Centralization in Proof-of-Stake Blockchains: A Game-Theoretic Analysis of Bootstrapping Protocols

No Author Given

No Institute Given

Abstract Proof-of-stake (PoS) has emerged as a natural alternative to the resource-intensive Proof-of-Work (PoW) blockchain, as was recently seen with the Ethereum Merge. PoS-based blockchains require an initial stake distribution among the participants. Typically, this initial stake distribution is called bootstrapping. This paper argues that, unless carefully designed, bootstrapping protocols are prone to centralization. Towards ideal bootstrapping, we define three conditions: (i) Individual Rationality (IR), (ii) Incentive Compatibility (IC), and (iii) $(\tau, \delta, \epsilon)-$ Decentralization that an *ideal* bootstrapping protocol must satisfy. (τ, δ, ϵ) are certain parameters to quantify decentralization. We propose a novel centralization metric, C-NORM, to measure centralization in a PoS System. We define a centralization game – Γ_{cent}, to analyze the efficacy of centralization metrics. We show that C-NORM effectively captures centralization in the presence of strategic players capable of launching Sybil attacks. To analyze all this, we propose a novel game $\Gamma_{\mathsf{bootstrap}}$ to analyze centralization due to bootstrapping. We analyze popular bootstrapping protocols such as Airdrop and Proof-of-Burn (PoB) and prove they do not satisfy IC and IR, respectively. Finally, motivated by the Ethereum Merge, we study W2SB (a PoW-based bootstrapping protocol) and prove it is ideal. In addition, we conduct synthetic simulations to empirically validate that W2SB bootstrapped PoS is decentralized.

1 Introduction

Blockchain, first introduced with Bitcoin [45], is an append-only, distributed ledger. To maintain a distributed ledger, we need a *distributed consensus* – i.e., all the parties (which we call players) agreeing on a single state of the ledger. *Public* blockchains employ consensus protocols such as Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Elapsed-Time (PoET), among others [64]. All these protocols rely on *incentive engineering* to achieve consensus. In PoW blockchains, the players solve cryptographic puzzles to propose the next block to be added to the ledger. In return, it obtains certain newly minted coins as a reward – *block reward*. With such incentive engineering, PoW achieves consensus if more than 50% of players are honest, whereas traditional consensus protocols require $\frac{2}{3}^{\text{rd}}$ players to be honest [9]. Due to the high energy requirements of PoW, energy-efficient PoS protocols evolved. The blockchain community is transitioning to more energy-efficient Proof-of-Stake (PoS) protocols (e.g., Ethereum [8], the second largest blockchain by market capitalization and share [1], shifted to PoS via the Merge [14]). In PoS, a block proposer is selected with probability proportional to its stake in the system and awarded the new coins. With incentives involved, the strategic players may amass higher stakes upfront to maximize their rewards, which might affect the security of the protocols. This paper focuses on the centralization of stakes that might happen in PoS consensus protocols.

Centralization in PoS blockchains – Practical Examples Polygon Hard fork [46] received criticism because it required signatures of just 13 validators out of a quorum of 100 due to centralization of resources. Furthermore, popular PoS-based blockchains such as ICON [16], Tezos [22], Cosmos [37], and Irisnet are highly centralized (top 10 stakeholders hold $\geq 1/3$ of the total stake [57]). This centralization exposes them to the risk of potential attacks[1].

Why is Decentralization Important? Governance and security of blockchains rely on the decentralization of resources among players. If a player/coalition collects disproportionate rewards, it might compromise the correctness of protocols [17,19]. In PoS blockchain, centralization is when a coalition (aka stake pool) holds a high amount of stake, exceeding their valuation for the system. A centralized PoS system is susceptible to threats such as denial of service (DoS), blacklisting, and double-spending [65], etc.

[1] E.g., the Luna Crash [56] resulted from offloading a massive volume of USDT in a very short interval. We suspect such coordinated de-pegging might be a repercussion of the centralization in the system.

Bootstrapping Protocol	IR	IC	DC	Ideal Bootstrapping
AirDrop [15]	✓	×	×⋆	×
Proof-of-Burn [32]	×	✓	✓†	×
W2SB	✓	✓	✓	✓

†: Depends on the parent cryptocurrency
⋆: We conjecture that it is decentralized, but no existing metric can yet assert to it

Table 1: W2SB compared with existing bootstrapping protocols

Among the multiple causes of centralization in PoS, two major causes are (1) Centralization due to initial stake distribution — called a *bootstrapping* protocol, and (2) centralization due to institutions like exchanges and staking pools. This paper primarily focuses on bootstrapping. We argue that ineffective bootstrapping can cause centralization in PoS, implying the crucial role of bootstrapping protocol. Thus, there is a need to analyze decentralization via bootstrapping protocols in the presence of strategic players.

Our Approach and Contributions

The Bootstrapping Model. Towards analyzing a bootstrapping protocol, first we model a novel construction of the bootstrapping of a PoS-based blockchain as a game, namely $\Gamma_{\mathsf{bootstrap}}$ (Section 4) among participating players. We propose that the bootstrapping protocol should satisfy: (i) *Individual Rationality* (IR) – participating in the protocol should give higher utility than abstaining from it; (ii) *Nash Incentive Compatibility* (IC) – following the bootstrapping protocol should be a Nash Equilibrium for all players and, (iii) *Decentralization* (DC), – the PoS system should be decentralized after the bootstrapping protocol. We define a bootstrapping protocol to be *ideal* if it simultaneously satisfies all three conditions (Definition 4). We need a measure to quantify centralization in PoS System to assert decentralization.

Quantifying Centralization. An ideal bootstrapping protocol's central goal must be to distribute the initial stake such that the PoS system is not centralized. Towards this, we use the notion of $(\tau, \delta, \epsilon)-$decentralization [38]. Naturally, to quantify centralization, we require an effective metric. It must be resilient to a player's *strategic* behaviour. Unfortunately, prior works on quantifying centralization in blockchains, such as using the Gini coefficient [20,21], the Nakamoto Coefficient [40] or Entropy-based metrics [63] are susceptible to manipulations by players who might game the metric to falsely make the system appear decentralized.

C-NORM. Given $\Gamma_{\mathsf{bootstrap}}$, the definitions of IR and IC follow the standard template. But, it is challenging to construct a strategyproof centralization metric. To this end, we propose the construction of a $\mathcal{G}$ – directed cyclic graph– DAG-based representation of PoS System transactions. $\mathcal{G}$ aims to represent (i) the current state and (ii) the history of the PoS system. With $\mathcal{G}$, we propose our novel centralization metric, C-NORM (Section 5.2). C-NORM incorporates the strategic behaviour of the players. Moreover, the metric also captures the dynamic arrival of the players to the PoS system, which corresponds to dynamic updates to $\mathcal{G}$.

The Centralization Game (Γ_{cent}). We introduce Γ_{cent}, a game that provides a unified framework to measure the effectiveness of any centralization metric, given transaction history $\mathcal{G}$ (Section 5.3). Γ_{cent} is a two-player game between a Metric Challenger (MC) and a Metric Descriptor (MD). If MD can distinguish between the centralized and decentralized (less centralized) systems MC presents, then MD wins. Otherwise, the metric is inept. We show that for famous blockchain centralization metrics – Nakamoto coefficient [40], Entropy [63], and Gini Coefficient [21], the Metric Descriptor loses the game. However, for C-NORM, the Metric Descriptor wins with a very high probability (Theorem 1). We also show that if a protocol is IC and has low C-NORM, then it satisfies our definition of $(\tau, \delta, \epsilon)-$ Decentralized (Theorem 2).

Analyzing Bootstrapping Protocols. We analyze the existing bootstrapping protocols are ideal or not (Section 6). First, we prove that *Airdrop* [15] and *Proof-of-Burn* (PoB) [32] are not ideal as they do not satisfy IC and IR, respectively. Second, we prove that a PoW-based bootstrapping protocol[2] (abbreviated as W2SB) is ideal. Table 1 summarizes these results.

[2] The recent Ethereum Merge [14] motivates the study of PoW-based bootstrapping for PoS blockchains.

We validate our findings in Section 7 with experimental simulations of PoS blockchains bootstrapped with W2SB for different setups based on random valuation distributions, random arrival of the players, different levels of decentralization, etc.

2 Related Work

Bootstrapping in Blockchains. Proof-of-Stake (PoS) blockchain protocols employ various methods to bootstrap their networks, e.g., Initial Coin Offering (ICO) [3,44], Airdrop [15], Proof-of-Burn [32], and others [33,34,39] – which focus on optimizing miners computational, communication, and memory costs. Airdrops are vulnerable to Sybil Attacks [41] and Privacy Leaks [25]. Smartdrop [29], lacks a game-theoretic analysis of its security and effectiveness. Ethereum [8,62], originally a Proof-of-Work (PoW) cryptocurrency, transitioned to a PoS-based blockchain in 2022 during the"Merge event" [14]. Though it was not by design, Ethereum's PoW to PoS transition appears serve as a good bootstrapping protocol.

Game-theoretic analysis of blockchain protocols is gaining traction [2,11,23,31,53,54] but still lacks a formal game-theoretic framework for analyzing bootstrap protocols.The need for such a formal study is crucial as bootstrapping is one of the significant causes of centralization in PoS-based blockchains [59,55,57].

Centralization in Networks and Multi-Agent Systems. There has been extensive research on quantifying centralization in different multi-agent systems [26,35]. While some of these centrality measures and analyses are for dynamic systems such as social networks, where agents do not behave strategically to game the system [5,42,47], there are centrality measures that discuss rational parties who try to game the metric [27,60,61]. Among these, Istrate *et al.* [27] discuss parties trying to game the system through coalitions and analyze network centrality.However, the work quantifies centrality in networks, while we quantify in a system with each node having its own private and public valuations, forming coalitions among themselves (i.e., Sybil attacks). Moreover, it is intractable to compute the metric. Other metrics such as [60] model the game as a Stackelberg Game where parties are trying to spoof the metric. However, the players are restricted to changing links in the networks, unlike our system, where they can report false valuations and perform stake redistribution (equivalent to weight redistribution among network nodes). Several metrics for measuring centralization exist in the blockchain literature as well [20,21,36,40,63]. E.g., metrics based on the Gini Coefficient [20] or the Nakamoto Coefficient [40]. We analyze the efficacy of these metrics in Section 5 and show that they fail in particular cases.

Kwon *et al.* [38] focuses on achieving perfect decentralization in blockchain protocols such as PoW, PoS, and dPoS. We note two significant differences between awesomeDecentralization and our work. (i) we analyze centralization caused during bootstrapping whereas they analyze centralization in PoW and PoS systems post-bootstrapping. (ii) Our utility model penalizes centralizationwhile Kwon *et al.* assume the protocol is Sybil-resistant, which is a strong assumption.

Rauchs and Hileman [51] study centralization in the application layer due to the concentration of stake with exchanges and third-player wallet services. Further, there also exists analysis on the governance layer of different blockchain protocols [4,18]. Note that C-NORM is more general, encompassing the entire PoS system and capturing the stake distribution across different accounts. Other forms of centralization, e.g., due to increased storage costs [24,50], are out of the scope of this paper. For further details, an extensive survey on blockchain centrality measures can be found in [55].

3 Preliminaries

In this section, we summarize relevant blockchain preliminaries and centralization metrics in the literature.

3.1 Blockchain Preliminaries

A blockchain system $\mathcal{B}$ is a decentralized ledger maintained by interested players $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$. They need to agree on the state of the ledger which can be achieved through Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Burn (PoB) etc. We briefly discuss such consensus algorithms below.

Proof-of-Work (PoW) [45]. A blockchain-based on PoW comprises a consensus mechanism where players (aka *miners*) compete to solve a cryptographic puzzle to propose the next block[3]. A miner mines blocks in discrete periods called *round*. Upon a successful query, the miner gets a reward r_{b} in that round. Each miner p_i's probability of mining a block is a_i, the fraction of the total mining power it controls. χ denotes the expected cost incurred per unit of mining power in a single round. If the total mining power is M, then the cost incurred in one round by miner p_i is $a_i M \cdot \chi$. The expected payoff for miner i becomes $a_i \cdot (r_{\mathrm{b}} - M\chi)$.

Proof-of-Stake (PoS) [12]. The energy-intensive nature of PoW has led to PoS-based blockchains gaining traction due to their significantly lower carbon footprint [30,49]. In PoS, players 'enroll' themselves for block creation by locking their *stake*. Then, the probability of a player getting selected to propose the next block is proportional to its relative stake. PoS-based blockchains face several challenges, including centralization, fairness, and security concerns [57]. Notice that a 'decentralized' PoS-based blockchain is one where each player has a stake proportional to its *valuation* for the system. This valuation, in theory, is reflected by the stake held (equivalently, the money invested) by the player. Thus, for any player i, the ratio of the stake ω_i held by it and its valuation θ_i should be the same for all p_i. We call this ratio as a *true effective stake* of a system. For p_i its effective stake is $\beta_i = \frac{\omega_i/\theta_i}{\sum_{j\in[n]}\omega_j/\theta_j}$. Initially, PoS blockchains require some stakes distribution for the mechanism to start, which is achieved through *bootstrapping*. We now discuss some bootstrapping protocols employed in practice.

Proof-of-Burn (PoB) [32]. In PoB, players 'burn' a fraction of their cryptocurrency, i.e., transfer of the currency to a provably unspendable address [32] and in return are issued a stake in the PoS blockchain. In PoB bootstrapped PoS system, a player burns y fraction of a certain old cryptocurrency and obtains x fraction of bootstrapped cryptocurrency's tokens.

Airdrop [41]. Airdrop distributes digital tokens/assets to eligible players. The eligibility is based on certain predetermined conditions specified by the cryptocurrency organization (e.g., posting a tweet). Airdrop, while useful for marketing a new cryptocurrency, suffers from privacy problems and is prone to *Sybil attacks* [25,41].

Sybil Attack [13]. Sybil attack is when an attacker creates pseudo-identities that enable them to gain higher utility. Sybil attack increases the reward obtained by the attacker. A blockchain with player p_i and pseudo-identities $e_1, e_2, \ldots, e_k$ and utility for k being U_k is prone to Sybil-attack if $U_{p_i} < \sum_{j=1}^{k} U_{e_j}$.

3.2 Centralization Metrics

In the literature, the following metrics are used to study centralization in blockchains.

Entropy-based Centralization. It is an information-theoretic metric to quantify centralization [36,40,63]. The entropy of a system H, normalized to the range $[0,1]$ is

$$H := -\frac{1}{\log(|P|)} \sum_{p_i \in P} \beta_i \log(\beta_i) \tag{1}$$

Gini Coefficient. It is a classic measure from economics that quantifies inequality in resource distribution using $G \in [0,1]$ where 0 represents perfect equality, and 1 represents maximal inequality. The Gini coefficient for a blockchain system $\mathcal{B}$ is [20,21,36,40]

$$G := \frac{1}{2|P|} \sum_{p_i \in P} \sum_{p_j \in P} |\beta_i - \beta_j| \tag{2}$$

Nakamoto Coefficient. Nakamoto coefficient [36,40,58], a recent metric for measuring decentralization, is the minimum number of players in the system that together control the majority (i.e. more than some threshold $\tau_{th} \in [0,1]$) of the system. τ_{th} is protocol-dependent and is usually the minimum control required to disrupt the protocol. Mathematically, for a blockchain system $\mathcal{B}$, N is,

$$N := \min \left\{ |A| \;:\; \sum_{p_i \in A} \beta_i > \tau_{th}, A \in 2^P \right\} \tag{3}$$

[3] the puzzle is solved by querying a cryptographic function with inputs specific to the miner.

If Ω is a centralization metric used to study bootstrapping protocol Π, we denote the blockchain system as $\mathcal{B} = (\Pi, \Omega)$. In the next section, we model bootstrapping as a game, $\Gamma_{bootstrap}$, to study centralization and the influence of rational agents (which can launch a Sybil attack) on the performance in $\mathcal{B}$.

4 Bootstrapping in PoS System

We need to define the players' strategies and utilities to model $\Gamma_{bootstrap}$. Next, we need to define the desirable properties of the game's outcome. $\mathcal{B}$ uses Π to mint the initial coins in PoS System, which runs till round T, which we call *stopping time*. After T rounds, Π terminates, and the system runs a PoS protocol. Each player $p_i \in P$ has a private valuation of PoS System, $\theta_i \in \mathbb{R}_{\geq 0}$, on joining the system. θ_i indicates the amount that player p_i will prefer to invest in PoS System. The private valuation profile of all the agents is $\boldsymbol{\theta} := (\theta_1, \theta_2, \ldots, \theta_n)$.

Each player p_i elicits its valuation as $\hat{\theta}_i \in \mathbb{R}_{\geq 0}$ (through some preference aggregation procedure which is part of Π). E.g., by simply obtaining the coins of the underlying cryptocurrency. The set of reported valuations is $\hat{\boldsymbol{\theta}} := (\hat{\theta}_1, \hat{\theta}_2, \ldots \hat{\theta}_n)$. In a PoS System, the goal is to ensure each player holds a stake proportional to its system valuation (see discussion in Section 3.1). Thus, Π must ensure that at the end of round T, the stake held by each player p_i is proportional to their reported valuation of the system, i.e., $\hat{\theta}_i$.

Partition of player set P. We distinguish *player* and *agent*. In the PoS blockchain system, each address that holds the token is a player p_i. An agent is a "person" or "organization" participating in the PoS system who may control multiple such addresses (i.e., players) (equivalent to launching a Sybil attack). Thus, we can assume the set P is partitioned into disjoint sets, each partition controlled by an agent. We assume that the valuations are *additive*. If an agent controls $A \subset P$, its true (private) valuation is $\vartheta(A) = \sum_{i \in A} \theta_i$.

4.1 Strategy Space

Decentralization is the central concept in the security of any blockchain. Its market price will drop if $\mathcal{B}$ is centralized. Thus, as players are strategic, each player p_i's goal in the system $\mathcal{B}$ is to maximize its stake while keeping the recorded value of the system's centralization (or Ω) as low as possible. Towards this, it makes two choices: (1) reported/disclosed valuation $\hat{\theta}_i$ and (2) whether to launch a Sybil attack.

Sybil-attack. The set P denotes all the identities part of the PoS System. However, if an agent has launched a Sybil attack, it has a subset of addresses, i.e., players under its control. We represent them in our game as partitions of the set P — each partition being the group of players controlled by one strategic agent. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_z\}$ be the partition of players such that a single agent controls all the players in P_i. $A : P \to \mathcal{P}$ denotes the memship for each player. A player p_i can perform redistribution of its stake through pseudo-identities in $A(p_i)$, making the system appear more decentralized to the centralization metric Ω. The redistribution of the stake cannot increase the allocated stake; therefore, $\sum_{p_j \in P_i} \hat{\theta}_j$ remains constant $\forall P_i$. Though, in reality, agents act on behalf of players, we focus on players as we expect an ideal bootstrapping will ensure $\mid P_i \mid= 1$. To summarize, the strategy space for p_i is $M = \mathbb{R}_{\geq 0} \times \mathcal{A}_i$; $\mathcal{A}_i$ indicates possible set of partitions P_j such that $A(p_i) = P_j$.

4.2 Utility Structure

Given a PoS System $\mathcal{B}$, we now quantify players' utilities.

Let r_{block} be the rewards offered by Π in bootstrapping, and let b_{spent} be the total cost across all players to construct and maintain the system till T. Let $b = (r_{\text{b}} - b_{\text{spent}}) \cdot \gamma$. γ is some constant translating rewards and costs to fiat currency. The total reward for player p_i is proportional to the stake allocated to it (which in turn is proportional to $\hat{\theta}_i$). We capture the loss in the stake's external value due to centralization via a function $g(\theta_i)$ that is non-decreasing in θ_i. Thus, the utility for each player $p_i \in P$ is,

$$U_i(\hat{\theta}_i, \hat{\boldsymbol{\theta}}_{-i}, A(p_i), \mathcal{A}_{-i}; \theta_i) := b \cdot \hat{\theta}_i - \Omega(\cdot) \cdot g(\theta_i) \tag{4}$$

In Eq. 4, $\mathcal{A}_{-i} = \mathcal{P}/\{A(p_i)\}$ and $\hat{\boldsymbol{\theta}}_{-i} = \hat{\boldsymbol{\theta}}/\{\hat{\theta}_i\}$. Note that Π and Ω would be typically fixed for a blockchain system under study, so whenever clear from context, we omit mentioning them in $U_i(\cdot)$. In summary, the bootstrapping model for PoS system $\mathcal{B} = (\Pi, \Omega, P)$ can be defined by $\Gamma_{\mathsf{bootstrap}} = \langle P, \boldsymbol{\theta}, (U_i)_{i \in [n]} \rangle$.

4.3 Ideal Bootstrapping Protocol

In an *ideal* bootstrapping, players should prefer to join Π than abstaining (IR), should invest their true valuation (IC) and should be decentralized. We define these properties formally.

The strategy of abstaining for any player $p_i \in P$ is $\hat{\theta}_i = 0$ and $A_i = \{i\}$. Formally,

Definition 1 (Individual Rationality (IR)). *Π is Individually Rational (IR) if* $\forall p_i \in P$, $\forall \boldsymbol{\theta} \in \mathbb{R}^n_{\geq 0}$, $\forall \hat{\boldsymbol{\theta}}_{-i} \in \mathbb{R}^{n-1}_{\geq 0}$, $\forall \mathcal{A}_{-i}$,

$$U_i(\theta_i, \hat{\boldsymbol{\theta}}_{-i}, \{i\}, \mathcal{A}_{-i}; \theta_i) > U_i(0, \hat{\boldsymbol{\theta}}_{-i}, \{i\}, \mathcal{A}_{-i}; \theta_i) \tag{5}$$

IC requires, honest valuation reporting (i.e.,$\hat{\theta}_i = \theta_i \; \forall p_i$) is the Nash Equilibrium strategy for each player. In the definition below, the expectation is over the randomness in the system due to (i) random dynamic arrival of players and (ii) randomness of Π.

Definition 2 (Nash Incentive Compatibility (IC)). *Π is nash incentive compatible if* $\forall p_i \in P, \forall \boldsymbol{\theta} \in \mathbb{R}^n_{\geq 0}, \forall \hat{\theta}_i \in \mathbb{R}_{\geq 0}, \forall A_i \in \mathcal{A}_i$, *where* $\mathcal{H} := \{\{1\}, \{2\}, \ldots, \{n\}\}$

$$\mathbb{E}[U_i(\theta_i, \boldsymbol{\theta}_{-i}, \{i\}, \mathcal{H}_{-i}; \theta_i)] \geq \mathbb{E}[U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A(p_i), \mathcal{H}_{-i}; \theta_i)] \tag{6}$$

For decentralization, we motivate our definition from [38, Definition 4.1] along with a Sybil-resistance condition. We require (1) at least a fraction $\tau \in (0,1]$ of the total players to have joined the system, (2) the *true scaled stake*[4] for each player p_i should be as close to each other as possible (3) the system should be Sybil-resistant.Our definition differs from [38, Definition 4.1] as we capture each player's valuation using *scaled stake* instead of the total stake held by the player. We also impose a condition of Sybil-resistance. We define decentralization as follows:

Definition 3 ($(\tau, \delta, \epsilon)-$Decentralization). *A PoS based blockchain system is said to be* $(\tau, \delta, \epsilon)-$ decentralized *for* $\tau \in (0,1]$, *δ (percentile)* $\in [0, 100]$ *and* $\epsilon \in \mathbb{R}_{\geq 0}$ *if it follows:*

– ***Minimum Participation:*** *The set of players joined the PoS system by round t, P_t, is such that* $\frac{|P_t|}{|P|} \geq \tau$.
– ***Proportionality:*** *The ratio of max (β_{max}) and $\delta-$percentile true scaled stake (β_δ) is* $\frac{\beta_{max}}{\beta_\delta} \leq 1 + \epsilon$.
– ***Sybil-proofness:*** *The ratio* $\frac{\beta_{max}}{\beta_\delta}$ *cannot be reduced by forging identities without a decrease in utility.*

With this, we define ideal bootstrapping.

Definition 4 (Ideal Bootstrapping Protocol). *Given $\mathcal{B} = (\Pi, \Omega))$ with player P, Π is an* ideal bootstrapping protocol *under a proposed metric Ω of measuring centralization of the PoS system, if it (i) individually rational, (ii) Nash incentive compatible, (iii) $(\tau, \delta, \epsilon)-$Decentralized for reasonable values of (τ, δ, ϵ).*

The next section focuses on constructing a good measure (Ω) capturing centralization in $\mathcal{B}$.

5 Measuring Centralization in a PoS System

In this section, we (i) model a given $\mathcal{B}$ as a *PoS System Graph* (PSG), (ii) discuss C-NORM and its properties.

5.1 PoS System Graph

Given a complete history of transactions in a PoS system ($\mathcal{B}$) (which is available as a public ledger), we discuss how we construct a PSG ($\mathcal{G}$) that captures strategic redistribution of stake among the colluding players. We later use $\mathcal{G}$ to define our metric C-NORM.

[4] In PoS blockchain $\mathcal{B}$, $\beta_{\max} := \max_{i \in [n]} \beta_i$ and $\beta_\delta := \beta_r$ where p_r is δ^{th} percentile player when arranged in decreasing order of stake.

Motivation. The PSG ($\mathcal{G}$) should capture the following two properties of the PoS System: (1) the current state stake owned by each player – captured through the weights of each vertex in $\mathcal{G}$ and (2) the history, i.e., redistribution of stake – captured through the weighted directed edges between different vertexes. Additionally, $\mathcal{G}$'s construction must only depend on publicly available information about $\mathcal{B}$.

PoS System Graph (PSG). The Graph $\mathcal{G} = ([n], C, W)$ is a tuple consisting of a set of vertices $[n]$, one per player. Each vertex (player) p_i has a total stake c_i with it. We assign weights to these nodes as $\boldsymbol{C} = (c_1, c_2, \ldots, c_n)$. A directed edge i to j with weight $w_{i,j}$ captures the transactions summary between players p_i and p_j. The set W contains $w_{i,j}$ which are determined as follows:

- Define $\sum t_{i,j}$ as net positive transaction from p_i (currently having stake c_i) to p_j (with stake c_j) and $\sum t_{j,i}$ as net positive transaction from p_j to p_i. If $\sum t_{i,j} > \sum t_{j,i}$ then there exists an edge from p_i to p_j with weight $w_{i,j} = \sum t_{i,j} - \sum t_{j,i}$ (see Figure 4 in Appendix H).
- If $\sum t_{i,j} = \sum t_{j,i}$ then there is no connection between p_i and p_j i.e. $w_{i,j} = w_{j,i} = 0$. By extension, $w_{i,i} = 0$ for all $i \in [n]$.
- Constructing such a graph might lead to a cycle (e.g. when p_1 transfers to p_2, p_2 transfers to p_3 and p_3 transfers to p_1). In such cases, a cycle-elimination procedure converts the graph to a Directed Acyclic Graph (DAG).

5.2 C-NORM: Quantifying Centralization in a PoS Blockchain System

We remark that most existing centralization metrics fail to capture either the collusion of players or the valuation of a player while calculating the centralization metric. A system is decentralized if[5] the stake held by each player is proportional to their system valuation. We propose a new metric for measuring centralization in a PoS System. Our metric uses PSG, $\mathcal{G}$ of $\mathcal{B}$. First, we calculate the *effective stake* of a player – capturing the net stake and the transaction value between the player and its neighbors in $\mathcal{G}$. Considering $nbr(i)$ to be the set of vertices adjacent to i, the effective stake ω_i of player p_i is calculated as: $\omega_i := c_i + \sum_{j \in nbr(i)} w_{j,i} - \sum_{j \in nbr(i)} w_{i,j}$. *Effective stake per unit of valuation* is denoted by $\frac{\omega_i}{\theta_i}$. For each $p_i \in P$, the normalized effective stake is called *scaled stake*, $\beta_i(\theta) := \frac{\omega_i/\theta_i}{\sum_{j\in[n]}\left(\omega_j/\theta_j\right)}$.

Since the allocated stake should be proportional to the reported valuation of each player p_i, $\frac{\omega_i}{\theta_i}$ should be the same for all players. For an IC mechanism Π, we should ideally have $\frac{\omega_i}{\theta_i} = \frac{\omega_j}{\theta_j}\ \forall\ i,j \in [n]$. Thus, the scaled stake should have the same value for each player in the PoS system for the system to be fully decentralized. Upon calculation, we find that β_i should (in the ideal case) be $\frac{1}{n}$. Thus, for any player p_i, the "error" is the deviation of their scaled stake from this target value (in a decentralized system) of $\frac{1}{n}$. Hence, we define our metric for measuring centralization as the summation of L_1-Norm of this deviation for each player. The normalization factor $\frac{1}{2}$ maps the range of Ω to $[0, 1]$. Formally,

Definition 5 (C-Norm (Ω)). *For a PoS system with player set P, PoS system graph G the C-Norm of the system $\Omega : [n] \times C \times W \to [0,1]$ is defined over $\boldsymbol{\theta}$ as $\Omega(\boldsymbol{\theta}) := \frac{1}{2}\sum_{j=1}^{[n]}\left|\beta_j(\boldsymbol{\theta}) - \frac{1}{n}\right|$. The centralization of the system in the worst-case is $\Omega^\star$ as:*

$$\Omega^\star := \max_{\boldsymbol{\theta}|\theta_i>0\forall i\in[n]} \frac{1}{2}\sum_{j=1}^{[n]}\left|\beta_j(\theta) - \frac{1}{n}\right| \tag{7}$$

Note. While constructing the PSG $\mathcal{G}$, the order of elimination of cycles using the `CycleElimination` Algorithm (see Appendix H) has no effect on the value of C-NORM. This is because the difference between $\sum_{j\in Nbr(i)} t_{i,j} - \sum_{j\in Nbr(i)} t_{j,i}$ remains the same and therefore ω_i, and by extension, $\Omega^\star$ does not change.

[5] this notion of decentralization follows from the idea of proportional inceitive towards security (incentive to maintain security in PoS for any player is proportional to their valuation of the system). It has not been proven or discussed if this notion of valuation-proportional stake is necessary, but it is sufficient.

$\Gamma_{\mathsf{cent}} = \langle \{M_C, M_D\}, S_{SA}, e_r, Q(\cdot), \kappa \rangle$

Metric Descriptor (M_C)**:**

❶ Samples $s_0 \in S_{SA}$ and sets $s_1 := e_r(s_0)$ such that $(s_0, s_1) \in S_{SA} \times S_{NSA}$.
❷ Chooses $(a, b) \in_R \{(0, 1), (1, 0)\}$ and communicates (s_a, s_b) to M_D.

Metric Challenger (M_D)**:**

① Evaluates $v_a := Q(s_a)$ and $v_b := Q(s_b)$.
② Distinguishes between v_a, v_b to get (a', b') using any program $\mathcal{D}$ by $(a', b') \leftarrow \mathcal{D}(v_a, v_b)$.

Success Probability: Consider a random variable $D(Q)$, that takes value 1 if M_D successfully guesses (a, b) i.e. $a' = a,\ b' = b$ and 0 otherwise. For $\kappa \in \mathbb{Z}_{\geq 1}$ trials of Γ_{cent}, we have $D_\kappa(Q) = 1$ if all κ trials are successful. M_D's success depends on the centralization metric it employs. We have,

Ineffective Metric: If $Q(\cdot)$ is an ineffective metric for quantifying centralization, success probability will be as good as a random guess across κ trials. Formally, for κ trials

$$\Pr(D_\kappa(Q) = 1) \leq \mathsf{negl}(\kappa)$$

Where $\mathsf{negl}(\kappa)$ is a negligible function in κ.

Effective Metric: If $Q(\cdot)$ is an effective metric, then M_D can distinguish between (s_0, s_1) and (s_1, s_0) with very high probability. Formally, $\forall \mathsf{negl}(\kappa)$

$$Pr(D_\kappa(Q) = 1) > 1 - \mathsf{negl}(\kappa)$$

Figure 1: The Centralization Game

Need for C-Norm: C-NORM has certain advantages: (i) while other metrics evaluate centralization based on each player's stake, C-NORM include player's *valuation* of the system, therefore defining effective stake. (ii) While other metrics use the system's current state, C-NORM uses previous state changes (transactions) via $\mathcal{F}$. Next, we formally argue why the proposed metric is good at capturing centralization in a PoS System.

5.3 Evaluating Decentralization Metrics

We introduce a novel *centralization game* to assess the efficacy of a given centralization metric for a PoS System. We illustrate with examples that widely used metrics (discussed in Section 3) namely Gini coefficient [20,21] (G_c), Nakamoto Coefficient [28,58] (N) and Entropy-based metrics [36,63] (H) fail to capture centralization in the proposed game. A strategic player can create instances where metrics fail to detect centralization, whereas C-NORM detects them. Next, we also show that any PoS System bootstrapped using an IC Π and a small C-NORM satisfies $(\tau, \delta, \epsilon)-$decentralization (Definition 3).

Centralization Game ($\boldsymbol{\Gamma_{cent}}$). The game has two players – Metric Descriptor M_D and Metric Challenger M_C. There are two types of PoS System. First, S_{SA}, which are centralized systems, with players (part of the PoS System) launching Sybil attacks to make them appear decentralized. It means S_{SA} is a set of PSGs which are DAGs with at least one directed edge (having non-negligible weight). Second, S_{NSA} are decentralized systems without Sybil attack. Additionally, there exists an onto function $e_r : S_{SA} \longrightarrow S_{NSA}$ which removes edges from the PSG $\mathcal{G}$ for the given $s_0 \in S_{SA}$. The Game is repeated for $\kappa \in \mathbb{Z}_{\geq 1}$ trials. At any trial, M_C gives randomly shuffled samplings $s_0 \in S_{SA}$ and $s_1 = e_r(s_0)$. M_D uses its centralization metric under analysis $Q(\cdot)$ to find the centralization value for both s_0 and s_1 and uses these values as inputs to any program $\mathcal{D}$ to report the ordering which was chosen by M_C. M_D is successful if it correctly guesses the ordering for all κ trials. We use $\Gamma_{cent} := \langle \{M_C, M_D\}, S_{SA}, S_{NSA}, e_r, Q(\cdot), \kappa \rangle$ to refer to this centralization game. Figure 1 formally defines Γ_{cent}.

Analyzing Centralization Metrics in Γ_{cent}. Towards this, we first discuss the sampling (say) (s_0, s_1) by M_C and then calculate the values $Q(s_0)$ and $Q(s_1)$ for different metrics in Table 2. We then argue why any program $\mathcal{D}$ cannot distinguish between s_0 and s_1 for other metrics except for C-NORM.

Centralization Metric	PoS Systems	
	s_0	s_1
Nakamoto Coefficient (N) [40]	3	3
Entropy (H) [63]	0.1405	0.1405
Gini Coefficient (G) [21]	0.0804	0.0804
C-NORM ($\Omega^\star$)	0.6	0

Table 2: Scores of existing centralization metrics compared with C-NORM distinguishing between centralized (S_{SA}) and decentralized (S_{NSA}) PoS systems (refer Example 1).

Example 1 (Analysing centralization metrics using Γ_{cent}) Consider the following steps.

- Step ❶. Consider s_0 such that the player set $P = \{p_1, p_2, \dots, p_7\}$ each currently holds stake $C = \{2, 5, 5, 5, 5, 5, 5\}$ and private valuation $\boldsymbol{\theta} = \{2, 5, 5, 5, 5, 5, 5\}$. However, there has been a redistribution of stake among players where p_1 has distributed a stake of 5 to both p_2 and p_3, which means there is a directed edge from p_1 to both p_2 and p_3 with weight 5 each. The state $s_1 = e_r(s_0)$ is the same set P and C without any edges between nodes.
- Step ❷. M_C now samples randomly $(a, b) \in_R \{(0, 1), (1, 0)\}$ and sends (s_a, s_b) to M_D. The reported valuation of each player is the same (proportional) to their allocated stake.
- Steps ① & ②. Based on the metric being used by M_D, it calculates $Q(s_a)$ and $Q(s_b)$. Now, if both values are different (w.l.o.g., $Q(s_a) > Q(s_b)$) then $s_a \in S_{SA}$ and thus $(a, b) = (1, 0)$. However, if $Q(s_a) = Q(s_b)$[6] then M_D cannot distinguish between s_a, s_b (using metric $Q(\cdot)$) better than a random guess. Without loss of generality, considering $s_a = s_1$ and $s_b = s_0$, we tabulate the values $Q(s_a)$ and $Q(s_b)$ for different centralization metrics – Gini Coefficient G_c (Eq. 2), Nakamoto Coefficient S_N (Eq. 3), Entropy H (Eq. 1) and C-NORM $\Omega^\star$ (Eq. 7) in Table 2.

Note that with Example 1, we show scenarios where C-NORM captures the centralization while the existing metrics fail to do so. With Theorem 1, we show that C-NORM is able to distinguish between $s_0 \in S_{SA}$ and $s_1 \in S_{NSA}$ for any $s_0 \in S_{SA}$ and $s_1 = e_r(s_0)$ with probability $1 - \mathsf{negl}(\kappa)$ for κ trials. We show this by constructing a distinguisher $D_\kappa(\cdot)$ using centralization measure C-NORM which distinguishes between any $s_0 \in S_{SA}$ and corresponding $s_1 \in S_{NSA}$. The proof is provided in Appendix A. Example 1 and this result together show that C-NORM is an effective centralization metric.

Theorem 1. *In $\Gamma_{cent}\langle\{M_C, M_D\}, S_{SA}, e_r, \Omega^\star, \kappa\rangle$, for any (s_0, s_1) chosen by M_C from the set $\{(s_0, s_1) : s_0 \in S_{SA}, s_1 = e_r(s_0)\}$, if M_D uses metric C-NORM ($\Omega^\star$) then $Pr(D_\kappa(\Omega^\star) = 1) > 1 - \mathsf{negl}(\kappa)$ for some negligible function $\mathsf{negl}(\kappa)$. Here, S_{SA} is the set of all Directed Acyclic Graphs with at least one edge with non-negligible weight.*

We observe as a corollary of Theorem 1 that C-NORM ($\Omega^\star$) also provides *Sybil-proofness* because it detects any attempts of Sybil-attack and reflects it through a change in the value of $\Omega^\star$.

We next show how C-NORM fits into the description of an ideal bootstrapping protocol. Towards this, in Theorem 2, we quantify decentralization (according to Definition 3) if we measure centralization using C-NORM $\Omega^\star$ of a PoS System with an IC bootstrapping protocol Π provided $\Omega^\star$ is small. The proof is in Appendix B. Note that the theorem provides sufficient (not necessary) conditions for the protocol to be $(\tau, \delta, \epsilon)-$decentralized.

Theorem 2. *If a PoS System bootstrapped using an Incentive-Compatible (IC) protocol Π and has C-NORM value $\Omega_1^\star \leq \alpha$, then the system is $(\tau, \delta, \varepsilon)$-Decentralized for any $\delta \in [0, 100]$ and $\varepsilon = \frac{2\alpha}{\boldsymbol{\beta}_\delta}$.*

Having introduced ideal bootstrapping and a centralization metric, we now analyze some of the widely used bootstrapping protocols for IC, IR, and decentralization properties.

[6] E.g., if the metric does not account for transaction history (represented through edges in $\mathcal{G}$) which might represent stake-redistribution among colluding parties

6 Analysis of Bootstrapping Protocols

In this section, we (i) prove why *Airdrop* and *Proof-of-Burn* are not Ideal Bootstrapping protocols. (ii) formally show that a PoW-based variant (abbreviated as W2SB) is an Ideal bootstrapping protocol.

6.1 Airdrop & Proof-of-Burn

Airdrop and PoB are protocols widely employed in Blockchain space [6,7,52,10] in different capacities including bootstrapping of protocols. For Airdrop and Proof-of-Burn based bootstrapping to be ideal, these protocols must satisfy all properties outlined in Definition 4. Based on this, in Claim 1, we show that Airdrop is not an ideal bootstrapping protocol as it is not IC.

Claim 1 *An Airdrop-based bootstrapping protocol is not IC.*

We defer the proof to Appendix C which uses the property of airdrop that launching a Sybil attack does not affect utility as it does not increase Ω. It is because pseudo-identities have (1) no on-chain transactions to establish a relationship with the player launching the Sybil attack and (2) no additional cost in creating additional identities; thus, the collusion is undetected. Furthermore, to show that Proof-of-Burn (PoB) is not an ideal bootstrapping protocol, Claim 2 proves that it does not satisfy IR.

Claim 2 *A Proof-of-Burn-based bootstrapping protocol is not IR.*

For the proof, refer to Appendix D, we show that a PoB bootstrapped cryptocurrency will always be upward-pegged (also referred to as one-way pegging [48]). Thus, a player's maximum utility from PoB bootstrapping in expectation is less than the utility from abstaining from the protocol. Motivated by the switch of Ethereum from PoW to PoS [14], we next discuss the potential of PoW as a bootstrapping protocol.

6.2 W2SB: PoW-based Bootstrapping

Proof-of-Work (PoW) is a promising choice for a bootstrapping protocol as it offers Sybil resistance by design (Section 3.1). PoW involves solving a cryptographic puzzle to mine (propose) a block. Let r_{b} be the reward obtained by the miner[7] on successfully solving the puzzle. We consider that each miner $p_i \in P$ invests some computational resource (aka. mining power). Consider m_i be the mining power if the invested cost is according to their true valuation (i.e. m_i is mining power when $\hat{\theta}_i = \theta_i$). The total mining power when all miners $p_i \in P$ report their true valuation is $M = \sum_{i\in[n]} m_i$. The cost incurred per unit of mining power in a round is χ in expectation. For IC, we require p_i gets a higher reward with mining power m_i (corresponding to $\hat{\theta}_i = \theta_i$) than with $m_i + a$ (corresponding to $\hat{\theta}_i > \theta_i$) or $m_i - a$ (corresponding to $\hat{\theta}_i < \theta_i$).

W2SB: IC and IR. We abstract out a Proof-of-Work based bootstrapping protocol which runs for a specified number of rounds (say T) and satisfies conditions stated in Lemma 1 as ***W**ork **to** **S**take **B**ootstrap* (W2SB). We show that W2SB is an Ideal Bootstrapping Protocol. Towards this, we first show with Lemma 1 that W2SB is both IC and IR (given some conditions on χ, r_{b} and M).

Lemma 1. *W2SB satisfies IC and IR if (1)* $\frac{\chi\cdot M}{r_b} \leq 1$ *and (2)* $\frac{\chi\cdot M}{r_b} \geq (1 - \frac{m_{\min}}{M})$ *for* $m_{\min} = \min_{i\in[n]} m_i$.

Appendix E presents the formal proof. In the proof, for IR, we show that the expected utility of any miner, in a single round, is greater than or equal to the utility of abstaining if $\frac{\chi\cdot M}{r_{\mathrm{b}}} \leq 1$. Next, for IC, we show that eliciting $\hat{\theta}_i < \theta_i$ and $> \theta_i$ both gives a lower utility when $\frac{\chi\cdot M}{r_{\mathrm{b}}} \geq (1 - \frac{m_{\min}}{M})$.

Note. Condition (1) in Lemma 1 is a natural requirement for PoW and states that the mining difficulty must be such that the mining cost does not exceed the expected reward from mining. On the other hand, condition (2) requires that for any set of valuations $\boldsymbol{\theta}$, there does not exist a miner who is incentivized to increase its mining power. We remark that these are mild requirements and can be satisfied by changing χ, which depends on the difficulty of the cryptographic puzzle (a tunable parameter in PoW/W2SB).

[7] We refer to the strategic players as miners here, as miners may be a more accessible term for PoW-based bootstrapping.

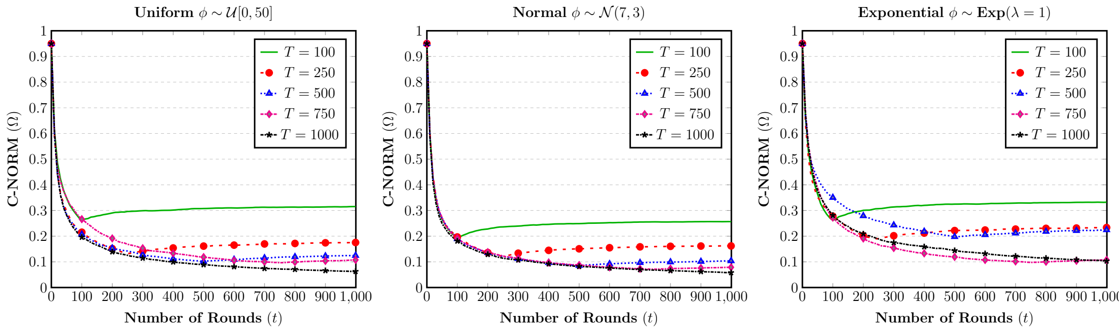


Figure 2: C-NORM against rounds for different stopping time T for different arrival distributions.

W2SB: Decentralization. To show that W2SB is decentralized, we show the existence of a finite T for an arbitrary $z \in \mathbb{R}_{>0}$ such that if W2SB is run for T rounds, $\Omega^\star < z$ We assume the dynamic participation of miners is according to an arbitrary distribution $J \leftarrow \mathcal{Z}(\mu, \sigma)$. The CDF ($\Psi$) is defined over non-negative integers $\Psi : \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$. Likewise, the PMF($\psi$) is also defined over the set of non-negative integers $\psi : \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ and made discrete using the PDF f as $\psi(J = q) = \int_{q-1}^{q} f(J = x)dx$. Under this setting, Theorem 3 proves that for every $z \in (0, 1]$, there exists a finite T such that if we run W2SB for T rounds, we get $\Omega^\star \leq z$. We prove this by first upper bounding $\Omega^\star$ for a given round T. Then, we show that $\exists T$ for every z such that $\Omega^\star \leq z$. Proof is in Appendix F.

Theorem 3. *In W2SB with miners arriving dynamically, given an arbitrary $z \in (0, 1]$, there always exists a finite T such that after $\geq T$ rounds, we have $\Omega^\star \leq z$.*

From Theorem 2 and Theorem 3, we see that that W2SB satisfies $(\tau, \delta, \epsilon)-$ Decentralization if it is run for T rounds.

Corollary 1. *W2SB on running for finite rounds is $(\tau, \delta, \epsilon)-$ Decentralized given miners arrive dynamically according to some distribution with CDF $\Psi(\cdot)$.*

Having shown that W2SB satisfies IR and IC (under some conditions) and is $(\tau, \delta, \epsilon)-$decentralized if run for T rounds, we conclude in Theorem 4 that W2SB is an ideal bootstrapping protocol.

Theorem 4. *W2SB is an* ideal bootstrapping protocol *for* $(1 - \frac{m_{\min}}{M}) \leq \frac{\chi M}{r_b} \leq 1$, *where* $m_{\min} = \min_{i \in [n]} m_i$.

Proof. Lemma 1 implies IC and IR, and Corollary 1 implies $(\tau, \delta, \epsilon)-$Decentralization. Hence, W2SB is Ideal Bootstrapping Protocol by Definition 4

7 W2SB: Experiments & Discussion

We now study the empirical change in C-NORM with a change in the number of rounds, T. From Theorem 3, we know that W2SB reaches an arbitrary level of decentralization (reflected by a decrease in C-NORM) for a sufficient T. Our experiments aim to quantify C-NORM in a PoS system when W2SB is run for different values of T. We begin by explaining our experimental setup, followed by the results and their discussion.

7.1 Experimental Setup.

We simulate a PoS-based blockchain bootstrapped using W2SB. The hyperparameters include (1) stopping time T and (2) distribution followed by the dynamically arriving players and (3) distribution of private valuations for the PoS system.

Stopping time T. To empirically measure C-NORM, we run W2SB for different stopping times $T \in \{100, 200, 500, 750, 1000\}$, after which the PoS protocol is run for remaining $(1000 - T)$ rounds.

δ	Stopping Round(T)		
	$\phi \sim \mathcal{N}(7,3)$	$\phi \sim \mathcal{U}[0,50]$	$\phi \sim \mathbf{Exp}(\lambda = 1)$
0.4	21	25	44
0.3	35	44	88
0.2	82	95	223
0.1	350	393	> 1000

Table 3: T values for varying δ.

Dynamic Arrival. To capture each participant i's dynamic arrival, we define the random variable $\mathcal{J}_{i,t}$, which takes the value 1 if i joins the system at round t and 0 otherwise. We model $\mathcal{J}_{i,t} \sim Chi(k = 3)$ from a chi-squared distribution with degree of freedom $k = 3$. We believe this distribution aptly exhibits participant arrival: sudden initial increase peaking close to the start, followed by a gradual decrease and long tail.

Private valuation. Each player's mining power is proportional to their private valuation (Lemma 1). We simulate three different instances where each p_i samples its private valuation ϕ_i (proportional to θ_i) from (1) Gaussian $\phi \sim \mathcal{N}(7,3)$, (2) Uniform $\phi \sim \mathcal{U}(0,50)$, and (3) Exponential $\phi \sim \mathbf{Exp}(\lambda = 1)$ distributions. We remark that the general trend presented remains similar for different distribution parameters (refer Appendix G).

7.2 Results & Inference.

Figure 2 depicts our results. We make the following key observations.

1. **In W2SB $\Omega^\star \to 0$ as $t \to \infty$.** From Figure 2, we observe that if the W2SB runs for a sufficiently large T, then C-NORM tends to zero, i.e., $\Omega^\star \to 0$.
2. **C-NORM does not decrease after Bootstrapping.** We observe that for rounds $> T$, C-NORM saturates to a fixed value. This is because the PoS protocol does not cause any change in C-NORM of the protocol, as desired.
3. **W2SB achieves $\Omega^\star \le z$ for any $z > 0$.** Any z can be achieved in a finite number of rounds in W2SB, as $\Omega^\star$ tends to 0 asymptotically. The smaller value of z, the larger number of rounds required. E.g., the green curve in Figure 2 with small T is relatively centralized.

Discussion. Our results (both theoretical and empirical) show that W2SB is an Ideal bootstrapping protocol that achieves sufficiently small C-NORM values. The number of rounds for which W2SB is run (T) is a hyper-parameter that is decided by protocol descriptor, allowing a tradeoff between higher levels of decentralization (by increasing T) and lower energy consumption (by decreasing T).

Ethereum Merge – an instance of W2SB. Ethereum also used PoW initially before switching to PoS (aka the Merge [14]). Although the intention of the Merge might not have been decentralized stake distribution, the consequence was that Ethereum became a decentralized PoS-based blockchain.

8 Conclusion & Future Work

Conclusion. This work attempted to resolve the problem of centralization during bootstrapping of PoS-based blockchains. Towards this, we first presented a game-theoretic model of bootstrapping, $\Gamma_{\mathsf{bootstrap}}$. With this, we defined an ideal bootstrapping protocol, i.e., a protocol that simultaneously satisfies IR, IC, and decentralization. To quantify centralization, we introduced C-NORM which measures centralization in PoS-based blockchains. We show the effectiveness of C-NORM against existing metrics, using the centralization game, Γ_{cent}. We then analyzed existing protocols under our model to show that while Airdrop and Proof-of-Burn are not IC and IR, respectively, PoW-based bootstrapping (W2SB) is an Ideal bootstrapping protocol. Our work lays the theoretical foundations for further analysis of PoS-based blockchains.

Future Work. Decentralized bootstrapping in PoS-based blockchains is relatively new. One potential future direction is to explore verifiable random functions [43] for greater energy efficiency than W2SB. Another challenge with PoS-based blockchains is post-bootstrapping centralization due to stake-pools. Tackling post-bootstrapping threats to decentralization may be interesting and is left for future work.

References

1. Coinmarketcap. coinmarketcap.com/ (2023)
2. Alkalay-Houlihan, C., Shah, N.: The pure price of anarchy of pool block withholding attacks in bitcoin mining. In: AAAI. pp. 1724–1731 (2019)
3. de Andres, P., Arroyo, D., Correia, R., Rezola, Á.: Challenges of the market for initial coin offerings. International Review of Financial Analysis (2021)
4. Azouvi, S., Maller, M., Meiklejohn, S.: Egalitarian society or benevolent dictatorship: The state of cryptocurrency governance. In: Financial Cryptography Workshops (2018)
5. Becker, R., D'Angelo, G., Gilbert, H.: Maximizing influence-based group shapley centrality. In: AAMAS. p. 1461–1463 (2021)
6. Bitcoinwhoswho: 2 btc burned in 2018 (Dec 2018)
7. BitcoinWiki: Proof of burn (Jan 2018)
8. Buterin, V., et al.: Ethereum white paper
9. Castro, M., Liskov, B.: Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation. p. 173–186. OSDI '99, USENIX Association, USA (1999)
10. Chong, J.A.: Opendao airdrops sos on opensea community (May 2023)
11. Chung, H., Shi, E.: Foundations of transaction fee mechanism design. In: ACM-SIAM Symposium on Discrete Algorithms (SODA). pp. 3856–3899 (2023)
12. David, B.M., Gazi, P., Kiayias, A., Russell, A.: Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In: International Conference on the Theory and Application of Cryptographic Techniques (2018)
13. Douceur, J.R.: The sybil attack. In: International Workshop on Peer-to-Peer Systems (2002)
14. Ethereum: The merge (Oct 2022), ethereum.org/en/upgrades/merge/
15. Fan, S., Min, T., Wu, X., Cai, W.: Altruistic and profit-oriented: Making sense of roles in web3 community from airdrop perspective. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23, Association for Computing Machinery, New York, NY, USA (2023)
16. Foundation, I.: Icon blockchain, https://docs.icon.foundation/ICON-Whitepaper-EN-Draft.pdf
17. Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: Analysis and applications. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015. pp. 281–310. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
18. Gervais, A., Karame, G.O., Capkun, V., Capkun, S.: Is bitcoin a decentralized currency? IEEE S&P **12**, 54–60 (2014)
19. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N.: Algorand: Scaling byzantine agreements for cryptocurrencies. Symposium on Operating Systems Principles pp. 51–68 (2017)
20. Gini, C.: Measurement of inequality of incomes. The Economic Journal **31**, 124 (1921)
21. Gochhayat, S.P., Shetty, S., Mukkamala, R., Foytik, P., Kamhoua, G.A., Njilla, L.: Measuring decentrality in blockchain based systems. IEEE Access **8**, 178372–178390 (2020)
22. Goodman, L.M.: Tezos : A self-amending crypto-ledger position paper (2014)
23. Grossi, D.: Social choice around the block: On the computational social choice of blockchain. In: AAMAS. p. 1788–1793 (2022)
24. Guo, Z., Gao, Z., Mei, H., Zhao, M., Yang, J.: Design and optimization for storage mechanism of the public blockchain based on redundant residual number system. IEEE Access **7**, 98546–98554 (2019)
25. Harrigan, M., Shi, L., Illum, J.: Airdrops and privacy: A case study in cross-blockchain analysis. In: 2018 IEEE International Conference on Data Mining Workshops (ICDMW). pp. 63–70 (2018)
26. Istrate, G., Bonchis, C.: Being central on the cheap: Stability in heterogeneous multiagent centrality games. In: AAMAS. p. 651–659 (2022)
27. Istrate, G., Bonchis, C., Gatina, C.: It's not whom you know, it's what you, or your friends, can do: Coalitional frameworks for network centralities. In: AAMAS. p. 566–574 (2020)
28. Jia, Y., Xu, C., Wu, Z., Feng, Z., Chen, Y., Yang, S.: Measuring decentralization in emerging public blockchains. In: 2022 International Wireless Communications and Mobile Computing (IWCMC). pp. 137–141 (2022)
29. Johnston, D.A., Thorsen, M., Liu, H., Kuebler, E., Torrellas, G.: The smartdrop model: How to bootstrap dapps and protocols without an ico (Jul 2018), djohnstonec.medium.com/the-smartdrop-model-859888916d94
30. Kapengut, E., Mizrach, B.: An event study of the ethereum transition to proof-of-stake. Commodities **2**(2), 96–110 (2023)
31. Karakostas, D., Kiayias, A., Zacharias, T.: Blockchain nash dynamics and the pursuit of compliance. In: Proceedings of the 4th ACM Conference on Advances in Financial Technologies. p. 281–293. AFT '22, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3558535.3559781, https://doi.org/10.1145/3558535.3559781

32. Karantias, K., Kiayias, A., Zindros, D.: Proof-of-burn. In: Financial Cryptography and Data Security. p. 523–540 (2020)
33. Kim, J.Y., Lee, J., Koo, Y., Park, S., Moon, S.M.: Ethanos: Efficient bootstrapping for full nodes on account-based blockchain. In: EuroSys. p. 99–113 (2021)
34. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., Ford, B.: Omniledger: A secure, scale-out, decentralized ledger via sharding. IEEE S&P pp. 583–598 (2018)
35. Kosny, W., Skibski, O.: Axiomatic analysis of medial centrality measures. In: AAMAS. p. 2188–2196 (2023)
36. Kusmierz, B., Overko, R.: How centralized is decentralized? comparison of wealth distribution in coins and tokens. In: IEEE International Conference on Omni-layer Intelligent Systems (COINS). pp. 1–6 (2022)
37. Kwon, J., Buchman, E.: Internet of blockchains, `v1.cosmos.network/resources/whitepaper`
38. Kwon, Y., Liu, J., Kim, M., Song, D., Kim, Y.: Impossibility of full decentralization in permissionless blockchains. In: ACM Conference on Advances in Financial Technologies. p. 110–123 (2019)
39. Leung, D., Suhl, A., Gilad, Y., Zeldovich, N.: Vault: Fast bootstrapping for the algorand cryptocurrency. In: NDSS (2019)
40. Lin, Q., Li, C., Zhao, X., Chen, X.: Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities. In: International Conference on Data Engineering Workshops (ICDEW). pp. 80–87 (2021)
41. Liu, Z., Zhu, H.: Fighting sybils in airdrops. ArXiv **abs/2209.04603** (2022)
42. Mazalov, V.V., Avrachenkov, K.E., Trukhina, L.I., Tsynguev, B.T.: Game-theoretic centrality measures for weighted graphs. Fundam. Informaticae **145**, 341–358 (2016)
43. Micali, S., Rabin, M.O., Vadhan, S.P.: Verifiable random functions. 40th Annual Symposium on Foundations of Computer Science pp. 120–130 (1999)
44. Momtaz, P.P.: Initial coin offerings. PLoS ONE **15** (2020)
45. Nakamoto, S.: Bitcoin : A peer-to-peer electronic cash system (2009)
46. Nambiampurath, R.: Polygon receives criticism as it completes hard fork with only 13 validators (Jan 2023), `https://www.investopedia.com/polygon-receives-criticism-after-hard-fork-7096331`
47. Narayanam, R., Narahari, Y.: A shapley value-based approach to discover influential nodes in social networks. IEEE Transactions on Automation Science and Engineering **8**, 130–147 (2011)
48. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and cryptocurrency technologies: A comprehensive introduction (2016)
49. Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., Ibañez, J.I.: The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: International Conference on Software Quality, Reliability and Security Companion (QRS-C). pp. 1135–1144 (2021)
50. Raman, R.K., Varshney, L.R.: Coding for scalable blockchains via dynamic distributed storage. IEEE/ACM Trans. Netw. p. 2588–2601 (dec 2021)
51. Rauchs, M., Hileman, G.: Global cryptocurrency benchmarking study (2017)
52. Redman, J.: Gas dao project forms to airdrop tokens to ethereum users that spent $1,559 in fees (Dec 2021)
53. Roughgarden, T.: Transaction fee mechanism design for the ethereum blockchain: An economic analysis of eip-1559. arXiv preprint arXiv:2012.00854 (2020)
54. Roughgarden, T.: Transaction fee mechanism design. ACM SIGecom Exchanges **19**(1), 52–55 (2021)
55. Sai, A.R., Buckley, J., Fitzgerald, B., Gear, A.L.: Taxonomy of centralization in public blockchain systems: A systematic literature review. Inf. Process. Manag. **58**, 102584 (2021)
56. Sandor, K., Genc, E.: The fall of terra: A timeline of the meteoric rise and crash of ust and luna (Dec 2022)
57. Schout, G.: Centralization of stake in pos (Apr 2020), `medium.com/stakin/centralization-of-stake-in-pos-f7ccb8f8254`
58. Srinivasan, B.S.: Quantifying decentralization (Jul 2017), `https://news.earn.com/quantifying-decentralization-e39db233c28e`
59. Sultanik, E., Remie, A., Manzano, F., Brunson, T., Moelius, S., Kilmer, S., Myers, M., Amir, T., Schriner, S.: Are blockchains decentralized? unintended centralities in distributed ledgers. Trail of Bits (2022)
60. Waniek, M., Woźnica, J., Zhou, K., Vorobeychik, Y., Rahwan, T., Michalak, T.P.: Strategic evasion of centrality measures. In: AAMAS. p. 1389–1397 (2021)
61. Wąs, T., Waniek, M., Rahwan, T., Michalak, T.: The manipulability of centrality measures-an axiomatic approach. In: AAMAS. p. 1467–1475 (2020)
62. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper **151**, 1–32 (2014)
63. Wu, K., Peng, B., Xie, H., Huang, Z.: An information entropy method to quantify the degrees of decentralization for blockchain systems. International Conference on Electronics Information and Emergency Communication (ICEIEC) pp. 1–6 (2019)
64. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials **22**, 1432–1465 (2020)
65. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Comput. Surv. (jul 2019)

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

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

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 $1 - \mathsf{negl}(\kappa)$.

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,

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

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

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

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

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

For Nash Incentive Compatibility (IC) from Equation 6 of Definition 2 we require $\forall\, \hat{\theta}_i \in \mathbb{R}_{\geq 0}, \forall\, A_i \in \mathcal{A}_i$

$$\begin{aligned} U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i) \geq& \quad U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \boldsymbol{\theta}) \\ b_{airdrop} \cdot \mathbf{1}_{\hat{\theta}_i > 0} - \Omega^\star \cdot g(\theta_i) \geq& \quad b_{airdrop} \cdot \sum_{j \in A_i} \mathbf{1}_{\hat{\theta}_j > 0} - \Omega^\star \cdot g(\theta_i) \end{aligned}$$

We therefore observe that by forging identities (Sybil-attack) which is equivalent to forming a coalition A_i 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 [48] 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 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.

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

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

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

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 $\forall p_i \in P$

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

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, that is $\mathbb{E}[U_i(\hat{\theta}_i, \boldsymbol{\theta}_{-i}, A_i, \emptyset; \theta_i) - U_i(\theta_i, \boldsymbol{\theta}_{-i}, \emptyset, \emptyset; \theta_i)]$ is therefore given by

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

The last inequality comes from the condition obtained from Individual Rationality $\chi M \leq r_\mathrm{b}$.

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,

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

Now, we can write the expected difference in utility as

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

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

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

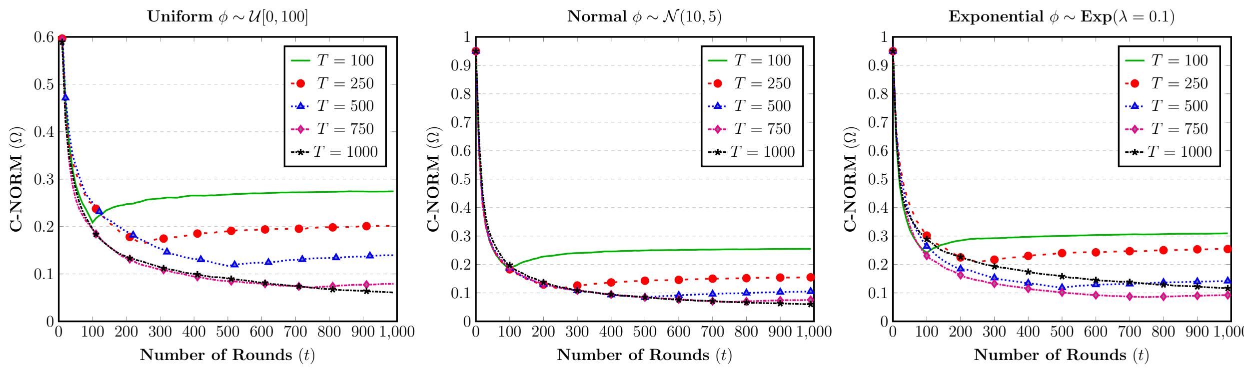


Figure 3: C-NORM against rounds for different T and different distributions of miner stake

F Proof for Theorem 3

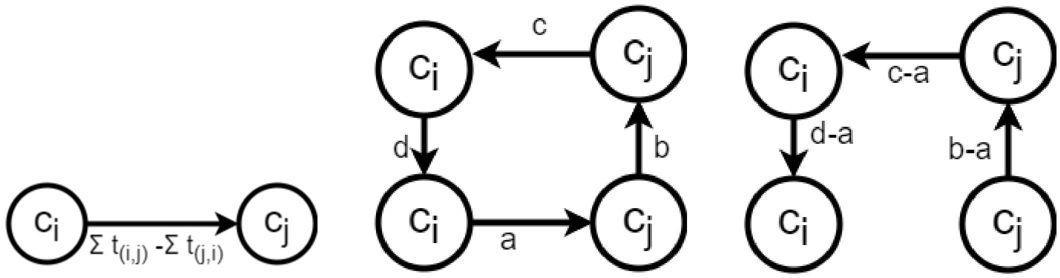
Proof. To prove the theorem, we run the W2SB for T rounds. We show that for any arbitrary desired value $z \in (0, 1)$ there always exists T such that after T rounds, $\Omega^{\star} \leq z$. Out of these T rounds, the first $T_0 < T$ rounds are such that the majority of players have joined the system 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

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

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 $T_0 r_{\mathrm{b}}$. Therefore, we use the inequality $\omega_i/\theta_i \leq T_0 + \omega_i^{'}/\theta_i$ to upper bound the numerator. (2) $\omega_j/\theta_j \geq \omega_j^{'}/\theta_j \geq$



(a) Edges (b) With cycles (c) Eliminated Cycle

Figure 4: PoS System graph and cycle elimination.

$(T-T_0)\chi$ since W2SB is IR means $\frac{\theta_i r_\mathrm{b}}{\sum_{j=1}^{n}\theta_j} \geq \chi$ 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

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

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 $c = r_\mathrm{b}/M \approx \chi/n$ (for very small m_{min}, see Lemma 1). Therefore,

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

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 3 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.

Algorithm 1 `CycleElimination` procedure

```
Input: 𝒢 = (P, 𝒞, 𝒲)                    ▷ PoS System Graph (might contain cycles)
Output: 𝒢′                               ▷ Directed Acyclic PoS System Graph
for each cycle (p_1, p_2, ..., p_k) do
    w_min := ∞
    for each p_i, p_j in the cycle do
        w_min = min(w_min, w_{i,j})
    for each p_i, p_j in the cycle do
        w_{i,j} = w_{i,j} − w_min
Updated weight set is 𝒲′
𝒢′ := (P, 𝒞, 𝒲′)
Return 𝒢′
```