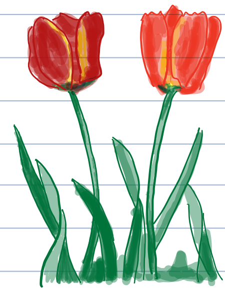
Secure Distributed Systems
CompSci 661 / 461



This video

- An explanation of the doublespend attack
- An (almost) complete derivation of the probability of attack success.

Doublespend Attacks

The most fundamental attack on blockchains

Scenario: Bob sells cars, and accepts blockchain coin as payment. Alice is our attacker. Her goal is to give Bob the correct amount of coin, then drive away with the car, then take her coin back (yoink!).

Alice is buying something that Bob can't rescind

Question: When can Bob release the car to Alice?

I) When Alice gives Bob a txn that will move coin to his address?

II) When that txn appears in a new block, B_1, on the main chain?

III) When blocks $B_2, \ldots, B_z$ follow B_1?

To answer, let's define some terms.

c_1 – an address with the exact amount needed to purchase the car, owned by Alice.

c_2 – an address owned by Alice

m – an address owned by Bob.

T – a valid txn that moves all coin from c_1 to m.

F – a valid txn that moves all coin from $\underline{c_1}$ to $\underline{c_2}$.

Option I (FAST!)

1. Bob validates T (how?)
2. Bob lets Alice drive away
3. Alice releases F to the miners
   - Alice can release F before or after T is released! Transactions are not processed in any FIFO ordering.

important

4. Only one of T or F can appear in the blockchain.

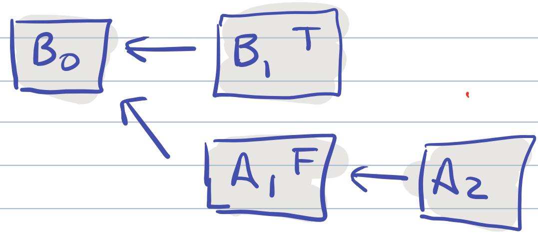
If it is F, Alice has her car and the coin.

If it is T, she has only the car.

Consider if Alice was purchasing US dollars from Bob. If the doublespend attack had failed, she'd lose out on only some fees.

Option II (not fast)

1. Bob validates T
2. Bob waits until T appears in newest block B_1.
3. Bob lets Alice drive away
4. Alice uses her mining power to mine a new block that contains F and has B_0 as its prior, and a block to follow that. (why two and not one?)



Note that Alice should start trying to mine A_1 as soon as B_0 appears.

When is this successful?

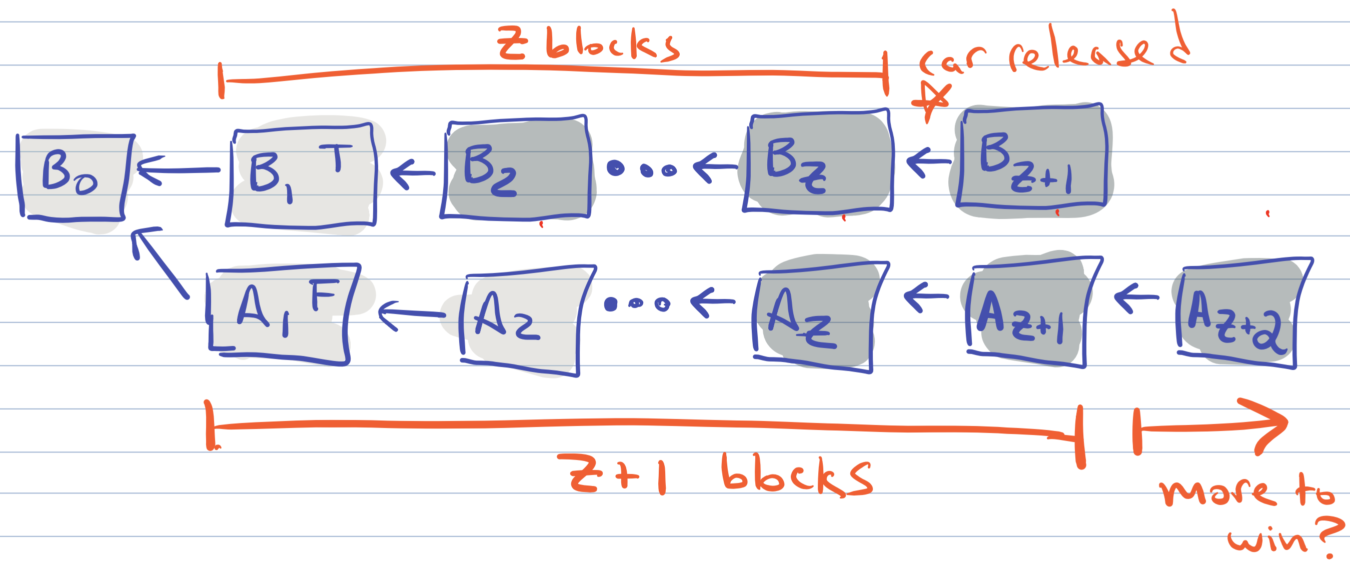
whenever she can mine A_2 before the honest miners can produce B_2 (why?)

What is the probability of success?

IT depends on Alice's mining power.
We'll get to that analysis.

Option III (very slow!)

1. Bob validates T
2. Bob waits until T appears in newest block B_1.
3. Alice starts mining a series of $z+1$ blocks, with F in the first.
4. Once the honest miners have mined block B_z, Bob lets Alice drive away.
5. IF Alice has mined $z+1$ blocks before B_{z+1} is produced, she releases them: Success!
6. Alice can keep trying to catch up and surpass the main chain by one block. IF so: Success! IF she never catches up, she fails.



Satoshi very quickly derives the probability of attack success.
Let's take a look at that equation...

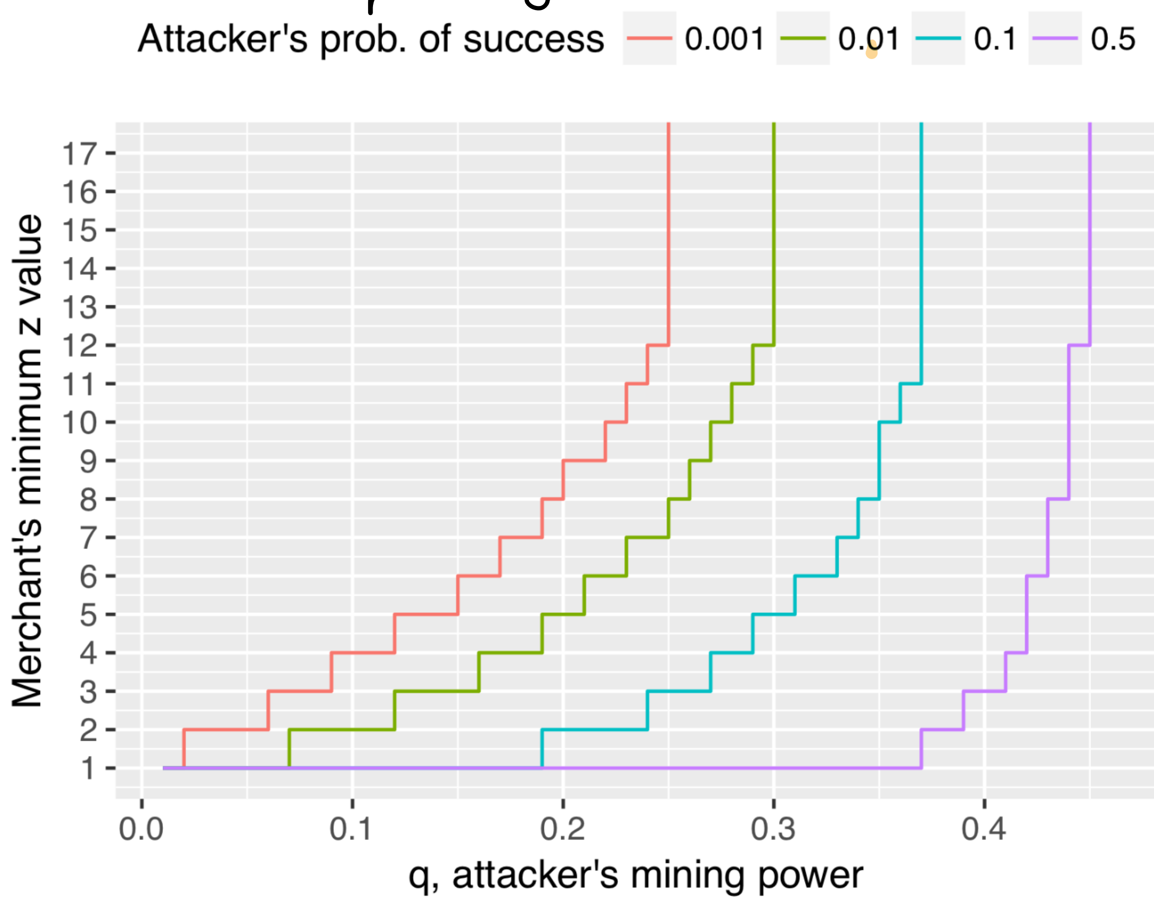
What is the probability of success?

p = honest miner's fraction of mining power
q = attacking miner's fraction of the mining power
so $p+q=1$

$$P(\text{attacker success}) = 1 - \sum_{k=0}^{z+1} \frac{\left((z+1)\cdot q/p\right)^k}{k!\,e^k}\left(1-\left(\frac{q}{p}\right)^{z+1-k}\right)$$

Before we derive that long thing, let's get a visual sense of things.

Select q and desired success prob, and I'll tell you the value of z required



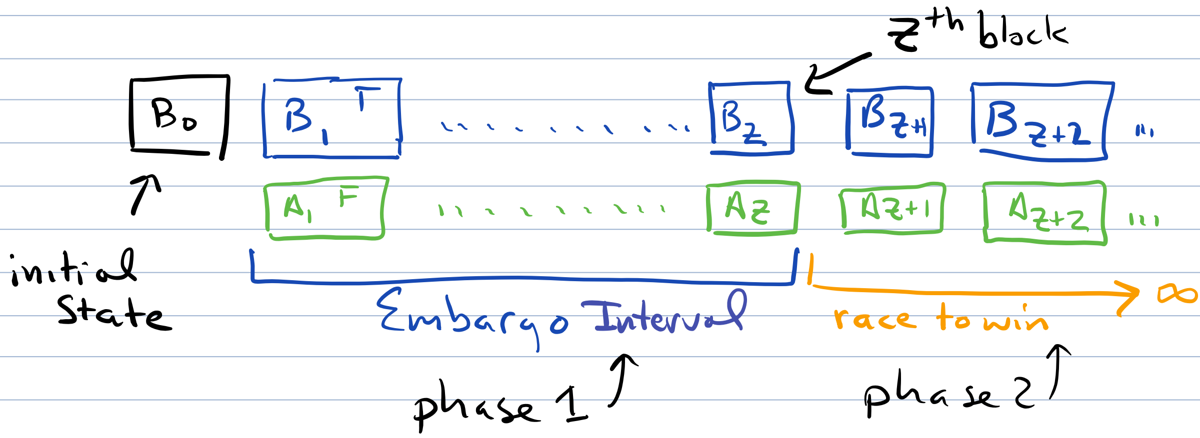
On the course web page, there is a PDF — "Excerpt from Walpole" That you should read before continuing.

It explains "Poisson Experiments" a bit — which will help you with the notes that follow.

Doublespend Attack Probability

- the car dealer is the victim here, not the honest miners.

The attack proceeds in two phases



① Embargo interval ends when the honest have z blocks
- During this time the attacker will produce $k \geq 0$ blocks
- If $k > z$, then the attacker has won

② During the race period, the goal of the attacker is to produce exactly one more block than honest.
- not simply $z+1$ blocks – honest is still working!
- no end to this race (in theory)

We analyze each period separately.
- for embargo interval we'll model as a "Poisson Experiment"
- for the race phase, we'll model as a variation of the "Gambler's Ruin"

Both models are useful outside of Blockchains.

I Embargo

We'll model as a **Poisson Experiment**

- Assumes that there is an average rate λ of event success per interval
- Assumes that the probability of success is constant.
- Assumes successes occur independently.

For us, we are concerned about the number of blocks produced by attacker during the interval.

Specifically, $\lambda = \frac{\text{sucesses}}{\text{interval}} = \frac{\text{blocks}}{\text{interval}}$

We define the interval length as the time it takes for honest miners to produce z blocks.

But the honest has only a fraction of the mining power. So the interval will last longer.

100% power? 10 minutes on average for 1 block

33% power? 30 minutes

10% power? 100 minutes

in general $\frac{T \text{ minutes}}{p \text{ blocks}}$ $\quad \frac{10}{1/3} = 30 \quad \frac{10}{1/10} = 100$

So $\frac{z \text{ blocks}}{\text{interval}} \cdot \frac{T \text{ minutes}}{p \text{ blocks}} = \frac{zT}{p} \frac{\text{minutes}}{\text{interval}}$

How many blocks will the attacker produce during that time?

$$\frac{z^T}{p} \frac{\text{minutes}}{\text{interval}} \cdot \frac{q \text{ blocks}}{T \text{ minutes}} = \frac{zq}{p} \frac{\text{blocks}}{\text{interval}}$$

$$\lambda = \frac{zq}{p} \frac{\text{blocks}}{\text{interval}}$$

again, attacker success per an interval that has a length determined by honest mining power.

Next we apply well-known formula for probability of X success given rate λ

$$P(X = k \text{ successes}; \lambda) = \frac{\lambda^k e^{-\lambda}}{k!}$$

e.g., $z = 3$

$q = 1/3$

$k = 3$

$$\lambda = \frac{3 \cdot 1/3}{2/3} = 3/2$$

$$P(X=3) = \frac{(3/2)^3 e^{-3/2}}{3!} = \frac{27/8 \, e^{-3/2}}{3 \cdot 2} = \frac{9}{e^{3/2} \cdot 16} \approx 12.6\%$$

We'll come back to this model in a bit.

II Race – The Gambler's Ruin

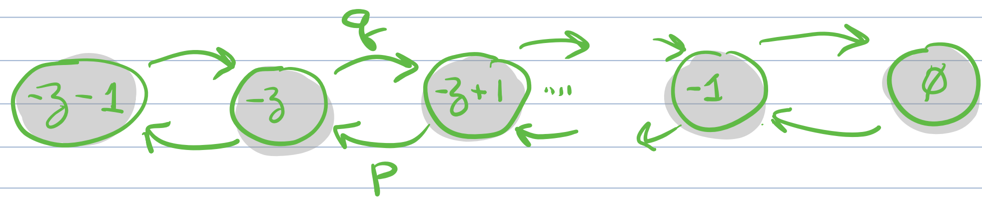
See the long handout for a full explanation/derivation. (optional)

Assumptions of the analysis

① We are taking a random walk along a line

② To take a step, we flip a biased coin.

③ We start z blocks back. Our goal is to get to $\emptyset$.



With probability q, we move towards $\emptyset$.

with probability $p = 1-q$, we lose ground.

What is the probability that attacker makes it to $\emptyset$?

$$Q_z = \begin{cases} 1 & , \text{ if } q \geq p \quad [q = \tfrac{1}{2} \text{ or larger}] \\ (q/p)^z & , \text{ if } q < p \quad [q < \tfrac{1}{2}] \end{cases}$$

(Why? Read the handout.)

III Putting the two pieces together

1) Embargo Interval

2) The RACE

At the end of the embargo period,

– The attacker has $0, 1, 2, \ldots$ blocks $\}$ $P(X = x; \lambda)$

– and if less than z, she must race from that loss. $\}$ Q_{z-x}

We can write out all cases

$$P(X=0)Q_z + P(X=1)Q_{z-1} + \cdots + P(X=k)Q_{z-k} + \cdots$$

$$= \sum_{k=0}^{\infty} P(X=k;\lambda)\,Q_{z-k}$$

$$= \sum_{k=0}^{\infty} \left(\frac{\lambda^k e^{-\lambda}}{k!}\right) Q_{z-k}$$

$$= \sum_{k=0}^{\infty} \left(\frac{\lambda^k e^{-\lambda}}{k!}\right) \begin{cases} 1, & \text{if } k > z \text{ or } q \geq p \\ \left(\frac{q}{p}\right)^{z-k}, & \text{if } k \leq z \text{ and } q < p \end{cases}$$

1 - doesn't catch up is equivalent

$$= 1 - \sum_{k=0}^{\infty} \left(\frac{\lambda^k e^{-\lambda}}{k!}\right) \begin{cases} 1-1, & \text{if } k > z \text{ or } q \geq p \\ 1-\left(q/p\right)^{z-k}, & k \leq z \text{ and } q < p \end{cases}$$

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

$$- \sum_{k=z+1}^{\infty} \left(\frac{\lambda^k e^{-\lambda}}{k!}\right)(1-1) \leftarrow \emptyset$$

In FACT, we need to not only catch up, but surpass the true formula is the following (Satoshi has an error!)

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

For homework, show the derivation (not just restatement)