Decent-BRM: Decentralization through Block Reward Mechanisms

Extended Abstract

Varul Srivastava
IIIT, Hyderabad
Hyderbad, India
varul.srivastava@research.iiit.ac.in

Sujit Gujar
IIIT, Hyderabad
Hyderbad, India
sujit.gujar@iiit.ac.in

ABSTRACT

Proof-of-Work (PoW) is a consensus algorithm where miners solve cryptographic puzzles to mine blocks and obtain the reward specified through the underlying blockchain's Block Reward Mechanism (BRM). Rewards from mining the block have a high associated risk (variance). Miners form mining pools to reduce this risk. The formation of mining pools leads to centralization in PoW blockchains. We study the role of BRMs in forming mining pools and propose a novel BRM that disincentivizes the formation of mining pools. For our analysis, we model the system as a two-player game between (1) an incoming miner and (2) the existing PoW blockchain system.

We categorize BRMs into (a) Memoryless — history independent and (b) Retentive BRMs. We show the impossibility of designing a Memoryless BRM that disincentivizes mining pool formation. We propose a novel retentive BRM – Decent-BRM, which incentivizes incoming miners to perform solo mining (leading to a decentralized PoW blockchain) over forming mining pools.

KEYWORDS

Mechanism Design, Centralization, Proof-of-Work Blockchains

ACM Reference Format:
Varul Srivastava and Sujit Gujar. 2024. Decent-BRM: Decentralization through Block Reward Mechanisms: Extended Abstract. In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024*, IFAAMAS, 3 pages.

1 INTRODUCTION

Nakamoto [13] introduced blockchain technology through Bitcoin; that employed the use of *Proof-of-Work* (PoW) consensus protocol. It involves maintaining a distributed transaction ledger — a chain of ordered blocks. Each block contains some transactions. The interested miners can join the network and must solve some cryptographic puzzle to *mine* (propose) the next block. In return for spending cost (in the form of energy) to mine the block, *miners* are compensated with newly minted coins according to some Block Reward Mechanism (BRM). The mining of a block is a random event with the probability of mining the next block proportional to the mining power for a miner.

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

Mining Pools. There has been 10x growth in computing power used for mining Bitcoins in the last five years [1]. Due to the increase in the total computing power of the system, the probability of mining a block has decreased for small miners. *Solo miners* with limited computing power face high risk (variance in reward from mining) as they often fail to mine any blocks for a prolonged duration. To minimize the risk, miners come together and form *mining pools* and distribute rewards according to some Reward Sharing Scheme (RSS) [16] 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.

Threat of centralization. Some mining pools have since grown disproportionately large, causing centralization in the system. For example, the top three mining pools in Bitcoin, Foundry USA ($\approx$ 29%), Ant Pool ($\approx$ 16%) and F2 Pool (14%) control a 59% of the total mining power. The security of the PoW-based blockchains relies on the fact that no authority controls $>$ 50% of the computing power. Such unprecedented levels of centralization could pose a severe security threat to the PoW blockchains [2]. The challenge of $>$ 50% majority with a single mining pool is not new. For example, GHash.IO controlled the majority (55%) of the Bitcoin network in June 2014, which eroded the public trust in the currency [12].

Game Theoretic approach to mining pools. Game Theory plays an important role in analyzing blockchains [4, 5, 7, 8, 10, 15, 17] as miners are rational and interested in maximizing rewards and minimizing risks. Hence, studying the event of a new miner joining mining pools as a game is natural. The researchers have examined mining pools focusing on optimal RSS [9, 16], or maximizing miner utility [3, 6]. In this work, we analyze the role of Block Reward Mechanisms (BRM) in the formation of mining pools and centralization of the PoW blockchain. We also propose a novel BRM — *decentBRM* which disincentivizes Mining Pool formation.

2 BLOCK REWARD MECHANISMS & GAME

In Proof-of-Work (PoW) blockchains, each block consists of the block-header and transaction data. Block-header for block B_k at height k on the chain (aka. ledger) contains information about parent block (B_{k-1}) and nonce (a random binary string). The ledger history corresponding to block B_k is $\mathcal{H}_k$. Miners try to propose (aka. mine) the block by choosing a nonce such that the hash of B_k is less than some target difficulty T set by the protocol. A **round** k is the duration after mining B_{k-1} in which block B_k is mined.

Block Reward Mechanism. The miner of block B_k is rewarded according to some *Block Reward Mechanism* (BRM) $\Gamma(B_k, \mathcal{H}_k)$. We categorize the BRMs into:

- **Memoryless-BRM** (Γ_{mls}): Here, block-reward for any block B_k is independent of ledger history $\mathcal{H}_k$. Mathematically, $\Gamma_{mls}(B_k, \mathcal{H}_k) = \Gamma_{mls}(B_k, \mathcal{H}_k^{'})$ for $\mathcal{H}_k \neq \mathcal{H}_k^{'}$. An example of a blockchain using memoryless BRM is Bitcoin [13].
- **Retentive-BRM** (Γ_{fc}): Here, block-reward for any block B_k depends on the history of the ledger. Fruitchains [14] is an example of blockchain implementing Retentive BRMs.

As a miner has very less computing power as compared to the system, the probability of it mining a block is very low. Hence, the associated risk (modelled as variance) is very high. To tackle this risk, miners form mining pools and mine a block together. They share the obtained reward through some reward-sharing scheme (RSS) ψ. The RSS of any mining pool should be **fair**, failing which no miner joins the pool. We call the RSS fair if it is an unbiased estimator of the hash rate distribution [16, Section 2.4].

Game Description. We consider a game between two players[1] $\mathcal{P} = \{p_1, p_2\}$. Solo-miner p_1 is joining the PoW blockchain system as a player and has to decide how to distribute their mining power among mining pools/solo mining. p_1 is characterized by $\theta_1 = (M_1, \rho)$ where M_1 is their mining power and ρ is their risk-tolerance. Player p_2 is an abstraction of the existing PoW blockchain system characterized by $\theta_2 = (M_2, \mathcal{A})$ where M_2 is the mining power and $\mathcal{A}$ is the set of mining pools ($p = |\mathcal{A}|$ pools) with pool i using reward sharing scheme ψ_i. We assume $M_2 >> M_1$. Game progression is as follows: (1) Player p_2 chooses strategy $\overline{f}$ – distribution of mining power among different mining pools f_i for pool i and f_0 for the set of solo miners. (2) p_1 (after observing $\overline{f}$) chooses strategy $\overline{g}$ to split their mining power among existing pools/solo mining. The utility of p_1 is defined as:

$$U_1(\overline{g}, \overline{f}; (\theta_1, \theta_2)) = \sum_{k=r_0}^{\infty} \delta^{r-r_0} \left(a\mathbb{E}[R_k] - b(\mathbb{E}[R_k^{\rho}])^{1/\rho} - cD(\overline{g}) \right)$$

Here, (1) R_k is the random variable associated with block reward from round k, (2) $\mathbb{E}[R_k^{\rho}]$ is ρ^{th} moment of R_k, capturing the risk and (3) $D(\overline{g})$ is the switching cost – incurred in changing between different mining pools in a round. We assume two properties of this switching cost (**P1**) $D(\overline{g})$ decreases monotonically with $|\ \{g_i | g_i \neq 0\}\ |$ and (**P2**) If $g_i^1 + g_j^1 = g_i^2 + g_k^2$ and $g_i^1 \cdot g_j^1 > g_i^2 \cdot g_j^2$ and g_q is same $\forall q \in [0, k]/\{i, j\}$ then $D(g^1) \leq D(g^2)$. Our goal is to obtain decentralization, which is defined as follows

Definition (Informal) (Decentralization) A mechanism (Γ, ψ) is $\rho-$decentralized if equilibrium strategy for p_1 is $\overline{g}$ such that for any strategy $\overline{f}$, the mining power of largest pool does not increase when p_1 joins the system.

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

3 ANALYSIS AND RESULTS

Memoryless BRMs. We perform an analysis of Memoryless BRMs to obtain pessimistic results. We depict our results through Figure 1 and informally state them below. The detailed results (with proofs) can be found in [18].

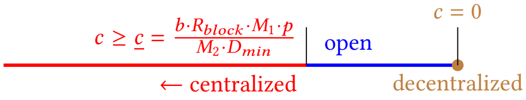
$c \geq \underline{c} = \frac{b \cdot R_{block} \cdot M_1 \cdot p}{M_2 \cdot D_{min}}$
open
$c = 0$
← centralized
decentralized

Figure 1: Bounds on switching cost parameter for Γ_{mls}

1 **Lemma 1**: PoW blockchain with Γ_{mls} is $\rho-$Decentralized for any $\rho > 1$ if there is no switching cost.
2 **Theorem 1**: Equilibrium for p_1 is to join the largest mining pool if switching cost parameter $c \geq \frac{b \cdot R_{block} \cdot M_1 \cdot p}{M_2 \cdot D_{min}}$.
3 **Theorem 2**: It is impossible to construct a memoryless BRM Γ_{mls} such that solo mining is equilibrium strategy.

Retentive BRMs. We analyse Fruitchains [14], one of the most popular retentive BRMs. Towards this, we show that:

1 **Theorem 3**: Retentive BRM Γ_{fc} provides lower risk to ρ risk-averse player than Memoryless BRM Γ_{mls}.
2 **Theorem 4**: Even in Retentive BRM Γ_{fc}, joining mining pools is incentivized over solo mining.

Our conclusion from this analysis is that Retentive BRMs reduce risk in mining. Towards this, we propose Decent-BRM, which achieves decentralization in PoW blockchains.

4 DECENT-BRM: DECENTRALIZED BLOCK REWARD MECHANISM

Decent-BRM In Decent-BRM reward from block B_k is distributed among miners of blocks $B_1, B_2 \ldots, B_k$ equally. Doing so 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 $r_0 + T$.

Implementing Decent-BRM. The implementation of this protocol can be through a special transaction that inputs the hash of two blocks B_x, B_y (for $x < y$) and transfers the share of the reward from B_y to the miner of B_x. Implementing Decent-BRM increases the transaction pool by $O(h^2)$ for chain height h. However, this can be tackled through (1) variable height of transaction (Merkle) tree – the depth of Merkle-tree at block height h should be $log(h)$ or (2) use recursive succinct proofs [11] to represent multiple transactions into small size. We leave formal cryptographic construction of blockchains employing Decent-BRM for future work.

Based on this, we show that the PoW blockchain that implements Decent-BRM achieves Decentralization (disincentivizing pool formation). We state the result informally below, but the details can be found in Lemma 2 and Theorem 5 [18].

Theorem (Informal) (Decent-BRM achieves Decentralization) In a PoW blockchain implementing $\Gamma_{\text{Decent-BRM}}$, the equilibrium strategy for $\rho-$risk averse p_1 joining the system is to perform solo-mining for any $\rho \in \mathbb{N}$. As a result, the PoW blockchain is $\rho-$decentralized, and no mining pools get formed.

ACKNOWLEDGMENTS

This work is partially funded by MeitY and the Ripple-IIITH CoE.

[1] the terms miners and players are used interchangeably

REFERENCES

[1] Andrew Asmakov. 2023. Bitcoin Hash Rate Hits New All-Time High Amid Stagnating Prices.

[2] Christian Badertscher, Yun Lu, and Vassilis Zikas. 2021. A Rational Protocol Treatment of 51% Attacks. In *Advances in Cryptology – CRYPTO 2021*, Tal Malkin and Chris Peikert (Eds.). Springer International Publishing, Cham, 3–32.

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

[4] Lin Chen, Lei Xu, Zhimin Gao, Ahmed Imtiaz Sunny, Keshav Kasichainula, and Weidong Shi. 2021. A Game Theoretical Analysis of Non-Linear Blockchain System. In *Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems* (Virtual Event, United Kingdom) *(AAMAS '21)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 323–331.

[5] Hao Chung and Elaine Shi. 2023. Foundations of Transaction Fee Mechanism Design. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Society for Industrial and Applied Mathematics (ACM SIAM), Philadelphia, United States, 3856–3899.

[6] Axel Cortes-Cubero, Juan Madrigal-Cianci, Kiran Karra, and Zixuan Zhang. 2023. Smoothening block rewards: How much should miners pay for mining pools?

[7] Sankarshan Damle, Varul Srivastava, and Sujit Gujar. 2024. No Transaction Fees? No Problem! Achieving Fairness in Transaction Fee Mechanism Design. arXiv:2402.04634 [cs.GT]

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

[9] Ben Fisch, Rafael Pass, and Abhi Shelat. 2017. Socially Optimal Mining Pools. In *Web and Internet Economics*, Nikhil R. Devanur and Pinyan Lu (Eds.). Springer International Publishing, Cham, 205–218.

[10] Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. 2021. 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* (Virtual Event, United Kingdom) *(AAMAS '21)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 1539–1541.

[11] Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla. 2022. Nova: Recursive Zero-Knowledge Arguments from Folding Schemes. In *Advances in Cryptology – CRYPTO 2022*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer Nature Switzerland, Cham, 359–388.

[12] Jon Matonis. 2014. The bitcoin mining arms race: Ghash. io and the 51% issue.

[13] Satoshi Nakamoto. 2009. Bitcoin : A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[14] Rafael Pass and Elaine Shi. 2017. FruitChains: A Fair Blockchain. In *Proceedings of the ACM Symposium on Principles of Distributed Computing* (Washington, DC, USA) *(PODC '17)*. Association for Computing Machinery, New York, NY, USA, 315–324.

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

[16] Tim Roughgarden and Clara Shikhelman. 2021. Ignore the Extra Zeroes: Variance-Optimal Mining Pools. In *Financial Cryptography and Data Security*, Nikita Borisov and Claudia Diaz (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 233–249.

[17] Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. 2020. BitcoinF: Achieving Fairness For Bitcoin In Transaction Fee Only Model. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems* (Auckland, New Zealand) *(AAMAS '20)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2008–2010.

[18] Varul Srivastava and Sujit Gujar. 2024. DECENT-BRM: Decentralization through Block Reward Mechanisms. arXiv:2401.08988 [cs.GT]