Bitcoin Mining with Transaction Fees
A Game on the Block Size

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

- A blockchain-based digital payment system
  - A distributed ledger using PoW mining mechanism
    - Prob. of solving a block puzzle relies on a miner’s computing rate
      \[ \lambda_i = \frac{\text{individual power}}{\text{total power}} \]
  - To win a block
    - Solve puzzle and then propagate the block to reach consensus
    - Propagation delay discounts the winning probability \( W_i \)
Each winner will be rewarded with $R_i$, including:

- **Block subsidies $S$:** finite supply and eventually become zero
- **Transaction fees $F_i$:** offered by users and gradually increase
  - Without $F_i$, miners have no incentive to include transactions in their blocks \([1]\)

Trend between $S$ and $F_i$:

- The sum of block subsidies and the average transaction fees collected per block remains **constant** \([2]\).

---


Miner’s Utility $U_i$

- **Utility** $U_i = R_i \times W_i$
  - Block reward $R_i = S + F_i$
    - Block subsidy $S$ is a fixed value in a block
    - Transaction (TX) fee $F_i \propto$ block size: $F_i = \alpha B_i$
  - Winning probability $W_i$
    - Positively related to computing rate $\lambda_i$
    - Discounted by propagation time $p_i$
      where $p_i \propto$ block size: $p_i = \beta B_i$ [3]

- **Block size** $B_i$
  - Default size $\bar{B} = 1$ MB
    - Recommended by system
    - Miner can choose any $B_i \leq \bar{B}$

Trade-off on Block Size

- Choose a large block size \( B_i \) a small block size

\[
\begin{align*}
\text{If } B_i & \uparrow \text{ then } R_i \uparrow \text{ but } W_i \downarrow \\
\text{If } B_i & \downarrow \text{ then } W_i \uparrow \text{ but } R_i \downarrow
\end{align*}
\]

- Find an optimal size \( B_i \) to maximize \( U_i \)
  - We want to find a suitable \( \overline{B} \) such that
    - \( \overline{B} \) is each miner's optimal size
2. Characterize $W_i$ Using $B_i$

- Distribution of block finding time $X_i$
  - **PDF:** $f_{X_i}(t; B_i, \lambda_i) = \begin{cases} 0 & t < p_i \\ \lambda_i e^{-\lambda_i(t-p_i)} & t \geq p_i \end{cases}$
  - **CDF:** $F_{X_i}(t; B_i, \lambda_i) = \begin{cases} 0 & t < p_i \\ 1 - e^{-\lambda_i(t-p_i)} & t \geq p_i \end{cases}$

- $W_i$ among n miners
  - Winner should have the smallest block finding time
  - $W_i = Pr\left(X_i = \min \{ X_j | j = 1, \ldots, n \} \right) = \frac{\lambda_i \sum_{j=1}^{n} e^{\sum_{j=1}^{n} \lambda_j (p_i - p_j)} - e^{\sum_{j=1}^{n} \lambda_j (p_i - p_j + 1)}}{\sum \lambda_j}$

Discounted by propagation delay
3. Game on Block Size

- Two types of players
  - Cheater: manipulate his block size $B_i$ for utility maximization
  - Honest miner: use default block size $\overline{B}$

- Game analysis on two different settings
  - Homogeneous miners
    - Assume all miners have the same computing rate
    - Analysis on Bitcoin mining network
  - Heterogeneous miners
    - Each miner can have different computing rate
    - Case studies on one cheater and two cheaters
4. Homogeneous Setting

- Bitcoin mining network
  - Approximated as 8 equal-size pools [4]
    - Viewed as 8 homogeneous cheaters
  - $S = 12.5$ and $F_i = B_i$ (that is $\alpha = 1$)
  - **Theorem 1.** In an 8-pool Bitcoin mining network, all cheaters' optimal block size is 4MB.
    - Thus, we recommend 4MB as default block size

---

5. Heterogeneous Setting

Qualitative analysis on utility and block size

- **Theorem 2.** A miner indirectly increases each of his rivals’ utility by increasing his own block size.

- **Theorem 3.** A miner’s optimal block size is positively related to his computing power (Fig. 1)

![Graph showing block size for two miners](image)

Miner 1’s mining power
Miner 2’s mining power

(a) \( S = 12.5, \alpha = 0.16, \beta = 8.2 \)  
(b) \( S' = 25, \alpha = 0.3, \beta = 8.2 \)

Fig. 1: Two miners 1 & 2: \( \lambda_1 < \lambda_2, \lambda_1 + \lambda_2 = 1 \)
Case Study: One Cheater

- **Setting:** miners are divided into two groups
  - Corrupted pool controlled by a cheater: Pool 1
    - Optimize $B_1$ for utility maximization
    - Computing rate: $\lambda_1$
  - The rest of the miners are honest: Pool 2
    - Use the default block size $\overline{B}$
    - Computing rate: $\lambda_2$ in total

Pool 1 and pool 2 are heterogeneous with regard to computing rate.
**Pool 1’s Utility Analysis**

- **Parameters affecting pool 1’s optimal size**
  - $B_1$ is positively related to computing rate $\lambda_1$
  - Decrease of subsidy $S$ leads to increase of $B_1$
  - Large network delay rate $\beta$ will reduce $B_1$

Fig. 2: Optimal block size using different sets of $(S, \alpha, \beta)$
Peaceful Equilibrium

- **Peaceful equilibrium** is a condition where
  - Pool 1’s optimal block size $B_1 = \bar{B}$
  - Upper bound of $\lambda_1$
    - Theorem 4. If $\lambda_1 \leq 1/3$, A’s optimal block size $B_1$ equals to $\bar{B}$
  - Block subsidy and equilibrium ($\lambda_1 > 1/3$)
    - The decrease of $S$ could lead to more equilibria (Fig. 3)
      - Since TX fees become main income, pool 1 has incentive to increase $B_1$

**Fig. 3**: Red area represents $B_1 = \bar{B}$ and black area represents $B_1 < \bar{B}$
Network Delay and Equilibrium ($\lambda_1 > 1/3$)

- When network delay is reasonable: (Fig. 4)
  - If $\alpha$ is high enough and $S$ is low, then $B_1 = \overline{B}$

- When network delay is serious: (Fig. 5)
  - Hard to see peaceful equilibrium, that is $B_1 < \overline{B}$
  - Damage Bitcoin network if attackers issue delay attacks

Fig. 4: $\beta = 8.2$
Fig. 5: $\beta = 82$
Case Study: Two Cheaters

- **Setting:** miners are divided into three groups
  - Two cheaters: L and H
    - L has a smaller pool with computing rate: $\lambda_L$
    - H has a larger pool with computing rate: $\lambda_H$
  - The rest of the miners $M$ are honest
    - Use the default block size $\bar{B}$ with computing rate: $\lambda_M$ in total

- Cheaters:
  - Pool L manipulate $B_L$
  - Pool H manipulate $B_H$

- Honest Pool $M$ set $B_M = \bar{B}$

L, H, and M are heterogeneous regarding to computing rate.
Sided Misbehaviors

- One side: only L cheats on his block size
  - If $\lambda_L > 8\%$, L's optimal size $B_L < \bar{B}$ (Fig. 6)

- Both sides: L and H cheat on block sizes
  - For $\bar{B} = 1$ MB, L and H always have optimal sizes smaller than $\bar{B}$, no matter what their computing rates are (Fig. 7)
  - Current default size must be redefined
6. Conclusion

- A game on block size
  - Consider tradeoff between propagation time and TX fees
  - Model the relation between winning probability and block size

- Game Analysis on two different settings
  - Homogeneous miners in bitcoin mining network
  - Heterogeneous miners for case studies

- Real-world data to confirm theoretical analysis
  - Future work: conduct experiments on real blockchain platform, eg. CITA [5], to measure real-time propagation delay influences.

Thank you

Q & A