# Blockchain Mining Games

Presentation
Lecturer: Hong-Sheng Zhou

Jianqiang Li, V#: v00821365

Apr 18 2017

# Selfish Mining

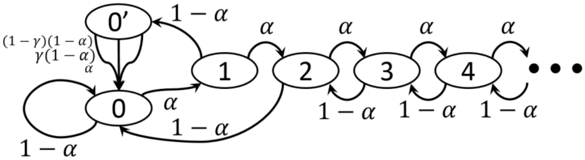


Figure: State machine with transition frequencies

## Stategy 1

When the selfish miner's branch is 1 blocks ahead, the selfish miner release entire branch immediately.

# Selfish Mining

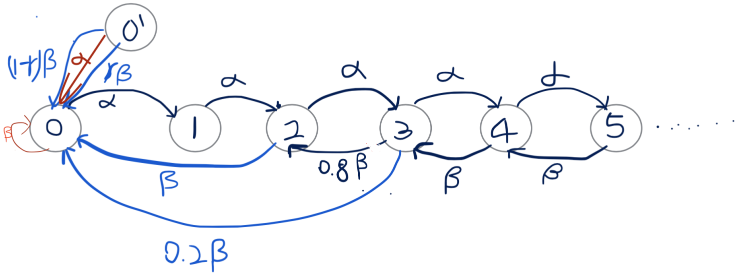


Figure: State machine with transition frequencies

## Stategy 2

When the selfish miner's branch is 2 blocks ahead, instead of keeping her own branch private from the public, the selfish miner now with probability 0.2 reveals her entire branch immediately.

# Selfish Mining Strategy

1 blocks ahead...

A miner with computational power at least 33% of the total power, provides rewards strictly better than the honesty strategy[2]

2 blocks ahead.....?

3 blocks ahead.....?

Which strategy is the optimal corresponding to the computational power?

What can we do?

# Blockchain Mining Games

Game-theoretic provide a systematic way to study the strengths and vulnerabilities of bitcoin digital currency[1].

## Game-theoretic abstraction of Bitcoin Mining

- Miner 1 is the miner whose optimal strategy (best response) we wish to determine($\alpha$)
- Miner 2 is assumed to follow the Honesty strategy or Frontier Strategy (Follow the longest chain) ($\beta$) $\alpha + \beta = 1$.
- the reward $r^*$ and computational cost $c^*$
- the depth of the game $d$, after $d$ new blocks attached to the chain, the reward will be paid for this block.

# Game-theoretic abstraction of Bitcoin Mining

## Sate

- A public state is simply a rooted tree. Every node is labeled by one of the players;
- A private state of a player i is similar to the public state except it may contain more nodes called private nodes and labeled by i.

We consider complete-information games (the private states of all miners are common knowledge).

# Game-theoretic abstraction of Bitcoin Mining

## Selfish (rational) miners want to know

- which block to mine
- when to release a mined block

## Strategy of a player (miner) i

- the mining function $\mu_i$ selects a node of the current public state to mine
- the release function $\rho_i$ determines the section of the private states is added to the public state
- Notation: follow the longest chain is Honesty strategy (Frontier strategy)

# Immediate-Release Game

miner 1: selfish
miner 2: honest

State
(a, b)
1 2

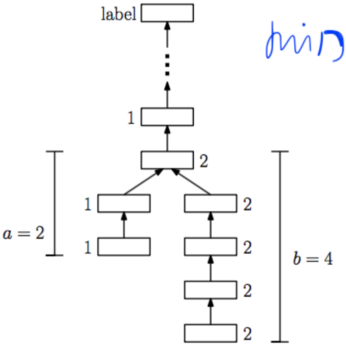


Figure: Typical State

# Immediate-Release Game

## Mining states

The set M, both miners keep mining their own branch. (0,0)$\in M$

## Capitulation states

The set C, miner 1 gives up on his branch and continues mining from some block of the other branch. e.g., when the game is truncated at depth d, the set contains (a,d) for a=0,....,d.

## Wining state

The set W of states in which Miner 2 capitulates, Miner 2 honesty (plays Frontier) $W = \{(a, a-1) : a \geq 1\}$.

# Immediate-Release Game)

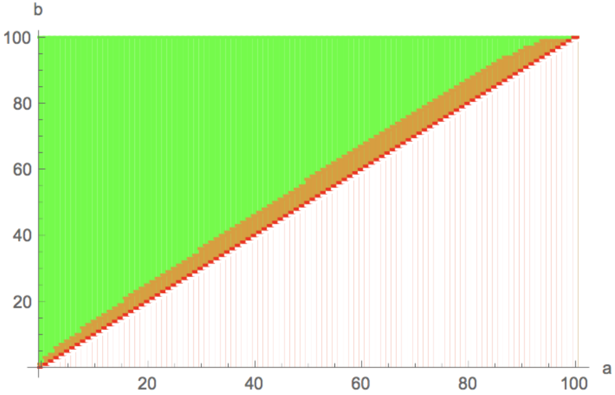


Figure: Upper-left green aprt is the set Capitulation states, red line of Wining states, orange part of Mining state

# Immediate-Release Game

## What happens when miner 1 capitulates?

- Miner 1 will abandons his private branch, he can choose to move to any state (0,s).
- Then set of deterministic strategies of Miner 1 is set of pairs (M,s), M is set of mining set.

# Immediate-Release Game

## Expected gain of Miner 1

- $g_k(a, b)$ denote the expected gain of Miner 1, when the branch of the honest miner in the tree is extended by k new levels starting from an initial tree in which Miner 1 and 2 have lengths $a$ and $b$ respectively.
- Then, for large k, $k^{'}$. we have

$$g_k(a, b) - g_{k'}(a, b) = g^*(k - k^{'}) \tag{1}$$

  $g^*$ represents the expected gain per level
- $g_k(a, b) = \mathrm{k}g^* + \psi(a, b)$
  $\psi(a, b)$ the potential function denote the advantage of Miner 1 for currently being at state (a,b)

# Immediate-Release Game

The objective of Miner 1 is to maximize $g^*$

## For a strategy (M,s)

- If (a,b)$\in$ M, Miner 1 succeeds to mine next block first with probability $\alpha$, then new state is (a+1,b);
- If (a,b)$\in$ C, Miner 1 abandons his branch and the new state is (0,s).
- If (a,b) $\in$ W, Miner 2 abandons his branch and the new state is (0,0).

# Immediate-Release Game

From above consideration and $p = \alpha, 1 - p = \beta$, we have

$$g_k(a,b) = \begin{cases} g_{k-1}(0,0) + a & a = b+1 \\ \max\left(\max_{s=0,\ldots,b-1} g_k(0,s), p g_k(a+1,b) + (1-p) g_{k-1}(a,b+1)\right) & \text{otherwise} \end{cases}$$

and by definition $g_0(a,b) = 0$. From this, we can get a similar recurrence for $\varphi$:

$$\varphi(a,b) = \begin{cases} \varphi(0,0) + a - g^* & a = b+1 \\ \max\left(\max_{s=0,\ldots,b-1} \varphi(0,s), p\varphi(a+1,b) + (1-p)\varphi(a,b+1) - (1-p)g^*\right) & \text{otherwise} \end{cases}$$

We also fix $\varphi(0,0) = 0$; note that the potential of all states is non-negative.

# Immediate-Release Game

## Definition

- Let $r_{(M,s)}(a, b)$ denote the wining probability starting at state (a,b),
- Let $r(a, b)$ denote the optimal strategy (M,s).

## Lemma 1 For every state (a,b)

$$r(a, b) \leq (\frac{\alpha}{\beta})^{1+b-a} \tag{2}$$

1+b-a captures the distance of state (a,b) and wining state.

# Immediate-Release Game

Lemma 2 For every state (a,b) and every nonnegative integers c and k

$$g_k(a+c, b+c) - g_k(a, b) \leq cr(a+c, b+c) \qquad (3)$$

Lemma 2 provide a useful relation between expected optimal gain and the wining probability.

Corollary 1. For every state (a,b) and every nonnegative integer c

$$\psi(a, b) \geq \psi(a+c, b+c) - cr(a+c, b+c) \qquad (4)$$

Corollary 1 provide a useful relation between the potential function and the wining probability.

# Immediate-Release Game

**Lemma 3** For every $\alpha$, we have

$$\psi(0,0) + r(1,1) \geq \psi(1,1) \geq \alpha\psi(2,1) + \beta\psi(1,2) - g^*\beta \tag{5}$$

Then we have

$$\psi(1,2) \leq \frac{2\alpha^2 - \alpha}{(1-\alpha)^2} + g^*\frac{1}{1-\alpha} \tag{6}$$

# Immediate-Release Game

Similarly, we have

Lemma 4 For $\alpha \leq 0.382$, if state (0,2)$\in M$, we have

Then we have

$$\psi(0,2) \leq \frac{2\alpha^2 - (1-\alpha)^3}{(1-\alpha)^2} \tag{7}$$

For $\alpha \leq 0.36$ state (0,2) is not a mining state

Lemma 5 For $\alpha \leq 0.382$, if state (0,1)$\in M$, then (0,2) is also a mining state and

$$\psi(0,1) \leq \beta\psi(0,2) - \alpha\frac{1-3\alpha+\alpha^2}{(1-\alpha)} \tag{8}$$

For $\alpha \leq 0.36$ state (0,2) is not a mining state

# Immediate-Release Game Results

Lemma 6 Honesty Strategy is a best response for Miner 1 iff $\psi(0,1) = \psi(0,0)$

Theorem 1, In the immediate-release model, Honesty strategy is a Nash equilibrium when every miner computational power less than 0.36

Theorem 2, In the immediate-release model, the best response strategy for Miner 1 is not honesty strategy when computational power larger than 0.455

# The Strategic-Release Game Results

Contrary to the immediate-release case, the state (a,b) could be that $a$ is strictly larger than $b + 1$

Similarly, we have

Theorem 3, In the Strategic-Release model, Honesty strategy is a Nash equilibrium when every miner computational power less than 0.308

- Kiayias, Aggelos, et al. "Blockchain mining games." *Proceedings of the 2016 ACM Conference on Economics and Computation. ACM*, 2016.
- Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *International Conference on Financial Cryptography and Data Security.* Springer Berlin Heidelberg, 2014.