DECENT-BRM: DECENTRALIZATION THROUGH BLOCK REWARD MECHANISMS

A PREPRINT

Varul Srivastava
Machine Learning Lab
IIIT Hyderabad
varul.srivastava@research.iiit.ac.in

Dr. Sujit Gujar
Machine Learning Lab
IIIT Hyderabad
sujit.gujar@iiit.ac.in

June 28, 2025

ABSTRACT

Proof-of-Work is a consensus algorithm where miners solve cryptographic puzzles to mine blocks and obtain a reward through some Block Reward Mechanism (BRM). PoW blockchain faces the problem of centralization due to the formation of mining pools, where miners mine blocks as a group and distribute rewards. The rationale is to reduce the risk (variance) in reward while obtaining the same expected block reward. In this work, we address the problem of centralization due to mining pools in PoW blockchain. We propose a two-player game between the new miner joining the system and the PoW blockchain system.

We model the utility for the incoming miner as a combination of (i) expected block reward, (ii) risk, and (iii) cost of switching between different mining pools. With this utility structure, we analyze the equilibrium strategy of the incoming miner for different BRMs: (a) memoryless – block reward is history independent (e.g., Bitcoin) (b) retentive: block reward is history-dependent (e.g., Fruitchains). For memoryless BRMs, we show that depending on the coefficient of switching cost c, the protocol is decentralized when $c = 0$ and centralized when $c > \underline{c}$. In addition, we show the impossibility of constructing a memoryless BRM where solo mining gives a higher payoff than forming/joining mining pools. While retentive BRM in Fruitchains reduces risk in solo mining, the equilibrium strategy for incoming miners is still to join mining pools, leading to centralization. We then propose our novel retentive BRM – Decent-BRM. We show that under Decent-BRM, incoming miners obtain higher utility in solo mining than joining mining pools. Therefore, no mining pools are formed, and the Pow blockchain using Decent-BRM is decentralized.

1 Introduction

In Proof-of-Work (PoW) blockchains, the participants are called *miners*. Each miner devotes some computing power to solving a cryptographic puzzle. If a miner solves this puzzle, a block is mined and the miner is rewarded. Each miner has a certain hash rate, which roughly translates to the total number of queries the miner can make to solve the puzzle in one unit time. However, with the wide adoption of PoW blockchains and the recent rapid growth in the performance of mining hardware (from CPUs to GPUs and now ASICs) an "arms race" of computing power has caused the total Hash-rate for the cryptocurrency to rise to unprecedented levels. Although the expected reward for each miner remains the same, their variance in reward has increased drastically.

Mining Pools. The probability of mining a block increases because of the increased mining power of the pool but the total reward obtained on each block for each miner part of the pool goes down. There exist multiple RSSs such as Pay-Per-Share (PPS), Pay-Per-Last-N-Shares (PPLNS), Proportional, Geometric etc. However, Roughgarden and Shikhelman [2021] analysed and showed that PPS and PPLNS are variance-optimal RSS under certain conditions. Increase in the popularity of mining pools as a lower-risk alternative to solo mining, the hash rate of these pools has been increasing. Due to this, few mining pools have grown disproportionately large and might be a cause of concern for the underlying PoW blockchain protocol.

Protocol Design for Decentralized PoW. There have been several protocols Kiffer and Rajaraman [2021], Lao [2014], Bazzanella and Gangemi [2023], Kim et al. [2023], 21- [2014], Luu et al. [2017], Bissias and Levine [2017], Pass and Shi [2017] proposed in an attempt to reduce centralization in PoW blockchains by disincentivizing pool formation. These work incentivize solo mining by (i) decreasing variance in block proposal Bazzanella and Gangemi [2023], Kim et al. [2023], or (ii) decreasing variance through different Block reward mechanisms Pass and Shi [2017], Kiffer and Rajaraman [2021]. However, utility for miners under this reduced variance still incentivizes the formation of mining pools, and such PoW blockchains are still centralized Stouka and Zacharias [2023].

With the increased popularity of peer-to-peer, *decentralized* cryptocurrencies such as Bitcoin and Ethereum, more and more users are interested in possessing those coins/tokens. Users obtain cryptocurrency tokens by purchasing from those who mint or themself mint the tokens. The cryptocurrencies keep transaction records through a distributed ledger, and a distributed consensus protocol is required to maintain a consistent ledger across all users. Nakamoto [2009] proposed a blockchain technology via a *Proof-of-Work* (PoW) consensus protocol for the same. In PoW, the interested parties can join the network and need to solve some cryptographic puzzle to *mine* the next block, thereby appending a set of transactions (contained in the block) to the ledger. In return, the first node, *miner*, to solve the puzzle is rewarded with newly minted coins according to some Block Reward Mechanism (BRM).

Mining Pools. Due to the increasing popularity of cryptocurrencies, there has been 10x growth in computing power used for mining Bitcoins in the last five years Asmakov [2023], as evident from Figure 1. The mining of a block is a random event, and *solo miners* with limited computing power face risk due to the uncertainty about mining any blocks for a prolonged duration. To minimize the risk, miners come together and form *mining pools* and distribute rewards when the pool mines a block. The formation of mining pools leads to the same expected rewards but much more frequent payment, reducing the risk. Due to this, few mining pools have grown disproportionately large. E.g., the top three mining pools in Bitcoin control a majority of the computing power in Bitcoin: Foundry USA ($\approx 29\%$), Ant Pool ($\approx 16\%$) and F2 Pool (14%) control a 59% of the total mining power (Figure 2). The top 3 pools in ZCash Hopwood et al. [2016] are Nanopool ($\approx 25\%$), Mining Pool Hub ($\approx 18\%$), and Suprnova ($\approx 8\%$), control the majority ($> 50\%$) of the mining power. The security of the PoW-based blockchains relies on the fact that no authority controls the majority of the computing power. Such unprecedented levels of centralization could pose a severe security threat to the PoW blockchains.

Threat Due to Centralization. The security of PoW protocols relies on honest majority assumption, i.e., $> 50\%$ of the mining power is controlled by honest players. However, if the majority of the mining power is concentrated with a small number of mining pools, then the protocol is under severe threat and faces the risk of censorship attacks, denial of service attacks, and security compromise, among other attacks. It would be easy to double-spend coins if the top mining pools, controlling $> 50\%$ computing power, come together Badertscher et al. [2021]. The challenge of $> 50\%$ majority with a single mining pool is not new. For example, GHash.IO Matonis [2014] controlled the majority (55%) of the Bitcoin network in June 2014. Due to this, the public trust in the currency dropped. GHash.IO has since committed to limiting its mining power to $< 40\%$ Matonis [2014].Thus, it is crucial to address the problem of centralization in the PoW blockchain caused by the formation of mining pools. Miners are rational and interested in maximizing their rewards while minimizing risks. Hence, studying the event of a new miner joining mining pools as a game is natural. The researchers have looked at how mining pools through game theory, focusing on optimal RSS Roughgarden and Shikhelman [2021], Fisch et al. [2017a], or maximizing miner utility Chatzigiannis et al. [2022], Cortes-Cubero et al. [2023]. However, a limited analysis of the centralization of PoW through mining pools necessitates its investigation.

Our Goal

This work aims to study a miner joining the PoW system as a game and analyze conditions under which the system tends to be centralized or decentralized. In addition, we aim to construct a mechanism under which the formation of mining pools is not profitable over solo mining, and the system remains decentralized.

Our Approach. To analyze the behavior of a miner joining the PoW blockchain system with different block-reward mechanisms (BRMs) represented by Γ. Towards this, we propose a two-player game $\mathcal{G}(\Gamma)$ for BRM Γ played between player p_1 deciding to join the system, and the PoW blockchain system represented as player p_2. We define the utility of p_1, which depends on (i) expected reward, (ii) risk, and (iii) function switching costs. (i) Expected rewards are a function of computing power. (ii) Since variance is an indicator of risk Chiu and Choi [2016], miners intend to reduce this risk. We model it via ρ^{th} moment of the reward, which is a more general representation of risk (in literature, it is usually represented as the 2^{nd} moment, i.e. variance Chiu and Choi [2016], Roughgarden and Shikhelman [2021]). (iii) modeling switching costs are needed to account for the cost in hash queries, network latency, etc., in switching from one mining pool to another during the mining process (Section 4.2). We also define the conditions of (i) Fairness (motivated by conditions of unbiased Reward Sharing Scheme of Roughgarden and Shikhelman [2021]) and (ii) ρ-Decentralization.

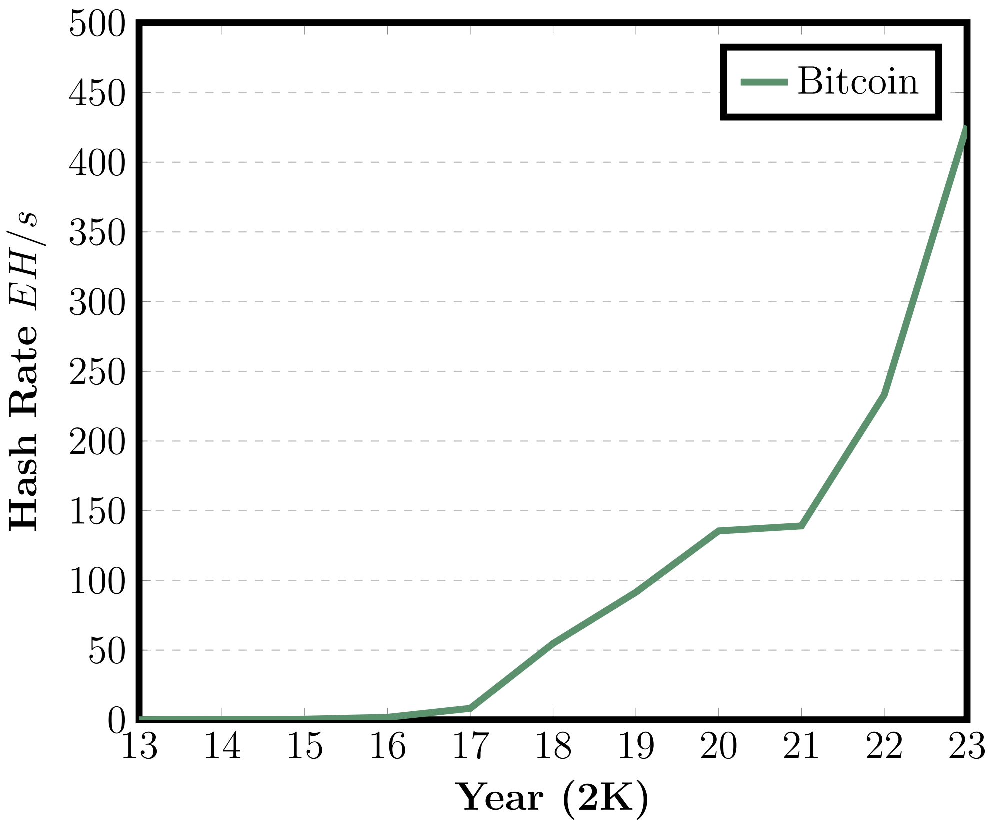

Figure 1: Bitcoin Hashrate over 10 years emp

To analyze $\mathcal{G}(\Gamma)$, we categorize BRMs into two types, *memoryless* and *retentive*. Suggestive by the nomenclature, memoryless BRMs (eg. Bitcoin Nakamoto [2009]) are such that the reward given for any block is independent of the ledger's history and retentive BRMs employ use of ledger's history while distributing reward (eg. Fruitchain Pass and Shi [2017]).

Our Contributions

First, we study memoryless BRMs and model switching costs through a parameter c and function D. If $c = 0$ (i.e., it does not assign any switching cost), player p_1 distributes the mining power across mining pools, implying decentralization is possible. However, we show an impossibility result that no memoryless BRM can assure ρ-decentralization if switching costs exceed a certain threshold. Hence, we turn to retentive BRMs (eg. Fruitchains Pass and Shi [2017]), where the reward given for any block depends on historical entries in the ledger. Our analysis shows that Fruitchain reduces risk and increases utility for solo mining. However, joining mining pools is still a better strategy than solo mining (because mining pools also experience reduced risk). Despite the above negative results, we show that retentive BRMs increase the utility of solo mining. Taking motivation from this, we propose our novel BRM decentBRM. In decentBRM, if a block is mined, the reward is distributed among all the miners who have mined blocks before the current block. This protocol is such that following the solo mining strategy is an equilibrium strategy (Lemma 2). Therefore, the PoW blockchain protocol using $\Gamma_{\textsf{decentBRM}}$ is ρ-Decentralized.

In summary, the following are our contributions:

- We define a two-player game to study these BRMs where player p_1 is the miner joining the system and p_2 is the rest of the system, comprising of mining pools and different solo miners. (Section 4.1)
- In Section 4.3, we introduce the notion of ρ-Decentralization.
- We prove two results for memoryless BRMs (i) for $c = 0$ protocol is ρ-Decentralized (Lemma 1) and (ii) for $c \geq \underline{c}$, centralization is bound to happen; where $\underline{c}$ is a threshold based on the other parameters (Theorem 1).

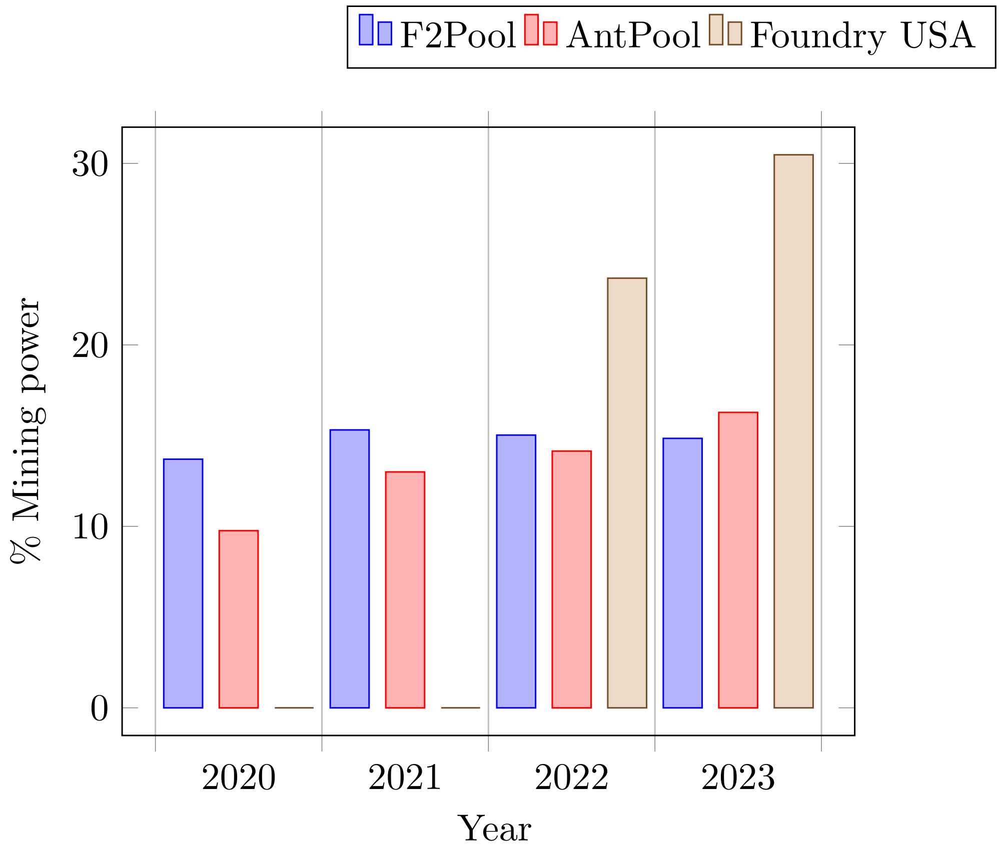

Figure 2: Centralization in Bitcoin over 4 years bit

- We also show through Theorem 2 that it is impossible to construct a memoryless BRM where solo mining is incentivized over joining mining pools.
- We propose a novel retentive BRM, namely decentBRM, that incentevizes solo mining over joining mining pools; thus, it is ρ-Decentralized. This helps in addressing the centralization of computing power in PoW blockchains.

2 Related Work

Game Theory is extensively employed for Blockchains security analysis Alkalay-Houlihan and Shah [2019], Grossi [2022], Karakostas et al. [2023], Jain et al. [2021], constructing Transaction Fees mechanism Roughgarden [2021], Chung and Shi [2023], Siddiqui et al. [2020], Consensus Chen et al. [2023], low-variance mining Roughgarden and Shikhelman [2021], Fisch et al. [2017a] et cetera.

Centralization in PoW & Mining pools. Centralization in PoW blockchains poses a major threat to protocol security Gans and Halaburda [2023], Kiayias et al. [2016], Arenas et al. [2020]. Tsabary and Eyal [2018] argues that centralization in PoW blockchains is due to high variance in reward for mining a block. As shown by Cortes-Cubero et al. [2023], the creation of mining pools reduces this variance in the reward, which miners will be willing to join even at (some limited) expense of their expected reward. Mining pools offer different reward schemes to the miners, such as the Pay-Per-Share (PPS), Proportional, Geometric, and Pay-Per-Last-N-Shares (PPLNS). Roughgarden and Shikhelman [2021] formally studied *reward sharing schemes* (RSS) opted by different mining pool strategies. While all RSS have the same expected payoff, they offer different risks (measured as variance in reward). Roughgarden and Shikhelman show that Pay-Per-Share (PPS) and Pay-Per-Last-N-Shares (PPLNS) are variance-optimal RSS under different conditions. Fisch et al. [2017a] also study reward schemes offered by mining pools from a Game Theoretic lens and find mining pool strategies that maximize optimal steady state social welfare for miners. However, these works Roughgarden and Shikhelman [2021], Fisch et al. [2017a] analyze reward-sharing schemes while our work involves analysis of Block reward mechanisms (BRMs) and the possibility of decentralization through them in the PoW system by disincentivizing the creation of mining pools. The role of BRMs for the security of blockchain Arenas et al.

[2020] and security and decentralization in PoS blockchain Motepalli and Jacobsen [2021] have already been studied. We study the role of BRMs in decentralizing PoW blockchains, which indirectly ensures security Badertscher et al. [2021], Kiayias et al. [2016] of the protocol.

Game Theoretic analysis of Miners. Game theoretic analysis of miner behaviour under PoW blockchains has also been performed previously through Mean Field Games Taghizadeh et al. [2020], Evolutionary Game Theory Liu et al. [2018] studying equilibrium under different conditions of computational power and network propagation delay. However, these works lack a general model capturing miner payoffs, risk and additional costs (such as switching costs), which are captured by our work. In addition, these works analyze the miner strategy to choose among different reward-sharing schemes under Bitcoin. In contrast, our work analyses the miner choice among different reward-sharing schemes under different block reward mechanisms, including (but not limited to) Bitcoin. Similarly, Xu et al. [2020] studies miner's dynamic choice among different mining pools. However, their utility structure is restricted to expected reward and does not account for risk (eg. variance) among other costs. Multiple other works analyze miner choice in joining pools based on reward sharing schemes, network delay, and cost of mining, such as Altman et al. [2020], Roughgarden and Shikhelman [2021], Fisch et al. [2017a], Cortes-Cubero et al. [2023], Motepalli and Jacobsen [2021]. Note that this is not an exhaustive list. Chatzigiannis et al. [2022] propose portfolio strategies for miners with different risk aversion levels to join across different mining pools and even different currencies. However, their analysis is completely empirical based on their computational tool. The goal of their experimental analysis is to find portfolio strategies which maximize risk-adjusted returns for miners, and in no way discuss and resolve centralization in PoW blockchains due to pool formation.

Protocols for Decentralized Mining. There also have been efforts to introduce mechanisms that reduce miner variance such as modification to Bitcoin Bazzanella and Gangemi [2023], Bobtail Bissias and Levine [2017], Fruitchains Pass and Shi [2017], Hybrid PoW protocols Kim et al. [2023], SmartPool Luu et al. [2017], Proof-of-Mining Lao [2014], Sign-to-Mine 21- [2014], Multi-nonce schemes Shi [2016], HaPPY-Mine Kiffer and Rajaraman [2021] among others. However, they all reduce the incentive to join mining pools or lead to small-sized mining pools. In any case, pool formation is still incentivized, and the PoW system is centralized. Stouka and Zacharias [2023] show that Fruitchains Pass and Shi [2017] reduce variance for solo mining and mining pools. Hence, it is centralized. We make similar observations in our analysis of fruitchains.

3 Preliminaries

In this section, we explain (i) blockchain preliminaries, (ii) block reward mechanisms, and (iii) the functioning of mining pools.

3.1 Blockchain Preliminaries

3.1.1 Proof-of-Work (PoW)

A *blockchain* is a ledger maintained and updated by a set of *miners* which we also refer to as *players*. The blockchain comprises an ordered chain of blocks, where a block at height k is B_k and is preceded by a "parent-block" B_{k-1} for all $k > 0$[1]. A block B_k consists of block-header and transaction data. The header contains information (1) hash (cryptographic digest) of the parent block B_{k-1} (Null genesis block), (2) height of the block k, (3) Merkle-root (cryptographic fingerprint) of the set of transactions included in the block, and (4) a random number n, called *Nonce*. Note that the block structure may vary among different PoW blockchains, but these four elements are invariably present in the block header and are sufficient for our understanding. The protocol decides on some *Target* T and considers a block *mined* if its header's hash is lesser than the target T. Thus, each miner searches for a nonce till the block is mined by investing in computing power to compute hashes. The **hash rate** of a miner is how many queries it can make in a time interval. Any **round** k is defined as the duration from after block B_{k-1} is mined till when block B_k is mined. The entire protocol is parameterized by the security parameter λ which is also the size of the Hash function.

3.1.2 Block Reward Mechanism

At round k, a PoW blockchain protocol rewards a miner for its work if it successfully mines the block B_k. Typically, the rewards are of two types: (i) *block reward* and (ii) *transaction fees*. We abstract out the *block-reward mechanism* (BRM) of the PoW blockchain for a block B_k mined in round k based on the history $\mathcal{H}_k$ at round k as $\Gamma(B_k, \mathcal{H}_k)$. At round k, for most of the PoW blockchains, BRMs offer block rewards to the miner independent of the chain's evolution till round k. We refer to such BRM as *memoryless BRM*. We formally define the memorylessness condition below.

[1] $k = 0$ is genesis block

Definition 1 (Memoryless BRM). *A BRM $\Gamma(\cdot,\cdot)$ has* memoryless *property if for any round k and any history $\mathcal{H}_k^1, \mathcal{H}_k^2$ we have*

$$\Gamma(B_k, \mathcal{H}_k^1) = \Gamma(B_k, \mathcal{H}_k^2) \tag{1}$$

A trivial BRM which is memoryless is $\Gamma(B_k, \mathcal{H}_k) = 0$ for all $B_k, \mathcal{H}_k$. Another example of memoryless BRM is bitcoin's BRM ($\Gamma_{memoryless}$). $\Gamma_{memoryless}$ rewards only the miner who has mined the current block B_k and is therefore invariant of the previous blocks mined (history). Reward in a memoryless BRM might depend on the block's height. (In Bitcoin, the block reward halves after every 210K blocks are mined.) More sophisticated BRMs can leverage the miners' historical activity and pay more to the miners working harder. Examples of such retentive (or non-memoryless) BRMs are Fruitchains Pass and Shi [2017] and decentBRM (protocol proposed in Section 6).

In memoryless BRMs, miners face much uncertainty in mining the block due to the increased competition. Instead of solo mining, often multiple miners come together for mining and share the rewards amongst themselves; though expected rewards remain the same, the risk (variance in the rewards) decreases. For example, suppose a solo miner starts mining; there is a 10% chance of mining a block with a reward of 10 coins. If two friends with the same computing power decide to mine jointly and split the rewards equally, the expected reward is still one coin each. However, now, the chance of '0' reward is 81% as opposed to 90% in solo mining. Thus, PoW mining leads to *mining pools*.

3.2 Mining Pools

In PoW blockchains, although the expected reward for each miner is sufficiently adequate, the frequency at which each miner gets rewarded (through mining a block) is very low. Multiple miners work together to mine a block. All these miners together are called a *mining pool*. As the pool has a higher mining power than individual miners, a higher chance of mining block in any round. The pool is managed by a pool manager and is constituted of multiple miners. We assume the PoW blockchain under analysis has $\mathcal{P} = \{1, 2, \ldots, p\}$ mining pools. Following is the working of mining pool i.

- Pool manager constructs the skeleton of the block the pool will attempt to mine. If the block is mined, the reward is transferred to the pool (with public key pk_i).
- Each miner tries different nonces to solve the difficulty puzzle. They send the results of some (or all) queries they made, which serve as input to the *reward-sharing scheme* (RSS) opted by the pool for when a block is mined.

We now describe the message transfer within the mining pool.

3.2.1 Message Distribution

Each mining pool comprises different miners. Miners send messages to the mining pool i, which usually comprises of the miner identity (public key) s of the miner and uniformly samples binary string $n \in \{0,1\}^\lambda$ (nonce for the block header) such that the hash of the block is $< T_i$ for some target decided by the pool. This target is easier than the PoW blockchain target (i.e. $T_i > T$). Each message belongs to the message set $\mathcal{M}$. We represent the set of messages obtained in a round k by pool i as $\mathcal{M}_k^i$. We represent the message as the tuple $m := (s, n)$.

RSS have been well studied in the literature Roughgarden and Shikhelman [2021], Fisch et al. [2017b]. Our work abstracts out the expected reward for analysis and is RSS agnostic[2].

3.2.2 Reward Sharing Scheme Roughgarden and Shikhelman [2021]

Reward Sharing Scheme (RSS) is a function that takes in the set of messages received by a mining pool, along with the identity of a miner s which is part of the pool, and outputs what fraction of the reward should be given to the miner. The set of messages received by a mining pool i in round k is $\mathcal{M}_i^k$. Then, for any miner s that is part of the pool, the RSS for pool i is a function $\psi_i(s, \mathcal{M}_i^k) \in [0,1]$. The reward given to the player s is therefore, $\Gamma_k^s := \Gamma(B_k, \mathcal{H})\psi_i(s, \mathcal{M}_i^k)$. If we are analyzing reward for a single player, then $\psi : \{s, s'\} \times \mathcal{M} \to [0,1]$ where s indicates the fraction of reward given to the miner, and s' represents the fraction given to rest of the miners. Details on Message distribution and reward sharing scheme can be found in Roughgarden and Shikhelman [2021].

As the introduction explains, we want to study centralization in mining pools. Few mining pools control most of the mining power, posing security concerns for the PoW blockchains. We assume all the miners are strategic players interested in maximizing their rewards and minimize the risk. Thus, we model problem of a player who want to join mining as a game in the next section.

[2] under certain conditions due to Claim 1

4 The Game

We consider the blockchain system with p mining pools as $\mathsf{M} = (\Gamma, \psi)$ which consists of Γ – block reward mechanism and ψ_i – reward sharing scheme opted by the mining pool i. As there is a large number of miners already in the system, we model the dilemma of a new player about how to distribute its computing power as a two-player game $\mathcal{G}(\Gamma)$ for BRM Γ. Player p_1 is the miner joining the system and p_2 abstracts the remaining system (comprising of mining pools and solo miners) into a single player.

In this section, (i) we explain different classes of player 1 – discussing risk tolerance of p_1, (ii) the strategy space of the players, (iii) the utility structure of p_1 that is joining the PoW system, and (iv) the desired properties for PoW system – fairness and decentralization.

4.1 Players

The Game consists of players $\mathcal{P} = \{p_1, p_2\}$. Player p_1 is characterized by $\theta_1 \in \mathbb{R}_{>0} \times \mathbb{N}$ represented as $\theta_1 = (M_1, \rho)$ where M_1 is the total hash rate of player p_1 and ρ is its risk-tolerance. The player p_2 has type $\theta_2 \in \mathbb{R}_{>0} \times \mathcal{A}$ where $\mathcal{A}$ is the set of possible reward sharing schemes followed by different mining pools. We make the following assumption wherever necessary: owing to the enormous mining power of the PoW blockchain system compared to any single miner bit.

Assumption 1. *For player p_1 characterized by $\theta_1 = (M_1, \rho)$ and p_2 by $\theta_2 = (M_2, A)$, the mining power of a single player is minimal compared to the rest of the system i.e. $M_1 << M_2$.*

4.1.1 Risk Tolerance

Let R_k be the random variable representing player p_1's reward in round k. The primary reason for p_1 to join one or more mining pools is minimizing the risk R_k. Solo mining has a very high variance (the second-order moment of R_k) in the reward obtained. According to Chiu and Choi [2016], `‘‘Pioneered by Nobel laureate Harry Markowitz in the 1950s, the mean-variance (MV) formulation is a fundamental theory for risk management in finance.’’`. MV is the difference between the mean reward and its standard deviation – the risk. Instead of just modelling risk through second moment of the reward, we parameterize it by a tolerance of player p_1 using $\rho \in \mathbb{N}$. A ρ-risk tolerant player will want to minimize $(\mathbb{E}[R_k^\rho])^{1/\rho}$. A very high ρ is characteristic of risk-averse whereas $\rho = 1$ is a risk-neutral. We do not consider risk-loving players as they would prefer solo mining.

4.1.2 Strategy Space and Environment

Each player follows a strategy sampled from the set $\mathcal{S} = \Delta(p+1)$ which is a $(p+1)-$simplex; $\overline{g}$ for player p_1 and $\overline{f}$ for player p_2. $\overline{g} = (g_0, g_1, \ldots, g_p)$ such that $\sum_{i=0}^{p} g_i = 1$. g_i indicates the fraction of mining power used to mine with mining pool i, and g_0 indicates the fraction used for solo mining. Similarly, $\overline{f}$ is the strategy for player p_2. Therefore, the hash rate for pool i is given by $M_2 \cdot f_i$ at the time p_1 is joining. Thus, the total of $M_2 f_0 + M_1 g_0$ computing power – solo miners use hash rate, and for each mining pool i, the hash rate is $M_2 f_i + M_1 g_i$. As $M_2 >> M_1$, we assume that the joining of a single player p_1 does not affect $\overline{f}$.

Discrete Strategy Space. The strategy space described above captures that a player can reallocate some of its mining power across different mining pools. However, practically, there will be some limit on the minimum computing power it can assign to a particular pool. Hence, we discretize the strategy space based on this minimum possible change. We define a strategy space with minimum permissible change being α as *α-Discrete Strategy Space*, formally defined in Definition 2 below.

Definition 2 (α-discrete Strategy Space)**.** *A strategy space S_α is α-discrete iff $\forall g^1, g^2 \in S_\alpha, \forall i \in \{0, 1, 2, \ldots, k\}$ $\exists l \in \mathbb{Z}_{\geq 0}$*

$$|g_i^1 - g_i^2| = l \cdot \alpha$$

4.2 Utility of a Player

Having defined players and the strategy space, we now define the utility for player p_1. Towards this, consider the random variable R_k representing the reward obtained by the player in round k. If $\Gamma(B_k, \mathcal{H}_k)$ is the (PoW protocol specific) BRM in a round k and $\psi_i : \{s_1, s_{-1}\} \times \mathcal{M} \to [0, 1]$ is the Reward Sharing Scheme (RSS) opted by pool i.

Then, the reward in round k is given by random variable R_k (randomness is due to distribution $\mathcal{M}(\overline{g}, \overline{f})$) as:

$$R_k = \begin{cases} \Gamma(B_k, \mathcal{H}_k) & \text{with prob. } \frac{g_0 M_1}{M_1+M_2} \\ \Gamma(B_k, \mathcal{H}_k)\psi_i(s_1, \mathcal{M}_{i,r}(\overline{g}, \overline{f})) & \text{with prob. } \frac{g_i M_1 + f_i M_2}{M_1+M_2} \\ 0 & \text{with prob. } \frac{f_0 M_2}{M_1+M_2} \end{cases} \tag{2}$$

4.2.1 Message Distribution

Miners who are part of some mining pool send messages to the pool during mining attempts. If the message was sent by player p_1, then public key $s = s_1$ and $s = s_{-1}$ otherwise. These messages are random variables $m \in \{s_1, s_{-1}\} \times \{0,1\}^\lambda$ induced by the hash rate distribution $\overline{g}, \overline{f}$ and is therefore represented as $\mathcal{M}(\overline{g}, \overline{f})$. The distribution is such that for any randomly sampled message $m \in \mathcal{M}_k^i(\overline{g}, \overline{f})$ in any arbitrary round k, we have:

$$m = \begin{cases} (s_1, n) & \text{with prob. } \frac{g_i M_1}{M_1 g_i + M_2 f_i} \\ (s_{-1}, n) & \text{with prob. } \frac{f_i M_2}{M_1 g_i + M_2 f_i} \end{cases}$$

Here, n is the solution to the puzzle (nonce), and λ is the size of the hash function output, also a security parameter of the protocol.

Pool Hopping / Switching Cost. Player p_1 typically may hop between different pools (called pool-hopping Cortesi et al. [2022]), to minimize risks. However, changing the pool incurs some costs, e.g., a drop in the effective hash rate. We model such pool hopping costs as *switching cost function* $D : \Delta(K+1) \to \mathbb{R}_{\geq 0}$. D has the following properties:

P1. $D(\overline{g})$ monotonically increases with $|\{g_i | g_i \neq 0; i \in \{0, 1, 2, \ldots, k\}\}|$.

P2. For $\overline{g}^1, \overline{g}^2 \in S_\alpha$, if conditions (i) $g_q^1 = g_q^2 \forall q \in [1,k]/\{i,j\}$, (ii) $g_i^1 + g_j^1 = g_i^2 + g_j^2$, and (iii) $g_i^1 \cdot g_j^1 > g_i^2 \cdot g_j^2$ holds, then $D(\overline{g}^1) \leq D(\overline{g}^2)$

The property **P1** states if a player hops across more pools, the switching cost increases as it needs to switch more frequently. The property **P2** corresponds to higher switching cost (due to more frequent switching between mining pools) if mining power is distributed more equally between two (or more) pools. In addition to this, if the strategy space is α-discrete, then the switching cost changes by at least some minimum amount D_{min} between two strategies. We call this Marginal Switching Cost and is formally defined in Definition 3.

Definition 3 (Marginal Switching Cost)**.** *For switching cost function $D(\cdot)$ and strategies $g^1, g^2 \in S_\alpha$ (when $D(\overline{g}^1) \neq D(\overline{g}^2)$) where S_α is an α-discrete Strategy space, the* Marginal cost *of switching $D_{min} > 0$ is*

$$D_{min} := \min_{g^1, g^2 \in S; g^1 \neq g^2} \left| D(g^1) - D(g^2) \right|$$

In summary, player p_1's utility constitutes reward (positively) and risk and switching costs (negatively). We weigh them with a, b, c, respectively. Thus, in a round k its utility is:

$$u_1\left(\overline{g}, \overline{f}, r; (\theta_1, \theta_2)\right) = a \cdot \mathbb{E}[R_k] - b \cdot (\mathbb{E}[R_k^\rho])^{1/\rho} - c \cdot D(\overline{g}) \tag{3}$$

Considering a discount factor $\delta \in [0,1]$ the utility of p_1 across rounds (starting from round r_0) is given by

$$U_1\left(\overline{g}, \overline{f}; (\theta_1, \theta_2)\right) = \sum_{r=r_0}^{\infty} \delta^{r-r_0} u_1\left(\overline{g}, \overline{f}, r; (M_1, \rho, M_2)\right) \tag{4}$$

We show the equilibrium strategy for player p_1 as well as fairness and decentralization defined in the next subsection are agnostic to player p_2's utility U_2 (see Remark 2). Thus, we do not need to define it and hence, we skip it.

4.3 Game Progression and Properties

The goal of this game is to model the event of player p_1 joining the system and following utility maximizing strategy $\overline{g}^* \in S_\alpha$.

4.3.1 Game

Our game progresses in two steps. First, player p_2 plays, disclosing its opted strategy $\overline{f}$ following which, player p_1 plays strategy $\overline{g}$ such that $U_1\left(\overline{g}, \overline{f}; (\theta_1, \theta_2)\right)$ is maximized. Note that p_1 observes $\overline{f}$ before playing $\overline{g}$. Thus, $\overline{g}$ can be a depends of $\overline{f}$. For notational ease, we slightly exploit notations and represent $\overline{g}_{\overline{f}}$ as just $\overline{g}$ unless necessary. Therefore optimal strategy $\overline{g}^*$ for a given strategy $\overline{f}$ is solution to the optimization problem for p_1 (after observing $\overline{f}$) given by:

$$\begin{aligned} \max_{\overline{g}} \quad & U_1\left(\overline{g}, \overline{f}; ((M_1, \rho), (M_2, A))\right) \\ \text{s.t.} \quad & g_i \geq 0 \forall i \in \{0, 1, \ldots, p\} \\ & \sum_{i \in \{0,1,\ldots,p\}} g_i = 1 \end{aligned}$$

Definition 4 (Equilibrium Strategy)**.** *For a BRM* Γ*, and game* $\mathcal{G}(\Gamma)$*, the strategy* $\overline{g}^*$ *is Equilibrium strategy for* p_1 *if* $\forall \theta_1 \in \mathbb{R}_{>0} \times \mathbb{N}, \forall \theta_2 \in \mathbb{R} \times \mathcal{A}, \forall \overline{g}^{'} \in S_\alpha$ *and* $\forall \overline{f}$ *we have*

$$U_1\left(\overline{g}^*, \overline{f}; (\theta_1, \theta_2)\right) \geq U_1\left(\overline{g}^{'}, \overline{f}; (\theta_1, \theta_2)\right)$$

We call strategy $\overline{g}^*$ *as Dominant Strategy for the given* $\overline{f}$*.*

Based on the outcome of the game, we consider the following properties which are required in our analysis.

4.3.2 Fairness

The reward sharing scheme for a mining pool i is fair for player p_1 if its reward sharing scheme serves as a hash rate estimator. This notion of fairness is motivated by the definition of unbiased RSS in Roughgarden and Shikhelman [2021]. For completeness, we define fairness wrt. our setting in Definition 5.

Definition 5 (Fairness Roughgarden and Shikhelman [2021])**.** *If mining pool* i *(controlling* f_i *fraction of total mining power* M_2*) follows Reward Sharing Scheme* $\psi_i : \{s_1, s_{-1}\} \times \mathcal{M}^* \to [0, 1]$*, then given mining pool is fair for player* p_1 *following strategy* $\overline{g}$ *if*

$$\mathbb{E}[\psi_i(1, \mathcal{M}_k^i)] = \frac{g_i M_1}{g_i M_1 + f_i M_2} \tag{5}$$

We show through the Claim 1 below that a mining pool should have a fair RSS to incentivize other miners to join the pool.

Claim 1. *If a mining pool* i *follows a RSS* ψ_i *that is not fair, then for any BRM* Γ *and corresponding game* $\mathcal{G}(\Gamma)$*, any strategy* $\overline{g}^2$ *with* $g_0^2 = x$ *and* $g_i^2 = y$ *is dominated by* $\overline{g}^1$ *with* $g_0^1 = x + y$ *and* $g_i^1 = 0$ *for* p_1*.*

4.3.3 Decentralization

The mechanism (Γ, ψ) is comprised of block reward scheme Γ and reward sharing scheme ψ. We define decentralization of a mechanism as $\rho-$Decentralized when miners joining the system have risk tolerance ρ. We call a Mechanism $\rho-$*Decentralized* if the relative mining power of the highest mining pool does not change upon a strategic player joining the system.

Definition 6 ($\rho-$Decentralized)**.** *Consider a mechanism* (Γ, ψ) *is* $\rho-$*Decentralized for game* $\mathcal{G}(\Gamma)$ *played between player* p_1 *and PoW blockchain system* p_2 *where:*

- p_1 *characterized by* $\theta_1 = (M_1, \rho)$ *follows equilibrium strategy* $\overline{g}^*$ *on observing* $\overline{f}$*.*
- p_2 *characterized by* $\theta_2 = (M_2, A)$ *follows any arbitrary strategy* $\overline{f}$

That is, $\overline{g}^*$ *satisfies*

$$\max_{i \in \{1,2,\ldots,k\}} f_i \geq \max_{j \in \{1,2,\ldots,k\}} \frac{g_j^* M_1 + f_j M_2}{M_1 + M_2} \tag{6}$$

Remark 1. *If a mechanism is* $\rho-$*Decentralized then for every player joining the system, the value of centralization decreases (or remains the same). Therefore, the mechanism ensures that the system decreases (or at least preserves) centralization in the PoW system.*

The remark follows from the definition of Decentralization (Definition 6). Consider miners m_1, m_2, m_3... joining the system leads to $G_j = \max_{i\in\{1,2,...,k\}} f_{i,j}$ where $f_{i,j}$ is the mining power of the pool i after miner m_j joins the system. Therefore, if a system is $\rho-$Decentralized, then after miners $m_1, m_2, m_3, \ldots$ with risk tolerance ρ join the system, by Definition 6, we have $G_1 \geq G_2 \geq G_3 \geq \ldots$. Therefore, centralization always decreases or remains the same.

Remark 2. *Fairness and Decentralization guarantees provided by mechanism* (Γ, ψ) *are agnostic to the utility function* $U_2(\cdot)$ *of* p_2.

Remark 2 follows from the observation that fairness property does not require any constraints on utility and decentralization property should be satisfied for all strategies followed by p_2.

In summary, the game used for analyzing centralization due to mining pools is defined as $\mathcal{G} := \langle\{p_1, p_2\}, \{\theta_1, \theta_2\}, S_\alpha, \Gamma, \mathcal{M}, (U_1, U_2)\rangle$. In the following section, we use this definition of $\mathcal{G}$ to analyse conditions that lead to centralization or decentralization of a PoW blockchain system with some BRM Γ.

5 Theoretical Analysis

This section provides analysis of (i) memoryless BRMs like Bitcoin Nakamoto [2009] ($\Gamma_{memoryless}$), (ii) retentive (non-memoryless) BRMs such as Fruitchains Pass and Shi [2017] ($\Gamma_{fruitchains}$). In this analysis, we find conditions under which these mechanisms lead to centralization and decentralization of the system. We use bitcoin reward function for memoryless BRMs because they abstract out the

5.1 Memoryless BRMs ($\Gamma_{memoryless}$)

Bitcoin is a well-known PoW-based blockchain protocol, which uses memoryless BRM (Definition 1). Consider indicator function $\mathbb{I}$ for block B_k and player with public-key s as $\mathbb{I}(s, B_k) = 1$ if the block is mined by player s and 0 otherwise. $\Gamma_{memoryless}$ in round k for player (or mining pool) with public key s is

$$\Gamma^{s_1}_{memoryless}(B_k, \mathcal{H}_k) = \mathbb{I}(s_1, B_k) R_{block}$$

For notational ease, we write the BRM $\Gamma^{s_1}_{memoryless}(B_k, \mathcal{H}_k)$ as $\Gamma^{s_1}_{memoryless,k}$. If the block is mined by the player p_1 or one of the p mining pools, p_1 gets rewarded proportionately as given by Equation 2. The game using Bitcoin-like memoryless BRMs $\Gamma_{memoryless}$ is $\mathcal{G}(\Gamma_{memoryless}) := \langle\{p_1, p_2\}, \{\theta_1, \theta_2\}, S_\alpha, \Gamma_{memoryless}, \mathcal{M}, (U_1, U_2)\rangle$. Consider player p_1 has public-key s_1 and mining pool i has public key pk_i. From Equation 2, the reward for p_1 in $\mathcal{G}(\Gamma_{memoryless})$ (after Assumption 1) is

$$R^{memoryless}_k = \begin{cases} \Gamma^{s_1}_{memoryless,k} & \text{with prob. } \frac{g_0 M_1}{M_2} \\ \Gamma^{pk_i}_{memoryless,k} \psi_i(s_1, \mathcal{M}_{i,r}(\overline{g}, \overline{f})) & \text{with prob. } f_i \\ 0 & \text{with prob. } f_0 \end{cases}$$

Due to Claim 1, mining pools follow a Fair Reward Sharing Scheme. Therefore, for pool i

$$\psi_i\left(s_1, \mathcal{M}_{i,k}(\overline{g}, \overline{f})\right) = \frac{g_i M_1}{g_i M_1 + f_i M_2} \approx \frac{g_i M_1}{f_i M_2}$$

Therefore, the utility for p_1 from Equation 3 is given as

$$\begin{aligned} U_1\left(\overline{g}, \overline{f}; ((M_1, \rho), (M_2, A))\right) \approx & a \sum_{i=1}^{p} \frac{g_i M_1}{M_2} R_{block} \\ & - b \cdot \left(R^{\rho}_{block} \cdot \sum_{i=1}^{k} \frac{g_i^{\rho}}{f_i^{\rho-1}}\right)^{1/\rho} \\ & - c \cdot D(\overline{g}) \end{aligned}$$

We first show through Lemma 1 that a PoW system with incoming player p_1 characterized by $\theta_1 = (M_1, \rho = 2)$ (i.e. variance is considered as the risk) is $\rho-$Decentralized for memoryless BRMs.

Lemma 1. *A PoW blockchain with memoryless BRM* $\Gamma_{memoryless}$ *is* $\rho-$*Decentralized under* $\mathcal{G}(\Gamma_{memoryless})$ *for any* $\rho > 1$ *if* $c = 0$.

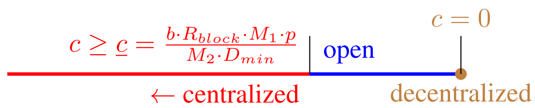

Figure 3: Bounds on switching cost parameter for $\Gamma_{memoryless}$

Proof. The proof follows by showing that given a strategy $\overline{f}$ followed by p_2 (which is observable by p_1 in $\mathcal{G}(\Gamma_{memoryless})$, the player p_1 following $\overline{g} = \overline{f}$ gives higher utility (because of lower value of risk + switching-cost) than any other strategy $\overline{g}^{'}$. The complete proof is provided in Appendix B. $\square$

We also discuss a scenario where joining the largest mining pool is the best response for a player p_1 joining the mining pool. If any new player joins the largest pool, then the PoW blockchain system will become centralized as more new miners join the system. We show in Theorem 1 below that joining the largest mining pools is the equilibrium strategy for any player p_1 joining the mining pool under certain conditions. The proof follows because this strategy's utility is higher than any other strategy given p_2 follows some $\overline{f}$. The complete proof is provided in Appendix C.

Theorem 1. *A PoW blockchain system with memoryless BRM $\Gamma_{memoryless}$ and game $\mathcal{G}(\Gamma_{memoryless})$ for player p_1 characterized by $\theta_1 \in \mathbb{R}_{>0} \times \mathbb{N}$ has equilibrium strategy $\overline{g}^*$ where $g_i^* = 1$ for $i = arg\max_{i \in \{1,2,\ldots,k\}} f_i$ if $c \geq \underline{c} = \frac{b \cdot R_{block} \cdot M_1 \cdot p}{M_2 \cdot D_{min}}$.*

For complete decentralization of the system, our goal is to ensure that mining pools are not formed. This can happen if, for any player p_1 joining the system, solo mining is incentivized over joining any subset of mining pools. For memoryless BRMs, we show the impossibility of constructing such BRMs that incentivize solo mining over pool mining for any value of $\rho > 1$ through Theorem 2.

Theorem 2. *It is impossible to construct a memoryless BRM Γ such that equilibrium strategy for p_1 characterized by $\theta_1 = (M_1, \rho)$ (for $\rho > 1$) in game $\mathcal{G}(\Gamma)$ is solo mining i.e. $\overline{g}^*$ such that $g_0^* = 1$.*

Proof. The proof follows by showing existence of another strategy $\overline{g}^{'}$ which obtains higher utility for any given $\overline{f}$ than the solo mining strategy. The complete proof is provided in Appendix D. $\square$

Need for Retentive BRMs. Lemma 1 and Theorem 1 help us find bound on c for which system is centralized, or ρ-Decentralized. We exhibit these bounds in Figure 3. We also make an interesting observation that $\underline{c}$ decreases as M_2 increases. Therefore, as the mining power of PoW blockchain system increases (which is already happening Asmakov [2023]), the system's new miners are more and more prone towards joining the largest mining pool. This fact, in addition to Theorem 2 makes us realize the need for a retentive BRM where the equilibrium strategy for miners is solo mining rather than joining or forming a mining pool.

5.2 Retentive BRMs ($\Gamma_{fruitchain}$)

In this section, we (i) provide construction of retentive BRM used in Fruitchain Blockchain Pass and Shi [2017], (ii) show that fruitchain reduces risk for solo miners (iii) show that fruitchains also fail to disincentivize the formation of mining pools.

5.2.1 Fruitchains Pass and Shi [2017]

It is a PoW-based blockchain that uses the concept of partial blocks to reduce risk in mining. Partial blocks have lesser target difficulty and are therefore easier to mine. A partial block refers to the most recent full block (blocks with higher target difficulty) B_k as their parent. When a partial block (referencing parent B_k) is mined, its status is *unconfirmed* (not a part of the ledger) and is represented as β_i^k (for the i^{th} unconfirmed partial block referencing B_k). These partial blocks are confirmed when a full block references them. That is, for some $r > k$, block B_k references β_i^k, then the partial block is considered confirmed (part of the blockchain) and represented as γ_i^k. A partial block gets rewarded when it's confirmed. The currently mined block can only confirm partial blocks that were mined within the z most recent full blocks mined. Partial blocks get rewarded $R_{partial}$ and full blocks get rewarded R_{full}. The parameters $R_{partial}, R_{full}, T_{full}$ (target difficulty of the full block), $T_{partial}$ (target difficulty of the partial block) and z are set by the system.

The current mined (full-block) is B_k then it's history is represented by

$$\begin{aligned}\mathcal{H} :=& \big(\{B_{k-1}, B_{k-2}, \ldots, B_1\}, \{\overline{\gamma}^{k-2}, \overline{\gamma}^{k-3}, \ldots, \overline{\gamma}^{2}\},\\ & \{\overline{\beta}^{k-1}, \overline{\beta}^{k-2}, \ldots, \overline{\beta}^{k-z}\}\big)\end{aligned}$$

5.2.2 Game Formulation

Consider the set of transactions confirmed in block B_k be contained in set $\mathcal{Z}_k$. Also, consider the indicator function $\mathbb{I}$ such that $\mathbb{I}(s_1, \gamma) = 1$ if some block γ is mined by player p_1 (having pub-key s_1) and 0 otherwise. Therefore, $\Gamma_{fruitchain}$ for block B_k and history $\mathcal{H}$ is represented for player p_1 as

$$\Gamma^{s_1}_{fruitchain}(B_k, \mathcal{H}_k) = R_{full}\mathbb{I}(s_1, B_k) + R_{partial} \sum_{\gamma \in \mathcal{Z}_k} \mathbb{I}(s_1, \gamma)$$

For ease of notation, we represent $\Gamma^{s_1}_{fruitchain,k}(B_k, \mathcal{H}_k) = \Gamma^{s_1}_{fruitchain,k}$. Similarly, $\mathbb{I}(pk_i, \gamma)$ is the indicator function representing if a block γ was mined by pool i with pub-key pk_i. The game using memoryless BRM similar to fruitchains is represented as $\mathcal{G}(\Gamma_{fruitchain,k})$. From Equation 2, the reward for player p_1 in $\mathcal{G}(\Gamma_{fruitchain,k})$ in round k under Assumption 1 is represented by

$$R_k^{fruitchain} = \begin{cases} \Gamma^{s_1}_{fruitchain,k} & \text{with prob. } \frac{g_0 M_1}{M_2} \\ \Gamma^{pk_i}_{fruitchain,k}\psi_i(s_1, \mathcal{M}(\overline{g}, \overline{f})) & \text{with prob. } f_i \\ 0 & \text{otherwise} \end{cases}$$

5.2.3 Analysis

The advantage of using retentive BRMs is they reduce risk for any new-coming player in case of solo mining. Consider two BRMs $\Gamma_{memoryless}, \Gamma_{fruitchain}$ as previously described and $\mathcal{G}(\Gamma_{memoryless})$ and $\mathcal{G}(\Gamma_{fruitchain})$ be the games defined over the respective BRMs. Through Theorem 3 we show that $\Gamma_{fruitchain}$ provides lower risk to player p_1 than $\Gamma_{memoryless}$.

Theorem 3. *Retentive BRM $\Gamma_{fruitchain}$ provides lower risk than $\Gamma_{memoryless}$ towards solo mining strategy to player p_1 characterized by $\theta_1 = (M_1, \rho)$ for any $\rho > 1$.*

Proof. To compare two different BRMs, we first impose the constraint that the reward distributed in one round is the same for both mechanisms. We then show that for a solo player p_1 that makes M_1 queries during which the rest of the system makes M_2 queries, we show that Utility is greater when BRM is $\Gamma_{fruitchain}$ than for $\Gamma_{memoryless}$. The complete proof is provided in Appendix E. □

Although Fruitchains reduce the risk of solo mining, it also reduces the risk for mining pools. Therefore, centralization is an issue in Fruitchains, as demonstrated by Theorem 4. Note that centralization in fruitchains has been studied under a different model by Stouka and Zacharias [2023] and the findings about fruitchains using our model align with their results.

Theorem 4. *Consider a player p_1 characterized by $\theta_1 = (M_1, \rho)$ joining the PoW blockchain system with BRM $\Gamma_{fruitchain}$. The player is always incentivized to join mining pools instead of solo mining.*

Proof. The proof follows by showing the existence of a strategy $\overline{g}$ where $g_i \neq 0$ for some $i \in \{1, 2, \ldots, p\}$ (joining mining pools). We show this strategy has higher utility than solo mining, therefore a rational player p_1 is incentivized to join mining pools than solo mining. The complete proof is provided in Appendix F. □

While fruitchains fail to achieve decentralization in the sense that solo mining is an equilibrium strategy for any new player joining the system, $\Gamma_{fruitchain}$ gives us an important insight. It reduces the gap between the optimal strategy $\overline{g}^*$ and solo mining strategy $(1, 0, 0 \ldots, 0)$. In the following section, we present a novel retentive BRM decentBRM. Under this BRM, solo mining becomes DSE after some number of rounds for any player p_1.

6 decentBRM : Optimal BRM

In this section, we (i) propose decentBRM, a risk-optimal BRM, and (ii) show that under the game $\mathcal{G}(\Gamma_{\text{decentBRM}})$, solo mining is the equilibrium strategy, which means using $\Gamma_{\text{decentBRM}}$ leads to a decentralized PoW blockchain.

decentBRM. The proposed BRM distributes rewards obtained from a block equally among miners who are part of the PoW blockchain. The reward from block B_k is distributed among miners of blocks $B_1, B_2 \ldots, B_k$ equally. This allows a player to obtain a reward proportional to its mining power in each round. Since mining is a random process, for any player joining at round r_0, we consider the expected number of blocks mined by the player to be proportional to its mining power after $r_0 + T$ with very high probability.

The implementation of this protocol can be through a special transaction that inputs two (1) block B_k, (2) B_q (for $q < k$) that was mined by public-key pk_q and (3) signature from pk_q to transfer $R_{block}\frac{B_k}{k}$ to the output address. This implementation is feasible and can be carried out through a *fork* in most of the existing PoW-based blockchains.

Next, we model this BRM under $\mathcal{G}$ and show that after T rounds from joining, p_1 performing solo mining is an equilibrium strategy.

Game Formulation. Consider a player p_1 joining the PoW blockchain with the BRM $\Gamma_{\text{decentBRM}}$. In round k where the block mined is B_k and the history $\mathcal{H}_k = \{B_{k-1}, B_{k-2}, \ldots, B_1\}$. The indicator function for block B is $\mathbb{I}(s, B) = 1$ if B is mined by a player with pub-key s and 0 otherwise. The reward R_k is given by

$$\Gamma^{s_1}_{\text{decentBRM}}(B_k, \mathcal{H}_k) = \sum_{i=1}^{k} \frac{R_{block}}{k}\mathbb{I}(s_1, B_i)$$

For ease of notation we represent $\Gamma^{s_1}_{\text{decentBRM}}(B_k, \mathcal{H}_k) = \Gamma^{s_1}_{\text{decentBRM},k}$. The game is represented as $\mathcal{G}(\Gamma_{\text{decentBRM}})$ where the reward obtained by player p_1 characterized by (M_1, ρ) in round k is given by R_k under Assumption 1. The public key for player p_1 is s_1 and for pool i is pk_i.

$$R_k^{\text{decentBRM}} = \begin{cases} \Gamma^{s_1}_{\text{decentBRM},k} & \text{with prob. } \frac{g_0 M_1}{M_2} \\ \Gamma^{pk_i}_{\text{decentBRM},k}\psi_i(s_1, \mathcal{M}(\overline{g}, \overline{f})) & \text{with prob. } f_i \\ 0 & \text{otherwise} \end{cases}$$

Analysis. We now show that decentBRM leads to a decentralized PoW blockchain system. Towards this, we show using Lemma 2 that for any player p_1 with type $\theta_1 = (M_1, \rho)$, solo mining $\overline{g}^{sm} = (1, 0, 0, \ldots, 0)$ is equilibrium strategy. The lemma follows by showing that after T rounds, the expected utility (expectation over the randomness of the mining protocol) is higher for solo mining than any other mining strategy with a very high probability. The proof is provided in Appendix G.

Lemma 2. *In the game $\mathcal{G}(\Gamma_{\text{decentBRM}})$, following solo mining strategy $\overline{g}^{sm}$ is a equilibrium strategy after T rounds from joining for player p_1 characterized by $\theta_1 = (M_1, \rho)$.*

Since following $\overline{g}^{sm}$ is DSE, then the protocol is strongly ρ-Decentralized for any ρ, in Theorem 5.

Theorem 5. *A PoW blockchain using $\Gamma_{\text{decentBRM}}$ block reward mechanism is ρ-Decentralized for any $\rho > 1$.*

Proof. From Lemma 2, we have $\Gamma_{\text{decentBRM}}$ is such that solo mining is a dominant strategy. After player p_1 joins the system:

$$\max_{i \in [1,p]} f_i > \max_{j \in \{1,2,\ldots,p\}} \frac{g_j M_1 + f_j M_2}{M_1 + M_2}$$

Therefore, the protocol is ρ-Decentralized. □

7 Conclusion & Future Work

Conclusion. To conclude, we understood through the rational decision of a new miner (player p_1) joining the PoW blockchain system (player p_2) about the decentralization guarantees of the BRM offered by the PoW blockchain under a more general utility model. We show that while bitcoin-like memoryless BRMs do not ensure decentralized BRMs, retentive BRMs offer better performance (lower risk for solo miners). We then propose decentBRM, a retentive BRM with solo mining as an equilibrium strategy. Therefore, the resulting PoW system will also be ρ-Decentralized for any ρ.

Future Work. We analyzed centralization/decentralization guarantees for the given protocol are such that for all $\rho > 1$ and $c \geq \underline{c}$ the PoW blockchain with $\Gamma_{memoryless}$ is centralized, and $c = 0$ it is ρ-Decentralized. However, there is an open gap $0 < c \leq \underline{c}$ where we don't know the guarantees of the protocol. Closing this gap is left for future work. In addition, analysis of other BRMs such as Kiffer and Rajaraman [2021], Luu et al. [2017], which uses different mining functions or smart contract functionality of another (external to the analyzed PoW system) blockchain, is left for future work.

References

Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. 2009. URL https://bitcoin.org/bitcoin.pdf.

Andrew Asmakov. Bitcoin hash rate hits new all-time high amid stagnating prices, 2023.

Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox, et al. Zcash protocol specification. *GitHub: San Francisco, CA, USA*, 4(220):32, 2016.

Total hash rate over time. https://www.blockchain.com/explorer/charts/hash-rate. Accessed: 2023-10-09.

Christian Badertscher, Yun Lu, and Vassilis Zikas. A rational protocol treatment of 51% attacks. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 3–32, Cham, 2021. Springer International Publishing. ISBN 978-3-030-84252-9.

Jon Matonis. The bitcoin mining arms race: Ghash. io and the 51% issue. *New York, NY, USA: CoinDesk, Tech. Rep*, 2014.

Tim Roughgarden and Clara Shikhelman. Ignore the extra zeroes: Variance-optimal mining pools. In Nikita Borisov and Claudia Diaz, editors, *Financial Cryptography and Data Security*, pages 233–249, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg. ISBN 978-3-662-64331-0.

Ben Fisch, Rafael Pass, and Abhi Shelat. Socially optimal mining pools. In *Web and Internet Economics: 13th International Conference, WINE 2017, Proceedings 13*, pages 205–218. Springer, 2017a.

Panagiotis Chatzigiannis, Foteini Baldimtsi, Igor Griva, and Jiasun Li. Diversification across mining pools: Optimal mining strategies under pow. *Journal of Cybersecurity*, 8(1):tyab027, 2022.

Axel Cortes-Cubero, Juan P Madrigal-Cianci, Kiran Karra, and Zixuan Zhang. Smoothening block rewards: How much should miners pay for mining pools? *arXiv preprint arXiv:2309.02297*, 2023.

Chun-Hung Chiu and Tsan-Ming Choi. Supply chain risk analysis with mean-variance models: A technical review. *Annals of Operations Research*, 240(2):489–507, 2016.

Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing*, PODC '17, page 315–324, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349925. doi:10.1145/3087801.3087809. URL https://doi.org/10.1145/3087801.3087809.

Hashrate distribution over time. https://www.blockchain.com/explorer/charts/pools-timeseries. Accessed: 2023-10-09.

Colleen Alkalay-Houlihan and Nisarg Shah. The pure price of anarchy of pool block withholding attacks in bitcoin mining. In *AAAI*, pages 1724–1731, 2019.

Davide Grossi. Social choice around the block: On the computational social choice of blockchain. In *AAMAS*, page 1788–1793, 2022.

Dimitris Karakostas, Aggelos Kiayias, and Thomas Zacharias. Blockchain nash dynamics and the pursuit of compliance. In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, AFT '22, page 281–293, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9781450398619. doi:10.1145/3558535.3559781. URL https://doi.org/10.1145/3558535.3559781.

Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. We might walk together, but i run faster: Network fairness and scalability in blockchains. In *Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems*, AAMAS '21, page 1539–1541, Richland, SC, 2021. International Foundation for Autonomous Agents and Multiagent Systems. ISBN 9781450383073.

Tim Roughgarden. Transaction fee mechanism design. *ACM SIGecom Exchanges*, 19(1):52–55, 2021.

Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 3856–3899, 2023.

Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. Bitcoinf: Achieving fairness for bitcoin in transaction fee only model. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems*, AAMAS '20, page 2008–2010, Richland, SC, 2020. International Foundation for Autonomous Agents and Multiagent Systems. ISBN 9781450375184.

Lin Chen, Lei Xu, Zhimin Gao, Ahmed Imtiaz Sunny, Keshav Kasichainula, and Weidong Shi. A game theoretical analysis of non-linear blockchain system. *Distrib. Ledger Technol.*, jul 2023. ISSN 2769-6472. doi:10.1145/3607195. URL https://doi.org/10.1145/3607195.

Joshua S. Gans and Hanna Halaburda. "zero cost" majority attacks on permissionless blockchains. Papers, arXiv.org, 2023. URL https://EconPapers.repec.org/RePEc:arx:papers:2308.06568.

Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, page 365–382, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450339360. doi:10.1145/2940716.2940773. URL `https://doi.org/10.1145/2940716.2940773`.

Marcelo Arenas, Juan Reutter, Etienne Toussaint, Martín Ugarte, Francisco Vial, and Domagoj Vrgoč. Cryptocurrency Mining Games with Economic Discount and Decreasing Rewards. In Christophe Paul and Markus Bläser, editors, *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*, volume 154 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 54:1–54:16, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. ISBN 978-3-95977-140-5. doi:10.4230/LIPIcs.STACS.2020.54.

Itay Tsabary and Ittay Eyal. The gap game. In *Proceedings of the 2018 ACM SIGSAC conference on Computer and Communications Security (CCS)*, pages 713–728, 2018.

Shashank Motepalli and Hans-Arno Jacobsen. Reward mechanism for blockchains using evolutionary game theory. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 217–224, 2021. doi:10.1109/BRAINS52497.2021.9569791.

Amirheckmat Taghizadeh, Hamed Kebriaei, and Dusit Niyato. Mean field game for equilibrium analysis of mining computational power in blockchains. *IEEE Internet of Things Journal*, 7(8):7625–7635, 2020. doi:10.1109/JIOT.2020.2988304.

Xiaojun Liu, Wenbo Wang, Dusit Niyato, Narisa Zhao, and Ping Wang. Evolutionary game for mining pool selection in blockchain networks. *IEEE Wireless Communications Letters*, 7(5):760–763, 2018. doi:10.1109/LWC.2018.2820009.

Chengzhen Xu, Kun Zhu, Ran Wang, and Yuanyuan Xu. Dynamic selection of mining pool with different reward sharing strategy in blockchain networks. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6, 2020. doi:10.1109/ICC40277.2020.9149279.

Eitan Altman, Daniel Sadoc Menasché, Alexandre Reiffers, Mandar Datar, Swapnil Dhamal, Corinne Touati, and Rachid El Azouzi. Blockchain competition between miners: A game theoretic perspective. In *Frontiers in Blockchain*, 2020.

Danilo Bazzanella and Andrea Gangemi. Bitcoin: a new proof-of-work system with reduced variance. *Financial Innovation*, 9(1):1–14, 2023.

George Dean Bissias and Brian Neil Levine. Bobtail: A proof-of-work target that minimizes blockchain mining variance (draft). *NDSS*, 2017.

Gyu Chol Kim, Gang Song Han, Ryong Chol Kim, Yong Bok Jong, Nam Hyok Kim, Il Min Han, Ung Il Han, and Je Sen Teh. Single-tiered hybrid pow consensus protocol to encourage decentralization in bitcoin. *Sec. and Commun. Netw.*, 2023, jul 2023. ISSN 1939-0114. doi:10.1155/2023/6169933. URL `https://doi.org/10.1155/2023/6169933`.

Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. {SmartPool}: Practical decentralized pooled mining. In *26th USENIX security symposium (USENIX security 17)*, pages 1409–1426, 2017.

Joe Lao. A network-dependent rewarding system: proof-of-mining. *arXiv e-prints*, pages arXiv–1409, 2014.

ziftrcoin, "a cryptocurrency to enable commerces,", 2014.

Ning Shi. A new proof-of-work mechanism for bitcoin. *Financial Innovation*, 2, 12 2016. doi:10.1186/s40854-016-0045-6.

Lucianna Kiffer and Rajmohan Rajaraman. Happy-mine: Designing a mining reward function. In Nikita Borisov and Claudia Diaz, editors, *Financial Cryptography and Data Security*, pages 250–268, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg. ISBN 978-3-662-64331-0.

A. Stouka and T. Zacharias. On the (de) centralization of fruitchains. In *2023 IEEE 36th Computer Security Foundations Symposium (CSF)*, pages 229–244, Los Alamitos, CA, USA, jul 2023. IEEE Computer Society. doi:10.1109/CSF57540.2023.00020. URL `https://doi.ieeecomputersociety.org/10.1109/CSF57540.2023.00020`.

Ben Fisch, Rafael Pass, and Abhi Shelat. Socially optimal mining pools. In *Web and Internet Economics: 13th International Conference, WINE 2017, Bangalore, India, December 17–20, 2017, Proceedings 13*, pages 205–218. Springer, 2017b.

Eugenio Cortesi, Francesco Bruschi, Stefano Secci, and Sami Taktak. A new approach for bitcoin pool-hopping detection. *Comput. Netw.*, 205(C), mar 2022. ISSN 1389-1286. doi:10.1016/j.comnet.2021.108758. URL `https://doi.org/10.1016/j.comnet.2021.108758`.

A Proof for Claim 1

Proof. Consider an arbitrary mining pool i following RSS ψ_i. Given BRM is Γ and $\mathcal{G}(\Gamma)$ is the corresponding game. We consider two cases (i) $\mathbb{E}[\psi_i(s_1, \mathcal{M}_k^i)] < \frac{g_i M_1}{g_i M_1 + f_i M_2}$ and (ii) $\mathbb{E}[\psi_i(s_1, \mathcal{M}_k^i)] > \frac{g_i M_1}{g_i M_1 + f_i M_2}$.

Case 1 $\left(\mathbb{E}[\psi_i(s_1, \mathcal{M}_k^i)] < \frac{g_i M_1}{g_i M_1 + f_i M_2}\right)$: In this case, consider the expected reward for player p_1 from investing $g_i = x$ in pool i.

$$\begin{aligned}
\mathbb{E}[R_k] =& \frac{\Gamma(B_k, \mathcal{H}_k) g_0 M_1}{M_1 + M_2} \\
&+ \sum_{j=1}^{p} \Gamma(B_k, \mathcal{H}_k) \psi_j(s_1, \mathcal{M}_k^j) \frac{f_i M_2 + g_i M_1}{M_1 + M_2} \\
=& \frac{R_{block} g_0 M_1}{M_1 + M_2} + \Gamma(B_k, \mathcal{H}_k) \psi_i(s_1, \mathcal{M}_k^i) \\
&+ \sum_{j=1, j\neq i}^{p} \Gamma(B_k, \mathcal{H}_k) \psi_j(s_1, \mathcal{M}_k^j) \frac{f_i M_2 + g_i M_1}{M_1 + M_2} \\
<& \frac{R_{block}(g_0 + g_i) M_1}{M_1 + M_2} \\
&+ \sum_{j=1, j\neq i}^{p} \Gamma(B_k, \mathcal{H}_k) \psi_j(s_1, \mathcal{M}_k^j) \frac{f_i M_2 + g_i M_1}{M_1 + M_2}
\end{aligned}$$

In the utility equation for player p_1 in the game $\mathcal{G}(\Gamma)$, coefficient a for expected reward $\mathbb{E}[R_k]$ is such that the coefficients for risk and switching cost b and c are negligible wrt. a. Further, since the increase in $\mathbb{E}[R_k]$ is non-negligible by switching from strategy $\overline{g}^2 = (g_0, g_1, \ldots, g_i, \ldots, g_p)$ to $\overline{g}^1 = (g_0 + g_i, g_1, \ldots, 0, \ldots, g_p)$, therefore player p_1 always prefers $\overline{g}^1$ over $\overline{g}^2$. Hence pool i does not get any computing resource from any p_1 of arbitrary type $\theta_1 \in \mathbb{R}_{>0} \times \mathbb{N}$.

Case 2 $\left(\mathbb{E}[\psi_i(s_1, \mathcal{M}_k^i)] > \frac{g_i M_1}{g_i M_1 + f_i M_2}\right)$: This case is infeasible for the mining pool. This is because, if for any incoming miner p_1 we have $\psi_i > \frac{g_i M_1}{g_i M_1 + f_i M_2}$, then summing over all the miners that are part of the system, we get $\psi_i > 1$. This is because for any miner part of the mining pool i, we established from Case 1 that $\psi_i \geq \frac{g_i M_1}{g_i M_1 + f_i M_2}$. However, $\psi_1 > 1$ means the mining pool is distributing more rewards than they obtain, which bankrupts the mining pool and therefore is not possible.

Having established both cases, we come to the conclusion that for any mining pool i, the RSS should be Fair according to the Definition 5 for the pool to survive and miners join the pool. ☐

B Proof for Lemma 1

Proof. We consider a game $\mathcal{G}(\Gamma_{memoryless})$ and analyse the DSE for player p_1. The utility for p_1 in any round r given by Equation 3. Since we study 2-decentralization, p_1 is of type $\theta_1 = (M_1, \rho)$ for any $M_1 \in \mathbb{R}_{>0}$. The utility for any round r is,

$$\begin{aligned}
u_i\left(\overline{g}, \overline{f}; (\theta_1, \theta_2)\right) \approx & a \sum_{i=1}^{p} \frac{g_i M_1}{M_2} R_{block} + \frac{g_0 M_1}{M_2} R_{block} \\
&+ (R_{block})^{\rho} \sum_{i=1}^{p} \frac{g_i^{\rho}}{f_i^{\rho-1}} + D(\overline{g})
\end{aligned}$$

We have due to Assumption 1, the probability of a miner p_1 solo-mining $\frac{g_0 M_1}{M_2}$ is also very small compared to her mining as part of a pool. We first show that $\overline{g} = \overline{f}$ is the minima for risk – $\mathbb{E}[R_{block}^2]$. Consider the risk when $\overline{g} = \overline{f}$.

$$(\mathbb{E}[R_{block}^{\rho}])^{1/\rho} = R_{block} \left(\sum_{i=1}^{p} \frac{g_i^{\rho}}{f_i}\right)^{1/\rho} = R_{block} \left(\sum_{i=1}^{p} f_i\right)$$

Now, consider for any $\overline{g}^{'} \neq \overline{f}$. We divide $g_i \in \overline{g}^{'}$ into three parts $X = \{i | g_i > f_i, g_i \in \overline{g}^{'}\}, Y = \{i | g_i < f_i, g_i \in \overline{g}^{'}\}$, and $Z = \{i | g_i = f_i, g_i \in \overline{g}^{'}\}$. The risk for $\overline{g}^{'}$ is given as

$$
\begin{aligned}
(\mathbb{E}[R^{\rho}_{block}])^{1/\rho} &= R_{block}\left(\sum_{l\in X}\frac{g_l^{\rho}}{f_l^{\rho-1}} + \sum_{m\in Y}\frac{g_m^{\rho}}{f_m^{\rho-1}} + \sum_{n\in Z}\frac{g_n^{\rho}}{f_n^{\rho-1}}\right)^{1/\rho} \\
&= R_{block}\left(\sum_{l\in X}\frac{(f_l+\tau_l)^{\rho}}{f_l^{\rho-1}} + \sum_{m\in Y}\frac{(f_m-\tau_m)^{\rho}}{f_m^{\rho-1}} + \sum_{n\in Z}\frac{f_n^{\rho}}{f_n^{\rho-1}}\right)^{1/\rho} \\
&\geq R_{block}\left(\sum_{i=1}^{p} f_i + \rho(\sum_{l\in X}\tau_l - \sum_{m\in Y}\tau_m)\right)^{1/\rho} \\
&= R^{\rho}_{block}\left(\sum_{i=1}^{p} f_i\right)^{1/\rho}
\end{aligned}
$$

We use the lower bound $x^v - v\cdot x^{v-1}y \leq (x-y)^v$ and $\sum_{l\in X}\tau_l = \sum_{m\in Y}\tau_m$ for obtaining the above inequality. We have obtained that if risk is $r_1 = (\mathbb{E}[R^{\rho}_{block}])^{1/\rho}$ when $\overline{g} = \overline{f}$ and $r_2 = (\mathbb{E}[R^{\rho}_{block}])^{1/\rho}$ when $\overline{g} \neq \overline{f}$, then $r_1 \leq r_2$. Hence, strategy $\overline{g} = \overline{f}$ is risk-otpimal for any ρ.

Since, (i) expected reward is the same for all strategies $\overline{g}$, (ii) risk is minimized for strategy $\overline{g} = \overline{f}$ and (iii) $c = 0$, the strategy $\overline{g} = \overline{f}$ gives the optimal utility for p_1. $\square$

C Proof for Theorem 1

Proof. To prove this theorem, we consider the utility from two strategies (1) $\overline{g}^1$ where $g_i^1 = 1$ for $i = arg\max_{j\in[1,p]} f_j$ and 0 otherwise, (2) any other $\overline{g}^2 \in S_\alpha$ in α-Marginal Strategy space. Wlog. we take $f_1 \geq f_2 \geq \ldots \geq f_p$. Consider the utility of player p_1 in Game $\mathcal{G}(\Gamma_{memoryless})$ following strategy $\overline{g}^1$ after Assumption 1 as

$$U_1 = u_1\left(\overline{g}^1, \overline{f}; (\theta_1,\theta_2)\right) \approx \frac{aR_{block}M_1}{M_2} - \left(\frac{b\cdot R_{block}M_1}{M_2 f_1^{(\rho-1)/\rho}}\right) - c\cdot D(\overline{g}^1)$$

Similarly, consider the utility for some strategy $\overline{g}^2 = (g_1, g_2, \ldots, g_p)$ after Assumption 1 is,

$$
\begin{aligned}
U_2 = u_1\left(\overline{g}^2, \overline{f}; (\theta_1,\theta_2)\right) &\approx \frac{aR_{block}M_1}{M_2} - c\cdot D(\overline{g}^2) \\
&\quad - \frac{b\cdot R_{block}M_1}{M_2}\left(\sum_{j=1}^{p}\frac{g_j^{\rho}}{f_j^{\rho-1}}\right)^{1/\rho}
\end{aligned}
$$

We now take the value $U_1 - U_2$ which gives us

$$
\begin{aligned}
U_1 - U_2 =& c\cdot(D(\overline{g}^2) - D(\overline{g}^1)) \\
&- \frac{b\cdot R_{block}M_1}{M_2}\left(\frac{1}{f_1^{(\rho-1)/\rho}} - (\sum_{j=1}^{p}\frac{g_j^{\rho}}{f_j^{\rho-1}})^{1/\rho}\right) \\
\geq& c\cdot(D(\overline{g}^2) - D(\overline{g}^1)) \\
&- \frac{b\cdot R_{block}M_1}{M_2}\left(p^{(\rho-1)/\rho} - 1\right) \\
\geq& c\cdot D_{min} - \frac{b\cdot R_{block}M_1 p^{(\rho-1)/\rho}}{M_2} \\
\geq& c\cdot D_{min} - \frac{b\cdot R_{block}M_1 p}{M_2} \geq 0
\end{aligned}
$$

The first inequality comes from the lower bound on $\left(\sum_i \frac{g_i^{\rho}}{f_i^{\rho-1}}\right) = 1$ from proof of Theorem 1 in Appendix B and $\frac{1}{f_1} \leq p$ by simple algebra (note $f_1 \geq f_2 \geq \ldots \geq f_p$). Second inequality comes since $\overline{g}^1, \overline{g}^2 \in S_\alpha$ are two distinct points on

α-Marginal Strategy Space, therefore $|D(\overline{g}^2) - D(\overline{g}^1)| \geq D_{min}$. However, by property **P1** of the function D, we have $D(\overline{g}^2) \geq D(\overline{g}^1)$. Therefore, $D(\overline{g}^2) - D(\overline{g}^1) \geq D_{min}$. The last inequality comes from $c \cdot M_2 \cdot D_{min} \geq b \cdot R_{block} \cdot M_1 p$.

Therefore, $U_1 \geq U_2$. This means strategy $\overline{g}^1$ is Equilibrium from Definition 4 and therefore the system becomes centralized as all the new miners are incentivized to join the largest mining pool. □

D Proof for Theorem 2

Proof. To prove this theorem, we consider payoff in any arbitrary round k where the block mined is B_k and history is $\mathcal{H}_k$. The memoryless BRM is $\Gamma_{memoryless}$ and game is $\mathcal{G}(\Gamma_{memoryless})$. Wlog. consider $f_1 \geq f_2 \geq \ldots f_p$. To show that any memoryless BRM will lead to the formation of mining pools, we compare utility for player p_1 of any type $\theta_1 \in \mathbb{R}_{>0} \times \mathbb{N}$ for two strategies:

- $\overline{g}^{lm}$ – when p_1 dedicates mining power largest mining pool. Here $g_i^{lm} = 1$ $i = arg\max_{j \in [1,k]} f_j$. Utility for this strategy is $U_{lm} = u_1\left(\overline{g}^{lm}, \overline{f}; (\theta_1, \theta_2)\right)$.
- $\overline{g}^{sm}$ – when miner dedicates their entire mining power to solo mining. In this case, $g_0^{sm} = 1$. Utility for this strategy is $U_{sm} = u_1\left(\overline{g}^{sm}, \overline{f}; (\theta_1, \theta_2)\right)$.

After Assumptions 1 utility U_{lm} and U_{sm} are given as

$$U_{lm} = \frac{a \cdot R_{block} \cdot M_1}{M_2} - \frac{b \cdot R_{block} \cdot M_1}{M_2}(f_1)^{1/\rho} - c \cdot D(\overline{g}^{lm})$$

$$U_{sm} = \frac{a \cdot R_{block} \cdot M_1}{M_2} - \frac{b \cdot R_{block} \cdot M_1^{1/\rho}}{M_2^{1/\rho}} - c \cdot D(\overline{g}^{sm})$$

We make the simple observation that (i) $D(\overline{g}^{sm}) \neq D(\overline{g}^{lm})$ and (ii) from Assumption$\frac{M_1}{M_2} << 1 \implies \left(\frac{M_1}{M_2}\right)^{1/\rho} > \frac{p \cdot M_1}{M_2} > \frac{f_1 \cdot M_1}{M_2}$. Therefore, $U_{lm} > U_{sm}$ for $\rho > 1$. With this, we conclude that $\overline{g}^{sm}$ (solo-mining strategy) is always dominated by $\overline{g} = \overline{f}$ which means mining pools will exist in Memoryless BRMs. □

E Proof for Theorem 3

Proof. To prove this theorem, we consider the ratio of the risk (ρ^{th} moment) to the expected payoff (raised to ρ^{th} power) for any player p_1 that is mining in the PoW blockchain in two cases – $\Gamma_{memoryless}$ and $\Gamma_{fruitchain}$. The Target difficulty for full blocks in Fruitchains as well as Bitcoin is T_{full} and for partial blocks in Fruitchains is $T_{partial}$. Since it is easier to mine a partial block, we have $T_{full} < T_{partial}$. The number of partial blocks mined in expectation, for every full block in fruitchains is, therefore, $\frac{T_{partial}}{T_{full}}$[3]. In addition, reward given on mining a full block in fruitchains should be equal to the reward from memoryless BRMs. Therefore,

$$R_{block} = R_{full} + \frac{T_{partial}}{T_{full}} \cdot R_{partial} \tag{7}$$

We now calculate $(\mathbb{E}[R_k^\rho])^{1/\rho}$ for both Memoryless BRMs which we call $Risk_{memoryless}$ and fruitchains which we call $Risk_{fruitchain}$.

Case 1 ($\Gamma_{memoryless}$): The game being played is $\mathcal{G}(\Gamma_{memoryless})$ and player p_1 has type $\theta_1 = (M_1, \rho)$ and player p_2 has type $\theta_2 = (M_2, A)$. This means, by the time system makes M_2 queries for mining, the player p_1 makes M_1 queries. The probability of a query made by p_1 in mining a block is $\gamma_1 = \frac{T_{full}}{2^\lambda}$. The reward obtained is R_{block}. Therefore,

$$Risk_{memoryless} = (E[R_k^\rho])^{1/\rho} = \gamma_1^{1/\rho} \cdot R_{block}$$

Case 2 ($\Gamma_{fruitchain}$): The game being played is $\mathcal{G}(\Gamma_{fruitchain})$ and the p_1 has type $\theta_1 = (M_1, \rho)$ and player p_2 has type $\theta_2 = (M_2, A)$. Probability of mining in one query a full block is $\gamma_1 = \frac{T_{full}}{2^\lambda}$ and for partial block is $\gamma_2 = \frac{T_{partial}}{2^\lambda}$. The reward obtained is R_{full} and $R_{partial}$ respectively. Therefore,

$$Risk_{fruitchain} = (E[R_k^\rho])^{1/\rho} = \left(\gamma_1 R_{full}^\rho + \gamma_2 R_{partial}^\rho\right)^{1/\rho}$$

[3]The result follows from simple probability theory, but details can be found in Pass and Shi [2017]

Now we calculate the ratio of risks below

$$\begin{aligned}\frac{Risk_{fruitchain}}{Risk_{memoryless}} &= \left(\frac{\gamma_1 R^{\rho}_{full} + \gamma_2 R^{\rho}_{partial}}{R^{\rho}_{block}\gamma_1}\right)^{1/\rho} \\ &\leq \left(1 - \frac{R_{partial}(\gamma_1 T^{\rho}_{partial} - \gamma_2 T^{\rho}_{full})}{R^{\rho}_{block} T^{\rho}_{full}\gamma_1}\right) \\ &< 1\end{aligned}$$

The first inequality is obtained from $R_{full} = R_{block} - \frac{T_{partial}}{T_{full}} R_{partial}$ and second inequality is obtained because for any $\rho > 1$ we have $\gamma_1 T^{\rho}_{partial} - \gamma_2 T^{\rho}_{full} > 0$. Therefore, we show that $Risk_{fruitchains} < Risk_{memoryless}$ for solo miners. Since strategy $\overline{g}$ is the same in both cases, the switching cost is the same for both Memoryless BRMs and Fruitchains. In addition, the expected reward remains the same due to Equation 7 in the Appendix. Hence, the utility for solo miners is higher in fruitchains than memoryless BRMs for the same expected block reward. □

F Proof for Theorem 4

Proof. Consider a player p_1 characterized by $\theta_1 = (M_1, \rho)$ and p_2 characterized by (M_2, A). The game being played is $\mathcal{G}(\Gamma_{fruitchain})$. Player p_1 plays after observing $\overline{f}$ (strategy chosen by p_2). Wlog. consider $f_1 \geq f_2 \geq \ldots f_p$. Consider a round k where block B_k is mined. We need to show that joining mining pools dominates the strategy to perform solo mining. We represent the strategies:

- $\overline{g}^{sm} = (1, 0, 0, \ldots, 0)$ as strategy for *solo-mining* with $g^{sm}_0 = 1$. The utility corresponding to solo-mining is U_{sm}.
- $\overline{g}^{lm} = (0, 1, 0, 0, \ldots, 0)$ as the strategy where the miner joins the **l**argest **m**ining pool. The corresponding utility is U_{lm}.

Our goal is to show that $U_{lm} > U_{sm}$ for all instances of $\mathcal{G}(\Gamma_{fruitchain})$ with different characterizations of p_1 and p_2. We first make the observation that $D(\overline{g}^{lm}) = D(\overline{g}^{sm})$ because in either case, there is no two pools to switch between. Now, U_{sm} is given by

$$\begin{aligned}U_{sm} = &\quad a \cdot \mathbb{E}[R_k] - b \cdot (\mathbb{E}[R^{\rho}_k])^{1/\rho} - c \cdot D(\overline{g}^{sm}) \\ = &\quad \frac{a \cdot \Gamma_{fruitchain,k} M_1}{M_2} - b \cdot \Gamma_{fruitchain,k} \cdot \left(\frac{M_1}{M_2}\right)^{1/\rho} - c \cdot D(\overline{g}^{sm})\end{aligned}$$

Similarly, we get U_{lm} as

$$\begin{aligned}U_{lm} = &\quad a \cdot \mathbb{E}[R_k] - b \cdot (\mathbb{E}[R^{\rho}_k])^{1/\rho} - c \cdot D(\overline{g}^{lm}) \\ = &\quad \frac{a \cdot \Gamma_{fruitchain,k} M_1}{M_2} - b \cdot \Gamma_{fruitchain,k} \cdot \frac{M_1}{M_2} \frac{1}{f_1^{(\rho-1)/\rho}} - c \cdot D(\overline{g}^{lm}) \\ \leq &\quad \frac{a \cdot \Gamma_{fruitchain,k} M_1}{M_2} - b \cdot \Gamma_{fruitchain,k} \cdot \frac{M_1}{M_2} - c \cdot D(\overline{g}^{lm})\end{aligned}$$

Therefore, taking $U_{lm} - U_{sm}$ and since $D(\overline{g}^{sm}) = D(\overline{g}^{lm})$, we get

$$U_{lm} - U_{sm} = b\Gamma_{fruitchain,k} \left(\frac{(}{M_1} M_2)^{1/\rho} - \frac{M_1}{M_2}\right) > 0$$

Inequality follows since for $M_1 < M_2$ (from Assumption 1) we have $\frac{M_1}{M_2} < \left(\frac{M_1}{M_2}\right)^{1/\rho}$ for any $\rho > 1$. Thus, joining the largest pool *strictly dominates* solo mining for any instance of $\mathcal{G}(\Gamma_{fruitchains})$. □

G Proof for Lemma 2

Proof. Consider player p_1 joining the protocol in round r_0. After T rounds, consider any round $k > r_0 + T$. The block proposed in this round is B_k and $\mathcal{H}_k$ be the history. We consider two strategies:

- $\overline{g}^{sm}$ – *solo mining* where $g_0^{sm} = 1$. The utility corresponding to this strategy is U_{sm}.
- $\overline{g}^{mp}$ – p_1 invests in *mining pools* according to $g^{mp} \in S_\alpha$. The utility corresponding to this strategy is U_{mp}.

The reward from the block B_k for p_1 playing the solo mining strategy is given by the random variable R_k^{sm}. The probability that a block was mined by player p_1 under Assumption 1 is $\frac{M_1}{M_2}$.

$$\mathbb{E}[R_k^{sm}] = \sum_{i=1}^{k} \frac{M_1}{M_2} \cdot \frac{R_{block}}{k} = \frac{R_{block} \cdot M_1}{M_2}$$

The risk is given as $(\mathbb{E}[(R_k^{sm})^\rho])^{1/\rho}$. We calculate this risk as

$$(\mathbb{E}[(R_k^{sm})^\rho])^{1/\rho} = \frac{R_{block} \cdot M_1}{M_2} \left(\frac{M_1}{M_2}\right)^{1/\rho}$$

Similarly, consider random variable for strategy $\overline{g}^{mp}$ is R_k^{mp}.

$$\mathbb{E}[R_k^{mp}] = \sum_{i=1}^{k} \sum_{j=1}^{p} f_j \frac{R_{block}}{k} \frac{g_j M_1}{f_j M_2} = \sum_{j=1}^{p} \frac{R_{block} g_j M_1}{M_2} = \frac{R_{block} \cdot M_1}{M_2}$$

The risk is given as $(\mathbb{E}[(R_k^{mp})^\rho])^{1/\rho}$. We calculate the risk as

$$\begin{aligned} (\mathbb{E}[(R_k^{mp})^\rho])^{1/\rho} &= \left(\sum_{i=1}^{k} \sum_{j=1}^{p} f_j \left(\frac{R_{block}}{k} \frac{g_j M_1}{f_j M_2} \right)^\rho \right)^{1/\rho} \\ &= \frac{R_{block} M_1}{M_2} \left(\sum_{j=1}^{p} f_j \left(g_j\right)^\rho \right)^{1/\rho} \end{aligned}$$

Difference in utility $U_{sm} - U_{mp}$ is given by

$$\begin{aligned} U_{sm} - U_{mp} = \quad & a(\mathbb{E}[R_k^{sm}] - \mathbb{E}[R_k^{mp}]) \\ & -b((\mathbb{E}[(R_k^{sm})^\rho])^{1/\rho} - (\mathbb{E}[(R_k^{mp})^\rho])^{1/\rho}) \\ & -c \cdot (D(\overline{g}^{sm}) - D(\overline{g}^{mp})) \end{aligned}$$

We know $D(\overline{g}^{sm}) - D(\overline{g}^{mp}) \leq 0$ because solo mining has no switching cost. In addition, the expected payoff is the same in both cases. Therefore,

$$U_{sm} - U_{mp} > \frac{R_{block} \cdot M_1 \cdot b}{M_2} \left(\left(\sum_{j=1}^{p} f_j \left(g_j\right)^\rho \right)^{1/\rho} - \left(\frac{M_1}{M_2}\right)^{1/\rho} \right) \gtrapprox 0$$

The last inequality is obtained because from Assumption 1 $\frac{M_1}{M_2}$ is very small. Therefore, we obtain $U_{sm} \gtrapprox U_{mp}$ which means solo mining is more profitable (or in worse cases, negligibly less profitable) than mining pools when BRM is $\Gamma_{\text{decentBRM}}$. □