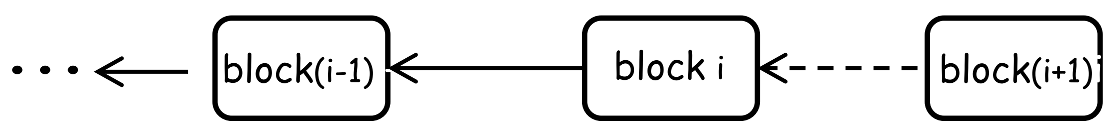
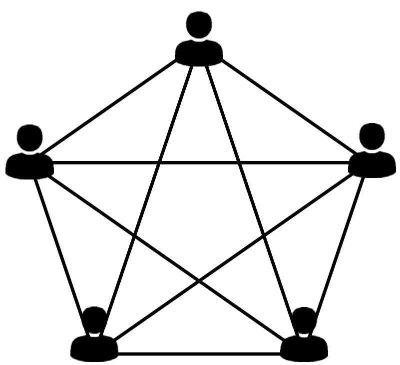
A Game-theoretic Approach to Storage Offloading in PoC-based Mobile Blockchain Mining

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

Blockchain Mining

- Blockchain is a digital ledger maintained by a P2P network
  - It records transactions in the form of chained blocks
  - It is duplicated and distributed across all miners in the network
- Mining is a process of adding new blocks
  - The mining network is decentralized
  - Miners must follow a consensus mechanism to append the blockchain
  - Example: Bitcoin and Proof of Work (PoW) mechanism





Proof-of-Capacity (PoC) Mechanism

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

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

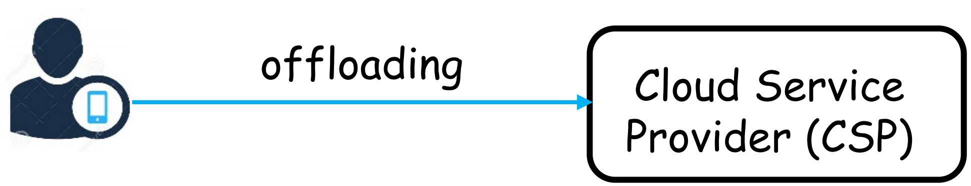
scoop / nonce	0	⋮	j	…	4095
1			v_1=350		
2			v_2=289		
3			v_3=251		
…			…		
s_i			v_{s_i}=511		

m_i's plot file

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

Motivation: Apply in Mobile Devices

- Few blockchain applications in mobile environments
  - Mobile devices cannot satisfy mining requirements
    - Limited storage space
    - PoC mining requires large space on the order of TB
  - Solution: storage offloading

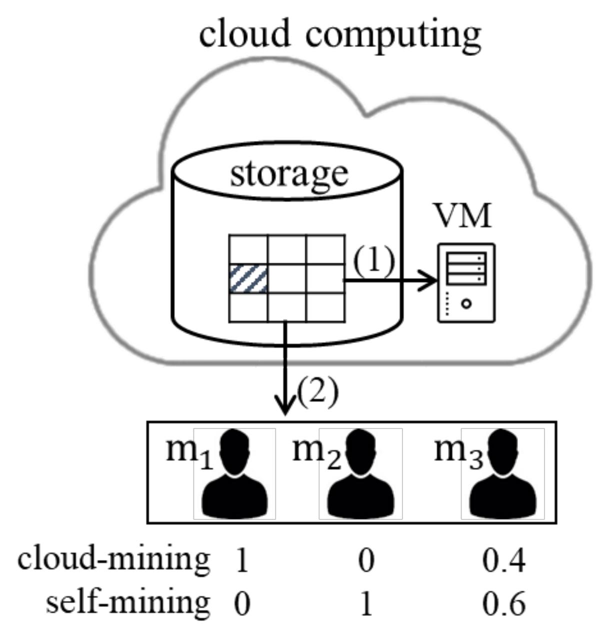


    - Offloading incurs two different mining method
      - self-mining and cloud-mining

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



Mining Reward, Cost, and Utility

- Individual utility (U_i):
  - Difference between expected rewards and costs

    $$U_i = RP_i - C_i$$

    - R: single-round mining reward for the winner
    - P_i: miner i's winning probability in a mining round
    - C_i: miner i's cost in a mining round

      $$C_i = C_i^s + C_i^c$$

      storage (C_i^s) computation (C_i^c)

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

    $maximize \quad U_i = RP_i - C_i$
  - Winning probability: $P_i = P_i^c + P_i^s$
    - effects of delay: $\beta(d, X) = 1 - (1 - \frac{d}{D})^X$, $X = \sum_{I=1}^{n} x_i$
    - *d* is the download delay and
    - D is the mining difficulty (block generation interval)
  - Cost: $C_i = p_s(x_i + y_i) + p_c x_i$

    (p_s: storage; p_c: computation)

Validation of Winning Probability

- 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 $P_i^s = \frac{y_i}{S} - \frac{y_i}{Y}\frac{Y}{S}\beta = y_i\frac{1-\beta}{S}$
    - where $X = \sum_{I=1}^{n} x_i$ and $Y = \sum_{I=1}^{n} y_i$
  - **Theorem 1**. P_i is valid to express winning probability of individual miners in a mobile blockchain mining network
    - Proof: We present the full verification process by checking that $\sum_{i=1}^{N} P_i = 1$ always holds.

Game Analysis

Theorem 2. 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

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

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

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

Best Response Algorithm

Algorithm 1 Best Response Algorithm

Output: $r = \{r_1, \cdots, r_n\}$ where $r_i = (x_i, y_i), \quad i \in \{1, n\}$

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) + Δ ∂U_i(r_i, r_{-i}^(k-1)) / ∂r_i
        Send the request r_i^(k) to CSP
    CSP collects the request profile r^(k)
    if r^(k) = r^(k-1) then Stop
    else set k ← k + 1
```

$$r_i^{(k)} = r_i^{(k-1)} + \Delta \frac{\partial U_i\left(r_i, r_{-i}^{(k-1)}\right)}{\partial r_i}$$

Extensions: Different Network Delays

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

Theorem 4. there exists at least one NE in the miner game under the variable delay setting.

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

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 Uniform Delay

- Miner i's optimal strategy is affected by
  - CSP's price set (p_s, p_c)
  - Download delay d
  - Self budget as well as other miners' budgets

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

$miners\ invest\ more\ on\ self\ mining\ as\ p_c\ increases$

5. Conclusion

- A Nash game among mobile PoC miners
  - Consider delay and cost tradeoff in mobile mining environment
  - Model the relation between winning probability and delay
  - Solve a price-based resource management problem
- Two network settings :
  - Uniform vs variable
- Experiments to confirm theoretical analysis

Thank you

Q & A