Selfish Mining

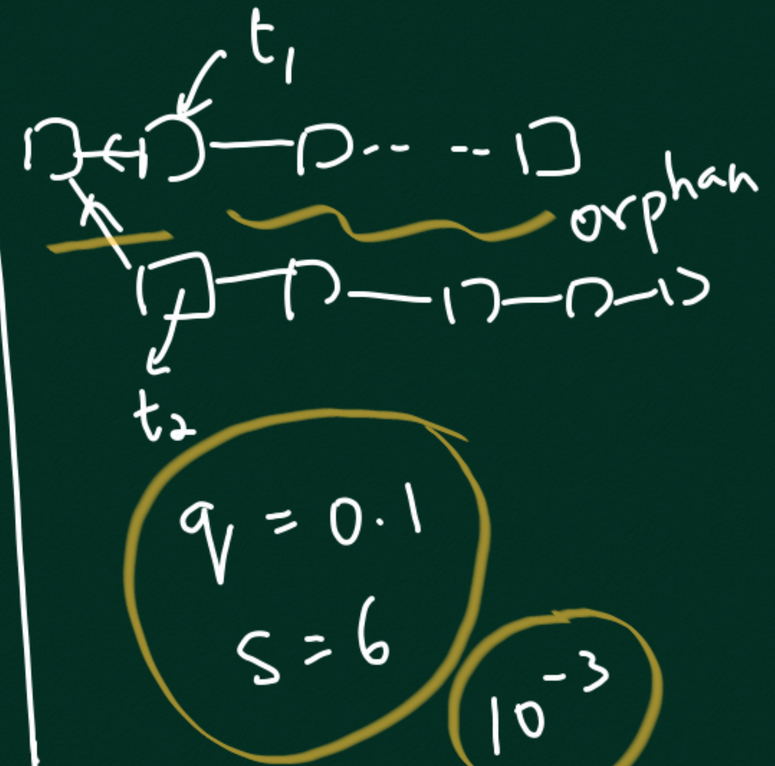
Gun Sirer et al. (Majority is not enough)

Hashing Power: α of attacker
Fraction

Honest behavior (by attacker)
: α fraction of blocks in chain

Malicious: $> \alpha$ fraction of block in chain
(under certain circumstances)

Attendance



G ← 1 ← 2 ← 3 ← 4 ← 5 ← 6 ← 7 ← 8 ← 9 ← 10 ← 11

A

A

H ← H ← H

orphaned

A ← A ← A ← A

H ← H

G

H ← H ← H

5 6 7

all orphaned

New Root

(1-γ)(1-α)

update target after 2016 blocks

Winning chain

10 11

H ← H ← H

8

one behind

H ← H ← H

new Root

A ← A ← A ← A

1 2 3 4

initial Root of attack

private

Release all blocks

new Root

9

γ(1-α)

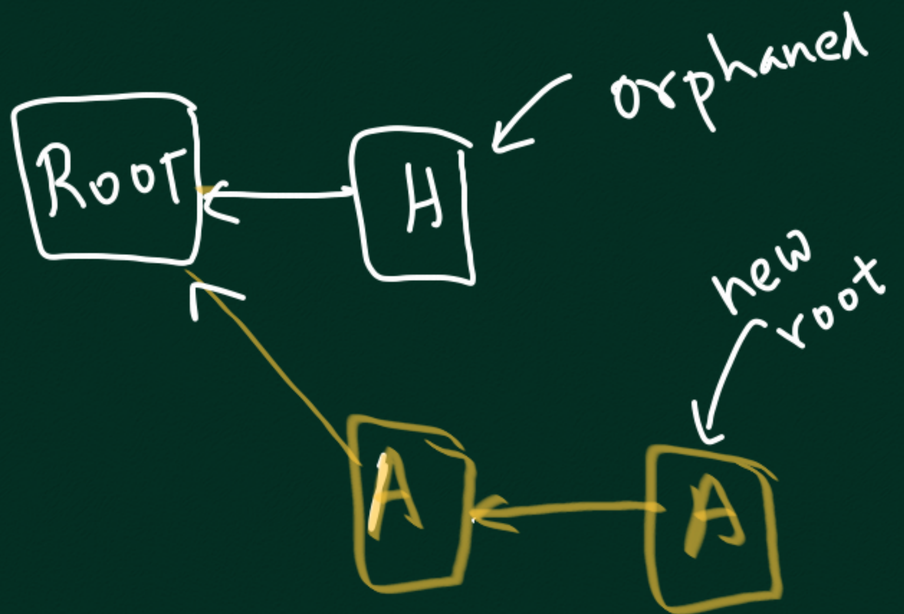
attacker (α) keeps mining

A

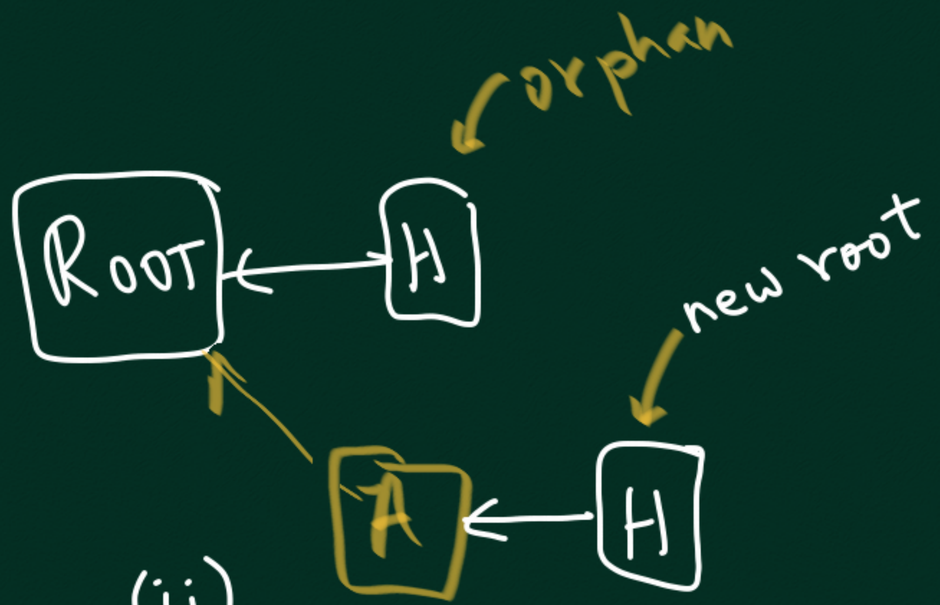
Orphaned

private

release immediately

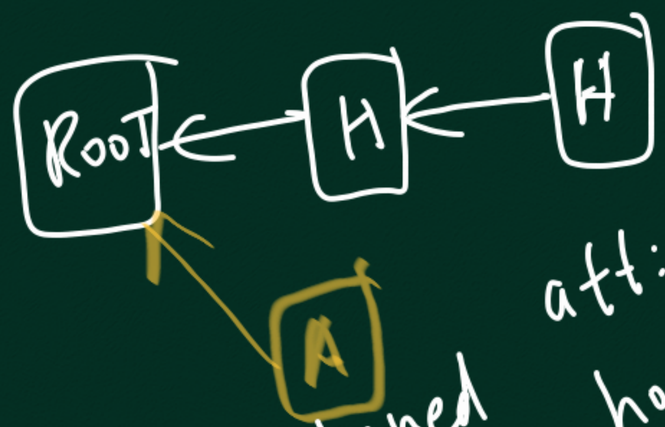


(i) aft. gets 2 blocks in chain



(ii) aft: 1 hon: 1

(iii)

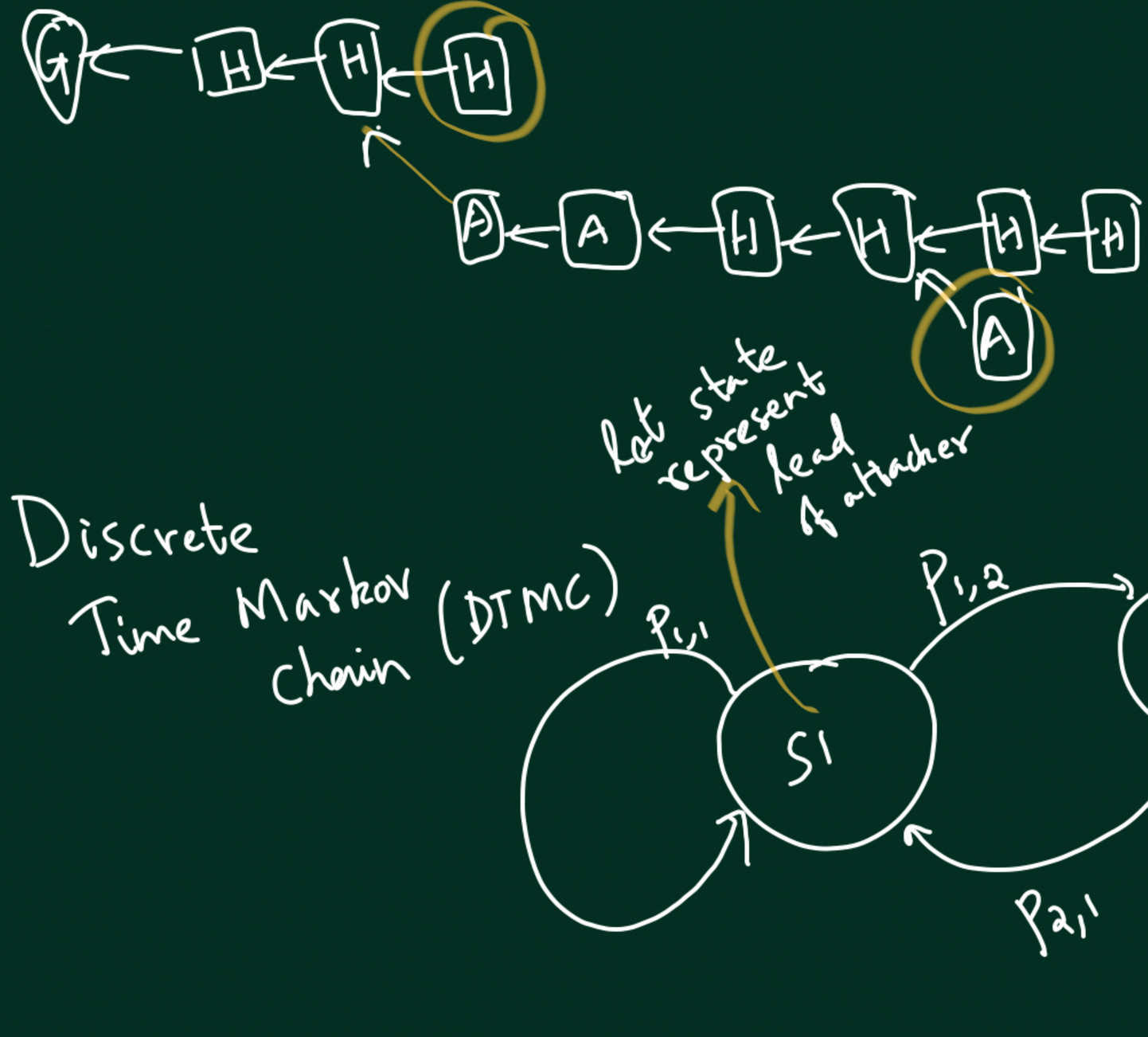


orphaned aft: 0 hon: 2

Intuition for attack: Increase fraction of Att. blks in heaviest chain to beyond α.

Note: target adjusts so that winning chain (excludes orphaned blks) has 2016 blks. every 2 weeks.

Hence attacker gets $> \alpha \cdot 2016$ blks. in winning chain every 2 weeks.


G
H
H
H
A
A
H
H
H
H
A
Let state represent head of attacker
Discrete Time Markov Chain (DTMC)
Markov Chain
S1
S2
S3
S4
S5
S6
P1,1
P1,2
P2,1
P2,3
P2,4
P2,5

DTMC: Seq. of Random Variables in which next r.v depends on value of only current variable (memoryless property)

Ex: $X_1, X_2, \ldots, X_n, X_{n+1}$

$$P_r\left[X_{n+1}=x \,\middle|\, X_1=x_1, X_2=x_2, \ldots, X_n=x_n \right] = P_r\left[X_{n+1}=x \,\middle|\, X_n=x_n \right]$$

transition prob

if $P_r\left[X_1=x_1, X_2=x_2, \ldots, X_n=x_n \right] > 0$

G H H

$R_H=1, R_A=1$

R_{root}

root

State: O^1

FELLER

A A H H H

$(1-\gamma)(1-\alpha)$

$R_H=2$

$(1-\gamma)(1-\alpha)$

O^1

$\gamma(1-\alpha)$

α $R_A=2$

$1-\alpha$

$R_A=2$ α

$R_A=1$

A

$\gamma(1-\alpha)$

α

$R_A=R_H=0$

0 1 2 3 4 5

$1-\alpha$

$1-\alpha$

$1-\alpha$

$1-\alpha$

$R_H=1$

$R_H=0;\ R_A=0$

$R_A=0;\ R_H=0$

α $R_A=1$

A H

A A A A

new root

$R_A=1$

to ∞

Procedure: 1) Calculate steady-state prob. p_i of being in state 'i'

2) Calculate avg. reward of attacker (and honest miners) per block generated in system

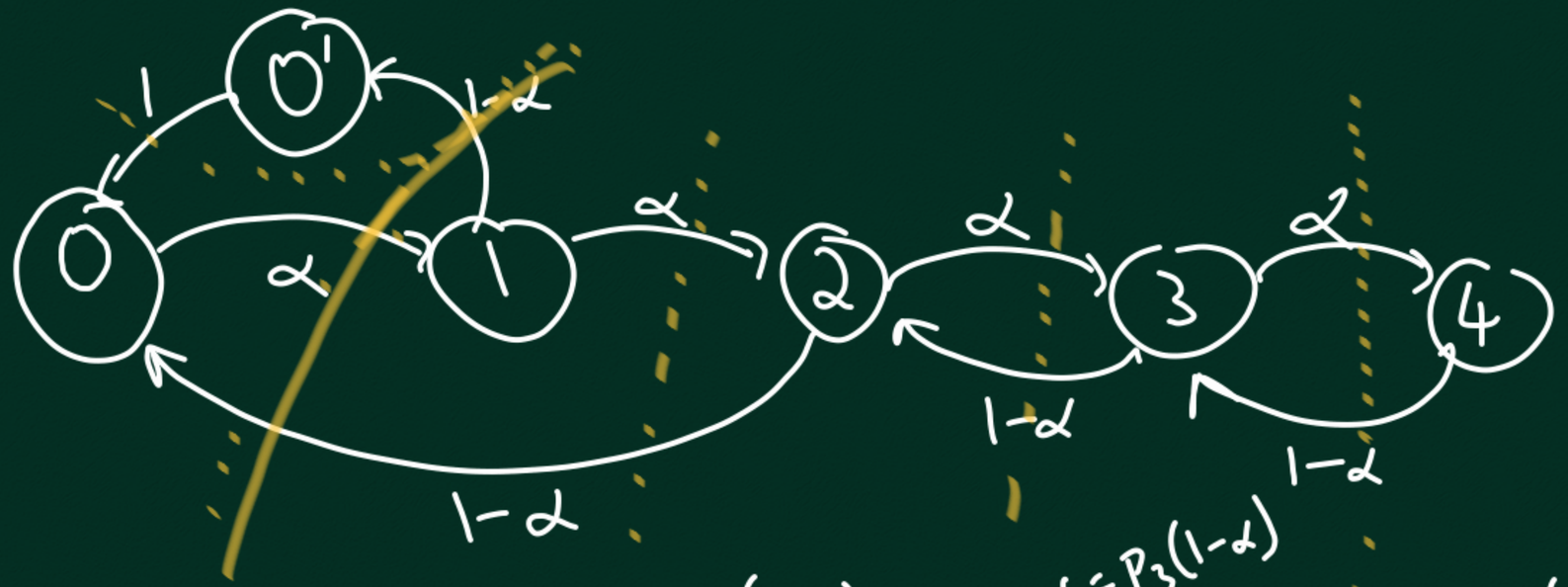
$$\text{(a Hacker)}\ r_A = \sum_i p_i \cdot \left(\sum_j p_{i,j} \cdot \left(R_A^{(i,j)} \right) \right)$$

$$r_H = \sum_i p_i \left(\sum_j p_{i,j} \left(R_H^{(i,j)} \right) \right)$$

$r_A < \alpha$

$r_H < (1-\alpha)$

3) Avg. att. blks in winning chain (excl. orphaned blks) $= \dfrac{r_A}{r_A + r_H}$ want this $> \alpha$



$p_1 \cdot \alpha = p_2(1-\alpha)$ $\quad p_2 \cdot \alpha = p_3(1-\alpha)$ $\quad p_3 \cdot \alpha = p_4(1-\alpha)$

$p_0' \cdot 1 = p_1 \cdot (1-\alpha)$

$p_0 \cdot \alpha = p_2(1-\alpha) + p_1 \cdot (1-\alpha)$

$\sum_i p_i = 1$ ↳ for all states

steady state prob. p_i means that as $n \to \infty$, prob. that when n^{th} blk is created we will be in state 'i'

Const. $C = \dfrac{\alpha - 2\alpha^2}{(2\alpha^3 - 4\alpha^2 + 1)}$

$P_0 = C/\alpha$

$P_0' = (1-\alpha)\, C$

$P_1 = C$

$k \geq 2$: $P_k = \left(\dfrac{\alpha}{1-\alpha}\right)^{k-1} \cdot C$