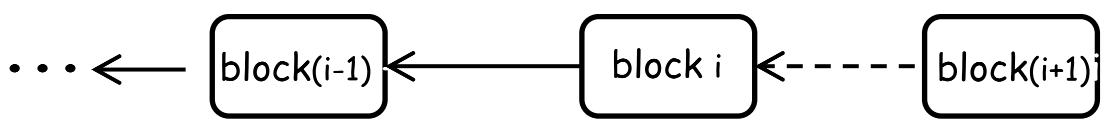
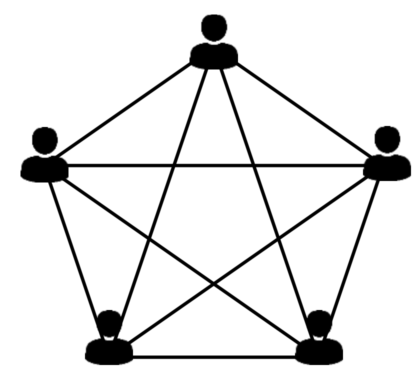
On Game-theoretic Computation Power Diversification in the Bitcoin Mining Network

Suhan Jiang and Jie Wu
Dept. of Computer and Information Sciences
Temple University, USA

Bitcoin Mining

- Proof-of-Work (PoW) based blockchain mining
  - Blockchain is a digital ledger maintained by a P2P network
  - Mining is a process of adding new blocks
  - Adding a block is a puzzle solving race on miners' computing power
- Mining incentive
  - Each block will be rewarded with R
  - Network difficulty D
  - Prob. of adding a block: W_i = computing rate





Solo Mining Vs Pooled Mining

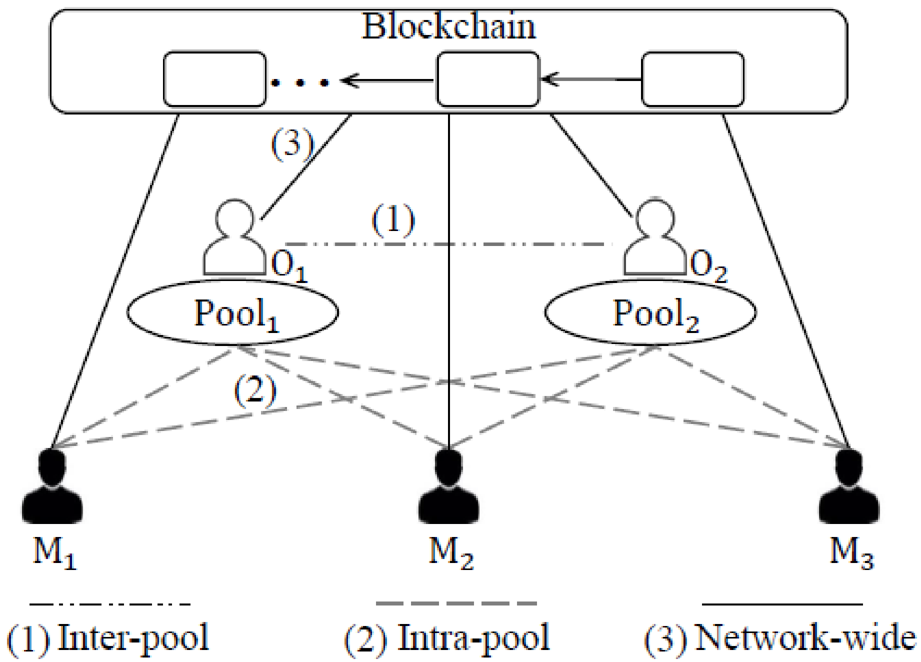
- Solo mining
  - A miner performs the mining operations alone
  - Pros: incur no extra fee
  - Cons: generate more erratic income
- Pooled mining
  - A group of miners cooperate on mining and share rewards
    - a trusted operator is responsible for identifying members' contributions and distributing rewards accordingly.
  - Pros: generate steadier income
  - Cons: pay service fee to the pool operator
- Current situation
  - miners tend to join mining pools for low risks and steady incomes.

Classic Policies in Mining Pools

- Member contribution identification
  - Share-based proofness
    - Share is a potential block solution
    - Contribution is measured based on the number of submitted shares
  - Share difficulty
    - Longer solving time under a higher share difficulty
    - Determined by the pool operator
    - Affect the operator's service cost as well as its member's benefits.
- Member service fee
  - In the form of a reward cutting rate
    - High cutting rate discourages miners' participation
    - Low cutting rate cannot cover the operator's service cost

Three competitions in the Bitcoin mining network

- Inter-pool game
  - Pool operators compete to attract miners
- Intra-pool game
  - All pool members compete for pool rewards
- Network-wide game
  - Among all solo power and pooled power

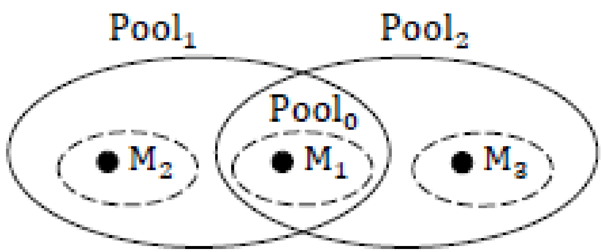


A Hierarchical Bitcoin Mining Network

- Operator-side Problem
  - How to determine its fee rate and difficulty level in order to attract more mining power?
- Miner-side Problem
  - When facing multiple pools, each risk-averse and profit-driven miner considers how to allocate his power to different pools and solo mining?
- Operator-Miner Interaction: A Stackelberg Game
  - M operators are leaders
  - N miners are followers

Virtual Pools

- Assuming M = 2 and N = 3
  - M_1's local view: three pools in total
    - Solo mining, treated as a virtual pool $Pool_0$
    - $Pool_1$ and $Pool_2$
  - Global view: five pools in total
    - Two are real pools (solid eclipses)
    - Three (dashed eclipses) are virtual pools



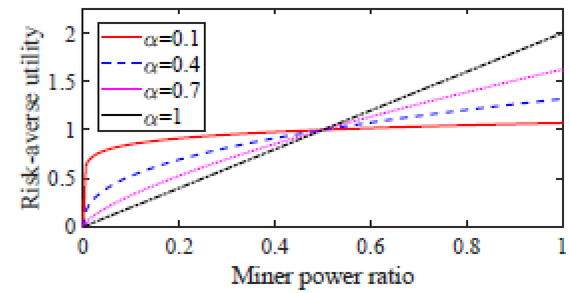
- Adding virtual pools
  - Separate a miner's dual roles of
    - Being an operator as well as
    - being a member when he mines solo
  - Each virtual pool is exclusive to a miner, which charges no service fee and sets share difficulty as network difficulty

Problem Formulation

- Miner objective
  - Determine power allocation vector $\boldsymbol{m}_j = (\beta_j^i)$ to

Problem 1 ($\mathrm{OP}_{\mathrm{MINER}}$).

$$\begin{aligned} &\textit{maximize} && U_j = \sum_{i=0}^{N} u_j^i, \\ &\textit{subject to} && 0 \le \beta_j^i < 1, \quad \sum_{i=0}^{N} \beta_j^i = 1 \end{aligned}$$



  - Single pool utility: $u_j^i = Pr_i \cdot (p_j^i)^{\alpha_j}$

risk tolerance level of M_j

the probability of Pool$_i$ finding a block

the payoff M_j can obtain when Pool$_i$ successfully finds a block

  - Single pool payoff: $p_j^i = r_j^i - c_j^i - v_j^i$

reward, cost, variance obtained in Pool$_i$

Problem Formulation

- Operator objective
  - Determine share difficulty d_i and cutting rate f_i to

Problem 2 ($\mathrm{OP}_{\mathrm{OPERATOR}}$).

$$\begin{aligned} &\textit{maximize} && V_i = \bar{r}_i - \bar{c}_i, \\ &\textit{where} && \bar{c}_i \leq b_i, \end{aligned}$$

where b_i represents O_i's budget constraint.

  - Expected reward: $\overline{r_i} = Pr_i \times R \times f_i$
  - Communication cost: $\overline{c_i}$

Equilibrium in Stackelberg Game

- Analysis method: backward induction
- Theorem 1. A Nash equilibrium exists among all miners if all operators' strategies are fixed.
- Theorem 2. A Nash equilibrium exists among all operators.
- Theorem 3. A Stackelberg equilibrium exists among all operators and all miners.

Experiment

- Part 1
  - Miner-side Equilibrium Analysis
  - Operator-side Equilibrium Analysis

- Part 2
  - Time-varying Bitcoin Market Price

Comparison of Different Investment Methods

- Compare our method with some existing works
  - SN, SA, MR, MNO, MAO
  - Setting: 3 pool operators and 20 miners

Power ratio	SN	SA	MR	MNO	MAO
0.05	0.5482	0.5477	0.5578	0.5890	*0.5719*
0.10	1.0982	1.0964	1.1773	1.1780	*1.1757*
0.15	1.6446	1.6446	1.7334	1.7670	*1.8007*
0.20	2.1954	2.1929	2.3451	2.3560	*2.4257*
0.25	2.7411	2.7501	2.8068	2.9449	*3.0507*

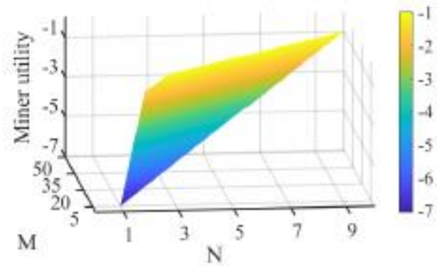
TABLE III: Miner's average income under different investment methods.

Power ratio	SN	SA	MR	MNO	MAO
0.05	560	562	147	123	*99*
0.10	378	391	108	115	*97*
0.15	282	282	110	107	*94*
0.20	180	185	111	105	*92*
0.25	128	123	102	101	*90*

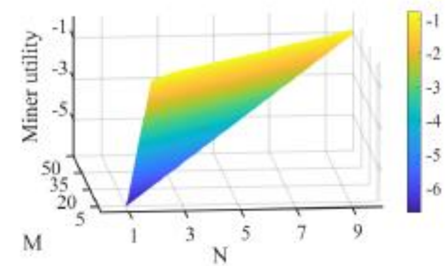
TABLE IV: Miner's variance under different investment methods.

Factors Affects Miner's Utilities

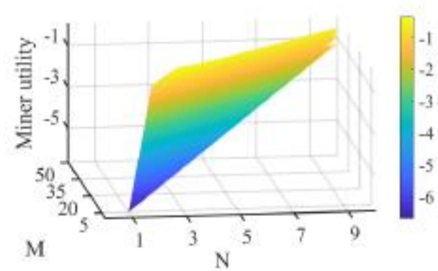
- Individual reasons
  - Computation power
  - Risk tolerance level
- External reason
  - the number of pools for miners to join in



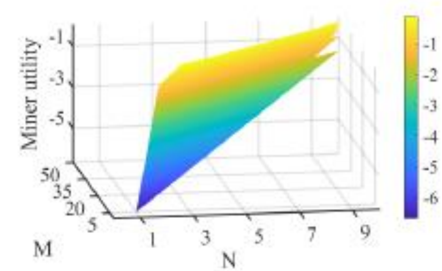
(a) $\alpha = 0.01$.



(b) $\alpha = 0.1$.



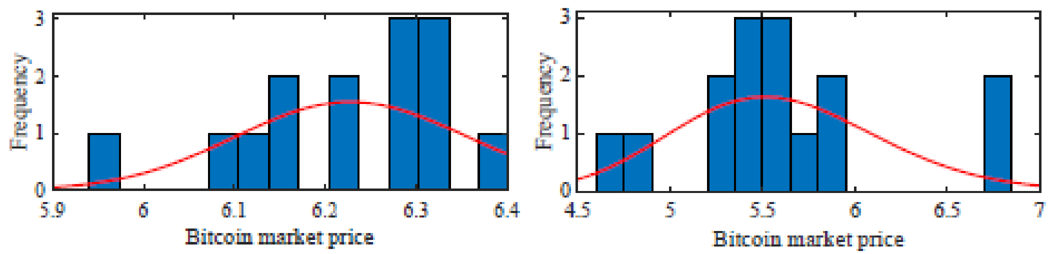
(c) $\alpha = 0.4$.



(d) $\alpha = 0.8$.

Bitcoin Market Price and Equilibrium

- Bitcoin Market Price
  - Time-varying and follows a log-normal distribution



(a) $\mu = 6.25$ and $\sigma^2 = 0.01$. (b) $\mu = 6.25$ and $\sigma^2 = 1$.

  - Setting: 3 pools in total and 100 homogeneous miners.

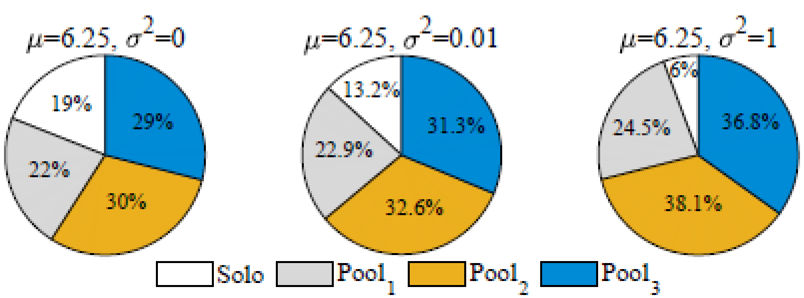


Fig. 6: Homogeneous miners' power allocation evolution.

5. Conclusion

- A Stackelberg game with two subgames
- A variance-involved power function to characterize risk-averse miners' utilities.
- Virtual pools are added to separate miners' dual role
- Impacts of time-varying Bitcoin Market Price
- Experiments to confirm theoretical analysis

Thank you

Q & A