Discussion Section #2

April 15, 2025

1. In this problem, we calculate the adversary's success probability in a private attack. Suppose the network delay $\Delta = 0$, and let λ_h and $\lambda_a < \lambda_h$ denote the mining rates of the honest and adversarial miners respectively. Recall that Bitcoin uses the k-deep confirmation rule.
   a) Give an upper bound on the probability that the adversary's private chain reaches depth d before the honest chain.
   b) Based on your answer to part (a), give an upper bound on the probability that the adversary succeeds in the private attack.

Answer:

a) Let X_h^i and X_a^i denote the gap between the arrival times of the i-th and $(i-1)$-th blocks mined by the honest and adversarial miners respectively (here, X_h^1 and X_a^1 denote the mining times of the first honest and adversary blocks after the attack begins). Recall that we model $\{X_h^i\}$ and $\{X_a^i\}$ as independent, exponentially-distributed random variables with rates λ_h and λ_a respectively. This implies that $\{X_h^i - X_a^i\}$ are i.i.d. random variables.

Let E_d denote the event that the adversary's private chain reaches depth d before the honest chain. Then $E_d \triangleq \{\sum_{i=1}^d X_h^i \geq \sum_{i=1}^d X_a^i\}$. Therefore,

$$\Pr[E_d] = \Pr\left[\sum_{i=1}^d X_h^i \geq \sum_{i=1}^d X_a^i\right] = \Pr\left[\sum_{i=1}^d (X_h^i - X_a^i) \geq 0\right] \tag{1}$$

$$\leq \min_{t\geq 0} \Pr\left[e^{\left(\sum_{i=1}^d (X_h^i - X_a^i)\right)t} \geq 1\right] \tag{2}$$

$$\leq \min_{t\geq 0} \mathbb{E}\left[e^{\left(\sum_{i=1}^d (X_h^i - X_a^i)\right)t}\right] \tag{3}$$

$$= \min_{t\geq 0} \prod_{i=1}^d \mathbb{E}\left[e^{\left(X_h^i - X_a^i\right)t}\right] \tag{4}$$

$$= \left(\min_{t\geq 0} \mathbb{E}\left[e^{X_h^1 t}\right] \mathbb{E}\left[e^{-X_a^1 t}\right]\right)^d \tag{5}$$

$$= \left(\min_{t\geq 0} \frac{\lambda_h}{\lambda_h - t}\frac{\lambda_a}{\lambda_a + t}\right)^d = \left(\frac{4\lambda_h\lambda_a}{(\lambda_a+\lambda_h)^2}\right)^d \tag{6}$$

Here, we employ a Chernoff bound. Equation (3) follows from Markov's inequality, equation (4) from the i.i.d. property of the random variables $\{X_h^i - X_a^i\}$, equation (5) from the independence of the random variables X_h^1 and X_a^1. Equation 6 follows from the fact that the moment generating function (MGF) of an exponential random variable is $F_{\mathsf{Exp}(\lambda),\mathsf{MGF}}(t) = \frac{\lambda}{\lambda - t}$.

Finally, Given $\lambda \triangleq \lambda_a + \lambda_h$ and $\beta \triangleq \lambda_a/\lambda < 1/2$, we can express the upper-bound as follows:

$$\Pr[E_d] \leq (4\beta(1-\beta))^d .$$

b) The adversary succeeds in the private attack if and only if its private chain reaches some depth $d \geq k$ before the honest chain. Let E denote the event that the adversary succeeds in the private attack. Then $E = \cup_{d=k}^{\infty} E_d$. This implies

$$\begin{aligned} \Pr[E] &= \Pr[\cup_{d=k}^{\infty} E_d] && (7)\\ &\leq \sum_{d=k}^{\infty} \Pr[E_d] && (8)\\ &\leq \sum_{d=k}^{\infty} (4\beta(1-\beta))^d = \frac{1}{1-4\beta(1-\beta)} (4\beta(1-\beta))^k && (9) \end{aligned}$$

Here, equation (8) follows from the union bound.

Note that for any $\beta < 1/2$, this upper bound can be made arbitrarily small (i.e., smaller than any $\epsilon > 0$ by picking a large enough k_ϵ).

---

2. What is the output of the following script? What function does it implement?

```
<7>
OP_DUP
OP_TOALTSTACK
OP_DUP
OP_ADD
OP_DUP
OP_ADD
OP_DUP
OP_ADD
OP_FROMALTSTACK
OP_DUP
OP_TOALTSTACK
OP_DUP
OP_ADD
OP_DUP
```

```
OP_ADD
OP_FROMALTSTACK
OP_ADD
OP_ADD
```

Answer:

It leaves 91 on the stack. It multiples the input by 13.

See the links below for collections of composite scripts: https://github.com/coins/bitcoin-scripts and https://github.com/coins/bitcoin-scripts/blob/master/composite-opcodes.md.
