Majority is not Enough: Bitcoin Mining is Vulnerable

Ittay Eyal and Emin G¨un Sirer

2019.03.25

Ittay Eyal

Ittay Eyal

Technion

Verified email at technion.ac.il - Homepage

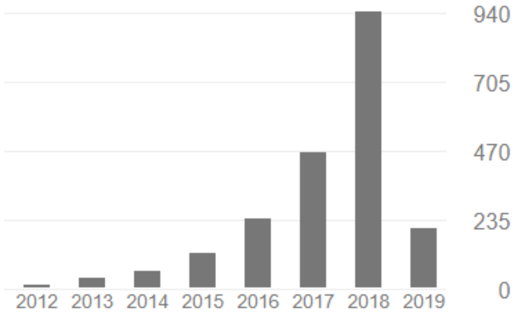
Distributed systems securit...

FOLLOW

TITLE	CITED BY	YEAR
Majority is not enough: Bitcoin mining is vulnerable I Eyal, EG Sirer Eighteenth International Conference on Financial Cryptography and Data ...	808 *	2014
Bitcoin-ng: A scalable blockchain protocol I Eyal, AE Gencer, EG Sirer, R Van Renesse 13th {USENIX} Symposium on Networked Systems Design and Implementation ...	389	2016
On scaling decentralized blockchains K Croman, C Decker, I Eyal, AE Gencer, A Juels, A Kosba, A Miller, ... International Conference on Financial Cryptography and Data Security, 106-125	376	2016
The Miner's Dilemma I Eyal Proceedings of the 36th IEEE Symposium on Security and Privacy (Oakland)	189	2015
Robust data sharing with key-value stores C Băsescu, C Cachin, I Eyal, R Haas, A Sorniotti, M Vukolić, I Zachevsky IEEE/IFIP International Conference on Dependable Systems and Networks (DSN ...	46	2012
Decentralization in bitcoin and ethereum networks AE Gencer, S Basu, I Eyal, R Van Renesse, EG Sirer arXiv preprint arXiv:1801.03998	41	2018

Cited by

	All	Since 2014
Citations	2132	2063
h-index	15	14
i10-index	17	15



Co-authors VIEW ALL

- Emin Gün Sirer — Cornell University
- Robbert van Renesse — Principal Research Scientist, Cor...
- Adem Efe Gencer — PhD, Computer Science, Cornell...
- Idit Keidar

Cryptocurrencies

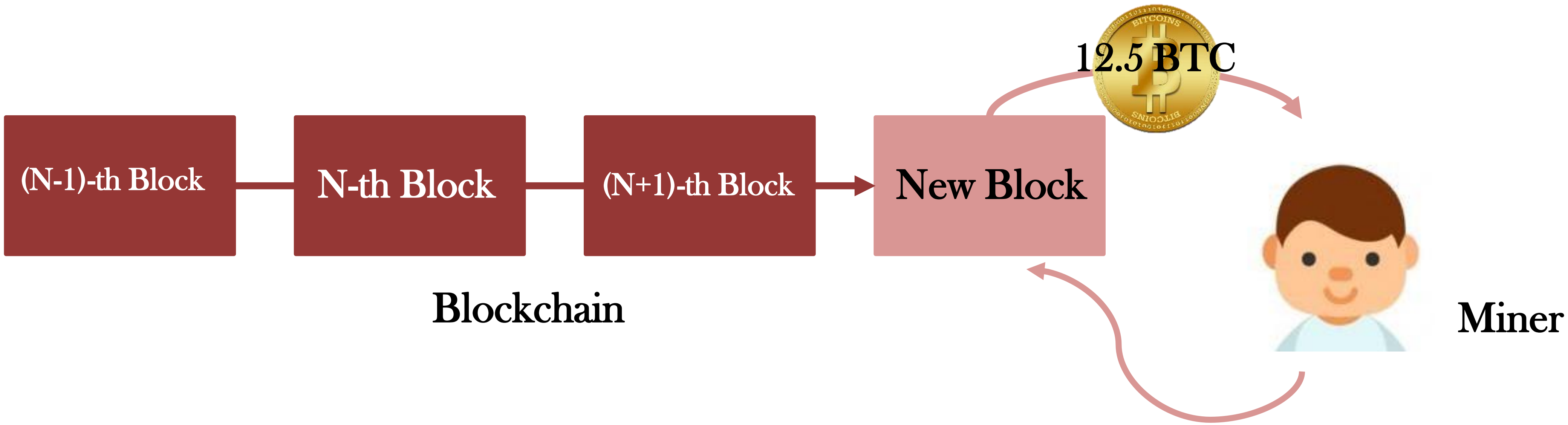
Popular algorithm: PoW

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

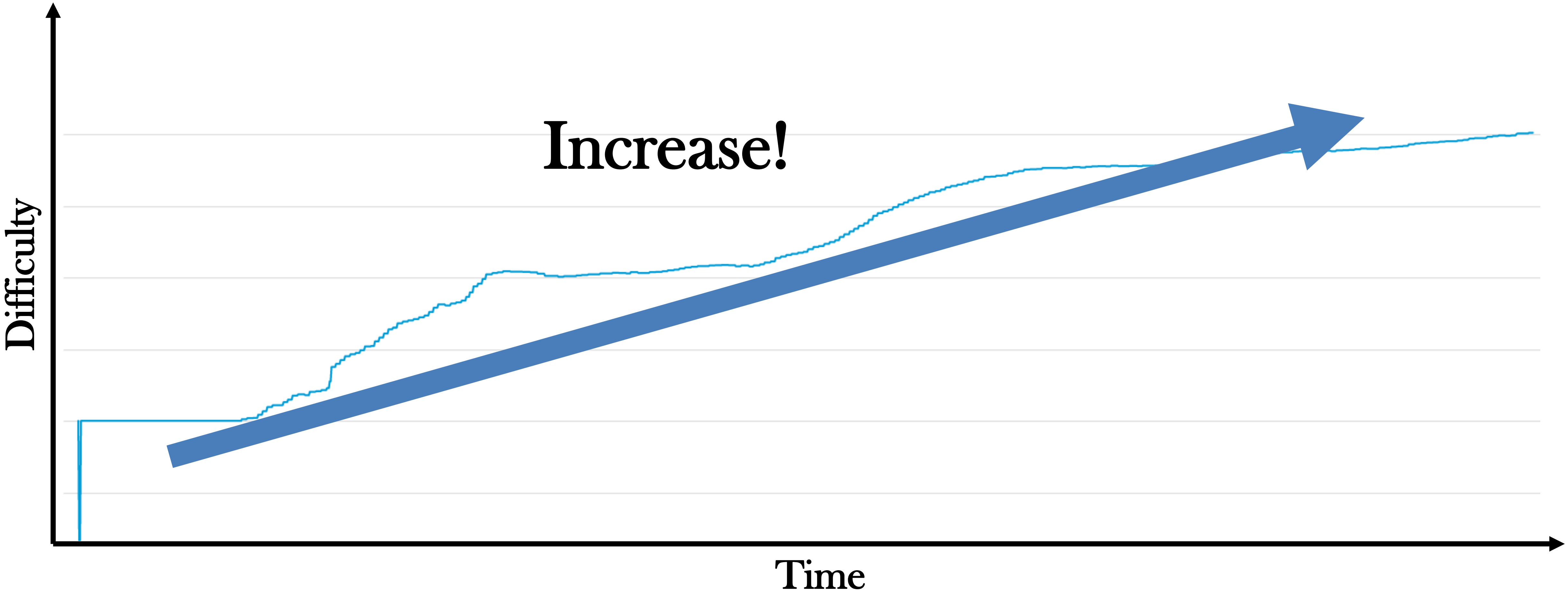
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$70,773,218,524	$4,019.46	$8,915,802,711	17,607,650 BTC	-0.20%	
2	Ethereum	$14,454,763,321	$137.18	$4,053,904,645	105,370,652 ETH	-0.43%	
3	XRP	$12,895,478,801	$0.309496	$600,330,476	41,666,017,553 XRP *	-0.69%	
4	Litecoin	$3,655,861,447	$59.91	$2,101,490,815	61,026,011 LTC	-1.82%	
5	EOS	$3,303,811,081	$3.65	$1,388,966,728	906,245,118 EOS *	-0.69%	
6	Bitcoin Cash	$2,919,181,847	$165.02	$411,585,974	17,690,000 BCH	0.06%	
7	Stellar	$2,052,666,388	$0.106769	$193,767,980	19,225,307,919 XLM *	-1.27%	
8	Cardano	$1,592,024,770	$0.061404	$112,386,088	25,927,070,538 ADA	-1.42%	
9	TRON	$1,578,286,194	$0.023669	$305,340,812	66,682,072,191 TRX	-1.45%	
10	Bitcoin SV	$1,170,414,897	$66.24	$80,843,318	17,670,348 BSV	-0.95%	

Proof-of-Work Mining

- They use **blockchain** to run without a trusted third party.
- Miners generate blocks by spending their **computational power**.
- If a miner generates a valid block, he earns **reward for the block.**
- This process is **competitive.**



Mining Difficulty



From "https://blockchain.info"

Can we earn the extra reward through fork?

❖ The change of mining difficulty

❖ Validators consider the expected relative revenue per one round (10 mins) as their payoff.

Can we earn the extra reward through fork?

❖ The change of mining difficulty

❖ Validators consider the expected relative revenue per one round (10 mins) as their payoff.

If a miner possesses 10% of the total computational power?

Can we earn the extra reward through fork?

❖ The change of mining difficulty

❖ Validators consider the expected relative revenue per one round (10 mins) as their payoff.

If a miner possesses 10% of the total computational power?

He earns 10% of the total reward.

Poisson distribution

- The Poisson distribution expresses the probability of a given number of events occurring in a fixed interval of time or space if these events occur with a known constant rate and ***independently*** of the time since the last event.

$$\Pr[k \text{ events in one interval}] = e^{-\lambda}\frac{\lambda^k}{k!}$$

Poisson distribution

- The Poisson distribution expresses the probability of a given number of events occurring in a fixed interval of time or space if these events occur with a known constant rate and ***independently*** of the time since the last event.

$$\Pr[k \text{ events in one interval}] = e^{-\lambda} \frac{\lambda^k}{k!}$$

In the Bitcoin system, one event means a generation of one block.

The 51% Attack

51% Attack

- Majority of hashing power has voted for transactions on longest chain.
  - It is costly to increase voting power
  - Players are not motivated to cheat

- If any party controls majority of hashing power, they can:
  - Undo the past
  - Deny mining rewards
  - Undermine the currency

Goldfinger Attack

- In the James Bond movie....
- The attacker's goal is to destroy Bitcoin by executing the 51% attack.
- Is a realistic attack?

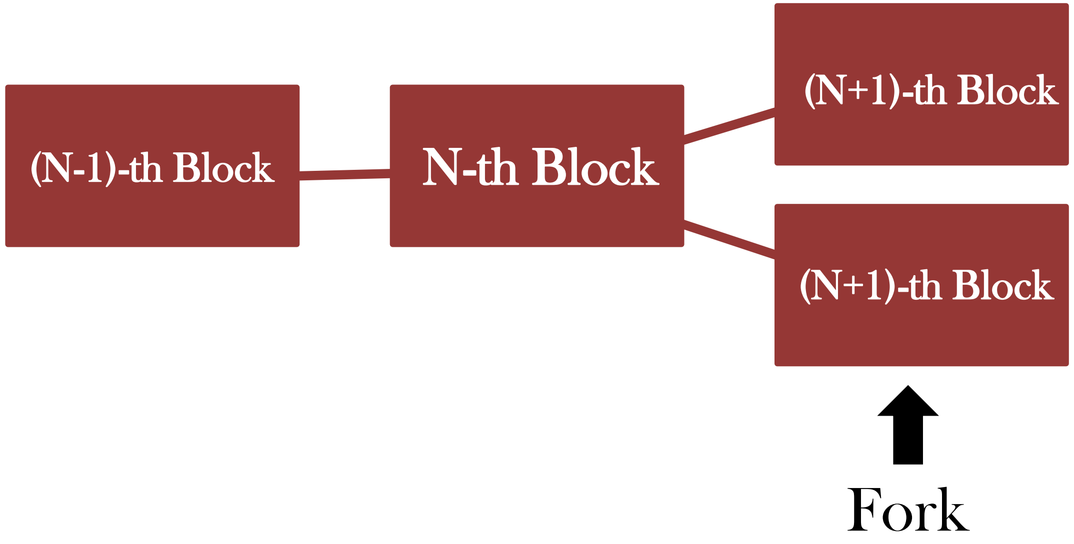
Selfish Mining

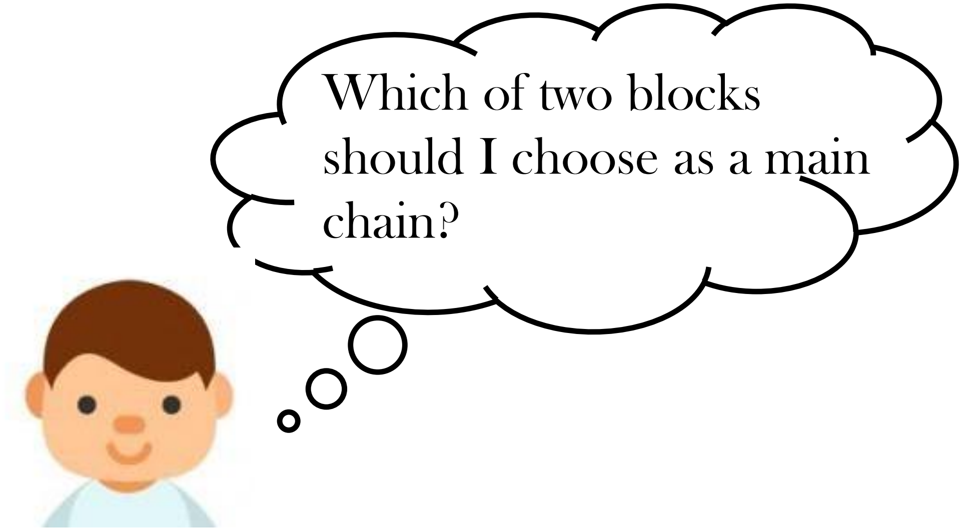
Selfish Mining

❖ Forks

– Due to the nonzero block propagation delay, nodes can have different views.

– When a fork occurs, only one block becomes valid.





Selfish Mining

- Generate intentional forks adaptively.
  - An attacker finds a valid block and propagates the block **when another block is found by an honest node.**

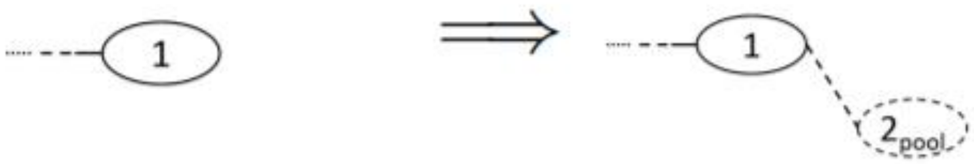
- Force the honest miners into wasting victims' computations on the stale public branch.

Strategy

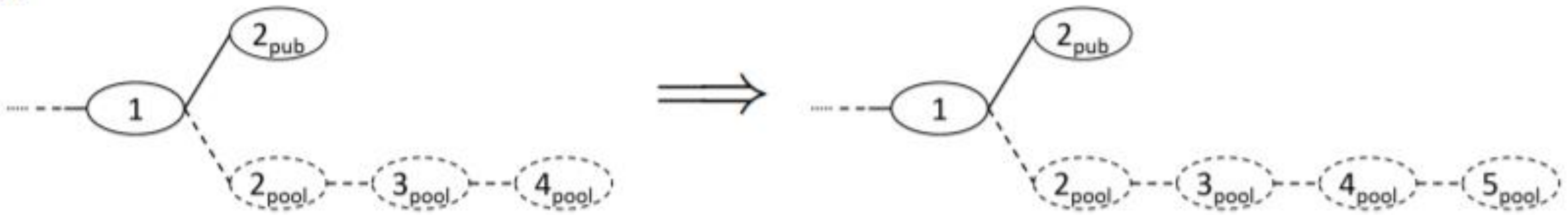
```
on My pool found a block
    Δ_prev ← length(private chain) − length(public chain)
    append new block to private chain
    privateBranchLen ← privateBranchLen + 1
    if Δ_prev = 0 and privateBranchLen = 2 then          (Was tie with branch of 1)
        publish all of the private chain                 (Pool wins due to the lead of 1)
        privateBranchLen ← 0
    Mine at the new head of the private chain.

on Others found a block
    Δ_prev ← length(private chain) − length(public chain)
    append new block to public chain
    if Δ_prev = 0 then
        private chain ← public chain                      (they win)
        privateBranchLen ← 0
    else if Δ_prev = 1 then
        publish last block of the private chain           (Now same length. Try our luck)
    else if Δ_prev = 2 then
        publish all of the private chain                  (Pool wins due to the lead of 1)
        privateBranchLen ← 0
    else                                                  (Δ_prev > 2)
        publish first unpublished block in private block.
    Mine at the head of the private chain.
```

Strategy

(a) *Any state but two branches of length 1, pools finds a block.* The pool appends one block to its private branch, increasing its lead on the public branch by one. The revenue from this block will be determined later.

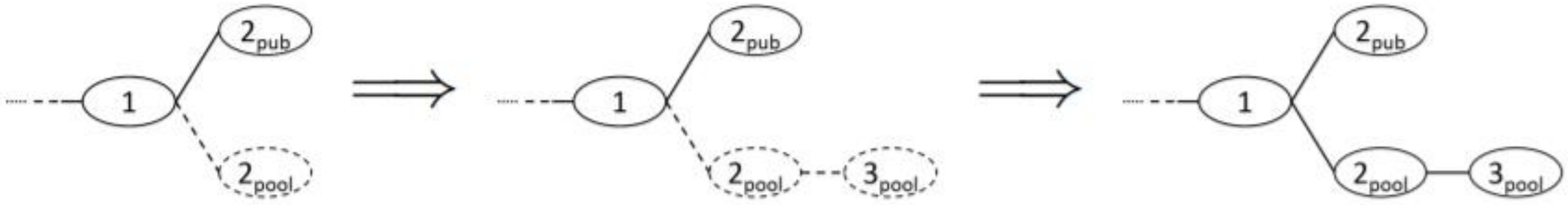


or

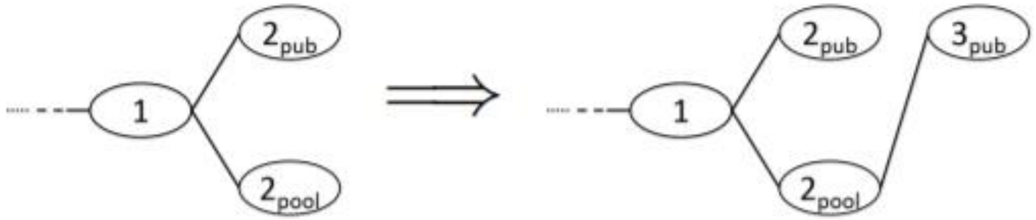


Strategy

(b) *Was two branches of length 1, pools finds a block.* The pool publishes its secret branch of length two, thus obtaining a revenue of two.



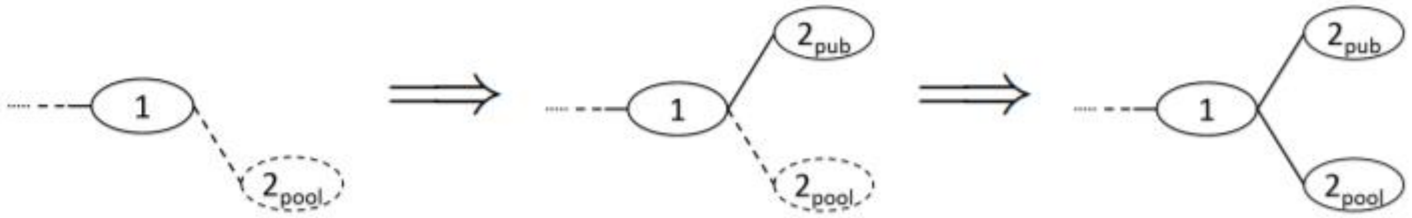
(c) *Was two branches of length 1, others find a block after pool head.* The pool and the others obtain a revenue of one each — the others for the new head, the pool for its predecessor.



Strategy

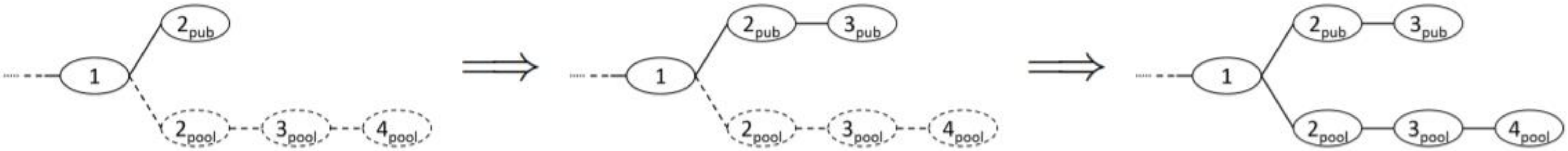
(f) *Lead was 1, others find a block.* Now there are two branches of length one, and the pool publishes its single secret block. The pool tries to mine on its previously private head, and the others split between the two heads. Denote by γ the ratio of others that choose the non-pool block.

The revenue from this block cannot be determined yet, because it depends on which branch will win. It will be counted later.



Strategy

(g) *Lead was 2, others find a block.* The others almost close the gap as the lead drops to 1. The pool publishes its secret blocks, causing everybody to start mining at the head of the previously private branch, since it is longer. The pool obtains a revenue of two.



SysSec
System Security Lab

Analysis

❖ The states of the system represent the lead of the selfish pool; that is, the difference between the number of unpublished blocks in the pool's private branch and the length of the public branch.

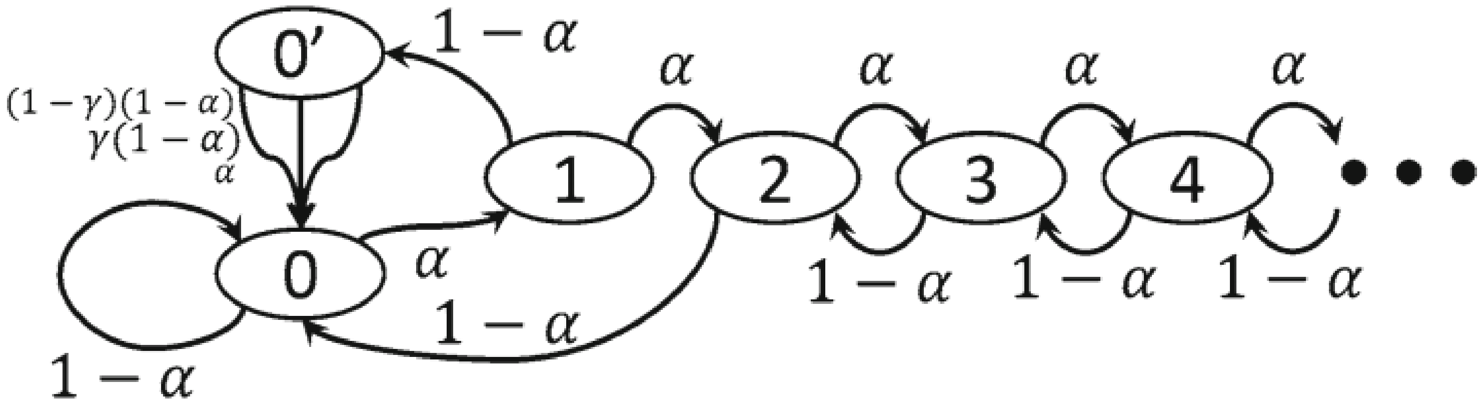


Fig. 1. State machine with transition frequencies.

State Probabilities

$$\begin{cases} \alpha p_0 = (1-\alpha)p_1 + (1-\alpha)p_2 \\ p_{0'} = (1-\alpha)p_1 \\ \alpha p_1 = (1-\alpha)p_2 \\ \forall k \geq 2 : \alpha p_k = (1-\alpha)p_{k+1} \\ \sum_{k=0}^{\infty} p_k + p_{0'} = 1 \end{cases}$$

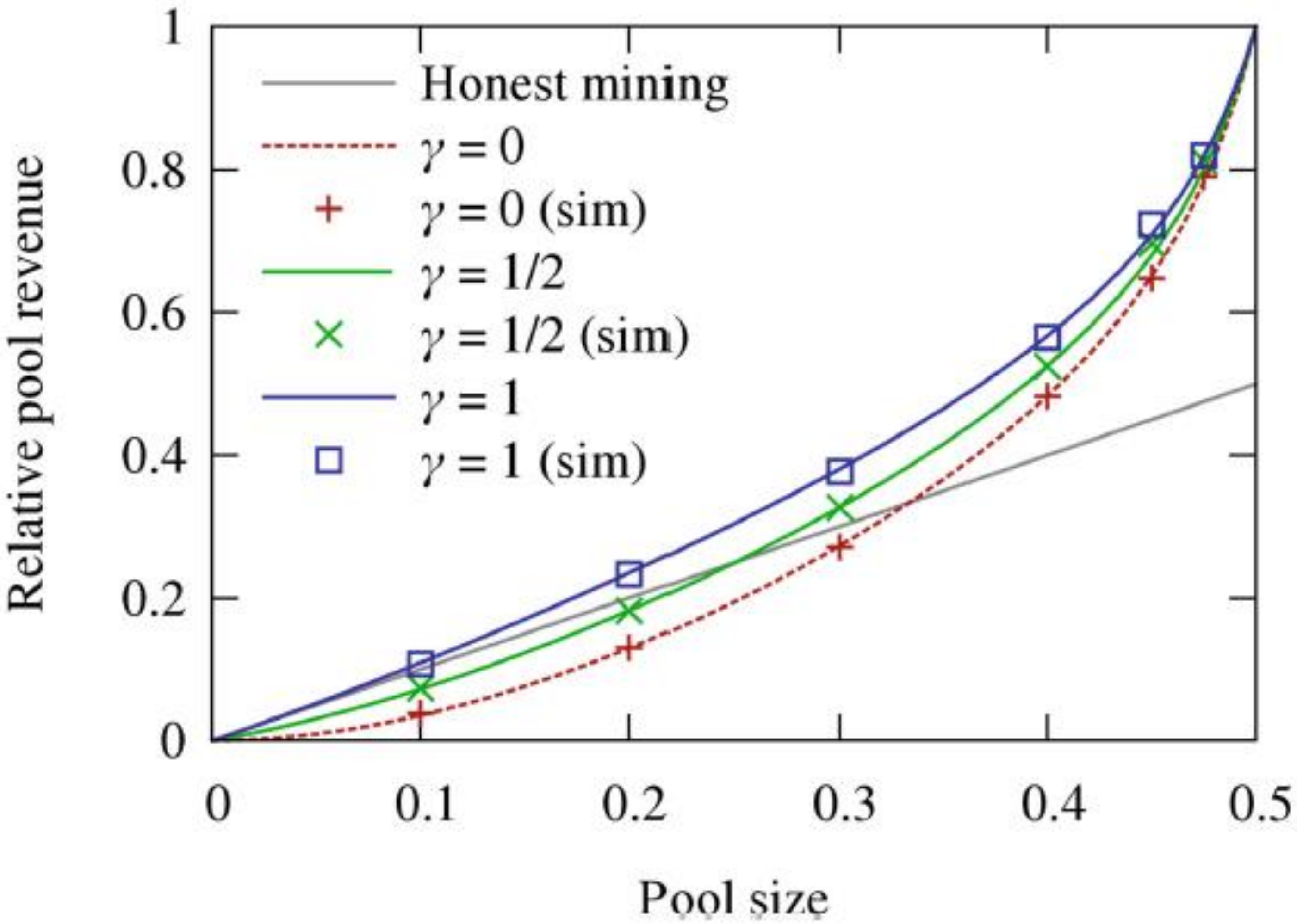
$$p_0 = \frac{\alpha - 2\alpha^2}{\alpha(2\alpha^3 - 4\alpha^2 + 1)}$$

$$p_{0'} = \frac{(1-\alpha)(\alpha - 2\alpha^2)}{1 - 4\alpha^2 + 2\alpha^3}$$

$$p_1 = \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1}$$

$$\forall k \geq 2 : p_k = \left(\frac{\alpha}{1-\alpha}\right)^{k-1} \frac{\alpha - 2\alpha^2}{2\alpha^3 - 4\alpha^2 + 1}$$

Simulation



- ❖ γ: An attacker's network capability
- ❖ When an attacker possesses more than 33% computational power, the attacker can always earn extra rewards.

Observation

Observation 1 *For a given* γ*, a pool of size* α *obtains a revenue larger than its relative size for* α *in the following range:*

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \ . \tag{9}$$

Observation 2 *For a pool running the Selfish-Mine strategy, the revenue of each pool member increases with pool size for pools larger than the threshold.*

Observation

Observation 1 *For a given γ, a pool of size α obtains a revenue larger than its relative size for α in the following range:*

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \; . \tag{9}$$

Observation 2 *For a pool running the Selfish-Mine strategy, the revenue of each pool member increases with pool size for pools larger than the threshold.*

The selfish pool would therefore increase in size, unopposed by any mechanism, *towards a majority*.

Countermeasure

- When a miner learns of competing branches of the same length, it should propagate all of them, and choose which one to mine on **uniformly at random**.

➡ $\gamma = \frac{1}{2}$, Threshold= $\frac{1}{4}$

Selfish Mining

Selfish Mining

Concurrent paper

- Theoretical Bitcoin Attacks with less than Half of the Computational Power

The basic block-discarding idea, and a strategy to secretly hold new mined block, were explicitly described in 2010-old thread of Bitcoin technical discussions forum[7] including numerical results of a simplified simulation[8]. Despite the participation of influential Bitcoin developers in this forum discussion, the attack has been long forgotten, probably due to allegedly being impractical. Surprisingly, two researchers of Cornell University have recently and independently published a pre-print paper mathematically analyzing the st_1 strategy, which they call "Selfish Mining"[9].[2]

[2] Unfortunately the paper results were misleadingly propagated via the web and media[10], causing disproportionate panic among Bitcoin users.

Impractical

- The value of γ cannot be 1 because when the intentional fork occurs, the honest miner who generated a block will select his block, not that of the selfish miner.

- Honest miners can easily detect that their pool manager is a selfish mining attacker.
  - If the manager does not propagate blocks immediately when honest miners generate blocks, the honest miners will know that their pool manager is an attacker.
  - The blockchain has an abnormal shape when a selfish miner exists.

Optimal selfish mining

- ❖ Optimal selfish mining strategies in bitcoin
- ❖ Stubborn mining: Generalizing selfish mining and combining with an eclipse attack

  .....

Thank You!

Yujin Kwon
dbwls8724@kaist.ac.kr