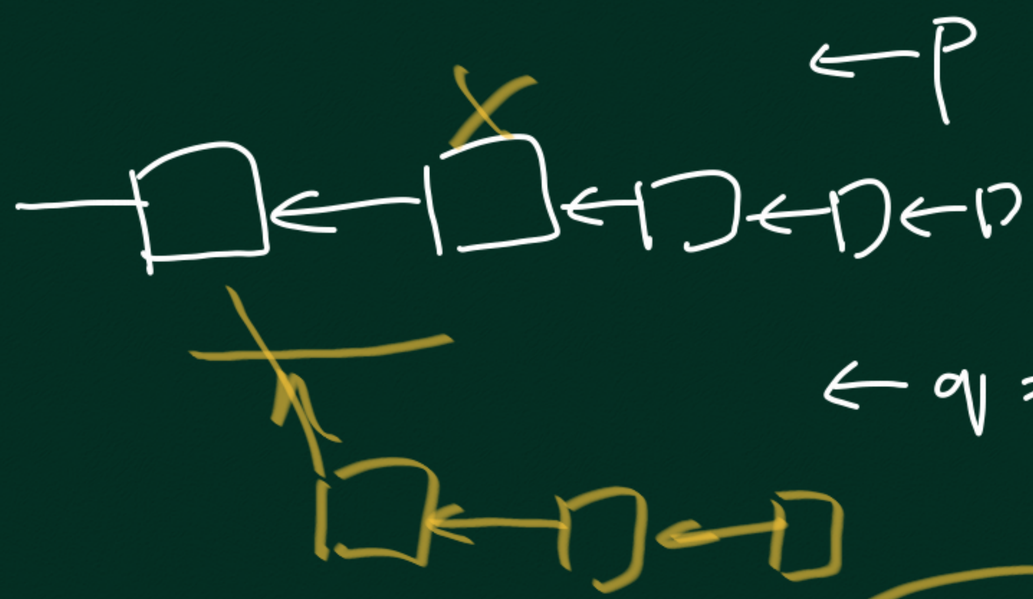
Bits (n Bits)



Attendance

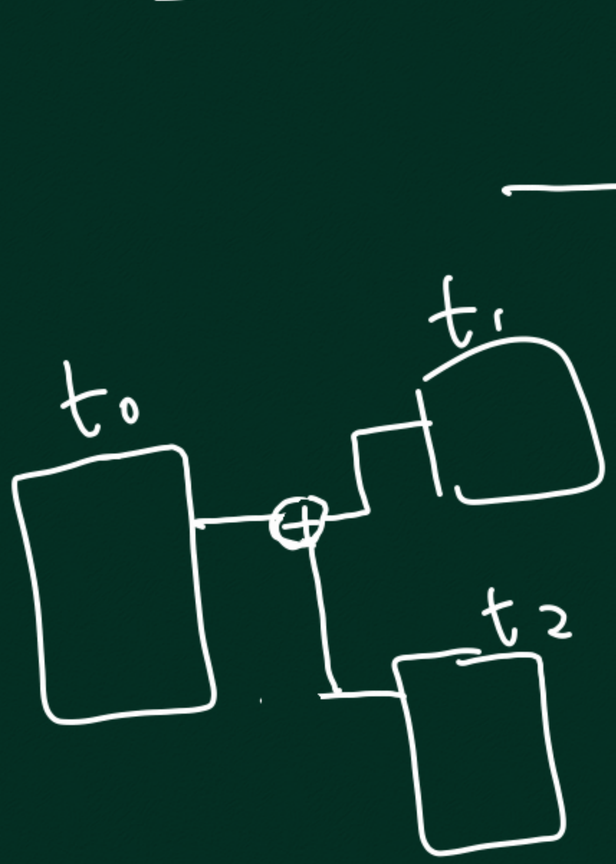
If q>p

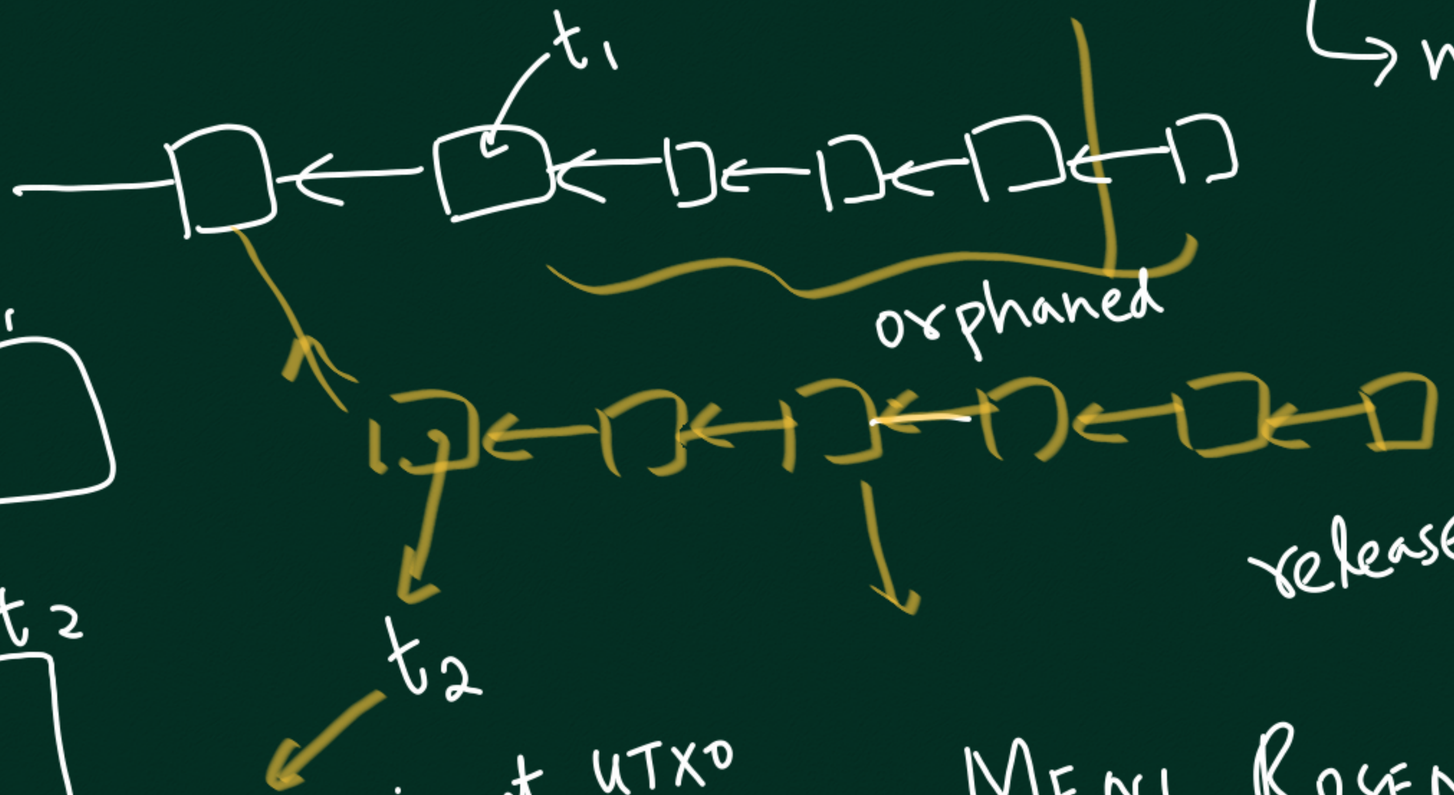
→ 51% attack

attacker has >50% hashing power

DOUBLE SPEND

Block gen. is Poisson process
↳ memoryless





release private chain

MENI ROSENFELD'S ANALYSIS

Lead in # blks of honest chain

Z

4
3
2
1

lead at time t_1

5^{th} confirmation created

honest

3 attacker blocks

P

V

1 2 3 4

prob. of hitting x-axis?

(Random Walk)

'S' confirmations

NEGLECT Network delay

(say) S=6

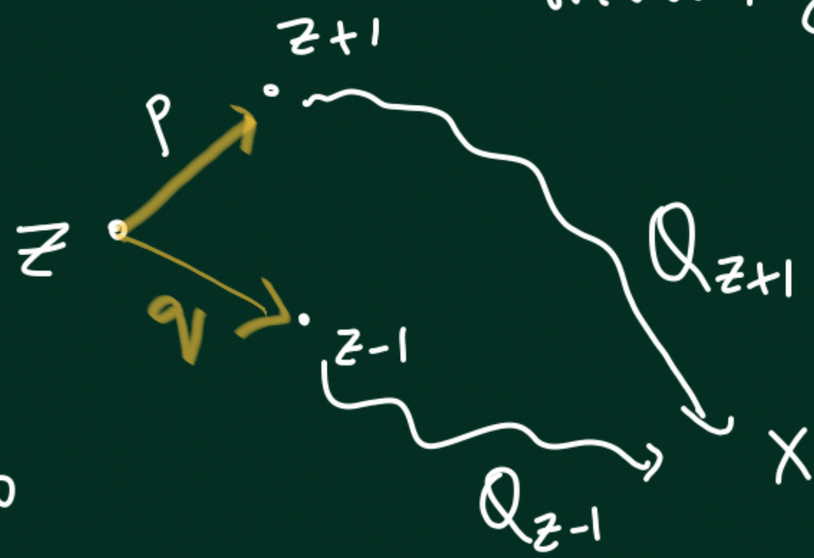
blocks generated in total after B_6

t_1 $(A \xrightarrow{3BTC} B)$

B_0 B_1 B_2 B_3 B_4 B_5 B_6

lead of 4

Q_z = Prob. of hitting X-axis if lead is initially z. (and $z>0$) (Define $Q_{z=1}$ if $z \le 0$)



$Z>0$

FELLER

$$Q_z = p \cdot Q_{z+1} + q \cdot Q_{z-1}$$

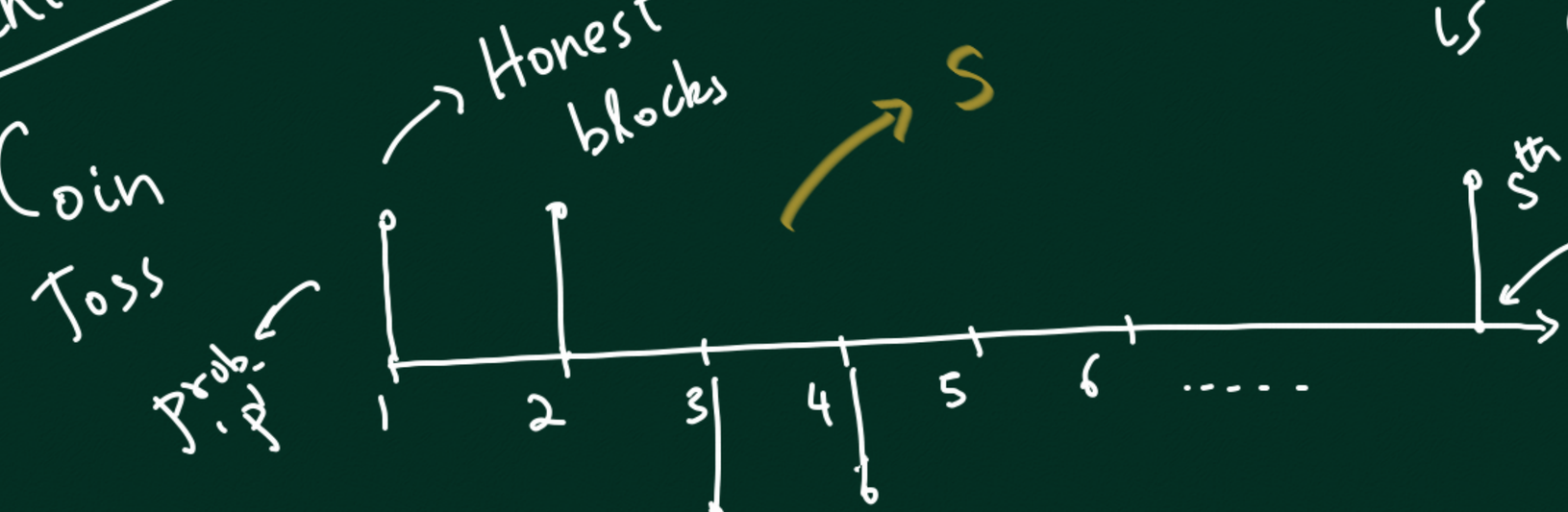
Try $Q_z = \left(\frac{q}{p}\right)^z$ (assuming $q<p$)

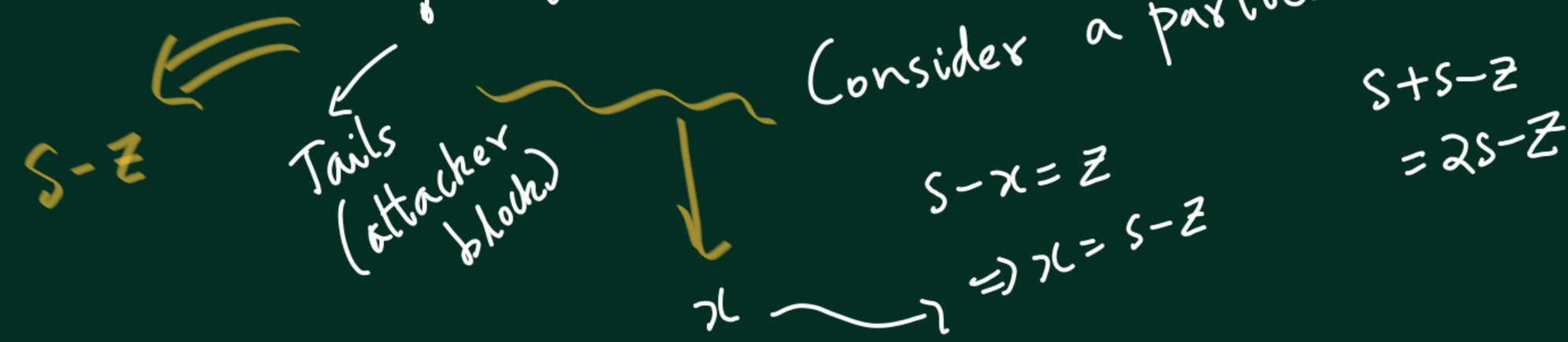
$$p \cdot \left(\frac{q}{p}\right)^{z+1} + q \left(\frac{q}{p}\right)^{z-1} = \left(\frac{q}{p}\right)^z \left[p \cdot \frac{q}{p} + q \cdot \frac{p}{q} \right]$$

$$= Q_z$$

What is prob. (P_z) that honest miners have lead of z when s^{th} confirmation is created

Meni Rosenfeld





$2s-z-1$ → $s-1$ honest

$2s-z-1$ → $s-z$ attacker

$$P_z = \binom{2s-z-1}{s-1} \cdot p^{s-1} \cdot q^{s-z} \cdot p$$

p ↓ last toss

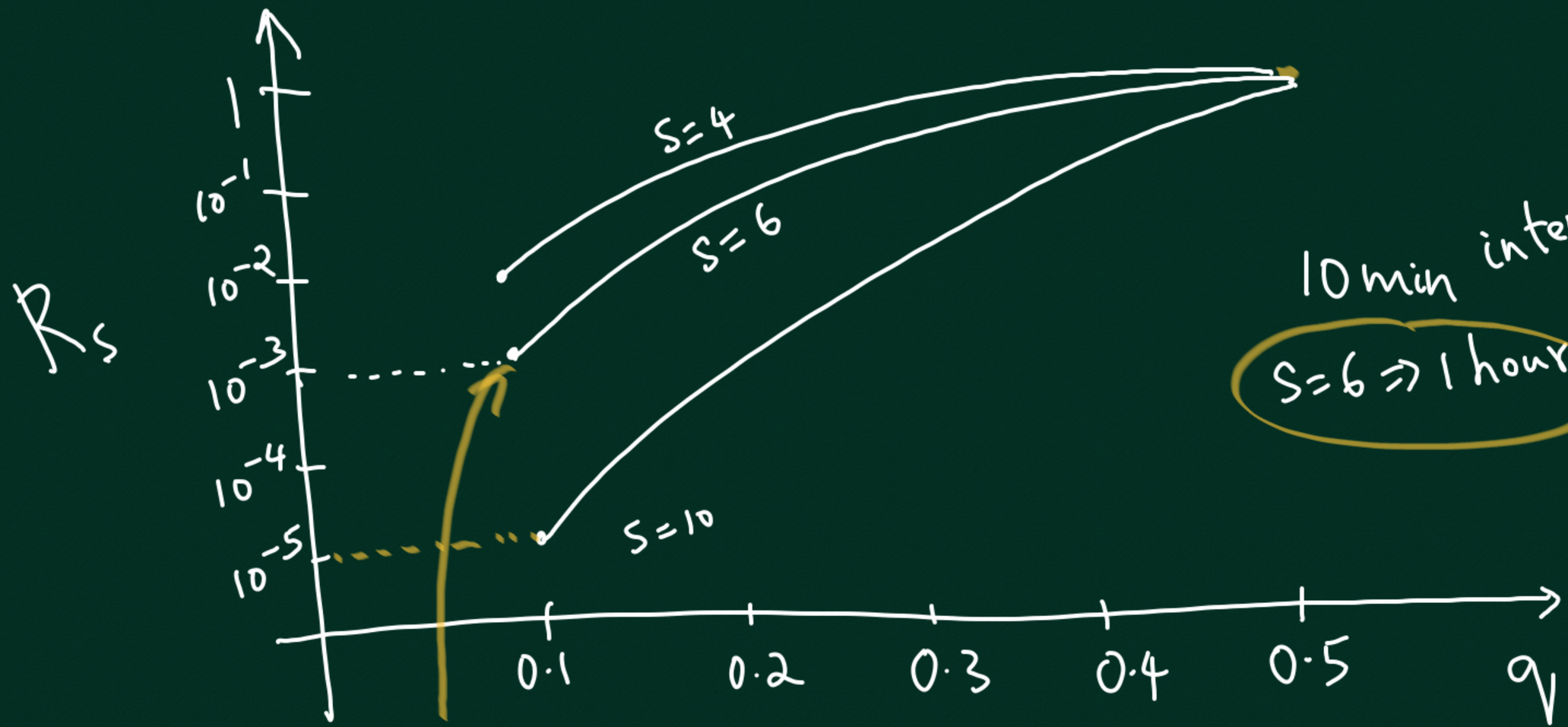
$$= \binom{2s-z-1}{s-1} p^{s} \cdot q^{s-z}$$

Prob. of Attacker releasing chain equal in length to honest chain after s^{th} confirmation

$$R_s = \sum_{z=-\infty}^{s} P_z \cdot Q_z$$

P_z: prob. initial lead is z

Q_z: prob. attacker catching up conditioned on initial lead of z



10 min inter-arrival

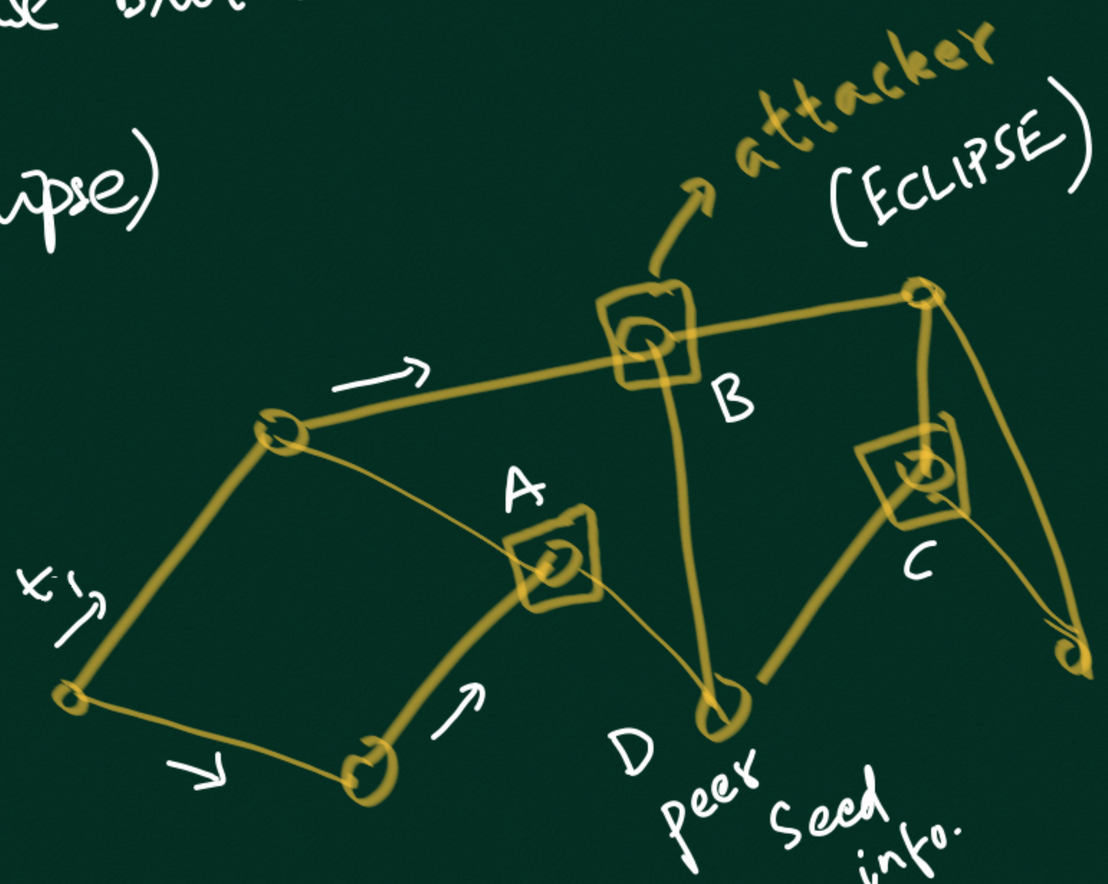
s=6 ⇒ 1 hour

s=6, q=0·1

"six confirmations are enough"

What attacks are possible?

- Private chain, release blocks later
- Network level (e.g. Eclipse)



SELFISH MINING ("Majority is not enough" — Gun Sirer et al.)

Goal: maximize fraction of attacker blocks in public chain (longest)

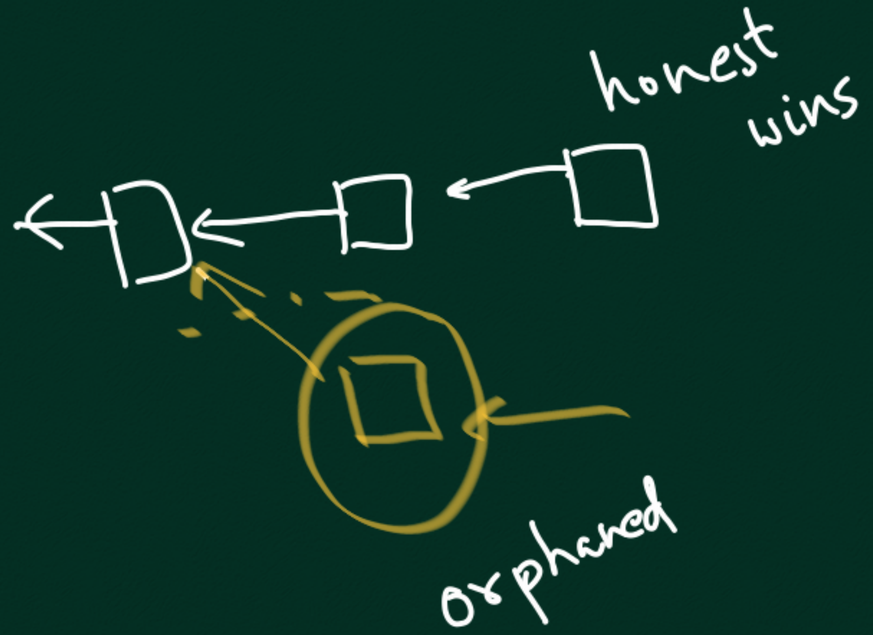
→ Avalanche

Craig ...

Leslie Lamport

'q' hashing power

want frac. of his blocks > q



HTVPZENH

YKKMAERL

HFJWTR