CERIAS

The Center for Education and Research in Information Assurance and Security

Towards A More Stable Bitcoin Transaction Fee Design

Tiantian Gong, Wenhai Sun, Baijian Yang {gong146, sun841, byang@purdue.edu}

1. Motive

Bitcoin currently provides block rewards and transaction fees as incentives for miners. This mechanism has been proven to be incentive incompatible. Further when the block rewards subside and fees become the incentivization pillar of Bitcoin system, the stability of the system is to be questioned due to the time-varying nature of transaction fees under current protocols[1]. We dig deeper into the complex security and economic implications in an attempt to reveal the impactful fee-choosing strategies and shed light on one transaction fee design to restore the equilibrium in the presence of deviate mining behaviors.

2. Goal

To design a transaction fee framework for block space market that:

- For miners – makes it **computationally indistinguishable** between operating on different platforms (eg. Bitcoin, Ethereum) and at different time on one platform;
- For users – moderates the queueing problem

3. Assumptions & Key Notations

- **Assumptions**

- Miners and users are rational and make the choices that maximize their respective utility;
- Miners always chose to mine on one specific platform with one mining strategy at a given time t;
- Users offer the minimal transaction fees that will maximize the probability of their transactions to be settled within a certain time interval;
- The reward distribution policy remains unchanged and fork resolving policy goes through changes, which makes this design backward compatible;
- No information propagation latency.

- **Notations**

- Mining Strategy Set: $S = \{S_1, S_2, \ldots, S_k\}$, where $S_i = (TX, Parent, Publish)$;
- Transaction Set: $TX = \{TX_{m,1,t}, TX_{m,2,t}, \ldots, TX_{m,s,t}\}$, where $TX_{m,i,t} = (l_{m,i,t}, F_{m,i,t})$ and $l_{m,i,t}$ denotes the msg length in bytes, $F_{m,i,t}$ denotes the transaction fee attached (+ child pays for parent);
- Platform Set: $P = \{P_1, P_2, \ldots, P_S\}$, we assume platforms are not completely substitutable;
- Fees per Byte: $F/B_{m,i,t} = F_{m,i,t} / l_{m,i,t}$, transaction fees per byte on platform m at time t;
- Interoperation costs: $C_{i,j}$, $i,j \in P$;

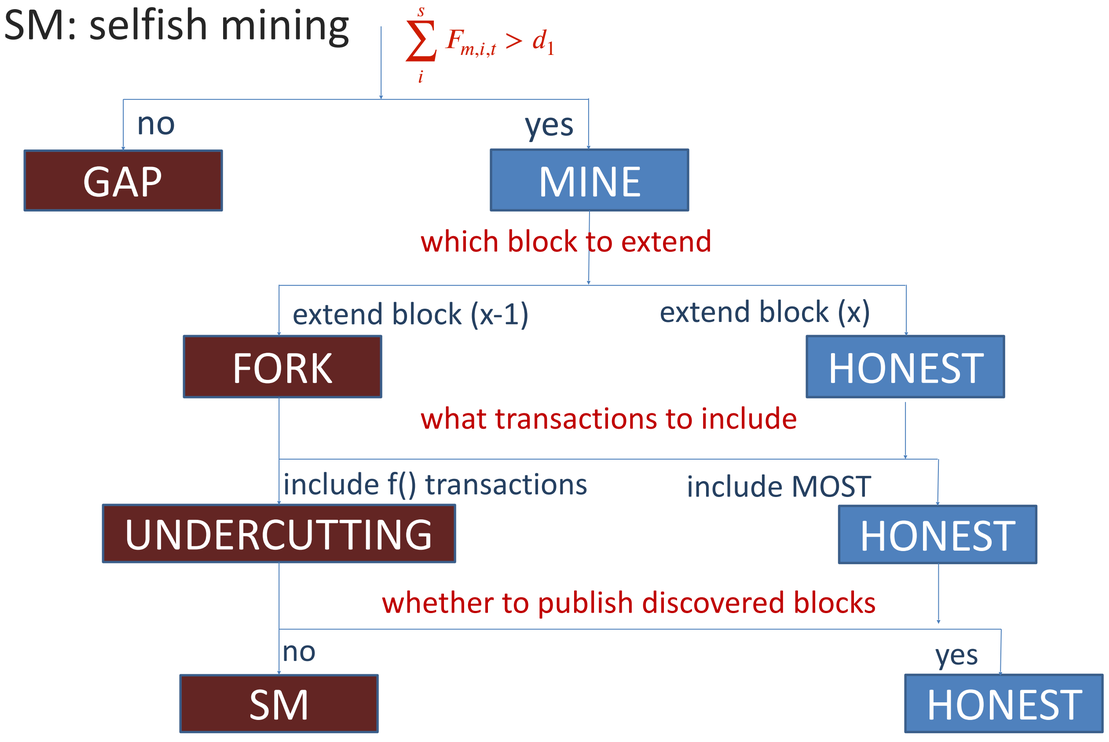
4. Model

- Miners' Choices

d_1 : threshold transaction fees for miners to start mining

GAP: wait until wealthy transactions appear

SM: selfish mining



- Time Indistinguishability

At time t, make undercutting profitable with negligible probability:

,

where π_m, π_f respectively the probability the next miner is to extend on the oldest block or the fork, ***F*** and ***F'*** respectively the transaction fees claimed on the aforementioned two blocks, and respectively the transaction fees unclaimed, ***B*** the block size.

- Space Indistinguishability,

where is the interoperation costs between platform m and k.

5. Simulation

1st one platform, model transaction fees considering transaction events as Poisson process with rate λ;

2nd two platforms with fixed interoperation costs

6. Reference

[1] M. Carlsten, H. Kalodner, S. Weinberg, and A. Narayanan. On the Instability of Bitcoin Without the Block Reward. CCS'16, 2016, doi:10.1145/2976749.2978408.

[2] I. Tsabry and I. Eyal. The Gap Game. CCS '18, 2018, doi: 10.1145/3243734.3243737.

[3] Nicolas Houy. The economics of Bitcoin transaction fees. Working paper GATE 2014-07. 2014.