Lecture 10: Double-spending attack

① Mathematical model

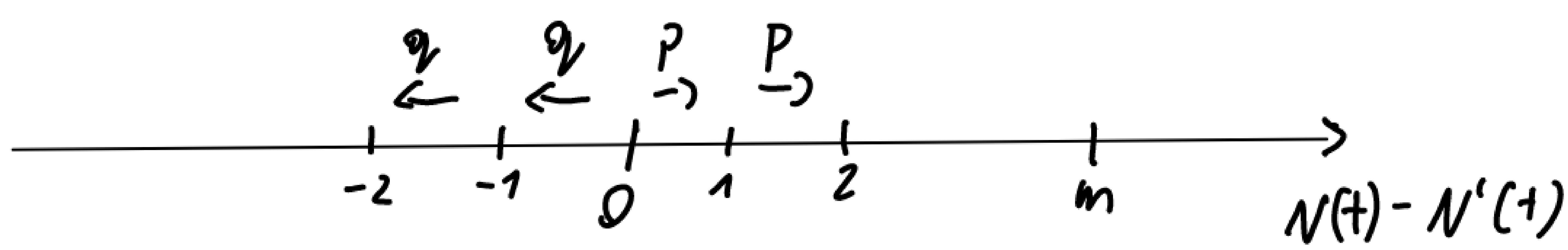
- T_k - time to generate block B_k, $T_k \sim Exp(\lambda)$, $E[T_k] = \frac{1}{\lambda} \approx 10$ min in Bitcoin
- $\{N(t), t \geq 0\}$, where $N(t)$ is a number of mined blocks up to time t is Poisson process with λ,

$$Pr[N(t) = n] = \frac{(\lambda t)^n e^{-\lambda t}}{n!}$$

- Adversary $\lambda' < \lambda$, $T \sim Exp(\lambda)$, $T' \sim Exp(\lambda')$, $Pr[T' < T] =$

$$= \frac{\lambda'}{\lambda + \lambda'} = q, \quad p = 1 - q, \quad q < \frac{1}{2}$$

- We can model it as random walk on the line



Problem: find probability $P(n)$ that $N(t) - N'(t) \leq 0$ ever after we have $\underline{n}$ moves to the right.

<u>Th3</u> Let E_m be an event that adversary „catches" the longest branch if he is missing $\underline{m}$ blocks. Let $q_m = Pr[E_m]$, thus $q_m = \left(\frac{q}{p}\right)^m$

P-f A - in the first step adversary wins

H - -||- honest -||-

$$q_m = Pr[E_m] = Pr[E_m | A] \cdot Pr[A] + Pr[E_m | H] \cdot Pr[H]$$

$= g_{m-1} \cdot q + g_{m+1} \cdot p \rightarrow g_m = C_1 \cdot C_2 \cdot \left(\frac{q}{p}\right)^m$

now we have to find C_1, C_2

- $g_0 = 1$
- $g_M = 0$, M - moment when adversary gives up (we assume $M \to \infty$)

g_0:

$g_0 = C_1 + C_2 \left(\frac{q}{p}\right)^0 \Rightarrow C_1 = 1 - C_2$

g_M:

$g_M = C_1 + C_2 \left(\frac{q}{p}\right)^M = 0 \Rightarrow C_2 = \frac{-1}{\left(\frac{q}{p}\right)^M - 1}$

$\xrightarrow[M \to \infty]{} 1$

$C_1 = 0$

$C_2 = 1$

We don't know how many blocks adversary needs to „catch",
when there are n confirmations.

- $S_n = T_1 + \dots + T_n$ ← honest nodes
- $P(n) = P[N'(S_n) > n] + \sum_{k=0}^{n} Pr[N'(S_n) = k] \cdot q_{n-k}$

he won

we still tries to catch

Nakamoto analysis

- assume $N'(S_n) \approx N'(E[S_n])$
- $E[T] = \frac{1}{\lambda} = \frac{\tau}{p}$, where $p = \frac{\lambda}{\lambda+\lambda'}$, $\tau = \frac{1}{\lambda+\lambda'}$
- $E[S_n] = n \cdot \frac{\tau}{p} \rightarrow N'(E[S_n]) \sim Poiss(\lambda' \cdot \underbrace{E[S_n]}_{\text{time}}) = Poiss(n \frac{\lambda}{\lambda+\lambda'} \cdot \frac{1}{p})$

$$= Poiss(\underbrace{n \cdot \frac{q}{p}}_{\alpha})$$

- $Pr[N'(E[S_n]) = k] = \frac{\alpha^k \cdot e^{-\alpha}}{k!}$

$$P(n) \approx Pr[N'(E[S_n]) > n] + \sum_{k=0}^{n} Pr[N'(E[S_n]) = k] \cdot g_{n-k}$$

$$= 1 - \sum_{k=0}^{n} Pr[N'(E[S_n]) = k] + \sum_{k=0}^{n} Pr[N'(E[S_n]) = k] \cdot g_{n-k}$$

$$= 1 - \sum_{k=0}^{n} Pr[N'(E[S_n]) = k](1 - g_{n-k}) = 1 - \sum_{k=0}^{n} \frac{\alpha^k \cdot e^{-\alpha}}{k!}(1 - g_{n-k})$$

$$\overset{g_0 = 1}{=} 1 - \sum_{k=0}^{n-1} \frac{\alpha^k \cdot e^{-\alpha}}{k!}(1 - g_{n-k})$$

Enumspan analysis

Th 4 Let X_n be a rand var denoting the number of blocks mined by the adversary, when honest miners mined n confirmations.

Then X_n has negative binomial distribution with parameter p and q: $Pr[X_n=k] = p^n q^k \binom{k+n-1}{k}$

p-f coin flipping: p-heads, q-tails, probability that we have k tails until n heads

The same can be shown: $Pr[X_n=k] = \int_0^\infty Pr(N(S_n)=k|S_n=t) f_{S_n}(t)\,dt$

Th 5 $P(n) = 1 - \sum_{k=0}^{n} (p^n q^k - q^n p^k)\binom{k+n-1}{k}$

p-f $P(n) = \sum_{k>n} Pr[X_n=k] + \sum_{k=0}^{n} Pr[X_n=k]\cdot q_{n-k} =$

$$= 1 - \sum_{k=0}^{n} p^n q^k \binom{k+n-1}{k} + \sum_{k=0}^{n} p^n q^k \binom{k+n-1}{k}\left(\frac{q}{p}\right)^{n-k} =$$

$$= 1 - \sum_{k=0}^{n} p^n q^k \binom{k+n-1}{k}\left(1 - q^{n-k}\cdot p^{k-n}\right) =$$

$$= 1 - \sum_{k=0}^{n} (p^n q^k - q^n p^k)\binom{k+n-1}{k} \quad \square$$

Th 6 $P(n) = I_{npq}\left(n, \frac{1}{2}\right) \sim \frac{(4pq)^n}{\sqrt{\pi(1-4pq)n}}$ - incomplete Beta function