Centralization in Proof-of-Stake Blockchains: A Game-Theoretic Analysis of Bootstrapping Protocols (supplementary material)

Anonymous Author(s)
Submission Id: 309

ACM Reference Format:
Anonymous Author(s). 2024. Centralization in Proof-of-Stake Blockchains: A Game-Theoretic Analysis of Bootstrapping Protocols (supplementary material). In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024*, IFAAMAS, 5 pages.

A PROOF FOR THEOREM 1

Proof. To show that C-NORM can distinguish between s_0 and s_1 we consider any (arbitrary) $s_0 \in S_{SA}$ and corresponding $s_1 \in S_{NSA}$. We show for each such sampling for s_0, s_1 we have $\Omega^\star(s_0) \neq \Omega^\star(s_1)$ which concludes our proof.

We are considering the experiment being conducted when the stake distribution is happening through an Incentive-Compatible bootstrapping protocol. Therefore, $\hat{\theta}_i = \theta_i$ for any player p_i. Consider two samples $s_0 \in S_{SA}$ and $s_1 = e_r(s_0)$. The goal is for $\Omega^\star$ to distinguish between (s_0, s_1).

First we calculate $\Omega^\star$ for s_1. Since there are no edges, $\omega_i = c_i$. According to the bootstrapping protocol, the allocated stake c_i is proportional to the valuation θ for a player p_i. Therefore, we get $\omega_i/\hat{\theta}_i = \theta_i \cdot z/\hat{\theta}_i$ for some constant $z > 0$. However, due to the Incentive Compatible property of the bootstrapping protocol, we have $\omega_i/\hat{\theta}_i = z$. Thus, scaled stake $\beta_i = \frac{z}{\sum_{i=1}^n z} = \frac{1}{n}$ which gives $\Omega^\star = 0$.

Now, to distinguish from the other case, we want $\Omega^\star > 0$ (by more than negligible value) for s_0. Consider $s_0 \in S_{SA}$. There is atleast one (non-negligible weighted) edge and the graph is a Directed Acyclic Graph, which means there is at least one sink node (node with only incoming edges). Wlog. let this node correspond to player p_i. The sum of weights of incoming edges be q. Therefore, $\omega_i/\hat{\theta}_i = (c_i + q)/\hat{\theta}_i = (z \cdot \theta_i)/\hat{\theta}_i + q/\hat{\theta}_i = z + q/\theta_i$. The scaled stake $\beta_i = \frac{z+q/\theta_i}{\sum_{j=1}^n \omega_j/\hat{\theta}_j} \geq \frac{z+q/\theta_i}{nz} = \frac{1}{n} + \frac{q}{n\cdot\theta_i}$. Now we get $\Omega^\star$ as

$$\Omega^\star = \frac{1}{2}\sum_{j=1}^{n}\left|\beta_j - \frac{1}{n}\right| \geq \beta_i - \frac{1}{n} = \frac{q}{n\cdot\theta_i}$$

Therefore, $\Omega^\star \geq \frac{q}{n\cdot\theta_i}$ which is a non-negligible value. Therefore, for any pair (s_0, s_1) we can distinguish between the two states. Let the player M_D be given (s_a, s_b) such that (wlog.) $\Omega^\star = 0$ for s_a and $\Omega^\star > 0$ for s_b. Then $a = 1, b = 0$. Similarly, M_D can also predict correctly in case of $a = 0, b = 1$. If we are repeating this κ times, then M_D correctly predicts the ordering of (a, b) with probability $1 - \mathsf{negl}(\kappa)$. □

Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), N. Alechina, V. Dignum, M. Dastani, J.S. Sichman (eds.), May 6 – 10, 2024, Auckland, New Zealand.

B PROOF FOR THEOREM 2

Proof. Consider $\Omega_1^\star = \alpha$. The set of players $P = \{p_1, p_2 \ldots, p_n\}$ and *scaled stake* is $\boldsymbol{\beta} = \{\beta_1, \beta_2, \ldots, \beta_n\}$. Wlog. we consider $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_n$. Therefore, $\beta_{max} = \beta_1$. Now, we can write $\Omega_1^\star$ as

$$\frac{1}{2}\sum_{i=1}^{n}\left|\beta_i - \frac{1}{n}\right| = \alpha$$

We consider δ^{th} percentile of $\boldsymbol{\beta}$ as the player p_i which has the next lowest stake to δ percentile of players. Let $\boldsymbol{\beta}_\delta$ be used to represent this δ^{th} percentile. Therefore, $\boldsymbol{\beta}_\delta := \beta_{\lceil(1-\delta)\cdot n\rceil}$.

Case 1: $\boldsymbol{\beta}_\delta \leq \frac{1}{n}$: In this case, we can write $\Omega_1^\star = \alpha$ as,

$$\begin{aligned}\frac{1}{2}\left(\left|\beta_{max} - \frac{1}{n}\right| + \left|\boldsymbol{\beta}_\delta - \frac{1}{n}\right|\right) &\leq \alpha \\ \beta_{max} - \frac{1}{n} + \frac{1}{n} - \boldsymbol{\beta}_\delta &\leq 2\alpha \\ \frac{\beta_{max}}{\boldsymbol{\beta}_\delta} &\leq 1 + \frac{2\alpha}{\boldsymbol{\beta}_\delta}\end{aligned}$$

Case 2: $\boldsymbol{\beta}_\delta \geq \frac{1}{n}$: In that case, we can write $\Omega_1^\star = \alpha$ as

$$\begin{aligned}\beta_{max} - \frac{1}{n} &\leq 2\alpha \\ \frac{\beta_{max}}{\boldsymbol{\beta}_\delta} &\leq \frac{1/n}{\boldsymbol{\beta}_\delta} + \frac{2\alpha}{\boldsymbol{\beta}_\delta} \leq 1 + \frac{2\alpha}{\boldsymbol{\beta}_\delta}\end{aligned}$$

The last inequality comes since $\boldsymbol{\beta}_\delta \geq \frac{1}{n}$. We have therefore shown that for $\Omega_1^\star = \alpha$, the system satisfies the Proportionality condition. Additionally, $\Omega^\star$ (C-NORM) captures attempts of sybil attacks successfully (as demonstrated from Theorem 1), and we can enforce on the protocol the condition for *Minimum Participation*. Therefore, if $\Omega_1^\star = \alpha$ then protocol (which ensures *Minimum Participation*) is $(\tau, \delta, \frac{2\alpha}{\boldsymbol{\beta}_\delta})$–Decentralized for any $\delta \in [0, 1]$. □

C PROOF FOR CLAIM 1

Proof. In proving non-IC property for Airdrop, we show that if a party forms pseudo-identities, they can always obtain a higher utility than honestly disclosing their valuations, even when other players are reporting their true valuations and are not a part of any coalition. This is because, in Airdrop, all players get the same reward irrespective of their valuation, which incentivizes them to split their valuation among pseudo-identities to obtain a higher utility. Consider an Indicator Function $\mathbf{1}_{\hat{\theta}_i > 0}$ which is 1 if $\hat{\theta}_i > 0$ else 0. The utility function for *airdrop* bootstrapping protocol for player p_i is written as

$$U_i(\hat{\theta}_i, \hat{\boldsymbol{\theta}}_{-i}, \emptyset, \emptyset; \theta_i) = b_{airdrop} \cdot \mathbf{1}_{\hat{\theta}_i > 0} - \Omega^\star \cdot g(\theta_i)$$

For Nash Incentive Compatibility (IC) from Equation 6 of Definition 4.2 we require $\forall\ \hat{\theta}_i \in \mathbb{R}_{\geq 0}, \forall\ A_i \in \mathcal{A}_i$

$$U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i) \geq U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \boldsymbol{\theta})$$

$$b_{airdrop} \cdot \mathbf{1}_{\hat{\theta}_i > 0} - \Omega^\star \cdot g(\theta_i) \geq b_{airdrop} \cdot \sum_{j \in A_i} \mathbf{1}_{\hat{\theta}_j > 0} - \Omega^\star \cdot g(\theta_i)$$

We therefore observe that by forging identities (Sybil-attack) which is equivalent to forming a coalition A_i (from Remark 1) we observe that a player can forge arbitrary number of identities and gain more reward than following the protocol honestly. This means for any A_i such that $|A_i| > 1$ the above inequality does not hold true. Thus, Airdrop does not satisfy Nash Incentive Compatibility (IC). □

D PROOF FOR CLAIM 2

Proof. Consider a Proof-of-Burn-based bootstrapping where cryptocurrency from an *Old Crypto Token* \$*OCT* is burnt to obtain *New Crypto Token* \$*NCT*. The conversion rate from *OCT* to *USD* is 1 *OCT* = *d USD* and for *NCT* is 1 *NCT* = *e USD*. The rule is set such that if a player burns *a OCT* they obtain *b NCT*. Payoff on not participating in the protocol for a player p_i is $U_i(0, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \boldsymbol{\theta}) = -\Omega^\star \cdot g(\theta_i)$. The payoff obtained from participating in the protocol honestly, for some constant $\gamma \in \mathbb{R}_{>0}$ is

$$U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i) = \quad (b \cdot e - a \cdot d)\gamma\theta_i - \Omega^\star \cdot g(\theta_i)$$

However, setting an exchange rate for the New Crypto Token (which is set by the protocol designers) does not establish the exchange rate, but sets a "one-way peg" or price-ceiling for *NCT* such that $b \cdot e \leq a \cdot d$ (See [45] Section 10.1 for more details). If we account for transaction-fees and expected utility, then we get

$$\begin{aligned}\mathbb{E}[U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)] &= \mathbb{E}[(b \cdot e - a \cdot d)\gamma\theta_i - \Omega^\star \cdot g(\theta_i)] \\ &< -\mathbb{E}[\Omega^\star g(\theta_i)] = \mathbb{E}[U_i(0, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \boldsymbol{\theta})]\end{aligned}$$

Therefore, PoB-based bootstrapping protocol is not Individually Rational (IR). □

E PROOF FOR LEMMA 6.1

Proof. Consider a PoW blockchian protocol such that if all players invest in mining proportionally to their true valuation then player p_i with valuation θ_i has mining power $m_i = \theta_i \cdot l$ (for some $l \in \mathbb{R}_{>0}$). The cost incurred per unit mining power for any player is χ and the reward obtained on mining a block be r_b.The minimum mining power which a player can have be m_{min}. This means $\forall p_i \in P, m_i \geq m_{min}$. Additionally, let $M = \sum_{i \in [n]} m_i$.

Consider for player p_i a random variable R_i which denotes the payoff of the player.

$$R_i = \begin{cases} r_b - \chi m_i, & \text{with probability } \frac{m_i}{M} \\ -\chi m_i, & \text{with probability } \frac{M - m_i}{M} \end{cases}$$

Individual Rationality: For IR, we require that expected block reward should exceed cost of mining for all players p_i. Therefore $\forall p_i \in P$ the expected utility on abstaining from the protocol is

$$\mathbb{E}[U_i(0, \hat{\boldsymbol{\theta}}_{-i}, \emptyset, A_{-i}; \theta_i)] = -\mathbb{E}[\Omega^\star \cdot g(\theta_i)]$$

The expected utility on participating in the protocol for each round is

$$\begin{aligned}\mathbb{E}[U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)] &= \mathbb{E}[R_i] - \mathbb{E}[\Omega^\star \cdot g(\theta_i)] \\ &= (r_b \frac{m_i}{M} - \chi m_i) - \mathbb{E}[\Omega^\star \cdot g(\theta_i)]\end{aligned}$$

For IR we require $\mathbb{E}[U_i(0, \hat{\boldsymbol{\theta}}_{-i}, \emptyset, A_{-i}; \theta_i)] \leq \mathbb{E}[U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)]$ which gives us $\forall p_i \in P$

$$\begin{aligned}(r_b \frac{m_i}{M} - \chi m_i) &\geq 0 \\ r_b \frac{m_i}{M} &\geq \chi m_i \quad \Rightarrow \frac{\chi M}{r_b} \leq 1\end{aligned}$$

Incentive Compatibility: For Incentive Compatibility, we will show for each player $p_i \in P$, reporting a valuation $\hat{\theta}_i \neq \theta_i$ will lead to a lower payoff. We proceed in two cases:

Case 1 $\hat{\theta}_i < \theta_i$: In this case, let $m_i^{'}$ be the mining power corresponding to the disclosed valuation $\hat{\theta}_i$. Clearly, $m_i^{'} < m_i$. Consider for some $a > 0, m_i^{'} = m_i - a$. The expected difference in utility $\mathbb{E}[U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \theta_i) - U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)]$ is therefore given by

$$\begin{aligned}&\mathbb{E}[U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \theta_i) - U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)] \\ &= r_b \left(\frac{m_i^{'}}{M - m_i + m_i^{'}} - \frac{m_i}{M} \right) - \chi(m_i^{'} - m_i) \\ &= \frac{a}{M - a} \left((M - a)\chi - r_b \right) \\ &< \frac{a}{M - a} \left(M\chi - r_b \right) \leq 0\end{aligned}$$

The last inequality comes from the condition obtained from Individual Rationality $\chi M \leq r_b$.

Case 2 $\hat{\theta}_i > \theta$: In this case, let $m_i^{'} = m_i + a$ (for some $a > 0$) be the mining power corresponding to reported valuation $\hat{\theta}_i$. Consider $R_i^{'}$ be the random variable denoting reward when reported valuation is $\hat{\theta}_i$. Therefore,

$$R_i^{'} = \begin{cases} r_b - \chi(a + m_i), & \text{with probability } \frac{m_i + a}{M + a} \\ -\chi(a + m_i), & \text{with probability } \frac{M - m_i}{M + a} \end{cases}$$

Now, we can write the expected difference in utility as

$$\begin{aligned}&\mathbb{E}[U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \theta_i) - U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)] = \mathbb{E}[R_i^{'} - R_i] \\ &= r_b \left(\frac{m_i + a}{M + a} - \frac{m_i}{M} \right) - \chi(m_i + a - m_i) \\ &= r_b \frac{a(M - m_i)}{M(M + a)} - a\chi \\ &= \frac{a r_b}{M + a} \left(1 - \frac{m_i}{M} - \frac{\chi(M + a)}{r_b} \right) \\ &\leq \frac{a r_b}{M + a} \left(1 - \frac{m_{min}}{M} - \frac{M\chi}{r_b} \right) < 0\end{aligned}$$

The last inequality uses the fact $\left(1 - \frac{m_{min}}{M}\right) < \frac{M\chi}{r_b}$.

In conclusion, we have shown that if $1 - \frac{m_{min}}{M} < \frac{M\chi}{r_b} \leq 1$ is satisfied, then the PoW-based bootstrapping protocol (W2SB) is both Individually Rational (IR) and Incentive Compatible (IC). □

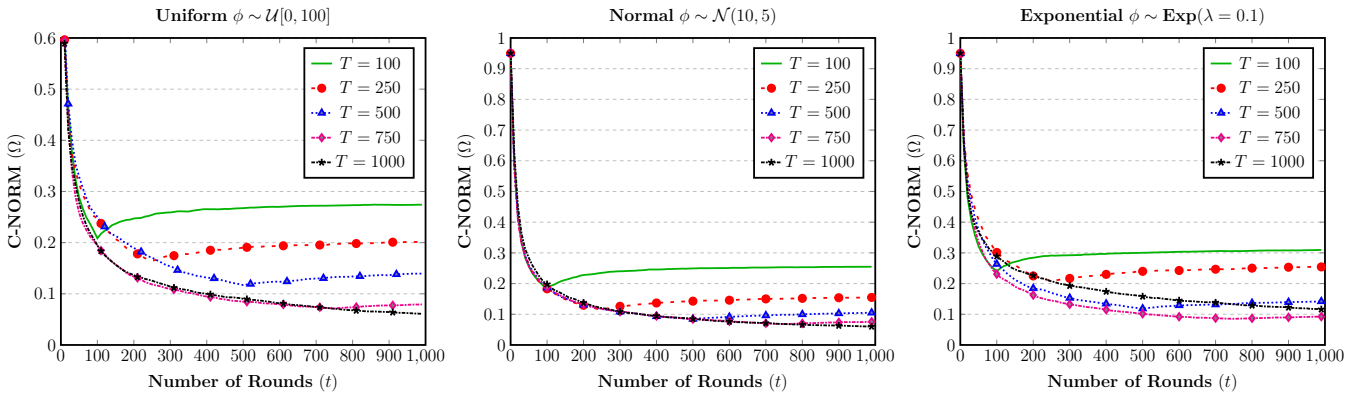

Figure 1: C-NORM against rounds for different T and different distributions of miner stake

F PROOF FOR THEOREM 3

Proof. To prove the theorem, we run the W2SB for T rounds. We show that for any arbitrary desired value $z \in (0, 1)$ there always exists T such that after T rounds, $\Omega^\star \leq z$. Out of these T rounds, the first $T_0 < T$ rounds are such that the majority of players have joined the system before this round. This means T_0 is such that $\Psi(T_0) = 1 - \frac{x}{n}$ for $x < z$. Wlog. we assume players join the system in the order $p_1, p_2, \ldots, p_n$. The C-NORM value is therefore given by

$$\begin{aligned}
\Omega^\star &= \frac{1}{2}\sum_{i=1}^{n}\left|\beta_i - \frac{1}{n}\right| \\
&= \frac{1}{2}\sum_{i=1}^{\Psi(T_0)n}\left|\beta_i - \frac{1}{n}\right| + \sum_{i=\Psi(T_0)n}^{n}\left|\beta_i - \frac{1}{n}\right| \\
&\leq \sum_{i=1}^{\Psi(T_0)n}\left|\beta_i - \frac{1}{n}\right| + \sum_{i=\Psi(T_0)n}^{n} 1 \\
&= \sum_{i=1}^{\Psi(T_0)n}\left|\beta_i - \frac{1}{n}\right| + n\cdot(1 - \Psi(T_0))
\end{aligned}$$

We get the last inequality because $|a - b| \leq \max(|a|, |b|)$ and $|\beta_i - \frac{1}{n}| \leq \max(|\beta_i|, \frac{1}{n}) \leq 1$. Now we consider $\left|\beta_i - \frac{1}{n}\right|$, which gives us

$$\begin{aligned}
\left|\beta_i - \frac{1}{n}\right| &= \left|\frac{\omega_i/\theta_i}{\sum_{j=1}^{n}\omega_j/\theta_j} - \frac{1}{n}\right| \\
&\leq \left|\frac{T_0\cdot r_\text{b} + (\omega_i^{'}/\theta_i)}{\sum_{j=0}^{n}\chi(T - T_0)} - \frac{1}{n}\right|
\end{aligned}$$

For the last inequality, (1) $\omega_i^{'}$ is the payoff from round T_0 to T, and before that any player can get at most $T_0 r_\text{b}$. Therefore, we use the inequality $\omega_i/\theta_i \leq T_0 + \omega_i^{'}/\theta_i$ to upper bound the numerator. (2) $\omega_j/\theta_j \geq \omega_j^{'}/\theta_j \geq (T - T_0)\chi$ since W2SB is IR means $\frac{\theta_i r_\text{b}}{\sum_{j=1}^{n}\theta_j} \geq \chi$ and therefore $\omega_j/\theta_j \geq \chi(T - T_0)$ as the stake is allocated for $T - T_0$ rounds.

We can also upper bound $\omega_i^{'}/\theta_i$ by considering the stake is distributed among only the players who have joined in round $\leq T_0$. In this case, $\omega_i^{'}/\theta_i = c\ \forall\ p_i$ joining before round T_0 for some constant c. We therefore get

$$\begin{aligned}
\Omega^\star &\leq n\Psi(T_0)\left|\frac{T_0 r_\text{b} + (T - T_0)c}{n\chi(T - T_0)} - \frac{1}{n}\right| + x \\
&= n\Psi(T_0)\left|\frac{c}{n\chi} + \frac{T_0 r_\text{b}}{n\chi(T - T_0)} - \frac{1}{n}\right| + x
\end{aligned}$$

When we increase T, we can reduce the mod term to a small enough value such that $\Omega^\star \leq z$. By IR we require $c = r_\text{b}/M \approx \chi/n$ (for very small m_{min}, see Lemma 6.1). Therefore,

$$\Omega^\star \lesssim \Psi(T_0)\left|\frac{T_0 r_\text{b}}{\chi(T - T_0)}\right| + x \quad \leq z \Rightarrow T \geq \frac{\Psi(T_0)T_0 r_\text{b}}{(z - x)\chi} + T_0$$

Thus, for any $z \in (0, 1]$ we can always obtain a finite T such that $\Omega^\star \leq z$ if W2SB is run for $\geq T$ rounds, assuming dynamic participation according to some distribution with CDF Ψ. □

G EXPERIMENTS

The plots are shown in figure 1 for distributions with different parameters to show that the trend remains the same.

H CYCLE ELIMINATION ALGORITHM

Cycle Elimination Procedure. Without loss of generality, consider there exists a cycle with edges from p_1 to p_2, p_2 to p_3 and so on till p_k to p_1. These cycles can be found using any cycle detection algorithm such as BFS, Floyd's algorithm. Let weight $w_{1,2}$ be the smallest of the weights. We eliminate the edge from p_1 to p_2 by subtracting the weight $w_{1,2}$ from each edge of the cycle. If there exist multiple cycles, the order of elimination will result in different DAGs. However, the resultant value of the centralization metric (proposed in Section 5.2) does not change.