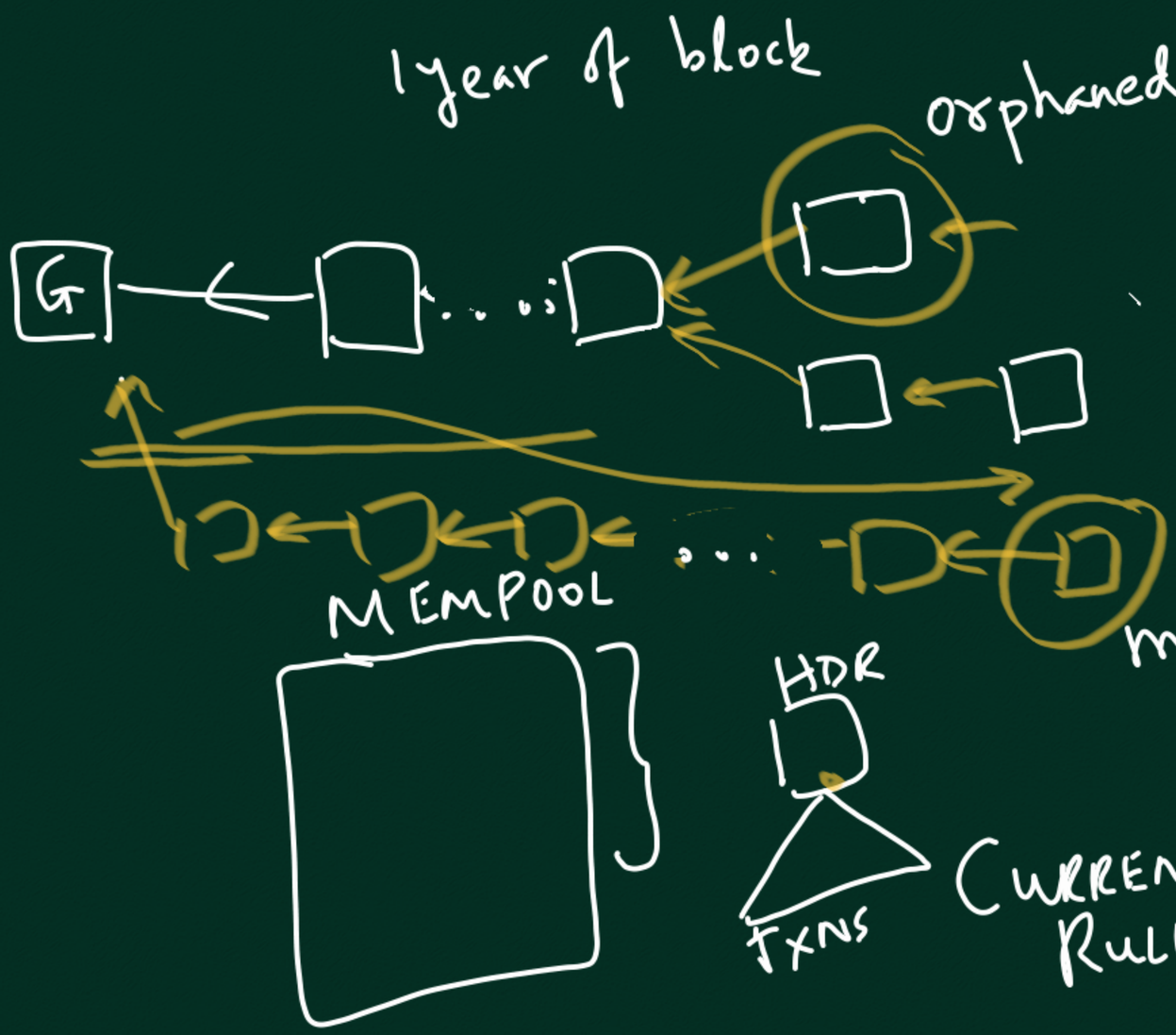
Attendance



(OLD)

Rule: Longest Chain (in #blocks)

must be extended by all miners

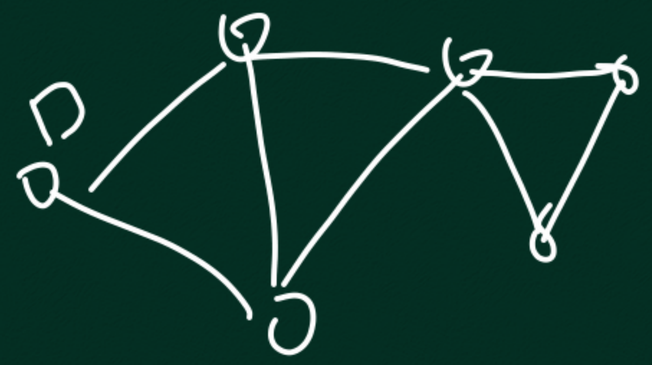
CURRENT RULE: MINE ON HEAVIEST CHAIN.

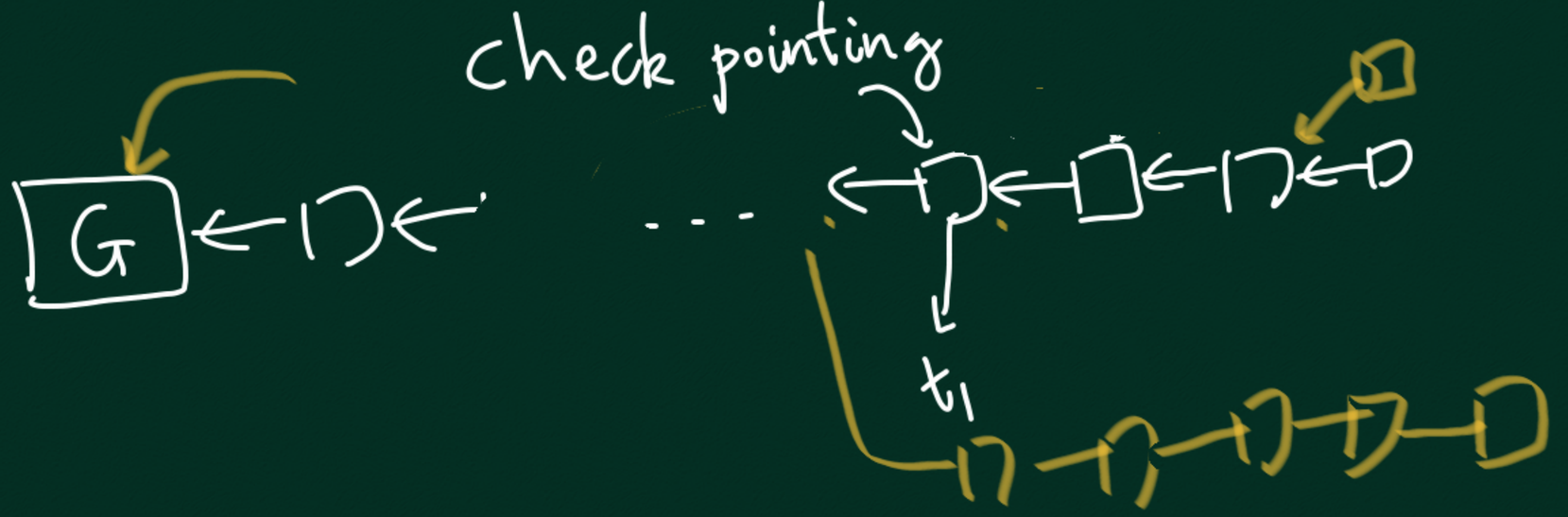
Suppose B_i has target T_i

Chain Wt = $\sum_{i=1}^{n} \frac{1}{T_i}$

of chain

of 'n' blocks

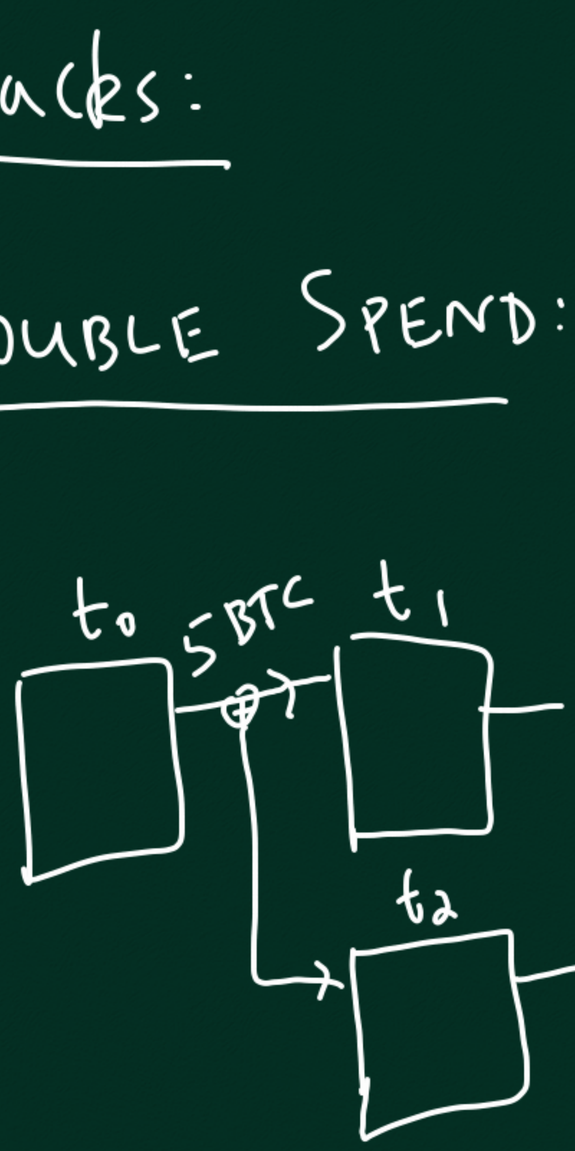


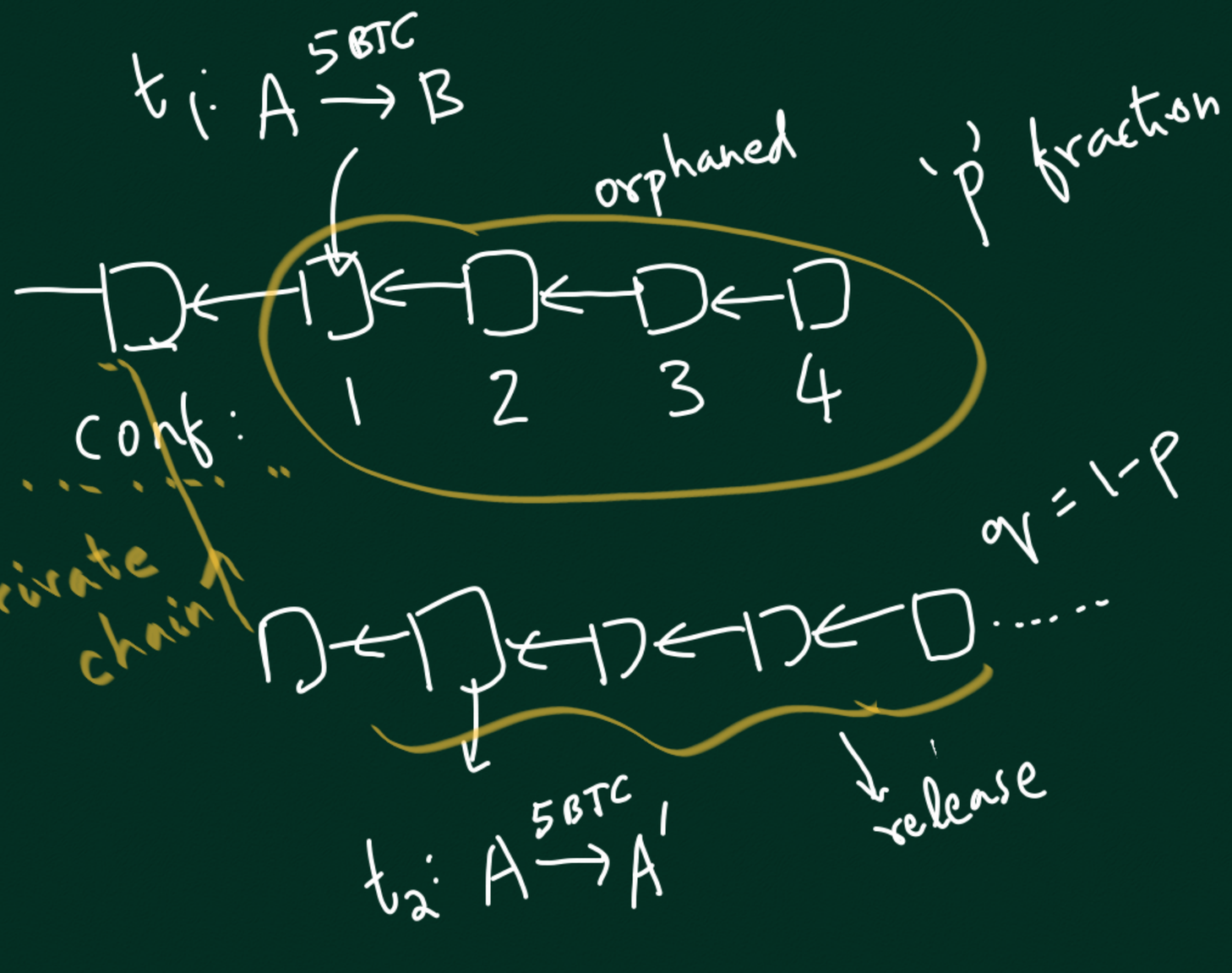


PoW Consensus: Heaviest chain is correct one

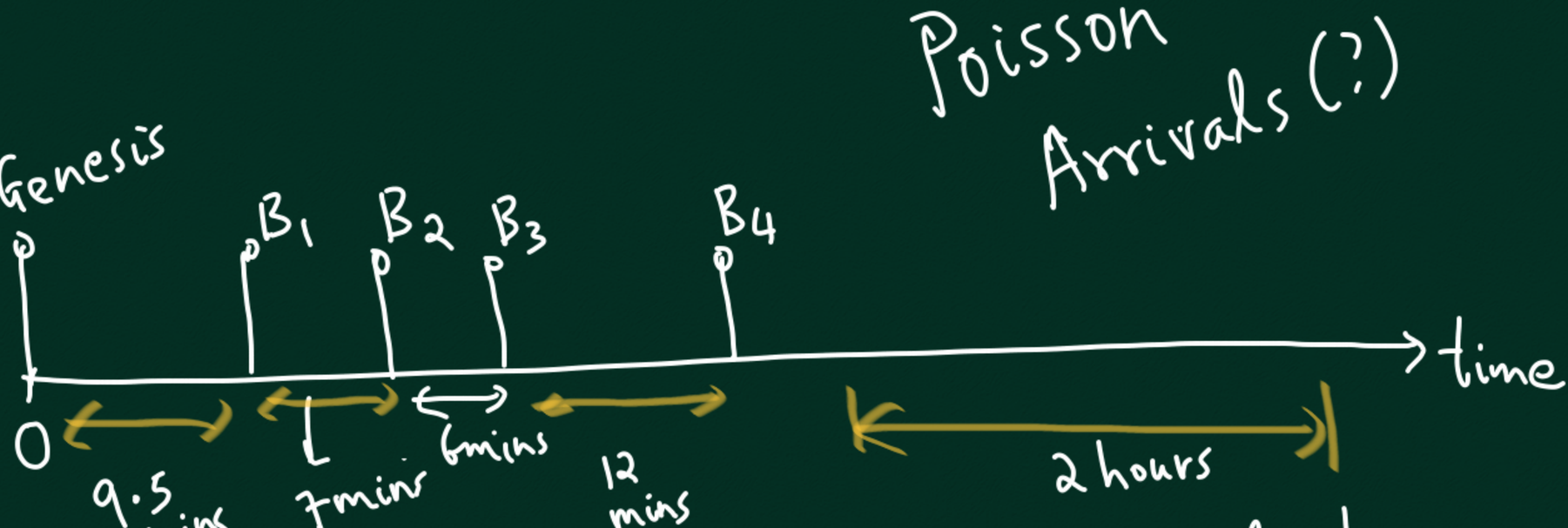
Attacks:

Double Spend:





Model for block generation



Poisson Arrivals (?)

Poisson Arrival Process: Inter-arrival time between consecutive arrivals is Exponential

$$\text{Prob.}(I > x) = e^{-\beta x}$$; $\beta > 0$ is a parameter

prob. density fn $f_I(x) = \beta e^{-\beta x}$

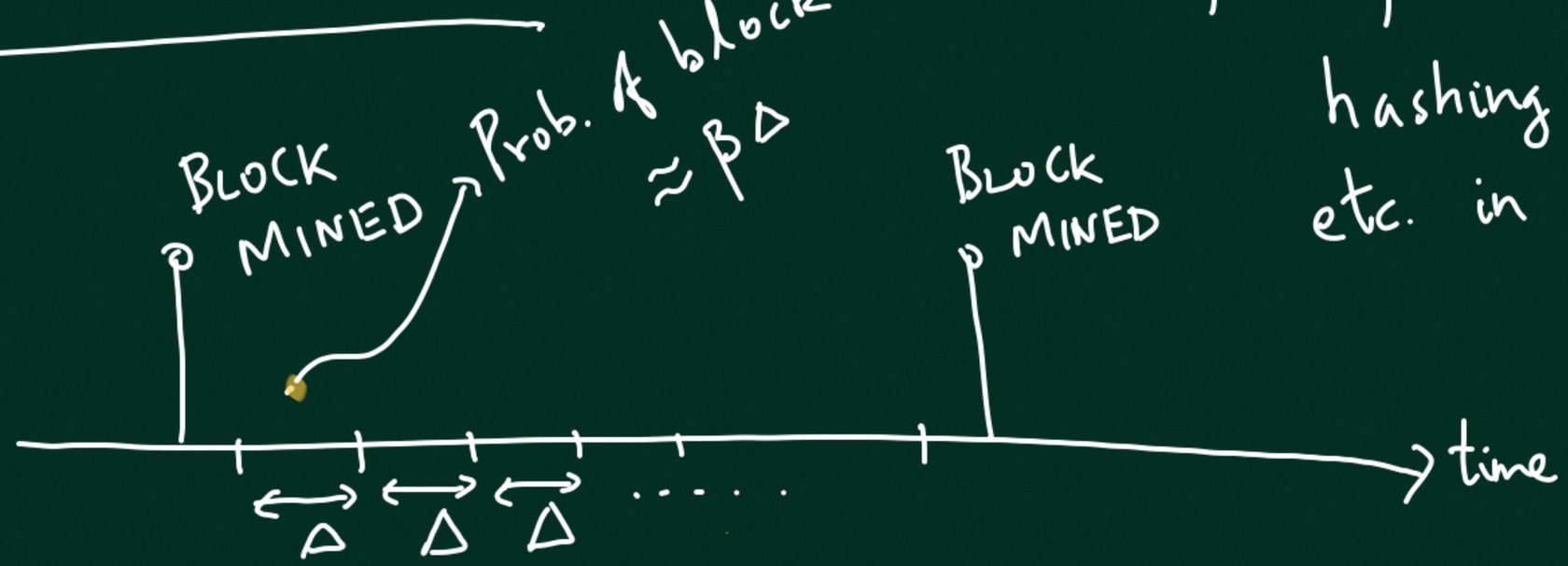
Given interval of size "T", call #arrivals A_T

$$P_r(A_T = n) = \frac{(\beta T)^n e^{-\beta T}}{n!}$$

Poisson Distribution

Block Mining Process

where β depends on hashing power, target etc. in network



$$Pr(I > n\Delta) = (1-\beta\Delta)^n = \left(1-\beta\cdot\frac{x}{n}\right)^n \xrightarrow{n\to\infty} e^{-\beta x}$$

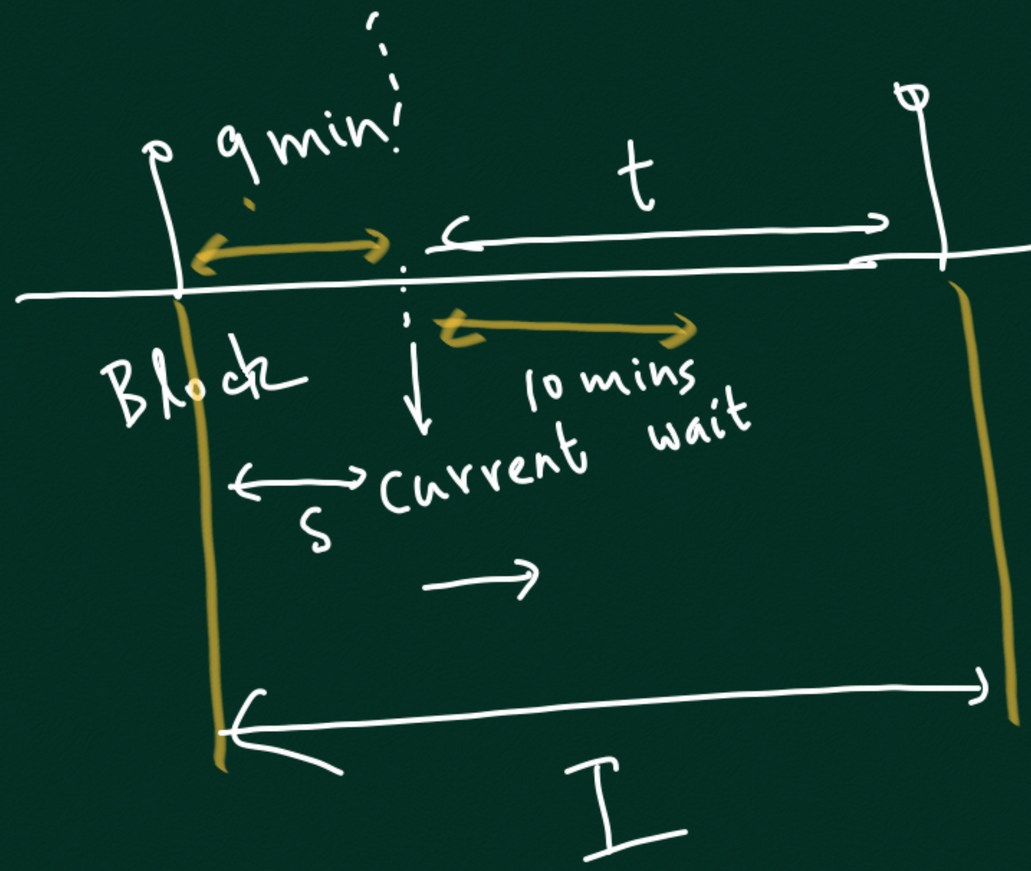
Set $x = n\Delta$

make $\Delta \to 0$, $n \to \infty$

s.t. $n\Delta = x$

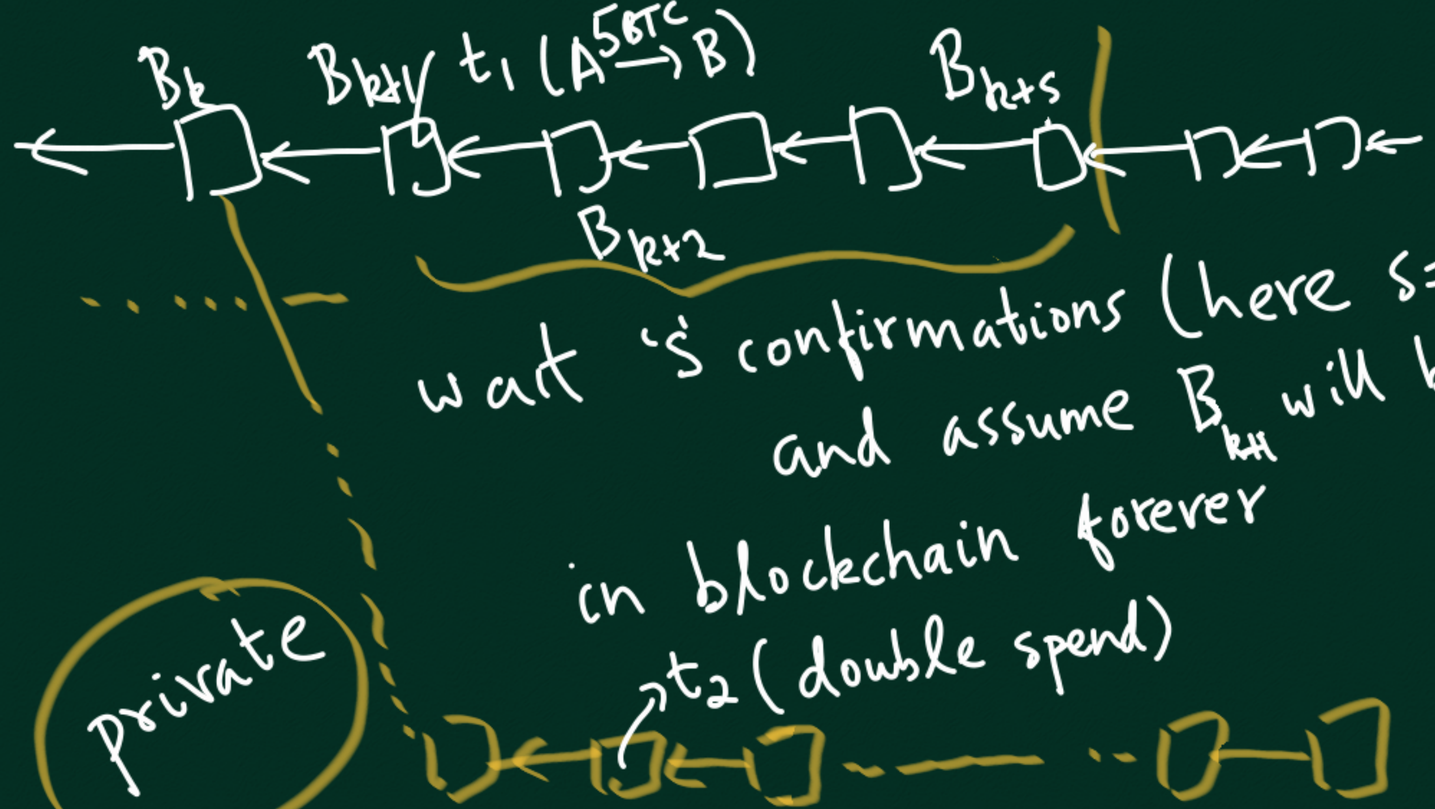
Memoryless Property of Exponential

$$Pr(E_1 | E_2) = \frac{Pr(E_1 \cap E_2)}{Pr(E_2)}$$



$$Pr\Big(\underbrace{I > s+t}_{E_1} \;\Big|\; \underbrace{I > s}_{E_2} \Big) = \frac{Pr\big(\{I > s+t\} \cap \{I > s\} \big)}{Pr(I > s)}$$

$$= \frac{Pr(I > s+t)}{Pr(I > s)} = \frac{e^{-\beta(s+t)}}{e^{-\beta s}} = e^{-\beta t}$$



unknown to B

Can A create private chain longer than public chain at any time after B_{k+s} is released

Honest chain

B_k B_{k+1} B_{k+1} B_{k+3}

'p' fraction hashing power

Exp: βp $(0<p<1)$

Attacker's chain

B'_{k+1} B'_{k+2} ....

$q = 1-p$ fraction

Exp: βq

B_{k+4}

B_{k+2} created

B_{k+5} created

Lead of Hon chain over attacker chain

2

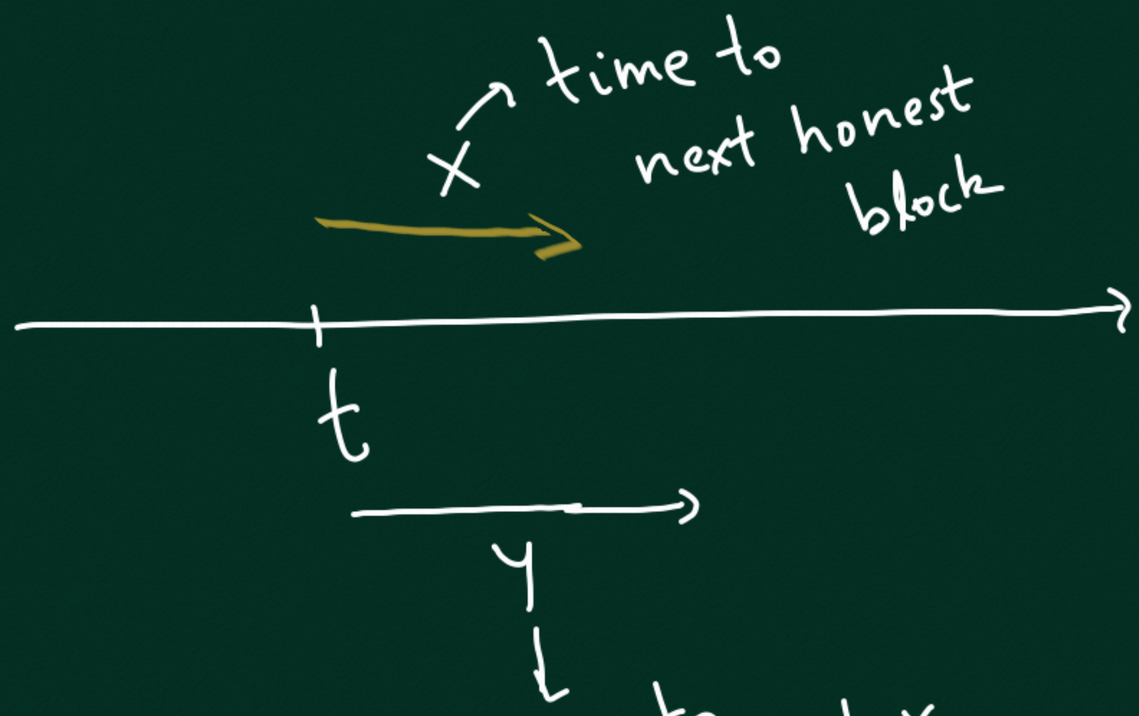
1

B_{k+3}

B_{k+1} created

B_{k+2}

B'_{k+1} created



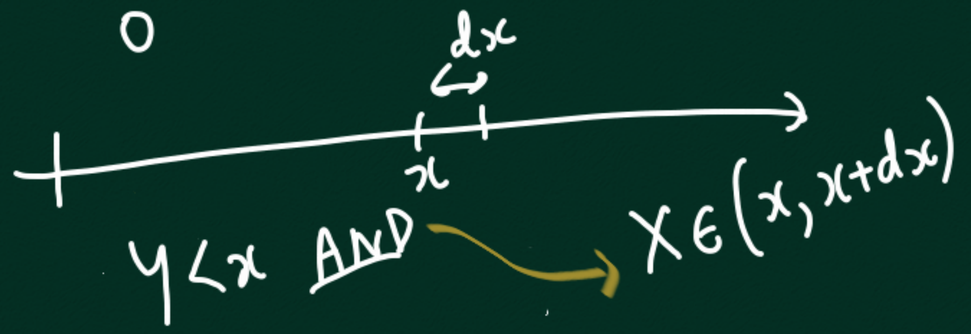
$$\text{Prob.}\left(\begin{array}{c}\text{attacker creates next blk}\end{array}\right) = Pr(Y < X) = \int_0^{\infty} Pr(Y<x) \cdot f_X(x)\, dx$$

$$Pr(X > x) = e^{-\beta p x}$$

$$Pr(Y > x) = e^{-\beta q x}$$

$$= \int_0^{\infty} \left[1 - e^{-\beta q x}\right] \cdot \beta p \cdot e^{-\beta p x}\, dx$$

$$= \int_0^{\infty} \beta p e^{-\beta p x}\, dx - p \int_0^{\infty} \beta e^{-\beta(p+q)x}\, dx$$



$$= \int_0^\infty \beta p e^{-\beta p x}\,dx - p\int_0^\infty \beta e^{-\beta x}\,dx$$

set $\beta' = \beta p$

$$\int_0^\infty \beta' e^{-\beta' x}\,dx = 1$$

$= 1$ (since $\beta e^{-\beta x}$ is a p.d.f.)

$$= 1 - p = q$$