Goal of this lecture note

- Attacker vs Honest Nodes
- From Hash Rate Ratio to Mining Probabilities
- Number of Blocks Minded during an Interval is Poisson
- Double Spending Attack
- Gambler's Ruin Problem
- Attack Success Probability

1 Attacker vs Honest Nodes

- Recall honest network guards the blockchain.
- Honest network's hash rate is published in the blockchain in the form of Target.
- Block generation speed is 1 block/600 sec.
- Suppose attacker's hash rate is slightly greater than honest network's.
- Then, the attacker can launch a 51% attack.
- We aim to calculate the probability of Double Spending success.

GIST

1 Attacker vs Honest Nodes

- From Target, the hash rate of honest network can be obtained.
- Lambda is 1 block/10 min.
- Given attacker’s hash rate, attacker’s lambda can be determined.
- Once we obtained the two parameters, given a new block mined, we can assign probability to which network the new block belongs.

GIST

2 From Hash Rate Ratio to Mining Probabilities

- Suppose Honest network hash rate R_H = 30 E hash/sec.
- Attacker's hash rate R_A = 10 E hash/sec.
  - Let p be the probability that given a new block is formed, the new block belongs to Honest chain.
  - Let q be the probability that given a new block is formed, the new block belongs to Attacker's chain.

GIST

2 From Hash Rate Ratio to Mining Probabilities

- Overall hash rate = 40 E hash/sec.
- Overall block generation speed is (4/3) block/10-min.

$$\lambda_{all} = \lambda_H + \lambda_A$$

- $\lambda_H = 1$ block/10-min
- $\lambda_A = \frac{1}{3}$ block/10-min

GIST

2 From Hash Rate Ratio to Mining Probabilities

- Each time a new block is formed, it belongs either to the Attacker's chain or to the Honest chain.
- The probability is given by

$$q = \frac{\lambda_A}{\lambda_H + \lambda_A}$$

$$p = \frac{\lambda_H}{\lambda_H + \lambda_A}$$

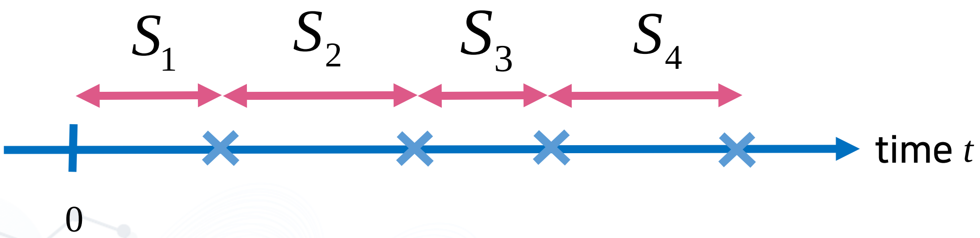
(Note also $\frac{q}{p} = \frac{R_A}{R_H}$)

$$p + q = 1$$

GIST

3 Number of Blocks Minded during an Interval is Poisson

- We now aim to know the distribution of number of blocks generated within a given time $t > 0$.

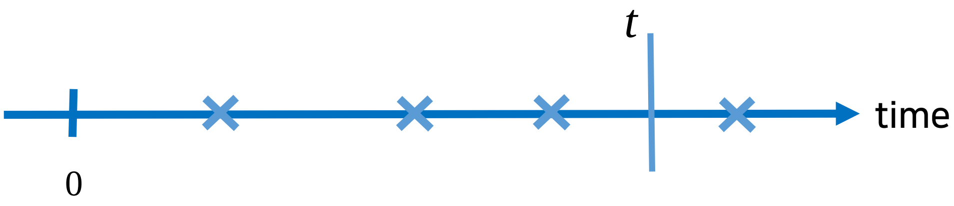


$$T_k^S := \sum_{i=1}^{k} S_i$$

GIST

3 Number of Blocks Minded during an Interval is Poisson

- We now aim to know the distribution of number of blocks generated within a given time $t > 0$.



$$P_\lambda\{k \text{ blocks in interval } t\} = e^{-\lambda t}\frac{(\lambda t)^k}{k!}$$

$$k = 1,2,3,\ldots$$

4 Double Spending Race Attack

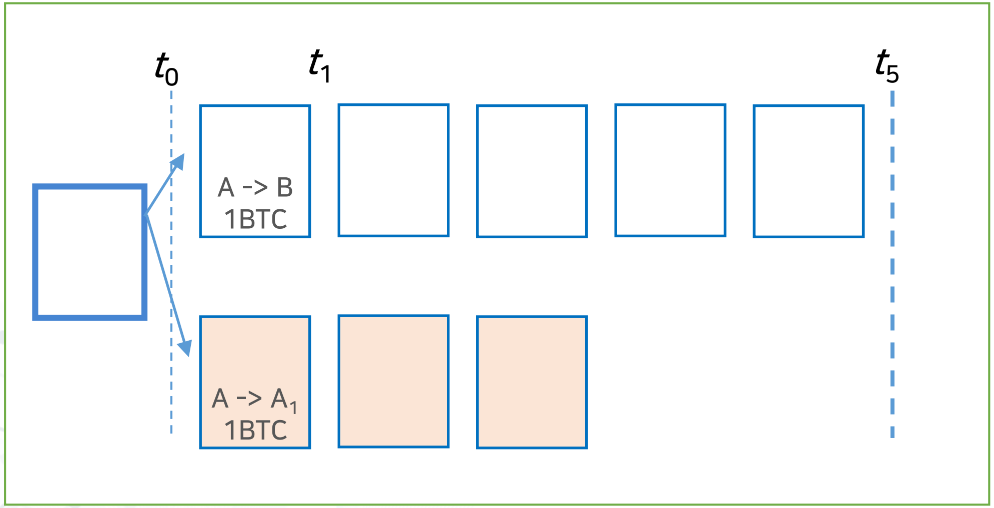
- Definition Double Spending Race Attack
  - Suppose A is the attacker.
  - B is the recipient.
  - B waits for z blocks. (Block confirmation)
  - Honest network's hash rate R_H
  - Attacker's hash rate R_A

4 Double Spending Race Attack

- Definition Double Spending Race Attack
  - Let $z = 5$ be block confirmation number.
  - *A* announces a TX showing A sends B 1 BTC at time t_0.
  - This TX gets into a block (1 confirmation) at t_1.
  - B waits until he gets 5th confirmation which occurs at t_5.
  - A starts preparation in secret for his double spend attack at t_0.
  - Namely, A grows its own chain.
    His chain has replaced the TX A ->B 1BTC with a fake TX, A -> A_1 1BTC. A_1 is another public key of A.
  - At t_5, A has mined 3 blocks and needs to decide if he continues to grow his own chain or not.

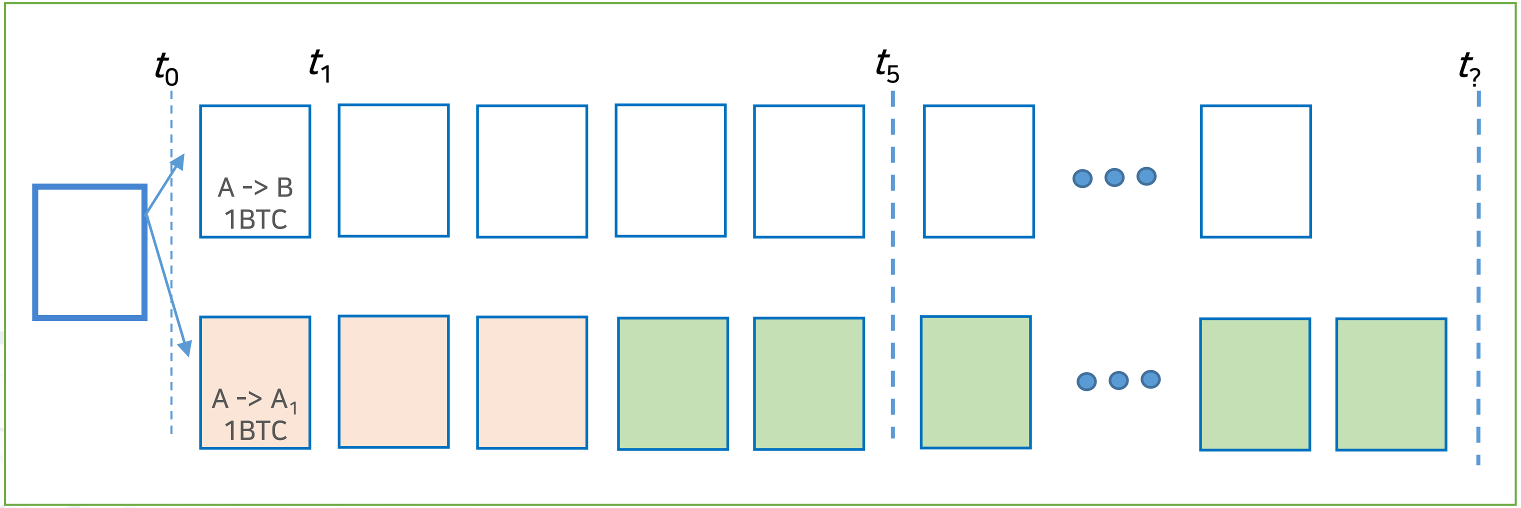
4 Double Spending Race Attack

- Double Spending Race Attack: Race begins.



4 Double Spending Race Attack

- Double Spending Race Attack: Success



Chain is announced!

GIST

4 Double Spending Race Attack

- Definition Double Spending Race Attack
  - The probability calculation has two phases.
  - First phase is the time interval in which the honest node mines z blocks.
    - Assume that the attacker has added k blocks to his chain.
    - Attacker's chain is thus $z - k$ blocks behind the honest chain.

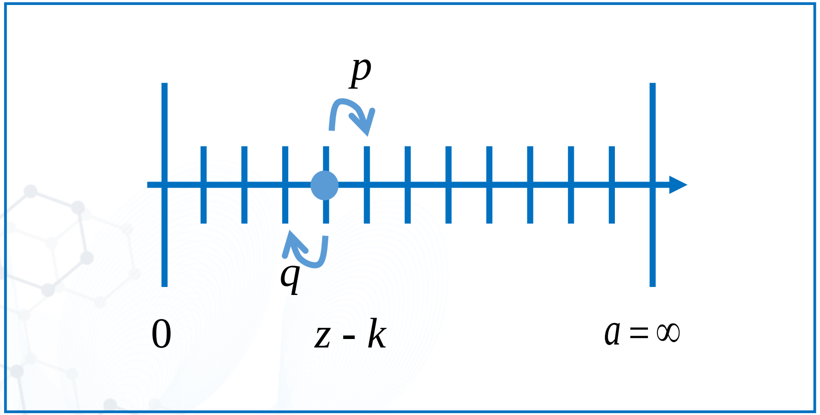
GIST

4 Double Spending Race Attack

- Definition Double Spending Race Attack
  - The probability calculation has two phases.
  - First phase is the time interval in which the honest node mines z blocks.
  - Second phase begins at the end of the first phase.
    - We aim to calculate the probability that the attacker catches up with the honest chain.

4 Double Spending Race Attack

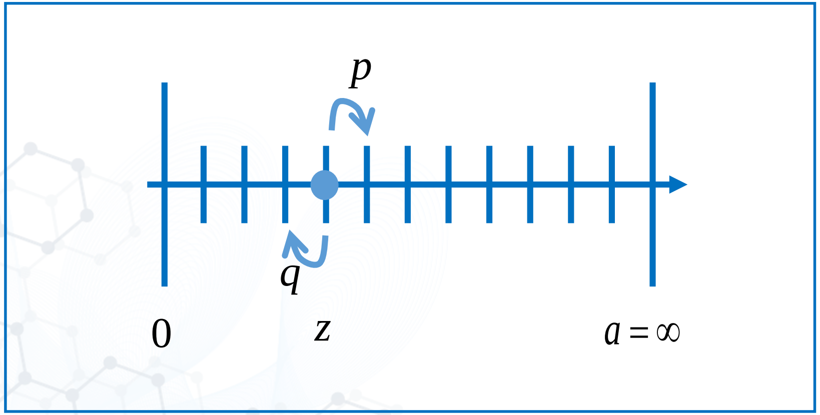
- Race begins with $z - k$ blocks behind.
  - When a new block mined belongs to the attacker with prob. q, move left.



GIST

5 Gambler's Ruin Problem

- Gambler's Ruin Problem
  - Feller's Gambler ruin result(Feller, vol.1, page 347)
  - Let z be the starting asset of the Gambler.



GIST

5 Gambler's Ruin Problem

- Feller's Gambler ruin result(Feller, vol.1, page 347)
  - There is a gambler who wins a dollar with probability p and loses with probability q in a game, i.e., $p + q = 1$.
  - Gambler starts with z dollars.
  - Gambler plays the game repeatedly against the dealer who has $a - z$ dollars, i.e., $a \geq z$.

GIST

5 Gambler's Ruin Problem

- Feller's Gambler ruin result(Feller, vol.1, page 347)
  - The probability q_z of the gambler's ultimate ruin (loses all his money).
  - Let p_z the probability of the gambler's ultimate winning.
  - Note $p_z + q_z = 1$.

5 Gambler's Ruin Problem

- Attack on the Mining Pool of Bitcoin and How to avoid?
  - Figure 1: The Gambler's Ruin Problem
    - The gambler starts with z dollars and the dealer with $a - z$ dollars.
    - Gambler wins a trial with probability p and loses with $q = 1 - p$.

1 After the first trial, the gambler's fortune is either increased by 1, $z+1$, or decreased by 1, z -1
Thus, we have

$$q_z = pq_{z+1} + qq_{z-1} \text{ for } 0 < z < a \qquad (1.1)$$

(with $q_0 = 1$ and $q_a = 0$)

GIST

5 Gambler's Ruin Problem

- Attack on the Mining Pool of Bitcoin and How to avoid?
  - Figure 1: The Gambler's Ruin Problem

2 Solving the difference equation Eq. (1.1), the result is obtained as

$$q_z = \frac{(q/p)^a - (q/p)^z}{(q/p)^a - 1} \qquad (1.2)$$

5 Gambler's Ruin Problem

- Attack on the Mining Pool of Bitcoin and How to avoid?
  - Figure 1: The Gambler's Ruin Problem

3 Letting $a \to \infty$,

$$
\begin{aligned}
q_z &= \lim_{a \to \infty} \frac{(q/p)^a - (q/p)^z}{(q/p)^a - 1} \\
&= \lim_{a \to \infty} \frac{1 - (q/p)^z (q/p)^{-a}}{1 - (q/p)^{-a}} \qquad (1.3) \\
&= \lim_{a \to \infty} \frac{1 - (q/p)^{z-a}}{1 - (q/p)^{-a}} = \begin{cases} 1 & if\ q \geq p \\ (q/p)^z & if\ q < p \end{cases}
\end{aligned}
$$

5 Gambler's Ruin Problem

- During z blocks added by the honest nodes, the number of blocks k mined by the attacker is Poisson.
- Given $z - k$ blocks behind, the attack can catch up in 2nd phase.
- Let $z \rightarrow z - k$ in (1.3).

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

GIST

5 Gambler's Ruin Problem

- Given z blocks added by the honest nodes, what is the average number of blocks mined by the attacker?
- The ratio is $z : p = \ ? : q$.

$$\lambda = z\frac{q}{p}$$

GIST

6 Attack Success Probability

- Gambler's ruin(z) → Replace $z = z - k$ for Attack Success Probability $(q, z-k)$

$$\sim \sum_{k=0}^{\infty} \begin{Bmatrix} (q/p)^{z-k} & k < z \\ 1 & k \geq z \end{Bmatrix} \text{Poisson}(\lambda = zq/p)$$

λ is the average number of blocks that the attacker mines in z unit of time.

$$= \sum_{k=0}^{\infty} \begin{Bmatrix} (q/p)^{z-k} & k < z \\ 1 & k \geq z \end{Bmatrix} \frac{(zq/p)^k e^{-zq/p}}{k!}$$

GIST

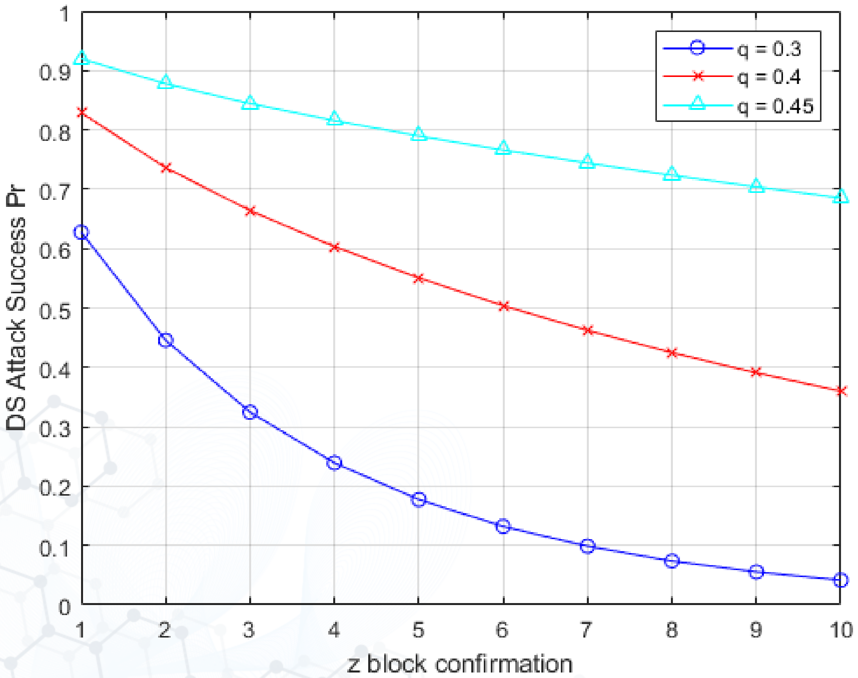
6 Attack Success Probability

- Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

- Converting to C code...

6 Attack Success Probability



GIST

6 Attack Success Probability

- Double Spending Attacks are possible even if hash rate of the attacker does not overpower (51% attack) that of the honest network.
- The DS success probability decreases rapidly with diminishing q.
- DS success probability decreases rapidly with growing z.