Blockchain Mining Game in Hierarchical Blockchain Mining Offloading

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

(Collaborator: Suhan Jiang)

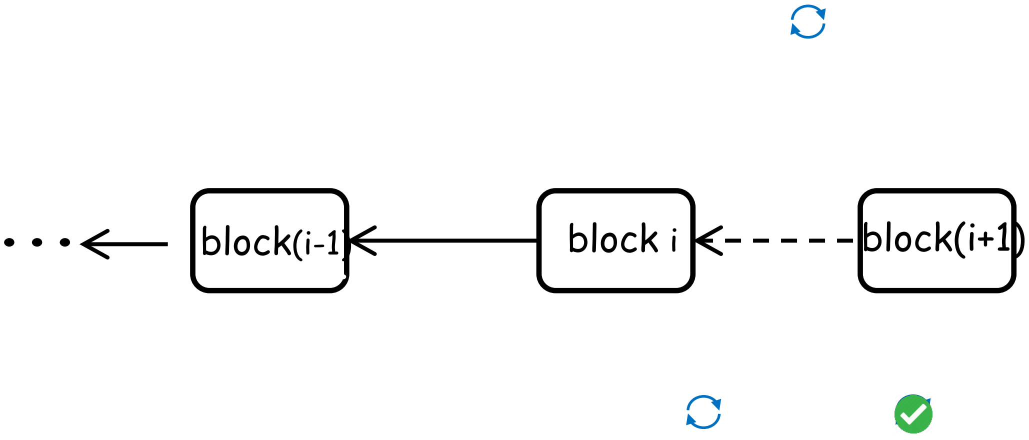
Outline

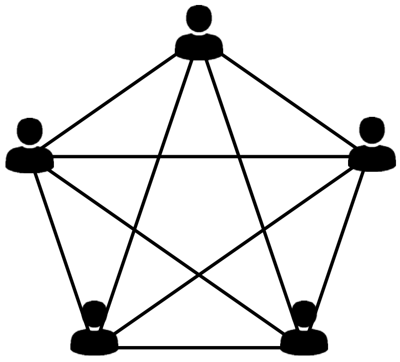
1. Mobile Blockchain Mining
2. Offloading Mining Game
3. Theoretical Analysis
4. Extensions
5. Performance
6. Other Game Applications
7. Conclusions

1. Mobile Blockchain Mining

- PoW-based blockchain mining
  - Mining a block requires puzzle solving (Nakamoto protocol)
- Mining incentive
  - Each block will be rewarded
  - Prob . of winning a puzzle solving race

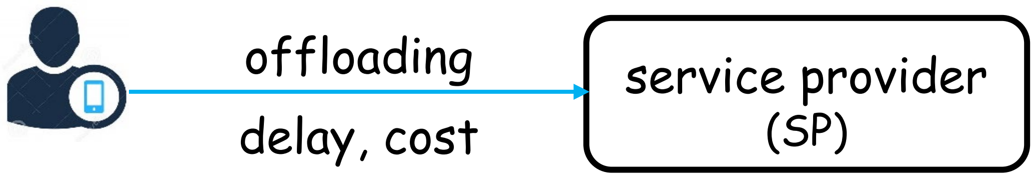
$$\text{computing rate} = \frac{\text{individual computing power}}{\text{total computing power}}$$





Mobile Devices Offloading

- Mobile devices
  - Blockchain smartphone: HTC, Samsung
  - Mobile blockchain (with edge): limited computing power & energy
- Solution: offloading



offloading

delay, cost

service provider (SP)

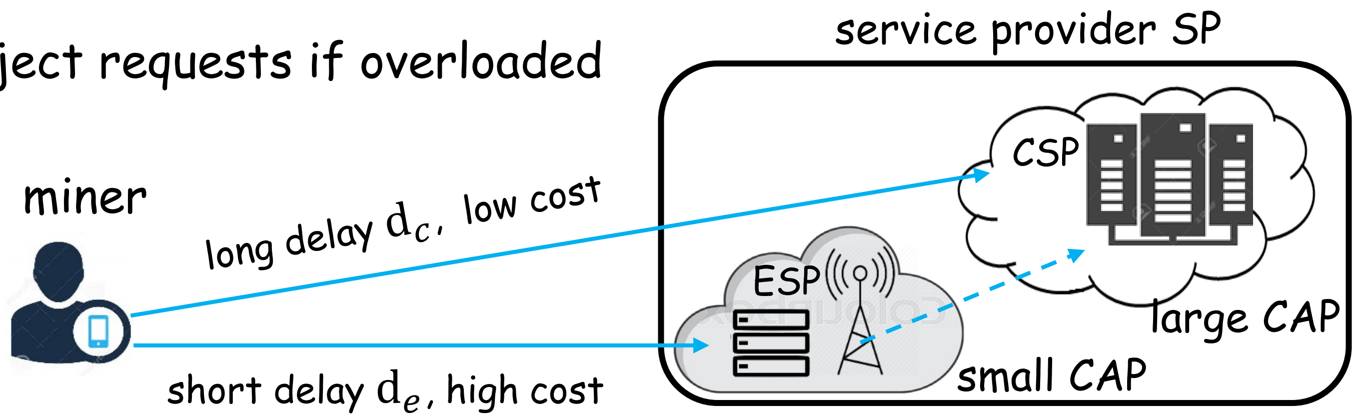
  - Offloading incurs delay (d) and cost (C) from SP
  - A miner's utility $\boxed{U_i = RW_i - C_i}$
  - $W_i = \left(1 - \beta(d)\right) \times$ computing rate

specific function of delay

proportional to computing power

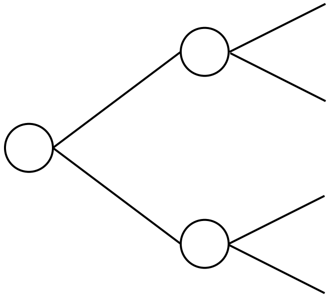
2. Offloading Mining Game

- Two SPs
  - A remote cloud computing service provider (CSP)
    - Large resource capacity, low price, long delay
  - A nearby edge computing service provider (ESP)
    - Limited resource capacity, high price, short delay
- Two operation modes
  - ESP is connected to CSP
    - Auto-transfer requests to CSP if overloaded (h: hit ratio)
  - ESP is standalone from CSP
    - Reject requests if overloaded



Game Theory: Basic

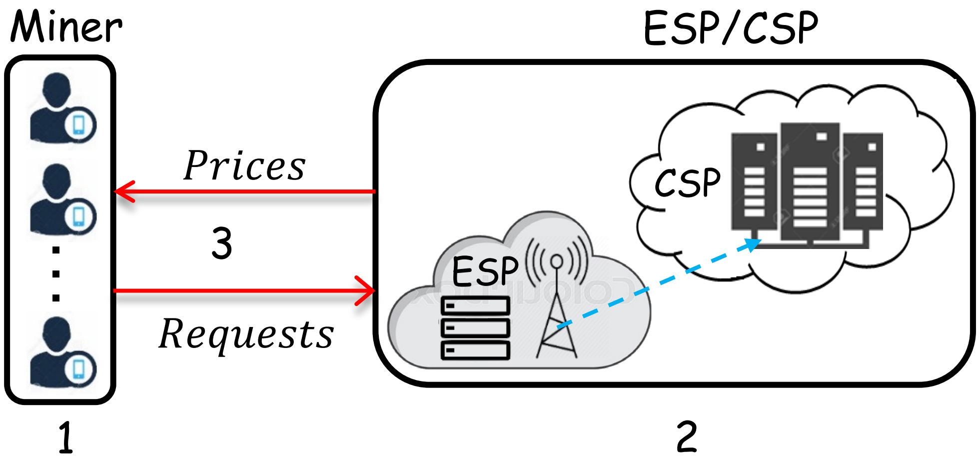
- Basic Elements
  - Player, utility, strategy, and rationality (self-interested)
- Types of Games
  - Cooperative vs. non-cooperative games
  - Static vs. dynamic (sequential) games
  - Stackelberg game: leaders and followers
  - Stochastic game: stochastic transitions among states



- Types of Equilibrium
  - Nash equilibrium
  - Stackelberg equilibrium: backward induction
  - Markov equilibrium

Hierarchical Games

1. Nash subgame of N miners that maximizes utility U_i
   - Decide on shared resource from ESP (e_i) and CSP (c_i)
2. Nash subgame of ESP/CSP that maximizes revenue $V_e(V_c)$
   - Decide on the resource unit price $P_e(P_c)$
3. Stackelberg game between miners and ESP/CSP
   - Interplay between leaders (ESP/CSP) and followers (miners).



Miners' Subgame

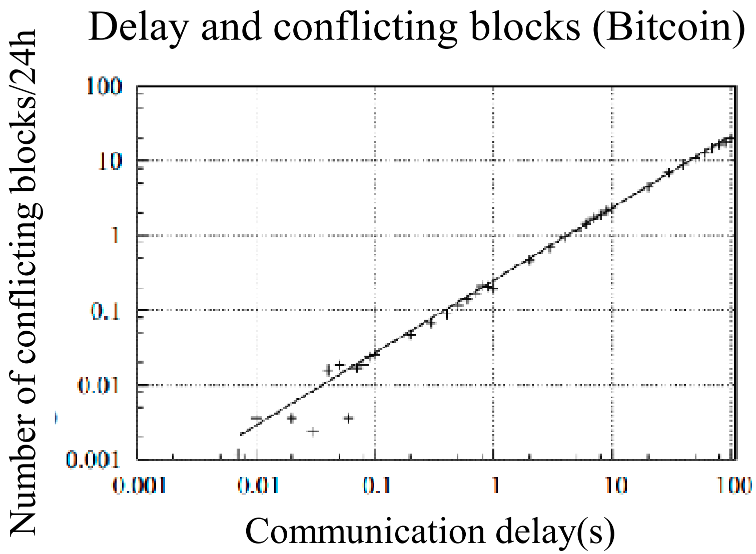
- Formulation of strategy and objective
  - Miner i determines e_i and c_i under budget limitation B_i to

$$\boxed{maximize \quad U_i = RW_i - (P_e e_i + P_c c_i)}$$

  - ESP, charged at ESP price, that is
    - connected: if overflow, forwarded to CSP
    - standalone: if overflow, ESP rejected
- Winning probability W_i
  - d discounts W_i by $\beta(d)$

$$\boxed{\beta(d) = 1 - e^{-\frac{d}{D}} \approx \frac{d}{D}}$$

D: a system-defined parameter



Delay and conflicting blocks (Bitcoin)

Winning Probability

- If miner i's edge request is satisfied by ESP

$\beta = \beta(\mathrm{d}_c - \mathrm{d}_e)$

$$W_i^h = \frac{e_i}{E+C}\left(1+\frac{\beta C}{E}\right) + \frac{c_i}{E+C}(1-\beta)$$

- If miner i's edge request cannot be satisfied by ESP
  - Connected: Miner i's edge request is redirected to CSP

$$W_i^{1-h} = \frac{e_i + c_i}{E+C}(1-\beta)$$

  - Standalone: Miner i's edge request is completely rejected

$$W_i^{1-h} = \frac{c_i}{E+C-e_i}(1-\beta)$$

- Expected winning probability

$$W_i = hW_i^h + (1-h)W_i^{1-h}$$

SPs' Subgame

- Formulation of strategy and objective
  - ESF $maximize \quad V_e = (P_e - C_e) \cdot E \quad where\ E = \sum_{i=1}^{N} e_i$

    ESP unit cost ESP sold-out units

  - CS $maximize \quad V_c = (P_c - C_c) \cdot C \quad where\ C = \sum_{i=1}^{N} c_i$

    CSP unit cost CSP sold-out units

Stackelberg Game

- A two-stage game
  - Stage 1 (leader): ESP/CSP subgame
    - ESP(CSP) optimizes its unit price $P_e(P_c)$ by predicting the miners' reactions, considering the rival's price strategy.
  - Stage 2 (follower): miner subgame
    - Each miner responds to the current prices, by sending requests to ESP/CSP, considering its budget and other miners' requests.
- Stackelberg equilibrium (SE)
  - Formed by the subgame perfect Nash equilibria (NE) in both the leader stage and the follower stage

3. Theoretical Analysis

- Heterogenous: miners with different budgets

Theorem 1. A unique NE exists in the miner subgame.

Theorem 2. Stackelberg game has a unique SE.

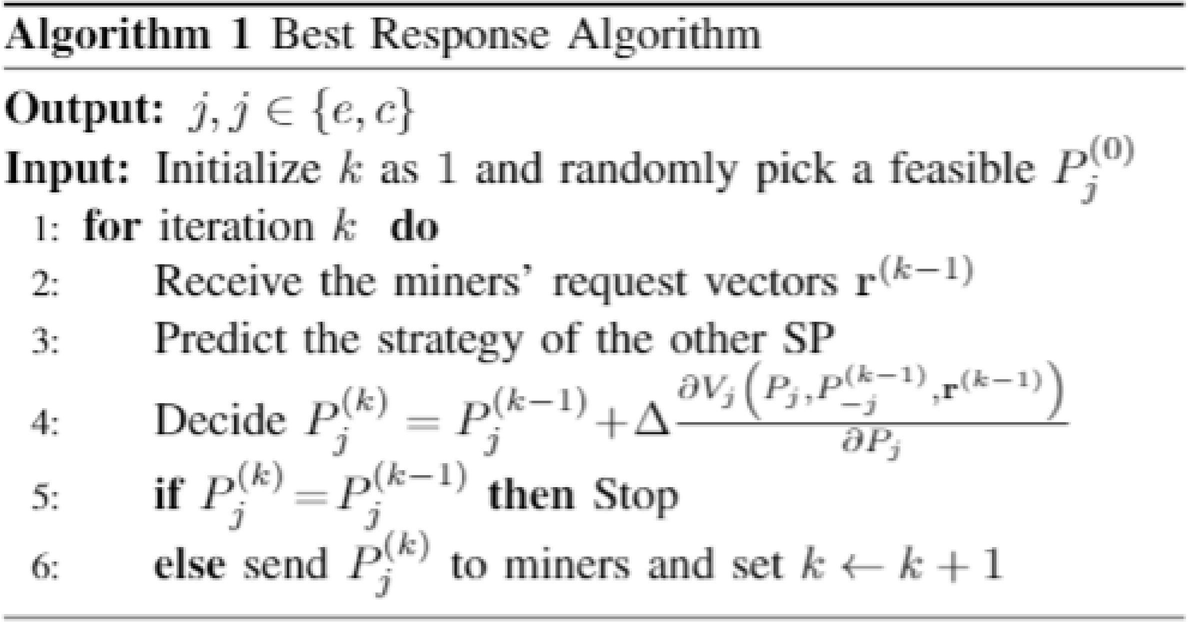
A *best response algorithm* to find the unique SE point in the Stackelberg game.

- Homogenous: miners with identical budgets (connected mode)

Theorem 3. If all miners have identical budgets B, each miner's request in NE can be expressed as

$$\begin{cases} e_i^* = \dfrac{B\beta h}{(1-\beta+h\beta)(P_e-P_c)}, \\ c_i^* = \dfrac{B\left[(1-\beta)(P_e-P_c)-P_c\beta h\right]}{P_c(1-\beta+h\beta)(P_e-P_c)} \end{cases}$$

Best Response Algorithm



Algorithm 1 Best Response Algorithm

```
Output: $j, j \in \{e, c\}$
Input: Initialize $k$ as 1 and randomly pick a feasible $P_j^{(0)}$
for iteration $k$ do
    Receive the miners' request vectors $\mathbf{r}^{(k-1)}$
    Predict the strategy of the other SP
    Decide $P_j^{(k)} = P_j^{(k-1)} + \Delta \frac{\partial V_j\left(P_j, P_{-j}^{(k-1)}, \mathbf{r}^{(k-1)}\right)}{\partial P_j}$
    if $P_j^{(k)} = P_j^{(k-1)}$ then Stop
    else send $P_j^{(k)}$ to miners and set $k \leftarrow k + 1$
```

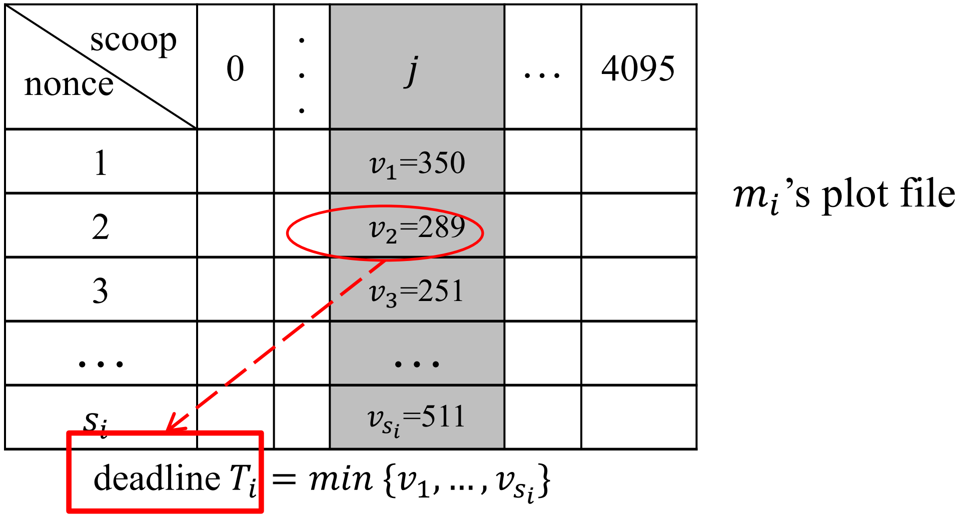
SPs use a *gradient ascent process* to maximize their utilities.

4. Extensions: Proof of Capacity (PoC)

PoC-based blockchain mining

- Mining is a deadline-finding race on miners' storage
- Sysems: Burst, Storj, Chia, SpaceMint, Steps: plotting and mining
- Probability of finding the smallest deadline

$$\text{storage fraction} = \frac{\text{individual storage space}}{\text{network-wide storage space}}$$



scoop nonce	0	⋮	j	…	4095
1			v_1=350		
2			v_2=289		
3			v_3=251		
…			…		
s_i			v_{s_i}=511		

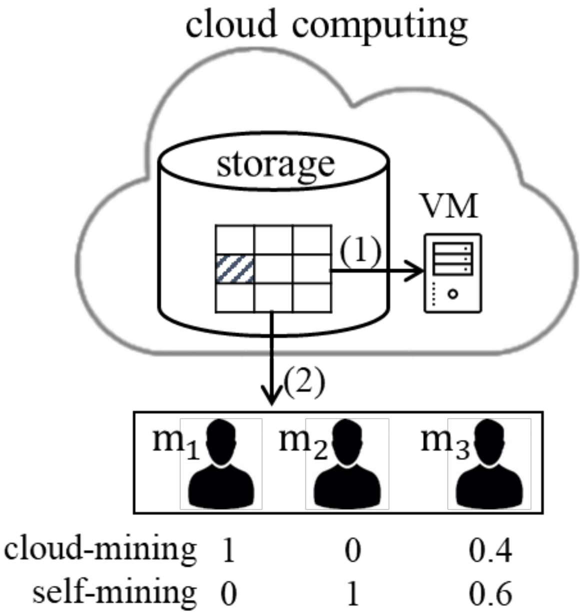
m_i's plot file

deadline $T_i = min\{v_1, \dots, v_{s_i}\}$

Self-Mining vs. Cloud-Mining

Tradeoff between delay and cost

- Cloud-mining (1)
  - Employ VMs provided by CSP
  - Eliminate download delay
  - Increase cost on VM employment
- Self-mining (2)
  - Download scoops and compute locally
  - Avoid extra cost
  - Incur download delay (d)
- Mixed strategy



Problem Formulation

- Nash game of n miners that maximizes utility U_i
  - Decide on how many storage units to buy from the CSP
  - Decide on the ratio between cloud-mining (x_i) and self-mining (y_i)

- Miner objective
  - Determine x_i and y_i under budget limitation b_i to

$$maximize\ \boxed{U_i = RP_i - C_i}$$

  - Winning probability: $P_i = \left(1 - \beta(d, Y)\right) \times$ storage fraction
    - $\beta(d, X) = 1 - (1 - \frac{d}{D})^Y$
    - d: uniform distribution of hash on [0, D], D difficulty level, $Y = \sum_{I=1}^{n} y_i$

Winning Probability and Cost

P_i combines winning both in cloud-mining and self-mining

- $P_i = P_i^c + P_i^s$
  - $P_i^c = \frac{x_i}{S} + \frac{x_i}{X}\frac{Y}{S}\beta$, and $P_i^s = \frac{y_i}{S} - \frac{y_i}{Y}\frac{Y}{S}\beta$

    where $X = \sum_{I=1}^{n} x_i$ and $Y = \sum_{I=1}^{n} y_i$

Offloading cost, with price p_s and p_c, for storage and computation

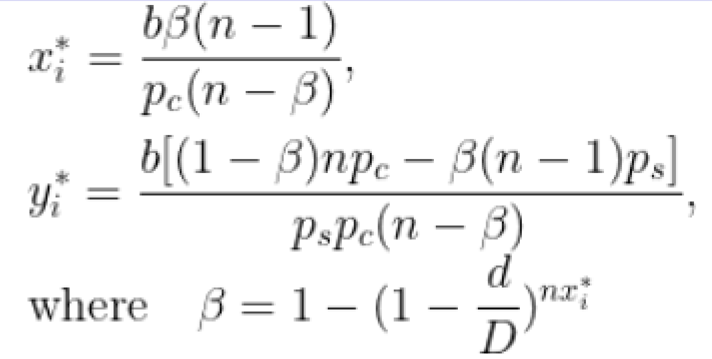
$$C_i = \underbrace{p_s(x_i + y_i)}_{\text{storage}} + \underbrace{p_c\ x_i}_{\text{computation}}$$

Game Analysis

Theorem 1'. A unique NE exists in a miner game.

A *best-response algorithm* to find the unique NE point.

Theorem 3'. If all miners have identical budgets b, each miner's request in NE can be expressed as



$$x_i^* = \frac{b\beta(n-1)}{p_c(n-\beta)},$$

$$y_i^* = \frac{b[(1-\beta)np_c - \beta(n-1)p_s]}{p_s p_c(n-\beta)},$$

$$\text{where} \quad \beta = 1 - (1 - \frac{d}{D})^{nx_i^*}$$

Extensions: Variable Delay

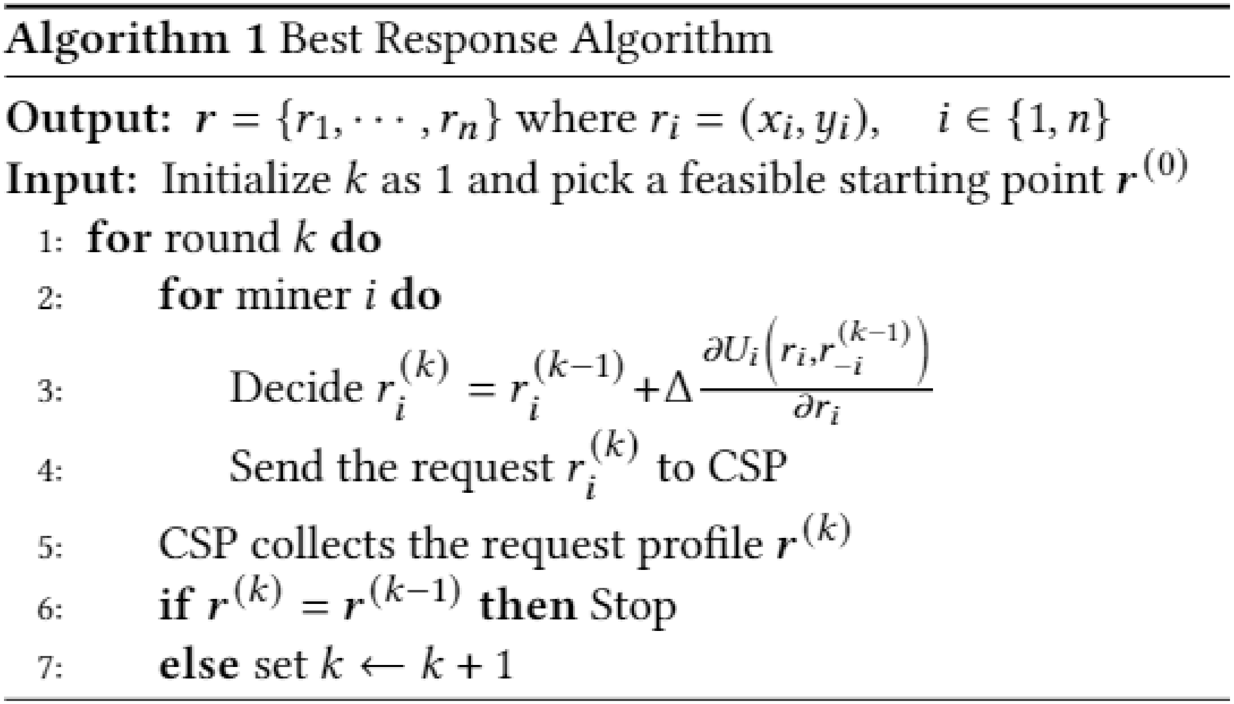
Different network settings

- Uniform delay
  - All miners experience an identical download delay
- Non-uniform delays
  - Miners use different network settings, e.g. 5G, 4G, or 3G

Theorem 4'. Given a price set (p_s, p_c), there exists at least one NE in the miner game.

A *best response* algorithm with guaranteed convergence is used to find one NE point.

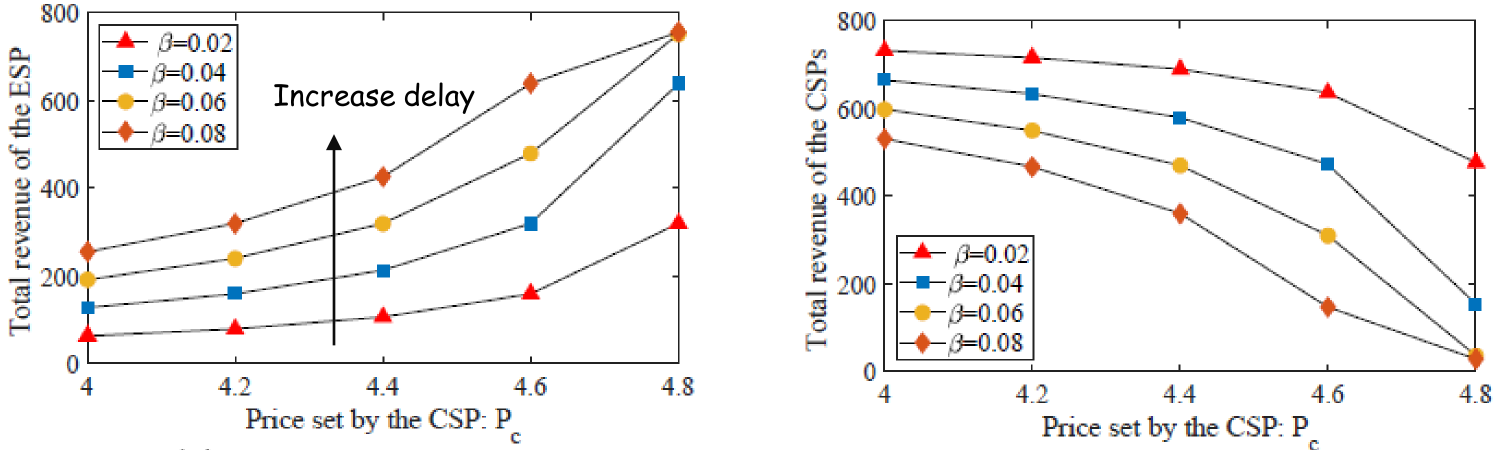
Best Response Algorithm



```
Algorithm 1 Best Response Algorithm
Output: $\boldsymbol{r} = \{r_1, \cdots, r_n\}$ where $r_i = (x_i, y_i)$,   $i \in \{1, n\}$
Input: Initialize $k$ as 1 and pick a feasible starting point $\boldsymbol{r}^{(0)}$
for round $k$ do
    for miner $i$ do
        Decide $r_i^{(k)} = r_i^{(k-1)} + \Delta \frac{\partial U_i\left(r_i, r_{-i}^{(k-1)}\right)}{\partial r_i}$
        Send the request $r_i^{(k)}$ to CSP
    CSP collects the request profile $\boldsymbol{r}^{(k)}$
    if $\boldsymbol{r}^{(k)} = \boldsymbol{r}^{(k-1)}$ then Stop
    else set $k \leftarrow k + 1$
```

5. Simulation

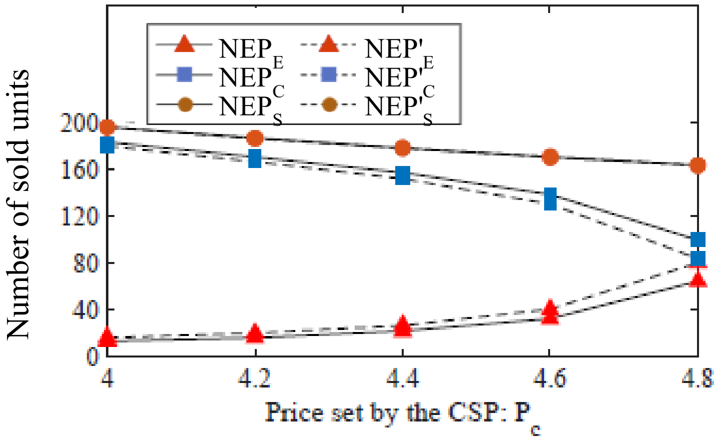
- Simulation setting
  - A small network of 5 miners with identical budgets B = 200
  - Each experiment is averaged over 50 rounds
- Miner subgame equilibrium
  - Influences of communication delay ($P_e = 5$)
    - Longer delay (higher CSP price) promotes ESP's revenue but reduces CSP's



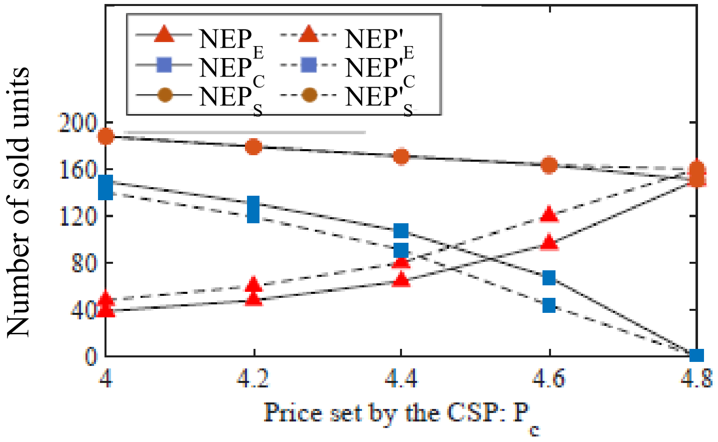
(a) The ESP's revenue. (b) The CSP's revenue.

Miner Subgame Equilibrium

- Influences of operation modes
  - NEP (connected mode) and NEP' (standalone mode)
  - Miners tend to buy more units from ESP in standalone mode as CSP price increases
  - Longer communication delay (higher CSP price) means a lower the number of units sold by ESP and CSP.



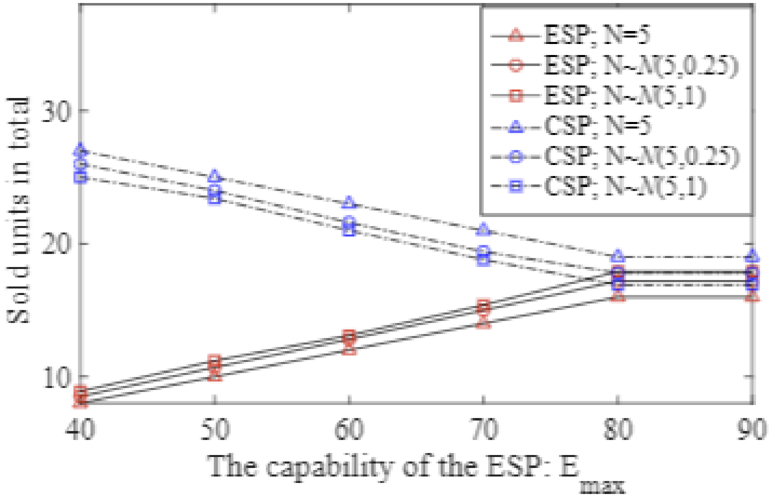
(a) $\beta = 0.02$.



(b) $\beta = 0.06$.

Population Uncertainty

- RL will learn the population uncertainty (Gaussian distribution)
- $P_e = 5, P_c = 4$
- The higher ESP capacity, the more sold units in ESP
- The higher uncertainty, the more units required from ESP



Experiment

- Testbed setting for storage offloading
  - Plotting: Google Cloud
  - Mining: Burstcoin, a PoC-based blockchain application

    Average block generation interval: 4 min

    Mining over a plot file of 18 TB: 30s to 60s

- Miners' optimal strategies
  - Unique equilibrium in uniform delay networks
  - Equilibrium in variable delay networks

Equilibrium in Variable Delay

- Influences of delay ratio
  - Settings:
    - 3 types of networks with a delay of $\theta_i d, i = 1, 2, 3$
    - Each network is used by 20 miners
    - Each miner has an identical budget 200, $(p_s, p_c) = (1, 12)$
  - Units sold (x, y), based on delay ratio, i.e., $\theta_1 : \theta_2 : \theta_3$

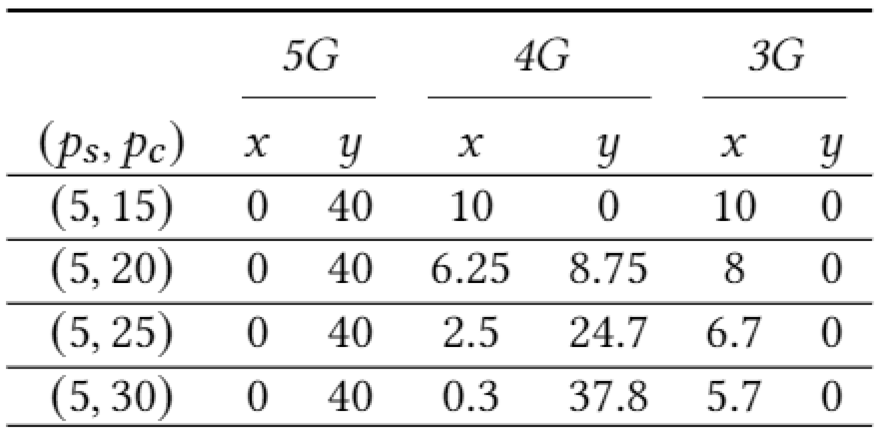
Miners' strategy profiles under different delay ratios.

	Type1		*Type2*		*Type3*	
$\theta_1 : \theta_2 : \theta_3$	x	y	x	y	x	y
3 : 4 : 5	7.3	88.9	11.8	0	16.8	0
4 : 5 : 6	12	31.7	13	0	14.8	0
5 : 6 : 7	12.3	4.4	13.3	0	14.2	0

miners with longer delays invest more on cloud mining

Equilibrium in Variable Delay (cont’d)

- Influences of the CSP prices
  - Settings:
    - 3 types of networks (5G, 4G, and 3G), where $\theta_1 : \theta_2 : \theta_3 = 3 : 20 : 500$
    - Type i network is used by 1 miner
    - Each miner has an identical budget 200
  - Units sold, based on CSP prices (p_s, p_c)



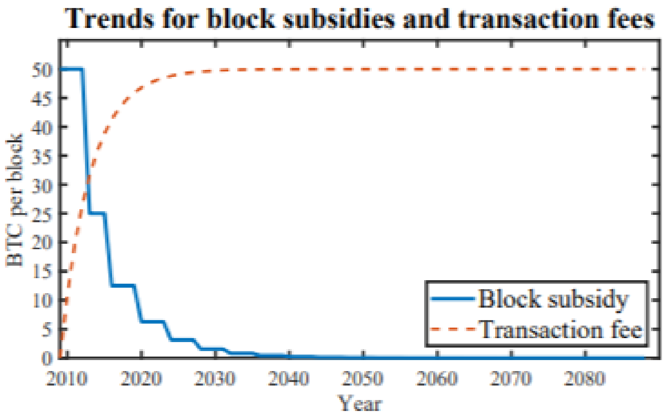
Miners’ strategy profiles under different price sets.

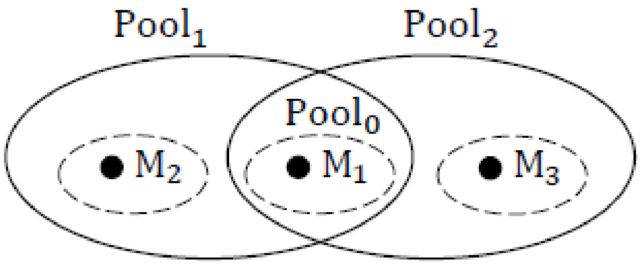
	5G		4G		3G	
(p_s, p_c)	x	y	x	y	x	y
(5, 15)	0	40	10	0	10	0
(5, 20)	0	40	6.25	8.75	8	0
(5, 25)	0	40	2.5	24.7	6.7	0
(5, 30)	0	40	0.3	37.8	5.7	0

miners invest more on self mining as Pc cost increases

6. Other Game Applications

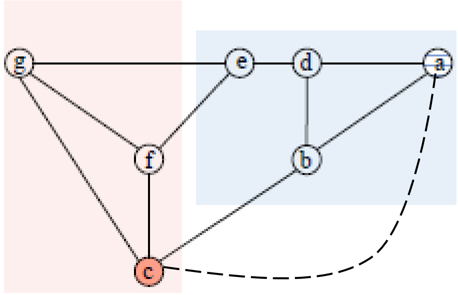
- Different attacks
  - Selfish mining attack: block withholding
  - Denial of Service (DoS) attack
- Mining management
  - Transaction selection
  - Computational power allocation
  - Fork chain selection
  - Transactions fees
  - Pool selection



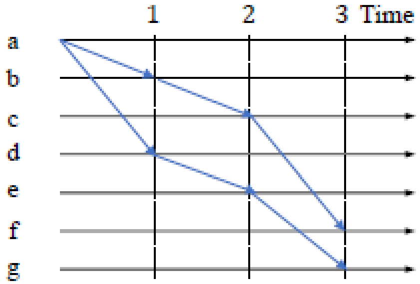


Game in Topology Design

- Topology design in P2P

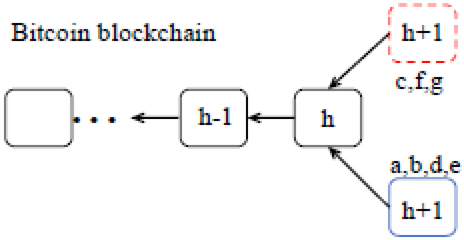


(a) Network topology.

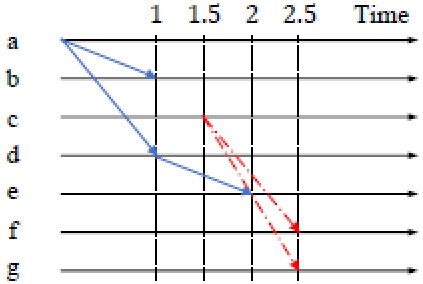


(b) At time 0, miner a finds and broadcasts his block.

- Propagation delay vs. fork rate
  - Will node c benefit from setting a new connection to node a?



(a) Blockchain forks and miners are divided into {a,b,d,e} and {c,f,g}.



(b) At time 1.5, miner b also finds and broadcasts his block.

7. Conclusion

- Blockchain Mining Offloading
  - Miners offloading to service providers (SPs): edge/cloud
- Hierarchical Games
  - Nash games among miners and among SPs
  - Stackelberg game between miners and SPs
- Equilibrium
  - Existence vs. explicit expression
- Challenges
  - Mechanism design and incentive
  - Heterogenous settings: mean field games (aggregate effect)

Questions

S. Jiang and J. Wu, "Bitcoin Mining with Transaction Fees: A Game on the Block Size," *Proc. of IEEE Blockchain*, 2019.

S. Jiang, X. Li, and J. Wu, "Hierarchical Edge-Cloud Computing for Mobile Blockchain Mining Game," *Proc. of IEEE ICDCS*, 2019.

S. Jiang and J. Wu, "A Game-theoretic Approach to Storage Offloading in PoC-based Mobile Blockchain Mining," *Proc. of ACM MobiHoc*, 2020.