Lecture 6 Security of Bitcoin.

truly permissionless ← means anyone can join and do anything.

1) Spam protection.

(a) network data. < tx / blocks.

* both data types have inbuilt cryptographic resistance to spam
* Tx: digital signature
* Block: PoW.

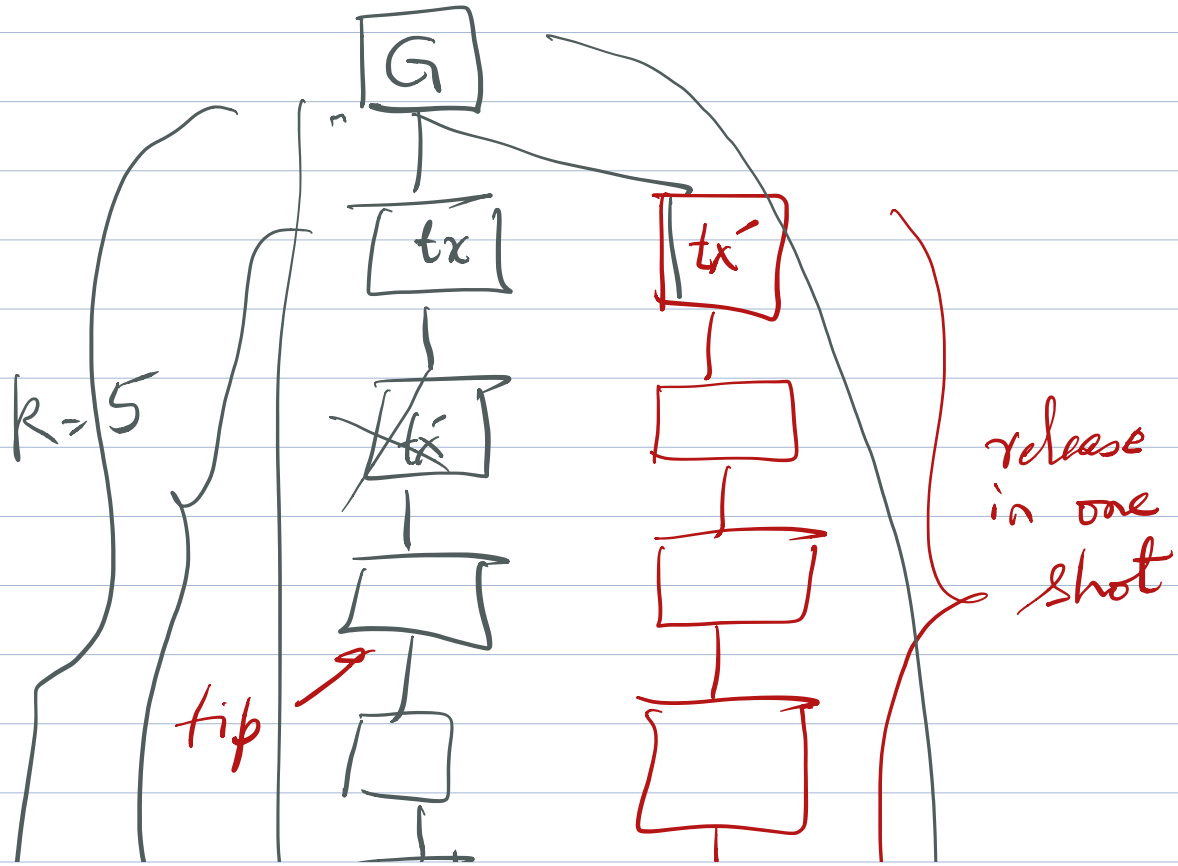
& syntax of the header.

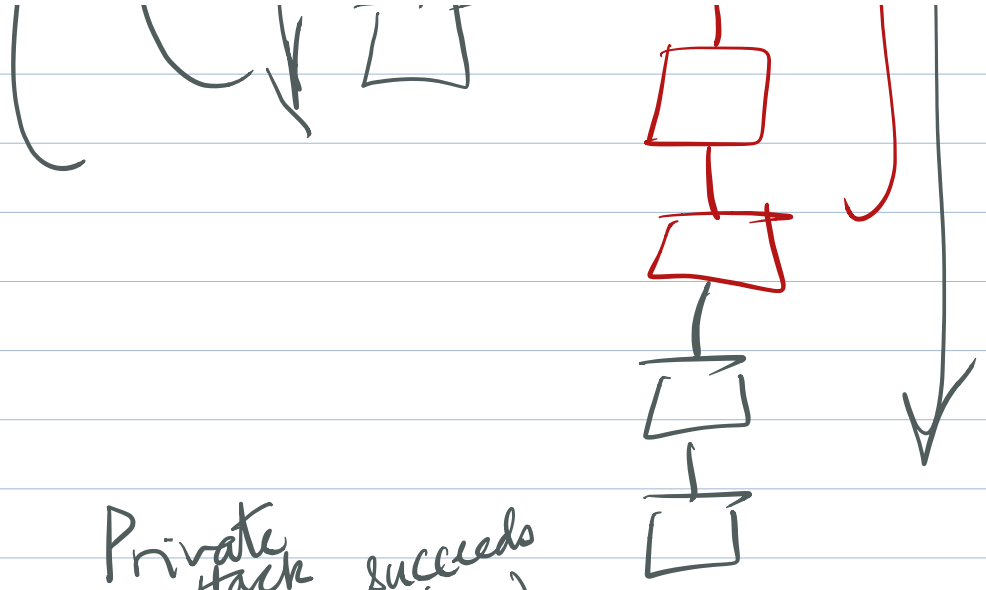
2) Adversary could meet the spam protection methods i.e, it creates a valid block but not follows the protocol.

(i) mine the block at the tip of the longest chain.

(ii) publish the block as soon as the mining is successful.

3) We looked at one strategy called Private attack.





Private attack succeeds when:

$$A \geq H$$

$$\geq k$$

Mining process:

Time to a successful mining event is Exp random variable

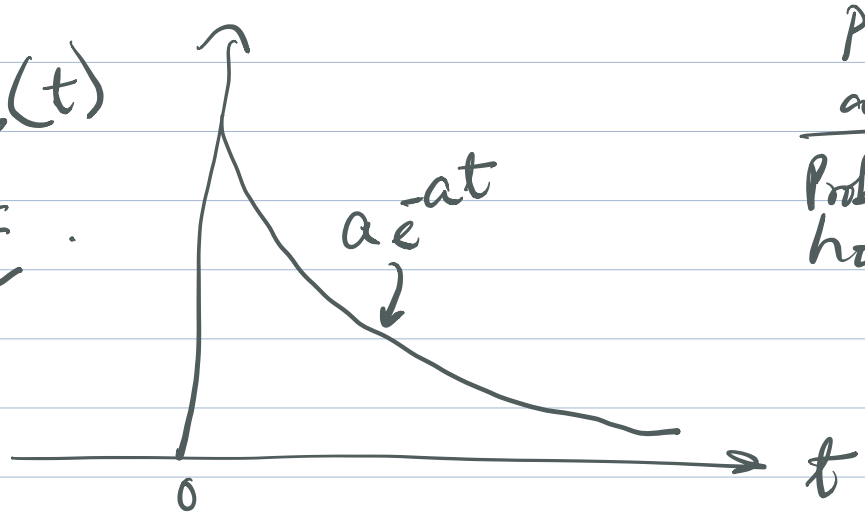
$$T \sim Exp(a) \quad \text{if}$$

$$\text{at}$$

$$P[T \geq t] = e^{-at}$$

$f_T(t)$

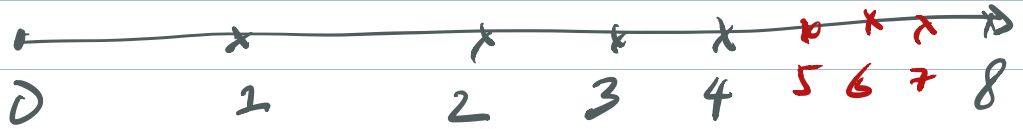
PDF.



$$\frac{\text{Prob of adv}}{\text{Prob of honest}} = \frac{\beta}{1-\beta}$$

# of mined block in time t is Poisson $\left(\frac{1}{a}\right)$.

Mining process:



Poisson process. (ECE 313)

Adv: Poisson process at rate λ_a

Honest: Poisson process at rate λ_h.

T_i^h = inter block time the i^{th} honest block

T_i^a = inter block time the i^{th} adv. block.

$$\sum_{i=1}^{k} T_i^h \geq \sum_{i=1}^{k} T_i^a$$

if this is true then the private attack is successful.

$$D_i = T_i^h - T_i^a$$

$$\frac{1}{K}\sum_{i=1}^{K} D_i \geq 0$$

$k \to \infty$ $\quad D_i$ are iid r.v.'s.

$E[D]$; by law of large numbers.

$$= \frac{1}{\lambda_h} - \frac{1}{\lambda_a}$$

So the private effort work only if

$$\frac{1}{\lambda_h} - \frac{1}{\lambda_a} \geq 0$$

"

or $\boxed{\lambda_a > \lambda_h.}$

i.e, $\beta \geq 50\%$

i.e, adversary controls more the half of the mining power

Other attacks are possible.

Network model: Δ - synchronous network

$\downarrow$

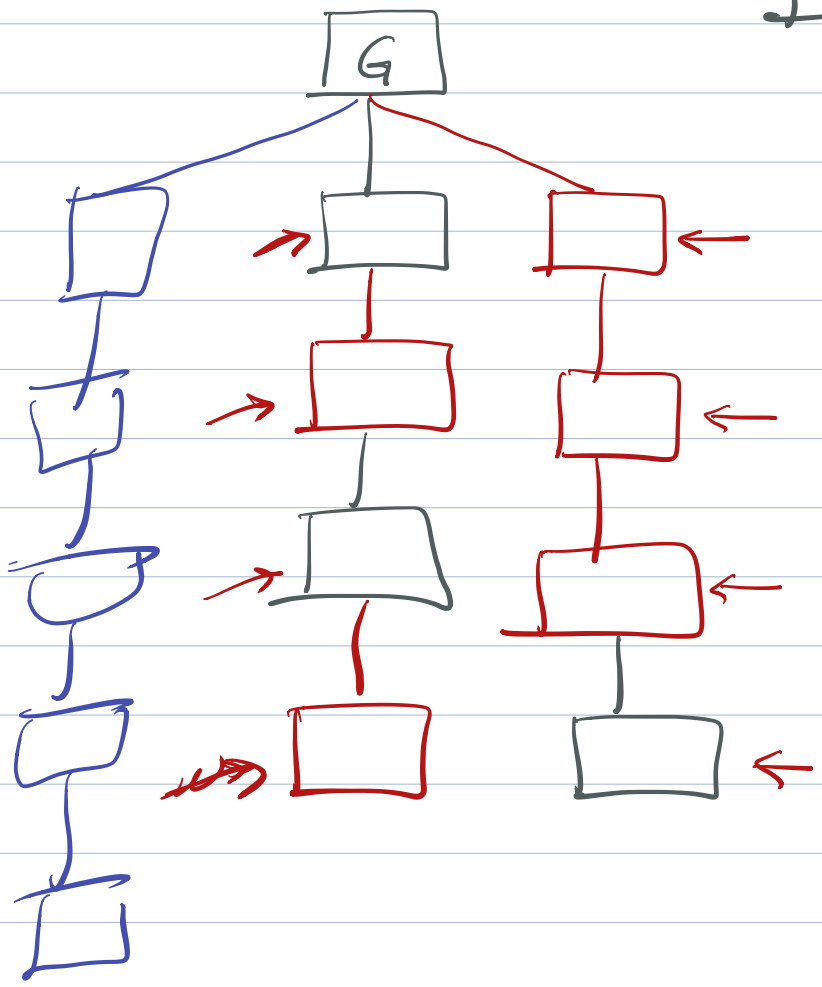
seconds.

PoW difficulty level is set so that one block every 10 minutes

15/8.

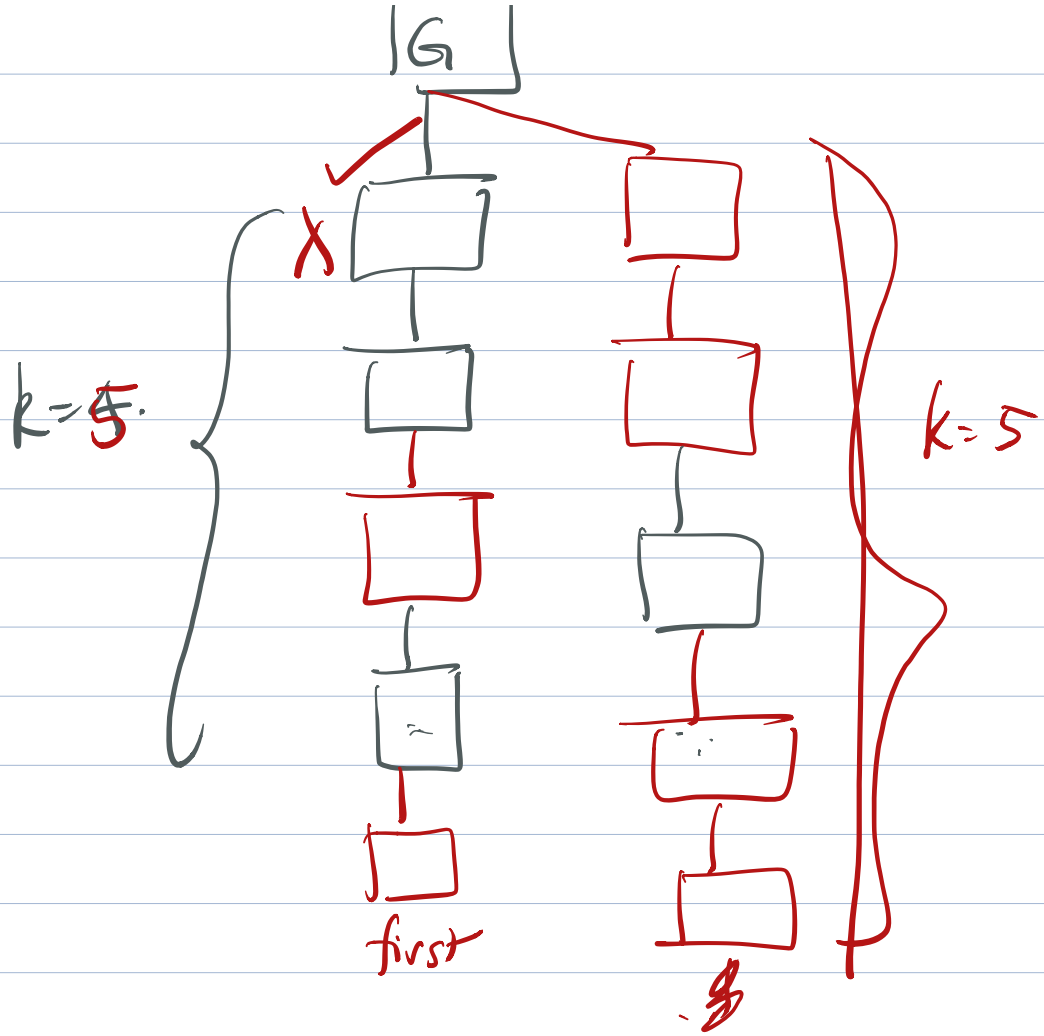
$$\frac{1}{\lambda_a + \lambda_n} = \text{inter-block arrival time.}$$

$$\boxed{\Delta = 0}$$



balance attack.

If an attack is successful then private attack is also successful.



A = adv. blocks

H = honest blocks.

$$A + H \geq 2k$$

$$\boxed{A \geq H} \qquad \boxed{\lambda_a > \lambda_h}$$

$$A \geq k \qquad 50\%$$

A ≥ max(k, H).

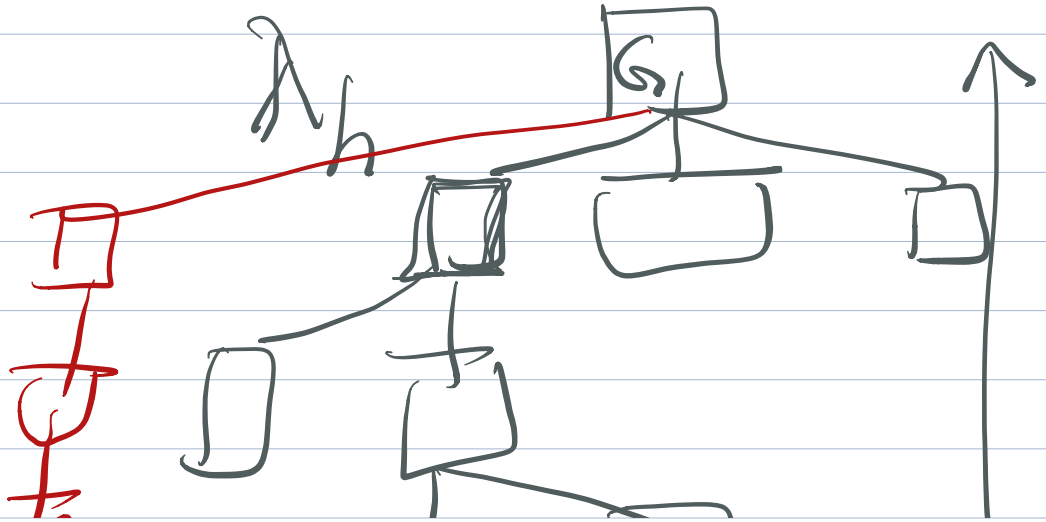
(a) Adv. get to k blocks first

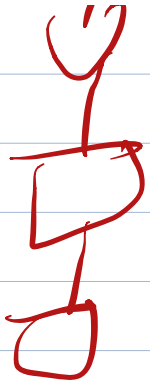
Then adv. waits to release its blocks. until H hits k.

(b) H gets to k first

A does a private attack.

$\Delta > 0$ then forking can happen naturally.





$\lambda_h \Delta$ = # of honest blocks mined in parallel.

So $\frac{\lambda_h}{1 + \lambda_h \Delta}$ is actual growth rate

Private attack succeeds if

$$\boxed{\lambda_a > \frac{\lambda_h}{1 + \lambda_h \Delta}}.$$