Impossibility of Full Decentralization in Permissionless Blockchains

Yujin Kwon*, Jian Liu†, Minjeong Kim*, Dawn Song†, Yongdae Kim*
*KAIST
{dbwls8724, mjkim9334, yongdaek}@kaist.ac.kr
†University of California, Berkeley
jian.liu@eecs.berkeley.edu, dawnsong@cs.berkeley.edu

***Abstract*—As the first decentralized cryptocurrency, Bitcoin uses *blockchain* technology and *proof-of-work* (PoW) mechanism where nodes spend computing resources and earn rewards in return for spending these resources. This incentive system has attracted many participants. However, at the same time, power has been significantly biased towards a few nodes, called *mining pools*. In addition, poor decentralization appears not only in PoW-based coins but also in coins that adopt other mechanisms such as *proof-of-stake* (PoS) and *delegated proof-of-stake* (DPoS) in which nodes should possess stakes instead of computing resources.**

In this paper, we target this centralization issue. To this end, we first define (m, ε, δ)-*decentralization* as a state that satisfies 1) there are at least m participants running a node and 2) the ratio between the total resource power of nodes run by the richest and δ-th percentile participants is less than or equal to $1 + \varepsilon$. Therefore, when m is sufficiently large, and ε and δ are 0, (m, ε, δ)-decentralization represents *full decentralization*, which is an ideal state. To see if it is possible to achieve good decentralization (with a large value of m and small values of ε and δ), we introduce sufficient conditions for the incentive system of a blockchain to reach (m, ε, δ)-decentralization. Then we find an incentive system satisfying these conditions. Through this incentive system, a blockchain system can reach full decentralization with probability 1, regardless of its consensus protocol. However, to adopt this incentive system, the blockchain system should be able to assign a positive Sybil cost, where the Sybil cost is defined as the difference between the cost for one participant running multiple nodes and the total cost for multiple participants each running one node. On the other hand, we prove that when there is no Sybil cost, the probability of reaching (m, ε, δ)-decentralization is upper bounded by a function of f_δ, where f_δ is the ratio between the resource power of the δ-th percentile and the richest participants, and the value of the upper bound is close to 0 for a small value of f_δ. This result implies that it is almost impossible for a system without Sybil costs to reach good decentralization, considering the current gap between the rich and poor.

To determine the conditions that each system cannot satisfy, we also analyze protocols of all PoW, PoS, and DPoS coins in the top 100 coins according to our conditions. Finally, we conduct data analysis of these coins to validate our theory as well as the result of the protocol analysis.

I. Introduction

Traditional currencies have a centralized structure with a bank as a central authority, and thus there exist several problems such as a single point of failure and corruption. For example, the global financial crisis in 2008 was aggravated by the flawed policies of banks that eventually led to many bank failures, followed by an increase in the distrust of these institutions. With this background, Bitcoin [1], which is the first decentralized digital currency, has received considerable attention. Given that it is a decentralized cryptocurrency, unlike traditional financial systems, there is no organization that controls the system.

To operate the system without any central authority, Bitcoin uses the *blockchain* technology. Blockchain as a public ledger stores transaction history, and nodes record the history on the blockchain by generating blocks through a consensus protocol, which provides a synchronized view among nodes. Bitcoin adopts a consensus protocol using the PoW mechanism in which nodes spend computational power to participate. Moreover, nodes receive coins as rewards in return for spending computational power, and the reward increases with the amount of spent computational power. This incentive system has attracted many participants. However, at the same time, computational power, which represents influence in PoW systems, has been significantly biased toward a few participants (i.e., mining pools) who possess advanced technology and great wealth. As a result, the Bitcoin system has achieved poor decentralization, deviating from its original aim [2]–[4].

Since the success of Bitcoin, many (currently over 1,500) cryptocurrencies have been developed. These cryptocurrencies have attempted to address several drawbacks of Bitcoin, such as low transaction throughput, a significant waste of energy due to the utilization of vast computational power, and poor decentralization. Therefore, some cryptocurrencies use consensus mechanisms different from PoW, such as PoS and DPoS, in which nodes should have a stake instead of a computing resource to participate in the system. While these new consensus mechanisms have addressed several of the drawbacks of Bitcoin, the problem of poor decentralization still remains unsolved. For example, similar to PoW systems, stakes, which represent influence in PoS and DPoS systems, are also significantly biased toward a few participants. This has caused concern for poor decentralization in PoS and DPoS coins, along with a heated debate between PoS and DPoS in terms of decentralization.

Currently, many coins suffer from two problems that degrade the level of decentralization: 1) insufficient number of independent participants because of coalition of participants (e.g., mining pools in PoW systems) and 2) a significantly biased power distribution among them. Therefore, many devel-

opers have attempted to create a good decentralized system [5], [6]. In addition, researchers such as Micali has noted that "incentives are the hardest thing to do" and believe that inappropriate incentive systems may cause blockchain systems to be significantly centralized [7]. This fact implies that it is currently an open problem as to whether we can design an incentive system that allows a system to achieve good or full decentralization.

Full decentralization. In this paper, for the first time, we study when full decentralization can be reached. To this end, we first define (m, ε, δ)-*decentralization* as a state satisfying 1) *the number of participants running nodes in a consensus protocol is not less than* m and 2) *the ratio between effective power of the richest and* δ*-th percentile participants is not greater than* $1 + \varepsilon$*,* where the effective power of a participant represents the total resource power of nodes run by that participant. The case when m is sufficiently large and ε and δ are 0 represents full decentralization in which everyone has the same power. To study if a high level of decentralization is possible, we model a blockchain system (Section III) and then find four sufficient conditions of the incentive system for the blockchain system to *converge in probability* to (m, ε, δ)-decentralization. If there is an incentive system satisfying these four conditions, the blockchain system can reach (m, ε, δ)-decentralization with probability 1, regardless of the underlying consensus protocol. The four conditions are: 1) *nodes with any resource power earn rewards*, 2) *it is not more profitable for participants to delegate their resource power to fewer participants than to run their own nodes*, 3) *it is not more profitable for a participant to run multiple nodes than to run one node*, and 4) *the ratio between the resource power of the richest and* δ*-th percentile nodes converges in probability to a value of less than* $1 + \varepsilon$.

Impossibility. Based on these conditions, we find an incentive system that allows a system to reach full decentralization. *In this incentive system, in order for the third condition to be met, the cost for one participant running multiple nodes should be greater than the total cost for multiple participants each running one node. The difference between the former cost and the latter cost is called a Sybil cost in this paper.* This implies that a system where Sybil costs exist can be fully decentralized with probability 1.

When a system does not have Sybil costs, there is no incentive system that satisfies the four conditions (Section V). More specifically, the probability of reaching (m, ε, δ)-decentralization is upper bounded by a function $G(f_\delta)$ that is close to 0 for a small ratio f_δ between the resource power of the δ-th percentile and the richest participants in the system. This fact implies that the achievement of good decentralization in the system without Sybil costs totally depends on the rich-poor gap in the real world. As such, the larger the rich-poor gap, the closer the probability is to zero. Currently, we recognize that the distribution of wealth in the real world is severely biased, and this wealth inequality is a significant well known problem among economists [8]–[10]. To determine the approximate ratio f_δ in actual systems, we investigate hash rates in Bitcoin and observe that f_0 $(\delta = 0)$ and f_{15} $(\delta = 15)$ are less than 10^{-8} and 1.5×10^{-5}, respectively. In this case, f_0 indicates the ratio between the resource power of the poorest and richest participants. This result supports the fact that, currently, *it is almost impossible for blockchain systems without Sybil costs to achieve good decentralization.*

Unfortunately, it is not yet known how permissionless blockchains that have no *real identity management* can have Sybil costs. Indeed, to the best of our knowledge, all permissionless blockchains do not currently have any Sybil costs. Therefore, considering this fact, we note that currently, it is almost impossible for permissionless blockchains to reach good decentralization. The existence of mechanisms to enforce a Sybil cost in permissionless blockchains is left as an open problem. The solution to this issue would be the key to determining how permissionless blockchains can reach a high level of decentralization.

Protocol analysis in top 100 coins. Next, to find out if what condition each system does not satisfy, we extensively analyze incentive systems of all existing PoW, PoS, and DPoS coins among the top 100 coins in CoinMarketCap [11] according to the four conditions (Section VI). According to this analysis, PoW and PoS systems cannot have both enough participants running nodes and an even power distribution among the participants. However, unlike PoW and PoS coins, DPoS coins can guarantee an even power distribution among a fixed number of participants when Sybil costs exist. Otherwise, if the Sybil costs do not exist, rational participants would run multiple nodes for higher profits. In this case, DPoS systems cannot guarantee that any participant possesses the same power.

Data analysis in top 100 coins. Furthermore, to validate the result of the protocol analysis and our theory, we conduct data analysis for PoW, PoS, and DPoS coins in the top 100 using three metrics: the number of block generators, Gini coefficient, and Shannon entropy (Section VII). Based on this empirical study, we can observe the expected rational behaviors in most existing coins. In addition, we *quantitatively confirm* that the coins do not currently achieve good decentralization. Moreover, interestingly, some DPoS coins are controlled by only two participants who create multiple nodes. As a result, this data analysis not only investigates the actual level of decentralization, but also empirically confirms the analysis results of incentive systems. Finally, we discuss a debate on incentive systems and whether we can relax the conditions for full decentralization (Section VIII).

In summary, our contributions are as follows.

- We formally define (m, ε, δ)-decentralization and find four sufficient conditions of an incentive system.
- We prove that it is almost impossible for a system without a Sybil cost to have a high level of decentralization.
- We analyze incentive systems of existing PoW, PoS, and DPoS coins in the top 100 according to the four

sufficient conditions. This result describes what condition each system does not satisfy.
- Data analysis for these coins validates our theory as well as showing quantitatively that current systems have poor decentralization.

II. Background

A. Blockchain

Blockchain – a distributed ledger shared among disparate users – makes digital transactions possible without a central authority. This great promise has fueled a number of innovations such as cryptocurrencies [1], allowing users to exchange funds by issuing transactions, and smart contracts [12], facilitating the execution of an arbitrary code on top of the blockchain. The issued transactions and smart contracts are validated and recorded on the blockchain by nodes called block generators, which produce a block in a different way depending on the respective consensus protocols.

Blockchains can be roughly classified as: permissionless and permissioned. Permissioned blockchains typically rely on some central authorities for *identity management*, whereas permissionless blockchains require some *Sybil-resistance* mechanisms to make attacks expensive. For example, most of the popular blockchains rely on PoW in which the number of Sybils that an adversary can spawn is limited based on her computing resources. Therefore, for the adversary to execute attacks in the PoW system, she should spend vast computing resources. However, this PoW mechanism results in low transaction throughput and a significant waste of energy [13]. Besides, from the cases of Bitcoin and Ethereum, it is observed that it is difficult for PoW systems to establish good decentralization because the computing resources are largely concentrated in few participants who have enormous capital and advanced technology.

To solve these problems, another mechanism called PoS has been proposed, which limits the adversary's power based on her stakes rather than her computing resource. Therefore, the adversary would have to spend a large stake to be successful in attacks. This mechanism addresses the issues of low transaction throughput and the wastage of energy. However, PoS still undermines decentralization because power would be concentrated in a few participants with considerable wealth, and this concern resulted in the advent of the DPoS mechanism, which deviates from existing permissionless blockchains. This mechanism forgoes the goal of full decentralization and instead is designed for nodes with large wealth to have the same power. This system allows users to delegate their stakes to a small set of nodes called delegates, which further determine the order of the transactions and generate blocks. Unlike PoW and PoS where anyone can generate blocks, DPoS gives the opportunity to only the delegates.

B. Decentralization

Decentralization is an essential factor that should be inherently considered in the design of blockchain systems. Even though people design systems for good decentralization, in practice, we often observe that blockchain systems are highly centralized. Bitcoin and Ethereum, as representative examples, are already well known to be highly centralized in terms of network and mining [4], [14]–[16]. Currently, most of the computational power (or mining power) in these systems is concentrated in only a few nodes, called *mining pool*,[1] where individual miners gather together for mining. This causes concern for not only the level of decentralization, but also the security of systems, because the mining power distribution is critical in terms of security in PoW systems. Note that an individual or organization with over 50% of the entire computational power can attempt double-spending attacks in PoW systems. Moreover, there is *selfish mining* [17] in which an attacker with over 33% power can earn unfairly higher profits at the expense of others.

In general, when a participant has large resource power, his behavior would significantly influence others in the consensus protocol. In other words, the more resources a participant has, the greater his influence on the system. Therefore, the resource power distribution implicitly represents the level of decentralization in the system.

At this point, we can consider the following questions: "What can influential participants do in practice?" and "Can these behaviors harm other nodes?" Firstly, as described above, there are attacks such as double spending and selfish mining, which can be executed by an attacker with over 33% or 50% resource power. These attacks would result in significant financial damage [18]. In addition, in a consensus protocol combined with Practical Byzantine Fault Tolerance (PBFT) [19], a malicious behavior of nodes that possess over 33% resource power can cause the consensus protocol to get into a stuck state. It would certainly be more difficult for such attacks to be executed by colluding with others when the resource power is more evenly distributed. In addition, nodes participating in the consensus protocol verify transactions and generate blocks. More specifically, in the process of generating a block, nodes choose which transactions will be included in the block. Therefore, they can only choose advantageous transactions while ignoring disadvantageous transactions. For example, participants can exclude transactions issued by rivals in the process of generating blocks, and if they possess large power, validation of these transactions would often be delayed because the malicious participant has many opportunities to choose transactions that will be validated. Even though the rivals can also retaliate against them, damage from the retaliation depends on the power gap between the malicious participants and their rivals.

Furthermore, transaction issuers should pay transaction fees including *gas* in blockchain systems, where gas refers to the cost associated with issuing smart contracts. The fees are usually determined by economic interactions [20]. This implies that the fees can depend on the behavior of block generators. For example, if block generators verify only transactions that

[1]More specifically, it refers to a centralized mining pool. Even though there is a decentralized mining pool, given that centralized pools are major pools, hereafter, we will simply call them mining pools.

have fees above a specific amount, the overall transaction fees can increase because users would have to pay a high fee for their transactions to be validated. In other words, some block generators can attempt to increase the transaction fees for higher profits, and when they possess larger resource power, the fees may increase to a larger value. Indeed, we have already experienced and observed a similar situation in the real world when considering oligopoly. Note that companies in oligopolistic industries can control the product price, and they often increase the price.

Meanwhile, in fully decentralized systems, it is significantly difficult for the aforementioned problems to occur. Moreover, the system would certainly be fair to anyone. This spurs the desire to achieve a fully decentralized system. Even though many discussions and attempts have been made to achieve good decentralization, existing systems, except for Bitcoin, Ethereum and Stellar, have rarely been analyzed [4], [21]. In this paper, for the first time, we not only study the possibility of full decentralization but also extensively investigate the existing coins.

III. System Model

In this section, we model a consensus protocol and an incentive system. Moreover, we introduce the notation used throughout this paper (see Table I).

Consensus protocol. A blockchain system has a consensus protocol where player p_i participates and generates blocks by running their own nodes. The set of all nodes in the consensus protocol is denoted by $\mathcal{N}$, and that of nodes run by player p_i is denoted by $\mathcal{N}_{p_i}$. Moreover, we define $\mathcal{P}$ as the set of all players running nodes in the consensus protocol (i.e., $\mathcal{P} = \{p_i | \mathcal{N}_{p_i} \neq \emptyset\}$). Therefore, $|\mathcal{N}|$ is not less than $|\mathcal{P}|$. In particular, if a player has multiple nodes, $|\mathcal{N}|$ would be greater than $|\mathcal{P}|$.

For nodes to join in the consensus protocol, they should possess specific resources, and their influences significantly depend on their resource power. The resource can be computational power and stake in consensus protocols with PoW and PoS mechanisms, respectively. Node $n_i \in \mathcal{N}$ possesses resource power $\alpha_{n_i} (> 0)$. Moreover, we define the vector of resource power for all nodes as follows: $\bar{\boldsymbol{\alpha}} = (\alpha_{n_i})_{n_i \in \mathcal{N}}$. We also denote the resource power owned by player p_i as α_{p_i} and the set of players with positive resource power as $\mathcal{P}_\alpha$ (i.e., $\mathcal{P}_\alpha = \{p_i | \alpha_{p_i} > 0\}$). Here, note that these two sets $\mathcal{P}_\alpha$ and $\mathcal{P}$ can be different because when a player delegates its own power to others, it does not run nodes but possesses the resource power (i.e., the fact that $\alpha_{p_i} > 0$ does not imply that $\mathcal{N}_{p_i} \neq \emptyset$). For clarity, we describe a mining pool as an example. In the pool, there are an operator and workers, where the workers own their resource power but delegate it to the operator without running a full node. Therefore, pool workers belong to $\mathcal{P}_\alpha$ but not $\mathcal{P}$ while the operator belongs to both $\mathcal{P}_\alpha$ and $\mathcal{P}$.

In fact, the influence of player p_i on the consensus protocol depends on the total resource power of the nodes run by the player rather than just its resource power α_{p_i}. Therefore, we define EP_{p_i}, *effective power* of player p_i as $\sum_{n_i \in \mathcal{N}_{p_i}} \alpha_{n_i}$. Again, considering the preceding example of mining pools, the operator's effective power is the sum of the resource power of all pool workers while the workers have zero effective power. The maximum and δ-th percentile of $\{EP_{p_i} | p_i \in \mathcal{P}\}$ are denoted by $EP_{\texttt{max}}$ and EP_δ, respectively, and $\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}$ represents a vector of resource power of the nodes owned by player p_i (i.e., $\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}} = (\alpha_{n_i})_{n_i \in \mathcal{N}_{p_i}}$). Note that $EP_{\texttt{max}}$ and EP_{100} are the same. In addition, we consider the average time to generate one block as a *time unit* in the system. We use the superscript t to express time t. For example, $\alpha_{n_i}^t$ and $\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}$ represent the resource power of node n_i at time t and the vector of resource power possessed by nodes at time t, respectively.

Incentive system. To incentivize players to participate in the consensus protocol, the blockchain system needs to have an incentive system. The incentive system would assign rewards to nodes, depending on their resource power. Here, we define the utility function $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ of the node n_i as the expected net profit per time unit, where $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}$ represents the vector of other nodes' resource power and the net profit indicates earned revenues, which subtracts all costs. Specifically, the utility function $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ of node n_i can be expressed as

$$U_{n_i} = E[R_{n_i} | \bar{\boldsymbol{\alpha}}] = \begin{cases} \sum_{R_{n_i}} R_{n_i} \times \Pr(R_{n_i} | \bar{\boldsymbol{\alpha}}) & \text{if } R_{n_i} \text{ is discrete} \\ \int_{R_{n_i}} R_{n_i} \times \Pr(R_{n_i} | \bar{\boldsymbol{\alpha}}) & \text{else,} \end{cases}$$

where R_{n_i} is a random variable with probability distribution $\Pr(R_{n_i} | \bar{\boldsymbol{\alpha}})$ for a given $\bar{\boldsymbol{\alpha}}$. This equation for U_{n_i} and R_{n_i} indicates that U_{n_i} is the arithmetic mean of the random variable R_{n_i} for given $\bar{\boldsymbol{\alpha}}$. In addition, while function U_{n_i} indicates the expected net profit that node n_i can earn for the time unit, random variable R_{n_i} represents all possible values of the net profit that node n_i can obtain for the time unit. For clarity, we give an example of the Bitcoin system, whereby R_{n_i} and $\Pr(R_{n_i} | \bar{\boldsymbol{\alpha}})$ are defined as:

$$R_{n_i} = \begin{cases} 12.5 \text{ BTC} - c_{n_i} & \text{if } n_i \text{ generates a block} \\ -c_{n_i} & \text{else,} \end{cases}$$

$$\Pr(R_{n_i} = a | \bar{\boldsymbol{\alpha}}) = \begin{cases} \frac{\alpha_{n_i}}{\sum_{n_j \in \mathcal{N}} \alpha_{n_j}} & \text{if } a = 12.5 \text{ BTC} - c_{n_i} \\ 1 - \frac{\alpha_{n_i}}{\sum_{n_j \in \mathcal{N}} \alpha_{n_j}} & \text{else,} \end{cases}$$

where c_{n_i} represents all costs associated with running node n_i during the time unit. This is because a node currently earns 12.5 BTC as the block reward, and the probability of generating a block is proportional to its computing resource. Moreover, R_{n_i} cannot be greater than a constant $R_{\texttt{max}}$, determined in the system. In other words, the system can provide nodes with a limited value of rewards at a given time. Indeed, the reward that a node can receive for a time unit cannot be infinity, and problems such as inflation would occur if the reward is significantly large.

In addition, if nodes can receive more rewards when they have larger resource power, then players would increase their resources by spending a part of the earned profit. In that case, for simplicity, we assume that all players increase their resource power per earned net profit R_{n_i} at rate r every time.

For example, if a node earns a net profit $R_{n_i}^t$ at time t, the node's resource power would increase by $r \cdot R_{n_i}^t$ after time t.

We also define the *Sybil cost function* $C(\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}})$ as an additional cost that a player should pay per time unit to run multiple nodes compared to the total cost of when those nodes are run by different players. The cost $C(\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}})$ would be 0 if $|\mathcal{N}_{p_i}|$ is 1 (i.e., the player p_i runs one node). Moreover, the case where $C(\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}) > 0$ for any set $\mathcal{N}_{p_i}$ such that $|\mathcal{N}_{p_i}| > 1$ indicates that the cost for one player to run $M(>1)$ nodes is always greater than the total cost for M players each running one node. Note that this definition does not just imply that it is expensive to run many nodes, which is usually mentioned as Sybil costs in the consensus protocol [22]. *This function implies that the total cost for running multiple nodes depends on whether one player runs those nodes.*

Finally, we assume that all players are rational. Thus, they act in the system for higher utility. More specifically, if there is a coalition of players in which the members can earn a higher profit, they delegate their power to form such a coalition (formally, it is referred to as a cooperative game). In addition, if it is more profitable for a player to run multiple nodes as opposed to one node, the player would run multiple nodes.

Table I
LIST OF PARAMETERS.

Notation	Definition
p_i	Player of index i
$\mathcal{P}$	The set of players running nodes in the consensus protocol
n_i	Node of index i
$\mathcal{N}$	The set of nodes in the consensus protocol
$\mathcal{N}_{p_i}$	The set of nodes owned by p_i
α_{n_i}, α_{p_i}	The resource power of node n_i and player p_i
$\bar{\boldsymbol{\alpha}}$	The vector of resource power α_{n_i} for all nodes
$\mathcal{P}_\alpha$	The set of players with positive resource power
EP_{p_i}	The effective power of nodes run by p_i
$EP_{\texttt{max}}, EP_\delta$	The maximum and δ-th percentile of effective power of players running nodes
$\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}$	The vector of resource power of nodes run by p_i
$\alpha_{n_i}^t$	The resource power of n_i at time t
$\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}$	The vector of resource power at time t
$\bar{\boldsymbol{\alpha}}_{\boldsymbol{-n_i}}$	The vector of resource power of nodes other than n_i
$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{\boldsymbol{-n_i}})$	Utility function of n_i
R_{n_i}	Random variable for a net reward of n_i per time unit
$R_{\texttt{max}}$	The maximum value of random variable R_{n_i}
r	Increasing rate of resource power per the net profit
$C(\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}})$	Sybil cost function of p_i

IV. CONDITIONS FOR FULL DECENTRALIZATION

In this section, we study when a high level of decentralization can be achieved. To this end, we first formally define (m, ε, δ)-decentralization and introduce the sufficient conditions of an incentive system in blockchain systems to reach (m, ε, δ)-decentralization. Then, based on these conditions, we find an incentive system that allows the system to be fully decentralized.

A. Full Decentralization

The level of decentralization largely depends on two elements: the number of players running nodes in a consensus protocol and the distribution of effective power among the players. In this paper, full decentralization refers to the case where a system satisfies 1) the number of players running nodes is as large as possible and 2) distribution of effective power among the players is even. Therefore, if a system does not satisfy one of these requirements, it cannot have full decentralization. For example, if only two players run nodes with the same resource power, this case only satisfies the second requirement. As another example, a system may have many nodes run by independent players while the resource power is biased toward a few nodes. Then, this case only satisfies the first requirement. Clearly, both of these cases have poor decentralization. Note that, as described in Section II, blockchain systems based on a peer-to-peer network can be manipulated by partial players who possess in excess of 50% or 33% of the effective power. Next, to reflect the level of decentralization, we formally define (m, ε, δ)-decentralization as follows.

Definition IV.1 ((m, ε, δ)-Decentralization)**.** *For $1 \leq m$, $0 \leq \varepsilon$, and $0 \leq \delta \leq 100$, a system is* $\boldsymbol{(m, \varepsilon, \delta)}$***-decentralized*** *if it satisfies the followings:*

1) *The size of $\mathcal{P}$ is not less than m (i.e., $|\mathcal{P}| \geq m$).*
2) *The ratio between the effective power of the richest player, $EP_{\texttt{max}}$, and the δ-th percentile player, EP_δ, is less than or equal to $1 + \varepsilon$ (i.e., $\frac{EP_{\texttt{max}}}{EP_\delta} \leq 1 + \varepsilon$).*

In Def. IV.1, the first requirement indicates that not only there are players that possess resources, but also that at least m players should run their own nodes. In other words, too many players with resources do not combine into one node (i.e., many players do not delegate their resources to others.). Note that delegation decreases the number of players running nodes in the consensus protocol. The second requirement presents an even distribution of effective power among players running nodes. Specifically, for the richest and δ-th percentile players running nodes, the gap between their effective power is small. According to Def. IV.1, it is evident that the greater m and the smaller ε and δ, the higher is the level of decentralization. Therefore, $(m, 0, 0)$-decentralization for a sufficiently large m indicates full decentralization in which there are sufficiently many independent players and everyone has the same power.

B. Sufficient Conditions for Fully Decentralized Systems

Next, we introduce four sufficient conditions of an incentive system to reach (m, ε, δ)-decentralization with probability 1. We first revisit two requirements of (m, ε, δ)-decentralization. For the first requirement in Def. IV.1, the size of $\mathcal{N}$ should be greater than or equal to m because the size of $\mathcal{P}$ is always not greater than that of $\mathcal{N}$. This can be achieved by assigning at least m nodes some rewards, which is represented in Condition 1 (GR-m). In addition, it should not be more profitable for too many players to combine into a few nodes than when they directly run nodes. If such delegating behavior

is more profitable than the one that is not, many players with resource power would delegate their power to a few players, resulting in $|\mathcal{P}| < m$. Condition 2 (ND-m) indicates that it should not be more profitable for nodes run by independent (or different) players to combine into fewer nodes when the number of all players running nodes is not greater than m.

Condition 1 (Give Rewards (GR-m))**.** *At least m nodes should earn net profit. Formally, for any $\bar{\boldsymbol{\alpha}}$, $|\mathcal{N}^+| \geq m$, where*

$$\mathcal{N}^+ = \{n_i \in \mathcal{N} \,|\, U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) > 0\}.$$

This condition states that some players can earn the reward by running a node, and this makes the number of existing nodes equal to or greater than m. Meanwhile, if the system does not give net profit, rational players would not run a node because the system requires a player to possess a specific resource (i.e., $\alpha_{n_i} > 0$) to run a node unlike other peer-to-peer systems such as Tor. Specifically, players should invest their resource power elsewhere for higher profits instead of participating in the consensus protocol where they cannot earn net profit, which is called an opportunity cost [23]. As a result, to reach (m, δ, ϵ)-decentralization, it is also necessary for a system to give net profit to some nodes.

Condition 2 (Non-delegation (ND-m))**.** *Nodes run by different players do not combine into fewer nodes unless the number of all players running nodes is greater than m. Before defining it formally, we denote by $\mathcal{S}^d$ a set of nodes run by different players. In other words, for any $n_i, n_j \in \mathcal{S}^d$, the two players running n_i and n_j are different. We also let s^d denote a proper subset of $\mathcal{S}^d$ such that $|\mathcal{P}(\mathcal{N} \backslash \mathcal{S}^d \cup s^d)| < m$, where*

$$\mathcal{P}(\mathcal{N} \backslash \mathcal{S}^d \cup s^d) = \{p_i \in \mathcal{P} \,|\, \exists n_i \in (\mathcal{N} \backslash \mathcal{S}^d \cup s^d) \text{ s.t. } n_i \in \mathcal{N}_{p_i}\}.$$

Then, for any node set $\mathcal{S}^d$,

$$\sum_{n_i \in \mathcal{S}^d} U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) \geq \max_{\substack{s^d \subsetneq \mathcal{S}^d \\ \bar{\boldsymbol{\alpha}}_{\boldsymbol{d}} \in s^d_\alpha}} \Big\{ \sum_{\alpha_{n_i} \in \bar{\boldsymbol{\alpha}}_{\boldsymbol{d}}} U_{n_i}(\alpha_{n_i}, \boldsymbol{\alpha}^-_{-\boldsymbol{n_i}}(\mathcal{S}^d \backslash s^d)) \Big\}, \quad (1)$$

where,

$$s^d_\alpha = \Big\{ \bar{\boldsymbol{\alpha}}_{\boldsymbol{d}} = (\alpha_{n_i})_{n_i \in s^d} \,\Big|\, \sum_{\alpha_{n_i} \in \bar{\boldsymbol{\alpha}}_{\boldsymbol{d}}} \alpha_{n_i} = \sum_{n_i \in \mathcal{S}_d} \alpha_{n_i} \Big\},$$

and $\boldsymbol{\alpha}^-_{-\boldsymbol{n_i}}(\mathcal{S}^d \backslash s^d) = (\alpha_{n_j})_{n_j \notin \mathcal{S}^d \backslash s^d, n_j \neq n_i}$.

The set $\mathcal{P}(\mathcal{N} \backslash \mathcal{S}^d \cup s^d)$ presents all players running nodes, which do not belong to $\mathcal{S}^d \backslash s^d$. In Eq. (1), the left-hand side represents the total utility of nodes in $\mathcal{S}^d$ that are individually run by different players. Here, note that given that $\mathcal{S}^d \subseteq \mathcal{N}$, $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}$ includes the resource power of the nodes in $\mathcal{S}^d$ except for node n_i. The right-hand side represents the maximum total utility of nodes in s^d when the nodes in $\mathcal{S}^d$ are combined into fewer nodes belonging to s^d by delegation of resource power of players. Note that $|s^d| < |\mathcal{S}^d|$ because $s^d \subsetneq \mathcal{S}^d$. Therefore, Eq. (1) indicates that the utility in the case where multiple players delegate their power to fewer players is not greater than that for the case where the players directly run nodes. As a result, ND-m prevents delegation that makes the number of players running nodes less than m, and the first requirement of (m, ε, δ)-decentralization can be met when GR-m and ND-m holds.

Next, we consider the second requirement in Def. IV.1. One way to achieve an even distribution of effective power among some players is to cause the system to have an even resource power distribution among nodes while each player has only one node. Note that, in this case where each player has only one node, an even distribution of their effective power is equivalent to an even resource power distribution among nodes. Condition 3 (NS-δ) indicates that, for any player with above the δ-th percentile effective power, running multiple nodes is not more profitable than running one node. In addition, to reach a state where the richest and δ-th percentile nodes possess similar resource power, the ratio between the resource power of these two nodes should *converge in probability* to a value of less than $1 + \varepsilon$. This is presented in Condition 4 (ED-(ε, δ)).

Condition 3 (No Sybil nodes (NS-δ))**.** *For any player with effective power not less than EP_δ, participation with multiple nodes is not more profitable than participation with one node. Formally, for any player p_i with effective power $\alpha \geq EP_\delta$,*

$$\max_{\substack{\{\mathcal{N}_{p_i} : |\mathcal{N}_{p_i}| > 1\} \\ \bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}} \in \mathcal{S}^{p_i}_\alpha}} \Big\{ \sum_{\alpha_{n_i} \in \bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}} U_{n_i}\Big(\alpha_{n_i}, \boldsymbol{\alpha}^+_{-\boldsymbol{n_i}}(\mathcal{N}_{p_i})\Big) - C(\bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}) \Big\} \leq U_{n_j}(\alpha_{n_j} = \alpha, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_{p_i}}}), \quad (2)$$

where node $n_j \in \mathcal{N}_{p_i}$, the set $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_{p_i}}} = (\alpha_{n_k})_{n_k \notin \mathcal{N}_{p_i}}$, $\boldsymbol{\alpha}^+_{-\boldsymbol{n_i}}(\mathcal{N}_{p_i}) = \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_{p_i}}} \| (\alpha_{n_k})_{n_k \in \mathcal{N}_{p_i}, n_k \neq n_i}$, and

$$\mathcal{S}^{p_i}_\alpha = \Big\{ \bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}} = (\alpha_{n_i})_{n_i \in \mathcal{N}_{p_i}} \,\Big|\, \sum_{\alpha_{n_i} \in \bar{\boldsymbol{\alpha}}_{\boldsymbol{\mathcal{N}_{p_i}}}} \alpha_{n_i} = \alpha \Big\}.$$

In Eq. (2), the left and right-hand sides represent the maximum utility of the case where a player runs multiple nodes of which the total resource power is α and a utility of the case that he runs only one node n_j with resource power α, respectively. Therefore, Eq. (2) indicates that a player with equal to or greater than the δ-th percentile effective power can earn the maximum utility when he runs one node.

Condition 4 (Even Distribution (ED-(ε, δ)))**.** *The ratio between resource power of the richest and δ-th percentile nodes should* ***converge in probability*** *to a value less than $1 + \varepsilon$. Formally, when $\alpha^t_{\texttt{max}}$ and α^t_δ represent the maximum and δ-th percentile of $\{\alpha^t_{n_i} | n_i \in \mathcal{N}^t\}$, respectively,*

$$\lim_{t \to \infty} \Pr\Big[\frac{\alpha^t_{\texttt{max}}}{\alpha^t_\delta} \leq 1 + \varepsilon \Big] = 1.$$

The above condition indicates that the ratio between the resource power of the richest and δ-th percentile nodes reaches a value of less than $1+\varepsilon$ with probability 1 when enough time is given. Note that $\alpha^t_{n_i}$ changes over time, depending on the behavior of each player. In particular, if it is profitable for a player to increase its effective power, $\alpha^t_{n_i}$ would be a random variable related to $R^t_{n_i}$ because a player reinvests part of its net profit $R^t_{n_i}$ to increase his resource. More specifically, in that case, $\alpha^t_{n_i}$ increases to $\alpha^t_{n_i}+rR^t_{n_i}$ after time t as described in Section III.

As a result, these four conditions can allow blockchain systems to reach (m,ε,δ)-decentralization with probability 1, which is presented in the following theorem.

Theorem IV.1. *For any initial state, a system satisfying GR-m, ND-m, NS-δ, and ED-(ε,δ) converges in probability to (m,ε,δ)-decentralization.*

C. Possibility of Full Decentralization in Blockchain

To determine whether blockchain systems can reach full decentralization, we study the existence of an incentive system that satisfies the four conditions for a sufficiently large m, $\delta=0$, and $\varepsilon=0$. In this section, we provide an example of incentive systems that satisfies the four conditions to achieve full decentralization.

It is also important to increase the total resource power involved in the consensus protocol in terms of security. This is because if the total resource power involved in the consensus protocol is small, an attacker can easily subvert the system. Therefore, to prevent this, we construct $U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ as an increasing function of α_{n_i}, which implies that players continually increase their resource power. In addition, we construct random variable R_{n_i} and its probability $\Pr(R_{n_i}|\bar{\boldsymbol{\alpha}})$ as follows:

$$R_{n_i}=\begin{cases}B_r & \text{if } n_i \text{ generates a block}\\ 0 & \text{else}\end{cases}, \tag{3}$$

$$\Pr(R_{n_i}=a\,|\,\bar{\boldsymbol{\alpha}})=\begin{cases}\frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j\in\mathcal{N}}\sqrt{\alpha_{n_j}}} & \text{if } a=B_r\\ 1-\frac{\sqrt{\alpha_{n_i}}}{\sum_{n_j\in\mathcal{N}}\sqrt{\alpha_{n_j}}} & \text{else}\end{cases}, \tag{4}$$

$$U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})=\frac{B_r\cdot\sqrt{\alpha_{n_i}}}{\sum_{n_j\in\mathcal{N}}\sqrt{\alpha_{n_j}}}, \tag{5}$$

where the superscript t representing time t is omitted for convenience. This incentive system indicates that when a node generates a block, it earns the block reward B_r and the probability to generate a block is proportional to the square root of the node's resource power. Under this setting, we can easily check that the utility function U_{n_i} is a mean of R_{n_i}.

Next, we show that this incentive system satisfies the four conditions. First, the utility satisfies GR-m for any m because it is always positive. ND-m is also satisfied because the below equation is satisfied.

$$\sum_{i=1}^{M}\sqrt{\alpha_{n_i}}>\sqrt{\sum_{i=1}^{M}\alpha_{n_i}}\Leftrightarrow\Big(\sum_{M<i}\sqrt{\alpha_{n_i}}+\sqrt{\sum_{i=1}^{M}\alpha_{n_i}}\Big)\times$$
$$\Big(\sum_{i=1}^{M}\sqrt{\alpha_{n_i}}\Big)>\sqrt{\sum_{i=1}^{M}\alpha_{n_i}}\times\Big(\sum_{M<i}\sqrt{\alpha_{n_i}}+\sum_{i=1}^{M}\sqrt{\alpha_{n_i}}\Big)\Leftrightarrow$$
$$\frac{\sum_{i=1}^{M}\sqrt{\alpha_{n_i}}}{\sum_{M<i}\sqrt{\alpha_{n_i}}+\sum_{i=1}^{M}\sqrt{\alpha_{n_i}}}>\frac{\sqrt{\sum_{i=1}^{M}\alpha_{n_i}}}{\sum_{M<i}\sqrt{\alpha_{n_i}}+\sqrt{\sum_{i=1}^{M}\alpha_{n_i}}}$$
$$\Leftrightarrow\sum_{i=1}^{M}U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})>U_{n_i}\Big(\sum_{i=1}^{M}\alpha_{n_i}\,\Big|\,(\alpha_{n_j})_{j>M}\Big)$$

Thirdly, to make NS-0 true, we can choose a proper Sybil cost function C of Eq. (2), which satisfies the following:

$$\sum_{i=1}^{M}U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})-U_{n_i}\Big(\sum_{i=1}^{M}\alpha_{n_i}\,\Big|\,(\alpha_{n_j})_{j>M}\Big)\le C((\alpha_{n_i})_{i\le M})$$

Under this Sybil cost function, the rational players would run only one node. Finally, to show that this incentive system satisfies ED-$(0,0)$, we use the following theorem, whose proof is presented in Appendix A.

Theorem IV.2. *Assume that R_{n_i} is defined as follows:*

$$R_{n_i}=\begin{cases}f(\bar{\boldsymbol{\alpha}}) & \textit{if } n_i \textit{ generates a block}\\ 0 & \textit{else}\end{cases},$$

where $f:\mathbb{R}^{|\mathcal{N}|}\mapsto\mathbb{R}^+$. Then if $U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ is a strictly increasing function of α_{n_i} and the below equation is satisfied for all $\alpha_{n_i}>\alpha_{n_j}$, ED-$(\varepsilon,\delta)$ is satisfied for all ε and δ.

$$\frac{U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}}<\frac{U_{n_j}(\alpha_{n_j},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_j}})}{\alpha_{n_j}} \tag{6}$$

On the contrary, if $U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ is a strictly increasing function of α_{n_i} and Eq. (6) is not satisfied for all $\alpha_{n_i}>\alpha_{n_j}$, ED-$(\varepsilon,\delta)$ cannot be met for all $0\le\varepsilon<\frac{EP^0_{\max}}{EP^0_\delta}-1$ and $0\le\delta<100$.

The above theorem states that when the utility is a strictly increasing function of α_{n_i} and Eq. (6) is satisfied under the assumption that the block reward is constant for a given $\bar{\boldsymbol{\alpha}}$, an even power distribution is achieved. Meanwhile, if Eq. (6) is not met, the gap between rich and poor nodes cannot be narrowed. Specifically, in the case where $\frac{U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}}$ is constant, the large gap can be continued.[2] Moreover, the gap would widen when $\frac{U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}}$ is a strictly increasing function of α_{n_i}. In fact, here we can consider $\frac{U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}}$ as an increasing rate of resource power of node n_i. Therefore, Eq. (6) indicates that the resource power of a poor node increases faster than that of a rich node.

Now, we describe why the incentive system defined by Eq. (3), (4), and (5) satisfies ED-$(0,0)$. First, Eq. (3) is a form of R_{n_i} described in Thm. IV.2, and Eq. (5) implies that U_{n_i} is a strictly increasing function of α_{n_i}. Therefore, ED-$(0,0)$ is met by Thm. IV.2 because Eq. (5) satisfies Eq. (6)

[2]Formally speaking, the probability to reach an even distribution of resource power among nodes is less than 1, and in Thm. V.3, we will deal with how small the probability is.

for all $\alpha_{n_i} > \alpha_{n_j}$. As a result, the incentive system defined by Eq. (3), (4), and (5) satisfies the four sufficient conditions, *implying that full decentralization is possible under a proper Sybil cost function C*. Moreover, Thm. IV.2 describes the existence of infinitely many incentive systems, which can achieve full decentralization. Interestingly, we find that an incentive scheme similar to this is being considered by the Ethereum foundation, and they also indicated that *real identity management* can be important [5]. This fact is in accordance with our results.

V. Impossibility of Full Decentralization in Permissionless Blockchains

In the previous section, we showed that blockchain systems can be fully decentralized under an appropriate Sybil cost function C, where the Sybil cost represents additional costs for a player running multiple nodes when compared to the total cost for multiple players each running one node. In order for a system to implement the Sybil cost function, we can easily consider real identity management in which a trusted third party (TTP) manages *real identities* of players. When real identity management exists, it is certainly possible to implement the Sybil cost. However, the existence of TTP contradicts the concept of decentralization, and thus we cannot adopt such identity management for a good decentralized system. Currently, it is not yet known how permissionless blockchains where such identity management does not exist can implement the Sybil cost. In fact, many cryptocurrencies are based on permissionless blockchains, and many people want to design permissionless blockchains by their nature. Unfortunately, as far as we know, currently, the Sybil cost function C of all permissionless blockchains is zero. Therefore, considering this fact (i.e., $C = 0$), in this section, we study whether blockchains without Sybil costs can reach good decentralization.

A. Almost Impossible Full Decentralization

To determine if it is possible for a system without a Sybil cost to reach full decentralization, we describe the below theorem for which the proof is presented in Appendix B.

Theorem V.1. *Consider a system without a Sybil cost (i.e., $C = 0$). Then the probability for the system to reach (m, ε, δ)-decentralization is always less than or equal to*

$$\max_{s \in \mathcal{S}} \Pr[\text{System } s \text{ reaches } (m, \varepsilon, \delta)\text{-decentralization}],$$

where $\mathcal{S}$ is the set of all systems satisfying GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0.

GR-$|\mathcal{N}|$ means that all nodes can earn net profit, and satisfaction of both ND-$|\mathcal{P}_\alpha|$ and NS-0 indicates that all players run only one node without delegating. **The above theorem implies that the maximum probability for a system satisfying GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0 to reach (m, ε, δ)-decentralization is equal to the global maximum probability.** Moreover, according to Thm. V.1, there is a system satisfying GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, NS-0, and ED-(ε, δ) *if and only if* there is a system that converges in probability to (m, ε, δ)-decentralization. As a result, it is sufficient to determine the maximum probability for a system satisfying GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0 to reach (m, ε, δ)-decentralization. Therefore, we first find a utility function that satisfies GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0 through the following lemma.

Lemma V.2. *When the Sybil cost function C is zero, GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0 are met if and only if*

$$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = F\Big(\sum_{n_j \in \mathcal{N}} \alpha_{n_j}\Big) \cdot \alpha_{n_i}, \tag{7}$$

where $F : \mathbb{R}^+ \mapsto \mathbb{R}^+$.

This lemma shows that the utility function is linear for given the total resource power of nodes, and players would run one node with their own resource power under this utility (i.e., net profit) because delegation of their resource and running multiple nodes are not more profitable than running one node with their resource power. The proof for this lemma is presented in Appendix C.

Then we consider whether Eq. (7) can satisfy ED-(ε, δ). Note that the fact that ED-(ε, δ) is met means that the probability to reach (m, ε, δ)-decentralization is 1. Therefore, it is sufficient to answer the following question: "What is the probability of a system defined by Eq. (7) to reach (m, ε, δ)-decentralization?" Thm. V.3 states the answer by providing the upper bound of probability. The proof of Thm. V.3 is presented in Appendix D. Before describing the theorem, we introduce several notations. Given that players start to run nodes in the consensus protocol at different times in practice, $\mathcal{P}$ would be different depending on the time. Thus, we use notations $\mathcal{P}^t$ and $\mathcal{P}^t_\delta$ to reflect this, where $\mathcal{P}^t_\delta$ is defined as:

$$\mathcal{P}^t_\delta = \{p_i \in \mathcal{P}^t | EP^t_{p_i} \geq EP^t_\delta\}.$$

In other words, $\mathcal{P}^t_\delta$ indicates the set of all players who possess above the δ-th percentile effective power at time t. Moreover, we define $\alpha_{\texttt{MAX}}$ and f_δ as

$$\alpha_{\texttt{MAX}} = \max\left\{\alpha^{t_i^0}_{p_i} \middle| \, p_i \in \lim_{t\to\infty} \mathcal{P}^t\right\},$$

$$f_\delta = \min\left\{\frac{\alpha^{t^0_{ij}}_{p_i}}{\alpha^{t^0_{ij}}_{p_j}} \middle| \, p_i, p_j \in \lim_{t\to\infty} \mathcal{P}^t_\delta,\, t^0_{ij} = \max\{t^0_i, t^0_j\}\right\},$$

where t^0_i denotes the time at which player p_i starts to participate in a consensus protocol. The parameter $\alpha_{\texttt{MAX}}$ indicates the initial resource power of the richest player among the players who remain in the system for a long time. Moreover, f_δ represents the ratio between the δ-th percentile and largest initial resource power of players who remain in the system for a long time. Considering these notations, we present the below theorem.

Theorem V.3. *When Sybil cost function C is zero, the following holds for any incentive system:*

$$\lim_{t\to\infty} \Pr\left[\frac{EP^t_{\texttt{max}}}{EP^t_\delta} \leq 1 + \varepsilon\right] < G^\varepsilon\left(f_\delta, \frac{rR_{\texttt{max}}}{\alpha_{\texttt{MAX}}}\right), \tag{8}$$

where $\lim_{f_\delta \to 0} G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ *and* $\lim_{\alpha_{MAX} \to \infty} G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ *are 0. Specifically, the function* $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ *is defined as Eq.* (36).

This theorem implies that the probability of reaching (m, ε, δ)-decentralization is less than $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$. Here, note that $rR_{\max}$ represents the maximum resource power that a player can increase for time unit. Given that $\lim_{f_\delta \to 0} G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}}) = 0$, *the upper bound would be smaller when the rich-poor gap in the current state is larger.* In addition, the fact that $\lim_{\alpha_{MAX} \to \infty} G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ implies that the more resource power the richest player possesses than the maximum value that a player can increase for time unit, the smaller the upper bound.

To determine how small $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ is for a small value of f_δ, we adopt a Monte Carlo method. This is because it requires a large complexity to directly compute a value of $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$. Fig. 1 represents the value of $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ in regard to f_δ and ε when $\frac{rR_{\max}}{\alpha_{MAX}}$ is 0.1. Note that $\varepsilon = 0$ means that a state should reach (m, ε, δ)-decentralization in which the effective power of the richest is equal to the δ-th percentile. In addition, the fact $\varepsilon = 9, 99$, and 999 indicates that the effective power of the richest is 10 times, 100 times, and 1000 times the δ-th percentile in (m, ε, δ)-decentralization, respectively.

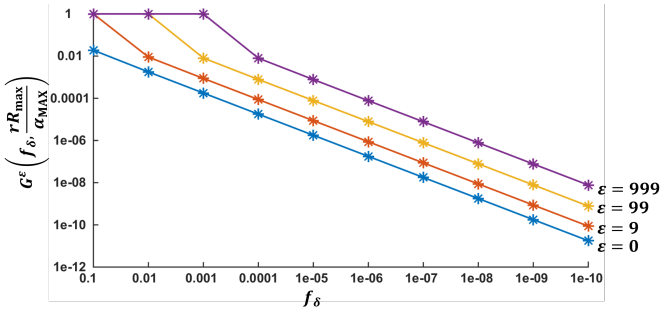


Figure 1. In this figure, when $\frac{rR_{\max}}{\alpha_{MAX}}$ is 0.1, $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ (y-axis) is presented with regard to f_δ (x-axis) and ε.

Fig. 1 shows that the probability to reach (m, ε, δ)-decentralization is smaller when f_δ and ε are smaller. Through Fig. 1, one can see that the value of $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ is significantly small for a small value of f_δ. This result states that the probability to reach good decentralization is close to 0 if there is a large gap between rich and poor and the resource power of the richest is large (i.e., the ratio $\frac{rR_{\max}}{\alpha_{MAX}}$ is not large[3]). The values of $G^\varepsilon(f_\delta, \frac{rR_{\max}}{\alpha_{MAX}})$ when $\frac{rR_{\max}}{\alpha_{MAX}}$ is 10^{-2} and 10^{-4} are represented in Appendix E, and the values are certainly smaller than that presented in Fig. 1.

To determine how small the ratio f_δ is at present, we use the hash rate of all users in the Slush mining pool [24] in Bitcoin as an example. We find miners with hash rate less than 3.061 GH/s and greater than 404.0 PH/s as of the time of writing. Referring to these data, we can see that the ratio f_0 (i.e., the ratio between resource power of the poorest and richest players) is less than about $7.58 \times 10^{-9} (\approx \frac{3.061 \times 10^9}{404.0 \times 10^{15}})$. In addition, we observe that 15-th percentile and 50-th percentile hash rates are less than 5.832 TH/s and 25.33 TH/s, respectively. Therefore, ratio f_{15} and f_{50} are less than approximately 1.44×10^{-5} and 6.27×10^{-5}, respectively. This example indicates that the rich-poor gap is significantly large. Moreover, we observe an upper bound of $\frac{rR_{\max}}{\alpha_{MAX}}$ in the Bitcoin system. Given that the block reward is 12.5 BTC ($\approx \$65,504$), the maximum value of $rR_{\max}$ is approximately 384 TH. This maximum value can be derived, assuming that a player reinvests all earned reward to increase his hash power. Then an upper bound of $\frac{rR_{\max}}{\alpha_{MAX}}$ would be 9.5×10^{-4}, and this value is certainly less than the value of 0.1 used in Fig. 1. **As a result, Thm. V.3 implies that, currently, it is almost impossible for a system without Sybil costs to reach good decentralization.**

[3]The ratio $\frac{rR_{\max}}{\alpha_{MAX}}$ does not need to be small.

B. Intuition and Implication

Here, we describe intuitively why a permissionless blockchain cannot reach good decentralization. In fact, because a player with great wealth can possess more resources, the initial distribution of resource power in a system significantly depends on the distribution of wealth in the real world when the system does not have any constraint of participation and can attract many players. Therefore, if wealth is equally distributed in the real world and many players are incentivized to participate in the consensus protocol, full decentralization can be easily achieved even in permissionless blockchains where anyone can join without any permission process. However, according to many research papers and statistics, the rich-poor gap has been significant in the real world [8]–[10]. In addition, the wealth inequality is well known as one of the most glaring deficiencies in today's capitalism, and resolving this problem is quite difficult.

In the permissionless blockchain, players can freely participate without any restriction, and large wealth inequality would initially appear. Therefore, for the system to have good decentralization, its incentive system should be designed to gradually narrow the rich-poor gap. To this end, we can consider the following incentive system, which gradually narrows the huge rich-poor gap: In the system, nodes receive net profit in proportion to a square root of their resource power on average (e.g., Eq. (5)). In Section IV-C, we have already proved that this incentive system can make the resource power distribution among nodes more even, implying that it satisfies ED-(ε, δ). However, this alone cannot satisfy NS-δ when there is no Sybil cost (i.e., $C = 0$). Therefore, to satisfy NS-δ, we can establish that the expected net profit decreases when the number of existing nodes increases. For example, B_r in Eq. (5) can be a decreasing function of the number of existing nodes. In this case, players with large resources would not run Sybil nodes because when they do so, their utilities decrease by increasing the number of nodes. However, this approach has a side-effect, which leads players to delegate their power to a few players because they can earn higher profits as this rational behavior decreases the number of existing nodes. As a result, the above example intuitively describes that *the four*

conditions are contradictory when the Sybil cost does not exist,[4] and whether the permissionless blockchain can achieve good decentralization completely depends on how wide the gap is between the rich and poor in the real world. This fact is supported by Thm. V.3.

On the other hand, if we can find out how to implement the Sybil costs in permissionless blockchains, which do not have real identity management, we would be able to design the permissionless blockchain reaching good decentralization. We leave this as an open problem.

C. Question and Answer

In this section, to further clarify the implications of our result, we present questions that academic reviewers or blockchain engineers have considered in the past and provide answers to them.

[Q1] "Sybil attacks are when one physical node claims multiple identities but creating more identities does not increase your mining power, so why is this a problem?" Firstly, note that decentralization is significantly related to *real identities*. In other words, when the number of independent players in a system is large and power distribution among them is even, the system has good decentralization. In this paper, we *do not claim* that the more Sybil nodes exist, the lower decentralization level is. We simply assert that a system should be able to know the current power distribution among players to reach good decentralization, and the system without real identity management can know the distribution when each player runs only one node. Moreover, we prove that, to reach good decentralization as much as possible, all players should run only one node (Thm. V.1).

[Q2] "Would a simple puzzle for registering as a block-submitter not be a possible sybil cost, without identity management?" According to the definition of Sybil cost (Section III), the cost to run one node should depend on whether a player runs another node. More specifically, the cost to run one node that a player with other nodes should pay should be more expensive than that for a player with no other nodes. Therefore, the proposed scheme cannot give Sybil cost. Again, note that the Sybil cost described in this paper is different from that usually mentioned in PoW and PoS systems [22].

[Q3] "If mining power is delivered in proportion to the resources one has available (which would be an ideal situation in permissionless systems), achievement of good decentralization is clearly an impossibility. This seems rather self-evident." Naturally, a system would be significantly centralized in the initial state because the rich-poor gap is large in the real world and only a few players may be interested in the system at the early stage. Considering this fact, our work studies *whether there is a mechanism, which causes a system to achieve good decentralization.* Note that our goal is to reduce the gap between the effective power of the rich and poor, not the gap between their resource power. In other words, even if the rich possess significantly large resource power, the decentralization level can be high when the rich participate in the consensus protocol with only part of their resource power and so not large effective power. To this end, we can consider a utility function, which is a decreasing function for a large input (e.g., a concave function). However, this function cannot still achieve good decentralization because it does not satisfy NS-δ. Note that, under a mechanism satisfying the four conditions, a system can *always* reach good decentralization whatever the initial state is. Unfortunately, our result states that there is no mechanism satisfying the four conditions, which implies that the probability to reach good decentralization is less than 1. To make matters worse, Thm. V.3 states that the probability is upper bounded by a value close to 0. *As a result, this implies that it is almost impossible for us to create a system with good decentralization without any Sybil cost, even if enough time is given.*

[Q4] "I think when the rich invest a lot of money in a system, the system can become popular. So, if the large power of the rich is not involved in the system, can it become popular?" In this paper, we focus on the decentralization level in a consensus protocol, which performs a role as a government of systems. Therefore, good decentralization stated in this paper implies a fair government rather than indicating that there is no rich and poor in the entire system. If the rich invest a lot of money in business (e.g., an application based on the smart contract) running on the system instead of the consensus protocol, the system may have a fair government and become popular. Indeed, the efforts to make a fair government also appear in the real world because people are extremely afraid of an unfair system where the rich influence government through a bribe.

VI. Protocol Analysis

In this section, to determine if what condition each system satisfies or not, we extensively analyze the incentive systems of the top 100 coins according to the four conditions. Based on this analysis, we can find out whether each system can have sufficient independent players and the even distribution of effective power among the players. This analysis also describes what each blockchain system needs for good decentralization.

A. Top 100 Coins

Before analyzing the incentive systems based on the four conditions, we classified the top 100 coins in CoinMarketCap [11] according to their consensus protocol. Most of them use one of the following three consensus protocols: PoW, PoS, and DPoS. Specifically, there exist 44 PoW, 22 PoS, and 11 DPoS coins. In addition, there are 15 coins that use other consensus protocols such as Federated Byzantine Agreement (FBA), Proof of Importance, Proof of Stake and Velocity [25], and hybrid. Furthermore, we classify five coins including XRP [26], NEO [27], VeChain [28], Ontology [29], and GoChain [30] into permissioned systems. This is because in these systems, only players that are chosen by the coin

[4]This does not imply the impossibility of full decentralization. It only represents that the probability to reach full decentralization is less than 1.

foundation can run nodes in the consensus protocol. Finally, there exist one token, Huobi Token, and two cryptocurrencies that are non-operational, BitcoinDark and Boscoin. Table II summarizes the classification of top 100 coins described above.

B. Analysis

Next, we analyze the blockchain systems of the top 100 coins according to the four sufficient conditions. In this study, we focus on the analysis of coins using PoW, PoS, and DPoS algorithms, which are major consensus mechanisms of non-permissioned blockchains, to identify which conditions cannot be currently satisfied in each system. If a system satisfies both GR-m and ND-m, we can expect that many players participate in its consensus protocol and run nodes. In addition, if the system satisfies both NS-δ and ED-(ε, δ), the effective power would be more evenly distributed among the players. Table III represents the results of analysis, where the black circle (●), half-filled circle (◐), and empty circle (○) indicate full, partial, and non-satisfaction of the corresponding condition, respectively. In addition, we mark each coin system with a triangle (▲) and an X (✗) when it partially implements and does not implement a Sybil cost, respectively. Here, partial Sybil cost means that multiple nodes run by one player can avoid paying the Sybil cost by pretending that they are run by different players (i.e., players who have different real identities). Note that PoW, PoS, and DPoS coins cannot have perfect Sybil costs because they are non-permissioned blockchains. In fact, it is currently not known how Sybil costs are implemented in blockchain systems without real identity management. We present detailed analysis results in the following sections.

1) Proof of Work: Most PoW systems are designed to give nodes a block reward in proportion to the relative computational power of each node to the total power. In addition, there exist electric bills that are dependent on the computational power and other costs associated with running a node, such as a large memory for storage of blockchain data, which is independent of the computational power. Considering these facts, we can express a utility (i.e., an expected net profit) $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ of node n_i as follows.

$$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = B_r \cdot \frac{\alpha_{n_i}}{\sum_{n_j} \alpha_{n_j}} - c_1 \cdot \alpha_{n_i} - c_2 \quad (9)$$

In Eq. (9), B_r represents the block reward (e.g., 12.5 BTC in the Bitcoin system) that a node can earn for a time unit, and $c_1 (> 0)$ and $c_2 (> 0)$ represent the electric bill per computational power and the other costs needed during the time unit, respectively. In particular, the cost c_2 is independent of the computational power. The values of the three coefficients, B_r, c_1, and c_2, determine whether the four conditions are satisfied.

Firstly, for the system to satisfy GR-m for any m, it should be able to assign rewards to nodes with small computational power. Considering Eq. (9) for appropriate values of B_r, there is $\bar{\boldsymbol{\alpha}} = (\alpha_{n_i})_{n_i \in \mathcal{N}}$ such that $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) > 0$ for all nodes n_i. However, there also exists α_{n_i} such that $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) < 0$ for given $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}$, which implies that the PoW system cannot satisfy GR-m for some m. For example, if $\sum_{n_j} \alpha_{n_j}$ is significantly large and α_{n_i} is small enough, Eq. (9) would be negative because the first term of the right-hand side of Eq. (9) is close to 0.

We can observe this situation in practical PoW systems. In these systems, nodes can generate blocks using CPUs, GPUs, FPGAs, and ASICs, with computational power ranging from low at the CPU level to high at the ASIC level. In particular, the value of c_1 decreases from CPUs to ASICs. In other words, ASICs have better efficiency than the others. Currently, PoW coins can be divided into ASIC-resistant coins and coins that allow ASIC miners. The latter (e.g., Bitcoin and Litecoin) allow miners to use ASIC hardware, which has rapidly increased their total computational power. However, as a side-effect, CPU mining has been unprofitable because the electric bill of CPU miners is larger than their earned rewards. For this reason, several coins such as Ethereum were developed to resist ASIC miners, but ASIC-resistant algorithms cannot be a fundamental solution. These algorithms only prevent the rapid growth of the total computational power; nodes with small computational power can still suffer a loss. For example, even though Ethereum has an ASIC-resistant algorithm, Ethash [119], CPU miners cannot earn net profit by mining Ethereum [120]. Therefore, these PoW coins only partially satisfy GR-m because there exists $\bar{\boldsymbol{\alpha}}$ such that $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) < 0$ for some nodes n_i. As special cases, we consider IOTA and BridgeCoin, where there is no block reward because coin mining does not exist or has already been completed. These systems do not satisfy GR-m at all because the utility U_{n_i} is negative for all $\bar{\boldsymbol{\alpha}}$.

In addition, PoW systems cannot satisfy ND-m. This is because when m players run their own node, they need to pay the additional cost $(m-1) \cdot c_2$, compared to the case in which they run only one node by cooperating with each other. This cooperation is commonly observed as a form of centralized mining pools. Of course, the variance of rewards can decrease when players join the mining pools, which would be another reason that many players join these pools. However, even though there are decentralized pools (e.g., P2Pool [121] and SMARTPOOL [122]) in which players can reduce the variance of rewards and run a full node, most players do not join the decentralized pools due to the cost of running a full node[5].

Meanwhile, for the above reason, the systems can satisfy NS-δ. Finally, ED-(ε, δ) cannot be satisfied in PoW systems. Firstly, Eq. (9) is a strictly increasing function of α_{n_i} for a proper value of $\sum_{n_j} \alpha_{n_j}$ and does not satisfy Eq. (6). Thus, according to Thm. IV.2, ED-(ε, δ) cannot be satisfied for the proper range of $\sum_{n_j} \alpha_{n_j}$. In addition, for a significantly large value of $\sum_{n_j} \alpha_{n_j}$, because all nodes suffer a loss regardless of their resource power, all of them would reduce their resource

[5]One can see that the percentage of resource power possessed by the decentralized pools is significantly small.

Table II
CLASSIFICATION OF TOP 100 COINS (SEP. 11, 2018)

Consensus	Coins	Count
PoW	Bitcoin (1) [1] , Ethereum (2) [12] , Bitcoin Cash (4) [31] , Litecoin (7) [32] , Monero (9) [33] , Dash (10) [34] , IOTA (11) [35] , Ethereum Classic (13) [36] , Dogecoin (18) [37] , Zcash (19) [38] , Bytecoin (21) [39] , Bitcoin Gold (22) [40] , Decred (25) [41] , Bitcoin Diamond (26) [42] , DigiByte (28) [43] , Siacoin (33) [44] , Verge (34) [45] , Metaverse ETP (35) [46] , Bytom (36) [47] , MOAC (43) [48] , Horizen (47) [49] , MonaCoin (51) [50] , Bitcoin Private (52) [51] , ZCoin (56) [52] , Syscoin (60) [53] , Electroneum (61) [54] , Groestlcoin (64) [55] , Bitcoin Interest (67) [56] , Vertcoin (70) [57] , Ravencoin (71) [58] , Namecoin (72) [59] , BridgeCoin (74) [60] , SmartCash (75) [61] , Ubiq (77) [62] , DigitalNote (82) [63] , ZClassic (83) [64] , Burst (85) [65] , Primecoin (86) [66] , Litecoin Cash (90) [67] , Unobtanium (91) [68] , Electra (92) [69] , Pura (96) [70] , Viacoin (97) [71] , Bitcore (100) [72]	44
PoS	Cardano (8) [73] , Tezos (15) [74] , Qtum (24) [75] , Nano (29) [76] , Waves (31) [77] , Stratis (37) [78] , Cryptonex (38) [79] , Ardor (42) [80] , Wanchain (44) [81] , Nxt (50) [82] , PIVX (57) [83] , PRIZM (63) [84] , WhiteCoin (76) [85] , Blocknet (79) [86] , Particl (80) [87] , Neblio (81) [88] , BitBay (87) [89] , GCR (89) [90] , NIX (93) [91] , SaluS (94) [92] , LEO (98) [93] , ION (99) [94]	22
DPoS	EOS (5) [95] , TRON (12) [96] , Lisk (20) [97] , BitShare (27) [98] , Steem (32) [99] , GXChain (48) [100] , Ark (49) [101] , WaykiChain (68) [102] , Achain (84) [103] , Asch (88) [104] , Steem Dollars (95) [99]	11
Others	Stellar (6) [105] , NEM (16) [106] , ICON (30) [107] , Komodo (39) [108] , ReddCoin (40) [25] , Hshare (41) [109] , Nebulas (53) [110] , Emercoin (54) [111] , Elastos (55) [112] , Nexus (58) [113] , Byteball Bytes (59) [114] , Factom (62) [115] , Skycoin (69) [116] , Nexty (66) [117] , Peercoin (73) [118]	15
Permissioned	XRP (3) [26], NEO (14) [27] , VeChain (17) [28] , Ontology (23) [29] , GoChain (65) [30]	5
Token	Huobi Token (45)	1
Not working	BitcoinDark (46) , Boscoin (78)	2

Table III
ANALYSIS OF INCENTIVE SYSTEMS

Coin name	Con 1	Con 2	Con 3	Con 4	N_{apos}	Sybil cost
PoW & PoS coins						
All PoW&PoS†	◐	○	●	○	–	✗
IOTA	○	○	●	●	–	✗
BridgeCoin	○	○	●	●	–	✗
Nano	○	○	●	●	–	✗
Cardano	◐	◐	◐	◐	–	✗
DPoS coins						
EOS	◐	◐	◐⋆	◐	21	▲
TRON	◐	◐	◐⋆	◐	27	▲
Lisk	◐	◐	◐	◐	101	✗
BitShare	◐	◐	◐	◐	27	✗
Steem	◐	◐	◐⋆	◐	20	▲
GXChain	◐	◐	◐	◐	21	✗
Ark	◐	◐	◐	◐	51	✗
WaykiChain	◐	◐	◐	◐	11	✗
Achain	◐	◐	◐	◐	99	✗
Asch	◐	◐	◐	◐	91	✗
Steem Dollars	◐	◐	◐⋆	◐	20	▲

† = except for IOTA, BridgeCoin, Cardano, and Nano; ●= fully satisfies the condition; ◐= partially satisfies the condition; ○= does not satisfy the condition; ▲= has partial Sybil costs; ✗= does not have Sybil costs;

power. Note that this behavior does not affect the power distribution, which represents relative resource power. As a result, PoW systems with the incentive system defined by Eq. (9) cannot satisfy ED-(ε, δ). **Through this analysis of PoW systems, we expect that the current PoW systems neither have sufficient independent players nor an even power distribution among players.**

Meanwhile, IOTA and Bridgecoin, which do not have any incentive, satisfy both NS-δ and ED-(ε, δ) as a trivial case because rational players would not run nodes.

2) Proof of Stake: In PoS systems, nodes receive block rewards in proportion to their stake. Therefore, in these systems, we can express the utility U_{n_i} as follows:

$$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = B_r \cdot \frac{\alpha_{n_i}}{\sum_j \alpha_{n_j}} - c \quad \text{if } \alpha_{n_i} \geq S_b \tag{10}$$

B_r and c in Eq. (10) represent the block reward that a node can earn for a time unit and the cost required to run one node, respectively. S_b indicates the least amount of stakes required to run one node. Therefore, Eq. (10) implies that only nodes with stakes above S_b can be run and earn a reward in proportion to their stake fraction.

Similar to PoW systems, the systems just satisfy GR-m for some m (i.e., partially satisfy GR-m) because there exists a large value of $\sum \alpha_{n_j}$ such that $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) < 0$ in PoS systems. In addition, it is more profitable for multiple players to run one node when compared to running each different node. For example, if a player has a stake below S_b, he cannot earn a reward by running nodes in the consensus protocol. However, he can receive a reward by delegating its stake to others. In addition, if multiple players run only one node, they can reduce the cost required to run nodes. Therefore, PoS systems do not satisfy ND-m. These behaviors are observed through PoS pools [123], [124] or leased PoS [125] in practice. This fact also implies that it is less profitable for one player to run multiple nodes than to run one node; thus, PoS systems satisfy NS-δ. Finally, the system cannot satisfy ED-(ε, δ). To describe the reason, we should consider when B_r is a constant and when it is not, where PIVX [83] belongs to the latter. If B_r is a constant, the utility U_{n_i} is a strictly increasing function of α_{n_i}. Because Eq. (6) is not met, according to Thm. IV.2, this case cannot satisfy ED-(ε, δ). Meanwhile, in the PIVX system, B_r is a decreasing function of $\sum_{n_j} \alpha_{n_j}$ due to the *seesaw effect* [83]. Therefore, for a large value of $\sum_{n_j} \alpha_{n_j}$, nodes earn less rewards compared to the case when $\sum_{n_j} \alpha_{n_j}$ is small. In this case, there is an equilibrium where all nodes reduce their resource power for higher profits, and in addition,

a strategy that allows a state to reach the equilibrium exists. This does not change the power distribution among nodes, which is only related to the relative resource power of the nodes. As a result, PIVX does not satisfy ED-(ε, δ) as well.

As shown in Table III, the results are similar to those for PoW coins. **Therefore, like in PoW coins, PoS coins would have a restricted number of independent players and a biased power distribution among them.** Note that we excluded Wanchain in this analysis because the specifications of its PoS protocol have not been provided yet at the time of writing [126]. Moreover, similar to IOTA and BridgeCoin, Nano does not provide incentives to run nodes. Therefore, the result of Nano is the same with IOTA and BridgeCoin. In addition, Cardano is planning to implement an incentive system different from that of usual PoS systems [6]. The system has a goal that there should be k nodes with similar resource power for given k. In fact, the incentive system has a similar property to DPoS systems, which will be described in the following section.

3) Delegated Proof of Stake: DPoS systems are significantly different from PoW and PoS systems. Unlike these systems, DPoS systems do not give nodes block rewards in proportion to their resource power. Instead, in the DPoS system, stake holders elect block generators through a voting process, where the vote power is in proportion to the stake owned by stake holders (i.e., voters). Then the block generators have the same opportunity to generate blocks and earn the same block rewards. Therefore, when we arrange $\bar{\boldsymbol{\alpha}} = \{\alpha_{n_i} | 1 \leq i \leq n\}$ in descending order, we can express the utility U_{n_i} in DPoS systems as follows:

$$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = \begin{cases} B_r - c & \text{if } i \leq N_{\texttt{dpos}} \\ -c & \text{else} \end{cases}, \tag{11}$$

where B_r is a block reward that a node can earn on average for a time unit, and c represents the cost associated with running one node. In addition, $N_{\texttt{dpos}}$ is a constant number given in the DPoS system. Eq. (11) means that only $N_{\texttt{dpos}}$ nodes with many votes can earn rewards by generating blocks. In fact, not all DPoS systems have the same incentive scheme with Eq. (11). For example, EOS with $N_{\texttt{dpos}} = 21$ gives small rewards to nodes ranked within 100th place [127]. In addition, Steem with $N_{\texttt{dpos}} = 20$ randomly chooses one node, ranked outside the 20th place, as a block generator [99]. Thus, the system also gives small rewards to nodes ranked outside 20th place. In WaykiChain, its incentive system is significantly different from the typical incentive scheme used in DPoS systems because nodes with small votes can also earn non-negligible rewards [128]. Even though incentive systems different from Eq. (11) exist, we describe the analysis result of DPoS coins by focusing on Eq. (11) because their properties are similar.

First, the DPoS system attracts players who can obtain high voting power because it provides them with the block reward. Meanwhile, rational players who are unable to obtain high voting power cannot earn any reward. Therefore, the system partially satisfies GR-m. Moreover, it is rational for multiple players with small stakes to delegate their stakes to one player by voting for him, and this is why this system is called a *delegated* PoS system. Meanwhile, rational players with high stakes would run their own nodes by voting for themselves. For example, if two players have sufficiently high stakes and run two nodes, they can earn a total value of $2(B_r - c)$ as net profit. However, when they run only one node, they earn only $B_r - c$. As a result, it is rational only for players with small stakes to delegate all their resource power to others, and ND-m is partially satisfied.

Next, we consider NS-δ. As described above, a player with small stakes would not run multiple nodes, but instead delegate its stakes to others. However, for a player with high stakes, this is divided into two cases: when weak identity management exists or not. Weak identity management indicates that nodes should reveal their pseudo-identity such as a public URL or social IDs. Firstly, in the latter case, the player with high stakes can earn a higher profit by running multiple nodes because there is no Sybil cost. Therefore, the DPoS system in which identity management does not exist partially satisfies NS-δ because only players with high stakes would run multiple nodes. Meanwhile, when the system has weak identity management, voters can partially recognize whether different nodes are run by the same player. Therefore, the voters can avoid voting for these multiple nodes run by the same player because they may want to achieve good decentralization in the system and recognize that the system can be centralized towards a few players when they vote for the nodes controlled by the same player. This fact makes it not more profitable for one player to run multiple nodes than to run one node (i.e., Sybil costs exist), and these DPoS systems satisfy NS-δ. Note that because the identity management is not perfect, a rich player can still run multiple nodes by *creating multiple pseudo-identities.* Thus, strictly speaking, systems with weak identity management do not still fully satisfy NS-δ. However, because it is certainly more expensive for the rich player to run multiple nodes in systems with weak identity management compared to systems without identity management, we mark such systems with $\mathbf{\mathbb{O}}^{\star}$ for NS-δ in Table III, to distinguish them from systems with no identity management.

Currently, EOS, TRON, Steem, and Steem Dollars have weak identity management. EOS and TRON propose some requirements for a player to register as a delegate, even though the requirements are not official [129]–[131]. The requirements include a public website, technical specifications, and team members, which can be regarded as pseudo-identities. Steem and Steem Dollars provide the information for activities in Steemit [132]–[134]. Note that Steem and Steem Dollars are indeed transacted under the same consensus protocol.

Finally, we examine whether the DPoS system satisfies ED-(ε, δ). To this end, we consider two cases: when a delegate shares the block reward with voters (e.g., TRON [135] and Lisk [136]) and when not sharing (e.g., EOS[6]). In the former

[6]A debate exists as to whether delegates should share their rewards with voters or not. Currently, some delegates have announced that they will share the rewards [137], [138].

case, if a delegator receives V votes, the voters who voted for the delegator can earn reward $\frac{B_r}{V} - f$ per vote in general, where f represents a fee per vote paid to the delegator. Here, note that the larger V is, the smaller is reward the voters earn. Therefore, when voters are biased toward a delegator, some voters could move their vote to other delegators for higher profits. In the latter case, delegators would increase their effective power by voting for themselves with more stakes to maintain or increase their ranking, and Eq. (6) is met in the DPoS system. This allows of a more even power distribution among the delegators. Therefore, in the two cases, the power distribution among delegators can converge to an even distribution. However, the wealth gap between nodes obtaining small voting power and nodes obtaining high voting power would increase, implying that the probability for poor nodes to generate blocks gradually becomes smaller. Consequently, the DPoS system partially satisfies ED-(ε, δ).

Table III represents the analysis result for DPoS coins according to the four conditions. **DPoS systems may potentially ensure the even power distribution among a limited number of players when weak identity management exists. However, the system has a limited number of players running nodes in the consensus protocol, which implies that they cannot have good decentralization.**

VII. Empirical Study

In this section, we extensively collected and quantitatively analyzed the data for PoW, PoS, and DPoS coins not only to measure how much they are currently centralized but also to validate the protocol analysis result and four conditions. Through this study, we empirically observed rational behaviors, such as delegation of resources to a few players and running multiple nodes, which eventually hinder the full decentralization.

A. Methodology

We considered the past 10,000 blocks before Oct. 15, 2018, for PoW and PoS systems and the past 100,000 blocks before Oct. 15, 2018, for DPoS systems, because some DPoS systems do not renew the list of block generators within 10,000 blocks. We parsed addresses of block generators from each blockchain explorer for 68 coins. Because IOTA and Nano are based on DAG technology instead of blockchain technology, the analysis of these two systems will be presented in Section VII-B3.

We determined the number NB_{A_i} of blocks generated by each address A_i, where the set of addresses is denoted by $\mathcal{A}$. Then we constructed a dataset $\mathcal{NB} = \{NB_{A_i} | A_i \in \mathcal{A}\}$ and rearranged $\mathcal{NB}$ and $\mathcal{A}$ in descending order of NB_{A_i}. Then we analyzed the dataset using three metrics, total number of addresses ($|\mathcal{A}|$), Gini coefficient, and entropy (H), where the Gini coefficient is the most commonly used term to measure the wealth distribution in economics. Moreover, in terms of security in blockchain systems, it would be meaningful to analyze how evenly not only the entire power but also 50% and 33% power are distributed because a player who possesses above 50% or 33% power can execute attacks as described in Section II. Therefore, we also measure the level of decentralization for 50% and 33% power in systems using the three metrics. To do this, we first define subset $\mathcal{A}^x$ of the address set $\mathcal{A}$ and subset $\mathcal{NB}^x$ of the data set $\mathcal{NB}$ as follows:

$$\mathcal{A}^x = \Big\{ A_i \in \mathcal{A} \Big| \frac{\sum_{j=1}^{i-1} NB_{A_i}}{\sum_{A_i \in \mathcal{A}} NB_{A_i}} < x \Big\},$$
$$\mathcal{NB}^x = \{ NB_{A_i} | A_i \in \mathcal{A}^x \},$$

where $0 \leq x \leq 1$. Here, note that if x is 0, the two sets are empty, and if x is 1, they are equal to $\mathcal{A}$ and $\mathcal{NB}$, respectively. The Gini coefficient and entropy (H) are then defined as:

$$Gini(\mathcal{NB}^x) = \frac{\sum_{A_i, A_j \in \mathcal{A}^x} |NB_{A_i} - NB_{A_j}|}{2|\mathcal{A}| \sum_{A \in \mathcal{A}^x} NB_{A_i}},$$

$$H(\mathcal{NB}^x) = -\sum_{A_i \in \mathcal{A}^x} \frac{NB_{A_i}}{\sum_{A_i \in \mathcal{A}^x} NB_{A_i}} \log_2 \Big(\frac{NB_{A_i}}{\sum_{A_i \in \mathcal{A}^x} NB_{A_i}} \Big).$$

The Gini coefficient measures the spread of the data set $\mathcal{NB}^x$. If the deviation of $\mathcal{NB}^x$ is small, its value is close to 0. Otherwise, the coefficient is close to 1. The entropy depends on both $|\mathcal{A}^x|$ and Gini. As $|\mathcal{A}^x|$ gets larger and the smaller the Gini coefficient, the entropy is larger. Therefore, entropy implicitly presents the level of decentralization, and large entropy implies a high level of decentralization. In fact, because a player can have multiple addresses, the measured values may not accurately represent the actual level of decentralization. However, since entropy is a concave function of the relative ratio (i.e., $\frac{NB_{A_i}}{\sum_{A_i \in \mathcal{A}^x} NB_{A_i}}$) of NB_{A_i} to the total number of generated blocks, the results show an upper bound of the current level of decentralization. Therefore, if the measured values of entropy are low, the current systems do not have good decentralization.

B. Data Analysis

1) Quantitatively analysis: Tables IV, V, and VI represent the results of PoW, PoS, and DPoS coins, respectively. Coins such as Monero [33], Bytecoin (21) [39], Electroneum [54], DigitalNote [63], and PIVX [83] include *stealth* or *anonymous* addresses that cannot be traced. Therefore, we excluded them in this data analysis. In other words, we conduct data analysis for 39 PoW, 19 PoS, and 10 DPoS coins in this section. In addition, the datasets for certain coins have *too much noise* to find out the actual level of decentralization, because they include *short-lived addresses*, which are used only for a short time and discarded later. We colored these coins in gray in the tables. Moreover, in the case of Cardano and WaykiChain, only trusted nodes are allowed to participate in the protocol at the time of writing, because they have not implemented their public consensus protocols yet [73], [139], [140]. In the tables, we assigned a color of blue to these coins. We do not consider these colored coins when interpreting the results below.

Firstly, one can see that there are not sufficient block generators in PoW, PoS, and DPoS coins. In particular, $|\mathcal{A}^{\frac{1}{2}}|$ and

Table IV
POW COINS

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$\text{Gini}^{\frac{1}{2}}$	$\text{H}^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$\text{Gini}^{\frac{1}{3}}$	$\text{H}^{\frac{1}{3}}$
Bitcoin	62	0.8192	3.89	4	0.1143	1.98	3	0.1103	1.57
Ethereum	65	0.8634	3.38	3	0.1402	1.53	2	0.0415	1.00
Bitcoin Cash	15	0.5729	3.06	3	0.2572	1.51	2	0.0859	0.12
Litecoin	35	0.8094	3.10	3	0.0176	1.58	2	0.0146	1.00
Dash	109	0.9005	3.79	4	0.2050	1.90	2	0.0770	0.98
Ethereum Classic	83	0.8916	3.17	2	0.1538	0.93	1	0	0
Dogecoin	400	0.8686	4.95	4	0.2123	1.89	2	0.1098	0.96
Zcash	75	0.8932	3.36	3	0.0615	1.52	2	0.0546	0.15
Bitcoin Gold	29	0.8585	2.36	1	0	0	1	0	0
Decred	17	0.7751	2.33	2	0.1471	0.35	2	0.1471	0.35
Bitcoin Diamond	16	0.7401	2.44	2	0.0707	0.99	2	0.0707	0.99
DigiByte	125	0.7791	5.09	7	0.2724	2.63	4	0.1879	1.90
Siacoin	1406	0.8582	3.02	2	0.1551	0.98	2	0.1551	0.98
Verge	82	0.7261	4.92	8	0.1762	3.03	5	0.0820	2.46
Metaverse ETP	36	0.7964	3.25	3	0.2914	1.49	2	0.1927	0.97
Bytom	12	0.7978	1.54	1	0	0	1	0	0
MOAC	28	0.7067	3.46	3	0.2330	1.53	2	0.1615	0.98
Horizen	96	0.9109	3.39	3	0.0882	1.56	2	0.0189	1.00
MonaCoin	44	0.8185	3.39	3	0.1373	1.56	2	0.0920	0.99
Bitcoin Private	135	0.8557	4.48	5	0.1260	2.28	3	0.0766	1.57
Zcoin	361	0.9562	1.75	1	0	0	1	0	0
Syscoin	5979	0.2529	10.37	1978	0.5055	6.78	644	0.7571	3.61
Groestlcoin	10	0.4969	2.67	3	0.3408	1.47	2	0.4110	0.45
Bitcoin Interest	19	0.7267	2.66	2	0.3109	0.70	1	0	0
Vertcoin	60	0.8390	3.61	3	0.2639	1.40	2	0.2064	0.87
Ravencoin	71	0.8014	4.12	4	0.2057	1.90	2	0.0488	0.99
Namecoin	3390	0.5693	8.00	49	0.8613	2.52	3	0.1913	1.48
BridgeCoin	1	0	0	1	0	0	1	0	0
SmartCash	7	0.6885	1.47	1	0	0	1	0	0
Ubiq	34	0.8440	2.58	1	0	0	1	0	0
Zclassic	41	0.7762	3.54	3	0.2394	1.43	2	0.0899	0.98
Burst	143	0.9054	3.45	2	0.2473	0.82	1	0	0
Prime	7477	0.2525	10.46	2476	0.5048	6.63	809	0.7565	3.22
Litecoin Cash	33	0.6788	3.78	5	0.0711	2.31	3	0.0557	1.58
Unobtanium	30	0.9463	0.89	1	0	0	1	0	0
Electra	1268	0.6608	8.34	46	0.5262	4.87	12	0.2622	3.53
Pura	19	0.6521	3.08	3	0.0778	1.58	2	0.0905	0.99
Viacoin	33	0.9141	1.78	1	0	0	1	0	0
Bitcore	116	0.9337	3.11	2	0.0956	0.97	2	0.0956	0.97

Table V
POS COINS

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$\text{Gini}^{\frac{1}{2}}$	$\text{H}^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$\text{Gini}^{\frac{1}{3}}$	$\text{H}^{\frac{1}{3}}$
Cardano	7	0.0039	2.81	3	0.0083	2.11	2	0.0111	1.50
Tezos	245	0.8391	5.54	9	0.1061	3.13	6	0.1168	2.55
Qtum	1853	0.7404	8.07	32	0.5923	4.12	7	0.2512	2.69
Waves	110	0.8606	4.24	4	0.1545	1.93	3	0.1628	1.51
Stratis	527	0.8113	6.78	20	0.2626	4.15	10	0.2007	3.23
Cryptonex	122	0.9231	3.30	4	0.0103	2.00	3	0.0078	1.58
Ardor	247	0.8623	4.91	8	0.5376	2.20	6	0.4554	1.95
Nxt	165	0.9150	3.30	2	0.0326	1.00	2	0.0326	1.00
PRIZM	82	0.8672	3.68	4	0.0053	2.00	3	0.0022	1.58
Whitecoin	239	0.6273	6.84	32	0.2954	4.75	15	0.2740	3.71
Blocknet	584	0.7965	6.54	10	0.3891	2.96	4	0.1778	1.92
Particl	1801	0.5989	9.48	141	0.4436	6.56	48	0.3713	5.21
Neblio	1177	0.8258	6.00	5	0.4523	1.74	2	0.3123	0.70
Bitbay	313	0.7839	6.02	9	0.3075	2.94	4	0.0890	1.97
GCR	263	0.8192	5.84	11	0.2515	3.43	6	0.1779	2.68
NIX	1130	0.4520	9.62	255	0.2224	7.86	135	0.2180	6.96
SaluS	27	0.6974	3.41	4	0.1577	1.97	3	0.1342	1.56
Leocoin	879	0.5988	8.72	106	0.3639	6.33	44	0.3268	5.16
ION	287	0.8998	4.24	2	0.0335	1.00	2	0.0335	1.00

Table VI
DPOS COINS

Coin name	100 %			50%			33%		
	$\lvert\mathcal{A}\rvert$	Gini	H	$\lvert\mathcal{A}^{\frac{1}{2}}\rvert$	$\text{Gini}^{\frac{1}{2}}$	$\text{H}^{\frac{1}{2}}$	$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$	$\text{Gini}^{\frac{1}{3}}$	$\text{H}^{\frac{1}{3}}$
EOS	22	0.0447	4.43	11	0.0002	3.46	7	0.0003	2.81
TRON	28	0.0358	4.79	14	0.0009	3.81	9	0.0008	3.17
Lisk	101	0.0023	6.66	51	0.0011	5.67	34	0.0010	5.09
BitShare	27	0.0009	4.75	14	0.0007	3.81	9	0.0003	3.17
Steem	140	0.8324	4.68	11	0.0002	3.46	7	0.0002	2.81
GXChain	21	0.0328	4.39	10	0.0016	3.32	7	0.0013	2.81
Ark	52	0.0200	5.69	25	0.0005	4.64	16	0.0003	4.00
WaykiChain	11	0.1688	3.27	5	0.0021	2.32	4	0.0022	2.00
Achain	99	0.0018	6.63	49	0.0009	5.61	32	0.0008	5.00
Asch	92	0.0769	6.50	42	0.0267	5.39	27	0.0184	4.75

$\lvert\mathcal{A}^{\frac{1}{3}}\rvert$ in PoW and PoS are quite small. However, PoS systems have generally more block generators than PoW systems. This may be because the pool concept is more common in PoW systems. Indeed, most PoS systems are currently in an early stage, and some of them do not have staking pools yet. For example, Qtum does not have staking pools yet at the time of writing and has a relatively large number of block generators compared to others.[7] Certainly, this fact allows the level of decentralization in Qtum to increase. However, we cannot assure that this situation will continue. There have already been some requests for pools and intention to run a business for Qtum staking pools [141]–[144]. When considering this fact, we expect that staking pools would become more popular in PoS systems. Note that Tezos and Waves, already allowing of delegation of stakes, have a smaller number of block generators. PoW protocols also did not originally have a pool concept. However, mining pools have become significantly popular, and most miners currently join mining pools. As a special case, BridgeCoin, which does not satisfy GR-m at all, has only one player. This implies that it cannot attract the participation of players. For the case of DPoS systems, they (except for Steem) have $\lvert\mathcal{A}\rvert$ similar to $N_{\mathtt{dpos}}$. The reason why $\lvert\mathcal{A}\rvert$ in Steem is relatively large when compared to $N_{\mathtt{dpos}} = 20$ is that one block generator is randomly chosen among all nodes as described in Section VI-B3. However, in all DPoS systems, $\lvert\mathcal{A}^{\frac{1}{2}}\rvert$ and $\lvert\mathcal{A}^{\frac{1}{3}}\rvert$ are close to $\frac{N_{\mathtt{dpos}}}{2}$ and $\frac{N_{\mathtt{dpos}}}{3}$, respectively. This indicates that only a small number of players have been block generators even though block generators are frequently elected, implying that the barriers to becoming a block generator are quite high.

Next, we describe the power distribution among nodes. As shown in Tables IV and V, PoW and PoS coins certainly have a high value of Gini, which implies that they have a significantly biased power distribution. Meanwhile, DPoS coins, except for Steem, have a low value of Gini and all DPoS coins have low values of $\text{Gini}^{\frac{1}{2}}$ and $\text{Gini}^{\frac{1}{3}}$. This is because the elected block generators have the same opportunity to generate blocks in DPoS systems. Again, note that in Steem, one block generator

[7]Note that the value of $\lvert\mathcal{A}\rvert$ in Table V does not accurately represent the number of block generators because a player can create multiple addresses.

Table VII
RESOURCE POWER IN DPOS COINS

Coin name	Delegates			100 %			50%			33%		
	$\lvert\mathcal{N}^{\mathrm{D}}\rvert$	$\mathrm{Gini}^{\mathrm{D}}$	H^{D}	$\lvert\mathcal{N}\rvert$	Gini	H	$\lvert\mathcal{N}^{\frac{1}{2}}\rvert$	$\mathrm{Gini}^{\frac{1}{2}}$	$\mathrm{H}^{\frac{1}{2}}$	$\lvert\mathcal{N}^{\frac{1}{3}}\rvert$	$\mathrm{Gini}^{\frac{1}{3}}$	$\mathrm{H}^{\frac{1}{3}}$
EOS	21	0.048	4.39	439	0.846	6.47	28	0.063	4.80	18	0.047	4.16
TRON	27	0.198	4.54	165	0.849	4.84	12	0.258	3.29	6	0.324	2.23
Lisk	101	0.031	6.65	1179	0.907	6.99	52	0.013	5.70	35	0.011	5.13
BitShare	27	0.070	4.74	140	0.550	6.35	21	0.051	4.34	14	0.038	3.80
Steem	20	0.052	4.32	150	0.588	6.37	23	0.061	4.52	15	0.042	3.90
GXChain	21	0.000	4.39	–	–	–	–	–	–	–	–	–
Ark	51	0.053	5.66	196	0.734	5.86	26	0.054	4.69	17	0.055	4.08
WaykiChain	–	–	–	–	–	–	–	–	–	–	–	–
Achain	–	–	–	–	–	–	–	–	–	–	–	–
Asch	91	0.041	6.49	633	0.745	7.63	71	0.028	6.15	46	0.032	5.52

is randomly chosen among all nodes, which makes Gini for *all* block generators in Steem high.

In fact, unlike Table IV and V, Table VI does not represent the resource power of nodes, where the resource power indicates the amount of stakes delegated to each node, because the probability to generate blocks is not proportional to the resource power in DPoS systems. Thus, to present the distribution of resource power among nodes, we analyze the instantaneous amount of stakes delegated to each node through block explorers. Table VII represents the distribution of stakes voted for nodes as of Nov. 19, 2018, where we mark with "–" the values that cannot be determined in the block explorer of the corresponding coin. In particular, the voting process in WaykiChain has not been implemented yet at the time of writing [140].

In Table VII, $|\mathcal{N}^{\mathrm{x}}|$, $\mathrm{Gini}^{\mathrm{x}}$, and H^{x} represent the size of $\mathcal{N}^{\mathrm{x}}$, Gini coefficient, and entropy for $\mathcal{N}^{\mathrm{x}}$, respectively. The *Delegates*, *100%*, *50%*, and *33%* columns present the number of nodes, Gini coefficient, and entropy of delegates ($\mathcal{N}^{D}$), nodes whose total resource power is 100% ($\mathcal{N}$), 50% ($\mathcal{N}^{\frac{1}{2}}$), and 33% ($\mathcal{N}^{\frac{1}{3}}$), respectively. $\mathrm{Gini}^{\mathrm{D}}$ is low in all DPoS systems, indicating that delegates possess similar resource power. In Section VI-B3, we explained that DPoS systems can converge in probability to the state where delegates have similar resource power. Here, the reason why $\mathrm{Gini}^{\mathrm{D}}$ of TRON is relatively high compared to the others is that the node [145] operated by the TRON foundation is ranked in the first place by a relatively large margin. However, we observe that delegates, except for this node, possess almost the same resource power in TRON. On the other hand, the value of Gini for all nodes is high, implying a large gap between the rich and poor. Moreover, Table VII shows that the resource power is significantly biased toward the delegates.

As a result, the quantitative data analysis validates our theory and the analysis result of the incentive systems in Section VI.

2) Multiple nodes run by the same player: In DPoS systems that do not even have weak identity management, a rich player can easily earn a higher profit by running multiple nodes. However, because they do not have any real identity management, it can be difficult to detect this rational behavior in practice. Nevertheless, we show that one player runs multiple nodes in several coins: GXChain, Ark, and Asch.

GXChain. GXChain has 21 delegates in the consensus protocol. We can see the activities of delegates via the official block explorer of GXChain [146], including their creator. As of writing, we observed that two players with `nathan` and `opengate` accounts run 16 and 5 active delegates, respectively. More specifically, `nathan` account created the delegates `aaron`, `caitlin`, `kairos`, `sakura`, `taffy`, `miner1`∼`11`, and `opengate` account created the delegates `hrrs`, `dennis1`, `david12`, `marks-lee`, and `robin-red`. This fact implies that the system is currently controlled by at most only two players.

Ark. We discover that two nodes, `biz_classic` and `biz_private`, are run by the same player. Firstly, we can see that a player who has address `AHsuUuhTNCGCbnPNkwJbeH27E4sDdcnmgp` votes for `biz_classic`, and the delegate `biz_classic` share rewards with the voter by issuing transactions. Because transactions issued in the Ark system include some messages, we were able to observe the following two messages sent from `biz_classic` to the voter [147], [148].

1) You meet the minimum for `biz_private`. Switch for higher payouts.
2) FYI: Change your vote to `biz_private` for higher payouts :)

Therefore, we can speculate that `biz_classic` and `biz_private` are owned by the same player.

Asch. There are 87 active delegates, and we were able to find 30 and 50 delegates with names such as `asch_team_i` and `at i`, respectively, where `i` is replaced by a number. For example, there exist delegate nodes with the names `asch_team_1` or `at5`. Even though these names are quite similar, this is not enough to suspect that these nodes are controlled by the same player. To determine whether the 80 nodes are owned by one player, we investigated their activities.

Firstly, we determine when they became delegates. Based on the transaction history, we can observe that the nodes named `asch_team_1`∼`5` have simultaneously participated in the consensus protocol as delegates since Sep. 11, 2017. Moreover, nodes named `asch_team_6`∼`15` and those named `asch_team_16`∼`35` simultaneously became delegates on Apr. 11, 2018, and Jun. 11, 2018, respectively. In fact, `asch_team_31`∼`35` among these nodes are inactive as of this writing (Oct. 2018). In addition, all 50 nodes named `at i` have become delegators since Jul. 6, 2018 at the same time.

Secondly, all these nodes received 100 XAS (i.e., a unit of Asch coin) from an address just before they became delegates. Even the address, which sent 100 XAS to `asch_team_1`∼`5`, is the same, and addresses for `asch_team_6`∼`15` and `asch_team_16`∼`34` are also the same, respectively. Furthermore, `asch_team_35` and all nodes named `at i` received 100 XAS from the same address. Finally, these 80 nodes sent currencies to the address `GADQ2bozmxjBfYHDQx3uwtpwXmdhafUdkN` almost at the same time on Aug. 20, 2018. As a result, from these

evidences, we speculate that the 80 delegate nodes are run by the same player (or organization).

Summary. In these systems, we were able to observe that one player runs multiple nodes for a higher profit. In particular, GXChain and Asch systems seem to be controlled by only two players and one player, respectively, implying a severely low level of decentralization. In summary, even though DPoS systems can achieve an even power distribution among part of nodes, the even power distribution among nodes does not translate to the players, which implies that the system has a lower level of decentralization than expected.

3) DAG: In this section, we describe the analysis result of IOTA and Nano, which adopt DAG. In IOTA, transaction issuers should validate their transactions by themselves, and currently, there are not enough issuers to stably run IOTA. Therefore, to solve this problem, the IOTA foundation controls the system as a central authority, which implies that IOTA has only one player [149], [150]. This result is in agreement with our protocol analysis in respect that many players do not exist in IOTA. Meanwhile, at the time of writing, even though Nano does not have enough players, there are *relatively* many players compared to IOTA. Specifically, there are 64 players in Nano, and two players possess approximately 45% power, indicating a significantly biased power distribution. This fact is derived referring to the data obtained from a node monitoring website [151]. We see that this situation of Nano is due to incentives outside of the blockchain system. Indeed, we observe that at least 37 players get incentives outside of the blockchain system by participating in the system, and these players possess approximately 80% power.[8] For example, BrainBlocks [152], which provides a platform related to Nano, is incentivized to run nodes in the Nano system for its business, and currently it is a rich player in the Nano system. As a result, in Nano, most players participate in the consensus protocol to receive external incentives, and they possess most resource power. We will discuss more about the external incentive in Section VIII-A.

VIII. Discussion

A. Debate on Incentive Systems

Recently, there was an interesting debate on incentive systems of Algorand [7], [23], [153]. Micali said that incentives are the hardest thing to do and the existing incentivization has led to poor decentralization. Our study supports this fact by proving that it is impossible to design incentive systems in a permissionless blockchain to reach good decentralization.

Then, can we create a permissionless blockchain to achieve good decentralization without any incentive system? The case where the incentive system does not exist represents $U_{n_i} = -c$, where c is the cost associated with running one node. This satisfies the second requirement of Def. IV.1 because NS-δ and ED-(ε, δ) are met as a trivial case. Meanwhile, it cannot satisfy the first two conditions, GR-m and ND-m. As examples, we can consider BridgeCoin, IOTA, and Byteball, which do not have an incentive system and have difficulty in attracting the participation of many players. BridgeCoin has only one player (refer to Table IV), and IOTA is also controlled by one player, the IOTA foundation. Byteball is another system that adopts DAG, and there are only four players. These examples show that blockchain systems with no incentive cannot have enough players.

However, our study considered only incentives inside the system and not incentives outside the system. Therefore, if there exist some incentives that players can get outside the blockchain system, they can participate in the system. For example, in Nano and Stellar, most players run nodes to get external incentives [21], [154], [155]. Note that this fact does not imply that these systems can reach good decentralization. Indeed, both these systems have poor decentralization. In other words, they do not have sufficiently many players and have a biased power distribution. Besides, through these cases, we can empirically see that organizations related to the coin system (e.g., the coin foundation or companies that do business with the coin) control the blockchain system, which may deviate from the philosophy of permissionless blockchains.

B. Relaxation of Conditions from Consensus Protocol

We proved that an incentive system in permissionless blockchains cannot simultaneously satisfy the four conditions. Nevertheless, if there is a consensus protocol that relaxes part of the four conditions, we can expect to be able to design an incentive system to achieve good decentralization. However, it seems to be quite difficult to design such consensus protocols. Here, we explain the reason why the design of consensus protocol relaxing the conditions is difficult by considering two ways to design such protocols: 1) designing non-outsourceable puzzles and 2) finding non-delegable or non-divisible resources.

Non-outsourceable puzzles. There exist several studies on the construction of non-outsourceable puzzles in PoW systems [156]–[159]. In those puzzles, if players outsource the puzzles, their rewards can be stolen. Therefore, this risk can cause a pool manager to refrain from outsourcing its work to pool miners. For example, in the proposed puzzles, if a pool manager outsources the puzzles, when a pool miner finds a valid block, he does not submit the valid block to the pool manager and can steal the block reward.

However, these puzzles still allow other types of mining pools, such as *cloud mining* [160], where individual miners buy hash rate from the service provider, and the provider directly solves PoW puzzles with computing resources gathered by spending the received funds. Miller et al. [158] claimed that they can prevent cloud mining as well, because the cloud service provider can steal block rewards in their protocol. However, with or without non-outsourceable puzzle, the provider can always steal the block reward without any clear evidence. Despite this risk, cloud mining has settled in types of popular mining [161] because cloud miners can reduce the cost of running hardware and nodes. Indeed, there

[8] We were not able to identify all such players because there are untraceable players.

exist several popular cloud mining services [162] such as Genesis Mining [163], HashNest [164] operated by BITMAIN [165], and Bitcoin.com [166]. This situation indicates that the delegation of resource power to part of players would still occur even in non-outsourceable PoW protocols [156]–[159], if profitable. Moreover, the more trust that the company providing the cloud mining service gets from users, the more the cloud service would become popular.

Even in the case of PoS coins, we can empirically see that players would delegate their resources to others for higher profits. One way is to delegate resources through investment in service providers, similar to cloud mining in PoW systems, and it seems to be difficult to prevent this if such a business is profitable. As a result, it would be difficult to make the delegating behaviors disappear by simply modifying the consensus protocol.

Non-delegable/non-divisible resources. Another way to relax the four conditions is to find non-delegable or non-divisible resources. These resources make it impossible for players to delegate their resources to others and run multiple nodes, respectively. Therefore, for each resource, it would be sufficient for the incentive systems to satisfy conditions except for ND-m and NS-δ, to achieve full decentralization.

We can consider reputation as one of such resources. Currently, GoChain uses proof of reputation (PoR) as a consensus algorithm in which nodes should have a high reputation score to participate. In this system, only the company can be a validator, and they believe that PoR can achieve almost full decentralization [30], [167]. Moreover, trust can be one of the non-delegable and non-divisible resources. In the Stellar system, nodes have a trust-based relationship with each other. Specifically, Stellar uses FBA as a consensus algorithm, where nodes configure their quorum slice, which is a set of dependable nodes during a consensus process, according to their trust relation. In addition, Bahri et al. proposed proof of trust (PoT), where more trusted nodes can easily solve puzzles [168]. However, both reputation and trust are not suitable for permissionless blockchains because players would need to know real identities of others. Even though Stellar is classified as a permissionless blockchain, for nodes to be effective validators, they should reveal identities. As a result, it remains an open question to answer as to whether we can find non-delegable or non-divisible resources that are suitable for permissionless blockchains.

IX. Related Work

Attacks. Eyal et al. [17] proposed selfish mining, which an attacker possessing over 33% computing power can execute in PoW-based systems. They mentioned that this attack makes rational miners join the attacker, eventually decreasing the level of decentralization. Eyal [169] and Kwon et al. [170] modeled a game between two pools. When considering block withholding attacks, the game is equivalent to *the prisoner's dilemma*, and the attacks make rational miners leave mining pools, and instead, directly run nodes in a consensus protocol [169]. Contrary to this positive result, a fork after withholding attack between two pools leads to a pool size game where a larger pool can earn extra profits, and thus, the Bitcoin system can be more centralized. Furthermore, two existing works analyzed the Bitcoin system in a transaction-fee regime where transaction fees in block rewards are not negligible [171], [172]. They described that this regime incentivizes large miner coalitions and make a system more centralized.

Analysis. Many papers have already examined centralization in the Bitcoin system. First, Gervais et al. described centralization of the Bitcoin system in terms of various aspects such as services, mining, and incident resolution processes [2]. Miller et al. observed a topology in the Bitcoin network and found that about 2% of high-degree nodes acquire three quarters of the mining power [173]. Moreover, Feld et al. analyzed the Bitcoin network, focusing on its autonomous systems (ASes), and showed that routable peers are concentrated only in a few ASes [174]. Recently, Gencer et al. analyzed the Bitcoin and Ethereum systems in terms of decentralization [4]. Kwon et al. analyzed a game in which two PoW coins with compatible mining algorithm exist [175]. They showed that a fickle mining behavior between two coins can make the decentralization level lower in the less-valued one of the two coins. In addition, Kim et al. analyzed the Stellar system and concluded that the system is significantly centralized [21].

Solutions. There are several works that address the issue of poor decentralization in blockchain systems. Many works [156]–[159] have proposed non-outsourceable puzzles to prevent mining pools from being popular. However, they cannot fully prevent the delegation as described in Section VIII-B. As another solution, Luu et al. proposed an efficient decentralized mining pool, SMARTPOOL, where individual miners who directly run nodes in the consensus protocol can consistently earn profits [122]. However, this does not still incentivize players to run nodes directly (See Section VI-B1). Another work [176] proposed a proof of human-work requiring labor from players with CAPTCHA as a human-work puzzle. Even though, as mentioned by [176], the gap among labor abilities of people is relatively small by their nature, rich players can hire more workers to solve more puzzles. Finally, we are aware of a recent paper [6] in which the authors addressed a similar problem to our paper. Brünjes et al. propose a reward scheme, which makes a system reach a state where k staking pools with similar resource power exist. They assumed our third condition, NS-δ (i.e., all players can run only one node), and thus, it seems difficult for their incentive system to reach good decentralization in practice. As described in previous sections, there is an incentive system that satisfies only GR-m, ND-m, ED-(ε, δ).

X. Conclusion

Developers are facing difficulties in designing blockchain systems to achieve good decentralization. Our study addresses the question of why it is significantly difficult to design a system to achieve good decentralization and proves that good

decentralization is impossible when a system does not have any Sybil costs. More specifically, we prove that when the ratio between the resource power of the poorest and richest is close to 0, the upper bound of the probability that systems without a Sybil cost reach full decentralization is close to 0. This result indicates that if we cannot narrow the gap between the rich and poor in the real world, the level of decentralization in such systems cannot be high forever with a high probability. Furthermore, we extensively analyzed and conducted data analysis on the PoW, PoS, and DPoS coins in top 100 coins. Based on this analysis, we observed rational behaviors that degrade the level of decentralization in most coins, which is in agreement with our theory. In addition, this analysis quantitatively confirm that the current systems do not exhibit good decentralization.

ACKNOWLEDGMENT

We are very grateful to the anonymous reviewers of the earlier version.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," *IEEE security & privacy*, vol. 12, no. 3, pp. 54–60, 2014.
[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Security and Privacy (SP), 2015 IEEE Symposium on*, IEEE, 2015.
[4] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in Bitcoin and Ethereum Networks," 2018.
[5] V. Buterin and G. Weyl, "Liberation Through Radical Decentralization." https://medium.com/@VitalikButerin/liberation-through-radical-decentralization-22fc4bedc2ac, 2018. [Online; accessed 23-Nov-2018].
[6] L. Brünjes, A. Kiayias, E. Koutsoupias, and A.-P. Stouka, "Reward sharing schemes for stake pools," *arXiv preprint arXiv:1807.11218*, 2018.
[7] "No Incentive? Algorand Blockchain Sparks Debate at Cryptography Event." https://www.google.com/amp/s/www.coindesk.com/no-incentive-algorand-blockchain-sparks-debate-cryptography-event/amp/. [Online; accessed 11-Nov-2018].
[8] "Global Inequality." https://inequality.org/facts/global-inequality/, 2018. [Online; accessed 12-Oct-2018].
[9] C. Stone, D. Trisi, A. Sherman, and B. Debot, "A guide to statistics on historical trends in income inequality," *Center on Budget and Policy Priorities*, vol. 26, 2015.
[10] D. Sikorski, "The rich-poor gap: A synopsis," 2015.
[11] "TOP 100 Cryptocurrencies By Market Capitalization." https://coinmarketcap.com/coins/, 2018. [Online; accessed 11-Sep-2018].
[12] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.
[13] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 2014.
[14] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in *Security and Privacy (SP), 2017 IEEE Symposium on*, IEEE, 2017.
[15] J. Song, "Mining Centralization Scenarios." https://medium.com/@jimmysong/mining-centralization-scenarios-b74102adbd36, 2018. [Online; accessed 17-Oct-2018].
[16] B. S. Srinivasan, "Quantifying Decentralization." https://news.earn.com/quantifying-decentralization-e39db233c28e, 2017. [Online; accessed 22-Oct-2018].
[17] I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in *International Conference on Financial Cryptography and Data Security*, Springer, 2014.
[18] "Bitcoin Gold suffers double spend attacks, $17.5 million lost." https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost/, 2018. [Online; accessed 14-Nov-2018].
[19] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999.
[20] "Big transaction fees are a problem for bitcoin — but there could be a solution." https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html. [Online; accessed 13-Nov-2018].
[21] M. Kim, Y. Kwon, and Y. Kim, "Is Stellar As Secure As You Think?," *arXiv preprint arXiv:1904.13302*, 2019.
[22] Dmitrii Zhelezov, "PoW, PoS and DAGs are NOT consensus protocols." https://medium.com/coinmonks/a-primer-on-blockchain-design-89605b287a5a, 2018. [Online; accessed 28-Mar-2019].
[23] A. Gauba and Z. Koticha, "The Need for an Incentive Scheme in Algorand." https://blockchainatberkeley.blog/the-need-for-an-incentive-scheme-in-algorand-6fe9db45f2a7. [Online; accessed 11-Nov-2018].
[24] "SLUSHPOOL." https://slushpool.com/stats/?c=btc, 2018. [Online; accessed 27-Oct-2018].
[25] L. Ren, "Proof of stake velocity: Building the social currency of the digital age," *Self-published white paper*, 2014.
[26] D. Schwartz, N. Youngs, A. Britto, *et al.*, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, 2014.
[27] "Neo White Paper." http://docs.neo.org/en-us/whitepaper.html, 2018.

[28] "Vechain." https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf, 2018. [Online; accessed 25-Oct-2018].
[29] "Ontology White Paper." https://ont.io/documents, 2018. [Online; accessed 30-Sep-2018].
[30] "Gochain." https://gochain.io/gochain-whitepaper-v2.1.2.pdf. [Online; accessed 25-Oct-2018].
[31] "Bitcoin Cash." https://www.bitcoincash.org/, 2018.
[32] "Litecoin." https://litecoin.org/, 2018.
[33] "Monero." https://monero.org/, 2018.
[34] E. Duffield and D. Diaz, "Dash: A privacycentric cryptocurrency," *Self-published*, 2015.
[35] S. Popov, "The tangle," *cit. on*, p. 131, 2016.
[36] E. classic community, "Ethereum Classic Documentation," *Self-published*, 2016.
[37] "Dogecoin." https://dogecoin.com/, 2018.
[38] "ZCASH." https://z.cash/, 2018.
[39] "Bytecoin." https://bytecoin.org/, 2018.
[40] "Bitcoin Gold." https://bitcoingold.org/, 2018.
[41] "Decred." https://www.decred.org/, 2018.
[42] "Bitcoin Diamond." https://btcd.io/, 2018.
[43] "DigiByte." https://www.digibyte.co/digibyte-global-blockchain, 2018.
[44] D. Vorick and L. Champine, "Sia: Simple decentralized storage," *Retrieved May*, vol. 8, p. 2018, 2014.
[45] "VERGE BLACK PAPER." http://vergecurrency.com/static/blackpaper/Verge-Anonymity-Centric-CryptoCurrency.pdf, 2018.
[46] H. Chen, E. Gu, and Y. Jiang, "Metaverse: The New Reality," *Self-published*, 2018.
[47] Bytom, "Bytom An Interoperation Protocol for Diversified Byte Assets," *Self-published*, 2017.
[48] X. Yang, X. D. Chen, and R. Wang, "The MOAC Platform: Advancing Performance with Layered Multi-Blockchain Architecture For Enhanced Smart Contracting," *Self-published*, 2018.
[49] R. Viglione, R. Versluis, and J. Lippencott, "Zen White Paper," *Self-published*, 2017.
[50] "MONACOIN." https://monacoin.org/, 2018.
[51] Bitcoin Private Community, J. Brutman, J. Layton, C. Sulmone, G. Stuto, G. Hopkins, and R. Creighton, "The Revolution of Privacy," *Self-published*, 2018.
[52] "ZCOIN." https://zcoin.io/, 2018.
[53] J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, IEEE, 2017.
[54] "Electroneum's Blockchain and Cryptonote Algorithm Technology." https://electroneum.com/technical-white-paper.pdf, 2018. [Online; accessed 30-Sep-2018].
[55] "GROESTLCOIN." https://www.groestlcoin.org/, 2018. [Online; accessed 30-Sep-2018].
[56] "BITCOIN INTEREST." https://www.bitcoininterest.io/, 2018. [Online; accessed 30-Sep-2018].
[57] "What is Vertcoin?." https://whitepaperdatabase.com/vertcoin-vtc-whitepaper/, 2018.
[58] B. Fenton and T. Black, "Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets," *Self-published*, 2018.
[59] "Namecoin." https://namecoin.org/, 2018. [Online; accessed 30-Sep-2018].
[60] "CryptoBridge." https://crypto-bridge.org/, 2018. [Online; accessed 30-Sep-2018].
[61] "SmartCash White Paper." https://res.tuoluocaijing.cn/20180629162045-7657.pdf, 2018. [Online; accessed 30-Sep-2018].
[62] "UBIQ." https://ubiqsmart.com/, 2018. [Online; accessed 30-Sep-2018].
[63] "DigitalNote." https://digitalnote.biz/whitepaper.pdf, 2015. [Online; accessed 30-Sep-2018].
[64] "Zclassic." https://zclassic.org/pdfs/whitepaper.pdf, 2015. [Online; accessed 30-Sep-2018].
[65] "BURST." https://www.burst-coin.org/, 2018. [Online; accessed 30-Sep-2018].
[66] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," *July 7th*, 2013.
[67] "LITECOIN CASH LTCH." https://litecoin-cash.io/Whitepaper.pdf, 2018. [Online; accessed 30-Sep-2018].
[68] "UNOBTANIUM." http://unobtanium.uno/, 2018. [Online; accessed 30-Sep-2018].
[69] "electra WHITE PAPER." https://cdn.electraproject.org/wp-content/uploads/2018/02/electra-white-paper_1.0.pdf, 2018. [Online; accessed 30-Sep-2018].
[70] "Pura (PURA)-Whitepaper." https://whitepaperdatabase.com/pura-pura-whitepaper/, 2018. [Online; accessed 30-Sep-2018].
[71] "Viacoin Whitepaper." https://media.abnnewswire.net/media/en/docs/91949-Viacoin_whitepaper.pdf, 2017. [Online; accessed 30-Sep-2018].
[72] "BITCORE BTX – White Paper." https://bitcore.cc/white-paper/, 2018. [Online; accessed 30-Sep-2018].
[73] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in *Annual International Cryptology Conference*, Springer, 2017.
[74] L. Goodman, "Tezos—a self-amending crypto-ledger White paper." https://www.tezos.com/static/papers/white_paper.pdf, 2014. [Online; accessed 9-Oct-2018].
[75] P. Dai, N. Mahi, J. Earls, and A. Norta, "Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform." https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf, 2017. [Online; accessed 30-Sep-2018].
[76] C. LeMahieu, "Nano: A feeless distributed cryptocurrency network," *nano. org. Accessed on May*, vol. 3, 2018.
[77] "Waves White Paper." https://blog.wavesplatform.com/waves-whitepaper-164dd6ca6a23, 2016. [Online; accessed 30-Sep-2018].
[78] "STRATIS White Paper." https://stratisplatform.com/files/Stratis_Whitepaper.pdf, 2017. [Online; accessed 30-Sep-2018].
[79] "Cryptonex." https://cryptonex.org/, 2018. [Online; accessed 30-Sep-2018].
[80] "ardor." https://www.ardorplatform.org/, 2018. [Online; accessed 30-Sep-2018].
[81] "WANCHAIN: Building Super Financial Markets for the New Digital Economy." https://www.ardorplatform.org/, 2018. [Online; accessed 30-Sep-2018].
[82] "Nxt Whitepaper." https://www.dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper_v122_rev4.pdf, 2014.
[83] "PIVX WHITE PAPERS." https://pivx.org/white-papers-2/, 2018.
[84] "Prizm Whitepaper." http://prizm.club/wp-content/uploads/2017/10/prizmwhitepaper_english.pdf, 2017.
[85] "The WhiteCoin Foundation Paper." https://www.whitecoin.info/whitecoin-foundation-paper/, 2017.
[86] "THE BLOCKNET DESIGN SPECIFICATION." https://www.blocknet.co/wp-content/uploads/2018/04/whitepaper.pdf, 2018.
[87] "Privacy-focused Decentralized Applications." https://particl.io/, 2018.
[88] "neblio: Next Generation Enterprise Blockchain Solutions." https://nebl.io/wp-content/uploads/2017/07/NeblioWhitepaper.pdf, 2017. [Online; accessed 30-Sep-2018].
[89] "Two Party double deposit trustless escrow in cryptographic networks and BitBay." https://bitbay.market/downloads, 2018. [Online; accessed 30-Sep-2018].
[90] "GCRCoin." http://www.gcrcoin.com/, 2018. [Online; accessed 30-Sep-2018].
[91] "NIX Platform whitepaper." https://nixplatform.io/docs/NIX-Platform-Whitepaper.pdf, 2018. [Online; accessed 30-Sep-2018].
[92] "SaluS Coin." https://saluscoin.info/, 2018. [Online; accessed 30-Sep-2018].
[93] "LEOcoin White Paper." https://www.leocoin.org/media/1027LEOcoinWhitePaper_V2.pdf, 2016. [Online; accessed 30-Sep-2018].
[94] "ION Technical Whitepaper." https://github.com/ionomy/ion/wiki/ION-Technical-Whitepaper, 2016. [Online; accessed 30-Sep-2018].
[95] "EOS.IO Technical White Paper." https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md, 2018. [Online; accessed 9-Oct-2018].
[96] "TRON." https://o836fhe91.qnssl.com/tron/whitebook/TronWhitepaper_en.pdf, 2018. [Online; accessed 9-Oct-2018].
[97] "Lisk Documentation." https://lisk.io/documentation/home, 2018. [Online; accessed 9-Oct-2018].
[98] "Lisk Documentation." https://bitshares.org/, 2018. [Online; accessed 9-Oct-2018].
[99] "Steem." https://steem.io/steem-whitepaper.pdf, 2018. [Online; accessed 13-Oct-2018].

[100] "GXChain." https://github.com/gxchain/whitepaper/blob/master/en/whitepaper.md, 2018. [Online; accessed 13-Oct-2018].

[101] "Ark." https://ark.io/Whitepaper.pdf, 2018. [Online; accessed 13-Oct-2018].

[102] "WaykiChain." https://www.waykichain.com/Whitepaper_en.pdf, 2018. [Online; accessed 13-Oct-2018].

[103] "Achain." https://www.achain.com/documents/Whitepaper.pdf, 2018. [Online; accessed 13-Oct-2018].

[104] "Asch." https://whitepaperdatabase.com/asch-xas-whitepaper/, 2018. [Online; accessed 13-Oct-2018].

[105] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus."

[106] "NEM Technical Reference." https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf, 2018.

[107] "ICON." https://docs.icon.foundation/ICON-Whitepaper-EN-Draft.pdf, 2017.

[108] Komodo, "Komodo: An Advanced Blockchain Technology, Focused on Freedom," *Self-published*, 2018.

[109] "Hcash." https://h.cash/themes/en/images/Hcash+Whitepaper+V0.8.5.pdf, 2017.

[110] "Nebulas Technical White Paper." https://nebulas.io/docs/NebulasTechnicalWhitepaper.pdf, 2018.

[111] "Emercoin." https://emercoin.com/en/documentation/about-emercoin.

[112] "elastos white paper." https://www.elastos.org/wp-content/uploads/2018/White%20Papers/elastos_whitepaper_en1.pdf?_t=1530976290, 2018.

[113] "Nexus: A Peer-to-Peer Network." https://nexusearth.com/nexus-white-paper, 2017.

[114] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value," *URL https://byteball. org/Byteball. pdf*, 2016.

[115] P. Snow, B. Deery, P. Kirby, and D. Johnston, "Factom ledger by consensus," 2015.

[116] "A Distributed Consensus Algorithm for Cryptocurrency Networks." https://github.com/skycoin/whitepapers/blob/master/whitepaper_skycoin_consensus_v01_jsm.pdf, 2016.

[117] "NextyCoin." https://nexty.io/nexty-whitepaper.pdf, 2018.

[118] "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake." https://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.

[119] "Ethash." https://github.com/ethereum/wiki/wiki/Ethash, 2018. [Online; accessed 8-Oct-2018].

[120] "Can you mine Ethereum using a CPU?." https://howtomine.co/2018/01/04/can-mine-ethereum-using-cpu/, 2018. [Online; accessed 8-Oct-2018].

[121] "DECENTRALIZED BITCOIN MINING POOL." http://p2pool.org/, 2019. [Online; accessed 18-Apr-2019].

[122] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "SMART POOL: Practical Decentralized Pooled Mining," vol. 2017, 2017.

[123] "SIMPLE POS POOL." https://simplepospool.com/#, 2018. [Online; accessed 28-Oct-2018].

[124] "STAKEMINERS.COM." https://stakeminers.com/index.php, 2018. [Online; accessed 19-Nov-2018].

[125] "Waves Docs." https://docs.wavesplatform.com/en/platform-features/leased-proof-of-stake-lpos.html, 2018. [Online; accessed 28-Oct-2018].

[126] D. Hockenberry, "Wanchain (WAN) Token Progress Report." https://cryptobriefing.com/wanchain-wan-token-progress-report/, 2018. [Online; accessed 28-Oct-2018].

[127] "How Reward Distribution in EOSIO Works." https://blog.springrole.com/how-reward-distribution-in-eosio-works-936e292dfbab, 2018. [Online; accessed 18-Nov-2018].

[128] "Everything You Need to Know About WaykiChain." https://medium.com/@waykichainwicc/everything-you-need-to-know-about-waykichain-3e81ea108e70, 2018. [Online; accessed 22-Nov-2018].

[129] "EOSPOTAL." https://eosportal.io/chain/12/producers, 2018. [Online; accessed 9-Oct-2018].

[130] "EOS Block Producer FAQ." https://medium.com/@bensig/eos-block-producer-faq-8ba0299c2896, 2018. [Online; accessed 9-Oct-2018].

[131] "TRON." https://tronscan.org/#/votes, 2018. [Online; accessed 9-Oct-2018].

[132] "steemit." https://steemit.com/, 2018. [Online; accessed 9-Oct-2018].

[133] "Witness Voting." https://steemit.com/~witnesses, 2018. [Online; accessed 9-Oct-2018].

[134] "Witness List." https://steemian.info/witnesses, 2018. [Online; accessed 20-Nov-2018].

[135] "TRX VOTING REWARDS CALCULATOR." https://www.tokengoodies.com/, 2018. [Online; accessed 26-Nov-2018].

[136] "EARN LISK." https://earnlisk.com/, 2018. [Online; accessed 26-Nov-2018].

[137] "Thomas Cox of Block.One Confirms Vote-Buying Will Be Against EOS.IO Proposed Constitution.." https://steemit.com/eos/@eosnewyork/block-one-confirms-vote-buying-will-be-against-eos-io-proposed-constitution, 2018. [Online; accessed 26-Nov-2018].

[138] D. Larimer, "Proposal for EOS Resource Renting & Rent Distribution." https://medium.com/@bytemaster/proposal-for-eos-resource-renting-rent-distribution-9afe8fb3883a, 2018. [Online; accessed 26-Nov-2018].

[139] "Cardano ADA Staking Rewards Will (Really) Let HODLers Down." https://crypto.bi/tape/blog/ada-staking/, 2018. [Online; accessed 20-Nov-2018].

[140] "WaykiChain Monthly Report - Oct 2018." https://medium.com/@waykichainwicc/waykichain-monthly-report-oct-2018-5739e9a077c3, 2018. [Online; accessed 22-Nov-2018].

[141] "QTUM Staking Pools." https://cryptopanic.com/news/43154/QTUM-Staking-Pools, 2017. [Online; accessed 20-Nov-2018].

[142] "Smart contract and stake delegation." https://forum.qtum.org/topic/229/smart-contract-and-stake-delegation, 2017. [Online; accessed 20-Nov-2018].

[143] "staking pool and QTUM MVP." https://bitcointalk.org/index.php?topic=4391854.0, 2018. [Online; accessed 20-Nov-2018].

[144] "Proof of Stake." https://www.poolofstake.io/wp-content/uploads/2018/09/Pool_of_Stake_whitepaper.pdf, 2018. [Online; accessed 20-Nov-2018].

[145] "Sesameseed." https://www.sesameseed.org/, 2018. [Online; accessed 20-Nov-2018].

[146] "GXChain." https://block.gxb.io/#/, 2018. [Online; accessed 16-Oct-2018].

[147] "Transactions." https://explorer.ark.io/wallets/AHsuUuhTNCGCbnPNkwJbeH27E4sDdcnmgp/transactions/all/2, 2018. [Online; accessed 16-Oct-2018].

[148] "API." https://explorer.ark.io:8443/api/transactions?senderId=AHsuUuhTNCGCbnPNkwJbeH27E4sDdcnmgp&recipientId=AHsuUuhTNCGCbnPNkwJbeH27E4sDdcnmgp&limit=25&offset=25&orderBy=timestamp:desc, 2018. [Online; accessed 16-Oct-2018].

[149] "The Tangle: an illustrated introductionl." https://blog.iota.org/the-tangle-an-illustrated-introduction-79f537b0a455, 2018. [Online; accessed 11-Nov-2018].

[150] "IOTA is centralized." https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d, 2017. [Online; accessed 11-Nov-2018].

[151] "My Nano Ninja." https://mynano.ninja/active, 2019. [Online; accessed 1-May-2019].

[152] "Free and instant NANO payments." https://brainblocks.io/, 2019. [Online; accessed 1-May-2019].

[153] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine Agreements for Cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles*, ACM, 2017.

[154] "stellarbeat.io." https://stellarbeat.io/, 2018. [Online; accessed 15-Nov-2018].

[155] "mystellar.tools." https://mystellar.tools/explorer/network/, 2018. [Online; accessed 15-Nov-2018].

[156] I. Eyal and E. G. Sirer, "How to Disincentivize Large Bitcoin Mining Pools." http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/, 2014. [Online; accessed 2-Nov-2018].

[157] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing Bitcoin Work for Data Preservation," in *2014 IEEE Symposium on Security and Privacy (SP)*, pp. 475–490, IEEE, 2014.

[158] A. Miller, A. Kosba, J. Katz, and E. Shi, "Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 680–691, ACM, 2015.

[159] G. Zeng, S. M. Yiu, J. Zhang, H. Kuzuno, and M. H. Au, "A Nonoutsourceable Puzzle Under GHOST Rule," in *2017 15th Annual*

Conference on Privacy, Security and Trust (PST), pp. 35–358, IEEE, 2017.
[160] "How Does Cloud Mining Bitcoin Work?." https://www.coindesk.com/information/cloud-mining-bitcoin-guide/, 2014. [Online; accessed 3-Nov-2018].
[161] "The 3 Top Bitcoin Mining Methods." https://www.lifewire.com/top-bitcoin-mining-methods-4157743, 2018. [Online; accessed 3-Nov-2018].
[162] "Best Bitcoin Cloud Mining Providers 2018." https://www.disruptordaily.com/best-bitcoin-cloud-mining-providers/, 2017. [Online; accessed 3-Nov-2018].
[163] "Genesis Mining." https://www.genesis-mining.com/, 2018. [Online; accessed 3-Nov-2018].
[164] "HASHNEST." https://www.hashnest.com/, 2018. [Online; accessed 3-Nov-2018].
[165] "BITMAIN." https://www.bitmain.com/, 2018. [Online; accessed 27-Oct-2018].
[166] "Bitcoin.com Pool." https://pool.bitcoin.com/en/, 2018. [Online; accessed 3-Nov-2018].
[167] "The Future of BlockChain: Proof Of Reputation." https://medium.com/gochain/the-future-of-blockchain-proof-of-reputation-318dea96100b. [Online; accessed 11-Nov-2018].
[168] L. Bahri and S. Girdzijauskas, "When Trust Saves Energy: A Reference Framework for Proof of Trust (PoT) Blockchains," in *The Web Conference 2018*, pp. 1165–1169, ACM Digital Library, 2018.
[169] I. Eyal, "The Miner's Dilemma," in *Symposium on Security and Privacy*, IEEE, 2015.
[170] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2017.
[171] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2016.
[172] I. Tsabary and I. Eyal, "The Gap Game," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2018.
[173] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, "Discovering bitcoin's public topology and influential nodes," *et al.*, 2015.
[174] S. Feld, M. Schönfeld, and M. Werner, "Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective," *Procedia Computer Science*, vol. 32, pp. 1121–1126, 2014.
[175] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?," *arXiv preprint arXiv:1902.11064*, 2019.
[176] J. Blocki and H.-S. Zhou, "Designing proof of human-work puzzles for cryptocurrency and beyond," in *Theory of Cryptography Conference*, pp. 517–546, Springer, 2016.

APPENDIX A
PROOF OF THEOREM IV.2

Because the function $U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ is a strictly increasing function of α_{n_i}, the players would want to increase their resource power and increase it at rate r per earned profit. Therefore, the resource power $\alpha^t_{n_i}$ of node n_i at time t increases to $\alpha^{t+1}_{n_i} = \alpha^t_{n_i} + r \cdot R^t_{n_i}$ at time $t+1$.

Then we sequence nodes at time t such that $\alpha^t_{n_i} \leq \alpha^t_{n_j}$ if $i < j$. Thus, $\alpha^t_{n_1}$ and $\alpha^t_{n_M}$ represent the smallest and largest resource power at time t, respectively. In addition, we assume that there exist M nodes (i.e., $|\mathcal{N}| = M$). At time $t+1$, the node n_i's resource power $\alpha^{t+1}_{n_i}$ and other node n_j's power $\alpha^{t+1}_{n_j}$ would be $\alpha^t_{n_i} + r \cdot f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})$ and $\alpha^t_{n_j}$, respectively, if node n_i generates a block with probability $\Pr(R^t_{n_i} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) \,|\, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})$. Then, we resequence M nodes at time $t+1$ such that $\alpha^{t+1}_{n_i} \leq \alpha^{t+1}_{n_j}$ if $i < j$. Here, for simplicity, we denote by β_{n_i} (or $\beta^t_{n_i}$) a resource power fraction of node n_i (at time t). In other words, $\beta_{n_i} = \frac{\alpha_{n_i}}{\sum_{n_i} \alpha_{n_i}}$ and $\beta^t_{n_i} = \frac{\alpha^t_{n_i}}{\sum_{n_j} \alpha^t_{n_j}}$. Moreover, $\frac{f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})}{\sum_{n_i} \alpha^t_{n_i}}$ is denote by B.

Now, we show that $\lim_{t\to\infty} E[\beta^t_{n_1}] = \lim_{t\to\infty} E[\beta^t_{n_M}]$. First, the following is met.

$$\frac{\beta_{n_i}}{\beta_{n_M}} \leq \frac{U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{U_{n_M}(\alpha_{n_M}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_M}})} \Rightarrow \frac{1}{\beta_{n_M}} \leq \frac{\sum_i U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{U_{n_M}(\alpha_{n_M}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_M}})}$$
$$\Leftrightarrow U_{n_M}(\alpha_{n_M}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_M}}) \leq \beta_{n_M} \sum_i U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}), \quad (12)$$

$$\frac{\beta_{n_i}}{\beta_{n_1}} \geq \frac{U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{U_{n_1}(\alpha_{n_1}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_1}})} \Rightarrow \frac{1}{\beta_{n_1}} \geq \frac{\sum_i U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{U_{n_1}(\alpha_{n_1}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_1}})}$$
$$\Leftrightarrow U_{n_1}(\alpha_{n_1}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_1}}) \geq \beta_{n_1} \sum_i U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}). \quad (13)$$

In Eqs. (12) and (13), the equal sign is true only if all nodes have the same resource power fraction $\frac{1}{M}$. Then we can derive the below equations.

$$E[\beta^{t+1}_{n_i} | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}] = \Pr(R^t_{n_i} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) \,|\, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) \Big(\frac{r \cdot B}{1 + r \cdot B} \Big) +$$
$$\sum_j \frac{\beta^t_{n_i} \Pr(R^t_{n_j} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})}{1 + r \cdot B} \leq \frac{r U_{n_i}(\alpha^t_{n_i}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}_{-\boldsymbol{n_i}})}{1 + r \cdot B} +$$
$$\sum_j \frac{\beta^t_{n_M} \Pr(R^t_{n_j} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})}{1 + r \cdot B}$$
$$\leq \frac{r \beta^t_{n_M} \sum_j U_{n_j}(\alpha^t_{n_j}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}_{-\boldsymbol{n_j}})}{1 + r \cdot B} + \frac{\beta^t_{n_M}}{1 + r \cdot B} = \beta^t_{n_M}$$

Similarly, we also prove the following equation.

$$E[\beta^{t+1}_{n_i} | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}] = \Pr(R^t_{n_i} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) \Big(\frac{r \cdot B}{1 + r \cdot B} \Big) + \quad (14)$$
$$\sum_j \frac{\beta^t_{n_i} \Pr(R^t_{n_j} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})}{1 + r \cdot B} \geq \frac{r U_{n_1}(\alpha^t_{n_1}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}_{-\boldsymbol{n_1}})}{1 + r \cdot B} + \quad (15)$$
$$\sum_j \frac{\beta^t_{n_1} \Pr(R^t_{n_j} = f(\bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}) | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}})}{1 + r \cdot B} \quad (16)$$
$$\geq \frac{r \beta^t_{n_1} \sum_j U_{n_j}(\alpha^t_{n_j}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}_{-\boldsymbol{n_j}})}{1 + r \cdot B} + \frac{\beta^t_{n_1}}{1 + r \cdot B} = \beta^t_{n_1}$$

Therefore, the following is satisfied:

$$\beta^t_{n_1} \leq E[\beta^{t+1}_{n_i} | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}] \leq \beta^t_{n_M},$$

where two equal signs are true if all nodes have the same power fraction. Because $E[\beta^{t+1}_{n_i}] = E[E[\beta^{t+1}_{n_i} | \bar{\boldsymbol{\alpha}}^{\boldsymbol{t}}]]$, the below equation is satisfied:

$$E[\beta^t_{n_1}] \leq E[\beta^{t+1}_{n_i}] \leq E[\beta^t_{n_M}].$$

By the above equation, $E[\beta^t_{n_1}]$ and $E[\beta^t_{n_M}]$ are increasing and decreasing functions of t, respectively, and converge according to the *monotone convergence theorem*. Moreover, if we assume that $\lim_{t\to\infty} E[\beta^t_{n_1}] = x < \lim_{t\to\infty} E[\beta^t_{n_M}] = y$, $E[\beta^{t+1}_{n_1} | \beta^t_{n_1} = x]$ is greater than x for any $t \geq 0$, and this is a contradiction because $E[\beta^{t+1}_{n_1} | \beta^t_{n_1} = x]$ should be x for a large value of t. Thus, x cannot be the limit, and

$\lim_{t\to\infty} E[\beta^t_{n_1}] = \lim_{t\to\infty} E[\beta^t_{n_M}]$. In addition, because $\beta^t_{n_M}$ is always not less than $\beta^t_{n_1}$,

$$\lim_{t\to\infty} E[\beta^t_{n_1}] = \lim_{t\to\infty} E[\beta^t_{n_M}] \Leftrightarrow \lim_{t\to\infty} E[|\beta^t_{n_M} - \beta^t_{n_1}|] = 0.$$

This fact implies that $\beta^t_{n_i}$ converges in mean to $\frac{1}{M}$. Because convergence in mean implies convergence in probability,

$$\lim_{t\to\infty} \Pr\Big[\frac{\beta^t_{n_M}}{\beta^t_{n_1}} = 1\Big] = 1.$$

As a result, Condition 4 is satisfied.

On the contrary, if

$$\frac{U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}} > \frac{U_{n_j}(\alpha_{n_j}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_j}})}{\alpha_{n_j}}$$

for any $\alpha_{n_i} > \alpha_{n_j}$, the following is met: $E[\beta^t_{n_M}] \le E[\beta^{t+1}_{n_M}]$. As a result, $\lim_{t\to\infty} E[\beta^{t+1}_{n_M}] = 1$, and $\beta^{t+1}_{n_M}$ converges in probability to 1, where the case indicates extreme centralization. Lastly, when

$$\frac{U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}} = \frac{U_{n_j}(\alpha_{n_j}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_j}})}{\alpha_{n_j}}$$

for any $\alpha_{n_i} > \alpha_{n_j}$, the following is satisfied: $E[\beta^{t+1}_{n_i}] = E[\beta^t_{n_i}] = \beta^0_{n_i}$. Therefore, if $\beta^t_{n_i}$ converges in mean to a value, the value would be $\beta^0_{n_i}$. However, the fact that $\lim_{t\to\infty} E[\beta^t_{n_i}] = \beta^0_{n_i}$ does not imply $\lim_{t\to\infty} E[|\beta^t_{n_i} - \beta^0_{n_i}|] = 0$, and indeed the following would be met: $\lim_{t\to\infty} E[|\beta^t_{n_i} - \beta^0_{n_i}|] > 0$. As a result, $\beta^t_{n_i}$ does not converge in probability to $\beta^0_{n_i}$, which implies that there is no convergence in probability of $\beta^t_{n_i}$. These facts can be proven, similar to the above proof.

APPENDIX B
PROOF OF THEOREM V.1

In this section, we prove Theorem V.1, and we introduce notations $\bar{\boldsymbol{EP}} = (EP_{p_i})_{p_i\in\mathcal{P}}$ and $\bar{\boldsymbol{EP}}^{\boldsymbol{t}} = (EP^t_{p_i})_{p_i\in\mathcal{P}^t}$. In addition, we assume that there is a mechanism $\mathcal{M}$, which stochastically makes a system (m,ε,δ)-decentralized. This mechanism $\mathcal{M}$ can be represented with two functions $\mathcal{M}^t_1$ and $\mathcal{M}^t_2$, which output the effective power distribution among players and resource power distribution among nodes after t time from when entering $\mathcal{M}$, respectively. Formally, the two functions are presented as $\mathcal{M}^t_1 : \Omega_{EP}\times\Omega_\alpha \mapsto \Omega_{EP}$ and $\mathcal{M}^t_2 : \Omega_{EP}\times\Omega_\alpha \mapsto \Omega_\alpha$, where

$$\Omega_{EP} = \{(EP_{p_i})_{p_i\in\mathcal{P}} \,|\, EP_{p_i}\in\mathbb{R}^+\} \text{ and}$$
$$\Omega_\alpha = \{(\alpha_{n_i})_{n_i\in\mathcal{N}} \,|\, \alpha_{n_i}\in\mathbb{R}^+\}.$$

We also define $\Omega_\alpha(\bar{\boldsymbol{EP}})$ as follows:

$$\Omega_\alpha(\bar{\boldsymbol{EP}}) = \left\{ (\alpha_{n_i})_{n_i\in\mathcal{N}} \,\middle|\, \alpha_{n_i}\in\mathbb{R}^+, \sum_{n_i\in\mathcal{N}_{p_i}} \alpha_{n_i} = EP_{p_i} \right\}.$$

Moreover, note that, because a system has zero Sybil cost (i.e., $C=0$), the following equation is met:

$$\mathcal{M}^t_2(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}}) = \mathcal{M}^t_2(\bar{\boldsymbol{EP}}', \bar{\boldsymbol{\alpha}}) \quad \forall \bar{\boldsymbol{EP}} \neq \bar{\boldsymbol{EP}}'. \tag{17}$$

In addition, we define $N(\bar{\boldsymbol{EP}})$ as

$$\bigcap_{k=0}^{\infty} \Big\{ \mathcal{M}^t_{c2}\Big(\bar{\boldsymbol{EP}}, f_{EP\to\alpha}(\bar{\boldsymbol{EP}})\Big) \,\Big|\, t>k, \mathcal{M}^t_{c1}\Big(\bar{\boldsymbol{EP}}, f_{EP\to\alpha}(\bar{\boldsymbol{EP}})\Big) = \bar{\boldsymbol{EP}} \Big\},$$

where the function $f_{EP\to\alpha} : \bar{\boldsymbol{EP}} \mapsto \bar{\boldsymbol{\alpha}}$ outputs the resource power distribution among nodes in which each player runs only one node (i.e., $f_{EP\to\alpha}(\bar{\boldsymbol{EP}}) = (\alpha_{n_i})_{n_i\in\mathcal{N}}$ and $\alpha_{n_i} = EP_{p_i}$ for $\mathcal{N}_{p_i} = \{n_i\}$). Note that $f_{EP\to\alpha}(\bar{\boldsymbol{EP}}) \in \Omega_\alpha(\bar{\boldsymbol{EP}})$. In the definition of $N(\bar{\boldsymbol{EP}})$, $\mathcal{M}^t_{c1}(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}})$ and $\mathcal{M}^t_{c1}(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}})$ output an effective power distribution among players and a resource power distribution among nodes, respectively, and the outputs are the same as $\mathcal{M}^t_1(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}})$ and $\mathcal{M}^t_2(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}})$, respectively, under the assumption that *a mechanism $\mathcal{M}$ does not change the resource power owned players*.

The set of all (m,ε,δ)-decentralized distribution $\bar{\boldsymbol{EP}}$ is denoted by $\boldsymbol{S}$. The probability to reach (m,ε,δ)-decentralization is

$$\lim_{t\to\infty} \Pr\left(\mathcal{M}^t_1(\bar{\boldsymbol{EP}}^{\boldsymbol{0}}, \bar{\boldsymbol{\alpha}}^0) \in \boldsymbol{S}\right).$$

Moreover, $I_{\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}}$ denotes a parameter that shows whether the mechanism $\mathcal{M}$ can learn the information about $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} = (EP_a)_{a\ge\delta}$, where $I_{\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}} = 1$ (or 0) indicates that mechanism $\mathcal{M}$ gets (or does not get) the information about $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}$. In other words, when $I_{\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}} = 1$, a system can know the effective power distribution among players above the δ-th percentile.

Lemma B.1. *$I_{\bar{\boldsymbol{EP}}_\delta} = 1$ if and only if $N(\bar{\boldsymbol{EP}})\cap N(\bar{\boldsymbol{EP}}') = \emptyset$ for any $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$, where $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \subset \bar{\boldsymbol{EP}}$ and $\bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}} \subset \bar{\boldsymbol{EP}}'$.*

Proof. If $I_{\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}} = 1$, there is a function $\mathcal{M}^t_2$ such that, for any $\bar{\boldsymbol{EP}}$ and $\bar{\boldsymbol{EP}}'$, which have $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}$ and $\bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$ $(\neq \bar{\boldsymbol{EP}}_{\boldsymbol{\delta}})$, respectively,

$$\mathcal{M}^t_2(\bar{\boldsymbol{EP}}, \bar{\boldsymbol{\alpha}}) \neq \mathcal{M}^t_2(\bar{\boldsymbol{EP}}', \bar{\boldsymbol{\alpha}}) \quad \forall \bar{\boldsymbol{\alpha}} \in N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}').$$

However, the above equation contradicts Eq. (17), and thus, $N(\bar{\boldsymbol{EP}})\cap N(\bar{\boldsymbol{EP}}')$ for $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$ should be the empty set. In addition, if $N(\bar{\boldsymbol{EP}})\cap N(\bar{\boldsymbol{EP}}') = \emptyset$, a system can determine the effective power distribution among players above the δ-th percentile. Therefore, $I_{\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}}} = 1$ if and only if $N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}') = \emptyset$ for any $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$. □

Lemma B.2. *$N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}') = \emptyset$ for any $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$ if and only if, for any effective power distribution $\bar{\boldsymbol{EP}}^\star$, $N(\bar{\boldsymbol{EP}}^\star) = \emptyset$ or it is not more profitable for any player with effective power $EP^\star_{p_i} \ge EP^\star_\delta$ to run multiple nodes than to run only one node.*

Proof. It is easy to prove $N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}') = \emptyset$ for any $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$, when it is most profitable for players to collude or when a player with effective power $EP_{p_i} \ge EP_\delta$ runs one node. Therefore, we describe the proof of the other direction. To do this, we assume that a player with effective power greater than or equal to $EP^\star_\delta$ runs multiple nodes in the state with effective power distribution $\bar{\boldsymbol{EP}}^\star$ and so the state has the

resource power distribution $\bar{\boldsymbol{\alpha}}^\star$ (i.e., $\bar{\boldsymbol{\alpha}}^\star \in N(\bar{\boldsymbol{EP}}^\star)$). Here, we define a function $f_{\alpha\to EP} : \bar{\boldsymbol{\alpha}} \mapsto \bar{\boldsymbol{EP}}$ as $f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}) = (EP_{p_i})_{p_i\in\mathcal{P}}$, where the output represents a state in which each player runs only one node and $EP_{p_i} = \alpha_{n_i}$. Then $\bar{\boldsymbol{\alpha}}^\star$ belongs to the set $N(f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}^\star))$. This is certainly true when it is not more profitable for some players to delegate their resource to others or run more than one node in the state with $f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}^\star)$. Even if it is more profitable for some players to run more than one node in the state with $f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}^\star)$, the state can come back to itself after going through a process where a player runs multiple nodes and then delegates its resource power to others because $\bar{\boldsymbol{\alpha}}^\star \in N(\bar{\boldsymbol{EP}}^\star)$. Lastly, if it is more profitable for some players to delegate their resource power to others, the state can also come back to itself after a player delegates its resource power to others. As a result, $\bar{\boldsymbol{\alpha}}^\star \in N(f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}^\star))$ and $N(\bar{\boldsymbol{EP}}^\star)\cap N(f_{\alpha\to EP}(\bar{\boldsymbol{\alpha}}^\star)) \neq \emptyset$. This fact implies that $N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}') = \emptyset$ for any $\bar{\boldsymbol{EP}}_{\boldsymbol{\delta}} \neq \bar{\boldsymbol{EP}}'_{\boldsymbol{\delta}}$ if and only if, for any $\bar{\boldsymbol{EP}}$, $N(\bar{\boldsymbol{EP}}) = \emptyset$ or players above the δ-th percentile should run only one node. Note that, in order to satisfy $N(\bar{\boldsymbol{EP}}) = \emptyset$, it should be more profitable for some players to delegate their resource to others in the state $\bar{\boldsymbol{EP}}$. □

Lemma B.3. *For any $\bar{\boldsymbol{EP}}$, $N(\bar{\boldsymbol{EP}})$ is the empty set or a player runs only one node if and only if it is most profitable for all players to form a grand coalition in which there is only one player running a node, or it is not more profitable for any player with effective power $EP_{p_i} \geq EP_\delta$ to run multiple nodes than to run one node.*

Proof. First, we consider that, for any $\bar{\boldsymbol{EP}}$, $N(\bar{\boldsymbol{EP}})$ is the empty set or a player runs only one node in the state $\bar{\boldsymbol{EP}}$. We also assume that $N(\bar{\boldsymbol{EP}}')$ is the empty set for a state $\bar{\boldsymbol{EP}}'$, and then the state $\bar{\boldsymbol{EP}}'$ moves to $\bar{\boldsymbol{EP}}^\star$ by delegating behaviors of some players. If the set $N(\bar{\boldsymbol{EP}}^\star)$ is not the empty set, $f_{EP\to\alpha}(\bar{\boldsymbol{EP}}^\star)$ would be in the set $N(\bar{\boldsymbol{EP}}^\star)$ because there is no player running multiple nodes. Here note that $f_{EP\to\alpha}(\bar{\boldsymbol{EP}}^\star) = (\alpha^\star_{n_i})_{n_i\in\mathcal{N}}$ and $\alpha^\star_{n_i} = EP^\star_{p_i}$ for $\mathcal{N}_{p_i} = \{n_i\}$. Otherwise, if the set $N(\bar{\boldsymbol{EP}}^\star)$ is empty, more players would engage in delegation of resource power in the state with $\bar{\boldsymbol{EP}}^\star$. This implies that all players would eventually cooperate by engaging in the delegation when $N(*)$ is continually empty for an arrival state $*$.

We consider the case where all players cooperate. The value of $U_{n_i}(\alpha = \sum_{p_i} EP^\star_{p_i})$ should be not less than $\sum_{\alpha_{n_i}\in f_{EP\to\alpha}(\bar{\boldsymbol{EP}}^\star)} U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ because it is most profitable for the player to run only one node in the state where only one player possesses positive effective power denoted by α. This implies that $N((\alpha))$ cannot be the empty set. As a result, if $N(\bar{\boldsymbol{EP}})$ is empty for any $\bar{\boldsymbol{EP}}$ except for (α), it is most profitable for all players to form a grand coalition where there is only one node. For the other direction, we omit the proof because it is trivial. □

When a system can find out whether $\frac{EP_{\max}}{EP_\delta} \leq 1+\varepsilon$ for the current state and get $EP_{\max}$ if the ratio is greater than $1+\varepsilon$, the probability to reach (m,ε,δ)-decentralization would be certainly greater than that for when it is not. This is because if $\frac{EP_{\max}}{EP_\delta}$ is greater than $1+\varepsilon$, the mechanism $\mathcal{M}$, which makes $\bar{\boldsymbol{EP}}$ belong to $\boldsymbol{S}$, should adjust $\frac{EP_{\max}}{EP_\mu}$[9] for some $\mu \geq \gamma$. Also, if the system adjusts $\frac{EP_{\max}}{EP_\mu}$ while not knowing the value of $\frac{EP_{\max}}{EP_\mu}$, the state cannot move in the best direction to (m,ε,δ)-decentralization. As a result, the following is met:

$$\max_{\mathcal{M}} \lim_{t\to\infty} \Pr(\mathcal{M}_1^t(\bar{\boldsymbol{EP}}^{\boldsymbol{0}}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{0}}) \in \boldsymbol{S} \,|\, I_{\boldsymbol{S}} = 0 \text{ or} \tag{18}$$

$$I^{\boldsymbol{S^c}}_{\bar{\boldsymbol{EP}}_{\mathbf{100}}} = 0) \leq \max_{\mathcal{M}} \lim_{t\to\infty} \Pr(\mathcal{M}_1^t(\bar{\boldsymbol{EP}}^{\boldsymbol{0}}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{0}}) \in \boldsymbol{S} \,| \tag{19}$$

$$I_{\boldsymbol{S}} = 1, I^{\boldsymbol{S^c}}_{\bar{\boldsymbol{EP}}_{\mathbf{100}}} = 1) =$$

$$\max_{\mathcal{M}} \lim_{t\to\infty} \Pr(\mathcal{M}_1^t(\bar{\boldsymbol{EP}}^{\boldsymbol{0}}, \bar{\boldsymbol{\alpha}}^{\boldsymbol{0}}) \in \boldsymbol{S} \,|\, N(\boldsymbol{S}) \cap N(\boldsymbol{S^c}) = \emptyset \tag{20}$$

$$\text{and } N(\bar{\boldsymbol{EP}}) \cap N(\bar{\boldsymbol{EP}}') = \emptyset \text{ for any } EP_{\max} \neq EP'_{\max}),$$

where $I_{\boldsymbol{S}} = 1$ (or 0) indicates that a system can (or cannot) learn the information about whether the current state is in $\boldsymbol{S}$, and $I^{\boldsymbol{S^c}}_{\bar{\boldsymbol{EP}}_{\mathbf{100}}} = 1$ (or 0) indicates that a system can (or cannot) learn effective power of the richest when the current state is not in $\boldsymbol{S}$. Note that Eq. (20) is derived by Lemma B.2. Considering Lemma B.1, B.2, and B.3, one can see that a mechanism satisfying 1) it is most profitable for all players to collude or for the richest to run only one node in a state that does not belong to $\boldsymbol{S}$ and 2) $N(\boldsymbol{S}) \cap N(\boldsymbol{S^c}) = \emptyset$, can maximize the probability to achieve (m,ε,δ)-decentralization. Moreover, $N(\boldsymbol{S}) \cap N(\boldsymbol{S^c}) = \emptyset$ implies that $N(\bar{\boldsymbol{EP}}) = \emptyset$ or $f_{\alpha\to EP}(N(\bar{\boldsymbol{EP}})) \subset \boldsymbol{S}$ for any $\bar{\boldsymbol{EP}} \in \boldsymbol{S}$.

Next, we consider a mechanism where, for a state $\bar{\boldsymbol{EP}}$, it is most profitable for all players to form a grand coalition running only one node. Then all players would share reward $R = U_{n_i}(\bar{\boldsymbol{EP}})$. Here, we consider a scheme sharing the reward among joined accounts, and a player can have multiple accounts if the behavior is more profitable than that the one that is not. We also denote by $U_{a_i}(\alpha_{a_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{a_i}})$ the received reward of account a_i owned resource power α_{a_i}. Similar to the above progress, we can show that, in this case, the probability to reach (m,ε,δ)-decentralization can be maximized when players above the δ-th percentile should have one account. Note that when A denotes the set of all accounts, $R = \sum_{a_i} U_{a_i\in A}(\alpha_{a_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{a_i}})$ for any A. Therefore, the conditions to maximize the probability to reach (m,ε,δ)-decentralization in the sharing scheme correspond to the following: At least the richest player runs only one node, and ND-2 is satisfied. As a result, by Lemma B.4, we can derive that the probability to reach (m,ε,δ)-decentralization is the maximum when the following is met:

$$U_{a_i}(\alpha_{a_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{a_i}}) = \frac{R\cdot\alpha_{a_i}}{\sum_{a_i\in A}\alpha_{a_i}}. \tag{21}$$

Second, we consider a mechanism in which it is not most profitable for all players to collude and it is most profitable for the richest player to run only one node when the state is not in $\boldsymbol{S}$. In fact, this is equivalent to the case where GR-2 and

[9] To get a fraction $\frac{EP_{\max}}{EP_\mu}$, the system should get $EP_{\max}$ and EP_μ.

ND-2 and NS-100 are satisfied. Therefore, from Lemma B.4, U_{n_i} should be Eq. (7) when the state is not in $\boldsymbol{\mathcal{S}}$.

As a result, because Eq. (21) is also a form of Eq. (7), we can see that, through Lemma V.2, the probability to reach (m, ε, δ)-decentralization can be maximized when GR-$|\mathcal{N}|$, ND-$|\mathcal{P}_\alpha|$, and NS-0 are met. Lastly, by presenting Lemma B.4, we completes the proof of Theorem V.1.

Lemma B.4. *Let us consider that GR-2, ND-2, and NS-100 are met. Then, in order that the probability of reaching (m, ε, δ)-decentralization is the maximum, the following should be met:*

$$U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = F\Big(\sum_{n_j \in \mathcal{N}} \alpha_{n_j}\Big) \cdot \alpha_{n_i}, \tag{22}$$

where $F : \mathbb{R}^+ \mapsto \mathbb{R}^+$.

Proof. According to ND-2 and NS-100, the following equation is satisfied for any α and set $\mathcal{N}_\alpha$ in which a node is an element and the total resource power of the elements is α:

$$\sum_{n_i \in \mathcal{N}_\alpha} U_{n_i}\Big(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}(\mathcal{N}_\alpha)\Big) = U_{n_j}(\alpha_{n_j} = \alpha), \tag{23}$$

where node $n_j \in \mathcal{N}_\alpha$ and $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}(\mathcal{N}_\alpha) = (\alpha_{n_k})_{n_k \in \mathcal{N}_\alpha, k \neq i}$. Therefore, for all $n \in \mathbb{N}$, the following is met:

$$U_{n_i}\Big(\frac{\alpha}{n}, \ \Big[\frac{\alpha}{n}\Big]^{n-1}\Big) = \frac{U_{n_i}(\alpha)}{n}, \tag{24}$$

where $\big[\frac{\alpha}{n}\big]^{n-1}$ represents the array, which has $n-1$ elements $\frac{\alpha}{n}$. Note that $\big[\frac{\alpha}{n}\big]^{n}$ is one of possible candidates for $\mathcal{N}_\alpha$ because the sum of elements is α.

Moreover, according to Eq. (23) and Eq. (2) in NS-100, the following equations are met for any natural number $l < \frac{n}{2}$:

$$U_{n_i}\Big(\frac{l\alpha}{n}, \ \Big(\frac{(n-l)\alpha}{n}\Big)\Big) + U_{n_i}\Big(\frac{(n-l)\alpha}{n}, \ \Big(\frac{l\alpha}{n}\Big)\Big) = U_{n_i}(\alpha),$$
$$U_{n_i}\Big(\frac{(n-l)\alpha}{n}, \ \Big(\frac{l\alpha}{n}\Big)\Big) \geq (n-l) \cdot U_{n_i}\Big(\frac{\alpha}{n}, \ \Big[\frac{\alpha}{n}\Big]^{n-1}\Big)$$

Because the lower the payoff of the richest, the more likely a system would reach (m, ε, δ)-decentralization, the below equations should be met to maximize the probability to reach (m, ε, δ)-decentralization.

$$U_{n_i}\Big(\frac{(n-l)\alpha}{n}, \ \Big(\frac{l\alpha}{n}\Big)\Big) = \frac{n-l}{n} \cdot U_{n_i}(\alpha),$$
$$U_{n_i}\Big(\frac{l\alpha}{n}, \ \Big(\frac{(n-l)\alpha}{n}\Big)\Big) = \frac{l \cdot U_{n_i}(\alpha)}{n}$$

This fact implies that Eq. (22) is satisfied for any $\mathcal{P}$ of which size is two.

Next, we assume that Eq. (22) is satisfied for any $\mathcal{P}$ of which size is $k(< n)$. Then we show that

$$U_{n_i}\Big(\frac{l_0\alpha}{n}, \ \Big(\frac{l_1\alpha}{n}, \cdots, \frac{l_k\alpha}{n}\Big)\Big) = \frac{l_0}{n} \cdot U_{n_i}(\alpha),$$

where $l_0, l_1, \cdots, l_k \in \mathbb{N}$ and $l_0 = \max\{l_0, l_1, \cdots, l_k\}$. According to Eq. (2) and the assumption, the following is met for any $0 < p \leq k$:

$$\frac{l_0 + l_p}{n} \cdot U_{n_i}(\alpha) = U_{n_i}\left(\frac{l_0\alpha}{n}, \ \left(\frac{l_1\alpha}{n}, \cdots, \frac{l_k\alpha}{n}\right)\right) +$$
$$U_{n_i}\left(\frac{l_p\alpha}{n}, \ \left(\frac{l_0\alpha}{n}, \cdots, \frac{l_{p-1}\alpha}{n}, \frac{l_{p+1}\alpha}{n}, \cdots, \frac{l_k\alpha}{n}\right)\right).$$

Moreover, the above equation derives the following.

$$k \cdot U_{n_i}\left(\frac{l_0\alpha}{n}, \ \left(\frac{l_1\alpha}{n}, \cdots, \frac{l_k\alpha}{n}\right)\right) + \sum_{p=1}^{k} U_{n_i}\left(\frac{l_p\alpha}{n}, \ *\right)$$
$$= \sum_{p=1}^{k} \frac{l_0 + l_p}{n} \cdot U_{n_i}(\alpha),$$

where $* = \big(\frac{l_1\alpha}{n}, \cdots, \frac{l_k\alpha}{n}\big)$. In addition, because

$$\sum_{p=1}^{k} U_{n_i}\left(\frac{l_p\alpha}{n}, \ *\right) = \sum_{p=1}^{k} \frac{l_p}{n} \cdot U_{n_i}(\alpha),$$

Eq. (22) is met for any $\mathcal{P}$ of which size is $k+1$. By mathematical induction, Eq. (22) holds for any n and $k(< n)$, which implies that Eq. (22) is true when relative resource power of all nodes to total resource power is a rational number. As a result, by *the density of the rational numbers*, Eq. (22) holds for any $\bar{\boldsymbol{\alpha}}$. This completes the proof. □

APPENDIX C
PROOF OF LEMMA V.2

The proof of Lemma V.2 is similar to that for Lemma B.4. Thus, we briefly describe this proof. First, it is trivial for Eq. (7) to satisfy GR-$|\mathcal{N}|$, ND-$|\mathcal{P}|$, and NS-0. Thus, we show the proof of the other direction. In other words, we prove that if the three conditions are met, the utility function should be Eq, (7). According to ND-$|\mathcal{P}|$ and NS-0, the following equation is satisfied for any α:

$$\sum_{n_i \in \mathcal{N}_\alpha} U_{n_i}\Big(\alpha_{n_i}, \boldsymbol{\alpha}^{+}_{-\boldsymbol{n_i}}(\mathcal{N}_\alpha)\Big) = U_{n_j}(\alpha_{n_j} = \alpha, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_\alpha}}),$$

where node $n_j \in \mathcal{N}_\alpha$, the total resource power in the node set $\mathcal{N}_\alpha$ is α, $\bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_\alpha}} = (\alpha_{n_k})_{n_k \notin \mathcal{N}_\alpha}$, and $\boldsymbol{\alpha}^{+}_{-\boldsymbol{n_i}}(\mathcal{N}_\alpha) = \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}_\alpha}} \| (\alpha_{n_k})_{n_k \in \mathcal{N}_\alpha, n_k \neq n_i}$. Therefore, for all $n \in \mathbb{N}$, the following is met:

$$U_{n_i}\Big(\frac{\alpha}{n}, \boldsymbol{\alpha}^{+}_{-\boldsymbol{n_i}}(\mathcal{N}^n_\alpha)\Big) = \frac{U_{n_j}(\alpha, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}^n_\alpha}})}{n},$$

where all nodes in $\mathcal{N}^n_\alpha$ possess $\frac{\alpha}{n}$ and $|\mathcal{N}^n_\alpha| = n$. Note that $\mathcal{N}^n_\alpha$ is one of possible candidates for $\mathcal{N}_\alpha$. The above equation derives the below equation:

$$U_{n_i}\Big(\alpha_{n_i}, \boldsymbol{\alpha}^{+}_{-\boldsymbol{n_i}}(\mathcal{N}^{\mathbb{Q}}_\alpha)\Big) = \frac{\alpha_{n_i}}{\alpha} \cdot U_{n_j}(\alpha, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{\mathcal{N}^{\mathbb{Q}}_\alpha}}),$$

where $\mathcal{N}^{\mathbb{Q}}_\alpha = \{n_i \,|\, \alpha_{n_i} = q_i\alpha, q_i \in \mathbb{Q}\}$ and node $n_j \in \mathcal{N}^{\mathbb{Q}}_\alpha$. Here, note that $\frac{\alpha_{n_i}}{\alpha}$ is a rational number. As a result, according to *the density of the rational numbers*, the utility U_{n_i} is a linear function for given the sum of resource power of

nodes (i.e., $\sum_{n_i \in \mathcal{N}} \alpha_{n_i}$), where the coefficient is denoted by $F(\sum_{n_i \in \mathcal{N}} \alpha_{n_i})$ as a function of $\sum_{n_i \in \mathcal{N}} \alpha_{n_i}$. Lastly, the coefficient $F(\sum_{n_i \in \mathcal{N}} \alpha_{n_i})$ should be positive to satisfy GR-$|\mathcal{N}|$.

APPENDIX D
PROOF OF THEOREM V.3

First, we consider that there is the minimum value of $\varepsilon(>0)$ such that $\max_{x \le A} xF(x) = (A-\varepsilon)F(A-\varepsilon)$ for a given value of A. Then, when $\sum \alpha_{n_i}$ is A,

$$U\left(\alpha_{n_k} \cdot \frac{A-\varepsilon}{A}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_k}} \cdot \frac{A-\varepsilon}{A}\right) = F(A-\varepsilon) \cdot \alpha_{n_k} \frac{A-\varepsilon}{A} > U\left(\alpha_{n_k} \cdot \frac{A-\varepsilon'}{A}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_k}} \cdot \frac{A-\varepsilon'}{A}\right) = F(A-\varepsilon') \cdot \alpha_{n_k} \frac{A-\varepsilon'}{A}, \tag{25}$$

for any $\varepsilon' < \varepsilon$. Therefore, when all players reduce resource power of their node at the same rate, their node power would decrease from α_{n_k} to $\alpha_{n_k} \cdot \frac{A-\varepsilon}{A}$, and they earn a higher profit. We also consider the case where a node does not reduce its power by $\frac{\sum \alpha_{n_i} - \varepsilon}{\sum \alpha_{n_i}}$ times. However, the retaliation of other nodes can make this behavior less profitable when compared to the case where the node reduces its power by $\frac{\sum \alpha_{n_i} - \varepsilon}{\sum \alpha_{n_i}}$ times, where retaliation strategies are often used in a repeated game for cooperation. A possible strategy of node n_i with resource power $\alpha^t_{n_i}$ is that the node updates its power $\alpha^t_{n_i}$ to $\alpha^{t+1}_{n_i} = \frac{A^{t+1} - \alpha^t_{n_i}}{A^t - \alpha^t_{n_i}} \cdot \alpha^t_{n_i}$ at time $t+1$, where A^t denotes the total resource power of nodes at time t. Under this strategy, because of Eq. (25), if even one node does not reduce its power by $\frac{A-\varepsilon}{A}$ times, all nodes earn a lower profit. As a result, there is a reachable equilibrium where all players reduce resource power of their node (i.e., effective power) by $\frac{A-\varepsilon}{A}$ times. Note that, in the equilibrium, the effective power distribution among players does not change.

Second, we consider that $\max_{x \le A} xF(x) = AF(A)$ for any A. This fact derives that

$$U_{n_i}(\alpha_{n_i} + \varepsilon, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = (\alpha_{n_i} + \varepsilon) F\left(\sum_{n_i} \alpha_{n_i} + \varepsilon\right) > U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) = \alpha_{n_i} F\left(\sum_{n_i} \alpha_{n_i}\right).$$

The above equation implies that the utility is a strictly increasing function for α_{n_i}: $U_{n_i}(\alpha_{n_i} + \varepsilon, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}}) > U_{n_i}(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ for any $\varepsilon > 0$. Thus, all nodes would increase their power for a higher profit.

To satisfy the second requirement of Def. IV.1, the following should be satisfied for any two players $p_i, p_j \in \mathcal{P}^t_\delta$:

$$\frac{EP^t_{p_i}}{EP^t_{p_j}} \le 1 + \varepsilon,$$

where $EP^t_{p_i} \ge EP^t_{p_j}$. Under the utility function Eq. (7), a player would run one node with its own resource, and the above equation can be expressed as follows: $\frac{\alpha^t_{n_i}}{\alpha^t_{n_j}} \le 1 + \varepsilon$, where $\mathcal{N}_{p_i} = \{n_i\}$ and $\mathcal{N}_{p_j} = \{n_j\}$. Because $U(\alpha_{n_i}, \bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})$ is a strictly increasing function of α_{n_i}, all nodes would increase their resource at rate r per earned net profit. Then the ratio $\frac{\alpha^{t+1}_{n_i}}{\alpha^{t+1}_{n_j}}$ between the resource power of nodes n_i and n_j at time $t+1$ is

$$\frac{\alpha^t_{n_i} + r \cdot R^t_{n_i}}{\alpha^t_{n_j} + r \cdot R^t_{n_j}} = \frac{\alpha^t_{n_i}}{\alpha^t_{n_j}} \cdot \frac{1 + r \cdot \frac{R^t_{n_i}}{\alpha^t_{n_i}}}{1 + r \cdot \frac{R^t_{n_j}}{\alpha^t_{n_j}}} > \frac{\alpha^t_{n_i}}{\alpha^t_{n_j}} \cdot \frac{1}{1 + r \cdot \frac{R^t_{n_j}}{\alpha^t_{n_j}}}.$$

For ease of reading, a state where $\alpha_{n_i} = \alpha$ and $\alpha_{n_j} = \beta$ is denoted by (α, β). Here, note that α is not less than β. Then we consider one step in which (α, β) moves to $(\alpha, \beta + ry)$ with probability p and $(\alpha + rx, \beta)$ with probability $1-p$, where $x, y \le R_{\texttt{max}}$. Because of $\frac{U_{n_j}(\beta)}{\beta} - \frac{U_{n_i}(\alpha)}{\alpha} = 0$, $p = \frac{x}{x + \frac{\alpha y}{\beta}}$. We also denote $\Pr(a \to b \,|\, (\alpha, \beta))$ by the probability for ratio $\frac{\alpha_{n_i}}{\alpha_{n_j}}$ to reach from a to less than b when a state $(\alpha_{n_i}, \alpha_{n_j})$ starts from (α, β). Then the following holds:

$$\Pr\left(\frac{\alpha}{\beta} \to 1 + \varepsilon \,\middle|\, (\alpha, \beta)\right) \le \frac{\beta x}{\beta x + \alpha y} \times \max \Pr\left(\frac{\alpha}{\beta + ry} \to 1 + \varepsilon \,\middle|\, (\alpha, \beta + ry)\right) + \frac{\alpha y}{\beta x + \alpha y} \times \max \Pr\left(\frac{\alpha + rx}{\beta} \to 1 + \varepsilon \,\middle|\, (\alpha + rx, \beta)\right), \tag{26}$$

where $\max \Pr(\frac{\alpha}{\beta + ry} \to 1 + \varepsilon \,|\, (\alpha, \beta + ry))$ indicates the maximum probability for $(\alpha_{n_i}, \alpha_{n_j})$ to reach from $(\alpha, \beta + ry)$ to a state satisfying that $\frac{\alpha_{n_i}}{\alpha_{n_j}} \le 1 + \varepsilon$, considering all possible random walks. Similarly, $\max \Pr(\frac{\alpha + rx}{\beta} \to 1 + \varepsilon \,|\, (\alpha + rx, \beta))$ represents the maximum probability for $(\alpha_{n_i}, \alpha_{n_j})$ to reach from $(\alpha + rx, \beta)$ to a state satisfying that $\frac{\alpha_{n_i}}{\alpha_{n_j}} \le 1 + \varepsilon$. Note that, in the range $0 \le x \le R_{\texttt{max}}$, the right-hand side of Eq. (26) is the maximum when $x = 0$.

We denote the right-hand side of Eq. (26) by $f(x, \alpha, \beta)$. Then, when assuming 1) $\lim_{\alpha \to \infty} f(x, \alpha, \beta)$ is a constant in terms of x and 2) $f(x, \alpha, \beta)$ is the maximum when $x = R_{\texttt{max}}$, the probability to reach (m, ε, δ)-decentralization is upper bounded by the maximum probability to reach (m, ε, δ)-decentralization under *a random walk where α_{n_i} changes to $\alpha_{n_i} + rR_{\texttt{max}}$ if it increases.* For the second assumption, Fig. 2

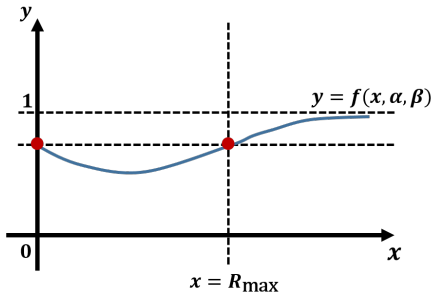


Figure 2. The function $f(x, \alpha, \beta)$ represents the right-hand side of Eq. (26). This graph shows that $f(R_{\texttt{max}}, \alpha, \beta)$ is the maximum in the range $x \le R_{\texttt{max}}$.

describes an example. Note that the value of when $x = 0$ cannot be greater than that for when $x = R_{\max}$ because $\max \Pr(\frac{\alpha}{\beta} \to 1+\varepsilon \,|\, (\alpha,\beta))$ is not greater than $f(x,\alpha,\beta)$. Moreover, the above fact derives that, even if we extend to one step in which (α,β) can move to $(\alpha,\beta+ry)$, $(\alpha+rx_1,\beta)$, $(\alpha+rx_2,\beta),\cdots,(\alpha+rx_n,\beta)$, the probability for the ratio $\frac{\alpha_{n_i}}{\alpha_{n_j}}$ to reach from $\frac{\alpha}{\beta}$ to less than $1+\varepsilon$ can be the maximum when $x_i = R_{\max}$ for $1 \le i \le n$. Also, when considering one step where (α,β) can move to $(\alpha,\beta+ry_1)$, $(\alpha,\beta+ry_2)$, $\cdots$, $(\alpha,\beta+ry_n)$, $(\alpha+rx,\beta)$, the probability for the ratio $\frac{\alpha_{n_i}}{\alpha_{n_j}}$ to reach from $\frac{\alpha}{\beta}$ to less than $1+\varepsilon$ can be the maximum if $x = R_{\max}$. This is because such steps can be expressed as a linear combination of a step s_i for $i \le n$ in which (α,β) can move to $(\alpha,\beta+ry_i)$ or $(\alpha+rx_i,\beta)$. As a result, these facts imply that it is sufficient to find a function $G(\alpha,\beta)$ satisfying the following.

1) The function $G(\alpha,\beta)$ is equal to or greater than $\max_{x=R_{\max}} \Pr\left(\frac{\alpha}{\beta} \to 1+\varepsilon \,\middle|\, (\alpha,\beta)\right)$.
2) The following equation is the maximum when $x = R_{\max}$.

$$\max_y \left\{ \frac{\beta x}{\beta x+\alpha y}\cdot G(\alpha,\beta+ry) + \frac{\alpha y}{\beta x+\alpha y}\cdot G(\alpha+rx,\beta) \right\}. \tag{27}$$

3) The limit value of Eq. (27) when α goes to infinity is a constant in terms of x.
4) The below equation holds:

$$G(\alpha,\beta) \ge \max_y \left\{ \frac{\beta R_{\max}}{\beta R_{\max}+\alpha y}\cdot G(\alpha,\beta+ry) + \frac{\alpha y}{\beta R_{\max}+\alpha y}\cdot G(\alpha+rR_{\max},\beta) \right\}.$$

Next, we consider the case where the ratio $\frac{\alpha_{n_i}}{\alpha_{n_j}}$ changes from $\frac{\alpha}{\beta}$ to less than $1+\varepsilon$ without a process in which α_{n_i} increases from α to $\alpha+rR_{\max}$. The probability for the case is denoted by $P_0^\varepsilon(\alpha,\beta)$. In addition, for the case where $\frac{\alpha_{n_i}}{\alpha_{n_j}}$ changes from $\frac{\alpha}{\beta}$ to less than $1+\varepsilon$ with a process in which α_{n_i} increases from α to $\alpha+krR_{\max}$ but not to $\alpha+(k+1)rR_{\max}$, its probability is denoted by $P_k^\varepsilon(\alpha,\beta)$. Fig. 3 represents examples for events of which probabilities are $P_0^\varepsilon(\alpha,\beta), P_1^\varepsilon(\alpha,\beta)$, and $P_2^\varepsilon(\alpha,\beta)$, respectively. For ease of reading, we also denote $\frac{R_{n_j}}{\alpha_{n_j}} - \frac{R_{n_i}}{\alpha_{n_i}}$ by D, and then, the following holds:

$$\begin{aligned}
&\frac{U_{n_j}(\alpha_{n_j},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_j}})}{\alpha_{n_j}} - \frac{U_{n_i}(\alpha_{n_i},\bar{\boldsymbol{\alpha}}_{-\boldsymbol{n_i}})}{\alpha_{n_i}} = 0 \\
&= \int_{D\ge d} D\Pr(D) + \int_{D<d} D\Pr(D) \\
&\ge d\Pr(D\ge d) - \frac{R_{\max}}{\alpha_{n_i}}(1-\Pr(D\ge d)) \\
&\Rightarrow \Pr(D\ge d) \le \frac{R_{\max}}{R_{\max}+d\alpha_{n_i}} \\
&\Rightarrow \Pr(\frac{R_{n_j}}{\alpha_{n_j}} \ge d, R_{n_i}=0) \le \frac{R_{\max}}{R_{\max}+d\alpha_{n_i}}
\end{aligned}$$

By the above equation, we can also derive the following:

$$\begin{aligned}
&\Pr\Big(\frac{\alpha_{n_i}^{t+1}}{\alpha_{n_j}^{t+1}} \le x \Big| \alpha_{n_i}^t, \alpha_{n_j}^t\Big) \\
&\le \Pr\Big(\frac{R_{n_j}^t}{\alpha_{n_j}^t} \le \frac{1}{r}\Big(\frac{1}{x}\cdot\frac{\alpha_{n_i}^t}{\alpha_{n_j}^t} - 1\Big) = d \Big| \alpha_{n_i}^t, \alpha_{n_j}^t\Big) \\
&\le \frac{R_{\max}}{R_{\max}+d\alpha_{n_i}^t} = \frac{R_{\max}(1+rd)}{(R_{\max}+d\alpha_{n_i}^t)(1+rd)} \\
&\le \frac{1}{1+rd} \le x\cdot\frac{\alpha_{n_j}^t}{\alpha_{n_i}^t} \quad \text{if} \quad R_{\max}\cdot r \le \alpha_{n_i}^t
\end{aligned} \tag{28}$$

Assuming that $\beta\prod_{t=1}^n(1+rd^t) = \frac{\alpha}{1+\varepsilon}$, Eq. (28) implies

$$\begin{aligned}
&P_0^\varepsilon(\alpha,\beta) = \prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha} = \prod_{t=1}^n \frac{R_{\max}(1+rd^t)}{(R_{\max}+d^t\alpha)(1+rd^t)} \\
&\le (1+\varepsilon)\cdot\frac{\beta}{\alpha} \quad \text{if} \quad R_{\max}\cdot r \le \alpha.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\max P_0^\varepsilon(\alpha,\beta) &= \max_{(d^1,\cdots,d^n)\in S_1} \prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha} \\
&\le \max_{(d^1,\cdots,d^n)\in S_2} \prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha},
\end{aligned}$$

where

$$\begin{aligned}
S_1 = \Bigg\{ (d^1,\cdots,d^n) \,\Big|\, &0 \le d^t \le \frac{R_{\max}}{\beta\prod_{i=1}^{t-1}(1+rd^i)}, \\
&\beta\prod_{t=1}^n(1+rd^t) = \frac{\alpha}{1+\varepsilon} \Bigg\} \subset \\
S_2 = \left\{ (d^1,\cdots,d^n) \,\middle|\, 0 \le d^t, \beta\prod_{t=1}^n(1+rd^t) = \frac{\alpha}{1+\varepsilon} \right\}&.
\end{aligned}$$

Because $\prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha}$ is a symmetric and convex function for variables $d^1, d^2, \cdots, d^n$, it would be the maximum when a point $(d^1,d^2,\cdots,d^n)$ is on the boundary of a set A_2. In other words, if

$$d^1 = \frac{1}{r}\left(\frac{\alpha}{\beta(1+\varepsilon)} - 1\right) \text{ and } d^t = 0 \quad \forall t > 1,$$

the value of $\prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha}$ is the maximum. Meanwhile, $\prod_{t=1}^n \frac{R_{\max}}{R_{\max}+d^t\alpha}$ is the minimum if $d^1, d^2, \cdots, d^n$ are the same. In addition, when $R_{\max}\cdot r = \alpha$, $P_0^\varepsilon(\alpha,\beta)$ can be maximized, and the value is $(1+\varepsilon)\frac{\beta}{\alpha}$.

We define $Pr_k\left((\alpha,\beta) \to (\alpha+krR_{\max},\beta')\right)$ as the probability of an event where a point $(\alpha_{n_i},\alpha_{n_j})$ starting from (α,β) reaches the line $\alpha_{n_i} = \alpha+krR_{\max}$ before satisfying $\frac{\alpha_{n_i}}{\alpha_{n_j}} \le 1+\varepsilon$, and the value of α_{n_j} of the point at which $(\alpha_{n_i},\alpha_{n_j})$ meets the line $\alpha_{n_i} = \alpha+kR_{\max}$ for the first time

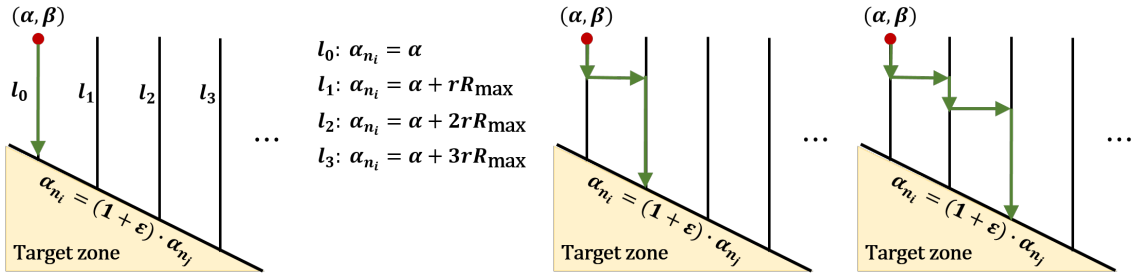


Figure 3. The figures represent examples for events of which probabilities are $P_0^{\varepsilon}(\alpha,\beta)$, $P_1^{\varepsilon}(\alpha,\beta)$, and $P_2^{\varepsilon}(\alpha,\beta)$, respectively. The red point (α,β) is a start point, and a random walk aims to enter the target zone in which $\frac{\alpha_{n_i}}{\alpha_{n_j}} \leq 1+\varepsilon$. The lines l_0, l_1, l_2 and l_3 represent $\alpha_{n_i} = \alpha, \alpha_{n_i} = \alpha + R_{\max}, \alpha_{n_i} = \alpha + 2R_{\max}$, and $\alpha_{n_i} = \alpha + 3R_{\max}$, respectively. The point $(\alpha_{n_i}, \alpha_{n_j})$ would descend along the current line or move to the next line.

is β'. Then, for the probability $P_k^{\varepsilon}(\alpha,\beta)$, the following holds:

$$P_k^{\varepsilon}(\alpha,\beta) = \sum_{\beta'} Pr_k\left((\alpha,\beta) \to (\alpha + krR_{\max}, \beta')\right) \times$$
$$P_0^{\varepsilon}(\alpha + krR_{\max}, \beta') \leq \sum_{\beta'} Pr_k\left((\alpha,\beta) \to (\alpha + krR_{\max}, \beta')\right)$$
$$\times \frac{rR_{\max}}{rR_{\max} + (\alpha + krR_{\max}) \cdot \left(\frac{\alpha + krR_{\max}}{\beta'(1+\varepsilon)} - 1\right)} \tag{29}$$

We denote the right-hand side of Eq. (29) by $H_k(\alpha,\beta)$. Note that the value of $H_k(\alpha,\beta)$ indicates the probability of an event in which the point $(\alpha_{n_i}, \alpha_{n_j})$ meets the line $\alpha_{n_i} = \alpha + krR_{\max}$ and moves from (α,β) to a point satisfying $\frac{\alpha_{n_i}}{\alpha_{n_j}} \leq 1+\varepsilon$. In this event, if $(\alpha_{n_i}, \alpha_{n_j})$ is on the point $(\alpha + krR_{\max}, \beta')$, it can reach a point satisfying $\frac{\alpha_{n_i}}{\alpha_{n_j}} \leq 1+\varepsilon$ with probability

$$\frac{rR_{\max}}{rR_{\max} + (\alpha + krR_{\max}) \cdot \left(\frac{\alpha + krR_{\max}}{\beta'(1+\varepsilon)} - 1\right)}. \tag{30}$$

Therefore, the value of $H_k(\alpha,\beta)$ depends on how the point $(\alpha_{n_i}, \alpha_{n_j})$ reaches the line $\alpha_{n_i} = \alpha + krR_{\max}$.

Next, we find when $H_k(\alpha,\beta)$ can be maximized. Note that the value of $H_0(\alpha,\beta)$ is determined as Eq. (30). Thus, we first consider when $k = 1$ and denote the value of $H_k(\alpha,\beta)$ under a random walk $\mathcal{W}$ by $H_k^{\mathcal{W}}(\alpha,\beta)$. Also, we assume that two random walks $\mathcal{W}_1$ and $\mathcal{W}_2$ exist. In $\mathcal{W}_1$, the point $(\alpha_{n_i}, \alpha_{n_j})$ on the line $\alpha_{n_i} = \alpha$ can move to either the point $(\alpha + rR_{\max}, \alpha_{n_j})$ or the point $(\alpha, \frac{\alpha}{1+\varepsilon})$. If the point is on the line $\alpha_{n_i} = \alpha + rR_{\max}$, it can move to either the point $(\alpha + 2rR_{\max}, \alpha_{n_j})$ or the point $(\alpha + rR_{\max}, \frac{\alpha + rR_{\max}}{1+\varepsilon})$. The random walk $\mathcal{W}_2$ is similar to $\mathcal{W}_1$ except that there is one additional path from the line $\alpha_{n_i} = \alpha$ to the line $\alpha_{n_i} = \alpha + rR_{\max}$ when compared to $\mathcal{W}_1$. Fig. 4 represents $\mathcal{W}_1$ and $\mathcal{W}_2$. While the random walk $\mathcal{W}_1$ has only one point $(\alpha + rR_{\max}, \beta)$ at which a state $(\alpha_{n_i}, \alpha_{n_j})$ can meet the line l_1, $(\alpha_{n_i}, \alpha_{n_j})$ can meet the line l_1 at two points $(\alpha + rR_{\max}, \beta)$ and $(\alpha + rR_{\max}, \beta(1 + rd_{01}))$ in random walk $\mathcal{W}_2$. Fig. 4a represents the possible path of random walk $\mathcal{W}_1$, and Figs. 4b and 4c show two possible paths of random walk $\mathcal{W}_2$.

We show that $H_1^{\mathcal{W}_2}(\alpha,\beta)$ is greater than $H_1^{\mathcal{W}_1}(\alpha,\beta)$. Referring to Fig. 4, the following is met:

$$\beta(1 + rd_0) = \frac{\alpha}{1+\varepsilon}, \quad \beta(1 + rd_1) = \frac{\alpha + rR_{\max}}{1+\varepsilon},$$
$$\beta(1 + rd_{01})(1 + rd_{02}) = \frac{\alpha}{1+\varepsilon},$$
$$\beta(1 + rd_{01})(1 + rd_1') = \frac{\alpha + rR_{\max}}{1+\varepsilon},$$
$$R_{\max}(R_{\max} + \alpha d_0) \leq (R_{\max} + \alpha d_{01})(R_{\max} + \alpha d_{02}). \tag{31}$$

Also, $H_1^{\mathcal{W}_1}(\alpha,\beta)$ and $H_1^{\mathcal{W}_2}(\alpha,\beta)$ are

$$\frac{R_{\max}}{R_{\max} + (\alpha + rR_{\max})d_1} \cdot \frac{\alpha d_0}{R_{\max} + \alpha d_0} \text{ and}$$
$$\frac{\alpha d_{01}}{R_{\max} + \alpha d_{01}} \cdot \frac{R_{\max}}{R_{\max} + (\alpha + rR_{\max})d_1} + \frac{R_{\max}}{R_{\max} + \alpha d_{01}}$$
$$\times \frac{\alpha d_{02}}{R_{\max} + \alpha d_{02}} \cdot \frac{R_{\max}}{R_{\max} + (\alpha + rR_{\max})d_1'},$$

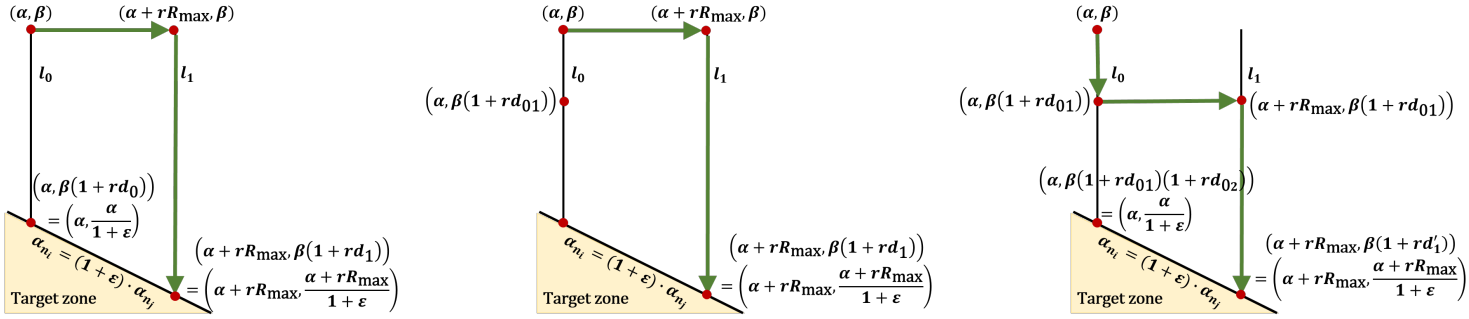
respectively. Because of Eq. (31), $H_1^{\mathcal{W}_2}(\alpha,\beta)$ is less than

$$\frac{\alpha d_{01}}{R_{\max} + \alpha d_{01}} \cdot \frac{R_{\max}}{R_{\max} + (\alpha + rR_{\max} d_1)} + \left(\frac{R_{\max}}{R_{\max} + \alpha d_{01}}$$
$$- \frac{R_{\max}}{R_{\max} + \alpha d_0}\right) \cdot \frac{R_{\max}}{(\alpha + rR_{\max})d_1'}. \tag{32}$$

By the below equations, Eq. (32) is greater than $H_1^{\mathcal{W}_1}(\alpha,\beta)$.

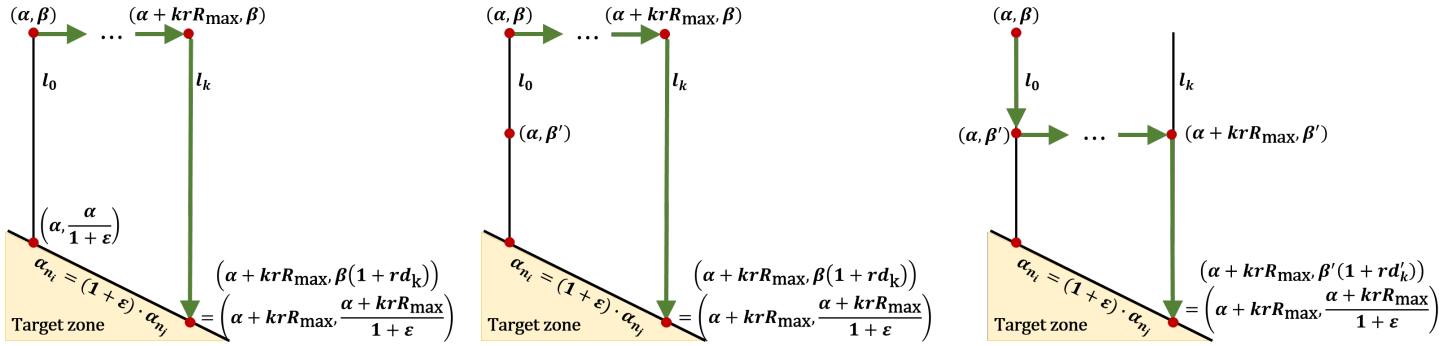
$$\frac{1}{R_{\max} + (\alpha + rR_{\max})d_1'} \geq \frac{1}{R_{\max} + (\alpha + rR_{\max})d_1} \Leftrightarrow$$
$$\frac{1}{R_{\max} + (\alpha + rR_{\max})d_1'} \times \left(\frac{R_{\max}}{R_{\max} + \alpha d_{01}} - \frac{R_{\max}}{R_{\max} + \alpha d_0}\right)$$
$$\geq \frac{1}{R_{\max} + (\alpha + rR_{\max})d_1} \times \left(\frac{\alpha d_0}{R_{\max} + \alpha d_0} - \frac{\alpha d_{01}}{R_{\max} + \alpha d_{01}}\right)$$
$$\Leftrightarrow H_1^{\mathcal{W}_1}(\alpha,\beta) < \text{Eq. (32)}$$

Here, note that $d_1' < d_1$. As a result, $H_1^{\mathcal{W}_2}(\alpha,\beta) > H_1^{\mathcal{W}_1}(\alpha,\beta)$. Moreover, $H_1^{\mathcal{W}_2}(\alpha,\beta)$ is a concave function of d_{01}, which implies that the value of $H_1^{\mathcal{W}_2}(\alpha,\beta)$ would more efficiently increase when d_{01} is closer to 0. Considering this fact, we can see that the more densely there exist points at



(a) Random walk $\mathcal{W}_1$ (b) Random walk $\mathcal{W}_2$ (c) Random walk $\mathcal{W}_2$

Figure 4. The figures represent two random walks $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively. The red points indicate points to which the state $(\alpha_{n_i},\alpha_{n_j})$ can move through each random walk. Moreover, green paths indicate the possible path in each random walk. In $\mathcal{W}_2$, there is one red point $(\alpha,\beta(1+rd_{01}))$ on line l_0 in addition to the red point of $\mathcal{W}_1$. Here, $1+rd_0=(1+rd_{01})(1+rd_{02})$.



(a) Random walk $\mathcal{W}_3$ (b) Random walk $\mathcal{W}_4$ (c) Random walk $\mathcal{W}_4$

Figure 5. The figures represent two random walks $\mathcal{W}_3$ and $\mathcal{W}_4$, respectively. The red points indicate points to which the state $(\alpha_{n_i},\alpha_{n_j})$ can change the moving direction. Moreover, green paths indicate the possible path in each random walk. In $\mathcal{W}_4$, there is another red point (α,β') on line l_0 in addition to the red point of $\mathcal{W}_3$.

which $(\alpha_{n_i},\alpha_{n_j})$ can meet the line $\alpha_{n_i}=\alpha+rR_{\max}$ for the first time, the greater the value of $H_1(\alpha,\beta)$ is.

Next, we consider two random walks, $\mathcal{W}_3$ and $\mathcal{W}_4$, and find when $H_k^{\mathcal{W}}(\alpha,\beta)$ can be maximized. Hereafter, a point $(\alpha_{n_i},\alpha_{n_j})$, which can move to the next line, (e.g., red points represented in Fig. 4) is called a break point. The random walk $\mathcal{W}_4$ has one additional break point on the line $l_0:\alpha_{n_i}=\alpha$ in comparison with $\mathcal{W}_3$. Therefore, the number of points at which $\mathcal{W}_4$ can meet the line $\alpha_{n_i}=\alpha+krR_{\max}$ for the first time is greater than that for $\mathcal{W}_3$ by 1. Fig. 5 represents the two random walks $\mathcal{W}_3$ and $\mathcal{W}_4$, and the following holds:

$$\begin{aligned}&\beta'=\beta(1+rx),\ \beta(1+rd_k)=\alpha+krR_{\max},\\&\beta'(1+rd'_k)=\alpha+krR_{\max},\\&\beta(1+rd_{k+1})=\alpha+(k+1)rR_{\max},\\&\beta'(1+rd'_{k+1})=\alpha+(k+1)rR_{\max}\end{aligned}$$

for $\beta'>\beta$. Then we find $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$.

First, $H_k^{\mathcal{W}_3}$ and $H_k^{\mathcal{W}_4}$ can be expressed as follows:

$$H_k^{\mathcal{W}_3}=\prod_{i=0}^{k-1}\frac{(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta}-1\right)}{rR_{\max}+(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta}-1\right)}\times\frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta}-1\right)},$$

$$\begin{aligned}H_k^{\mathcal{W}_4}=&\prod_{i=1}^{k-1}\frac{(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta}-1\right)}{rR_{\max}+(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta}-1\right)}\\&\times\frac{\alpha x}{R_{\max}+\alpha x}\cdot\frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta}-1\right)}\\&+\frac{R_{\max}}{R_{\max}+\alpha x}\cdot\prod_{i=0}^{k-1}\frac{(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}{rR_{\max}+(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}\\&\times\frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}.\end{aligned}$$

In fact, when $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is positive, it is always greater than $\frac{H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3}}{x}$ for any $0<x<\frac{1}{r}\cdot\left(\frac{\alpha}{(1+\varepsilon)\beta}-1\right)$. In addition, if $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is negative, $H_k^{\mathcal{W}_3}$ is greater than $H_k^{\mathcal{W}_4}$. These facts implies that if $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is positive, $H_k^{\mathcal{W}}$ can be maximized when there exist densely break points on

the line l_0. Meanwhile, if $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is negative, $H_k^{\mathcal{W}}$ can be maximized when there is no break point on line l_0.

The derivative $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is equal to $\frac{\partial H_k^{\mathcal{W}_4}}{\partial x}\Big|_{x=0}$ because $\mathcal{W}_3$ is constant in terms of x. In addition, the value of $\frac{\partial H_k^{\mathcal{W}_4}}{\partial x}\Big|_{x=0}$ is equal to the value of $\frac{\partial A^k}{\partial x}\Big|_{x=0}$, where

$$A^k = \prod_{i=0}^{k-1} \frac{(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}{rR_{\max}+(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)} \times \frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}$$

The value of $\frac{\partial A^k}{\partial x}\Big|_{x=0}$ is expressed as

$$-r\cdot A^k\cdot\sum_{i=0}^{k-1}\frac{(l+i)^2}{((l+i)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-i+1)^2}\times \frac{1+(l+i)((l+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}{(l+i)((l+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}+r\cdot A^k\times \frac{(l+k)^2}{((l+k)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-k+1)^2}\times \left(1+(l+k)((l+k)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)\right),$$

where $R'_{\max}=rR_{\max}$ and $l=\frac{\alpha}{R'_{\max}}$. Through the above equation, one can see that if $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is positive when $l=l_0$, $\frac{\partial(H_k^{\mathcal{W}_4}-H_k^{\mathcal{W}_3})}{\partial x}\Big|_{x=0}$ is also positive for all $l\geq l_0$. In other words, when the derivative value is positive for $\alpha=\alpha_0$, it is positive for all $\alpha>\alpha_0$.

Also, we assume that $H_k^{\mathcal{W}_3}(\alpha,\beta)>H_k^{\mathcal{W}_4}(\alpha,\beta)$. This fact implies that

$$f_1\cdot\frac{R_{\max}}{R_{\max}+(\alpha+krR_{\max})d_k}+f_2\cdot\frac{R_{\max}}{R_{\max}+(\alpha+krR_{\max})d'_k} < f_3\cdot\frac{R_{\max}}{R_{\max}+(\alpha+krR_{\max})d_k},$$

where f_1, f_2, and f_3 are determined by $\mathcal{W}_3$ and $\mathcal{W}_4$. To prove that $H_{k+1}^{\mathcal{W}_3}(\alpha,\beta)>H_{k+1}^{\mathcal{W}_4}(\alpha,\beta)$, it is sufficient to show the following:

$$\frac{f_1\cdot(\alpha+krR_{\max})d_k}{R_{\max}+(\alpha+krR_{\max})d_k}\cdot\frac{R_{\max}}{R_{\max}+(\alpha+(k+1)rR_{\max})d_{k+1}}+ \frac{f_2\cdot(\alpha+krR_{\max})d'_k}{R_{\max}+(\alpha+krR_{\max})d'_k}\cdot\frac{R_{\max}}{R_{\max}+(\alpha+(k+1)rR_{\max})d'_{k+1}}< \frac{f_3\cdot(\alpha+krR_{\max})d_k}{R_{\max}+(\alpha+krR_{\max})d_k}\cdot\frac{R_{\max}}{R_{\max}+(\alpha+(k+1)rR_{\max})d_{k+1}}. \tag{33}$$

Then the above equation can be derived as follows:

$$\begin{aligned}&(\alpha+krR_{\max})^2(\beta'-\beta)+(\alpha+(k+1)rR_{\max})^2(\beta-\beta')<0\\ &\Leftrightarrow(\alpha+krR_{\max}-\beta)(\beta'rR_{\max}+(\alpha+(k+1)rR_{\max})\times\\ &(\alpha+(k+1)rR_{\max}-\beta')>(\alpha+krR_{\max}-\beta')\times\\ &(\beta rR_{\max}+(\alpha+(k+1)rR_{\max})(\alpha+(k+1)rR_{\max}-\beta))\\ &\Leftrightarrow d_k(R_{\max}+(\alpha+(k+1)rR_{\max})d'_{k+1})>d'_k\times\\ &(R_{\max}+(\alpha+(k+1)rR_{\max})d_{k+1})\Rightarrow\text{Eq. (33)}.\end{aligned} \tag{34}$$

This fact implies that if $\frac{\partial H_k^{\mathcal{W}_4}}{\partial x}\Big|_{x=0}$ is negative when $k=k_0$, $\frac{\partial H_k^{\mathcal{W}_4}}{\partial x}\Big|_{x=0}$ is negative for all $k>k_0$.

Now, we consider when l_k for $k\geq 1$ has an additional break point. Let us assume that there are two random walks $\mathcal{W}_1^k$ and $\mathcal{W}_2^k$, where $\mathcal{W}_2^k$ has an additional break point $(\alpha+krR_{\max},\beta_2)$ on l_k $(k\geq 1)$ below the final break point $(\alpha+krR_{\max},\beta_1)$ located on l_k $(k\geq 1)$ in the random walk $\mathcal{W}_1^k$. Here, we assume that $\beta_2=(1+rx)\beta_1$. Then, $H_{k+1}^{\mathcal{W}_1^k}<H_{k+1}^{\mathcal{W}_2^k}$, and this is easily proven by using the proof of that $H_1^{\mathcal{W}_1}<H_1^{\mathcal{W}_2}$, which is described above. In addition, if $\frac{\partial H_{k+1}^{\mathcal{W}_2^k}-H_{k+1}^{\mathcal{W}_1^k}}{\partial x}\Big|_{x=0}$ positive, it is always greater than $\frac{H_{k+1}^{\mathcal{W}_2^k}-H_{k+1}^{\mathcal{W}_1^k}}{x}$ for any $0<x<\frac{1}{r}\cdot\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta_1}-1\right)$, and thus $H_{k+1}^{\mathcal{W}_2^k}(\alpha,\beta)$ can more efficiently increase when x is closer to 0.

Next, we consider $H_{k+N}^{\mathcal{W}_1^k}(\alpha,\beta)$ and $H_{k+N}^{\mathcal{W}_2^k}(\alpha,\beta)$. The derivative $\frac{\partial(H_{k+N}^{\mathcal{W}_2^k}-H_{k+N}^{\mathcal{W}_1^k})}{\partial x}\Big|_{x=0}$ is equal to $\frac{\partial H_{k+N}^{\mathcal{W}_2^k}}{\partial x}\Big|_{x=0}$, and it can be expressed as

$$-rA_k^N\cdot\sum_{i=0}^{N-1}\frac{(l+k+i)^2}{((l+k+i)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-k-i+1)^2}\times \frac{1+(l+k+i)((l+k+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}{(l+k+i)((l+k+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}+rA_k^N\times \frac{(l+k+N)^2}{((l+k+N)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-k-N+1)^2}\times \left(1+(l+k+N)((l+k+N)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)\right),$$

where $R'_{\max}=rR_{\max}$, $l=\frac{\alpha}{R'_{\max}}$, and

$$A_k^N=\prod_{i=k}^{k+N-1}\frac{(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}{rR_{\max}+(\alpha+irR_{\max})\left(\frac{\alpha+irR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}\times\frac{rR_{\max}}{rR_{\max}+(\alpha+(k+N)rR_{\max})\left(\frac{\alpha+(k+N)rR_{\max}}{(1+\varepsilon)\beta(1+rx)}-1\right)}.$$

This implies that if $\frac{\partial H_{k+N}^{\mathcal{W}_2^k}}{\partial x}\Big|_{x=0}$ is positive when $k=k_0$, $\frac{\partial H_{k+N}^{\mathcal{W}_2^k}}{\partial x}\Big|_{x=0}$ is positive for all $k>k_0$. In fact, when $k=1$, $\frac{\partial H_{k+N}^{\mathcal{W}_2^k}}{\partial x}\Big|_{x=0}$ is positive regardless of N and α. Therefore, for

all $k>0$, $\frac{\partial H_{k+N}^{\mathcal{W}_2^k}}{\partial x}\Big|_{x=0}$ is positive regardless of N and α. In other words, $H_k^{\mathcal{W}}(\alpha,\beta)$ can be maximized when line l_i has infinitely many break points for all $0<i<k$.

When we define the random walk $\mathcal{W}_{\max}^k$ as $\mathcal{W}_{\max}^k = \arg\max_{\mathcal{W}} H_k^{\mathcal{W}}(\alpha,\beta)$, the random walk $\mathcal{W}_{\max}^k$ has infinite break points on l_i for $0<i<k$. Formally, there always exist break points in interval $(\alpha+irR_{\max},(\beta_1,\beta_2))$, for $\beta\le\beta_1<\beta_2\le\frac{\alpha+irR_{\max}}{1+\varepsilon}$. Meanwhile, $\mathcal{W}_{\max}^k$ has no break point on l_k. In other words, in $\mathcal{W}_{\max}^k$, whenever a point moves to the line $l_k:\alpha_{n_i}=\alpha+krR_{\max}$, the point can reach the target zone where $\frac{\alpha_{n_i}}{\alpha_{n_j}}\le 1+\varepsilon$, without break points. Considering the above facts, the following holds:

$$\max_{\mathcal{W}} H_k^{\mathcal{W}}(\alpha,\beta) = H_k^{\mathcal{W}_{\max}^k}(\alpha,\beta) = \lim_{d\to 0}\sum_{\forall j<k:\sum_{i=0}^{j}x_i<m_j^d}\left\{\frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\cdot D_k}\times\prod_{i=0}^{k-1}h_i(x_i,d)\right\}, \tag{35}$$

where

$$m_j^d=\log_{1+rd}\left(\frac{\alpha+jrR_{\max}}{(1+\varepsilon)\beta}\right)\text{ for }j>0,\ m_0^d=\log_{1+rd}\left(\frac{\alpha+jrR_{\max}}{(1+\varepsilon)\beta^\star}\right),$$
$$D_k=\frac{1}{r}\cdot\left(\frac{\alpha+krR_{\max}}{(1+\varepsilon)\beta(1+rd)^{\sum_{i=0}^{k-1}x_i}}-1\right),$$
$$h_i(x_i,d)=\left(\frac{rR_{\max}}{rR_{\max}+(\alpha+irR_{\max})d}\right)^{x_i}\cdot\left(\frac{(\alpha+irR_{\max})d}{rR_{\max}+(\alpha+irR_{\max})d}\right)$$

The notation $\beta^\star$ denotes the root of the following equation for β:

$$\sum_{i=0}^{k-1}\frac{(l+i)^2}{((l+i)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-i+1)^2}\times\frac{1+(l+i)((l+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}{(l+i)((l+i)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)}=\frac{(l+k)^2}{((l+k)^2\frac{R'_{\max}}{(1+\varepsilon)\beta}-l-k+1)^2}\times\left(1+(l+k)((l+k)\frac{R'_{\max}}{(1+\varepsilon)\beta}-1)\right),$$

where $R'_{\max}=rR_{\max}$ and $l=\frac{\alpha}{R'_{\max}}$. Note that the root is unique. Then we denote $g_k(\alpha,\beta)$ by $H_k^{\mathcal{W}_{\max}^k}(\alpha,\beta)$ for ease of reading.

Finally, because

$$\max_{x=R_{\max}}\Pr\left(\frac{\alpha}{\beta}\to 1+\varepsilon\,\middle|\,(\alpha,\beta)\right)=\max\sum_{k=0}^{\infty}P_k^{\varepsilon}(\alpha,\beta)\le\sum_{k=0}^{\infty}\max P_k^{\varepsilon}(\alpha,\beta)=\sum_{k=0}^{\infty}g_i(\alpha,\beta),$$

the probability for a state $(\alpha_{n_i},\alpha_{n_j})$ starting from (α,β) to reach the target zone in which satisfies $\frac{\alpha_{n_i}}{\alpha_{n_j}}\le 1+\varepsilon$ is upper bounded by

$$\lim_{\substack{d\to 0\\ n\to\infty}}\sum_{k=0}^{n}\left\{\sum_{\forall j<k:\sum_{i=0}^{j}x_i<m_j^d}\left\{\frac{rR_{\max}}{rR_{\max}+(\alpha+krR_{\max})\cdot D_k}\times\prod_{i=0}^{k-1}h_i(x_i,d)\right\}\right\}, \tag{36}$$

which is denoted by $G(\alpha,\beta)$. Note that

$$g_0(\alpha,\beta)\ge\frac{R_{\max}}{R_{\max}+\alpha d}\cdot g_0(\alpha,\beta(1+rd))\text{ and}$$
$$g_i(\alpha,\beta)\ge\frac{R_{\max}}{R_{\max}+\alpha d}\cdot g_i(\alpha,\beta(1+rd))+\frac{\alpha d}{R_{\max}+\alpha d}\cdot g_{i-1}(\alpha+rR_{\max},\beta)\ \ \forall i>0.$$

Therefore, the following holds:

$$G(\alpha,\beta)\ge\frac{R_{\max}}{R_{\max}+\alpha d}\cdot G(\alpha,\beta(1+rd))+\frac{\alpha d}{R_{\max}+\alpha d}\cdot G(\alpha+rR_{\max},\beta).$$

Also, Eq. (27) is the maximum when $x=R_{\max}$. More specifically, Eq. (27) has a similar form to that shown in Fig. 2. Lastly, because the limit value of $G(\alpha,\beta)$ when α goes to infinity is 0, it is a constant in terms of x. As a result,

$$\lim_{t\to\infty}\Pr\left[\frac{EP_{\max}^t}{EP_\delta^t}<1+\varepsilon\right]<G(\alpha_{\texttt{MAX}},\alpha_\delta),$$

and $G(\alpha_{\texttt{MAX}},\alpha_\delta)$ is denoted by $G^\varepsilon(f_\delta,\frac{rR_{\max}}{\alpha_{\texttt{MAX}}})$ in Theorem V.3. Moreover, the limit value of $G^\varepsilon(f_\delta,\frac{rR_{\max}}{\alpha_{\texttt{MAX}}})$ when f_δ goes to 0 is 0. This completes the proof of Theorem V.3.

Appendix E
Simulation

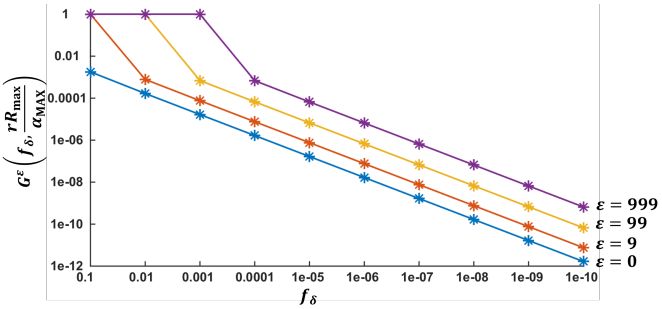


Figure 6. In this figure, when $\frac{rR_{\max}}{\alpha_{\texttt{MAX}}}$ is 10^{-2}, $G^\varepsilon(f_\delta,\frac{rR_{\max}}{\alpha_{\texttt{MAX}}})$ (y-axis) is presented with regard to f_δ (x-axis) and ε.

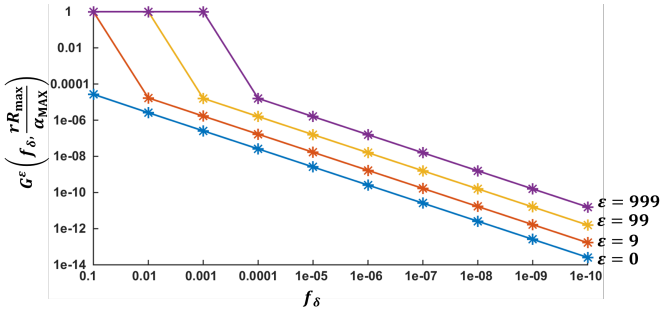


Figure 7. In this figure, when $\frac{rR_{\max}}{\alpha_{\max}}$ is 10^{-4}, $G^{\varepsilon}(f_{\delta}, \frac{rR_{\max}}{\alpha_{\max}})$ (y-axis) is presented with regard to f_{δ} (x-axis) and ε.