Game Theoretical Analysis of a Reputation-Based Cryptocurrency Mining Paradigm

Mehrdad Nojoumian
Department of Computer & Electrical Eng. and Computer Science
Florida Atlantic University

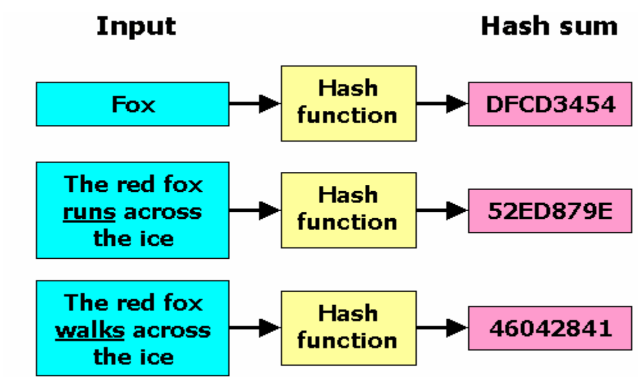
18th International Symposium on Dynamic Games and Applications
Grenoble, France
July 10, 2018

Contents of the Talk

Preliminary Material: Hash Function

➢ Hash Function:

- ✓ A **hash function** is any function that can be used to map data of arbitrary size to data of fixed size.



- ✓ If a **single bit** is changed, the hash value will be changed completely.

Example: suppose the hash value is 4 bits, the total possibilities are 2^4=16

0000	0001	0010	0011
0100	0101	0110	0111
1000	1001	1010	1011
1100	1101	1110	1111

The probability of having a hash value **0** X X X, where X is 0 or 1 → 8/16 = **0.5**
I.e., a hash value smaller than or equal to 7

The probability of having a hash value **0** **0** X X, where X is 0 or 1 → 4/16 = **0.25**
I.e., a hash value smaller than or equal to 3

Picture created by David Gothberg

Blockchain

➢ Terminologies:

- ✓ Transactions are grouped in blocks in order to be verified by a subset of nodes in the network, known as **miners**.
- ✓ The mining process, a.k.a., **proof-of-work**, is computationally intensive with a difficulty factor that is increased overtime as the computational power of hardware systems/miners grows.
- ✓ Nodes form **mining pools** under the supervision of pool managers to accomplish the mining task.
- ✓ The first mining pool that accomplishes the proof-of-work is rewarded, e.g., by **freshly mined Bitcoins***, as an incentive for miners' works.
- ✓ As soon as a block is verified, it is attached to the list of existing verified blocks, a.k.a., **Blockchain**. Immediately after that, miners stop the mining process of the verified block and start working on the next block.
- ✓ The hashing rate, a.k.a., **mining power**, is the total number of hashes that a miner can calculate during a specific time interval. The pool manager distributes the revenue among miners based on their mining powers.

* The maximum number of Bitcoins is limited to about 21 Million

Mining Mechanism

➢ Proof-of-Work:

✓ Each block of transactions is connected to the next block by its hash value, which is smaller than a threshold, e.g., **000**X…X.

Block #	77
Nonce	272931
Transactions	25B Alice → Bob ... 50B Alex → Mary
Previous	000937af19be17
Current Hash	0007ae291da311

Block #	78
Nonce	171943
Transactions	10B Sara →Eli ... 55B Eve → Cory
Previous	0007ae2913da11
Current Hash	0009da7537eb68

Block #	79
Nonce	**Try diff values**
Transactions	15B John → Ed ... 30B Dan → Geff
Previous	0009da7537eb68
Current Hash	**Find a valid hash**

- The next block of transactions **cannot be verified** unless the previous block is first verified.
- Miners should change the nonce value randomly until they find a valid hash value that is smaller than the predefined threshold, a.k.a., solving a **mathematical puzzle**.
- The threshed defines the difficulty of the math puzzle. The **difficulty factor** is increased periodically so that it takes almost 10 minutes to solve the puzzle, i.e., from **000**X…X to **0000**X…X.

Dishonest Mining Strategies

- **Why?** The mining process is very resource intensive, therefore, miners form coalitions to verify each block of transactions in return for a reward where only the first coalition that solves the puzzle will be rewarded.

  - ✓ **Block withholding attack:** where a dishonest player only reveals a partial solution of the verification problem whenever he has the complete solution to act in favor of another competing coalition.
  - ✓ **Selfish mining:** where the players of a coalition keep their discovered blocks private and continue to verify more blocks privately until they get a sub-chain that is larger than verified blocks.
  - ✓ **Eclipse attack:** makes a node invisible in the network, i.e., a single node monopolizes all possible connections to a victim & eclipses it from the network.
  - ✓ **Stubborn mining:** mining on its private chain more than the selfish mining strategy. In selfish mining, miner withholds blocks when he is ahead of others (i.e., he has created a private chain longer than that of the honest network), but cooperates with the honest network when he falls behind.
  - ✓ **Distributed denial-of-service attack, and many more upcoming attacks.**

Reputation-Based Mining Paradigm

➢ **Motivation:** it is necessary to **regulate** the mining process to make miners accountable for any dishonest mining behavior.

i	1	2	3	...	$I-1$	I
p_i	250B	125B	0B	...	200B	75B

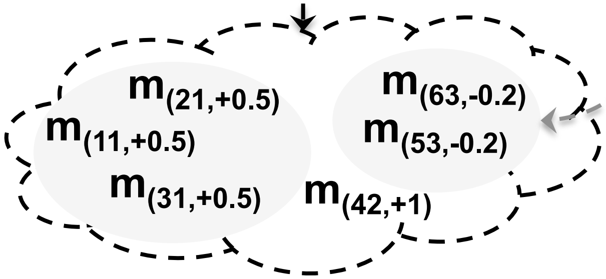
Pool Manager $M_{(1,\,250B)}$

Managers: $M_{(i,\,p_i)}$

$1 \le i \le I$: *identity*

$0 \le p_i$: *profit*

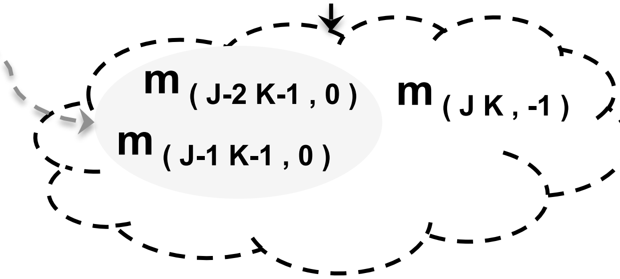
Pool Manager $M_{(I,\,75B)}$



First Mining Pool

Ally Miners

...



Last Mining Pool

Miners: $m_{(j\,k,\,r_k)}$

$1 \le j \le J$: *identity*

$1 \le k \le K$: *reputation id*

$-1 \le r_k \le +1$: *reputation*

k	1	2	3	...	$K-1$	K
j	1, 2, 3	4	5, 6	...	J-2 , J-1	J
r_k	+0.5	+1	-0.2	...	0	-1

Reputation-Based Mining Paradigm (Cont.)

➢ Mechanism:

- ✓ A mining game is repeatedly played among a set of pool managers and miners where the **reputation** of each miner or mining ally is continuously measured.
- ✓ Two actions are considered, i.e., disrupt computations of mining pools, i.e., **dishonest mining**, or conduct the proof-of-work honestly, i.e., **honest mining**.
- ✓ At each round of the game, the pool managers send **invitations** only to a subset of miners based on a non-uniform probability distribution defined by the miners' reputation values.

➢ Our Result in Nutshell:

- ✓ We show that by using our proposed solution concept, the **honest mining** strategy becomes Nash Equilibrium in our setting.
  1. It will not be in the best interest of the miners to employ dishonest mining strategies even by gaining **a short-term utility**.
  2. This is due to the consideration of **a long-term utility** in our model and its impact on the miners' utilities overtime.

Reputation-Based Mining Paradigm (Cont.)

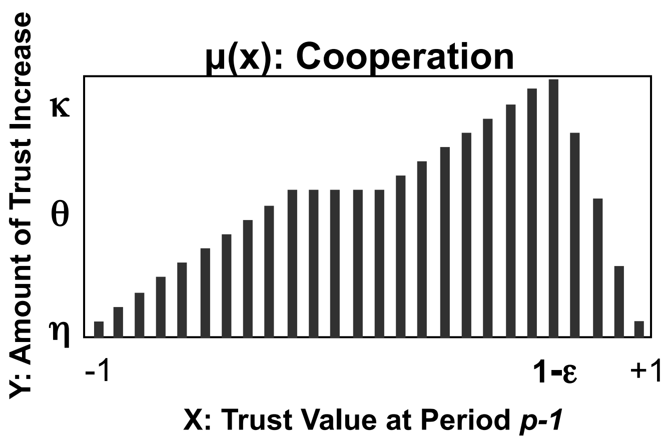
➢ **Highlights:**

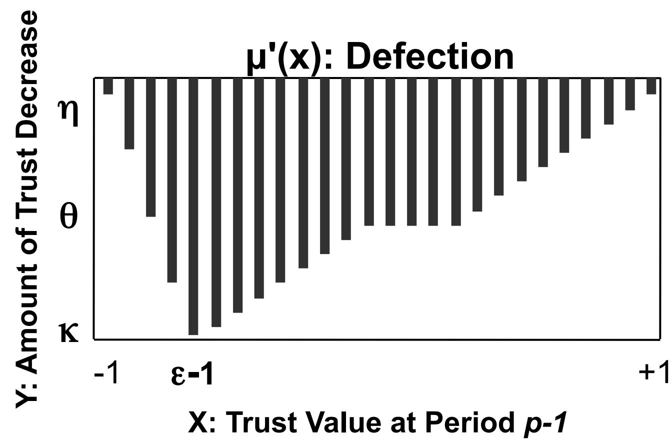
- ✓ A subset of miners who highly trust each other (due to partnerships, common nationality, or geographical proximity) can form an alliance, named **ally miners**.
- ✓ Once in a while, the pool managers rearrange their groups to form new coalitions for the proof-of-work. They send **invitations** to miners/ally miners.
- ✓ The miners/ally miners **can also chose** to whom they would like to join if they receive multiple invitations.
- ✓ Note that the underlying reputation system must be immune against **re-entry attack**, i.e., cheat and come back to the scheme with a new identity.
- ✓ While ally miners are incentivized to form larger coalitions to gain/sustain a high reputation value and consequently more revenue, they are **not incentivized** to admit any new miner to their alliance unless they fully trust the newcomer.

Sample Trust Model and Re-Entry Attack

➢ **Sample function** is not just a function of a single round, but of the history:

Trust Value	Cooperation	Defection
$T_{Bad\ P_j} \in [-1,\beta)$	Encourage	**Penalize**
$T_{New\ P_j}: [\beta,\alpha]$	Give/Take Opportunities	
$T_{Good\ P_j} \in (\alpha,+1]$	**Reward**	Discourage





➢ **Prevention of the Re-Entry Attack*:**

✓ Function f_1 based on previous trust value and current action.

✓ Function f_2 based on previous trust value, current action, & **lifetime indicator**.

* Rational Trust Modeling: **https://arxiv.org/abs/1706.09861**

Detection Mechanisms

- **Block Withholding Attack:**
  - ✓ A pool can detect if is under a block withholding attack with a high accuracy. Difference between the **expected mining power** and **actual mining power** that is above a threshold, can be an indication of a block withholding attack.
  - ✓ To determine which registered miner is the perpetrator/committing to the attack:
    1. If the mining power of a miner/ally miners is high enough, the **ratio** of the full proof-of-work over the partial proof-of-work can indicate whether the miner/alliance is committing to the block withholding attack.
    2. If the mining power is not high, the frequency of success to find the full proof-of-work is very low, and statistically, we may not be able to define if a miner is really committing to the block withholding attack. This has a **negligible** impact on the mining process.

- **Selfish or Stubborn Mining:**
  - ✓ An increase in the **# of orphaned** blocks can be an indication of selfish mining*.
  - ✓ The amount of time taken to release consecutive blocks in the Blockchain can potentially provide evidence of selfish mining. I.e., two blocks in **close succession** should be a very rare incident when miners are honest.

 * http://scienceblogs.com/builtonfacts/2014/01/11/is-bitcoin-currently-experiencing-a-selfish-miner-attack/

Detection Mechanisms (Cont.)

- **Eclipse Attack:**

  - ✓ It has several signatures and properties that make it detectable, for instance, a **flurry of short-lived incoming TCP connections** from diverse IP addresses.
  - ✓ Moreover, an attacker that suddenly **connects a large number of nodes** to the Bitcoin network could also be detected.
  - ✓ Therefore, **anomaly detection** software systems that look for similar behaviors can be helpful to detect the attacker.

- **Other Detection Mechanisms:**

  - ✓ To detect **bribes** and illegal money exchanges among registered miners in the transparent network of Bitcoin; unless they exchange bribes outside of the network. This is how the government agencies detect illegal money exchanges.
  - ✓ Detection of these bribes might be an indication of **collusion**; why miners from two competing pools should frequently exchange money with a certain amount.

Without a Reputation-Based Mechanism

➢ Dishonest Mining Is Nash Equilibrium:

- ✓ We consider a scenario in which two miners have to **decide** whether to collude with an attacker to disrupt another mining pool's effort or not.
  - ✓ If both miners collude, they each gain a **half-unit of utility**. In other words, the attacker's budget will be equally shared between both miners.
  - ✓ However, if one miner colludes but the other one acts honestly, the colluding miner will receive **one unit of utility** from the attacker.

$m_{(jk,r_k)}$ \ $m_{(j'k',r'_k)}$	$\mathscr{H}$: Honest Mining	$\mathscr{D}$: Dishonest Mining
$\mathscr{H}$: Honest Mining	(฿0, ฿0)	(฿0, ฿Ω)
$\mathscr{D}$: Dishonest Mining	(฿Ω, ฿0)	$(฿\frac{\Omega}{2}, ฿\frac{\Omega}{2})$

Table 1. Payoff in Colluding Miner's Dilemma

Assumptions

$u_j(a)$ denote $m_{(jk,r_k)}$'s long-term utility in outcome a

$u'_j(a)$ denote $m_{(jk,r_k)}$'s short-term utility

$$d_j(a) \in \{0,1\}$$

$$\Delta(a) = \sum_i d_j(a)$$

- **Miners' Preferences:**

$$d_i(a) = d_i(a') \ \&\ r_k^a(p) > r_k^{a'}(p) \Rightarrow u_j(a) > u_j(a')$$

$$d_i(a) > d_i(a') \Rightarrow u'_j(a) > u'_j(a')$$

$$d_i(a) > d_i(a') \ \&\ \Delta(a) < \Delta(a') \Rightarrow u'_j(a) > u'_j(a')$$

With a Reputation-Based Mechanism

➢ Honest Mining Is Nash Equilibrium:

decision making

- ✓ Each miner prefers to sustain a high reputation value overtime despite of employing honest or dishonest mining strategies as he can potentially **gain a higher long-term utility**.
- ✓ If a miner utilizes a dishonest mining strategy, he **gains a short-term utility** from the attacker.
- ✓ If a miner employs dishonest mining strategies and the # of dishonest miners in outcome_1 is less than the # of dishonest miners in outcome_2, the miner **gains a higher short-term utility** in outcome_1.

U

$m_{(jk,r_k)}$ \ $m_{(j'k',r'_k)}$	$\mathscr{H}$: Honest Mining	$\mathscr{D}$: Dishonest Mining
$\mathscr{H}$: Honest Mining	(฿1.5, ฿1.5)	(฿1.5, ฿0)
$\mathscr{D}$: Dishonest Mining	(฿0, ฿1.5)	(฿ − 0.17, ฿ − 0.17)

Table 2. $(2,2)$-Game Between Two Miners

Thank You Very Much

Questions?