DAT650 Lecture

Attacks on bitcoin mining

Leander Jehl

Attacks

51% Attack

- If the attacker owns $\alpha > 51\,\%$ of the mining power in the network, he
  - Can grow a private chain faster than the public chain.

Private chain:

Fork with blocks that are not broadcast through the network.

51% Attack

- If the attacker owns $\alpha > 51\,\%$ of the mining power in the network, he
  - Can grow a private chain faster than the public chain.

  - Attacker can:
    - Double spend
    - Get all minig rewards

Attacks

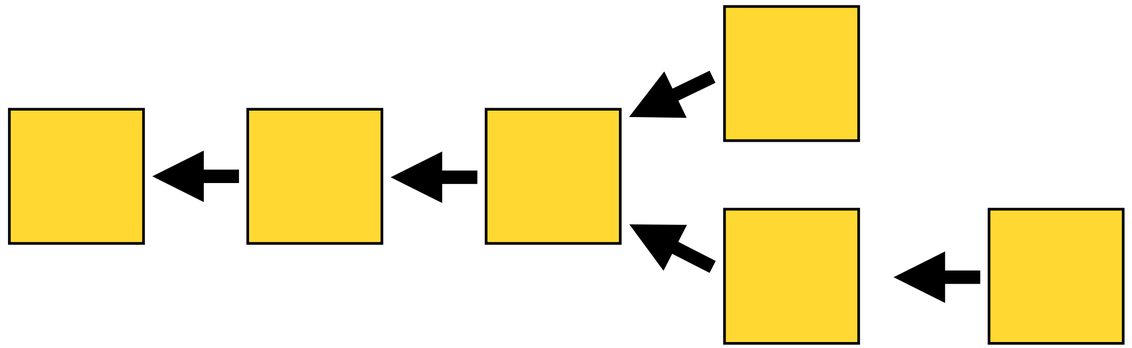
Attacks on bitcoin mining

- Longest chain rule is not enforced.

Attacks

Attacks on bitcoin mining

- Longest chain rule is not enforced.

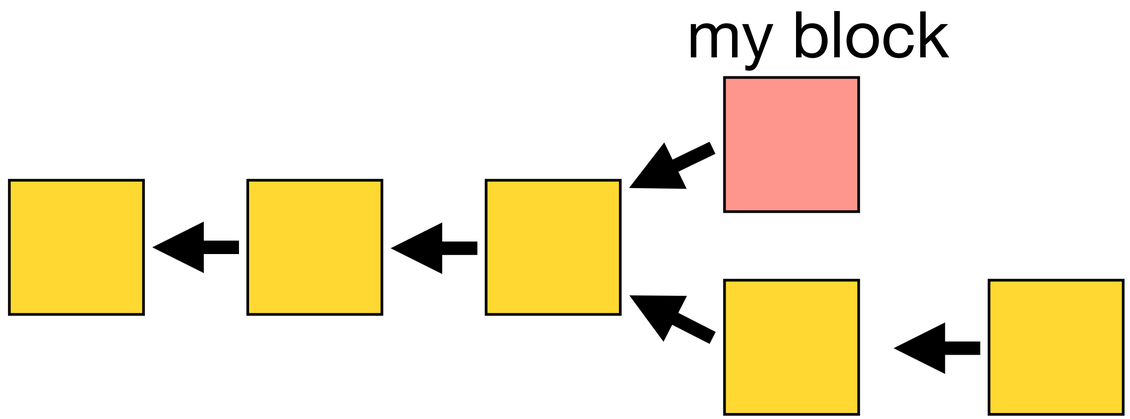


Switch to longest chain!

Attacks

Attacks on bitcoin mining

- Longest chain rule is not enforced.



Switch to longest chain!

But want to safe my block!

Stubborn mining

- Let α be the percentage of the systems mining power, that the attacker controls.
- Assume:
  - $p = \alpha$, attacker mines next block
  - $p = 1 - \alpha = \beta$, not-attacker mines next block

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

P	Outcome attack	Outcome no attack
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

P	Outcome attack	Outcome no attack
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- $p = \alpha$, attacker mines next block
- $p = 1 - \alpha = \beta$, not-attacker mines next block
- First: Run attack for the next two blocks:

Profitable if $E[\text{attack}] \geq E[\text{no attack}]$

$$3\alpha^2 + \alpha\beta \geq 2\alpha^2 + 2\alpha\beta$$

$$\alpha^2 \geq \alpha\beta$$

$$\alpha \geq 0.5$$

P	Outcome attack	Outcome no attack
$\alpha\alpha$	3	2
$\beta\beta$	0	0
$\alpha\beta$	0	1
$\beta\alpha$	1	1

Stubborn mining

- Run attack for 2 blocks: profitable for $\alpha \geq 0.5$
- Run attack for 4 blocks: profitable for $\alpha \geq 0.455$
- Run attack without early stop: profitable for $\alpha \geq 0.42$

Stubborn mining

- Running the attack forever, can be analysed using Markov models:

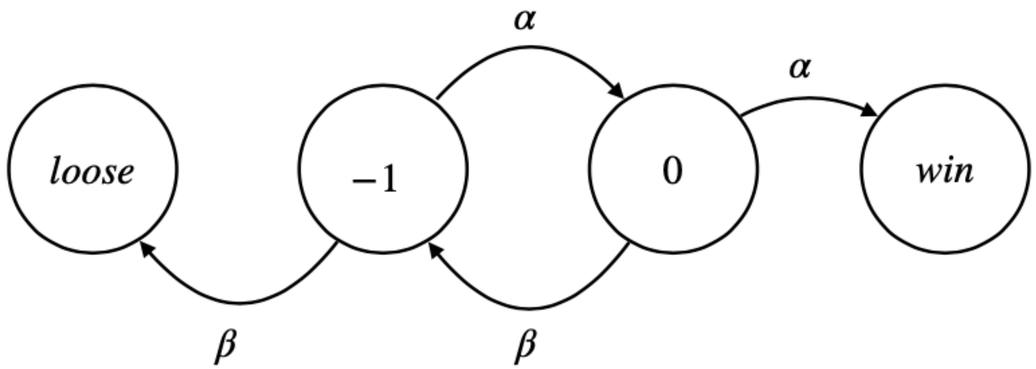


Figure 3.4: Stubborn mining states and transitions.

51% Attack

- If the attacker owns $\alpha > 51\,\%$ of the mining power in the network, he
  - Can grow a private chain faster than the public chain.

Private chain:

Fork with blocks that are not broadcast through the network.

51% Attack

- If the attacker owns $\alpha > 51\,\%$ of the mining power in the network, he
  - Can grow a private chain faster than the public chain.

  - Attacker can:
    - Double spend
    - Get all minig rewards

Selfish mining Attack

- Attacker does not violate longest chain rule
- Attacker does create secret chain

Algorithm 3 Selfish mining

Idea: Mine secretly, without immediately publishing newly found blocks
Let l_p be length of the public chain
Let l_s be length of the secret chain
if a new block b_p is published, i.e. l_p has increased by 1 **then**
    if $l_p > l_s$ **then**
        Start mining on b_p
    else if $l_p = l_s$ **then**
        Publish secretly mined block b_s
        Mine on b_s and immediately publish new block
    else if $l_p = l_s - 1$ **then**
        Push all secretly mined blocks
    end if
end if

Selfish mining

When is an attack profitable

Attack profitable if

1. Attacker gets more blocks.
2. Attacker gets a larger fraction of the blocks on the longest chain.
    - Selfish mining is profitable under the second variant.

Selfish mining

When is an attack profitable

Theorem:

Using selfish mining, the attacker receives this fraction of blocks:

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

- γ is share of honest mining power ($\beta = 1 - \alpha$) that the attacker can reach first.

Selfish mining

When is an attack profitable

- γ is the attackers networking power. $F(\alpha, \gamma)$

$$F(\alpha,0) > \alpha \text{ if } \alpha > \frac{1}{3}$$

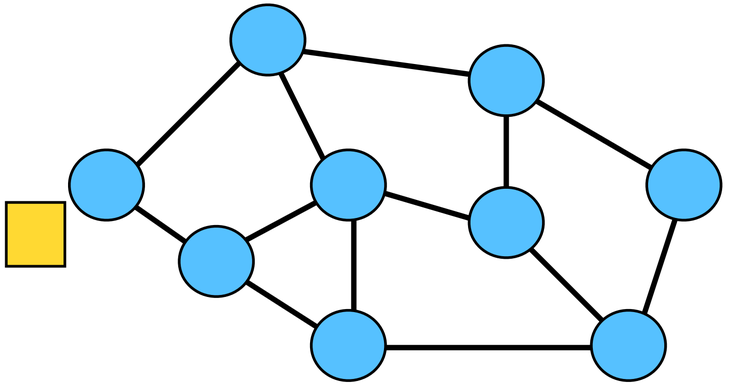
$$F(\alpha,0.5) > \alpha \text{ if } \alpha > \frac{1}{4}$$

$$F(\alpha,1) > \alpha \text{ if } \alpha > 0$$

- $\gamma = 1$ means attacker can delay any message in the network.

P2P Networking

P2P Networking



Bitcoin:

- 10.000 nodes
- each node randomly chooses 8 nodes to connect to
- nodes refuse connection when they have 128.

How can you broadcast a 1Mb block?