Attacks

Theorem

$$P[\text{fork}] = 1 - (1-p)^{\delta}$$

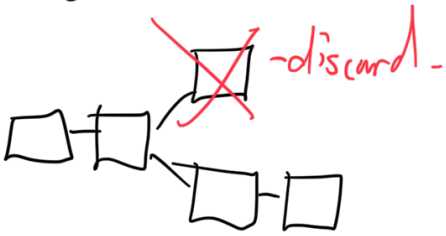
Corrolary: Length ℓ fork has

$$P[\ell\text{-fork}] \leq P[\text{fork}]^{\ell}$$

Ex1

Attacks

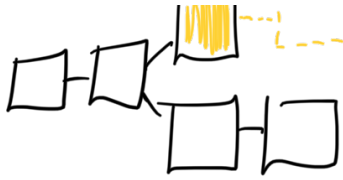
- Longest chain rule:



- Longest chain rule is not enforced.
- Attacks profitable if a Hacker has high mining power α.

Stubborn mining

- Try to extend block that is not on longest chain.



and loose reward.

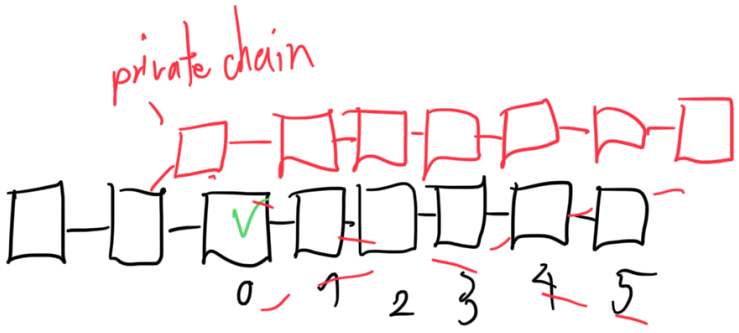
Only profitable if you have more than 42% of mining power.

51% Attack

- Work on a private chain.
- Publish when it is long enough.

Private chain:
Fork with blocks that are not broadcast through the network.

- If $\alpha > 51\%$ attacker can grow a private chain faster than the public chain.
- In 51% attack the attacker
  - can double spend
  - gets all mining rewards



discarded.

get 51% on small blockchain through mining as a service.

→ exercise

Selfish mining

- Attacker does not violate longest chain
- Attacker does keep blocks secret.

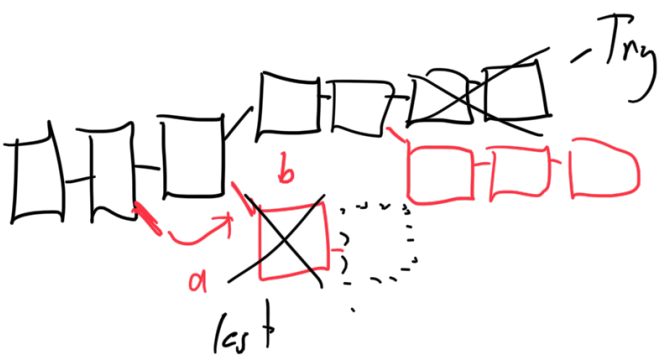
Alg:

Let l_p length of public chain
l_s length of secret chain
if block on public chain is found:
if $l_p > l_s$: work on public chain a)
if $l_p == l_s$: publish secret chain b)

and next block.

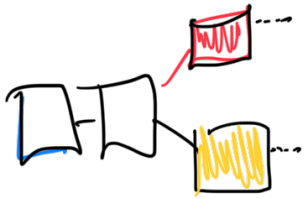
if $l_p == l_s - 1$
publish secret chain

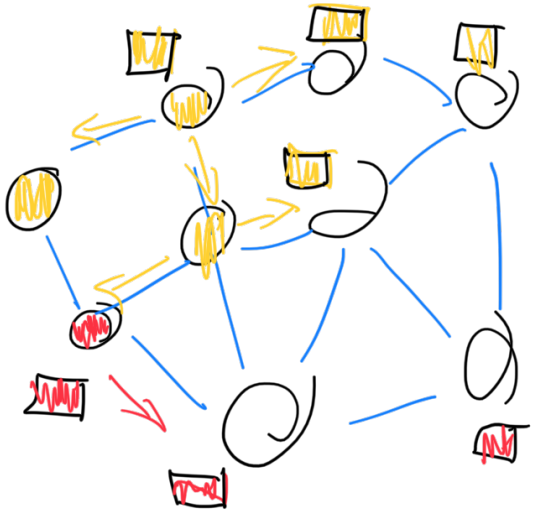
c)



Try to make public blocks discarded.

Attacker does not get more blocks, but a larger fraction of the blocks.





Attacker has network power γ:
His block reaches γ fraction of the network first.
↑ remaining

Theorem:

Selfish mining is profitable if:

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

if $\gamma = 0$ profitable if $\alpha > \frac{1}{3}$

$\gamma = 0{,}5$ " if $\alpha > \frac{1}{4}$

$\gamma = 1$ " if $\alpha > 0$

$\frac{6}{15} = \frac{2}{5}$ $\frac{10}{30} = \frac{1}{6}$