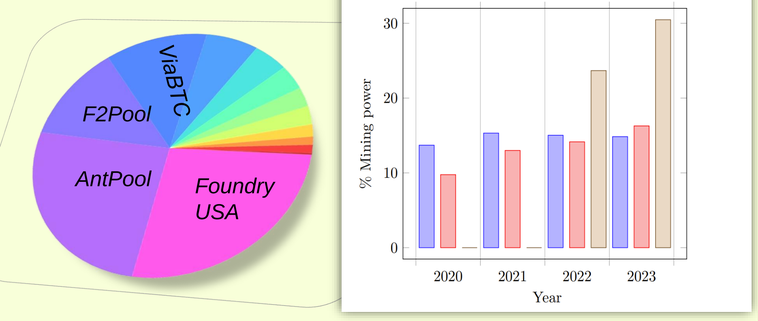
DecentBRM: Decentralization through Block Reward Mechanisms

Varul Srivastava and Sujit Gujar
Machine Learning Lab, IIIT, Hyderabad
varul.srivastava@research.iiit.ac.in sujit.gujar@iiit.ac.in

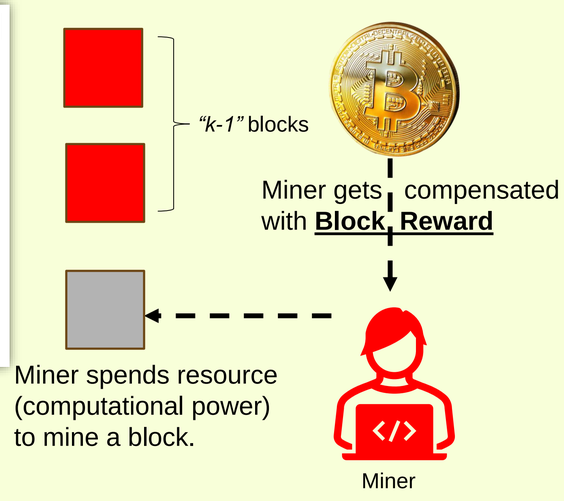
Question: Are Proof-of-Work (PoW) Blockchains truly decentralized?

WHAT is Centralization?



Solo Mining: Get 1 Bitcoin 1/100 times.
Join Mining Pool: Get 0.1 Bitcoin 1/10 times.

WHY does it happen?



PoW mining

What would you rather pick $100 bill or a lottery ticket?

Choice 1: Get $1 million with a probability of 1/10,000
Choice 2: Get $100 with certainty.

*Both choices have same expected reward, but **Choice 2** is preferred by many as has lesser variance.*

Takeaway: Out of different strategies with same expected payoff, **risk-averse** players opt for a lower variance strategy.

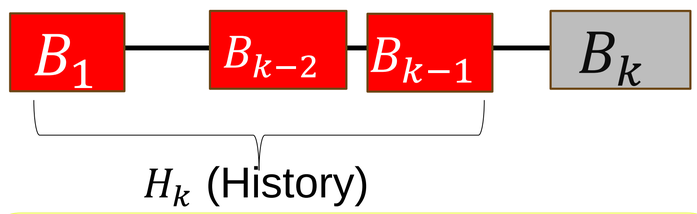
HOW does it impact blockchain?

Centralized Bitcoin — Insecure Bitcoin

PoW blockchain security relies on honest majority. Mining pools pose a threat to this through "centralization of power"

Block Reward Mechanisms (BRM)

Definition: BRMs are mechanisms to distribute cryptocurrency (payment) among miners for participating in the (cost consuming) mining process.

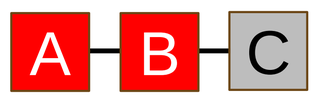


BRM = $\Gamma(H_k, B_k)$

- Memoryless BRM $\Gamma(H^1{}_k, B_k) = \Gamma(H^2{}_k, B_k)$
- Retentive BRM $\Gamma(H^1{}_k, B_k) \neq \Gamma(H^2{}_k, B_k)$

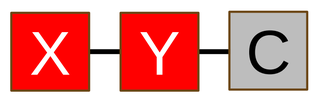
Rewards for a block are *independent of history* of the blockchain ledger.

Memoryless BRMs



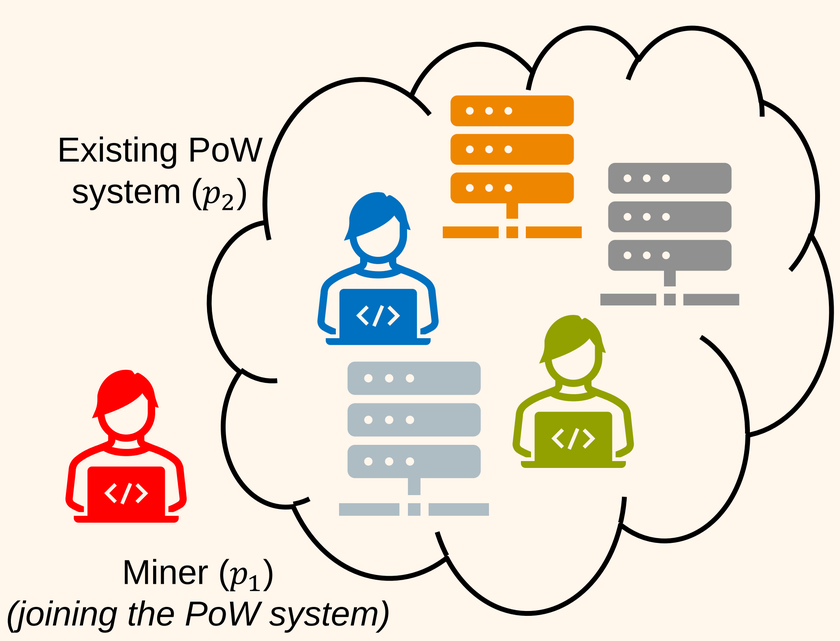
Rewards for a block is *dependent of history* of the blockchain ledger.

Retentive BRMs



Reward for block C in both chains is same in Memoryless BRMs and (can be) different for Retentive BRMs.

Modelling as a Game/Optimization Problem



Players:
p_1 is the *miner joining the system*.
p_1 has mining power $\boldsymbol{M_1}$ and risk averseness $\boldsymbol{\rho}$

p_2 is the *current PoW system*.
p_2 has mining power $\boldsymbol{M_2}$ $(M_2 \gg M_1)$

There are $\boldsymbol{n}$ mining pools, each controlling $\boldsymbol{f_i}$ fraction of M_2

Strategy Space:
Strategy for p_1 is choosing
$$\boldsymbol{g} := \{g_0, g_1, g_2, \dots, g_n\}$$
g_i is fraction of M_1 given to pool i

Strategy for p_2 is choosing
$$\boldsymbol{f} := \{f_1, f_2, \dots, f_n\}$$

Game Progression: (Stackelberg type game)
1. $\boldsymbol{p_2}$ chooses $\boldsymbol{f}$
2. $\boldsymbol{p_1}$ chooses $\boldsymbol{g}$ with the knowledge of $\boldsymbol{f}$

Reward: Each block is mined by pool i with probability $z_i := \frac{f_i M_2 + g_i M_1}{M_1 + M_2}$. Reward for round k:
$$R_k = \Gamma(H_k, B_k)\psi_i \qquad w.p.\ z_i$$

Utility: Utility is given for p_1 with (M_1, ρ) is:
$$U = \underbrace{a\boldsymbol{E}[\boldsymbol{R_k}]}_{\text{Expected Reward}} + \underbrace{b\left(\boldsymbol{E}\left[\boldsymbol{R_k^{\rho}}\right]\right)^{\boldsymbol{1/\rho}}}_{\text{RISK}} - \underbrace{c\ D(\boldsymbol{g})}_{\text{Switching Cost (Penalty)}}$$

Decentralization: A PoW blockchain is decentralized if the following holds:
$$\arg\max_i f_i \geq \arg\max_i \frac{f_i M_1 + g_i M_2}{M_1 + M_2}$$

Theoretical Results

For *Memoryless BRMs*

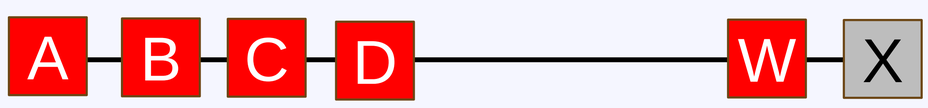
Theorem (Informal). It is impossible to have a decentralized PoW system using a *Memoryless Reward Mechanism* when $c \geq \underline{c}$.

For *Retentive BRMs*

For Retentive BRMs:
- Risk is reduced (still non-zero).
- Fruitchain[1] is still centralized (pool formation incentivized)

DecentBRM[2]

DecentBRM *A Retentive BRM* which has higher utility for solo mining than pool formation.



Block Reward Rule: For any new block X, total reward R_{block} for block X is distributed equally among all miners till block X equally.

Theorem (Informal). Following solo-mining in DecentBRM is (weakly dominant) equilibrium strategy for p_1 after T rounds of the protocol.

DecentBRM serves as existence proof for decentralized Retentive BRMs.

[1]Rafael Pass and Elaine Shi. 2017. FruitChains: A Fair Blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC '17).

[2]Srivastava, Varul, and Sujit Gujar. "DECENT-BRM: Decentralization through Block Reward Mechanisms." *arXiv preprint arXiv:2401.08988* (2024).