# Is Shapley cost sharing optimal under false-name strategies? Analysis of public excludable goods mechanisms under Sybil strategies

Bruno Mazorra Roig
Universitat Pompeu Fabra
brunomazorra@gmail.com

November 20, 2023

**Abstract**

In the realm of cost-sharing mechanisms, the vulnerability to false-name strategies (also known as Sybil attacks or Sybil strategies), where agents can create fake identities to manipulate outcomes, has not yet been studied. In this paper we delve into the intricacies of different cost-sharing mechanism proposed in the literature, highlighting its non Sybil-resistance nature. Furthermore, we demonstrate that under mild conditions, a Sybil-proof (also referred to as false-name proof or Sybil resistant) cost-sharing mechanism for public excludable goods is at least $(n/2+1)-$approximate. This finding reveals an actual exponential increase in the worst-case social cost in environments where agents are restricted from using Sybil strategies. We introduce the concept of *Sybil Welfare Invariant* mechanisms, where a mechanism maintains its worst-case welfare under Sybil-strategies for every set of prior beliefs with full support even when the mechanism is not Sybil-proof. Finally, we prove that the Shapley value mechanism for public excludable goods holds this property, and so deduce that the worst-case welfare of this mechanism is $\mathcal{H}_n$ for any set of beliefs with full support, matching the worst-case welfare bound for cost-sharing mechanism without false-name strategies.

## 1 Introduction

Cost-sharing mechanisms in public goods allocation are fundamentally grounded in mathematical models that define the interaction between participants and outcomes. Formally, a cost-sharing mechanism design problem can be conceptualized as involving a set $[n]$ of players and a cost function $C : 2^{[n]} \to \mathbb{R}_+$. This function delineates the cost incurred by the mechanism as a function of the outcome, specifically the set $S$ of “winners”. Each player $i$ in this set has a private, nonnegative value $v_i$ for winning, reflecting their valuation of the good or service in question.

In the realm of public excludable goods, the problem is twofold: determining whether to finance a public good and, if so, identifying the users who are granted access. This is represented by a cost function $C$ where $C(\emptyset) = 0$ and $C(S) = 1$ for every non-empty subset $S$, encapsulating scenarios where various cost functions might apply, including those where public excludable goods are at the forefront.

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,” focusing on the impact of single-player deviations [LSM06; Mül+08; Yu+09; Lin+17; CPR19], and “false-name proofness,” examining the equilibrium in scenarios where players can represent multiple entities on mechanisms [YSM01; SY05; TIY11; AHV14;

FM22]. These studies highlight the vulnerabilities of even well-established mechanisms such as combinatorial auctions and the VCG mechanism.

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 welfare costs for mechanisms satisfying properties like Sybil-proofness.

Building upon these insights, this paper presents 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 welfare scenario.

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.

Our paper makes several key contributions to the field:

- We introduce a framework for analysing cost-sharing mechanism for public excludable goods with unknown number of agents and Sybil strategies.
- We prove that the cost-sharing mechanism for public excludable goods 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, we prove that welfare social cost is $(n/2+1)$ of cost-sharing mechanisms that are strong-monotonic, anonymous, individually rational, and Sybil-proof.
- We introduce Sybil welfare invariant mechanisms, and we prove that the Shapley value cost-sharing mechanism holds this property.

### 1.1 Organization of the paper and notation

The paper will be organized as follows. In section 2, we will introduce tools from mechanism design, cost-sharing mechanism 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. Finally, we will prove that under some mild conditions, upper and lower bound the worst-case welfare of Sybil-proof mechanisms. In section 3.2, we will introduce the concept of Sybil welfare invariant mechanisms, and we will prove that the Shapley value mechanism holds this property.

| Symbol | Description |
|---|---|
| $[n]$ | Set $\{1, \ldots, n\}$. |
| $2^{[n]}$ | Set of subsets of $[n]$. |
| $\mathbb{N}$ | Set of natural numbers $\{1, 2, 3, 4, ...\}$. |
| $S_\infty$ | 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 $\mathbf{x}$. |
| $\mathcal{H}_n$ | Harmonic number for $n$. |
| $\mathbb{R}^\infty$ | 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. |

## 1.2 Related work

This paper explores the nuanced domain of cost-sharing mechanisms of public excludable goods, particularly emphasizing their non-false-name proofness guarantees. 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 [MS01], who discussed the strategy-proof sharing of submodular costs, with budget-balance constraints. This work, alongside Myerson's seminal [Mye81] study 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 [Mou99; MS01] initiated a rich vein of research into the efficiency loss of budget-balanced cost-sharing mechanisms. Subsequent studies by Feigenbaum et al. [Fei+03] and Roughgarden et al. [RS09], along with others [BS08; BS07; CRS06; Gup+15], expanded the understanding of these mechanisms under various constraints and objectives. More aligned with our paper, in [Dob+08], 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, where a single malicious entity creates multiple fake identities was first brought to light by Douceur [Dou02], poses a significant threat across different domains, from peer-to-peer networks [DH06; SR11] and online social networks [Yu+06; Yu+08] to blockchain systems [ZL19], 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. [YSM01; YSM04] 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 false-name-proof combinatorial auction mechanisms [Iwa+10] and the strategic dynamics of shill bidding [She12].

Parallel to these developments, research in non-monetary mechanisms and voting systems, such as the facility location problem [TIY11] and voting rules with costs [WC08; FM22], has been instrumental in characterizing and tackling false-name proof mechanisms. These studies highlight the pervasive nature of false-name strategies across various decision-making and resource allocation systems.

In their exploration of false-name proofness and Sybil-proof mechanisms, the authors in [MDP23] have developed a comprehensive framework that is notably adaptable for analyzing

Sybil extensions in cost-sharing mechanisms.

# 2 Preliminary

## 2.1 Introduction to Mechanism Design

Mechanism design, 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 it 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 [MR85; Kri09], it is common to assume that agents have private valuations and quasilinear utilities (this is not always the case, but in this paper, we will restrict to this model). This means that an agent's utility is additive over money and the agent's valuation for the allocated item or service. Let's denote:

- $v_i \in \mathbb{R}$ 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 $b_{-i}$.

Given these, 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 [Mye81])**.** 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.

However, 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, players might not have complete information about the game or about other players' types, preferences, or payoffs. Bayesian games, introduced by John C. Harsanyi [Har68], are a class of games that model such situations of incomplete information. In many strategic situations, 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 an unknown set of players $\mathcal{I}$ that can take actions in a topological set $A_i$ for $i \in \mathcal{I}$. Players have utility functions continuous utility function $u_i : \prod_{i \in \mathcal{I}} A_i \to \mathbb{R}$ unknown to other players. Each player has a private belief distribution $\mathcal{D}_i$ that models the $i$th players' belief of other players take 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* $\mathcal{D}_i$ if they choose strategies in

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

In some cases, we can restrict that maximization problem to a subset $B \subsetneq A_{-i}$. For example, when $B$ holds the following property. For every action $a_i \in A_i$, there is an action $a'_i \in B_i$ such that $u_i(a'_i, a_{-i}) \geq u_i(a_i, a_{-i})$ for every action profile $a_{-i} \in A_{-i}$. In this scenario, we say that $B$ is a *dominant strategy set*. Moreover, if for every $a_i \in A \setminus B$, there is an $a'_i \in B$ such that $u_i(a'_i, a_{-i}) \geq u_i(a_i, a_{-i})$ for every action profile $a_{-i} \in A_{-i}$ and the inequality is strict for some $a_{-i} \in A_{-i}$, we say that $B$ is a *strictly dominant strategy set*. Observe that, if a player $i$ has a strictly dominant state set $B_i$, then this set is unique. An example of (strictly) dominant strategy set on a mechanism is the set $B_i = \{v_i\}$ in a second price auction with private valuations where $v_i$ is the valuation of the item of player $i$.

**Definition 2.2.** A mixed Bayes Nash equilibrium with private beliefs (BNEPB) is a tuple of distributions $(d_1, ..., d_n)$ over the set of strategies such that there exist a tuple of priors $(\mathcal{D}_1, ..., \mathcal{D}_n)$ that hold:

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

If the distributions $\mathcal{D}_1, ..., \mathcal{D}_n$ have full support, we say the tuple of distributions $(d_1, ..., d_n)$ is mixed *Bayes Nash equilibrium with full support private beliefs* (BNESPB). Note that the tuple $(d_1, ..., d_n)$ is a BNESPB, and player $i$ has a strictly dominant strategy set $B_i$ then $\Pr_{d_i}[B_i] = 1$. 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.

Observe that this notion of equilibrium is very weak. Every mixed Nash equilibrium and Bayes Nash equilibrium with common priors are mixed Bayes Nash equilibrium with private beliefs.

## 2.2 Public excludable goods

In this section we introduce the notation and key concepts proposed in [Dob+08] within the context of cost-sharing mechanism design. In the following sections, we will use the concepts introduced to study cost-sharing mechanism under false-name strategies.

In a cost-sharing mechanism design problem [Dob+08; Sun09], 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.

This section 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, with that the cost function is $C(S) = c \in \mathbb{R}_+$ (wlog in this paper we will assume that $c = 1$), for every $S \neq \emptyset$ and $C(\emptyset) = 0$. Let $V_i = \mathbb{R}_+$. A (deterministic)*cost-sharing mechanism* consists of an allocation rule $\mathbf{x} : V_1 \times ... \times V_n \to \{0,1\}^n$ and a payment rule $\mathbf{p} : V_1 \times ... \times V_n \to \mathbb{R}^n$ that for a reported bid vector profile $\mathbf{b} = (b_1, ..., b_n)$ will determine which set $S = \{i \in S : x_i(b) = 1\}$, 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 $u_i(b, p) = x_i(b)v_i - p_i(b)$, where $(S, p)$ is the output of the mechanism.

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., $p_i(\mathbf{b}) \leq x_i(b)b_i$.
- *Anonymity/Symmetry*: For any permutation $\sigma \in S_n$ 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, we say that the mechanism is budget-balance.
- *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

$$x_i(v_i, \mathbf{b}_{-i})v_i - \mathbf{p}_i(v_i, \mathbf{b}_{-i}) \geq x_i(b_i, \mathbf{b}_{-i})v_i - \mathbf{p}_i(b_i, \mathbf{b}_{-i}). \tag{1}$$

  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, see [Dob+08] 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 $\mathbf{b}' \geq \mathbf{b}$ holds $x_i(\mathbf{b}') = 1$.

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 revenue.

- A cost sharing mechanism is *group-strategyproof* (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 $u_K(\mathbf{b}) > u_K(\mathbf{v})$.

In [Mou99] 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 [Sun09],

- A *cost-sharing method* is a function $\zeta : 2^{[n]} \to \mathbb{R}^n_{\geq 0}$ 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 $\zeta$ so 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 $\alpha$-approximate [Dob+08], 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. 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 [Dob+08][1]. Is know, [Dob+08] that there are nor better than $\mathcal{H}_n$-approximated randomized or deterministic truthfully and no-deficit mechanism, where $\mathcal{H}_n = \sum_{i=1}^n \frac{1}{i} = \Theta(\log(n))$.

[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.

**Observation 2.3.** 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 $\varepsilon$ (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 $\varepsilon$ converge to zero, we obtain that the mechanism is at least $(n-1+1/n)-$worst-case welfare.

Now, we would like to note that the given definitions 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 [Var09] or use multiple public keys to interact with a DeFi protocol [MRD22; MDP23]. This provides a new challenge and problems that are worth studying in permissionless mechanism design. For example, in [Dob+08] 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 the following 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 has no deficit, however, has $\mathcal{H}_n$-approximately welfare, where $\mathcal{H}_n$ are the harmonic numbers. The Shapley value mechanism has no-deficit and is $\mathcal{H}_n$-approximate for monotone cost functions $C$. Moreover, the authors prove that this mechanism is tight (up to a constant) 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, [MDP23], the mechanisms are not Sybil-proof/false-name proof. In the following section, we will give negative and positive results to the cost-sharing mechanism in this setting.

# 3 False-name proof and Cost-sharing mechanisms

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 that 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 this result by proving that a negative result that states that all non-deficit, strong-monotonic, and truthful mechanism are at least $(n+1)/2-$approximated. Finally, we will introduce the concept Sybil welfare invariance and prove that the Shapley value mechanism holds this property.

## 3.1 Sybil-proofness of Cost-sharing mechanisms

In general, truthfulness captures the idea that players can not act strategically in order to obtain more utility from the mechanisms. However, in pseudo-anonymous environments such as blockchain, this is not necessarily true [MDP23], 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 [MDP23]. 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

[MRD22] 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 is a set 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 holds:

- *Anonymity*: The maps $\mathbf{x}^n$ and $\mathbf{p}^n$ are equivariant under the action of $S_n$, that is for all $\sigma \in S_n$, $\mathbf{x}(\sigma b) = \sigma \mathbf{x}(b)$ and $\mathbf{p}(\sigma b) = \sigma \mathbf{p}(b)$ and for all $b \in \mathbb{R}^n_+$.
- *Consistent*: 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 projection $p_{n,m} : \mathbb{R}^m_+ \to \mathbb{R}^n_+$ such that $p_{n,m} \circ i_{n,m} = id_{\mathbb{R}^n_+}$. Then, the mechanism we have the following diagram commutes:

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

**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

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

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 set of bids $b^{K_i} = (b_i^1, ..., b_i^{k_i})$, where $K_i = [k_i]$. Then, we take $m = \sum_{i=1}^n k_i$, $\mathbf{b} = (b^{K_1}, ..., b^{K_n})$ 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, $\mathbf{p}_i(\mathbf{b}) = \sum_{j\in K_i} p_j^m(\mathbf{b})$. In our paper, we consider that the players' allocation, is the best allocation among all its Sybils' allocation. That is, $\mathbf{x}_i(b_i) = \max_{k\in K_i}\{x_k^m(b^{K_i}||\mathbf{b}_{-K_i})\}$. Therefore, its utility is

$$v_i \max_{k\in K_i}\{x_k^m(b^{K_i}||\mathbf{b}_{-K_i})\} - \sum_{k\in K_i} p_k^m(b^{K_i}||\mathbf{b}_{-K_i}), \tag{3}$$

where $\mathbf{b}_{-K_i}$ is the vector of bids reported by other players and $b^{K_i}||\mathbf{b}_{-K_i}$ is the concatenation of vectors. 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 be allocated the good. This is type of Sybil extension is motivated for the underlying mechanisms that are public goods funding mechanisms, since agents do not have extra utility by being able to use another identity to have access to the public good. This will be crucial for the following results[2]. 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 $\mathbf{b}_{-i} \in \mathbb{R}^\infty_+$ of bids, for every set of sybils $K_i$ and bid vector $b^k \in \mathbb{R}^{|K|}_+$, we have that

$$v_i\mathbf{x}_i(v_i, \mathbf{b}_{-i}) - \mathbf{p}_i(v_i, \mathbf{b}_{-i}) \geq v_i \max_{k\in K_i}\{x_k^m(b^{K_i}||\mathbf{b}_{-K_i})\} - \sum_{k\in K} p_k(b^{K_i}||\mathbf{b}_{-K_i}) \tag{4}$$

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

[2]We plan to study other types of utility functions and Sybil extensions in future work.

We will see, that the mechanisms proposed in [Dob+08] and [DO17] are not Sybil-proof. The mechanisms proposed in [Dob+08] are the VCG mechanism applied to the excludable public good problem and the Shapley value mechanism, the mechanism proposed in [DO17] is a modified version of the VCG mechanism with adding a cost per user. In the following, we will add these mechanisms for completness.

**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**

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

**Potential mechanism**

1. Choose the an outcome $S^\star \in \text{argmax}_{S\subseteq[n]}\{\sum_{i\in S} b_i - \mathcal{H}_{|S|}\}$.
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 previous mechanisms are symmetric, individually rational, and truthful [Dob+08]. The potential mechanism and the Shapley value mechanism have no deficit, while the VCG mechanism has deficit [Dob+08; DO17]. Moreover, the Shapley value mechanism is group-strategyproof. 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 $\emptyset \neq S \subseteq \mathbb{N}$.

**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.

**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 $S^\star = \emptyset$. 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**: Assume that $v_1 = 1 + \varepsilon$ 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 $\varepsilon$ On the other hand, the player 1 splits its bid in two $b_1 = 1/4$ and $b_1 = 1/4$, the outcome is $S = \{1, 2, 3, 4\}$ with payment total payment $p = 1/2$, and so total utility $1/2 + \varepsilon$. Therefore, the mechanism is not Sybil-proof.

**Potential mechanism**: Suppose 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 $p_1 = p_{n+1}$. Making $\varepsilon \to 0$, we have that with the sybil strategy, the utility of the player is $1-1/(n+1) > 0$, making the strategy profitable. □

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 [Dob+08], 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 3.4).

**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, $(n+1)/2-$budget-balance, and $(n+1)/2-$approximate.

*Proof.* 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 [Sun09] for more details. The weak-budget balance 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 $(n-1)/2+1$. 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 payments $C([n])$. Making a Sybil will not decrease its payment since at most will decrease the payment of the original identity, from $C([n])$ to $C([n])/2$ but will add the payment of the Sybil identity $C([n])/2$.

□

In fact, we will prove that this upper bound on social costs matches the lower bound when the mechanism is group-strategy-proof and Sybil-proof.

**Theorem 3.4** (Social-cost lower bound)**.** If a cost-sharing mechanism $\mathcal{M}$ is individually rational, $\alpha(n)-$approximate, no-deficit, symmetric, truthful, strong-monotonic, and Sybil-proof, then $\alpha(n) \geq (n+1)/2$.

To make the proof more readable, we will break the proof into different lemmas. In the proof we assume without loss of generality that $C$ is constant 1 for non-empty subsets.

**Lemma 3.5.** If a cost-sharing mechanism is strong-monotonic, symmetric, 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.* Lets 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 $j$ its 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. $\square$

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 $\mathbf{v}^n(\varepsilon) := (v_1 - \varepsilon, ..., v_n - \varepsilon)$.

**Lemma 3.6.** The sequence $\{v_n\}_{n\in\mathbb{N}}$ is well defined and is monotone non-increasing, in other words, $v_n \geq v_{n+1}$ for every $n \in \mathbb{N}$.

*Proof.* If $\alpha(n)$ is finite, then it implies that the mechanism is consumer sovereign for $n$ players (otherwise the worst-case welfare would be infinite, see a similar prove in [Dob+08]). Now, lets prove that 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 $\varepsilon > 0$. 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 non-decreasing. $\square$

**Lemma 3.7.** 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 $S = [n]$.

*Proof.* 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 3.5 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 $[k]$. If $k < n$, 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 has access to the public good when the bid vector profile is $(v_1 - \delta/2, ..., v_{n-1} - \delta/2))$. 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 $v_1 - \delta/4 - (v_1 - \delta/2) = \delta/4 > 0$. And so, the mechanism would not be Sybil-proof, leading to a contradiction.

□

**Lemma 3.8.** 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. $S = [n]$.

*Proof.* 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 $[n]$. □

**Lemma 3.9.** For every $n$, it holds $v_1 \leq 2v_n$.

*Proof.* Let's 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 let's prove it for $n$. If $v_n = v_{n-1}$, then clearly $v_1 \leq 2v_{n-1} = 2v_n$, and so let's assume that $v_n < v_{n-1}$. By the previous lemma, 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. 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 lemma 3.7, 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 $0 \leq v_1 - 2p_1 \leq (v_1 - \varepsilon/2) - 2v$, Making $v \to v_n$ and $\varepsilon \to 0$, we have that $2v_n \leq v_1$. □

**Lemma 3.10.** It holds $\sum_{i=1}^{n} v_i \leq \alpha(n)$.

*Proof.* Since for all $\varepsilon > 0$ 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 theorem 3.4 by using the previous lemmas. We know that, $2v_n \geq v_1$ for all $n \in \mathbb{N}$ so:

$$
\begin{aligned}
\alpha(n) &\geq \sum_{i=1}^{n} v_i && \text{(by lemma 3.9)} \\
&\geq v_1 + \sum_{i=2}^{n} \frac{v_1}{2} && \text{(by lemma 3.10)} \\
&= \frac{n+1}{2} v_1 \geq \frac{(n+1)}{2} && \text{(Since the mechanism is no deficit)}
\end{aligned}
$$

This concludes the prove to the theorem 3.4. Now, since every group-strategyproof is separable, we have that in particular is strong monotonic, and so we deduce the following corollary.

**Corollary 3.11.** If a cost-sharing mechanism $\mathcal{M}$ is incentive compatible, upper semi-continuos $\alpha(n)-$approximate, no-deficit, symmetric, group-strategyproof, and Sybil-proof, then $\alpha(n) \geq (n+1)/2$.

Therefore, by results 3.4 and 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.

### 3.2 Sybil Welfare invariant mechanisms

In the preceding section, we demonstrated that the Shapley cost-sharing mechanism is not Sybil-proof and the limitations of Sybil-proof, truthful, strong-monotonic and no deficit mechanisms. As reported in [MDP23], 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 welfare from $\mathcal{H}_n$ to $(n+1)/2$. 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. 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, Sybil-proof and has welfare bounded by the welfare of cost-sharing mechanism assuming that the number of players is known and can not generate Sybil identities. Lets first introduce this property for general mechanisms.

**Definition 3.12.** Let $\mathcal{M}$ be a one-parametric truthfull 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 mechanism outcome. The definition of social welfare strictly depends on the mechanism being studied, in our case we will use the social cost $\pi$ defined in the preliminaries. Suppose that for every agent $i$, with valuation $v_i$, there exists a strictly dominant set $B(v_i)$. We say that the mechanism $\mathcal{M}$ is *Sybil welfare invariant* if the worst-case welfare under private beliefs with full support of the Sybil mechanism is not larger than the original mechanism. That is, for every $n \in \mathbb{N}$ holds

$$\inf_{v\in\mathbb{R}^n_+} \mathcal{W}^{\mathcal{M}}(v,v) \leq \inf_{(v,b)\in\mathcal{Q}} \mathcal{W}^{\mathbf{Sy}(\mathcal{M})}(b,v)$$

where $v=(v_1,...,v_n)\in\mathbb{R}^n_+$, $B(v)=B(v_1)\times ... \times B(v_n)$, and $\mathcal{Q}=\{(v,b) : v\in\mathbb{R}^N_+, b\in B(v)\}$.

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

$$\sup_{v\in\mathbb{R}^n_+} \pi(v,v) \geq \sup_{(v,b)\in\mathcal{Q}} \pi^{\mathbf{Sy}(\mathcal{M})}(v,b). \tag{5}$$

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 of Sybil welfare invariant (SWI) mechanisms are those mechanisms such that its Sybil extension have strictly dominant sets for every valuation and that all BNESPB have at least the same welfare as the output of the mechanism with truthful reports. An SWI 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. SWI 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 attacks are a concern but eliminating them entirely is not feasible to identify the identities reported to the mechanism or too costly in terms of ex-post economic efficiency. An example of Sybil welfare invariant mechanisms are the Sybil-proof mechanisms. 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.

**Proposition 3.13.** The Shapley value mechanism is strong-monotonic. 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.

*Proof.* The Shapley value is the cost-sharing mechanism with cost-sharing method $\zeta(S) = 1/|S|$. Now lets $\mathbf{b}$ and $\mathbf{b}'$ 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 $b_i' \geq 1/|S'|$. On the other hand, $b_i \geq b_i' \geq 1/|S'|$. Therefore, $S' \subseteq \operatorname{argmax}_X\{|X| : b_i \geq 1/|X|\} = S$. 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 $1/|S|$. □

We know by the proposition 3.2 that the Shapley value mechanism is not Sybil-proof. In the following, we will study the Sybil-strategies of the Shapley-value mechanism with more detail. We will compute dominant sets and strictly 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. In the Sybil-extension mechanism, the space of actions of a player is

$$\mathcal{A} = \{(b_1, ..., b_k, ...) \mid \forall i \geq 1, b_i \geq 0, \text{ and } b_i = 0 \text{ for all but finitely many } i\}. \tag{6}$$

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

$$\mathcal{A}_v = S_\infty \cdot \{(v, 1/n_2, ..., 1/n_k, 0, ...) \in \mathcal{A} \mid \forall n_i \in \mathbb{N} \cap [i/v, +\infty), \quad n_k \geq n_{k-1} \geq ... \geq n_2\} \tag{7}$$

In the following lemma, we will see that a rational agent will prefer to pick strategies from $\mathcal{A}_v$, since is a dominant strategy set.

**Lemma 3.14.** The set of strategies $\mathcal{A}_v$ is a dominant strategy set of $\mathcal{A}$. That is, for every action $\mathbf{b}_i \in \mathcal{A} \setminus \mathcal{A}_v$, there is a $\mathbf{z}_i \in \mathcal{A}_v$ such that

$$u_i(\mathbf{z}, \mathbf{b}_{-i}) \geq u_i(\mathbf{b}_i, \mathbf{b}_{-i}) \text{ for every tuple of actions } \mathbf{b}_{-i}. \tag{8}$$

*Proof.* Given a vector $\mathbf{b}_i = (b_1, ..., b_k, 0, ...)$ (w.l.o.g. 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 8 by cases. 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 we would have that $z_2 \geq 1/n(\mathbf{z})$, but $b_1 \geq b_2 \geq z_2$ and so the first two identities would also be allocated when reporting $\mathbf{b}_i$, leading to a contradiction.

Since the mechanism is incentive compatible, we have that 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 $b_j \geq 1/n(\mathbf{b})$. On the other hand, since no Sybil identity has access when reporting $\mathbf{z}$, it holds that $z_{j(\mathbf{b}_i)} < 1/n(\mathbf{b}_i)$ and so $v/j(\mathbf{b}_i) < 1/n(\mathbf{b}_i)$. Since the payment when reporting $\mathbf{b}_i$ is $j(\mathbf{b}_i)/n(\mathbf{b}_i)$, we have that 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, 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, we have that 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 $z_{j(\mathbf{b}_i)} < 1/n(\mathbf{b}_i)$, and so $v/j(\mathbf{b}_i) < 1/n(\mathbf{b}_i)$ (or $1/j(\mathbf{b}_i) < 1/n(\mathbf{b}_i)$ if $v \geq 1$)). On the other hand, $z_{j(\mathbf{z})} \geq 1/n(\mathbf{z})$, and so $v/j(\mathbf{z}) \geq 1/n(\mathbf{z})$ (or $1/j(\mathbf{z}) \geq 1/n(\mathbf{z})$ in case $v \geq 1$) . Using both equations, in both cases, we deduce that $j(\mathbf{b}_i)/n(\mathbf{b}_i) > j(\mathbf{z})/n(\mathbf{z})$. Now, the utility is $u_i(\mathbf{b}_i, \mathbf{b}_{-i}) = v - j(\mathbf{b}_i)/n(\mathbf{b}_i)$ and $u_i(\mathbf{z}, \mathbf{b}_{-i}) = v - j(\mathbf{z})/n(z)$ since both have access to the public good and the payments for each Sybil is $1/n(\mathbf{b}_i)$ (resp. $1/n(\mathbf{z})$. And so, we deduce the result. $\square$

The bound 8 is not necessarily strict for some vector $\mathbf{b}_{-i}$, and so, the set $\mathcal{A}_v$ is not a strictly dominant set. For example, suppose $v = 1/2$ take the bid vector $b'_i = (2/3, 0, ...) \notin \mathcal{A}_v$ and $b_i = (1/2, 0, ...) \in \mathcal{A}_v$, then for every bid vector profile holds $\mathbf{b}_{-i}$, $u_i(b'_i, \mathbf{b}_{-i}) = u_i(b_i, \mathbf{b}'_{-i})$. So let's consider the sets

$$\mathcal{A}_v[x] := \left\{ b \in \mathcal{A} : \left\lfloor \frac{1}{b_i} \right\rfloor = \left\lfloor \frac{1}{x_i} \right\rfloor \text{ or } x_i = b_i = 0 \text{ for all } i \in \mathbb{N} \right\} \tag{9}$$

$$\overline{\mathcal{A}_v} := \bigcup_{x \in \mathcal{A}_v} \mathcal{A}_v[x] \tag{10}$$

**Observation 3.15.** If $b \in \mathcal{A}_v[x]$, then $u_i(x, \mathbf{b}_{-i}) = u_i(b, \mathbf{b}_{-i})$ for all $\mathbf{b}_{-i} \in \mathcal{A}$.

**Lemma 3.16.** The set $\overline{\mathcal{A}_v}$ is a strictly dominant strategy set.

*Proof.* Let $\mathbf{b}_i = (b_1, b_2, ...) \in \mathcal{A} \setminus \overline{\mathcal{A}_v}$, and $\mathbf{z}$ as defined in the previous lemma. Wlog of generality, we can assume that $b_1 \geq b_2 \geq ...$ by taking an appropriate permutation of indexes. Then, there exists a coefficient $j$ such that $b_j \geq v_i/(j-1)$. Take the last index with this property. And consider $n = \left\lfloor \frac{1}{b_j} \right\rfloor$ and $\mathbf{b}_{-i} = \underbrace{(1/n, ..., 1/n)}_{n-j \text{ times}}$. If we consider the vector profile $\mathbf{b}_i, \mathbf{b}_{-i}$, we have that, the first $j$ elements of $\mathbf{b}_i$ holds $b_k \geq b_j \geq 1/n$ for $j = 1, ..., k$. By definition, all the elements of $\mathbf{b}_i$ are equal to $1/n$ and so all these elements are allocated. Since the mechanism is budget-balance, we have that the total payment is 1, i.e. $\sum p_j = 1$. Since the payment of the non $i$th Sybil identities pay at most $1/n$, we have that the total payment of $i$ (taking into account the sybils) is at least $j\frac{1}{n}$. Now if $v_i > 0$,

$$\begin{aligned} u_i(\mathbf{b}_i, \mathbf{b}_{-i}) &= v_i - \mathbf{p}_i \\ &\leq v_i - j/n \\ &\leq v_i - \frac{j}{j-1} v_i < 0. \end{aligned}$$

In the first inequality, we are using that $\mathbf{p}_i \geq j/n$ and in the second inequality, we are using that $\frac{j-1}{v} \geq \left\lfloor \frac{1}{b_j} \right\rfloor = n$. On the other hand, consider the vector profile $\mathbf{z}$ as the previous one. The allocation of the vector profile $\mathbf{z}, \mathbf{b}_{-i}$ is null, and so the utility of the player $i$ is zero. Observe that $nv < j$, since $b_j \geq v_i/(j-1)$ and $n = \left\lfloor \frac{1}{b_j} \right\rfloor$ So, we have that

$$z_{j+k} \leq \frac{\min\{v_i, 1\}}{j+k} < \frac{1}{n+k}$$

for all $k \geq 0$, by definition of $\mathbf{z}$. Therefore, the allocation profile of the bid vector profile $(\mathbf{z}, \mathbf{b}_{-i})$ is null, leading to zero utility to the agent $i$. And so, we deduce the result. □

**Observation 3.17.** Since the Sybil Shapley value mechanism is not truthful, the agents can be strategic to maximize its utility. 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 $z \in \mathcal{A}_v$ 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

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

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

$$\underset{x \in \mathcal{A}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x, \mathbf{b}_{-i})] = \underset{x \in \overline{\mathcal{A}_v}}{\operatorname{argmax}} \quad \mathbb{E}_{\mathbf{b}_{-i} \sim \mathcal{D}}[u_i(x, \mathbf{b}_{-i})] \tag{11}$$

by using that $\overline{\mathcal{A}_v}$ is a strictly dominant set. So, we will assume that, in equilibrium, agents will choose strategies from $\overline{\mathcal{A}_v}$. Now, since the Shapley value mechanism is no longer truthful under the Sybil extension, the agents will choose actions or strategies that maximize their expected utility over their private beliefs.

**Theorem 3.18** (Sybil welfare invariance)**.** The Shapley value mechanism is Sybil welfare invariant.

*Proof.* 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 3.16, the agents take actions in $\overline{\mathcal{A}_{v_1}} \times ... \times \overline{\mathcal{A}_{v_n}}$. Now, lets $x = (x_1, ..., x_n)$ be the actions taken by the players. Since the outcome of every element in $\mathcal{A}_{v_i}[x_i]$ does not change, we will assume without loss of generality $x_i \in \mathcal{A}_v$. Now, 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 $\mathcal{A}_v$, we have that 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-balance, we have that the sum of payments is either 0 if no agent is allocated or $C([n])$ otherwise. Now, we will prove that $\pi(S(x)) \leq \mathcal{H}_n \pi(S^\star)$ by cases.

**Case 1** $S(v) = S(x) = \emptyset$. There is nothing to prove since 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** $S(x) \neq \emptyset$ and $S(v) \neq \emptyset$. since we have that $S(v) \subseteq S(x)$, we have that $\sum_{i \notin S(v)} v_i \geq \sum_{i \notin S(x)} v_i$. Also, since both sets are non-empty, we have that $C(S(v)) = C(S(x)) = C([n])$. Putting all together, we deduce that $\pi(S(x)) \leq \pi(S(v)) \leq \mathcal{H}_n \pi(S^\star)$.

**Case 3** $S(x) \neq \emptyset$ and $S(v) = \emptyset$. Since $S(v) = \emptyset$ and the worst-case social cost is $\mathcal{H}_n$, and so $\sum_{i \in [n]} v_i \leq \mathcal{H}_n$, see [Dob+08] for more details. For every $i \in S(x)$ consider the number of $i$ Sybil identities $k_i$ such that the public good is allocated. Since $x \in \mathcal{A}_{v_i}$, we have that $v_i/j \geq x_i^j$

for $j = 1, ..., k_i$. Let $m = \sum_{i=1}^{n} k_i$ be the total number of Sybil identities that have access to the public good. Then we have that $x_i^j \geq 1/m$, and using both inequalities we deduce that $v_i \geq k_i/m$. Therefore $\sum_{i \in S(x)} v_i \geq \sum_{i \in S(x)} k_i/m \geq 1$. In this case, we have that

$$\begin{aligned}
\pi(S(x)) &= C([n]) + \sum_{i \notin S(x)} v_i = C([n]) + \sum_{i \in [n]} v_i - \sum_{i \in S(x)} v_i \\
&\leq C([n]) + \sum_{i \in [n]} v_i - 1 \\
&= \sum_{i \in [n]} v_i \leq \mathcal{H}_n \pi(S^\star).
\end{aligned}$$

□

In summary, we have proved that even when the number of agents is unknown to the mechanism designer, and the agents participating in the mechanism, the Shapley value mechanism has the same worst-case welfare 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 organization (DAO) 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. Probably, to maintain the same worst-case equilibria under false-name strategies the mechanism will have to shield the bids, similar to [FW20], by using different cryptographic tools such as commit-and-reveal.

# 4 Discussion

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 [DO17] and [BMS22], are Sybil welfare invariant. To do so, we will need to extend the definition of SWI under combinatorial domains. Also, we leave as future work, to see if 3.4 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 $C$. Outside the cost-sharing literature, we aim to study if mechanisms such as the one proposed in [BGR23] are Sybil welfare invariant and if not, make adjustments to the mechanism to maintain the worst-case welfare.

# 5 Acknowledgments

The author would like to express sincere gratitude to the Ethereum Foundation for generously funding the scholarship that made this research possible.

# References


[Har68] JOHN C Harsanyi. “Part II: Bayesian equilibrium points”. In: *Management Science* 14 (1968), pp. 320–334.

[Mye81] Roger B Myerson. “Optimal auction design”. In: *Mathematics of operations research* 6.1 (1981), pp. 58–73.

[MR85] Eric S Maskin and John G Riley. “Auction theory with private values”. In: *The American Economic Review* 75.2 (1985), pp. 150–155.

[Mou99] Hervé Moulin. “Incremental cost sharing: Characterization by coalition strategy-proofness”. In: *Social Choice and Welfare* 16 (1999), pp. 279–320.

[MS01] Hervé Moulin and Scott Shenker. “Strategyproof sharing of submodular costs: budget balance versus efficiency”. In: *Economic Theory* 18 (2001), pp. 511–533.

[YSM01] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. “Robust combinatorial auction protocol against false-name bids”. In: *Artificial Intelligence* 130.2 (2001), pp. 167–181.

[Dou02] John R Douceur. “The sybil attack”. In: *International workshop on peer-to-peer systems*. Springer. 2002, pp. 251–260.

[Fei+03] Joan Feigenbaum et al. “Hardness results for multicast cost sharing”. In: *Theoretical Computer Science* 304.1-3 (2003), pp. 215–236.

[YSM04] 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.

[SY05] Takayuki Suyama and Makoto Yokoo. “Strategy/false-name proof protocols for combinatorial multi-attribute procurement auction”. In: *Autonomous Agents and Multi-Agent Systems* 11 (2005), pp. 7–21.

[CRS06] 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.

[DH06] 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.

[LSM06] Brian Neil Levine, Clay Shields, and N Boris Margolin. “A survey of solutions to the sybil attack”. In: *University of Massachusetts Amherst, Amherst, MA* 7 (2006), p. 224.

[Yu+06] 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.

[BS07] 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.

[BS08] 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.

[Dob+08] 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.

[Mül+08] Wolf Müller et al. "Sybil proof anonymous reputation management". In: *Proceedings of the 4th international conference on Security and privacy in communication netowrks*. 2008, pp. 1–10.

[WC08] Liad Wagman and Vincent Conitzer. "Optimal False-Name-Proof Voting Rules with Costly Voting." In: *AAAI*. Vol. 8. 2008, pp. 190–195.

[Yu+08] 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.

[Kri09] Vijay Krishna. *Auction theory*. Academic press, 2009.

[RS09] Tim Roughgarden and Mukund Sundararajan. "Quantifying inefficiency in cost-sharing mechanisms". In: *Journal of the ACM (JACM)* 56.4 (2009), pp. 1–33.

[Sun09] Mukund Sundararajan. *Trade-offs in cost sharing*. Stanford University, 2009.

[Var09] Hal R Varian. "Online ad auctions". In: *American Economic Review* 99.2 (2009), pp. 430–434.

[Yu+09] Haifeng Yu et al. "Dsybil: Optimal sybil-resistance for recommendation systems". In: *2009 30th IEEE Symposium on Security and Privacy*. IEEE. 2009, pp. 283–298.

[Iwa+10] 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.

[SR11] 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.

[TIY11] 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.

[She12] Itai Sher. "Optimal shill bidding in the VCG mechanism". In: *Economic Theory* 50 (2012), pp. 341–387.

[AHV14] Colleen Alkalay-Houlihan and Adrian Vetta. "False-name bidding and economic efficiency in combinatorial auctions". In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 28. 1. 2014.

[Gup+15] Anupam Gupta et al. "Efficient cost-sharing mechanisms for prize-collecting problems". In: *Mathematical Programming* 152 (2015), pp. 147–188.

[DO17] Shahar Dobzinski and Shahar Ovadia. "Combinatorial cost sharing". In: *Proceedings of the 2017 ACM Conference on Economics and Computation*. 2017, pp. 387–404.

[Lin+17] Jian Lin et al. "Sybil-proof incentive mechanisms for crowdsensing". In: *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE. 2017, pp. 1–9.

[CPR19] Xi Chen, Christos Papadimitriou, and Tim Roughgarden. "An axiomatic approach to block rewards". In: *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. 2019, pp. 124–131.

[ZL19] 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.

[FW20] 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.

[BMS22] 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.

[FM22] Federico Fioravanti and Jordi Massó. “False-name-proof and strategy-proof voting rules under separable preferences”. In: *Available at SSRN 4175113* (2022).

[MRD22] 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.

[BGR23] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. “When Bidders Are DAOs”. In: *arXiv preprint arXiv:2306.17099* (2023).

[MDP23] Bruno Mazorra and Nicolás Della Penna. “The Cost of Sybils, Credible Commitments, and False-Name Proof Mechanisms”. In: *arXiv preprint arXiv:2301.12813* (2023).