *Anonymity/Symmetry*: For any permutation $\sigma \in S_n$, it holds $x_i(\mathbf{b}) = x_{\sigma(i)}(\sigma(\mathbf{b}))$ and $p_i(\mathbf{b}) = p_{\sigma(i)}(\sigma(\mathbf{b}))$.
- *No-Deficit*: For an allocation (S, p), the sum of payments exceeds the costs incurred by providing the service, i.e. $\sum_{i=1} p_i(\mathbf{b}) \geq C(S)$.
- *β-Budget-balance* for $\beta \geq 1$ if for every allocation (S, p) if $C(S) \leq \sum_{i=1}^{n} p_i(\mathbf{b}) \leq \beta C(S)$. In case, that a mechanism is $1-$budget balance, it is said that the mechanism is budget-balanced.
- *Truthful*: Following the definition of truthfulness made in 2.1, a cost-sharing mechanism is truthful if for every bid valuation vector $\mathbf{b}_{-i}$, true valuation v_i and reported valuation $b_i \in V_i$, holds
$$x_i(v_i, \mathbf{b}_{-i})v_i - p_i(v_i, \mathbf{b}_{-i}) \geq x_i(b_i, \mathbf{b}_{-i})v_i - p_i(b_i, \mathbf{b}_{-i}). \tag{1}$$
where S is the allocation with reports $v_i, \mathbf{b}_{-i}$ and S' is the allocation with reports $\mathbf{b}$.
- *Consumer sovereignty* (CS): For all players i and bids $\mathbf{b}_{-i}$, there exist a bid b_i such that player i has access to the public good when the bid profile is $(b_i, \mathbf{b}_{-i})$.

Another weaker version of anonymity [17] is the following:

- *Equal treatment* (EQ): Every two players i and j that submit the same bid receive the same allocation and price.

Furthermore, we assert the following technical property: if all players are served with a specific bid, then those same players are also served for all bids that are larger in their component. Formally,

- *Monotonicity*: For all i, if $x_i(b_i, \mathbf{b}_{-i}) = 1$, then for all $b'_i \geq b_i$, $x_i(b'_i, \mathbf{b}_{-i}) = 1$.

Another stronger version of monotonicity is the following one that states that for every player i, will not have a negative impact on the allocation of the public good if some players increase their bid. More formally:

- *Strong-monotonicity*: For all i, if $x_i(\mathbf{b}) = 1$, then for all $\mathbf{b}' \geq \mathbf{b}$ (that is $b'_i \geq b_i$ for all $i = 1, ..., n$) holds $x_i(\mathbf{b}') = 1$.

This principle implies that an increased valuation of the public good by any number of players will not negatively influence the allocation outcome for all involved players. Essentially, strong monotonicity ensures that higher valuations by some players don't lead to a disadvantageous allocation for others.

Another (stronger) version of strategy-proofness also includes the notion of a mechanism being resistant to coordinated manipulation by users or in other words, preventing users to have incentives to collude in order to individually maximize their utility.

- A cost sharing mechanism is *group strategy-proof* (GSP) if for all true valuations $v \in \mathbb{R}_{+}^{n}$ and all non-empty coalitions $K \subseteq [n]$, there is no $\mathbf{b}$ such that $\mathbf{b}_{-K} = \mathbf{v}$ with $u_K(\mathbf{b}) > u_K(\mathbf{v})$.

Moulin et. al. [5] proved that if a mechanism $\mathcal{M}$ is an upper-semi continuous and group-strategy proof then the mechanism is *separable*, i.e. all players that have access to the public just depends on the set (and not the bid). More formally [22]:

- A *cost-sharing method* is a function $\zeta : 2^{[n]} \to \mathbb{R}_{\geq 0}^{n}$ that associates each set of players to a cost distribution, where for all $S \subseteq [n]$ and all $i \notin S$ it holds that $\zeta_i(S) = 0$. A cost-sharing mechanism $\mathcal{M} = (\mathbf{x}, \mathbf{p})$ is *separable* if there exists a cost-sharing method ζ such that $\mathbf{p}(\mathbf{b}) = \zeta(S(\mathbf{b}))$, where $S(\mathbf{b}) = \{i \in [n] : x_i(\mathbf{b}) = 1\}$.

Observe that if the mechanism is separable and symmetric and C is symmetric (i.e. $C(S)$ just depends on the number of elements in S) then $\zeta_i(S) = \zeta_j(S)$ for all $i, j \in S$.

Now, for economic efficiency, the service cost and the rejected players' valuations should be traded off as good as possible. A measure for this trade-off is the *social cost* of function $\pi : 2^{[n]} \to \mathbb{R}_{\geq 0}$. Given the cost C and the true valuations functions $v_1, ..., v_n$, social costs are defined by

$$\pi(S) := C(S) + \sum_{i \notin S} v_i.$$

That is, the social cost of an allocation S is the cost of granting access to the public good to S players, and the valuations of the agents that do not have access to the public good.

A mechanism is said to be α-approximate [17], with respect the social cost objective if for every tuple of valuations $(v_1, .., v_n)$, the allocation S of the mechanism satisfies

$$\pi(S) \leq \alpha \pi(S^\star) \tag{2}$$

where $S^\star$ is the optimal allocation, that is, the allocation that minimizes the social cost. As an observation, a mechanism is $\alpha-$approximate for some $\alpha \in \mathbb{R}^+$ if and only if the mechanism holds the consumer sovereignty property [17][1]. Is know, [17] that there are nor better than $\mathcal{H}_n$-approximated randomized or deterministic truthfully and no-deficit mechanism, where $\mathcal{H}_n = \sum_{i=1}^{n} \frac{1}{i} = \Theta(\log(n))$.

Let us justify why is more economically efficient to fund excludable goods than non-excludable ones with private valuations. If we place the constraint that all or non must be served the public good (making the public good non-excludable), we have that all non-deficit truthfully mechanisms are at least $(n - 1 + 1/n)-$worst-case welfare. Let's prove it. Assume that the cost of the public good is $c = 1$ without lost of generality. Now, suppose that there is a mechanism $(\mathbf{x}, \mathbf{p})$ with this constraint. Assume that all players have valuation $v_i = 1 - \varepsilon$ and suppose that all agents have access to the public good, for sufficiently small ε (otherwise, the mechanism has worst-case welfare lower bounded by n finishing the proof). Let $p_1, ..., p_n$ be their respective payment. Since the mechanism has no-deficit, we know that $\sum_{i=1}^{n} p_i \geq 1$. And so, there exists i such that $p_i \geq 1/n$. Therefore, the vector profile $(1 - \varepsilon, ..., 1/n - \varepsilon, ..., 1 - \varepsilon)$ has the empty allocation, leaving to a social cost $n - 1 + 1/n - n\varepsilon$. Making ε converge to zero, we obtain that the mechanism is at least $(n - 1 + 1/n)-$worst-case welfare.

3 Sybil-Proof and Cost-sharing mechanisms

Note that the given definitions in the preliminaries presume the mechanism designer is aware of the number of identities. Additionally, agents can only submit a bid to the mechanism without the ability to create or alter other identities to influence the mechanism. However, in general, this is not true. For example, one can create multiple identities to access a social network, multiple bank accounts to bid in an ad auction [23] or use multiple public keys to interact with a DeFi protocol [36, 38]. This provides a new challenge and problems that are worth studying in permissionless mechanism design. For example, in [17] the authors analyze two different truthful mechanisms for public excludable good. The VCG mechanism and the Shapley value mechanism. For completeness, we will write these mechanisms in this section. The first one is efficient (welfare maximizer) however, in general, has deficit (i.e. the users' payments do not cover the costs incurred by financing the public good). The second one, the shapley value mechanism, is budget-balance, however, has $\mathcal{H}_n$-approximately welfare, where $\mathcal{H}_n$ are the harmonic numbers. Moreover, the authors prove that this mechanism is worst-case welfare optimal (up to a constant)

[1] One of the implications is not proved explicitly in the paper but the argument of the proof is fundamentally the same to the other implication.

in the set of truthful, incentive-compatible, budget-balance, and equal treatment mechanisms. However, none of these mechanisms are truthful in the permissionless setting. In other words, [38], the mechanisms are not Sybil-proof/false-name proof.

In this section, we will discuss the public excludable good in permissionless settings. First, we will formalize the public excludable good problem with an unknown number of identities where agents can use Sybils to maximize their payoff. Then, we will prove that the VCG mechanism, the Shapley value mechanism and the potential mechanism are not Sybil-proof. Moreover, we will generalize it by proving that all non-deficit, strong-monotonic, and truthful mechanisms are at least $(n+1)/2-$approximated. In other words, we will effectively establish both upper and lower bounds for the worst-case social cost match. This finding underscores a critical trade-off: achieving a completely strategy-proof (truthful, resistant to Sybil attacks, and immune to group strategies) cost-sharing mechanism necessitates a compromise in terms of economic efficiency.

3.1 Sybil extension of Cost-sharing mechanisms

In general, truthfulness captures the idea that players cannot act strategically in order to obtain more utility from the mechanisms. However, in pseudo-anonymous environments such as blockchain, this is not necessarily true [38], since players can create multiple identities and strategically manipulate the outcome of a truthful mechanism. When agents have no incentives to create multiple identities, we say that the mechanism is Sybil-proof or false-name proof [38]. To define it, we must extend the definition of a mechanism when 1) the number of identities is unknown 2) users can use more than one identity. This is presented in [36] and is called the Sybil extension mechanism. First, we have to define the mechanism with unbounded but finite number of players, called *anonymous mechanism.* An anonymous mechanism $\mathcal{M}$ is a sequence of maps $\{(\mathbf{x}^n : \mathbb{R}^n_+ \to \{0,1\}^n, \mathbf{p}^n : \mathbb{R}^n_+ \to \mathbb{R}^n_+)\}_{n\in\mathbb{N}}$ such that the following two properties hold:

- *Anonymity*: The maps $\mathbf{x}^n$ and $\mathbf{p}^n$ are equivariant under the action of S_n, that is, for all $\sigma \in S_n$, $b \in \mathbb{R}^n_+$, $\mathbf{x}(\sigma b) = \sigma \mathbf{x}(b)$ and $\mathbf{p}(\sigma b) = \sigma \mathbf{p}(b)$.
- *Consistency*: Let $i_{n,m} : \mathbb{R}^n_+ \hookrightarrow \mathbb{R}^m_+$ be any inclusion map that comes from taking the identity map on the first n components and zero-filling the remaining $m-n$ components and permutating the m components by a permutation of S_m. Let $p_{n,m} : \mathbb{R}^m_+ \to \mathbb{R}^n_+$ be the projection such that $p_{n,m} \circ i_{n,m} = id_{\mathbb{R}^n_+}$. Then, the following diagram commutes[2]:

$$\begin{tikzcd}
\mathbb{R}^n_+ \arrow[r, "\mathbf{x}^n"'] \arrow[d, hook, "i_{n,m}"'] \arrow[dr, phantom, "\circlearrowleft"] & \{0,1\}^n \arrow[d, hook, "i_{n,m}"] \\
\mathbb{R}^m_+ \arrow[r, "\mathbf{x}^m"'] & \{0,1\}^m
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{R}^n_+ \arrow[r, "\mathbf{p}^n"'] \arrow[d, hook, "i_{n,m}"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{R}^n_+ \arrow[d, hook, "i_{n,m}"] \\
\mathbb{R}^m_+ \arrow[r, "\mathbf{p}^m"'] & \mathbb{R}^m_+
\end{tikzcd}$$

Now, given an anonymous mechanism, we can define the *Sybil extension mechanism.* The Sybil extension mechanism of an anonymous mechanism $\{(\mathbf{x}^n, \mathbf{p}^n)\}_{n\in\mathbb{N}}$ consists of extending action space of each player i from $\mathbb{R}_+$ to $\mathbb{R}^\infty_+$. Every agent i can report a finite with arbitrary length set of bids $b_i = (b_i^1, ..., b_i^{k_i}, 0, 0, ...)$, for some $k_i \in \mathbb{N}$, and we define $K_i = [k_i]$. Then, we take $m = \sum_{i=1}^n k_i$, $\mathbf{b} = (b_1, ..., b_n)$ and compute $x_j(\mathbf{b})$ and $p_j(\mathbf{b})$ for every $j = 1, ..., m$. This is well-defined since the mechanism $(\mathbf{x}^m, \mathbf{p}^m)$ is symmetric. Now, the total payment of player i consists of the sum of payments of its Sybil identities. That is, $\mathbf{p}_i(\mathbf{b}) = \sum_{j\in K_i} p^m_j(\mathbf{b})$. In

[2] **Category theory observation**: If we take A_n to be the set of symmetric mechanisms with n agents, and $f_n : A_n \to A_{n-1}$ to be $(\mathbf{x}^n, \mathbf{p}^n) \mapsto (\mathbf{x}^n \circ i_{n-1,n}, \mathbf{p}^n \circ i_{n-1,n})$, then anonymous Sybil mechanisms are elements of the inverse limit

$$\varprojlim A_i = \{(a_i)_{i\in\mathbb{N}} \mid a_i \in A_i \text{ for all } i \in \mathbb{N} \text{ and } f_{ij}(a_j) = a_i \text{ for all } i \leq j\}.$$

this paper, we consider that the players' allocation, is the best allocation among all its Sybils' allocation. That is, $\mathbf{x}_i(b_i) = \max_{k \in K_i}\{x^m_k(b_i, b_{-i})\}$. Therefore, its utility is

$$v_i \max_{k \in K_i}\{x^m_k(b_i, b_{-i})\} - \sum_{k \in K_i} p^m_k(b_i, b_{-i}), \tag{3}$$

where b_{-i}. We note the mechanism $(\mathbf{x}, \mathbf{p})$ as the Sybil extension mechanism and denote it by $\mathbf{Sy}(\mathcal{M})$. Observe that in this definition of agents utility in the Sybil setting, we are assuming that the agents have no extra utility to have more Sybil identities to have access to the public good. The motivation for this particular type of Sybil extension stems from the nature of the mechanisms involved, which are geared towards funding and using public goods. In these scenarios, agents gain no additional utility from possessing multiple identities. This is because access to the public good is not enhanced by having more than one identifier. In simpler terms, if the mechanism employs a whitelisting process for identifiers, having more than one does not provide any extra benefit to the users. Once a user has one identifier, they already have the necessary access to utilize the public good. Thus, multiple identifiers do not translate into increased utility in the context of these public goods funding mechanisms. In this context, we say that an anonymous mechanism is Sybil-proof if no agents have incentives to create Sybil identities to increase its payoff. More formally:

- An anonymous cost-sharing mechanism is *Sybil-proof* if for every player i, every vector $b_{-i} \in \mathbb{R}^\infty_+$ of bids, bid vector $b_i \in \mathbb{R}^\infty_+$ with sybils K_i, we have that

$$v_i \mathbf{x}_i(v_i, \mathbf{b}_{-i}) - \mathbf{p}_i(v_i, b_{-i}) \geq v_i \max_{k \in K_i}\{x^m_k(b_i, b_{-i})\} - \sum_{k \in K} p_k(b_i, b_{-i}). \tag{4}$$

In other words, the mechanism is Sybil-proof if the Sybil extension mechanism is truthful.

3.2 Limits of Sybil-Proof cost-sharing mechanisms

We will see next that the mechanisms proposed in [17] and [30] are not Sybil-proof. The mechanisms proposed in [17] are the VCG mechanism applied to the excludable public good problem and the Shapley value mechanism. On the other hand, the mechanism proposed in [30] is a modified version of the VCG mechanism with adding a cost per user. In the following, we will describe these mechanisms for completeness.

Cost-sharing mechanism for public excludable goods

Input: Bids $b_1, ..., b_n$.
Output: The set of agents $S^\star$ that are served and the payment vector $p = (p_1, ..., p_n)$.
VCG mechanism

1. Choose the outcome $S^\star = [n]$ if $\sum_{i=1}^{n} b_i > 1$ and $S = \emptyset$ otherwise.
2. Charge each player $i \in [n]$ the amount $p_i = \max\{0, \sum_{j\in[n]\setminus i} b_j\}$.

Shapley mechanism for submodular monotone cost functions

1. Order the bids in descending order, wlog $b_1 \geq b_2 \geq ... \geq b_n$.
2. Take $k = \text{argmax}_i\{b_i \geq C([i])/i\}$.
3. The players $i = 1, ..., k$ have access to the public good, i.e. $S^\star = [k]$ and each player pays $p_i = C([k])/k$ for $i = 1, ..., k$.

Potential mechanism

1. Choose the outcome $S^\star \in \text{argmax}_{S\subseteq[n]} \left\{\sum_{i\in S} b_i - \mathcal{H}_{|S|}\right\}$.
2. Charge the players $i \in S^\star$ the amount $p_i = [\sum_{i\in S^\star_{-i}} b_i - \mathcal{H}_{S^\star_{-i}}] - [\sum_{i\in S^\star\setminus i} b_i - \mathcal{H}_{S^\star}]$ and zero otherwise. Where $S^\star_{-i}$ is the set that maximizes the previous function with $b_i = 0$.

Observation 3.1. All the previous mechanisms are symmetric, individually rational, and truthful [17]. The potential mechanism and the Shapley value mechanism have no deficit, while the VCG mechanism has deficit [17, 30]. Moreover, the Shapley value mechanism is group strategy-proof. Finally, all mechanisms are strong-monotonic.

Before stating the results, we must extend the definition of C to capture the cost of developing the public good with an arbitrary number of sybils. The extension of the cost function is defined, as one would anticipate, by $C(S) = C([n])$ for every $\emptyset \neq S \subseteq \mathbb{N}$ in case of the public goods problem. Otherwise, we will assume that the cost function is a monotone symmetric function $C : 2^{\mathbb{N}} \to \mathbb{R}_+$.

Proposition 3.2. The Shapley mechanism, the VCG for public excludable goods, and the potential mechanism are not Sybil-proof.

Proof. Wlog we assume that C is constant 1 for non-empty subsets. We prove it separately for each mechanism.

VCG-mechanism: Assume that there are two players with valuations $v_1 = v_2 = 1/3$. In this case, the public good is not funded and so $S^\star = \emptyset$. In this case, the utility of this outcome is zero for both players. If the first player generates two identities 3 and 4 and bids $v_3 = v_4 = 1$, then the allocation is $S = \{1, 2, 3, 4\}$ and the payment of all players is 0. In this case, the utility of the player is 1/3 and so the mechanism is not Sybil-proof.

Shapley value mechanism: Now, let's assume that there are three players with valuations $v_1 = 1 + \varepsilon$ and $v_2 = v_3 = 1/3 - \varepsilon$. Then, the outcome of the mechanism is $S = \{1\}$ with $p_1 = 1$, and so, has utility ε. On the other hand, player 1 splits its bid in two $b_1 = 1/4$ and $b_1 = 1/4$, and the outcome is $S = \{1, 2, 3, 4\}$ with total payment $p = 1/2$, therefore the total utility $1/2 + \varepsilon$. Therefore, the mechanism is not Sybil-proof.

Potential mechanism: Assume that the valuations are $v_1 = 1 + \varepsilon$ and $v_i = 1/i - \varepsilon$ for $i = 2, ..., n$. Then, the allocation of the potential mechanism is $S^\star = \{1\}$ and payment $p_1 = 1$. If the first player creates a Sybil with valuation $v_{n+1} = 1+\varepsilon$, then, in this setting, the allocation is $S^\star = [n+1]$. Now, let us compute the payment. We have that $S^\star_{-1} = \{n+1\}$ and $S^\star_{-(n+1)} = \{1\}$. Therefore, the payments are:

$$p_{n+1} = -[1+\varepsilon+\sum_{i=2}^{n}(1/i-\varepsilon) - \mathcal{H}_{n+1}] = 1/(n+1) - (n-2)\varepsilon$$

and analogously $p_1 = p_{n+1}$. When ε tends to 0, with the Sybil strategy, the utility of the player is $1 - 1/(n+1) > 0$, making the strategy profitable. □

Observe that this is not true for generic cost functions. For example, for symmetric additive cost functions, i.e. $C(S) = |S|$ the Shapley-value mechanism is Sybil-proof and welfare maximizing. The proof is actually simple. The Shapley value mechanism with additive valuation allocated the public good to the bidders with cost larger than 1 and the payment is 1 for each player, therefore making Sybils increase the payments. And so, in this section, we will focus on constant cost functions.

The last proposition opens the following question. What is the maximum $\alpha(n)$ such that there is a $\alpha(n)-$approximated truthful, no-deficit, and Sybil-proof cost-sharing mechanism? By [17], we know that the unique truthful, incentive-compatible, budget-balance, equal treatment, and upper continuous mechanism is the Shapley Value mechanism. Therefore, to have Sybil-proof mechanism, we will have to sacrifice at least one of the previous properties. If we sacrifice budget-balance, we will obtain the Optimal Sybil-Proof mechanism (the use of the word "optimal" will be clear by the Theorem 3.6).

Optimal Sybil-Proof mechanism

1. Accept bids $b_1, ..., b_n$.
2. Order the bids in descending order, wlog $b_1 \geq b_2 \geq ... \geq b_n$.
3. Take $k = \text{argmax}_i\{b_i \geq C([n])/2\}$.
4. If $k = 1$, then do not allocate the public good to any player and set the payments to zero, unless $b_1 \geq C([n])$, then serve the public good to the first player and set $p_1 = C([n])$. Otherwise, the players $i = 1, ..., k$ have access to the public good and each player pays $p_i = C([n])/2$ for $i = 1, ..., k$, and $p_i = 0$ for the remaining players.

Proposition 3.3. The Optimal Sybil-Proof mechanism is individually rational, group-strategy proof, Sybil-proof, non-deficit, and $(n+1)/2-$approximate.

Proof. Again, wlog we assume that $C(S) = 1$ for all $S \neq \emptyset$. Observe that the mechanism is separable with function $\zeta(S) = \begin{cases} \frac{1}{2}, \text{ if } |S| \geq 2, \\ 1, \text{ if } |S| = 1, \\ 0, S = \emptyset \end{cases}$ and so is incentive compatible and group strategy-proof. See [22] for more details. The non-deficit condition follows by construction. The worst-case welfare can be proved by considering the bid vector profile $(1-\varepsilon, 1/2-\varepsilon, ..., 1/2-\varepsilon)$ for $\varepsilon > 0$. Observe that no player is allocated and so the social cost is $n/2 - n\varepsilon$. Making $\varepsilon \to 0$, we obtain that the worst-case social cost is lower bounded by $n/2+1$. Now, lets prove that the worst-case welfare is upper bounded by $(n+1)/2$. Lets $v_1 \geq ... \geq v_n$ be a bid vector profile. Suppose that the first k are allocated the public good. If $k = 0$, then $v_1 < 1$, and $v_2, ..., v_n < 1/2$, therefore the social cost is upper bounded by $1 + (n-1)/2$. If $k \geq 1$, then $n-k$ players do not have access to the public good, and so, having valuations $v_i < 1/2$ for $i = k+1, ..., n$. And so, again the social cost is bounded by $(n+1)/2$. This concludes the proof that the mechanism is $((n+1)/2)-$approximate. The mechanism is clearly Sybil-proof. Given a vector of reports $v_1, ..., v_n$, if just one is allocated, then its payment is 1. Making a Sybil will not decrease its payment since at most will decrease the payment of the original identity, from 1 to 1/2 but will add the payment of the Sybil identity $C([n])/2$.

□

We will prove that this upper bound on social costs matches the lower bound when the mechanism is group strategy-proof and Sybil-proof. In fact, we will prove a more general result, that states that every cost-sharing mechanism that is individually rational, $\alpha(n)-$approximate, no-deficit, symmetric, truthful, strong-monotonic, and Sybil-proof, then $\alpha(n) \geq (n+1)/2$. In other words, to add Sybil-proofness and strong-monotonicity, we must increase exponentially the worst-case social cost from $\mathcal{H}_n$ to $(n+1)/2$.

To make the proof more understandable, we will break the proof into different Lemmas and propositions. In the proof, we assume without loss of generality that C is constant 1 for non-empty subsets. From now on, we will fix the mechanism $(\mathbf{x}, \mathbf{p})$ and assume that holds all previous stated properties.

Lemma 3.4. If a cost-sharing mechanism is strong-monotonic, anonymous, truthful, individually rational, and Sybil-proof, then for every $\mathbf{b}$, such that $b_i \geq b_j$, holds that $x_i(\mathbf{b}) \geq x_j(\mathbf{b})$.

Proof. Let us prove it by contradiction. Suppose that there exists $\mathbf{b}$ such that $b_i \geq b_j$, and $x_i(\mathbf{b}_i) < x_j(\mathbf{b})$. The case where $b_i = b_j$ is not possible since the mechanism is symmetric and in particular holds the equal treatment property. Therefore, we will assume that $b_i > b_j$. Now, we have that $x_i(\mathbf{b}) = 0$ and $x_j(\mathbf{b}) = 1$. By strong monotonicity, $x_i(\mathbf{b}_{-j}, 0) = 0$. If the valuation vector profile is $\mathbf{b}_{-j}$, then the utility of the player i is zero. On the other hand, if the agent i reports another Sybil with bid b_j, the public good is allocated to the agent since j is his Sybil. By incentive compatibility, the j identity pays at most b_j. So the total utility of the player reporting the bids (b_i, b_j) is at least $b_i - b_j > 0$, making the mechanism not Sybil-proof, leading to a contradiction. □

Now, consider the following sequence:

$$v_n = \sup_{v \geq 0}\{v \mid \mathbf{x}(v_1 - \varepsilon, ..., v_{n-1} - \varepsilon, v) = \vec{0}, \text{ for all } \varepsilon \in (0, \min\{v_i : i, ..., n-1\})\}$$

Observe that since the mechanism is no-deficit, we have that $v_1 \geq 1$. For a given $\varepsilon > 0$, we define $\mathbf{v}^n(\varepsilon) := (v_1 - \varepsilon, ..., v_n - \varepsilon)$.

Proposition 3.5. Let $\{v_n\}_{n\in\mathbb{N}}$ be the sequence defined previously. Then:

1. The sequence is well defined and is monotone non-increasing, i.e. $v_n \geq v_{n+1}$ for every $n \in \mathbb{N}$.

2. If $v_{n-1} > v_n$, then for every $v \in (v_n, v_{n-1})$, there exists $\delta > 0$ such that for all $\varepsilon \in (0, \delta)$, the vector profile $(v_1 - \varepsilon, ..., v_{n-1} - \varepsilon, v)$ has allocation $S = [n]$.

3. If $v_{n-1} > v_n$, then there exists a $\delta > 0$ such that for every $\varepsilon \in (0, \delta)$ the bid vector profile $\mathbf{w}^n(\varepsilon) = (v_1 - \varepsilon, v_1 - \varepsilon, ..., v_n - \varepsilon)$ has the total allocation set, i.e. $S = [n]$.

4. For every n, it holds $v_1 \leq 2v_n$.

5. It holds $\sum_{i=1}^{n} v_i \leq \alpha(n)$.

Proof. 1. If $\alpha(n)$ is finite, then it implies that the mechanism is consumer sovereign for n players (otherwise the worst-case social cost would be infinite, see a similar proof in [17]). Therefore, v_n must be finite for every n, otherwise, the worst-case social cost would be infinite, contradicting the fact that the mechanism holds the consumer sovereignty property. Now, let's prove that is monotone non-increasing. First, for the bid vector profile $\mathbf{w} = \mathbf{v}^n(\varepsilon)$ no agent is assigned the public good by definition of $v_1, ..., v_n$. Moreover, the bid vector profile with l elements $(w_{i_1}, ..., w_{i_l})$, and $i_1, ..., i_k \in [n]$ being pairwise different, also does not allocate the public good to any player. To prove it, consider the set $L = \{i_1, ..., i_l\}$, then, the vector profile $\mathbf{w} = (w_{i_1}, ..., w_{i_l}, w_{-L})$ up to symmetry, and so has the same outcome since the mechanism is anonymous. Also, $\mathbf{w} \geq (w_{i_1}, ..., w_{i_l}, \vec{0}_{n-l})$, therefore since the mechanism is monotonic, we have that $x_{i_j}(w_{i_1}, ..., w_{i_l}) = x_{i_j}(w_{i_1}, ..., w_{i_l}, \vec{0}_{n-l}) = 0$ for all $j = 1, ..., l$. Now lets use this to prove that $v_1 \geq ... \geq v_n$. By contradiction, suppose not, let i be the smallest element such that exist $j > i$ that $v_j > v_i$. Then, since the vector profile is $\mathbf{v}^n(\varepsilon)$ no player has access to the public good, we have that $(v_1 - \varepsilon, ..., v_{i-1} - \varepsilon, v_j - \varepsilon)$ has also null allocation for all sufficiently small $\varepsilon > 0$ by the previous argument. But this contradicts the fact that v_i is the largest element that holds that the bid vector profile $(v_1 - \varepsilon, ..., v_{i-1} - \varepsilon, v)$ has the null allocation for all $\varepsilon > 0$. Therefore, we have that the sequence is monotone decreasing.

2. First, by definition, we have that the allocation of the bid vector profile $\mathbf{v}^{n-1}(\varepsilon)$ is the empty set. Now, by definition of v_n, for every $v \in (v_n, v_{n-1})$, there exists $\delta > 0$ such that for all $\varepsilon \in (0, \delta)$, the allocation of $(v_1 - \varepsilon, ..., v_{n-1} - \varepsilon, v)$ is not null. Since the sequence is non-increasing by Lemma 3.4 we have that the allocation is a set $[k]$ for some $1 \leq k \leq n$. Moreover, by strong-monotonicity, there is a $\delta > 0$ such that for all $\varepsilon \in (0, \delta)$, the allocation set is $[k]$. Now, lets prove it by contradiction. Suppose that $S \neq [n]$. By the previous observations, we have that $k < n$, and we know that the allocation of the bid vector profile $(v_1 - \varepsilon, ..., v_k - \varepsilon)$ is null for all $\varepsilon > 0$. If we assume that the valuation profile is $v_1 - \delta/4, ..., v_k - \delta/2$, we have that this reporting induces the null allocation, and so the first agent has 0 utility. If the first player reports extra bids $v_{k+1} - \delta/2, ..., v$, then the first player has access to the public good. On the other hand, the payment of the first identity is at most $v_1 - \delta/2$ by Myerson lemma (since the first identity is the only Sybil identity that has access to the public good when the bid vector profile is $(v_1 - \delta/2, ..., v_{n-1} - \delta/2, v)$). Since the other identities are not served, their payment is 0, and so the total utility of the player in this case is at least $v_1 - \delta/4 - (v_1 - \delta/2) = \delta/4 > 0$. Therefore, the mechanism would not be Sybil-proof, leading to a contradiction.

3. Observe that $\mathbf{w}^n(\varepsilon) \geq (v_1 - \varepsilon, ..., v_n + \varepsilon)$ for sufficiently small $\varepsilon > 0$. By the previous lemma, since the allocation of the second vector is $[n]$, we have, by strong monotonicity, that the allocation of the first vector is $[n]$.

4. We will prove it by induction. The first case is trivial, since $v_1 \leq 2v_1$. Now lets assume that it is true for $k < n$ and we will prove it for n. If $v_n = v_{n-1}$, then clearly $v_1 \leq 2v_{n-1} = 2v_n$, and so we can assume that $v_n < v_{n-1}$. By the 3 of proposition, there exists $\delta > 0$ such that for every $\varepsilon \in (0, \delta)$ the bid vector profile $(v_1 - \varepsilon, v_1 - \varepsilon, ..., v_{n-1} - \varepsilon)$ has full allocation. On the other hand, by definition of v_{n-1} the bid vector profile $(v_1 - \varepsilon, ..., v_{n-1} - \varepsilon)$ is null for every $\varepsilon > 0$, and so, the bid vector profile $(v_1 - \varepsilon/2, v_2 - \varepsilon, ..., v_{n-1} - \varepsilon)$ also has the null allocation. Lets assume that the first player has valuation $v_1 - \varepsilon/2$. If the first player reports two bids $v_1 - \varepsilon$, we have that the bid vector profile is $(v_1 - \varepsilon, v_1 - \varepsilon, ..., v_{n-1} - \varepsilon)$, having full allocation. By the point 2 of this proposition, we have that for every $v \in (v_n, v_{n-1})$ the bid vector profile $(v_1 - \varepsilon, ..., v_{n-1} - \varepsilon, v)$ has full allocation for sufficiently small $\varepsilon > 0$. Therefore, by Myerson lemma, the payment p_1 of the Sybil identities of the player 1 are, at most v. So, since the mechanism is Sybil-proof, we have that the utility of reporting without sybils is at least the one without Sybils and so $0 \geq (v_1 - \varepsilon/2) - 2p_1 \geq (v_1 - \varepsilon/2) - 2v$. When $v \to v_n$ and $\varepsilon \to 0$, we get $2v_n \geq v_1$.

5. Since for all $\varepsilon > 0$ it holds that $x(\mathbf{v}^n(\varepsilon)) = \vec{0}$, we have that the social cost is $\sum_{i=1}^n (v_i - \varepsilon)$. Since the mechanism is $\alpha(n)$-approximate, we have that $\sum_{i=1}^n (v_i - \varepsilon) \leq \alpha(n)$, making $\varepsilon \to 0$,

we have that $\sum_{i=1}^{n} v_i \leq \alpha(n)$. □

Now, we are ready to prove the following theorem by using the previous lemmas.

Theorem 3.6 (Social-cost lower bound)**.** If a cost-sharing mechanism $\mathcal{M}$ is individually rational, $\alpha(n)-$approximate, no-deficit, anonymous, truthful, strong-monotonic, and Sybil-proof, then $\alpha(n) \geq (n+1)/2$.

We know that, $2v_n \geq v_1$ for all $n \in \mathbb{N}$ so:

$$\begin{aligned}
\alpha(n) &\geq \sum_{i=1}^{n} v_i && \text{(by proposition 4)}\\
&\geq v_1 + \sum_{i=2}^{n} \frac{v_1}{2} && \text{(by proposition 5)}\\
&= \frac{n+1}{2} v_1 \geq \frac{(n+1)}{2} && \text{(Since the mechanism has no deficit)}
\end{aligned}$$

This concludes the proof of the Theorem 3.6. Now, since every group strategy-proof is separable, we have that in particular is strong monotonic, and so we deduce the following corollary.

Corollary 3.7. If a cost-sharing mechanism $\mathcal{M}$ is incentive compatible, upper semi-continuos $\alpha(n)-$approximate, no-deficit, symmetric, group strategy-proof, and Sybil-proof, then $\alpha(n) \geq (n+1)/2$.

Therefore, by Theorem 3.6 and proposition 3.3 we have upper and lower bounded the worst-case welfare match. This result shows that if one wants a completely strategy-proof (truthful, Sybil-proof, and group strategy-proof) cost-sharing mechanism, then the mechanism must sacrifice economic efficiency.

4 Sybil Welfare invariant mechanisms

In Section 3, we demonstrated that the Shapley cost-sharing mechanism for public excludable goods is not Sybil-proof and the limitations of Sybil-proof, truthful, strong-monotonic and no deficit mechanisms. As reported in [38], the creation of Sybils can potentially reduce social welfare in some mechanisms and cause negative externalities. As shown previously, when considering Sybil-proof mechanisms we increase the worst-case social cost from $\mathcal{H}_n$ to $(n+1)/2$ for the public excludable good problem. However, does this doom the economic efficiency of cost-sharing mechanisms with an unknown number of agents? In this section, we will argue that does not in the case of the Shapley value mechanism for symmetric submodular monotone cost functions. To analysed it, we will have to extend the model assumption and accept that agents have private beliefs about other agents actions. We will see that if we consider the Sybil-extension of the Shapley value mechanism, we will have a cost-sharing mechanism that is no-deficit, and has welfare bounded by the welfare of cost-sharing mechanism assuming that the number of players is known and cannot generate Sybil identities. We start introducing this property for general mechanisms.

Let $\mathcal{M}$ be a one-parametric truthful and individual rational anonymous mechanism and $\mathbf{Sy}(\mathcal{M})$ be its Sybil extension. And let $\mathcal{W}^{\mathcal{M}}$ and $\mathcal{W}^{\mathbf{Sy}(\mathcal{M})}$ be the social welfare maps, that take as input the agents actions and their true valuations and outputs the social welfare of the outcome. The definition of social welfare strictly depends on the mechanism being studied, in our case we will use the social cost π defined in the preliminaries. Now, we restrict to mechanisms that its Sybil extension have a weak dominant strategy set $B(v_i)$ for every player i with valuation v_i.

Definition 4.1. We say that the mechanism $\mathcal{M}$ is *Sybil welfare invariant* if the welfare under private beliefs with full support of the Sybil extension mechanism is greater or equal than the original mechanism. That is, for every $n \in \mathbb{N}$ the following inequality holds

$$\mathcal{W}^{\mathcal{M}}(v,v) \leq \mathcal{W}^{\mathbf{Sy}(\mathcal{M})}(b,v)$$

where $v = (v_1, ..., v_n) \in \mathbb{R}^n_+$, and $(v,b) \in \mathcal{Q} = \{(v,b) : v \in \mathbb{R}^n_+, b \in \prod_{i=1}^n B(v_i)\}$.

In the case of cost-sharing mechanism, our notation of welfare is given by the social cost function π. Defining $\mathcal{W} = -\pi$, a cost-sharing mechanism is Sybil welfare invariant if and only if

$$\pi(v,v) \geq \pi^{\mathbf{Sy}(\mathcal{M})}(v,b), \tag{5}$$

where $\pi(v,b)$ is the social cost when the agents report b and have true valuations v. That is, if the allocation set is S when reporting b, $\pi(v,b) = \sum_{i \notin S} v_i + C(S)$. Similarly, $\pi^{\mathbf{Sy}(\mathcal{M})}(v,b)$ is defined as the social cost of the Sybil cost-sharing mechanism extensions when the agents report b and their true valuations are v. More formally, let K_i be the set of Sybils of agent i, S the allocation set (taking into account the Sybils) and $S' = \{i \in [n] : K_i \cap S \neq \emptyset\}$, the Sybil social cost function is defined as $\pi^{\mathbf{Sy}(\mathcal{M})}(v,b) = \sum_{i \in S'} v_i + C(S')$.

In other words, Sybil welfare invariant mechanisms are those mechanisms such that its Sybil extension have weak dominant strategy sets for every valuation and that all NESPB have at least the same welfare as the output of the mechanism with truthful reports. A Sybil welfare invariant mechanism ensures that the addition of Sybils does not result in a worse outcome in terms of welfare. Essentially, this means the mechanism is resilient to the negative impact of Sybils. Sybil welfare invariant mechanisms are particularly valuable in scenarios where the primary goal is to safeguard the system against loss of welfare due to false-name strategies. They are suitable in environments where Sybil strategies are a concern but eliminating them entirely is not feasible, or identify the identities reported to the mechanism or too costly in terms of ex-post economic efficiency. An example of Sybil welfare invariant mechanism is a Sybil-proof mechanism. For example, a second price auction with private valuations is Sybil welfare invariant with the welfare map being the maximum valuations among the bidders. In the following, we will see that the Shapley value mechanism is also Sybil welfare invariant even though is not Sybil-proof. Another interpretation of Sybil-welfare invariant mechanisms is the property that hold those mechanisms such that their (subjective) Bayesian Price of anarchy [31] does not increase when agents can employ Sybil strategies under the no-overbidding condition. More formally, let NESP be the set of subjective Bayes Nash equilibrium holding the no-overbidding condition, the Bayesian price of anarchy of the Sybil extension mechanism is

$$\text{BPoA}^{\mathbf{Sy}} = \sup_{v,\sigma \text{ is NESP}} \frac{\text{Opt}(v)}{\mathbb{E}_{b\sim\sigma}[\mathcal{W}^{\mathbf{Sy}(\mathcal{M})}(b,v)]}$$

where $\text{OPT}(v)$ is the optimal welfare with the valuation profile v. Therefore,

$$\text{BPoA}^{\mathbf{Sy}} = \sup_{v,\sigma \text{ is NESP}} \frac{W^{\mathcal{M}}(v,v)}{\mathbb{E}_{b\sim\sigma}[\mathcal{W}^{\mathbf{Sy}(\mathcal{M})}(b,v)]} \frac{\text{Opt}(v)}{W^{\mathcal{M}}(v,v)} \leq \sup_{v} \frac{\text{OPT}(v)}{\mathcal{W}^{\mathcal{M}}(v,v)} = \text{PoA} \tag{6}$$

deducing the previous claim.

Now we will focus on proving that the Shapley value mechanism with symmetric submodular cost functions is Sybil welfare invariant. To do so, we will break the result in different propositions.

Proposition 4.2. The Shapley value mechanism over symmetric submodular cost functions C holds:

1. Strong-monotonicity. In particular, if a player i decides to make a Sybil strategy and commit extra bids, then all the other players' utility will not decrease.

2. At most $\mathcal{H}_n-$approximate.

The proof is mechanical in nature and, for the sake of brevity, is relegated to the appendix for interested readers. We know by the Proposition 3.2 that the Shapley value mechanism is, in general, not Sybil-proof. To prove that the Shapley value mechanism with symmetric submodular cost functions is a Sybil welfare mechanism, we will study the optimal Sybil-strategies of the Shapley-value mechanism with more detail. We will compute subweak dominant strategy sets and weak dominant strategy set of the game induced by a given valuation v_i and the Sybil Shapley value mechanism. We will use it to prove that this mechanism is Sybil welfare invariant. We will assume that the cost function $C : 2^{\mathbb{N}} \to \mathbb{R}_+$ is monotone non-decreasing, symmetric and submodular, and so, there exists $f : \mathbb{R}_+ \to \mathbb{R}_+$ such that $f(0) = 0$, is monotone non-decreasing, and concave such that $C(S) = f(|S|)$.

In the Sybil-extension mechanism, the space of actions of a player is

$$\mathcal{A} = \{(b_1, ..., b_k, ...) \mid \forall i \geq 1, b_i \geq 0, \text{ and } b_i = 0 \text{ for all but finitely many } i\}. \tag{7}$$

Now, if the private valuation of a player is v, we consider the following subset of actions

$$B(v) = \bigcup_{\sigma \in S_\infty} \sigma \cdot \{(x_1, ..., x_k, ...) \in \mathcal{A} : x_1 = v, v/l \geq x_l \text{ for } l \geq 2\}. \tag{8}$$

In the following lemma, we will prove that $B(v)$ is a subweak dominant strategy set, and so, rational agents will prefer to choose strategies from $B(v)$.

Proposition 4.3. If an agent has valuation v, then the following holds:

1. The set of strategies $B(v)$ is a subweak dominant strategy set of $\mathcal{A}$. That is, for every action $\mathbf{b}_i \in \mathcal{A} \setminus B(v)$, there is a $\mathbf{z}_i \in B(v)$ such that

$$u_i(\mathbf{z}, \mathbf{b}_{-i}) \geq u_i(\mathbf{b}_i, \mathbf{b}_{-i}) \text{ for every tuple of actions } \mathbf{b}_{-i}. \tag{9}$$

2. There exists a unique weak dominant strategy set $\overline{B(v)}$. Moreover, for every element $\mathbf{b} \in \overline{B(v)}$ there is an element in $\mathbf{z} \in B(v)$ such that $u_i(\mathbf{z}_i, \mathbf{b}_{-i}) = u_i(\mathbf{b}_i, \mathbf{b}_{-i})$ for every tuple of actions $\mathbf{b}_{-i}$.

3. For any vector of reports $\mathbf{b} \in \prod_{i=1}^n \overline{B(v_i)}$, and $\mathbf{z} \in \prod_{i=1}^n \overline{B(v_i)}$ such that $\mathbf{z}_i =_{u_i} \mathbf{b}_i$ for $i = 1, ..., n$, the social cost of both reports are the same, i.e $\pi(v, \mathbf{b}) = \pi(v, \mathbf{z})$.

The proof follows directly from the previously established lemmas, employing straightforward, mechanical arguments. For clarity and conciseness, it is provided in the appendix. Now, let's argue why rational agents will choose strategies on the set $\overline{B(v)}$. Since the Sybil Shapley value mechanism is not truthful, the agents can maximize its utility by being strategic. Suppose now the valuation of the player is v and that the bids $\mathbf{b}_{-i}$ are drawn from a distribution $\mathcal{D}$ over $\mathcal{A}$. Therefore, a rational agent maximizes its utility and, therefore wants to solve the optimization problem

$$\underset{x \in \mathcal{A}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x, \mathbf{b}_{-i})].$$

Now, let $x^\star$ be an element that maximizes the expected utility, then we know that there exists $z \in B(v)$ such that $u_i(z, \mathbf{b}_{-i}) \geq u_i(x^\star, \mathbf{b}_{-i})$ for all $\mathbf{b}_{-i} \in \mathcal{A}$, and the inequality is strict for some element in $\mathbf{b}_{-i} \in \mathcal{A}$. In particular, we deduce that $\mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(z, \mathbf{b}_{-i})] \geq \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x^\star, \mathbf{b}_{-i})]$, and so

$$\underset{x \in \mathcal{A}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x, \mathbf{b}_{-i})] \cap \underset{x \in \overline{B(v)}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x, \mathbf{b}_{-i})] \neq \emptyset.$$

Moreover, if the distribution $\mathcal{D}$ has full support (all open sets under the final topology have non-zero probability), it holds

$$\underset{x\in\mathcal{A}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i}\sim\mathcal{D}}[u_i(x,\mathbf{b}_{-i})] = \underset{x\in\overline{B(v)}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i}\sim\mathcal{D}}[u_i(x,\mathbf{b}_{-i})] \tag{10}$$

by using that $\overline{B(v)}$ is a weak dominant strategy set. So, we will assume that, in equilibrium, agents will choose strategies from $\overline{B(v)}$. Now, since the Shapley value mechanism is no longer truthful in the Sybil extension, the agents will choose actions or strategies that maximize their expected utility over their private beliefs. However, as we will see, this will not have an impact on the worst-case social cost of the Shapley value mechanism.

Theorem 4.4. The Shapley value mechanism for public excludable goods with symmetric submodular monotone cost function is Sybil welfare invariant.

Proof. First, recall that since the cost function is symmetric and submodular, there exists a monotone non-decreasing concave function f such that $C(S) = f(|S|)$ for every $S \subseteq \mathbb{N}$. Since f is concave, we have that $f(m)/m \leq f(n)/n$ for all $n \leq m$. Also, we deduce that $(m-n)f(m)/m \geq f(m) - f(n)$ for all $n \leq m$. Now, suppose that there are n players with private valuations $v_1, ..., v_n$ and private beliefs with full support $\mathcal{D}_1, ..., \mathcal{D}_n$. By Lemma 2.2, the agents take actions in $\prod_{i=1}^n \overline{B(v_i)}$. Now, let $x = (x_1, ..., x_n)$ be the actions taken by the players. First, we will see that wlog we can assume that $(x_1, ..., x_n) \in \prod_{i=1}^n B(v_i)$ by the point 3 of proposition 4.3. Let $S(v)$ (resp. $S(x)$) be the set of players that have some identity having access to the public good when reporting v (resp. x). By definition of $B(v)$, the first element is v, therefore $S(v) \subseteq S(x)$, and so $\sum_{i\in S(x)} v_i \geq \sum_{i\in S(v)} v_i$. Since the mechanism is budget-balanced, the sum of payments is $C(S)$ with winners set S. We will prove that $\pi(S(x)) \leq \pi(S(v))$ by cases.

Case 1 $S(x) = \emptyset$. We know that $S(v) \subseteq S(x)$ and so $S(v) = \emptyset$, in both cases we have the null allocation and so the social cost of both cases coincide. Therefore $\pi(S(v)) = \pi(S(x)) \leq \mathcal{H}_n \pi(S^\star)$.

Case 2 $S(x) \neq \emptyset$. For every $i \in S(x)$, let k_i be the number of i Sybil identities k_i such that the public good is allocated. Since $x \in B(v_i)$, $v_i/j \geq x_i^j$ for $j = 1, ..., k_i$, in particular $v_i \geq f(|S(x)|)/|S(x)|$. Therefore,

$$\sum_{i\in S(x)\setminus S(v)} v_i \geq (|S(x)| - |S(v)|)f(|S(x)|)/|S(x)| \geq f(|S(x)|) - f(|S(v)|)$$

where the last inequality is deduced from f being concave and $|S(v)| \leq |S(x)|$. So,

$$\begin{aligned}
\pi(S(x)) &= f(|S(x)|) + \sum_{i\notin S(x)} v_i = f(|S(x)|) + \sum_{i\notin S(v)} v_i - \sum_{i\in S(x)\setminus S(v)} v_i \\
&\leq f(|S(x)|) + \sum_{i\notin S(v)} v_i - f(|S(x)|) + f(|S(v)|) \\
&= \pi(S(v)).
\end{aligned}$$

□

As a corollary, it can be shown that if agents do not overbid, the Bayesian price of anarchy of the Sybil extension of the Shapley value mechanism is $\mathcal{H}_n$. In summary, we have proved that even when the number of agents is unknown to both the mechanism designer, and the agents participating in the mechanism, the Shapley value mechanism for submodular monotone cost functions has the same worst-case social cost as the same mechanism with known number of agents. Therefore, we have shown the robustness of Shapley value mechanism over permissionless environments such as Peer-to-Peer (P2P) Networks and decentralized finance (DeFi) platforms, and in particular can be practical and robust when members of a decentralized autonomous organizations (DAOs) want to deploy a public excludable good. Since the Shapley value mechanism is no longer truthful, to implement this mechanism in a public blockchain will be necessary to make some small adjustments. To maintain the same worst-case equilibria under false-name strategies the mechanism will have to shield the bids, similar to [33], by using different cryptographic tools such as commit-and-reveal or multiparty computation protocols. For example, the mechanism could have two phases. The commit phase and the reveal phase. In the commit-phase, agents send a commitment of a bid and some cash as a collateral (for example the cost of the public good). After the finish of the first phase, the agents reveal their bid, and the allocation and the payment is computed following the rules of the Shapley value mechanism. If an agent does not reveal its bid in time, they lose their collateral, making weak dominant strategy to reveal their bid. Without this two-phase mechanism or a trusted third party that keeps the bids private, some agents would have access to other agents' bids, changing the structure of the mechanism from one-shoot mechanisms to sequential mechanisms with multiple rounds.

5 Conclusion

In this paper, we have formalized false-name strategies in cost-sharing mechanisms. We established an impossibility result, indicating that many mechanisms from existing literature are vulnerable to these strategies. Furthermore, we characterized the worst-case welfare for mechanisms that satisfy the properties of individual rationality, no-deficit, symmetry, truthfulness, strong-monotonicity, and Sybil-proofness. These mechanisms have a worst-case welfare of at least $(n+1)/2$, and we demonstrated that this bound is tight. Additionally, we introduced the concept of the Sybil welfare invariant property and showed that the Shapley value mechanism possesses this property. This means that regardless of the priors held by agents, the Shapley value mechanism with sybils achieves the same worst-case welfare as the Shapley value mechanism without sybils. As a direction for future research, we aim to explore the vulnerabilities of combinatorial cost-sharing mechanisms to false-name strategies and determine whether mechanisms cited in the literature, such as [30] and [34], are Sybil welfare invariant. To do so, we will need to extend the definition of Sybil welfare invariant under combinatorial domains. Also, we leave as future work, to see if Theorem 3.6 holds for weaker conditions such as removing the strong monotonic condition. Finally, in the cost-sharing literature, we aim to study Sybil-proof and Sybil-welfare invariant mechanisms with general cost functions C. Beyond the cost-sharing literature, we aim to study if mechanisms such as the one proposed in [37] are Sybil welfare invariant and if not, make adjustments to the mechanism to maintain the worst-case welfare under private beliefs.

6 Acknowledgments

The author would like to express sincere gratitude to the Ethereum Foundation for generously funding the scholarship that made this research possible. Special thanks are also extended to Vanesa Daza, for her invaluable feedback and meticulous corrections.

References

[1] Jhon C Harsanyi. "Part II: Bayesian equilibrium points". In: *Management Science* 14 (1968), pp. 320–334.

[2] Roger B Myerson. "Optimal auction design". In: *Mathematics of operations research* 6.1 (1981), pp. 58–73.

[3] Eric S Maskin and John G Riley. "Auction theory with private values". In: *The American Economic Review* 75.2 (1985), pp. 150–155.

[4] Roger B Myerson. *Mechanism design.* Springer, 1989.

[5] Hervé Moulin. "Incremental cost sharing: Characterization by coalition strategy-proofness". In: *Social Choice and Welfare* 16 (1999), pp. 279–320.

[6] Hervé Moulin and Scott Shenker. "Strategyproof sharing of submodular costs: budget balance versus efficiency". In: *Economic Theory* 18 (2001), pp. 511–533.

[7] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. "Robust combinatorial auction protocol against false-name bids". In: *Artificial Intelligence* 130.2 (2001), pp. 167–181.

[8] John R Douceur. "The sybil attack". In: *International workshop on peer-to-peer systems.* Springer. 2002, pp. 251–260.

[9] Martin Dufwenberg and Mark Stegeman. "Existence and uniqueness of maximal reductions under iterated strict dominance". In: *Econometrica* 70.5 (2002), pp. 2007–2023.

[10] Joan Feigenbaum et al. "Hardness results for multicast cost sharing". In: *Theoretical Computer Science* 304.1-3 (2003), pp. 215–236.

[11] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. "The effect of false-name bids in combinatorial auctions: New fraud in Internet auctions". In: *Games and Economic Behavior* 46.1 (2004), pp. 174–188.

[12] Shuchi Chawla, Tim Roughgarden, and Mukund Sundararajan. "Optimal cost-sharing mechanisms for steiner forest problems". In: *Internet and Network Economics: Second International Workshop, WINE 2006, Patras, Greece, December 15-17, 2006. Proceedings 2.* Springer. 2006, pp. 112–123.

[13] Jochen Dinger and Hannes Hartenstein. "Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration". In: *First International Conference on Availability, Reliability and Security (ARES'06).* IEEE. 2006, 8–pp.

[14] Haifeng Yu et al. "Sybilguard: defending against sybil attacks via social networks". In: *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications.* 2006, pp. 267–278.

[15] Janina Brenner and Guido Schäfer. "Cost sharing methods for makespan and completion time scheduling". In: *Annual Symposium on Theoretical Aspects of Computer Science.* Springer. 2007, pp. 670–681.

[16] Yvonne Bleischwitz and Florian Schoppmann. "Group-strategyproof cost sharing for metric fault tolerant facility location". In: *International Symposium on Algorithmic Game Theory.* Springer. 2008, pp. 350–361.

[17] Shahar Dobzinski et al. "Is Shapley cost sharing optimal?" In: *Algorithmic Game Theory: First International Symposium, SAGT 2008, Paderborn, Germany, April 30-May 2, 2008. Proceedings 1.* Springer. 2008, pp. 327–336.

[18] Liad Wagman and Vincent Conitzer. "Optimal False-Name-Proof Voting Rules with Costly Voting." In: *AAAI.* Vol. 8. 2008, pp. 190–195.

[19] Haifeng Yu et al. "Sybillimit: A near-optimal social network defense against sybil attacks". In: *2008 IEEE Symposium on Security and Privacy (sp 2008).* IEEE. 2008, pp. 3–17.

[20] Vijay Krishna. *Auction theory.* Academic press, 2009.

[21] Tim Roughgarden and Mukund Sundararajan. “Quantifying inefficiency in cost-sharing mechanisms”. In: *Journal of the ACM (JACM)* 56.4 (2009), pp. 1–33.

[22] Mukund Sundararajan. *Trade-offs in cost sharing.* Stanford University, 2009.

[23] Hal R Varian. “Online ad auctions”. In: *American Economic Review* 99.2 (2009), pp. 430–434.

[24] Atsushi Iwasaki et al. “Worst-case efficiency ratio in false-name-proof combinatorial auction mechanisms”. In: *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1.* 2010, pp. 633–640.

[25] Jung Ki So and Douglas S Reeves. “Defending against sybil nodes in bittorrent”. In: *International Conference on Research in Networking.* Springer. 2011, pp. 25–39.

[26] Taiki Todo, Atsushi Iwasaki, and Makoto Yokoo. “False-name-proof mechanism design without money”. In: *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 2.* 2011, pp. 651–658.

[27] Itai Sher. “Optimal shill bidding in the VCG mechanism”. In: *Economic Theory* 50 (2012), pp. 341–387.

[28] Anupam Gupta et al. “Efficient cost-sharing mechanisms for prize-collecting problems”. In: *Mathematical Programming* 152 (2015), pp. 147–188.

[29] Agnieszka Wiszniewska-Matyszkiel. “Belief distorted Nash equilibria: introduction of a new kind of equilibrium in dynamic games with distorted information”. In: *Annals of Operations Research* 243 (2016), pp. 147–177.

[30] Shahar Dobzinski and Shahar Ovadia. “Combinatorial cost sharing”. In: *Proceedings of the 2017 ACM Conference on Economics and Computation.* 2017, pp. 387–404.

[31] Tim Roughgarden, Vasilis Syrgkanis, and Eva Tardos. “The price of anarchy in auctions”. In: *Journal of Artificial Intelligence Research* 59 (2017), pp. 59–101.

[32] Shijie Zhang and Jong-Hyouk Lee. “Double-spending with a sybil attack in the bitcoin decentralized network”. In: *IEEE transactions on Industrial Informatics* 15.10 (2019), pp. 5715–5722.

[33] Matheus VX Ferreira and S Matthew Weinberg. “Credible, truthful, and two-round (optimal) auctions via cryptographic commitments”. In: *Proceedings of the 21st ACM Conference on Economics and Computation.* 2020, pp. 683–712.

[34] Georgios Birmpas, Evangelos Markakis, and Guido Schäfer. “Cost sharing over combinatorial domains”. In: *ACM Transactions on Economics and Computation* 10.1 (2022), pp. 1–26.

[35] Federico Fioravanti and Jordi Massó. “False-name-proof and strategy-proof voting rules under separable preferences”. In: *Available at SSRN 4175113* (2022).

[36] Bruno Mazorra, Michael Reynolds, and Vanesa Daza. “Price of MEV: Towards a Game Theoretical Approach to MEV”. In: *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security.* 2022, pp. 15–22.

[37] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. “When Bidders Are DAOs”. In: *arXiv preprint arXiv:2306.17099* (2023).

[38] Bruno Mazorra and Nicolás Della Penna. “The Cost of Sybils, Credible Commitments, and False-Name Proof Mechanisms”. In: *arXiv preprint arXiv:2301.12813* (2023).

A Appendix

A.1 Notation

Symbol	Description
$[n]$	Set $\{1, \ldots, n\}$.
$2^{[n]}$	Set of subsets of $[n]$.
$\mathbb{N}$	Set of natural numbers $\{1, 2, 3, 4, ...\}$.
S_∞	Set of permutations of $\mathbb{N}$.
u_i	Player i's utility function.
v_i	Player i's private valuation.
$\mathbf{x}$	Allocation map.
$\mathbf{p}$	Payment map.
x_i	The i-th component of the allocation map $\mathbf{x}$.
p_i	The i-th component of the payment map $\mathbf{x}$.
$\mathcal{H}_n$	n-th harmonic number.
$\mathbb{R}^\infty$	Space of sequences of real numbers where only finitely many terms are non-zero.
$\mathbb{R}^\infty_+$	Space of sequences of non-negative real numbers where only finitely many terms are non-zero.

A.2 Proofs

Proof 2.2 Let's first prove it assuming that the subweak dominant strategy set $B_i(t_i)$ is sequentially compact. Let's define the following relation. We say that $x \geq_{u_i} y$ if and only if $u_i(t_i, x, z) \geq u_i(t_i, y, z)$ for every $z \in A_{-i}$. Observe that the relation is reflexive and transitive, but is not symmetric. We say that $x =_{u_i} y$ if and only if $x \geq_{u_i} y$ and $y \geq_{u_i} x$ and $x >_{u_i} y$ if $x \geq_{u_i} y$ and $x \neq_{u_i} y$. For every, $x \in A_i$, we define $[x]_{\geq_{u_i}} = \{y \in A_i : x \geq_{u_i} y\}$. First, we consider the subset $\overline{B_i(t_i)} = \{x \in A_i : \nexists y \in B_i(t_i) \text{ s.t. } y >_{u_i} x_i\}$.

We claim that $\overline{B_i(t_i)}$ is non-empty and is a weak dominant strategy set. First, lets prove that is non-empty. We will use Zorn's lemma and that $B_i(t_i)$ is sequentially compact. Consider a chain in $B_i(t_i)$, that is a totally order sequence $\{x_n\}_{n\in\mathbb{N}}$, by sequentially compactness of $B_i(t_i)$, there exists a subsequence x_{n_j} that converges to an element $x^\star \in B_i(t_i)$. Using the upper-continuity of u_i follows easily that $x^\star \geq_{u_i} x_n$ for all $n \in \mathbb{N}$. Therefore, every chain has a maximal element. Now, by Zorn's lemma, there exists at least one maximal element x in $B_i(t_i)$. Now, suppose that $\overline{B_i(t_i)}$ is an empty set then, there is no maximal element in A_i, implying that for every $x \in A_i$ there is an element $y \in A_i$ such that $y >_{u_i} x$. Let $x^\star$ be a maximal element of $B_i(t_i)$. Then, there exists $y \in A_i$ such that $y >_{u_i} x^\star$. Since $B_i(t_i)$ is subweak dominant strategy set, there exists y' such that $y' >_{u_i} x^\star$, but this contradicts the fact that $x^\star$ is a maximal element in $B_i(t_i)$, therefore $\overline{B_i(t_i)}$ is non-empty. Moreover, with this argument, we have seen that all maximal elements of $B_i(t_i)$ are elements of $\overline{B_i(t_i)}$.

Now, we claim that $\overline{B_i(t_i)}$ is the unique strictly dominant strategy set. Let's prove it. Given an element $a_i \in A_i \setminus B_i(t_i)$ there is an element $a_i' \in B_i(t_i)$ such that $a_i' \geq_{u_i} a_i$. Now, since $\overline{B_i(t_i)}$ contain all maximal elements, we have that there exists an element $a_i'' \geq_{u_i} a_i'$, deducing the first property of weak dominant strategy sets. The second condition clearly holds by definition.

The uniqueness follows similarly. If there are two different strictly dominant sets M_1 and M_2, then wlog there exists $x \in M_2 \setminus M_1$. Since M_1 is a strictly dominant strategy set, there is $y \in M_1$ such that $y >_{u_i} x$. But this contradicts the fact that M_1 is a dominant strategy set.

Now let's suppose that there exists a chain $C_1 \subseteq C_2 \subseteq ...$ that holds the hypothesis of the lemma. For every $j \in \mathbb{N}$, $B_i(t_i) \cap C_j$ is a dominant strategy set when restricting the game to

C_j. And so by the previous argument, there exists $\overline{B}(t_i)_i^j$ strictly dominant strategy set of the normal form game where the agent i has action space C_i. Now, the set $\cup_{j\in\mathbb{N}}\overline{B}_i(t_i)^j$ is a strictly dominant strategy set in A_i.

Proof 4.2

1. The Shapley value is the cost-sharing mechanism with cost-sharing method $\zeta(S) = 1/|S|$. Now let $\mathbf{b}$ and $\mathbf{b}'$ be two bid vector profiles such that $\mathbf{b} \geq \mathbf{b}'$. Let S' be the allocation set of $\mathbf{b}'$ and S be the allocation set of $\mathbf{b}$. Then, for every $i \in S'$, we have that $b'_i \geq C(S')/|S'|$. On the other hand, $b_i \geq b'_i \geq C(S')/|S'|$. Therefore, $S' \subseteq \text{argmax}_X\{|X| : b_i \geq C(X)/|X|\} = S$. The utility of other players will not decrease under more bids, since the allocation set will be at least S, and the payment will be at most $C(S)/|S|$.

2. To do so, we will see that the allocation of the Shapley value mechanism S_1 with subadditive symmetric valuations contains the set of agents allocated S_2 allocated using the Hybrid mechanism provided in [17]. In this proposition, we use that the cost function is submodular, otherwise, the Shapley value mechanism would not be truthful in general [6]. The hybrid mechanism consists of the following:

   Hybrid mechanism

   (a) Accept bids $b_1, ..., b_n$.

   (b) Take $S^\star \in \text{argmax}_S\{\sum_{i\in S} b_i - C(S)\}$.

   (c) Initialize $S := S^\star$.

   (d) If $b_i \geq C(S^\star)/|S|$ for every $i \in S$, then halt with winners S.

   (e) Let $i^\star \in S$ be a player with $b_{i^\star} < C(S^\star)/|S|$.

   (f) Set $S \leftarrow S \setminus \{i\}$ and return to Step 4.

   (g) Charge each winner $i \in S$ a payment equal to the minimum bid at which i would continue to win (holding b_{-i} fixed).

   First, wlog, we order the bids $b_1 \geq ... \geq b_n$. Observe that since the cost function is symmetric and subadditive, if $k \in S_i$ for $i = 1, 2$, then $[k] \subseteq S_i$ for $i = 1, 2$. Let k_i be the largest element of S_i. So, proving that $S_2 \subseteq S_1$ is equivalent to prove that $k_2 \leq k_1$. Then, $b_l \geq C(S^\star)/|S_2| \geq C(S_2)/|S_2|$ for $l = 1, ..., k_2$, where $S^\star$ is the set that maximizes $\sum_{i\in S} b_i - C(S)$. In particular, $k_2 \in \{i : b_i \geq C(S)/|S|\}$ and so $k_2 \leq \text{argmax}\{b_i \geq C([i])/i\}$. □

Proof 4.3 With out loss of generality, we will assume that $f(1) = 1$.

1. Given a vector $\mathbf{b}_i = (b_1, ..., b_k, 0, ...)$ (wlog we assume $b_1 \geq b_2 \geq ... \geq b_k$), we consider the vector $\mathbf{z} = (z_1, ..., z_k, 0, ...)$ defined by

$$z_1 = v$$
$$z_l = \min\left\{b_l, \frac{v}{l}, \frac{1}{l}\right\}, \text{ for } l = 2, ..., k.$$

   Clearly, $z_1 \geq ... \geq z_l$. We will prove that $\mathbf{z}$ holds the inequality 9 by cases will depend on the number of Sybils that both bid vector profiles will have access to the public good. Let $j(\mathbf{b}_i)$ (resp. $j(\mathbf{z})$) be the total number of Sybil identities of agent i that are allocated when reporting $\mathbf{b}_i$ (resp. $\mathbf{z}$). Similarly, let $n(\mathbf{b}_i)$ (resp. $n(\mathbf{z})$) be the total number of identities that are allocated when reporting $\mathbf{b}_i$ (resp. $\mathbf{z}$).

Case 1 $j(\mathbf{b}_i) = 0$ and $j(\mathbf{z}) \geq 1$. Suppose that no identity is allocated when reporting $\mathbf{b}_i$, then, in this case, the utility is zero. Now, when reporting $\mathbf{z}$, at most the first identity will have access to the public good, otherwise $z_2 \geq f(n(\mathbf{z}))/n(\mathbf{z})$. As $b_1 \geq b_2 \geq z_2$, then the first two identities would also be allocated when reporting $\mathbf{b}_i$, leading to a contradiction. Since the mechanism is incentive compatible, the utility reporting $\mathbf{z}$ is greater than zero, proving this case.

Case 2 $j(\mathbf{b}_i) \geq 1$, $j(\mathbf{z}) = 0$ and $v \leq 1$. Then, we have the last sybil identity that has access holds $b_j \geq f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$. On the other hand, since no Sybil identity has access when reporting $\mathbf{z}$, it holds that $z_{j(\mathbf{b}_i)} < f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$ and so $v/j(\mathbf{b}_i) < f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$. Since the payment when reporting $\mathbf{b}_i$ is $j(\mathbf{b}_i)f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$, the utility when reporting $\mathbf{b}_i$ is negative, and is zero when reporting $\mathbf{z}$.

Case 3 $j(\mathbf{b}_i) \geq 1$, $j(\mathbf{z}) = 0$ and $v > 1$. It is not possible since the first bid reported by the agent i is $v > 1$ and so that identity has access to the public good, since $v > f(1)/1 \geq f(n)/n$ for all $n \in \mathbb{N}$, leading to $j(\mathbf{z}) \geq 1$.

Case 4 $j(\mathbf{b}_i) \geq 1$ and $j(\mathbf{z}) \geq 1$. In this case, wlog, we can assume that $b_1 \geq v$ and so $\mathbf{b}_i \geq \mathbf{z}$. By construction and the strong-monotonicity of the Shapley value mechanism, if a Sybil identity is allocated when reporting $\mathbf{z}$, then the same identity is allocated when the report is $\mathbf{b}_i$. Therefore, $j(\mathbf{b}_i) \geq j(\mathbf{z})$ and also $n(\mathbf{b}_i) \geq n(\mathbf{z})$. If $j(\mathbf{b}_i) = j(\mathbf{z})$, then the utility of both cases is the same. So, lets assume that $j(\mathbf{b}_i) > j(\mathbf{z})$. This implies that $z_{j(\mathbf{b}_i)} < f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$, and so $v/j(\mathbf{b}_i) < f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$ (or $1/j(\mathbf{b}_i) < f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$ if $v \geq 1$)). On the other hand, $z_{j(\mathbf{z})} \geq f(n(\mathbf{z}))/n(\mathbf{z})$, and so $v/j(\mathbf{z}) \geq f(n(\mathbf{z}))/n(\mathbf{z})$ (or $1/j(\mathbf{z}) \geq f(n(\mathbf{z}))/n(\mathbf{z})$ in case $v \geq 1$) . Using both equations, in both cases, we deduce that $j(\mathbf{b}_i)f(n(\mathbf{b}_i))/n(\mathbf{b}_i) > j(\mathbf{z})f(n(\mathbf{z}))/n(\mathbf{z})$. Now, the utility is $u_i(\mathbf{b}_i, \mathbf{b}_{-i}) = v - j(\mathbf{b}_i)f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$ and $u_i(\mathbf{z}, \mathbf{b}_{-i}) = v - j(\mathbf{z})f(n(\mathbf{z}))/n(z)$ since both have access to the public good and the payments for each Sybil is $f(n(\mathbf{b}_i))/n(\mathbf{b}_i)$ (resp. $f(n(\mathbf{z}))/n(\mathbf{z})$). And so, we deduce the result.

2. Observe that the space $\mathcal{A}$ has structure of a metric space with the metric $d(x, y) = \sqrt{\sum_{i=1}^{\infty} |x_i - y_i|^2}$. To prove the proposition, first we prove the following claim: there is a chain of sets C_i such that $\cup_{i \in \mathbb{N}} C_i = \mathcal{A}_i$ and $B(v) \cap C_i$ is sequentially compact for every $v \in \mathbb{R}_+$. Take the set $C_i = \mathbb{R}^i_+ \times \{0\}^{\mathbb{N}} \subseteq \bigoplus_{i=j}^{\infty} \mathbb{R}_+$. Clearly the set $B(v) \cap C_i = \bigoplus_{l=1}^{i} [0, v/l] \times \{0\}^{\mathbb{N}}$ is compact since is the product of compact spaces. Therefore, by lemma 2.2, there exists a strictly dominant strategy set $\overline{B(v)}$.

3. Given bid vector profile $\mathbf{b} \in \prod_{i=1}^{n} \overline{B(v_i)}$ with components $\mathbf{b}_i$, consider the element $\mathbf{z}_i$ as defined in 1). Since $\overline{B(v_i)}$ are strictly dominant strategy sets and $\mathbf{z}_i \geq_{u_i} \mathbf{b}_i$, we have that $\mathbf{z}_i =_{u_i} \mathbf{b}_i$. We will see that the set of allocated sybils is the same for the bid vector profiles $\mathbf{b}$ and $\mathbf{z}$. We know that $\mathbf{z}_i =_{u_i} \mathbf{b}_i$, and we claim that it implies that for every $j \in \mathbb{N}$, there exists n_j such that $f(n_j)/n_j \leq \mathbf{z}_{ij}, \mathbf{b}_{ij} < f(n_j - 1)/(n_j - 1)$. Suppose not, take the minimum j such that the claim does not hold and so, there exists $n \in \mathbb{N}$ such that $f(n)/n \leq \mathbf{z}_{ij} < f(n-1)/(n-1) \leq \mathbf{b}_{ij}$. Since $\mathbf{z}_{i1} = \mathbf{b}_{i1} = v$, we have that $j \geq 2$. Consider now the bid vector profile $\mathbf{b}_{-i} = \underbrace{(f(n-1)/(n-1), ..., f(n-1)/(n-1))}_{n-j-1 \text{ components}}$. By definition of $\mathbf{z}_i$ and the previous inequality, we have that $\mathbf{z}_{ij} = \min\{v/j, 1/j\}$ and so, we deduce that $jf(n-1)/(n-1) > v \geq jf(n)/n$ if $v \leq 1$ and $jf(n-1)/(n-1) > 1 \geq jf(n)/n$ otherwise. Now, let's compute the utility of the bid vector profiles $(\mathbf{z}_i, \mathbf{b}_{-i})$ and $(\mathbf{b}_i, \mathbf{b}_{-i})$. The allocation of the vector $(\mathbf{z}_i, \mathbf{b}_{-i})$ if $v < 1$ is null, and if $v \geq 1$ is just the Sybils of player i inducing in the first case utility of 0 and in the second case has utility of $v - f(1)$.

   When reporting $\mathbf{b}_i$ all elements $\mathbf{b}_{il}$ for $1 \leq l \leq k$ are greater than $f(n-1)/(n-1)$, therefore, all the identities reported in the bid vector $\mathbf{b}_{-i}$ are allocated. Therefore, his payment is at least $j\frac{f(n-1)}{n-1}$ and so, his utility is, at most, $v - j\frac{f(n-1)}{n-1}$. When $v \leq 1$, we have that $v - j\frac{f(n-1)}{n-1} < 0$ since $jf(n-1)/(n-1) > v$ and for $v > 1$, we have that $v - f(1) > v - j\frac{f(n-1)}{n-1}$ since $jf(n-1)/(n-1) > 1 = f(1)$. This contradicts the claim that $\mathbf{z}_{u_i} = \mathbf{b}_i$, and so for every $j \in \mathbb{N}$, there exists n_j such that $f(n_j)/n_j \leq \mathbf{z}_{ij}, \mathbf{b}_{ij} < f(n_j - 1)/(n_j - 1)$. Now, clearly the allocation of both bid vector profiles is the same since the Shapley value mechanism consists of choosing the biggest set S such that all bids are greater or equal $f(|S|)/|S|$.