Subversive Miners Strategies/Attacks in Bitcoin

Chen Yongxing

June 26, 2014

Outline

- Background Information
  - Bitcoin features
  - Longest Chain Rule
- Miners Strategies
  - 51% Attack
  - 25-33% Attack/ Selfish Mining
  - Block Withholding
- From Theoretical to Practice
  - Block Withholding Example
  - Ghash.IO and BetCoin

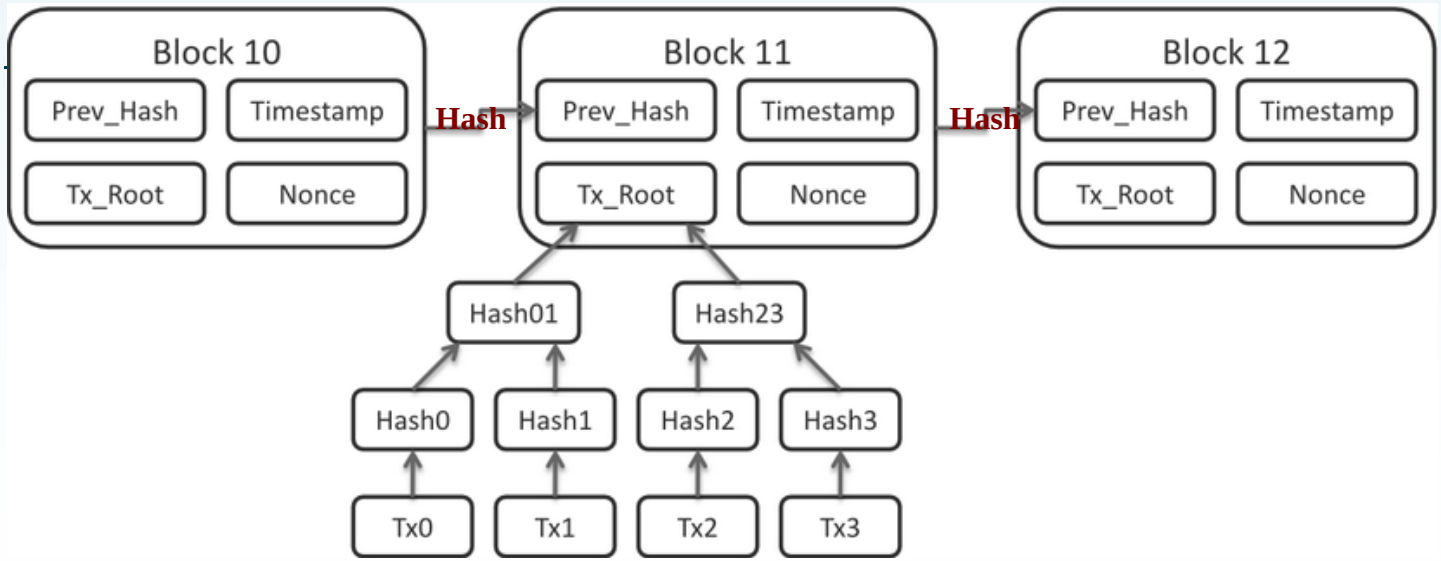
Background Information

Bitcoin System Features

- Decentralized, Distributed
  - Decentralized: No central issuing or verification authority;
  - Distributed: Purely peer-to-peer version of electronic cash
- Cryptographic Security Instead of Trust
  - Not rely on financial institutions as trusted third parties
  - Based on Block Chain: a growing general public ledger of cryptographically-signed transactions
  - Consensus-driven
    - consensus about the past history
    - consensus about the future (software spec)

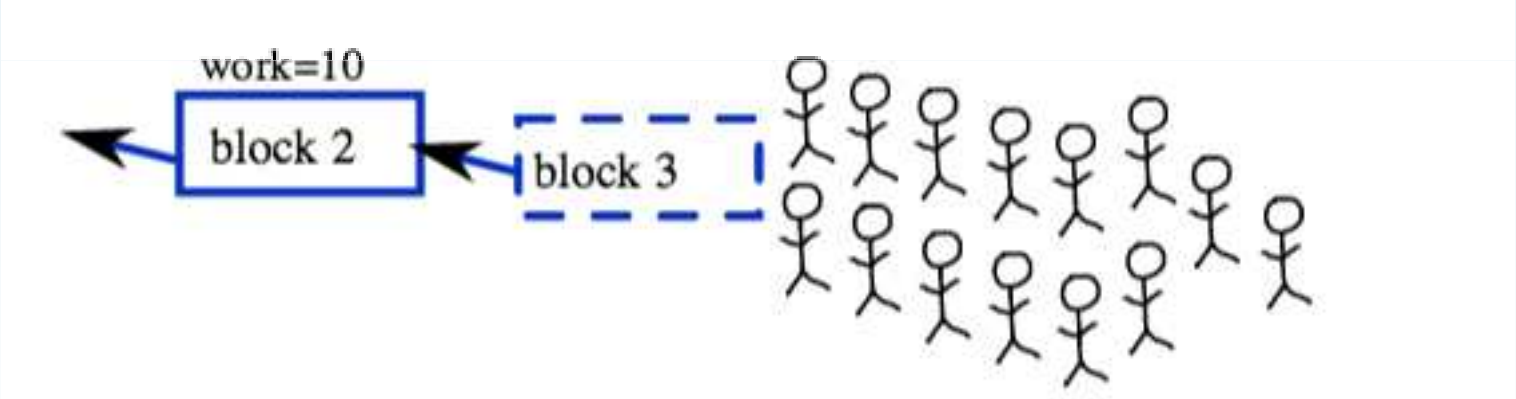
Longest Block Chain Rule - 1/4

- PoW (Proof of Work) System
  - Earning bitcoins: work (Hashing) / pay (ASICs+electricity)
  - Majority decision making: one-ASIC-one-vote
    - The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.



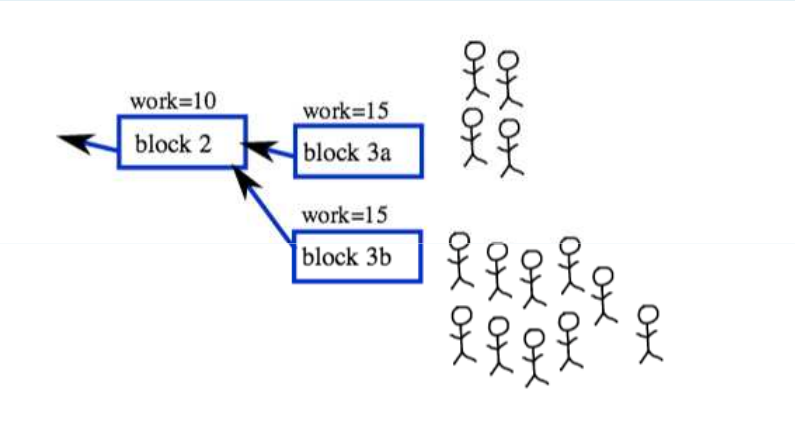
Longest Block Chain Rule - 2/4

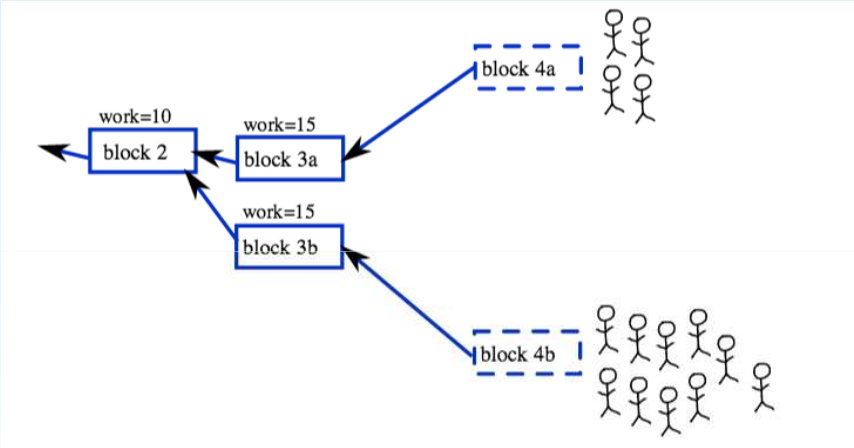
- Start with the same block

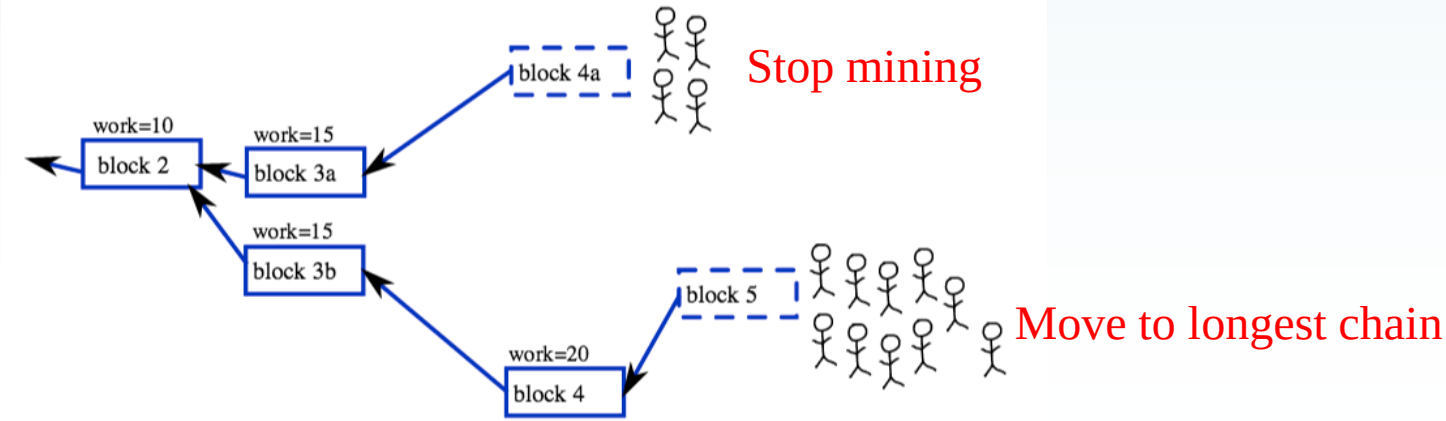


Longest Block Chain Rule - 3/4

- **Fork** – Miners Mine On Both Branches

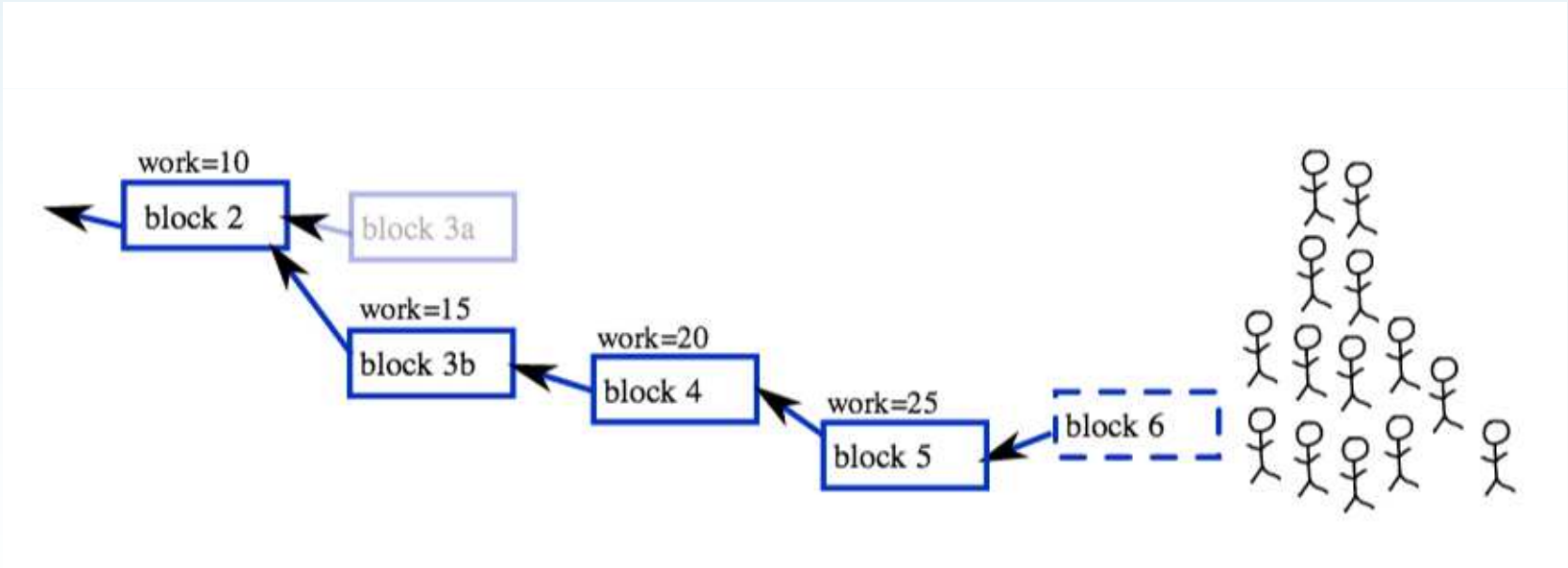






Longest Block Chain Rule - 4/4

- Longest Block Chain Rule:
  - Accept the valid block chain with most cumulative work



Miners Strategies

51% or 33% or 25%

51% Attack

- To execute a 51% attack, a coordinated group of people would need to control (at least temporarily) or influence the data entering in the double hashing process, for at least 51% of the hash power in the Bitcoin network,
- not static,
- not even a number between 0 and 100%, could be 500% of what we had at the beginning of the attack.

- Example: The Mining Cartel Attack
  - A large fraction of miners such as 51% decide to ignore some or all blocks generated by miners which are not members of the cartel.
  - Force others to join the cartel or just exclude permanently

51% Attacks

- Satoshi Nakamoto(2009):
  - "If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."
  - So Satoshi thinks that it is about a static threat by a powerful attacker!

- Dr Nicolas T. Courtois (2014):
  - Many things which we hear about 51 % attacks is really either ignorance or brain washing, highly misleading, misses the point totally, makes you look in the wrong direction.
    - Computing power can be temporarily displaced.
    - You do NOT have to be powerful to run such attack !

25 / 33% Attacks – Selfish Mining

- Paper: Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *arXiv preprint arXiv:1311.0243* (2013).

- Main Idea:

  –A group of miners can form a group that behaves as a single agent with a centralized coordinator, following the so called “selfish mining strategy”.

  –Simplified Strategy:

  - Private chain: the chain attacker keeps it secretly
  - If private chain < public chain, the attacker resets his private chain to the public chain.
  - If private chain >= public chain, attacker mines on the private chain.
  - Selfish Miners publish private chain as soon as public chain catches up.

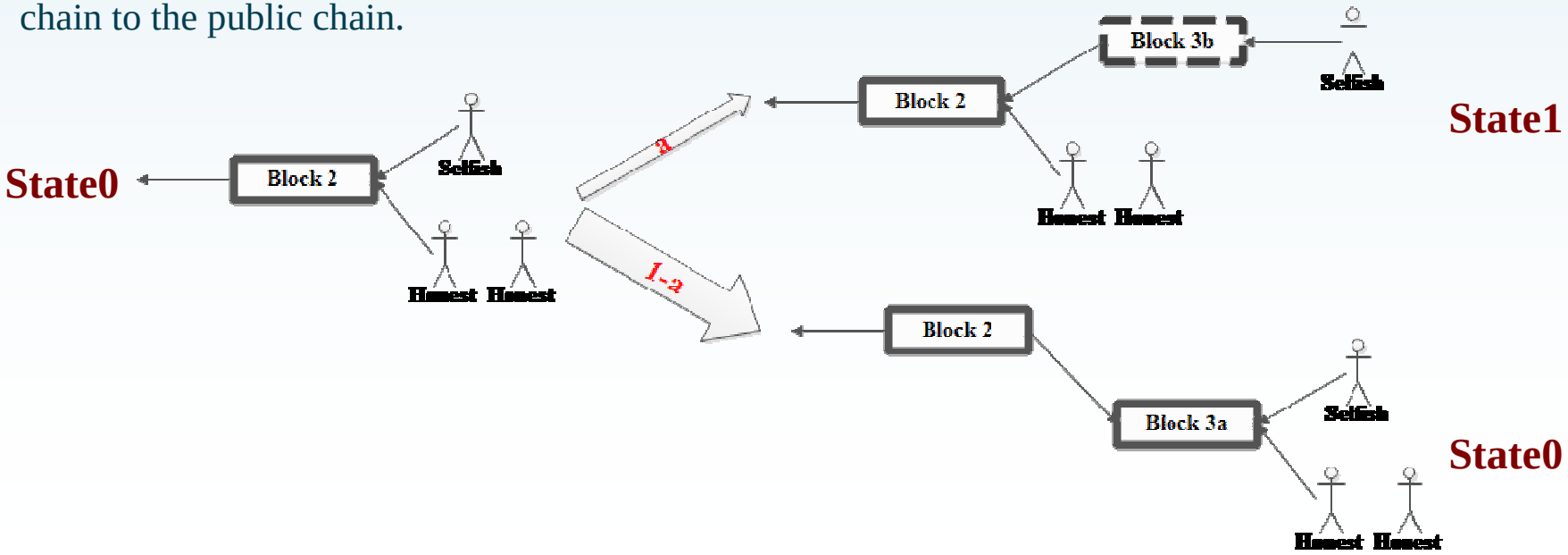
  –Key idea: Force the honest miners to waste their computations on the invalid public branch.

Selfish Mining Strategies

Assume: α; a fraction of selfish miners' mining power (<50%)

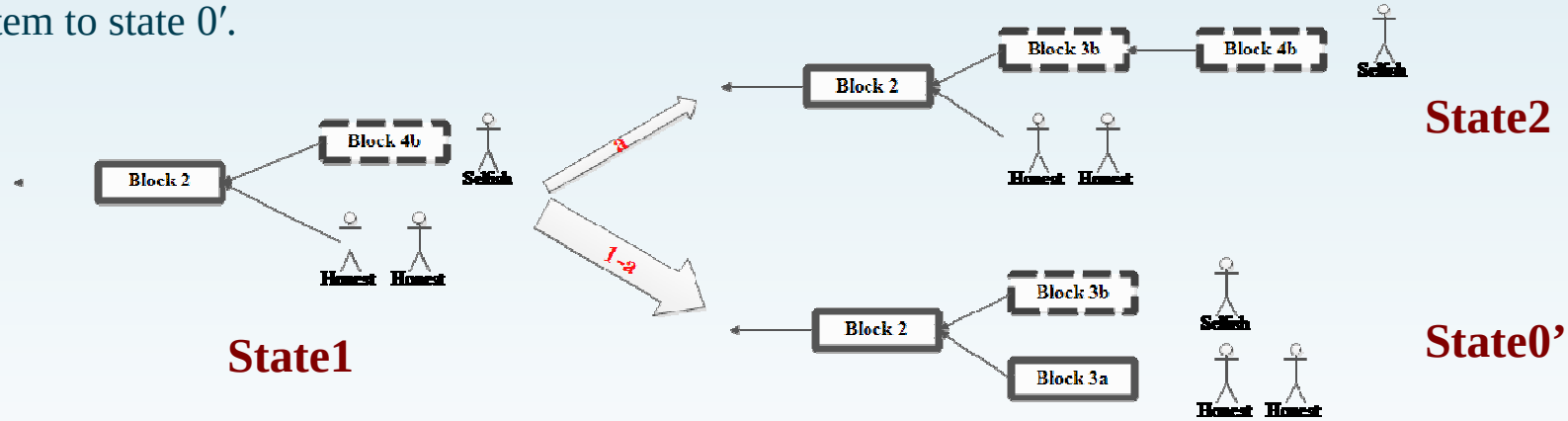
γ: Network advantage -- when there are two competing public chains the portion of the network that picks up on the attacker's chain is γ

➢State 0: the state where there are no branches, selfish miners and honest miners mine on the same block. With probability α, the attacker discovers a block switch to state 1 (private chain 1 block ahead). With probability $1-\alpha$, the public network discovers a block, and the attacker resets his private chain to the public chain.

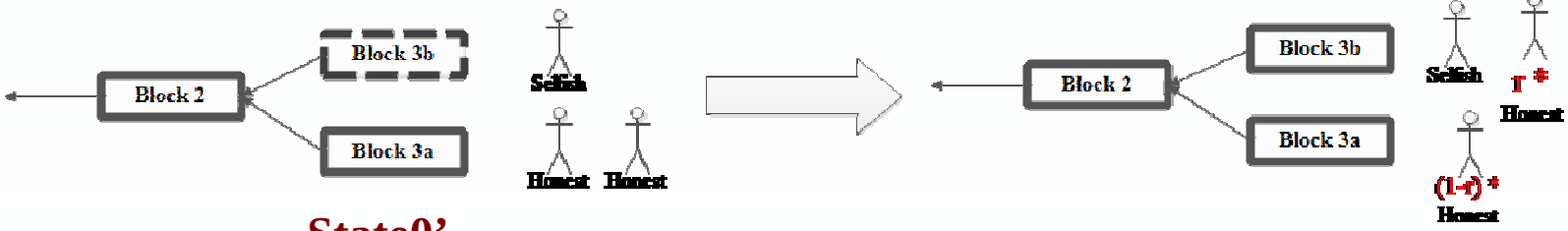


Selfish Mining Strategies

- State 1: Private chain 1 block ahead, mine on the private chain. With probability α, the attacker advances to state 2.With probability 1-α, the public network discovers a block, setting the system to state 0′.

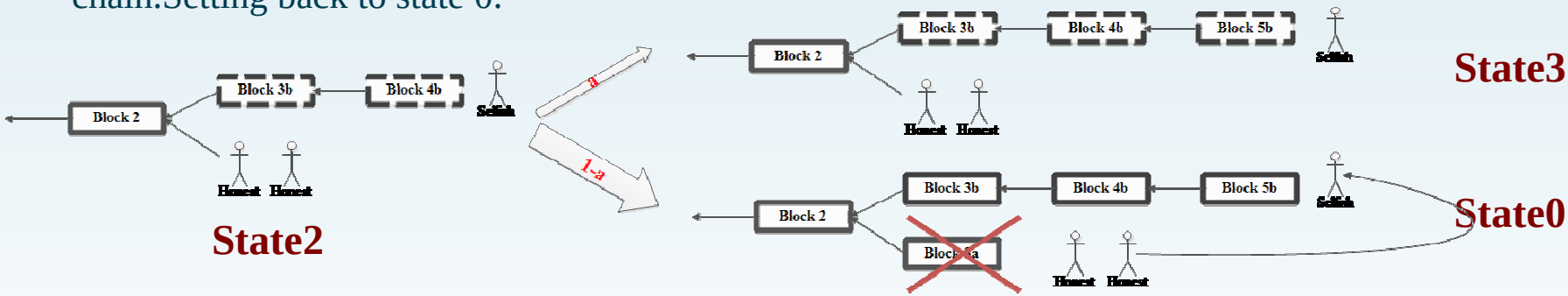


- State 0′: the state where there are two public branches of length one -- the main branch, and the branch that was private to the selfish miners, and published to match the main branch. With probability α+γ(1-α), another block will be found on attacker’s chain, causing the network to switch over to the selfish miners’ chain, and the system resets to state 0.

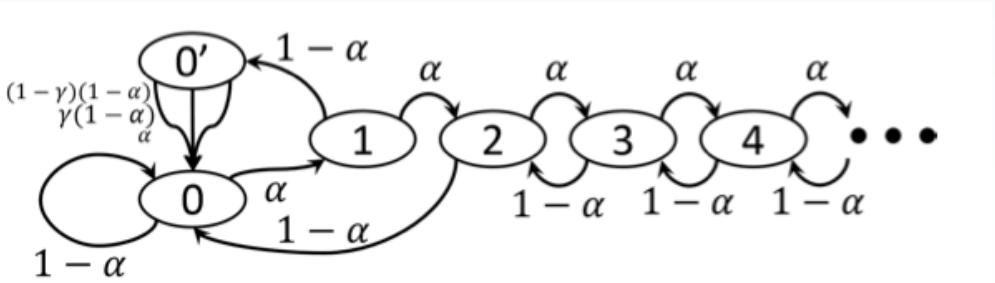


Selfish Mining Strategies

- State 2: Private chain 2 block ahead. With probability α, the attacker advances to state 3. With probability 1-α, the network finds a block, so the attacker publishes his 2-block private chain.Setting back to state 0.



- State n (n > 2): Private chain n block ahead. With probability α, the attacker advances to state n+1. With probability 1-α, the attacker falls back to state n-1.



State Transition

Selfish Mining – Revenue Analysis

- Case a: Any state but two branches of length 1, pools finds a block.
- Case b: Was two branches of length 1, pools finds a block.
- Case c: Was two branches of length 1, others find a block after pool head.
- Case d: Was two branches of length 1, others find a block after others' head.
- Case e :No private branch, others find a block.
- Case f: Lead was 1, others find a block.
- Case g: Lead was 2, others find a block.
- Case h: Lead was more than 2, others win.

$$r_{\text{others}} = \overbrace{p_{0'} \cdot \gamma(1-\alpha) \cdot 1}^{\text{Case (c)}} + \overbrace{p_{0'} \cdot (1-\gamma)(1-\alpha) \cdot 2}^{\text{Case (d)}} + \overbrace{p_0 \cdot (1-\alpha) \cdot 1}^{\text{Case (e)}}$$

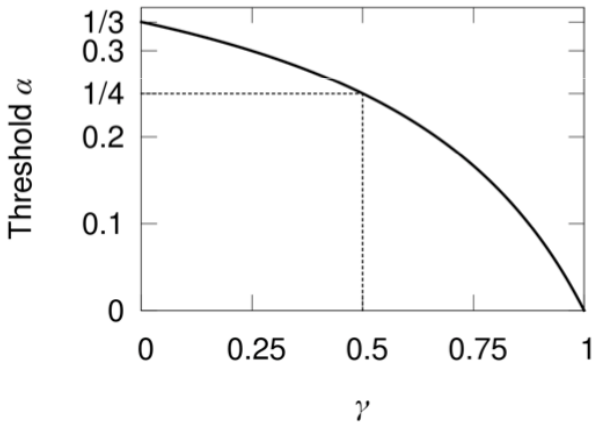
$$r_{\text{pool}} = \overbrace{p_{0'} \cdot \alpha \cdot 2}^{\text{Case (b)}} + \overbrace{p_{0'} \cdot \gamma(1-\alpha) \cdot 1}^{\text{Case (c)}} + \overbrace{p_2 \cdot (1-\alpha) \cdot 2}^{\text{Case (g)}} + \overbrace{P[i>2](1-\alpha) \cdot 1}^{\text{Case (h)}}$$

Selfish Mining – Conclusion

$$R_{\text{pool}} = \frac{r_{\text{pool}}}{r_{\text{pool}} + r_{\text{others}}} = \cdots = \frac{\alpha(1-\alpha)^2(4\alpha + \gamma(1-2\alpha)) - \alpha^3}{1 - \alpha(1 + (2-\alpha)\alpha)}$$

$R_{pool} > \alpha$

➔ $\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2}$



- Authors' Patching: Fixing the Bitcoin Protocol
  - Current Bitcoin protocol has $\gamma \to 1$, and therefore a threshold of almost zero.
  - Sets γ to 1/2, and therefore the threshold to 1/4.

Selfish Mining Statements

- There is only one selfish mining group.
  - Dr Nicolas T. Courtois : Only one selfish mining group is not realistic
    - Several competing subversive groups of equal size might be competing against each other and this will likely decrease the benefits of each other's benefits.
  - ED Felten: Selfish mining group is not stable
    - A fair-weather miner pretends to be part of the team of selfish miners, but in fact secretly switches teams so that mines for the selfish mining team if that team is ahead in the race, otherwise mines on public chain.

Selfish Mining Statements

- Selfish Mining is hard to detect.
  - Nicholas Weaver: can be detected by timestamp.
    - Other pool servers look at the delta between the block's timestamp and when it arrived, and use the shortest delta between block timestamp and arrival when two blocks arrive in close succession,
    - so one CAN with very high probability rejecting the selfish block.

- Same incentive mechanisms
  - Vitalik Buterin: theoretical attack
    - In practice, most Bitcoin miners act selflessly to support the network(--), both out of ideological considerations and because they do not want to destabilize the source of their own revenue.

Block Withholding Attack

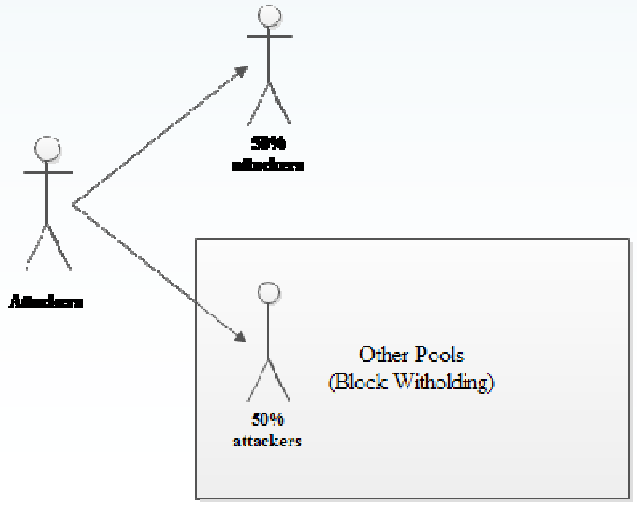
- Paper: Courtois, Nicolas T., and Lear Bahack. "On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency." *arXiv preprint arXiv:1402.1718* (2014).

- Initial version: A pool member decreases the pool revenue by never publishing blocks it finds.
  - Gained nothing: everybody lost

- Improved version: Courtois&Bahack Jan. 2014
  - They show that this attack cannot be detected, not even in theory.
  - They show that for very large pools, it will be visible, but nobody can say who is responsible!

Block Withholding Attack

- Strategies: Can be applied by any miner or group, with any fraction of hash power, split 50-50.
  - 50 % of subversive miners join other pools in a distributed way, then withhold blocks they mined
  - 50 % mine solo normally (or in other pools).
    - They show that in paper: 50-50 split maximizes the gain.



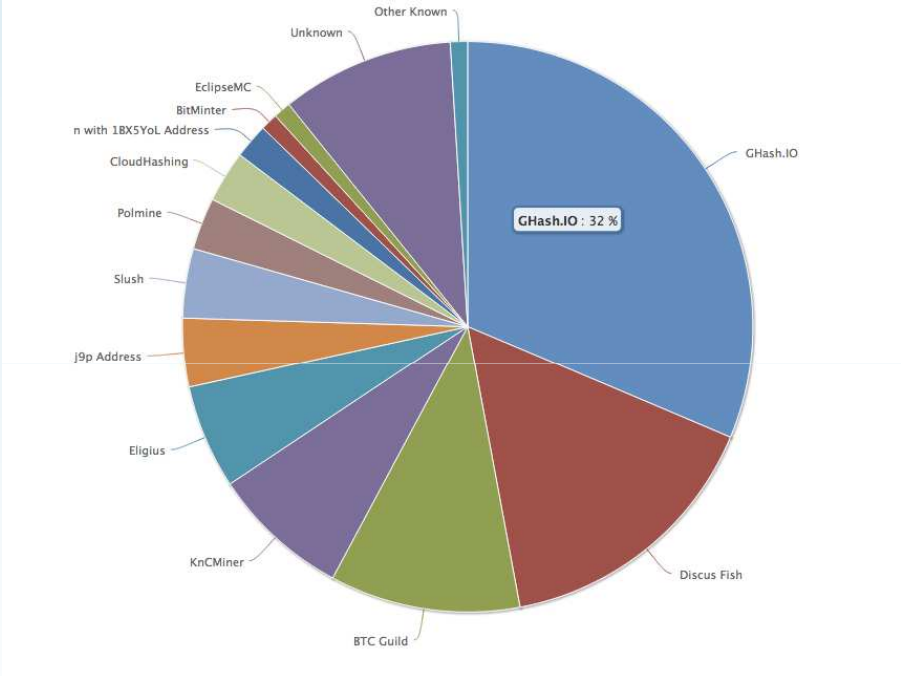
Will the theoretical attacks put into practice?

Breaking News

- A large-scale block-withholding attack was executed against the mining pool Eligius
  - https://bitcointalk.org/?topic=441465.msg7282674
  - Losses are very substantial and were estimated to be about 300 BTC - at the expense of honest miners
  - Cornell researchers "the attacker doesn't gain anything from this behavior, either; it's purely destructive ".
    - If this attack follow Nicolas et al. strategy, attackers had extra profits should be like half of the other people lose!
    - Otherwise, it maybe purely destructive action to force miners to leave this pool.

GHash.IO

- Largest: GHash.IO
  - Usually Between 30 - 40%
  - Sometimes more than 55%



- Current Situation:
  - Still accept new miners
  - BitFury Pulls 1.5PH/s of Mining Power from GHash.io

- GHash.io:
  - Public statement: They Will Never Launch a 51% Attack Against Bitcoin.

Can GHash.IO be Trusted?

- GHash.IO double-spending against BetCoin Dice
  - Post on bitcointalk (https://bitcointalk.org/index.php?topic=327767.0)
  - Time: 25th and 27th Sept. 2013
  - The mechanism: send betcoin a TX with 0 fee, then wait for a result TX, if your bet is a win, then confirm your TX, otherwise double-spend it.

  - Evidence:
    - Transaction records
    - GHash.io, being about 25% of network at that time, but they didn't find a single block between 25th and 27th of September

Thanks Listening!