Cost sharing mechanism for relayers

Bruno Mazorra Roig
Universitat Pompeu Fabra
brunomazorra@gmail.com

September 11, 2023

1 Introduction

In the landscape of Ethereum's proof-of-stake (PoS) ecosystem, node operators are tasked with running three software elements: a validator client, a consensus client, and an execution client. Emerging from this landscape is MEV-boost, a uniquely independent open-source software that acts as a sidecar to the beacon node, facilitating block-building operations through a network of builders. These builders are tasked with producing full blocks, with the objective of optimizing the blocks' efficiency. The blocks are then submitted to relays, entities that aggregate and select the blocks with the highest fees in an English auction fashion.

In this intricate setup, one instance of MEV-boost can be set up by a validator to connect with multiple relays. The most profitable block received from MEV-boost is then proposed by the validator's consensus layer client to the Ethereum network for attestation and block inclusion. There are three integral components in the MEV-Boost architecture: the validator, the builder, and the relayer. Each of these components plays a unique role in maintaining a fair and functional system, with the relayer acting as the trusted third party to ensure the integrity of the exchange process between the validator and the builder.

Despite this well-orchestrated system, the relayer remains an expensive software piece that is currently misaligned with the overall ecosystem due to its inability to generate profits incurring net costs by the relay operators. This paper aims to present the leverage of different techniques of cost-sharing mechanisms to produce a Dominant-Strategy Incentive Compatible (DSIC) and no-deficit mechanism to finance the relayers, with the ultimate goal of making relayer operation a non-subsidizing venture. We will delve into the theoretical framework and practical implementation of this mechanism, providing insights into how this critical component of the MEV-Boost ecosystem can be adequately funded, thus ensuring the long-term viability and stability of MEV-Boost and PBS.

2 Our contribution

3 Preliminary

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 the false-name proofness of this mechanism and its applications on funding relayer sets in Blockchain and in particular in PBS/MEV-Boost. In particular, we will prove that the mechanisms proposed in [Dob+08] are not Sybil-proof.

In a cost-sharing mechanism design problem, several participants with unknown preferences vie to receive some goods or services, and each possible outcome has a known cost. Formally, we consider problems defined by a set of players N and a set of services m with cost functions

$C : [m] \times 2^N \to \mathbb{R}^+$ that describes the cost incurred by the mechanism as a function of the outcome (i.e., $C(i, S)$ is the cost of the public good with set of winners S).

This section focuses on the study of the *public excludable good* problem, which involves determining whether to finance a set public good and, if so, identifying who is permitted to use them. We will assume that for every i, $C(i, S) = c_i \in \mathbb{R}_{\geq 0}$ for every $S \neq \emptyset$ and $C(i, \emptyset) = 0$. A *cost-sharing mechanism* will consist of an allocation rule $\mathbf{x} : \mathbb{R}^\infty \to 2^N$ and a payment rule $\mathbf{p} : \mathbb{R}^N \to \mathbb{R}^N$ that will determine which set S is allocated the public good and how much each player must pay. Player i has a private value v_i for being included in the chosen set (having access to the public good). We assume that players have quasi-linear utilities, meaning that each player i aims to maximize $u_i(S, p_i) = v_i x_i - p_i$ where $x_i = 1$ if $i \in S$ and $x_i = 0$ if $i \notin S$.

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

- *No positive transfers* (NPT): Players never get paid, i.e., $p_i(\mathbf{b}) \geq 0$.
- *Incentive compatible* (IC): When allocated, players never pay more than they bid, otherwise, they are charged nothing, i.e., if $i \in x_i(b)$ then $p_i(\mathbf{b}) \leq b_i$.
- *Symmetry*: For any permutation $\sigma \in S_\infty$ holds $x_i(\mathbf{b}) = x_{\sigma(i)}(\sigma(\mathbf{b}))$ and $p_i(\mathbf{b}) = p_{\sigma(i)}(\sigma(\mathbf{b}))$.
- *Truthful*: For every bid vector $\mathbf{b}_{-i}$, true valuation v_i and bid $b_i \in \mathbb{R}_{\geq 0}$, holds

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

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 this context, 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 $\pi : 2^{\mathbb{N}} \to \mathbb{R}_{\geq 0}$. Given the cost C and the true valuations vector $v \in \mathbb{R}^\infty$, social costs are defined by $\pi(S) := C(S) + \sum_{i \notin S} v_i$.

In [Dob+08] the authors propose three different truthful mechanisms, the VCG mechanism, the Shapley mechanism, and the Hybrid mechanism. 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 Hybrid 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.

4 Applications of Cost-sharing mechanisms

The relayers naturally inherit the structure of a public excludable good, since they can control which builders have access to bid in the auction, which validators can sell the right to build a block in a specific slot, and finally, which constraints must the block hold (e.g. giving access to the execution of some protocols or users). For example, due to the potential legal costs, some relayers excluded Tornado cash from using their service. Due to this structure, we can apply the cost-sharing mechanism to publicly fund the relayers without incurring costs to the organization or agents responsible for them. In this section, we will discuss two models, the basic cost-sharing model and the codependent model. We will give truthful mechanisms for both mechanisms, but both will fail to be Sybil-proof. With minimal changes to the mechanism and making a weaker truthful condition, we will obtain a Sybil-proof mechanism with the same welfare in equilibrium as the previous mechanism.

4.1 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 called the Sybil-extension mechanism. But 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 $\{(\mathbf{x}^n : \mathbb{R}^n \to \mathbb{R}^n, \mathbf{p}^n : \mathbb{R}^n \to \mathbb{R}^n)\}_{n\in\mathbb{N}}$ such that is:

- *Anonymity*: The maps $\mathbf{x}^n$ and $\mathbf{p}^n$ are equivariant under the action of S_n, that is $\pi \in S_n$, $\mathbf{x}(\pi b) = \pi\mathbf{x}(b)$ and $\mathbf{p}(\pi b) = \pi\mathbf{p}(b)$ and for all $b \in \mathbb{R}^n$.
- *Consistent*: Let $i_{n,m} : \mathbb{R}^n \hookrightarrow \mathbb{R}^m$ be an 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:

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

More formally:

- A symmetric cost-sharing mechanism is *Sybil-proof* if for every vector $\mathbf{b}_{-i} \in \mathbb{R}^\infty$ of bids, for every set of sybils K and bid vector $b^k \in \mathbb{R}^{|K|}$, we have that

$$v_i\mathbf{x}_i(v_i, \mathbf{b}_{-i}) - \mathbf{p}_i(v_i, \mathbf{b}_{-i}) \geq v_i \max_{i\in K}\{\mathbf{x}_i(b^k||\mathbf{b}_{-i})\} - \sum_{i\in K} p_k(b^k||\mathbf{b}_{-i}) \tag{2}$$

where $b^k||\mathbf{b}_{-i}$ is the concatenation of vectors.

We will see, that the mechanisms proposed in [Dob+08] are not Sybil-proof (we will show that the Hybrid mechanism is not Sybil-proof, the others follow similarly).

Proposition 1. *The Hybrid mechanism, the Shapley mechanism, and the VCG for public excludable goods are not Sybil-proof.*

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.

Here we will give a bound on the worst-case welfare that a cost-sharing mechanism that is no-deficit, Sybil-proof, and truthful mechanism can guarantee.

Sybil-proof non-trivial 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. The players $i = 1, ..., k$ have access to the public good and each player pays $p_i = C(N)/2$ for $i = 1, ..., k$.

Proposition 2. *The SP Hybrid mechanism is incentive compatible, truthful, Sybil-proof, weak-budget-balance, and* $(n/2+1)-$*approximate social welfare.*

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

Theorem 1. *If a cost-sharing mechanism* $\mathcal{M}$ *is* $\alpha(n)-$*approximate, symmetric, group-strategy proof (in particular truthful) and Sybil-proof, then* $\alpha(n) = \Omega(n)$.

To prove this first we will use the result, proved in [Mou99] which shows 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 [**empty citation**],

- 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 $\mathcal{M} = (\mathbf{x}, \mathbf{p})$ if there exists a cost-sharing method ζ so that $\mathbf{p} = \zeta \circ \mathbf{x}$.

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, we have the tools to proceed with the proof.

Therefore, by results 1 and 2 we have upper and lower bounded the worst-case welfare match asymptotically. 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 its efficiency the mechanism.

4.2 Positive Externalities of Sybil strategies

In the preceding section, we demonstrated that the Shapley cost-sharing mechanism is not Sybil-proof and the limitations of Sybil-proof, symmetric, Group strategy-proof, and no deficit mechanisms. As reported in [MDP23], the creation of Sybils can potentially reduce social welfare in some mechanisms and cause negative externalities. However, this is not the case for cost-sharing mechanisms. We will see that if we consider the Sybil-extension of the cost-sharing mechanism we will have a mechanism that is no-deficit, group strategy-proof, Sybil-proof and has welfare bounded by the welfare of cost-sharing mechanism assuming that players can not generate Sybil identities.

Notes: Using one real identity is a strictly dominant strategy (against other strategies). Even if Sybils have costs. What happens if Sybils have costs? Redefine mechanism to not have costs in Sybils (players can send $(v_i^1, ..., v_i^n)$.

In equilibrium, (Bayesian whatever) the welfare is lower bounded by the truthful one (and just one I think). By tim theorem is also upper bounded.

Defines another notion of the Positive externality of Syibls. Sybils increase welfare expost (even more, more utility for all players). Weak the notion of truthfulness, we have Sybil-proofness.

In summary, we have that without truthfulness we can achieve pseudo-truthfullnes and Sybil-proofness without Sacrificing welfare.

Is a weird result not gonna lie.

5 Builders-Validator Codependent model

Previously, we have assumed that both, validators and builders have private and independent valuations. However, in reality, this is not the case. In other words, we assumed that the expected payoff realized by builders and validators is independent of which builders and validators have access to the relayer. However, the base cost-sharing model is not accurate enough for modeling the realized utility of agents having access to the relayers in PBS. More specifically, if a validator of a slot does not have access to the relayer, she must build the block on its own, not allowing builders to produce a block and so decreasing its expected payoff. On the other hand, if a builder or set of builders does not have access to the relayer, the competition pressure decreases in the slot english auction, decreasing the block efficiency and the highest bid of the auction in equilibrium.

Example: assume that for each slot, each builder produces a block with private value v_i drawn from distribution X_i. Assuming that the random variables $X_1, ..., X_n$ are i.i.d. (where n is the number of builders that have access to the relayer), the validator profit is $\mathbb{E}[X^{(2)}]$, where $X^{(n-1)}$ is the $(n-1)$th order statistic of $X_1, ..., X_n$, i.e. $X^{(n-1)} = 2\text{-max}\{X_1, ..., X_n\}$.

We have a set of builders $\mathcal{B} = [n]$, a set of validators $\mathcal{V} = [m]$, and a set of relayers $\mathcal{R} = [r]$. We will assume that $r = 1$. Every validator $i \in \mathcal{V}$ has a number of assets $s_i \in \mathbb{R}_{\geq 0}$ staked and therefore has a probability $\alpha_i = \frac{s_i}{\sum_{l \in \mathcal{V}} s_l}$ of being selected as a block proposal.

In this context, builders valuations are a monotone function $v_b : 2^{\mathcal{V}} \to \mathbb{R}_{\geq 0}$, where $v_b(V)$ represents the expected value of builder $b \in \mathcal{B}$ if he has access to the relayer and the validators on V have access to the relayer. If builders are risk-neutral agents, then we can assume that $v_b(\alpha) = u_b \alpha$ since the expected payoff of the player is the expected profit in the English auction times the probability of the validator having access to the relayer.

On the other hand, validators' valuations are of the form $v_i : 2^{\mathcal{B}} \to \mathbb{R}_{\geq 0}$ for $i \in \mathcal{V}$ and depend on the (we will assume that v_i is symmetric and submodular).

In this model, we want to maximize

$$\sum_{i \in B'} v_i(V') + \sum_{j \in V'} \phi_i(\mathcal{B}')$$

subject to the no-deficit condition.

For online-learning algorithms, we need to assume that validators and builders are myopic.

First, let's propose the family of mechanisms parametrized by $\gamma \in [0, 1]$. The mechanisms $\mathcal{M}_\gamma$ consists of choosing:

$$(B^\star, V^\star) \in \text{argmax}\left\{\sum_{b \in B'} v_i(V') + \sum_{j \in V'} \phi_j(B') : (B', V') \in \mathcal{A}_\gamma\right\},$$

$$\mathcal{A}_\gamma := \left\{(B', V') \in 2^B \times 2^V : v_b(V') \geq \gamma \frac{c_r}{|B'|} \text{ and } v_i(B') \geq (1-\gamma)\frac{c_r}{|V'|}, \text{ for all } b \in \mathcal{B}, \quad i \in \mathcal{V}\right\},$$

$$p_b = \gamma \frac{c_r}{|B'|} \text{ if } b \in B^\star, 0 \text{ if } b \notin B^\star,$$

$$p_i = (1-\gamma)\frac{c_r}{|V'|} \text{ if } i \in V^\star, 0 \text{ if } i \notin V^\star.$$

The parameter γ models the proportion of the relayer cost that must be paid by the builders and validators as independent sets. The set of parametric mechanisms gives more freedom for the relayer to be funded depending on which set in aggregation values more the existence of a relayer. For example, if the expected MEV is very high and the competition is a high builder concentration. This happens, for example, such as when builders have i.i.d private valuations and the second order statistic converges rapidly to the support upper bound. Therefore, the builders' expected payoff is small compared to the validators' expected payoff. On the other hand, if there is not enough competition, for example when the difference between the first and the second order statistic is very high, the expected payoff of the builder increases and the validator payoff decreases.

In the case where the MEV extracted and observed is modelled by i.i.d cumulative distribution functions, then the relayer could approximate the first and second-order statistic and choose the parameter γ that maximizes the total welfare of the mechanism $\mathcal{M}_\gamma$. However, in general, the lack of accurate priors, the changes in the block-space demand, and asymmetry between To compute, the solution of the previous optimization algorithm we propose the following greedy algorithm:

Greedy algorithm

1. Take $v_1, ..., v_n$ and $\phi_1, ..., \phi_m$, $B = [n]$ and $V = [m]$.
2. Order the elements of V and B by its valuations with $\alpha_T = \sum_{i \in V} \alpha_i$ and B.
3. Set $B \leftarrow \{i \in B : v_i(V) \geq \gamma \frac{c_r}{|B|}\}$.
4. Set $V \leftarrow \{j \in V : \phi_i(B) \geq (1-\gamma) \frac{c_r}{|V|}\}$.
5. Check if all elements $i \in B$ hold $v_i(V) \geq \gamma \frac{c_r}{|B|}$, then output (B, V) otherwise go back to step 2).

Lemma 1. *The greedy algorithm computes a solution to the previous optimization problem.*

Proof. Let (B', V') be the solution of the greedy approximation algorithm and let $(B^\star, V^\star)$ be the solution of the optimization problem. Let $\alpha' = \sum_{i \in V'} \alpha_i$ and $\alpha^\star = \sum_{i \in V^\star} \alpha_i^\star$. First, $B' \subseteq B^\star$ and $V' \subseteq V^\star$. This follows by considering the tuple $(B' \cup B^\star, V' \cup V^\star)$. This tuple is feasible and has at least the sum of payoffs of $(B^\star, V^\star)$. Since the last is an optimal solution, we conclude the claim. Now, assume that the output is not the same and that there is an iteration k of the greedy algorithm such that $B_k \not\subseteq B^\star$ or $V_k \not\subseteq V^\star$, however in the iteration $k-1$, we have that $B_{k-1} \supseteq B^\star$ and $V_{k-1} \supseteq V^\star$. Since $V_{k-1} \supseteq V^\star$, we must have that for all $i \in B^\star$ holds $v_i(\alpha_{k-1}) \geq v_i(\alpha^\star) \geq \gamma \frac{c_r}{|V^\star|} \geq \gamma \frac{c_r}{|V_{k-1}|}$ and so $B^\star \subseteq B_k$. Now, similarly, we must have that $V^\star \subseteq V_k$, leading to a contradiction, therefore proving the result. In the proof we fundamentally proved that the maps v_i and ϕ_j are monotone for all $i \in [n]$ and $j \in [m]$. □

Theorem 2. *For every $\gamma \in [0, 1]$, the mechanism $\mathcal{M}_\gamma$ is incentive compatible, truthful and has no deficit.*

Proof. The non-deficit condition and the incentive compatibility are held by construction. Let's now prove the truthfulness. Now let's prove that is truthful. Let v the true valuation of an agent $b \in B$. Let $\tilde{v}$ be another report of the agent. If in both allocations the agent has access to the public good, then the payment is the same and therefore, in this case, the agent has the same utility. In the case that with the misreport $\tilde{v}$, he has no access to the public good, then the truthful conditions hold. Now assume that the agent does not have access to the public good when reporting v. If he has access when reporting $\tilde{v}$, means that the payment is higher than its real valuation, leading to negative utility. This finishes the proof. The proof is analogous for the set agents in the set V. □

Compute worst-case welfare for $\gamma = 0, 1$. The problem is trivial.

5.1 Online learning

$$\text{Regret}_T(\mathcal{A}) = \underset{(\mathbf{v}_1,\boldsymbol{\phi}_1),\ldots,(\mathbf{v}_T,\boldsymbol{\phi}_T)\in l\times 2^{[n]}}{\text{supremum}} \left\{ \max_{\gamma\in[0,1]} W(\mathbf{v}_t,\boldsymbol{\phi}_t,\gamma) - \sum_{t=1}^{T} W(\mathbf{v}_t,\boldsymbol{\phi}_t,\gamma^{\mathcal{A}}) \right\} \tag{3}$$

Since the function W_t is piecewise constant in terms of then we need to have lower bounds on the minimum length of the intervals of the parameters to have a good upper bound on the number of necessary steps for reaching global maximum.

Conjectured lemma: Let $f_t : [0,1] \to \mathbb{R}_+$ such that $f_t(x) \geq \min\{f(a), f(b)\}$ for all $x \in [a,b]$ and lets assume that is a piecewise constant function. Moreover, let's assume that the discontinuities $a_1 \leq ... \leq a_l$ hold $|a_{i+1} - a_i| \geq \delta$ for some fixed δ.

For one function the natural has worst case convergence $1/2^n \geq \delta$ and so $n \leq \log(1/\delta)/\log(2)$. What in the online setting?

To me looks like randomizing which action to take in the intervals $[i\delta/n, (i+1)\delta/n]$ seems a natural no-regret algorithm. Is not deterministic, but the mechanism designer can randomize γ before committing to it. Since the mechanism is truthful for all γ the randomization for γ is also truthful.

If we assume som sparsity in the distribution of holds in γ, then we can assume that we have a set up of regret algorithm with finite sets, and use any no-regret algorithm such has MWU.

May be we do not need previous assumption. We can consider the randomized version of the mechanism, and start with the uniform distribution and update the distribution. We can first break the interval with finite set of points $\gamma_1 = 0, ..., \gamma_r = 1$ and define distributions over these elements. If M_γ is "discrete" convex, probably is convex in the randomized version. Then, we can use convex online learning to minimize regret. Probably, we can do this without discretizing.

Conjecture: For any triple $\gamma_1 < \gamma_2 < \gamma_3$, we have that $W(\gamma_2) \geq \min\{W(\gamma_1), W(\gamma_3)\}$. Conjecture is false! Even when both v_i and φ are linear.

6 Discussion

References

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

[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.

[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.

[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).

Proof. 1 Assume that C is constant for non-empty subsets, and $v_1 = 1+\varepsilon$ and $v_2 = v_3 = 1/3-\varepsilon$. Then the outcome of the mechanism is $S = \{1\}$ with $p_1 = 1$. 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 $p \leq 1/2$. Similar arguments are valid for the VCG mechanism. □

Proof. 2

□

Proof. 1 Let's assume that the mechanism is $\alpha(n)-$approximate. Let $p(1)$ be the minimum bid such that a player must bid in order to obtain when presenting itself to the mechanism alone. And let $p(n) = \inf_{p \geq 0}\{x(\mathbf{v}) = [n] | \mathbf{v} \in \mathbb{R}^n_+ \text{ and } \mathbf{v} = (p(1), p, ..., p)\}$ for $n \geq 2$.

Claim: $p(n)$ is well-defined for all n or the claim is proved. Assume that for all n, $p(n)$ does not exist, then we can make $p \to +\infty$ obtaining that the mechanism is ∞-approximate with n players and so we deduce the result for the numbers n with this property. If it does not exist, we define $p(n) = +\infty$.

Now we will assume that $p(n)$ exists, and moreover that $p(n) \leq 1$, otherwise again the claim would be proved. First, we know that since is $\alpha(n)-$approximate, we have that $1 + (n-1)p(n) \leq \alpha(n)$. If the first player creates l new identities with bid $p(n)$, then two things can happen:

Case 1: The mechanism just serves the public good to the first player for an infinite succession of sybils $l_1, l_2, ...$ Then, we would have that if the distribution of valuations where $p(1)$ and $v_2 = ... = v_{n+l_k} = p(n)$, then $\alpha(n + l_k) \geq (n - 1 + l_k)p(n)$. Making $k \to +\infty$ we have that $\alpha(n) = \Omega(n)$.

Case 2: Exist M such that all players (and Sybils get served) for $n \geq M$. In this case, the player that made the Sybil strategy pays $lp(n - 1 + l)$. Since the mechanism is Sybil-proof, we have that

$$0 \geq p(1) - lp(n - 1 + l)$$

and so $lp(n - 1 + l) \geq p(1)$ for all $n \geq M$. Therefore, we have that $p(n + 1) \geq p(1)/2$ for all $n \geq M$, and so $\alpha(n) = \Omega(n)$. □