Gini index based initial coin offering mechanism

Mingyu Guo1 · Zhenghui Wang1 · Yuko Sakurai2

Accepted: 28 October 2021 / Published online: 9 November 2021 © Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
As a fundraising method, Initial Coin Offering (ICO) has raised billions of dollars for thousands of startups. Existing ICO mechanisms place more emphasis on the short-term benefits of maximal fundraising while ignoring the problem of unbalanced token allocation, which negatively impacts subsequent fundraising and has bad effects on introducing new investors and resources. We propose a new ICO mechanism which uses the concept of Gini index for the very first time as a mechanism design constraint to control allocation inequality. Our mechanism has an elegant and straightforward structure, which makes it explainable. It allows the agents to modify their bids as a price discovery process, while limiting the bids of whales. Under natural technical assumptions, we show that under our mechanism most agents have simple dominant strategies and the equilibrium revenue approaches the optimal revenue asymptotically in the number of agents. We verify our mechanism using real ICO dataset we collected, and confirm that our mechanism performs well in terms of both allocation fairness and revenue.

Keywords Mechanism design · Initial coin offering · Gini index

1 Introduction

As a primary fundraising tool for startups, Initial Coin Offering (ICO) is very eye-catching in the capital market. According to [5], 718 ICOs ended in 2017 and raised around 10 billions (USD) in total. By 2018, the ICO fundraising market has grown significantly. The total fundraising for the year reached 11.5 billions (USD), and the number of ended ICOs increased to 2517.

Despite the popularity and the huge amounts of funds being raised, popular ICO mechanisms are surprisingly unsophisticated. Vitalik Buterin [1] analyzed some token sale
models and claimed that an optimal token sale model has not been discovered yet. There are two commonly used ICO mechanisms. One is simply the fixed price mechanism. The fixed price mechanism does not offer a price discovery process. Many cryptocurrencies released via ICOs have different degrees of appreciation immediately after ICO. The average ICO is under priced by 8.2% [6], while some tokens appreciated by more than 1000% [9]. Another commonly used mechanism is the Dutch auction, which offers a much better price discovery process. It starts the auction with a high price, which keeps decreasing until enough participants are willing to purchase all coins according to the market price. The Dutch auction also has its drawbacks. E.g., it requires the participants actively monitor the auction progress (lasting for weeks for some ICOs).

For both the fixed price mechanism (with capped number of tokens) and the Dutch auction, whales (large investors) can end the auction early by putting in large investments, which takes away the investment opportunities from the smaller investors. Wealth inequality is a significant problem in the cryptocurrency community, which goes against the principle of decentralization, especially if the coin is based on proof-of-stake (that favors richer holders). It is also worth mentioning that the tokens sold in an ICO normally amount to no more than 50% of the tokens. The unsold tokens are still in the hands of the release team. The hidden danger of sharp depreciation (dumping large amounts of coins) caused by whales is a vital threat for the development team.

Roubini [8] testified in a hearing of the US Senate Committee on Banking, Housing and Community Affairs: *wealth in crypto-land is more concentrated than in North Korea where the inequality Gini coefficient is 0.86 (it is 0.41 in the quite unequal US): the Gini coefficient for Bitcoin is an astonishing 0.88*. Many cryptocurrency buyers expressed dissatisfaction to the wealth gap on Internet forums, calling "whale-sale completely against the ethos of Ethereum and Cryptocurrency" [12]. We collected the data from a few ICOs. Based on our calculation, the Gini index of token allocation in most of the ICOs is higher than 0.88. For example, for Gnosis (with a Gini index of 0.92), the top 5% of the users invested 78%. In sharp contrast, the bottom 64% of the users invested only 4% in total! The top two investors invested 31% and 15%, respectively.

As a means of balance, in this paper, we introduce a Gini index based ICO mechanism to achieve a more balanced token allocation by limiting whales. Since Corrado Gini proposed the concept of Gini index for the first time in 1912, Gini index has been widely used to measure wealth gap. Gini index was also studied recently in mechanism design [11]. The authors used Gini index in simulations to evaluate allocation fairness. In our paper, the Gini index is a mechanism design constraint. Our analysis is based on the specific mathematical structure of the Gini index.

The Gini index may not be meaningful in environments where false name bids [13] are possible, as a whale may simply divide her investment and participate via multiple accounts. Existing ICOs in practise do often involve the *Know Your Customer (KYC)* process and only the users in the *whitelist* can join the ICO. KYC is a process in which a business verifies its customers’ identities, as well as the risk of illegal intent. KYC processes are also being used to comply with anti-bribery and other regulations (e.g., it is illegal to sell cryptocurrencies to customers from countries/territories where cryptocurrencies are banned). The US Securities and Exchange Commission (SEC) has announced the intent to legally require ICOs to have proper KYC processes.

In this paper, we aim to allocate fairly. Another way to achieve fairness is via redistribution. [4] studied the allocation of indivisible goods between a group of unit demand sellers and a group of unit demand buyers. The authors proposed a few ideas of achieving fairness, such as lump sum to the poorer agents from the richer agents, and rationing (i.e.,
raising the minimum selling price to prevent the price competition among the sellers). In our model, similar ideas could be achieved by, for example, requiring the agents who buy more coins to pay higher unit prices, and the extra charges go to the poorer agents. As [4] mentioned, price control is threatened by aftermarket. For our setting, the cryptocurrencies are meant to be currencies, so it is difficult to set different “exchange rates” for different levels of demand. The richer investors can always purchase from the aftermarket after the end of the ICO, which easily avoids any surcharges.

Our Gini mechanism has a list of desirable properties:

- It is a simple prior-free mechanism with an elegant explainable description. Being explainable is necessary for practical applications, as well as being prior-free. Data related to ICO events are extremely volatile. It is unrealistic to assume a known prior distribution. Therefore, computational approaches that are based on prior distributions (e.g., deep learning mechanism design [3, 10] and classic automated mechanism design [2]) are not feasible.
- The Gini mechanism offers a price discovery process. Before an ICO starts, the agents have no idea whether the coin is valuable or is a complete bust, because the value of a cryptocurrency depends heavily on its popularity. We believe any mechanism that asks for agents’ valuations is not realistic for ICOs. We have to step out of the comfort zone of classic allocation mechanism design, where typically we assume the mechanism makes decisions based on the agents’ valuations. Our Gini mechanism only asks for the agents’ budgets (i.e., how much do you plan to invest—most existing ICO mechanisms are like this). Based on the budgets, the mechanism calculates a price. The Gini mechanism has the property that it produces higher prices if there are higher budgets and more agents. That is, the more popular the coin is, the higher the price gets.
- For most agents, (e.g., about 99% of the agents according to our experiments), the strategies are straightforward. They either truthfully reveal their maximum budgets or not join the ICO (by reporting 0s as budgets). Only a handful of agents have room for calculated equilibrium behaviors—they face the situations where investing too much results in a price that is too high, while investing too little results in little utility gain. However, the existence of agents with non-straight-forward strategies is not a flaw of our mechanism, as we show that if we require all agents have straight-forward strategies, then well-performing mechanisms do not exist.
- The mechanism produces nearly optimal revenue in experiments. In terms of theoretical guarantee, asymptotically (when the number of agents goes to infinity), under natural technical assumptions, the mechanism’s revenue converges to the optimal revenue.

2 Model description

The unit size of digital currencies tend to be tiny. For example, satoshi is the name for the smallest unit of bitcoin, which equals one hundred millionth of a bitcoin. In our model, we treat coins as infinitely divisible, which allows us to normalize the number of coins to 1. That is, we are selling one divisible item (one coin) to n agents. For presentation purposes, we say that agent i receives ai coin (0 ≤ ai ≤ 1) if she receives ai fraction of the
coin. Agent $i$’s type is denoted as $(v_i, b_i)$, where $v_i$ is her valuation for the coin\(^1\) and $b_i$ is her budget. For now, we defer any discussion on the difference between an agent’s private true budget limit and her reported budget limit. We will discuss the agents’ strategies in Sect. 4.

Since we are selling currencies, we believe all agents should face the same exchange rate. In an ICO mechanism, the agents would pay monetary payments (e.g., USD or other cryptocurrencies like Ether) in exchange of a fraction of the coin. Let $i$ and $j$ be two agents, each receiving $a_i$ and $a_j$ coin ($a_i, a_j > 0$), and each paying $c_i$ and $c_j$. We should have $\frac{a_i}{c_i} = \frac{a_j}{c_j}$.

This exchange ratio can also be interpreted as the price of the coin. Essentially, we require that our mechanism offers the same price $p$ to all agents. If we charge $c$ from an agent, then this agent should receive $\frac{c}{p}$ coin.

For agent $i$, having a budget of $b_i$ does not necessarily mean that the mechanism will charge her exactly $b_i$. Let $c_i$ be agent $i$’s actual spending under the mechanism. The budget constraint is $0 \leq c_i \leq b_i$. Agent $i$ receives $c_i p$ coin and her utility equals $c_i p (v_i - p)$. The agents aim to maximize their utilities.

A mechanism outputs the price $p$ and an allocation $(a_1, a_2, \ldots, a_n)$. $a_i \geq 0$ for all $i$ and $\sum a_i = 1$. An allocation is feasible only if it honours the budget constraint: $a_i p \leq b_i$ for all $i$.

We introduce a new mechanism design constraint to limit the degree of inequality in our allocations, based on the popular Gini index. The mechanism designer chooses a constant Gini cap $g$ on the final allocation’s Gini index, where $g$ is a mechanism parameter ($0 < g < 1$). That is, a feasible allocation’s Gini index should never exceed $g$. A higher Gini cap implies that we have a higher tolerance on allocation inequality. The standard way to compute the Gini index is as follows. Let $(a_1, a_2, \ldots, a_n)$ be the allocation. We sort the $a_i$ in ascending order to obtain the $y_i$. So $y_1$ is the smallest value among the $a_i$ and $y_n$ is the largest value among the $a_i$. The Gini index equals

\[
\frac{2 \sum_{i=1}^{n} i y_i}{n \sum_{i=1}^{n} y_i} - \frac{n + 1}{n} = \frac{2 \sum_{i=1}^{n} i y_i}{n \sum_{i=1}^{n} y_i} - \frac{n + 1}{n}
\]

However, there is one issue with the above definition. The whole point of considering the Gini index is to ensure allocation equality. Generally speaking, we want to avoid situations where some agents receive too little while some other agents receive too much. If an agent has a huge budget, to prevent her from receiving too much, the mechanism can simply set an investment cap. That is, any investment beyond the cap is not accepted. On the other hand, if an agent has a tiny budget, to prevent her from receiving too little, we have to reduce the price to accommodate her tiny budget, which may significantly reduce the mechanism revenue.

Let us consider an extreme example with $g = 0.5$ and $n = 100$. Let us assume that 75 agents have 0 budgets and the remaining 25 agents have unlimited budgets. In this case, there are no feasible allocations. All allocations’ Gini indices exceed 0.5. To show this, we note that $y_1 = y_2 = \ldots = y_{75} = 0$, so the Gini coefficient becomes

\[
\frac{2 \sum_{i=76}^{100} i y_i}{100 \sum_{i=76}^{100} y_i} - \frac{101}{100} \geq \frac{2 \cdot 76}{100} - 1.01 = 0.51
\]

\(^1\) If the whole coin reserve is released via the ICO mechanism, then an agent’s valuation is essentially her view of the market cap.
Actually, for any constant $g < 1$, we can find type profiles that make it impossible to allocate (to meet the Gini cap). We do not wish to simply fail the ICO in these scenarios. Instead, we allow the mechanism to *ignore agents who receive nothing from the Gini index calculation*. For the above example, if we ignore all 75 agents who receive nothing, then feasible allocation is possible. For the remaining 25 agents, we could simply allocate every agent an equal share ($a_i = \frac{1}{25}$). Equal sharing has a Gini index of 0. Therefore, ignoring agents saves us from infeasible situations. There are two arguments for the flexibility of ignoring agents who receive nothing:

- We are not considering all 7 billion people when calculating the Gini index anyway. People who have not joined the ICO are not fundamentally different from agents who receive nothing in the ICO.
- We are able to achieve much higher revenue under this assumption. We can construct example situations where *one tiny-budget agent* becomes the revenue bottleneck. By not allocating anything to this agent and not including her in the Gini index calculation, we can increase the revenue by infinite many times.

Based on the above reasoning, in this paper, we calculate the Gini index as follows:

**Definition 1 (Flexible Gini Index)** We allow the mechanism to pick the number of winners $k$ from a set $K$. $K$ includes all the allowed winner numbers.

The $n - k$ non-winners all receive nothing, and they are not included in the Gini index calculation.

Let $(a_1, a_2, \ldots, a_k)$ be the allocation for the $k$ winners. We still have that $\sum_{i=1}^k a_i = 1$ and $a_i \geq 0$. We sort the $a_i$ in ascending order to obtain the $y_i$. So $y_1$ is the smallest value among the $a_i$ and $y_k$ is the largest value among the $a_i$. The Gini index for $k$ winners is defined as:

$$
\frac{2 \sum_{i=1}^k iy_i}{k \sum_{i=1}^k y_i} - \frac{k + 1}{k}
$$

(1)

Here are a few example setups for $K$:

- $K = \{n\}$: No agents can be ignored. We fall back to the standard Gini index definition.
- $K = \{\lfloor 0.5n \rfloor, \lfloor 0.6n \rfloor, \lfloor 0.7n \rfloor, \lfloor 0.8n \rfloor, \lfloor 0.9n \rfloor, n\}$: The mechanism can ignore 50%, 40%, …, 0% of the agents.
- $K = \{\lfloor 0.5n \rfloor, \lfloor 0.5n \rfloor + 1, \ldots, n\}$: The mechanism picks at least a half of the agents as winners.

$K$ is also the mechanism’s parameter(s). $\min(K)$ is the minimum number of winners. We should not allow the mechanism to pick too few winners. Having only one winner leads to a very nice Gini index—it is always 0, but it is also meaningless. In our experiments, our setup up is that at least a half of the agents are winners.

The set of feasible allocations is determined by the allowed winner numbers $K$, the Gini cap $g$, the price $p$, and finally the agents’ budgets. If we increase the price $p$, then every agent’s allocation upper limit is reduced. Therefore, the set of feasible allocations either stays the same or shrinks as we increase the price. The total revenue of a mechanism is exactly the price. Therefore, to maximize revenue, a natural idea is to push
up the price to the point so that any further price increment makes feasible allocation impossible. We propose the Gini mechanism based on exactly this idea.

**Informal description of the Gini mechanism** The Gini mechanism does not ask for the agents’ valuations at all. The mechanism produces a price based on the agents’ budgets alone. We start with an infinitesimally small price and raise the price until any further price increment results in no feasible allocations. At the final price, the feasible allocation is unique subject to tie-breaking.

### 3 Formal mechanism description

We start with a procedure that will be used as a building block of the Gini mechanism. The procedure answers the following question: given the agents' budgets (the $b_i$), given the price $p$ and the number of winners $k$, what is the allocation that minimizes the Gini index?

In the context of the above question, we do not have a Gini cap. Instead, we search for an allocation that minimizes the Gini index. An allocation $(a_1, a_2, \ldots, a_n)$ is feasible if it satisfies the following:

- $a_i \geq 0$ and $\sum a_i = 1$.
- $a_i p \leq b_i$. $a_i p$ is agent $i$’s spending and $b_i$ is the budget limit. If $a_i p = b_i$, then we say this agent is maxed out.
- At least $n - k$ elements of the $a_i$ are 0s.

Without loss of generality, we assume $0 \leq b_1 \leq b_2 \leq \ldots \leq b_n$. Let $(a_1^*, a_2^*, \ldots, a_n^*)$ be the feasible allocation that minimizes the Gini index. We first notice that it is without loss of generality to assume $0 \leq a_1^* \leq a_2^* \leq \ldots \leq a_n^*$. The reason is that if we have $i < j$ and $a_i^* > a_j^*$, then swapping $a_i^*$ and $a_j^*$ results in a feasible allocation with the same Gini index. This also means that we can set $a_1$ to $a_{n-k}$ to 0s as we have only $k$ winners.

We then consider only the winners (agent $n - k + 1$ to $n$). If agent $i$ is not maxed out ($a_i^* p < b_i$), then agent $i + 1$ must receive the same allocation amount (i.e., $a_{i+1}^* = a_i^*$). For if it is not, we could increase $a_i^*$ by a small $\varepsilon$ (still affordable by $i$) and decrease $a_{i+1}^*$ by the same $\varepsilon$ (ensuring that we still have $a_i^* \leq a_{i+1}^*$). We end up with a feasible allocation with a strictly smaller Gini index.

Furthermore, among the $k$ winners, let $t$ be the agent that is not maxed out with the smallest index $t$. Agent $t + 1$ must have the same allocation amount as $t$. This implies that $t + 1$ is also not maxed out, which implies that agent $t + 2$ should also have the same allocation. That is, the only allocation structure we need to consider is

$$
\left(0, 0, \ldots, 0, \underbrace{\frac{b_{n-k+1}}{p}, \frac{b_{n-k+2}}{p}, \ldots, \frac{b_{t-1}}{p}}_{n-k}, C, C, \ldots, C\right)
$$

In this allocation, we refer to $C$ as the allocation cap. $n - t + 1$ is the number of capped agents.

By definition of $C$, we have $\frac{b_{t-1}}{p} < C \leq \frac{b_{t}}{p}$, so the above structure can be rewritten into

\[ \left(0, 0, \ldots, 0, \frac{b_{n-k+1}}{p}, \frac{b_{n-k+2}}{p}, \ldots, \frac{b_{t-2}}{p}, C, C, \ldots, C\right) \]
The total allocation must be 1, hence \( C \) must satisfy the following equation:

\[
(0, 0, \ldots, 0, \min_{n-k} \left\{ \frac{b_{n-k+1}}{p}, C \right\}, \min_{n-k} \left\{ \frac{b_{n-k+2}}{p}, C \right\}, \ldots, \min_{n-k} \left\{ \frac{b_n}{p}, C \right\})
\]  

(2)

The only constraint on \( C \) is that it serves as a cap, so \( 0 < C \leq \frac{b_n}{p} \). The left side of Eq. (3) is strictly increasing in \( C \). The only way Eq. (3) does not have a solution is when \( C \) has already reached \( \frac{b_n}{p} \) but the left side is still less than 1.

\[
\sum_{i=n-k+1}^{n} \min \left\{ \frac{b_i}{p}, C \right\} = 1
\]

(3)

If this happens, then we do not have any feasible allocations. For convenience, we define the minimum Gini index to be 1 for this case (1 indicates that this allocation violates the Gini cap). When Eq. (3) has solutions, the solution is unique. By solving for \( C \), we can find the allocation that minimizes the Gini index, based on Expression (2). The optimal (Gini-index-minimizing) allocation is unique subject to a consistent tie-breaking rule. The allocation essentially does not allocate to the lowest \( n - k \) agents (in terms of budgets). This is the only place where we need tie-breaking. We may simply break ties by favoring agent \( i \) over agent \( j \) if \( i > j \). The optimal allocation then sets an allocation cap \( C \). All agents below \( C \) max out their budgets and all agents at least \( C \) can only get \( C \).

Let us then consider the relationship between \( p \) and the minimum Gini index, while fixing the agents’ budgets and the winner number \( k \). We define \( g^*(p) \) to be the minimum Gini index for price \( p \).

**Proposition 1** When \( 0 < p \leq kb_{n-k+1} \), \( g^*(p) = 0 \).

*Interpretation* Our mechanism starts with an infinitesimally small initial price. At that price, feasible allocations exist if at least \( k \) agents have positive budgets.\(^2\)

**Proof** When \( 0 < p \leq kb_{n-k+1} \), we set \( C = \frac{1}{k} \) and Eq. (3) is satisfied and every winner receives the same allocation \( \frac{1}{k} \), which corresponds to a Gini index of 0.

**Proposition 2** When \( p > \sum_{i=n-k+1}^{n} b_i \), \( g^*(p) = 1 \).

*Interpretation* We cannot increase the price infinitely. At some point, no feasible allocations exist.

**Proof** This is based on Inequality (4).

\(^2\) Even if less than \( k \) agents have positive budgets, we may still be able to find an infinitesimally small price that makes feasible allocation possible. If feasible allocation does not exist even with infinitesimally small price, then our mechanism fails. In this case, the mechanism designer should consider raising the Gini cap.
Proposition 3 As we increase $p$ in $(0, \sum_{i=n-k+1}^{n} b_i]$, $g^*(p)$ is continuously nondecreasing in $p$.

Interpretation The minimum Gini index is continuously nondecreasing in the price. As we increase the price, at some point, any further price increment results in a minimum Gini index that is strictly above the Gini cap.

Proof As we increase $p$, every agent’s allocation upper limit ($b_i/p$) is decreased. So the set of allowed allocations either stays the same or shrinks. Therefore, the minimum Gini index is nondecreasing with the price. Based on Eq. (3), the cap $C$ is continuous in $p$. The allocation with minimum Gini index (Expression (2)) changes continuously in $p$. So the Gini index changes continuously in $p$.

Combining all propositions, we have the following theorem:

Theorem 1 Fixing the agents’ budgets and the number of winners $k$, we define the maximum price $p^*$ to be the maximum price where the minimum Gini index is at most the Gini cap $g$. At price $p^*$, there are feasible allocations. Any increment in $p^*$ results in no feasible allocations.

$p^*$ exists. At price $p^*$, the corresponding feasible allocation is unique subject to tie-breaking.

Proof Based on Proposition 2, if the minimum Gini index at $p = \sum_{i=n-k+1}^{n} b_i$ is at most $g$, then this is the maximum price. Any higher price results in a Gini index of 1. At this price, the only feasible allocation is that the lowest $n - k$ agents in terms of budgets do not receive anything and the highest $k$ agents all max out.

We then consider situations where the minimum Gini index at $p = \sum_{i=n-k+1}^{n} b_i$ is strictly higher than $g$. When $p = kb_{n-k+1}$, the minimum Gini index is 0, so $p^* \in [kb_{n-k+1}, \sum_{i=n-k+1}^{n} b_i]$. Let $S = \{p | g^*(p) = g, p \in [kb_{n-k+1}, \sum_{i=n-k+1}^{n} b_i]\}$. Given that $g^*(p)$ is continuously nondecreasing based on Proposition 3, $S$ contains either one point, or $S$ is a closed interval. In both cases, $p^* = \max S$ exists. At price $p^*$, the only feasible allocations are the Gini-index-minimizing allocations, which are unique subject to tie-breaking. If an allocation is not Gini minimizing and is feasible, then the minimum Gini index must be strictly below $g$, which means that the price can still be pushed up due to the continuity between the price and the minimum Gini index.

Next, we formally define the Gini mechanism.

Definition 2 (Gini mechanism) $g$ and $K$ are mechanism parameters. Given the agents’ budgets, for every allowed winner number $k \in K$, we find the maximum price $p^*_k$ where the minimum Gini index is at most the Gini cap $g$. We then choose the price to be the overall maximum $\max_{k \in K} p^*_k$. If there are multiple $k$ values with the same overall maximum price, then we break ties by favoring more winning agents. We pick the unique feasible allocation corresponding to the price.

Given $k$, the optimal $p^*_k$ can be calculated via a binary search inside the interval $[kb_{n-k+1}, \sum_{i=n-k+1}^{n} b_i]$. The lower and upper bounds on the $p^*_k$ are from Propositions 1 and 2, respectively. Proposition 3 establishes the monotone relationship between $p^*_k$ and
the corresponding minimum Gini index. Let \( mid \) be the middle point of the above interval. We calculate the minimum Gini index when the coin price is \( mid \). If the minimum Gini index for price \( mid \) does not meet the Gini cap, then \( mid \) becomes the new upper bound on \( p_k^* \). Otherwise, \( mid \) becomes the new lower bound. We end the searching process when the upper bound and the lower bound is within a small \( \delta \) and set \( p_k^* \) to be the lower bound. In practise, the price we calculated is at most \( \delta \) away from the highest possible price that still meets the Gini cap. For the coin issuer, this is negligible as long as \( \delta \) is small enough.

Later in this paper, we will see that under our mechanism, for most agents, the strategy is straight-forward. For most agents, as long as there is a tiny gap between the agent’s valuation and the coin price, then the decision is trivial: report the full budget if the valuation is higher than the coin price, or report 0 otherwise. A tiny \( \delta \) will not swing the decisions of many agents. We will also show that an individual agent’s influence on the final coin price is very limited. In summary, our mechanism’s performance is not sensitive to numerical errors on the coin price.

It should be noted that the optimal number of winners depends on the agents’ budgets. Sometimes, having a high number of winners leads to a high coin price. For example, if all agents have the same budget \( b \), then we want as many agents to join in as possible. Let \( k \) be the number of winners. A Gini index of 0 can be trivially achieved by allocating every winner \( \frac{1}{k} \) proportion of the coin. The final coin price is \( kb \), which increases in \( k \). If the agents’ budgets are uneven, then sometimes we have to exclude some agents in order to meet the Gini cap. In these cases, having a smaller number of winners leads to a higher coin price.

### 4 Equilibrium under the Gini mechanism

In this section, we start the discussion on the agents’ strategies. The way we would implement the Gini mechanism in practise is as follows: We announce a time frame for the ICO. During the time frame, the agents can join/leave anytime, and can change their investment amounts (budgets) anytime. (Technically, joining and leaving are special cases of changing budgets.) The Gini mechanism maintains the current coin price and allocation throughout the time frame. We assume that the time frame is long enough so that at some point, after all interested agents have joined, an equilibrium on the budgets are to be reached.\(^4\) The equilibrium price/allocation eventually become the final coin price/allocation.

Our discussion involves three closely related concepts:

- We use \( b_i^M \) to denote agent \( i \)’s true maximum budget. This is \( i \)’s private information.
- We use \( b_i \) to denote agent \( i \)’s reported budget. Agent \( i \) can report arbitrary nonnegative budget, including reporting a value above \( b_i^M \).
- We use \( c_i \) to denote agent \( i \)’s spending. The spending is always at most the reported budget. That is, \( 0 \leq c_i \leq b_i \).

---

3 Given the coin price, according to Eq. \( (3) \), the cap \( C \) can be found in linear time (i.e., by finding the \( i \) index value that makes \( b_i \leq C \leq b_{i+1} \)). Once \( C \) is obtained, the minimum Gini value can be solved for in linear time. That is, every binary search step takes linear time only.

4 In practise, most ICOs are conducted over the Ethereum network. Here, an equilibrium will always be reached due to the transaction fees. In this paper, we do not consider transaction fees. Instead, we show that an approximate equilibrium does exist.

Springer
We use $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ to denote the current budget profile. We can also call this the agents' current strategies. We still assume that $0 \leq b_1 \leq b_2 \leq \ldots \leq b_n$. For every winner number $k \in K$, we use $p_k^*(\mathbf{b})$ to denote the maximum price for $k$ winners and budget profile $\mathbf{b}$. The Gini mechanism’s price (the coin price) $p^*(\mathbf{b})$ for budget profile $\mathbf{b}$ is the maximum over the $p_k^*(\mathbf{b})$ for $k \in K$.

Now we introduce a few technical propositions, which will be used for analyzing agents’ strategies.

**Proposition 4** For any $k$, $p_k^*(\mathbf{b})$ is nondecreasing in every coordinate (every $b_i$). This also means that $p^*(\mathbf{b})$ is nondecreasing in every coordinate, because the maximum of monotone functions are still monotone.

**Interpretation** For every agent, raising her budget will not decrease the coin price.

**Proof** When we increase agent $i$'s budget $b_i$, feasible allocations remain feasible allocations. If previously we can push the price to a certain point, then we still can (and may be able to push the price up even more).

**Proposition 5** For any $k$, $p_k^*(\mathbf{b})$ is continuous in every coordinate (every $b_i$). This also means that $p^*(\mathbf{b})$ is continuous in every coordinate, because the maximum of continuous functions are still continuous.

**Interpretation** For every agent, the coin price changes continuously with her budget.

**Proof** We focus on a specific $k$. If we change $b_i$ to $\alpha b_i$ for every $i$, then the maximum price also changes by $\alpha$ times (to offset the change in budgets). Let $p$ be the maximum price. For an arbitrary $\epsilon > 0$, to change the price from $p$ to $p + \epsilon$, we can increase every $b_i$ to $b_i \frac{p + \epsilon}{p}$. This also means that for a specific $i$, if the increment in $b_i$ is at most $b_i \frac{p + \epsilon}{p} - b_i$, and we do not change the other coordinates (this means less increment in price because the price is monotone in every coordinate), then the price increment is at most $\epsilon$. The same argument works for decrement.

**Proposition 6** Agent $i$ faces a minimum investment amount $b_{\text{min}}(\mathbf{b}_{-i})$ and a maximum investment cap $b_{\text{max}}(\mathbf{b}_{-i})$. Both are determined by the other agents’ budgets (i.e., $\mathbf{b}_{-i}$). Agent $i$’s spending is 0 when her budget is below $b_{\text{min}}(\mathbf{b}_{-i})$ and her spending stays at $b_{\text{max}}(\mathbf{b}_{-i})$ when her budget grows beyond the cap. In between the minimum and the maximum investment amounts, the price $p^*$ strictly increases in $i$’s reported budget.

**Interpretation** An agent’s budget needs to reach a minimum amount to become a winner. She can drive up the coin price by offering more than the minimum. However, there is also a maximum investment amount. Any budget above that has no impact on the coin price.

**Proof** We raise $i$’s budget from 0. At some point when her budget reaches $b$, for the first time she becomes a winner under the Gini mechanism. Due to tie-breaking, it could be that $i$’s budget must be strictly above $b$ for her to become a winner. We ignore this technicality. Once $i$ becomes a winner. That means at the current price, $i$ is a winner in at least one feasible allocation. Let the set of feasible allocations where $i$ is a winner be $S_i$. If $i$ is not
capped in at least one allocation in $S_i$, then by increasing $i$’s budget, the cap of this allocation decreases at the current price, which leads to strictly smaller Gini index. This then means the overall price $p^*$ should strictly increase as a result. If $i$ is capped in all feasible allocations in $S_i$, then any increment in $i$’s budget has no effect anywhere, this means that $i$ has already reached her maximum investment cap.

\[ k = \left( \sum_i \left\lfloor \frac{b_i}{p^*_k} \right\rfloor \right) > 0. \]

much as possible (by reporting the true maximum budget) or not buy at all (by reporting $b^*$). As a result, for most agents, the strategies are simple. As the valuations are not very close to the coin price, the optimal strategy is to buy as long as the prices are bounded above by a constant. We will later on use this to show that most agents’ impact allocations in $S_i$ will only change the agents’ utilities infinitesimally. We focus on a specific winner to remove ties. We have shown that the price function is continuous, so perturbing the budgets infinitesimally if the budget profile contains ties, then we can simply perturb the budgets infinitesimally. We consider the Gini index, which makes the allocation infeasible. If no agents is capped, then $b_i/p^*_k(b) = b_i/\sum_{j=n-k+1}^n b_j$, which is also nondecreasing in $b_i$.

Proposition 7 For any $k$ and $i$, $b_i/p^*_k(b)$ is nondecreasing in $b_i$. This also means that $b_i/p^*_k(b)$ is nondecreasing in $b_i$, because the minimum of monotone functions are still monotone.

Interpretation For every agent, higher budget leads to equal or more coin won.

Proof If $b_i$ is small and $i$ is not a winner, then increasing $b_i$ has no effect on the price. If $b_i$ is large and $i$ is capped, then again, the increment in $b_i$ has no effect on the price. When price stays the same, $b_i/p^*_k(b)$ is nondecreasing in $b_i$. When $b_i$ is a winner and not capped, when increasing $b_i$, the price gets strictly higher. If $i$’s allocation $b_i/p^*_k(b)$ decreases, then all uncapped agents’ allocations decrease. If any agent is capped, then the cap increases. This results in strictly higher Gini index, which makes the allocation infeasible. If no agents is capped, then $b_i/p^*_k(b) = b_i/\sum_{j=n-k+1}^n b_j$, which is also nondecreasing in $b_i$.

Proposition 8 Assuming $0 < b_1 < b_2 < \ldots < b_n$, for any $i$,

\[
\frac{\partial p^*_k(b)}{\partial b_i} \leq \frac{g + 3}{1 - g}.
\]

This also means that the partial derivative of $p^*(b)$ against $b_i$ is bounded above by $\frac{g + 3}{1 - g}$.

Interpretation The partial derivative between the coin price and an agent’s budget is bounded above by a constant. We will later on use this to show that most agents’ impact on the coin price is very limited. As a result, for most agents, the strategies are simple. As long as the valuations are not very close to the coin price, the optimal strategy is to buy as much as possible (by reporting the true maximum budget) or not buy at all (by reporting 0).

Proof We focus on budget profiles without ties for convenience. In an actual equilibrium, if the budget profile contains ties, then we can simply perturb the budgets infinitesimally to remove ties. We have shown that the price function is continuous, so perturbing the budgets will only change the agents’ utilities infinitesimally. We focus on a specific winner number $k$ and a specific budget profile $(b_1, b_2, \ldots, b_n)$ with $0 < b_1 < b_2 < \ldots < b_n$.

Let $z = \left[ (n - k) + \frac{1}{2} (g + \frac{g + 1}{k}) \right]$. Let us analyze the derivative with respect to $b_i$ when $i > z$. If $b_i$ is already capped under this budget profile, then the derivative is 0. So we only need to consider the situation where $b_i$ is not capped. We reduce $b_i$ to $b_i - \epsilon$ and change the price from $p^*$ to $p^* - \epsilon$. We consider a new allocation where every other agent’s spending stays the same, but $i$’s spending is reduced by $\epsilon$. This is still a feasible allocation but may not meet the Gini cap. We consider the Gini index of the new allocation. Let us consider the definition of the Gini index in (1). For the new allocation, the only change is a reduction in proportion of $y_i$ in both the numerator and the denominator. The numerator is multiplied by $2(i - n + k)$ (the indices are from 1 to $k$ for the $k$ winners in (1)). The denominator is multiplied by $k$. Since $i > z$, we have $i \geq z + 1$ and
We want the first term of (1) to be at most \( g + \frac{k+1}{k} \) to meet the Gini cap. So lowering \( y_i \)'s proportion only helps this goal. This means that the new allocation also meets the Gini cap. So the overall price should be at least \( p - \epsilon \). In conclusion, the derivative is at most 1 when \( i > z \).

We then consider \( i \leq z \). If \( i \leq n - k \), then \( i \) is not a winner and the derivative is 0. We only present the proof for \( i = n - k + 1 \). This is the winner with the lowest budget. This budget has the highest impact on the price. \( b_{n-k+1} \) is not capped, for otherwise the Gini index equals 0. Therefore, we can adjust \( b_{n-k+1} \) both up and down. \( n - k + 1 \)'s spending is the same as her budget.

We first consider the case where \( b_{z+1} \) is not capped. We define a few terms (the \( c_i \) are the actual spendings of the agents):

- \( x' = \sum_{i=z+1}^n (i - n + k)c_i \)
- \( x = \sum_{i=z+1}^n c_i \)
- \( y' = \sum_{i=z+1}^n (i - n + k)c_i \)
- \( y = \sum_{i=z+1}^n c_i \)

The first term of (1) is then \( r = \frac{x' + y'}{x + y} \). When the Gini cap is met, \( r = \frac{k}{2}(g + \frac{k+1}{k}) \). (If the Gini cap is not met, then all \( k \) agents spend all their budgets, in which case any change in budget corresponds to a derivative of at most 1.) We use \( s \) to denote \( x + y \).

We change \( b_{n-k+1} \) to \( b_{n-k+1} + \epsilon \). We consider a new allocation with the following spendings. Agent \( n - k + 1 \)'s spending is increased from \( b_{n-k+1} \) to \( b_{n-k+1} + \epsilon \). Other agents from \( n - k + 2 \) to \( z \) keep their current spendings. The agents from \( z + 1 \) to \( n \) reduce their spendings by a factor of \( \alpha \).

The first term of the Gini index of this new allocation is then \( \frac{x' + \epsilon + \alpha y'}{x + \epsilon + \alpha y} \). We set \( \alpha \) so that this term equals \( r \).

\[
\alpha = \frac{(x - x')\epsilon + (y - y')\epsilon + x'y - xy'}{x'y - xy'} < 1
\]

This implies that the new allocation is still feasible given the above \( \alpha \). Since we assume agent \( z + 1 \) is not capped, there is room for pushing down the spendings of agent \( z + 1 \) to \( n \) by multiplying the original spendings by \( \alpha \). The price corresponding to the new allocation is the denominator of the first term of the Gini index, which is \( x + \epsilon + \alpha y \) (under the Gini mechanism, the price is always equal to the total spending). The derivative of \( x + \epsilon + \alpha y \) against \( \epsilon \) equals

\[
\frac{(x + y)(y' - y)}{xy' - x'y} = 1 + y\frac{r - 1}{y' - ry}
\]

To maximize the derivative, we minimize \( \frac{y' - ry}{y} = \frac{y'}{y} - r \) instead. \( \frac{y'}{y} \) is minimized when all \( b_i \) are the same for \( i \geq z + 1 \). The ratio is minimized to

\[
\frac{(z + 1 - n + k + n)(n - z)}{2(n - z)} = \frac{z + 1 - n + k + n}{2} \geq \frac{r + n}{2}
\]

So \( \frac{y' - ry}{y} \) is minimized to \( \frac{r - \epsilon}{2} \). The derivative is maximized to
\[
1 + \frac{2(r - 1)}{n - r} = 1 + \frac{2k(g + \frac{k+1}{k}) - 4}{2n - k(g + \frac{k+1}{k})} = 1 + \frac{2kg + 2(k + 1) - 4}{2n - kg - (k + 1)}
\]

The above increases with \( k \), but \( k \) is at most \( n \), so the above is maximized to

\[
1 + \frac{2ng + 2(n + 1) - 4}{2n - ng - (n + 1)} = 1 + \frac{(2g + 2)n - 2}{(1 - g)n - 1} = (\frac{g + 3}{1 - g})n - 1
\]

The above expression increases with \( n \). When \( n \) goes to infinity, we have the final upper bound \( \frac{g + 3}{1 - g} \).

When \( z + 1 \) is capped, we consider changing \( b_{n-k+1} \) to \( b_{n-k+1} - \epsilon \) instead. All analysis is almost identical. After the change, \( \alpha > 1 \), but if \( z + 1 \) and future agents are capped, there is room for increasing the spendings.

Given the above propositions, we demonstrate that for most agents, the strategies are fairly simple. We start with a sufficient condition for an agent to report 0 budget.

**Proposition 9** If \( p^*(0, b_{-i}) \geq v_i \), then an agent’s best strategy is to report a budget of 0.

**Interpretation** \( p^*(0, b_{-i}) \) is the minimum coin price agent \( i \) faces. If this is still considered too expensive, then \( i \) will not invest.

Now we provide a sufficient condition for an agent to report her true maximum budget. It is not as simple as, for example, if \( p^*(b_i^M, b_{-i}) \leq v_i \), then an agent would report her actual maximum. For reporting the maximum budget, an agent’s valuation must be slightly higher than the \( p^*(b_i^M, b_{-i}) \). This is to ensure that the utility gain for buying more is always greater than the utility loss caused by price increment for the existing purchase.

**Proposition 10** If \( v_i \geq \frac{p^*(H_i, b_{-i})}{1 - v_i M_{\frac{1}{1-g}}^i(b_{-i})} \), then agent \( i \)’s best strategy is to report her true maximum budget. Here, \( H_i = \min\{b_i^M, b_{\max}(b_{-i})\} \), which represents the highest “effective” budget for agent \( i \). Any higher budget is essentially the same or violates the budget constraint. \( a_i^M \) is \( i \)'s allocation when her budget is \( H_i \).

**Interpretation** If an agent’s valuation is slightly higher than the coin price, then the agent would prefer to report her true maximum budget. In experiments, generally we have that \( p^*(H_i, b_{-i}) \) is very close to \( p^*(b_i, b_{-i}) \). \( a_i^M \) is generally very small for most agents. For example, if there are 3000 agents in total, then we know for sure that at most 1000 agents can get allocations at least 0.1%. That means for the remaining 2000 agents, we have \( a_i^M \leq 0.001 \). Let us consider \( g = 0.6 \), so \( \frac{g + 3}{1 - g} = 9 \). For an agent among these 2000 agents, if her valuation is at least the coin price, divided by 0.991, then reporting the true maximum budget is the optimal strategy.

**Proof** Due to Proposition 6, agent \( i \) faces a minimum and a maximum investment amount. If her true maximum budget is below the minimum amount, then this agent is irrelevant. We only consider agents who can meet the minimum investment amounts. We use \( u_i(b_i, b_{-i}) \) to denote \( i \)'s utility. Let us analyze the derivative of \( u_i \) against \( b_i \) when \( b_i \) is identical to the spending \( c_i \). That is, we consider \( b_i \) in between the minimum investment amount and \( H_i \).
\[
\frac{u_i(b_i, b_{-i})}{p^*(b_i, b_{-i})} = \frac{b_i}{p^*(b_i, b_{-i})}(v_i - p^*(b_i, b_{-i})) = \frac{v_i b_i}{p^*(b_i, b_{-i})} - b_i
\]

\[
\frac{\partial u_i(b_i, b_{-i})}{\partial b_i} = \frac{p^*(b_i, b_{-i}) v_i}{p^*(b_i, b_{-i})} - \frac{\partial p^*(b_i, b_{-i})}{\partial b_i} \frac{v_i b_i}{p^*(b_i, b_{-i})} - 1
\]

\[
= \frac{v_i}{p^*(b_i, b_{-i})} \left( 1 - \frac{b_i}{p^*(b_i, b_{-i})} \frac{\partial p^*(b_i, b_{-i})}{\partial b_i} \right) - 1
\]

\[
\geq \frac{v_i}{p^*(b_i, b_{-i})} \left( 1 - a_i^M g + \frac{3}{1 - g} \right) - 1 \quad (5)
\]

\[
\geq \frac{v_i}{p^*(H_i, b_{-i})} \left( 1 - a_i^M g + \frac{3}{1 - g} \right) - 1 \quad (6)
\]

In the last two steps, we relied on two facts. One is that due to Proposition 7, \( a_i^M \) is the highest allocation \( i \) can get. The other is that the derivative is bounded according to Proposition 8.

We demonstrated that under the Gini mechanism, most agents have straight-forward strategies: either truthfully report the maximum budget or 0. Unfortunately, under the Gini mechanism, there do exist agents with more complex strategic behaviors. These agents have valuations very close to the coin price, so they need to set their budgets to create a nice balance between price increment and their marginal utility gains.

What if we require all agents have straight-forward strategies? We define “truthful” mechanisms as mechanisms under which all agents always report their maximum budgets if their valuations are above the coin price. Otherwise, they report 0 budgets. It turns out all truthful mechanisms have abysmal performances.

**Proposition 11** We assume the mechanism under consideration is truthful. Let the budget profile be \((b_i, b_{-i})\). Let \( a_i \) be agent \( i \)'s allocation. Let \( p \) be the price determined by the mechanism based on the current budget profile.

We consider another budget profile where agent \( i \) increases her budget to \( b_i' \). Let \( a_i' \) and \( p' \) be the new allocation and new price.

If \( a_i > 0 \), then \( a_i' \geq a_i \) and \( p' \leq p \).

**Proof** When agent \( i \) reports \( b_i \), her utility is \( a_i v_i - p \). When agent \( i \) reports \( b_i' \), her utility is \( a_i' v_i - p' \). Assume that \( a_i' < a_i \). If agent \( i \)'s valuation \( v_i \) is approaching infinity, then \( a_i v_i - p > a_i' v_i - p' \). That is, in this case, when agent \( i \)'s true maximum budget is \( b_i' \), agent \( i \) will under report her budget (by reporting \( b \)) in order to achieve a higher utility, which contradicts with our assumption that the mechanism is truthful. So we must have that \( a_i' \geq a_i \).

We then assume \( p' > p \). Let \( v_i \) be a value in between \( p' \) and \( p \). When agent \( i \)'s true maximum budget is \( b_i' \), her utility is 0 because she cannot afford \( p' \). She could under report by reporting \( b \) in order to receive a positive utility, which contradicts with our assumption that the mechanism is truthful. So we must have \( p' \leq p \).

The above proposition basically says that as a winning agent increases her budget, the price must stays the same or decreases. This is not desirable as we prefer the price to go up.
when the agents invest more. Let us consider a truthful mechanism $M$. Let $p_{\min}$ be the minimum price under $M$ where feasible allocations exist (e.g., at least one agent has positive allocation). Let $b$ be the corresponding budget profile. We can modify the budget profile by picking a winning agent and increase her budget to infinity. The agent must still be a winning agent and the new price must still be $p_{\min}$. We can repeatedly do this until all winning agents have infinite budgets. The final price is still $p_{\min}$. Let $b'$ be the final budget profile. Under the final budget profile, all winning agents have infinite budgets and it is possible to satisfy the Gini constraint by allocating only to these winning agents. This implies that under the Gini mechanism, the coin price should be infinity, which is infinitely times better than $p_{\min}$.

Next, we compare the Gini mechanism’s revenue against the first-best optimal revenue. The first-best optimal revenue is calculated as an optimization problem, assuming that we know all the agents’ private valuations and private budgets. Given a price $p$, we filter out all agents who can afford $p$, and then derive the Gini-index-minimizing allocation based on the true maximum budgets. If the Gini index is at most the Gini cap $g$, then $p$ is an achievable price. We solve for the highest $p$.

**Theorem 2** Under the following assumptions, the Gini mechanism’s equilibrium revenue approaches the first-best optimal revenue with probability 1, as the number of agents goes to infinity.

- The agents’ private valuations are drawn i.i.d. from a distribution with a value upper bound $U$. For any $\epsilon > 0$, $\text{Prob}(v \in (U - \epsilon, U)) > 0$. This basically assumes that the upper bound is a meaningful upper bound, in the sense that there is a positive probability to draw a value close to the upper bound.
- The agents’ private budgets are drawn i.i.d. from a distribution with a positive expectation.
- There is a constant minimum winner number. Above that, all winner numbers are allowed.

**Proof** We find a constant integer $n_0$ so that $\text{Prob}(b \geq U/n_0) > 0$ and $n_0$ is at least the minimum winner number. $n_0$ can always be found. There is a positive probability to draw an agent with valuation above $U - \epsilon$ and budget above $U/n_0$. As the number of agents goes to infinity, the probability of drawing $n_0 + n_1$ such agents equals 1, where $n_1$ is another constant integer. Among these $n_0 + n_1$ agents, for at least $n_0$ of them, the allocation is at most $\frac{1}{n_1}$. (For example, there are at most 1000 agents who allocation is at least $\frac{1}{1000}$.) If the equilibrium price is less than $\frac{U - \epsilon}{\frac{1}{n_1 + \frac{1}{U - \epsilon}}}$, then according to Expression (5), these $n_0$ agents would max out their budgets under the equilibrium. Each of these $n_0$ agents has a budget that is at least $U/n_0$. So at the equilibrium price, only allocating to these agents alone results in an allocation with a Gini index of 0, which means that any equilibrium price strictly lower than $\frac{U - \epsilon}{\frac{1}{n_1 + \frac{1}{U - \epsilon}}}$ is not possible. (If it is lower, then it should be raised due to the existence of an allocation with 0 Gini index.) Given that $\epsilon$ and $n_1$ are arbitrary constants, we have that the equilibrium price can be made arbitrarily close to $U$. $U$ is obviously an upper bound on the first-best optimal revenue. ☐

The theoretical analysis of this section assumes that an agent actually has a specific valuation, even though our mechanism never asks the agents to report these values. Based
on the theoretical analysis, we proved that an agent’s strategy is straight-forward as long as there is a tiny gap between her valuation and the coin price. Specifically, an agent will report her maximum budget if her valuation is above the coin price and otherwise she will report 0. For agents whose valuations are very close to the coin price, they may benefit by strategic reporting. We showed that an individual agent’s influence on the final coin price is very limited, so as long as the number of agents do not have straight-forward strategies is small, the equilibrium coin price will be close to the coin price assuming all agents are truthful. In practise, agents may not have specific valuations. But still, we believe many agents’ strategies remain to be straight-forward. For example, an agent may have a vague feeling of how much the coin is worth. An example thought process is the following: “I think this coin is similar to another coin who just raised 10 millions, so a vague assessment is that this coin’s value is somewhat close to 10 millions”. If the current coin price is 7 millions, then the straight-forward strategy is to invest by reporting the full budget. Similarly, if the current coin price is 15 millions, then the straight-forward strategy is not to invest and report 0. Essentially, an agent still has straight-forward strategies as long as there is a gap between her valuation and the coin price. It is just that in practise, the gap is much larger. Even though our model cannot perfectly describe practise, we still feel that it is better than classic mechanism design models where we ask the agents to report valuations.

5 Experiments

In this section, we evaluate the Gini mechanism using real ICO data. Our dataset is compiled based on previous Dutch auction based ICOs. Each ICO dataset contains the agents’ budgets and their entering prices to the Dutch auction. In an ICO Dutch auction, even if an agent enters early, she still pays according to the ending price. So for agents with small budgets (who cannot buy all the coins and stop the auction), entering the auction when the price meets the valuation is a reasonable strategy. For this reason, we use the entering prices as the agents’ valuations. In our experiments, we also included a list of generated bids. The reason for this is that there are many observing agents whose data are missing from our datasets. An observing agent is someone who has low valuation. The auction ended before such an agent logs her bid. If the dataset contains \( n \) agents, then we add in another \( n \) generated agents. The generated agents’ budgets are sampled from real budgets, and the valuations are just the ending price times a random value from 0 to 1 (drawn according to the uniform distribution).

We numerically compute an approximate Nash equilibrium. We first calculate the first-best optimal price and use it to initialize the budget profile. An agent reports the true maximum budget if her valuation is at least the first-best optimal price, and reports 0 otherwise. From this point on, we go through the agents one-by-one and have each agent update the budget to her best response. We stop when an equilibrium has been reached.

Our experiments involve thousands of agents, which seems very daunting when it comes to equilibrium computation. Fortunately, with the help of Propositions 9 and 10, we test these two sufficient conditions and find that most agents either report the maximum budget or 0.

\footnote{Our dataset and code can be found at: https://github.com/mingyuguo/gini_index_based_initial_coin_offering_mechanism.}
For a handful of agents who do prefer to report a budget that is somewhat in between 0s and their maximum budgets, we use numerical simulation to calculate their best responses. We focus on a specific agent \( i \). Figure 1 (Left) shows \( i \)'s real allocation curve. When \( i \)'s budget is below a minimum investment amount (denoted as \( B_{\text{min}} \) in the figure), her allocation is 0. When \( i \)'s budget grows above a maximum amount (denoted as \( B_{\text{max}} \) in the figure), her allocation stays the same. In between, her allocation curve is approximately concave: by investing more, \( i \) pushes up the price, so the marginal gain gets smaller and smaller. The real allocation curve is unknown to us, so we resort to its approximation in our equilibrium calculation. We use piecewise straight lines to approximate the real allocation curve, by sampling a few allocation values and then connect them together. We call the sampled points the turning points in our piecewise linear curve. To ensure that we end up with a concave curve, we use a linear program to move the turning points slightly up or down. For example, let the \( y_i \) be the y-coordinates of the turning points (\( y_0 = 0 \)). The linear program is constructed as follows (the \( y_i \) are constants and the variables are the \( y_i' \)):

\[
\begin{align*}
\min & \quad \delta \\
\text{s.t.} & \quad y_i - \delta \leq y_i' \leq y_i + \delta \\
& \quad y_i'_{i+1} + y_i'_{i-1} \leq 2y_i' \\
& \quad y_i' \leq y_i'_{i+1} \\
& \quad y_0' = 0
\end{align*}
\]

(7)

It should be noted that in our approximation, we used a non-horizontal straight line in between 0 and \( B_{\text{min}} \). This is fine because both before or after the approximation, the agents’ best strategies do not involve any budget strictly in between 0 and \( B_{\text{min}} \).

With a concave allocation curve, the agent’s utility function is also concave. For example, when the budget is in between \( B_{\text{min}} \) and \( B_{\text{max}} \), the utility curve is just the allocation curve times a constant (the agent’s valuation), then subtracts a linear term (the payment). According to [7], for a \( n \)-person game with concave utility function, a pure strategy Nash equilibrium always exist. Our experiments show that after the approximation, a pure strategy Nash equilibrium (a deterministic budget profile) is very easy to find.
Our approximation introduces two sources of errors. First, we have the error $\delta$ from the linear program. Then, as shown in Fig. 1 (Right), there is error due to using a straight line to approximate the real curve. Let $BL$ and $BR$ be the x-coordinates of two adjacent turning points. The price at $BL$ is lower than the price at $BR$. For any budget value $B$ in between $BL$ and $BR$, the allocation is in between $B/p(BR)$ and $B/p(BL)$. The gap is at most $B \frac{p(BR) - p(BL)}{p(BL)p(BR)}$, which is maximized when $B$ approaches the larger budget $BR$. We go through every adjacent pair of turning points to get the largest error. Given these two sources of errors, our computed Nash equilibrium is not an exact equilibrium. Suppose when we calculate the best response for agent $i$, the maximum error in terms of $i$’s utility is $\epsilon$, then we can only say this agent’s response is at most $2\epsilon$ away from the best response (we could be underestimating the actual best response and overestimating the approximate best response).

For the five ICOs studied in this section, their original Gini indices are between 0.88 and 0.95.

The experiments are conducted using parameter $g = 0.6$ and

$$K = \{\lceil0.5n\rceil, \lceil0.6n\rceil, \lceil0.7n\rceil, \lceil0.8n\rceil, \lceil0.9n\rceil, n\}$$

Table 1 shows the decomposition of agents for different ICOs. The data format is “total number of agents = agents who report 0 based on Proposition 9 + agents who report the true maximum budget based on Proposition 10 + agents with nontrivial strategies.” As shown in the table, the number of agents with nontrivial strategies are only a handful. Table 2 compares the equilibrium revenue under the Gini mechanism (Gini Rev.) against the first-best optimal revenue (Opt. Rev.).\(^6\) The unit is Ether. Err. represents the maximum utility error. That is, under our equilibrium, an agent’s response may be slightly off from the actual best response, but

---

\(^6\) Gini Rev. is higher than Opt. Rev. for Metronome due to numerical error.
it’s at most 0.145\% away in terms of this agent’s budget in the worst case across all agents. Errors for the other ICOs are significantly better.

Lastly, as described earlier, the revenue numbers mentioned in Table 2 are from mechanisms that consider the Gini index as the fairness constraint. The five ICOs’ real revenue (not considering the fairness constraint and not considering generated bids) are as follows: Raiden 109165, Metronome 30927, Polkadot 204818, GoNetwork 27799, and Gnosis 250014. The unit is again Ether.

6 Conclusion

This paper proposed a mechanism for initial coin offering based on the Gini index. The proposed mechanism is elegant and explainable. The mechanism stepped out of the comfort zone of classic mechanism design, in that our mechanism, due to the nature of ICOs, must make decisions without asking for the agents’ valuations. The mechanism offers a price discovery process where the price of the coin is determined by the coin’s popularity—the agents’ pledged budgets. For most agents, the strategies are straight-forward. The agents either truthfully reveal the maximum budgets or stay out of the auction. The mechanism produces nearly optimal revenue in experiments based on real ICO data, and it is proven to be optimal when the number of agents goes to infinity.

Threats to Validity It should be noted that for practical application purposes, we prefer the mechanism to be as simple as possible and the strategies to be as straight-forward as possible. So the simple nature of our mechanism is not a disadvantage. However, in order to keep our model simple, we did omit a few blockchain specific complications, as listed below.

- We are not considering transactions fees anywhere in our model. ICOs typically are held on Ethereum, where every action costs a small amount of money. Under our mechanism, an agent that does not win still have to pay the transaction fee (for entry). The coin issuer may choose to cover the fees for the agents, but then that means we need to set a minimum budget threshold. Otherwise, a malicious attacker could bankrupt the coin issuer (by keep charging the coin issuer transaction fees). On the other hand, realistically speaking, serious investors most likely will not be deterred by transaction fees.
- Our mechanism allows the agents to remove their budget pledges. This means that the coin issuer could manipulate the market by pledging large amounts earlier on in order to hype up the ICO.

References

1. Buterin, V. (2017). Analyzing token sale models, https://vitalik.ca/general/2017/06/09/sales.html
2. Conitzer, V., & Sandholm, T. (2002). Complexity of mechanism design. In A. Darwiche, & N. Friedman (Eds.), UAI ’02. Proceedings of the 18th conference in uncertainty in artificial intelligence, University of Alberta, Edmonton, Alberta, Canada, Morgan Kaufmann (pp. 103–110).
3. Duetting, P., Feng, Z., Narasimhan, H., Parkes, D., & Ravindranath, S. S. (2019). Optimal auctions through deep learning. In K. Chaudhuri, & R. Salakhutdinov (Eds.), Proceedings of the 36th international conference on machine learning, PMLR, Long Beach, California, USA, Proceedings of Machine Learning Research (Vol. 97, pp. 1706–1715).
4. Dworczak, P., Kominers, S. D., & Akbarpour, M. (2021). Redistribution through markets. In *Econometrica* (Vol. 89, Issue 4).
5. ICObench. (2018). ICO market analysis 2018, https://icobench.com/reports/ICO_Market_Analysis_2018.pdf
6. Momtaz, P. P. (2020). Initial coin offerings. *PLOS ONE, 15*(5), e0233018. https://doi.org/10.1371/journal.pone.0233018.
7. Rosen, J. B. (1965). Existence and uniqueness of equilibrium points for concave n-person games. *Econometrica, 33*(3), 520–534.
8. Roubini, N. (2018). Testimony for the hearing of the US senate committee on banking, housing and community affairs on “exploring the cryptocurrency and blockchain ecosystem”, https://www.banking.senate.gov/imo/media/doc/Roubini_Testimony_10-11-18.pdf
9. Sanchez, D. C. (2017). An optimal ICO mechanism. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3040343
10. Shen, W., Tang, P., & Zuo, S. (2019). Automated mechanism design via neural networks. In *Proceedings of the 18th international conference on autonomous agents and multiagent systems*, international foundation for autonomous agents and multiagent systems, Richland, SC, AAMAS ‘19 (pp. 215–223).
11. Sinha, A., & Anastasopoulos, A. (2015). Mechanism design for fair allocation. In *2015 53rd annual allerton conference on communication, control, and computing (Allerton)*, IEEE, Monticello, IL, USA. https://doi.org/10.1109/allerton.2015.7447041
12. Wit22. (2019). Bat ICO whale-sale—completely against the ethos of ethereum and cryptocurrency, https://www.reddit.com/r/ethtrader/comments/6efsc8/bat_ico_whale_sale_completely_against_the_ethos_of/
13. Yokoo, M., Sakurai, Y., & Matsubara, S. (2004). The effect of false-name bids in combinatorial auctions: New fraud in internet auctions. *Games and Economic Behavior, 46*(1), 174–188.

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.