Lecture 6 Security of Bitcoin

Truly permissionless means anyone can join and do anything.

1) Spam protection

(a) network data < blocks

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

2) Adversary could meet the spam protection methods i.e. it creates a valid block but not follow 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: $A \geq H > k$

Mining process:

Time to a successful mining event is a random variable $T \sim \text{Exp} (a)$ if $\text{Prob}(\text{at least } k)$
\[ P(T > t) = e^{-\lambda t} \]

\[ f_T(t) = \frac{\lambda e^{-\lambda t}}{t} \]

PDF \( f_T(t) \)

\[ P(\text{no} \mid \text{imb}) = \frac{\beta}{1 - \beta} \]

\[ P(\text{imb} \mid \text{no}) = \frac{1 - \beta}{\beta} \]

\( \lambda \) of mined block in time \( t \)

is Poisson \( \left( \frac{1}{\lambda} \right) \).

Mining process.

\[ 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \]

Poisson process. (ECE 313)
Adv: Poisson process at rate $2h$

Honest: Poisson process at rate $2h$.

$h$ inter block

$T_i = \text{time the } i^{th} \text{ honest block}$

$a$ inter block

$T_i = \text{time the } i^{th} \text{ adv. block}$

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

If this is true then the private attack is successful.
$$D_i = T_i - T_i$$

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

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

$$E[D] \leq \text{by law of large numbers}$$

$$\frac{1}{\lambda_b} - \frac{1}{\lambda_a}$$

So the private attack will only work if

$$\frac{1}{\lambda_b} - \frac{1}{\lambda_a} \geq 0$$
or $2a > 2n$

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

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

Other attacks are possible.

Network model: $\Delta$-synchronous network

15 seconds.

Pow difficulty level is set so that one block every 10 minutes...
\[ \frac{1}{\lambda + \Delta n} = \text{inter-block arrival time}. \]

\[ \Delta = 0 \]

If an attack is successful then private attack is also successful.
A = new blocks
H = honest blocks.

A + H \geq 2k
\begin{align*}
A & \geq H \\
A & \geq k
\end{align*}
\[2a \geq 2h\]
\[50\%\]
A \overset{\text{mal}}{\rightarrow} (k, H).

(a) Adu. get to k blocks first.
Then adu. waits to release its blocks until it hits k.

(b) H gets to k first.
A does a private attack.

A \overset{\text{do}}{\rightarrow} \text{then forking can happen naturally.}

Diagram:
[Diagram image]
\( \lambda_h \Delta = \# \text{ of honest blocks mined in parallel} \)

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

Private attack succeeds if

\[
\lambda_a > \frac{\lambda_h}{1 + \lambda_h \Delta}
\]