Lecture 6: Bitcoin Safety

https://web3.princeton.edu/principles-of-blockchains/

Professor Pramod Viswanath
Princeton University

This lecture:
Safety of the Bitcoin system
Mathematical model of mining and adversary action

Bitcoin Security

- **Safety:** A transaction/block confirmed by one user is soon confirmed by all other users and remains confirmed forever after.
  - Focus of this lecture

- **Liveness:** all (honest) transactions get included into blocks, and further that the blocks feature in the longest chain.
  - Next lecture

Spam protection

Truly permissionless: anyone can join and do anything

Network data: transactions and blocks
Both data types have inbuilt cryptographic resistance to spam

- Transaction: digital signature
- Blocks: PoW & syntax of the header

Protocol level attacks

√ Create valid blocks

x Mine on the tip of the longest chain

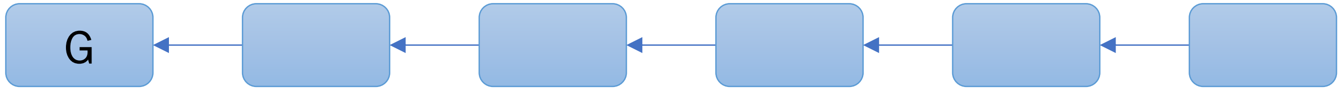
x Publish the blocks once mined

We looked at one strategy called private attack

Longest Chain Protocol

Where should the mined block hash-point to?

Latest block?



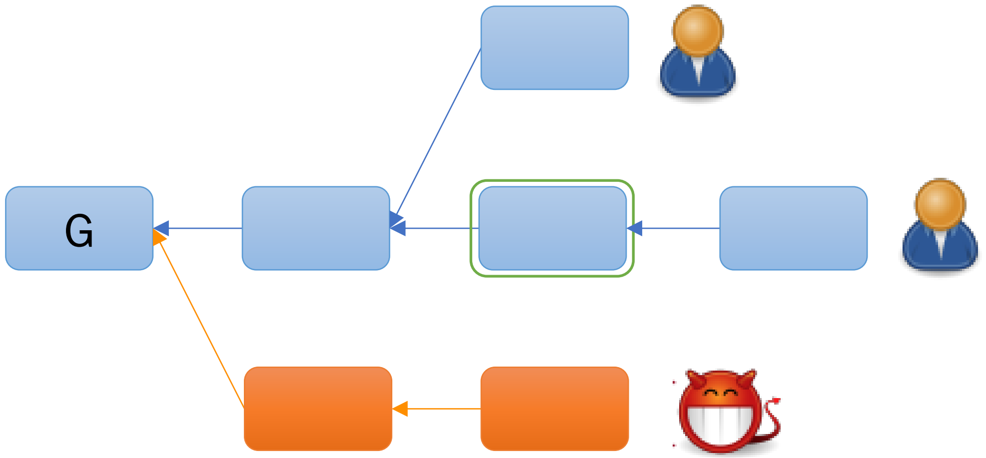
Longest Chain Protocol

Where should the mined block hash-point to?

However, blockchain may have **forks**

because of network delays

because of adversarial action



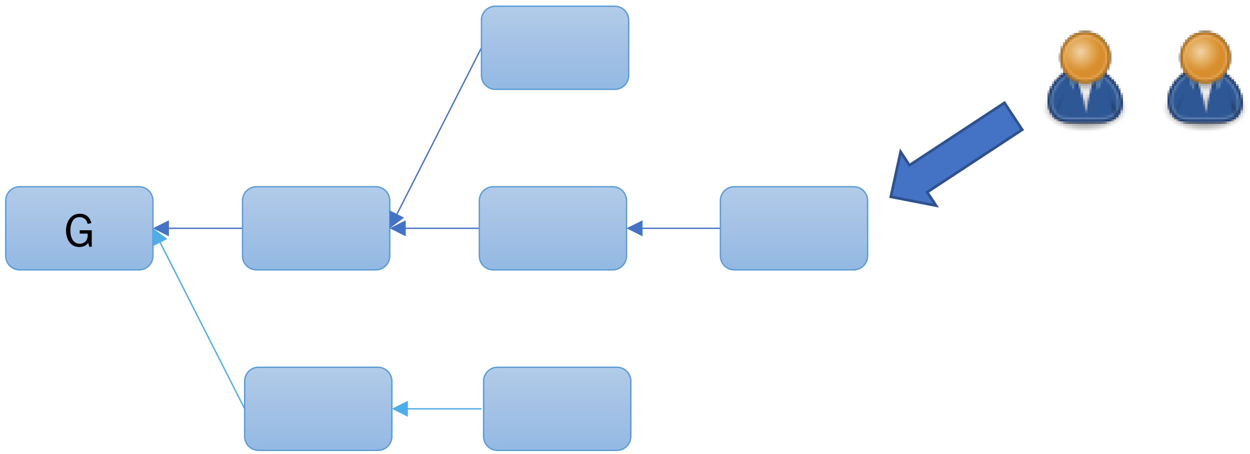
Longest Chain Protocol

Where should the mined block hash-point to?

Blockchain may have **forks**

because of network delays

because of adversarial action



Longest chain protocol

attach the block to the leaf of the longest chain in the block tree

Double Spend Attack

Adversary can point its block to an older part of the chain

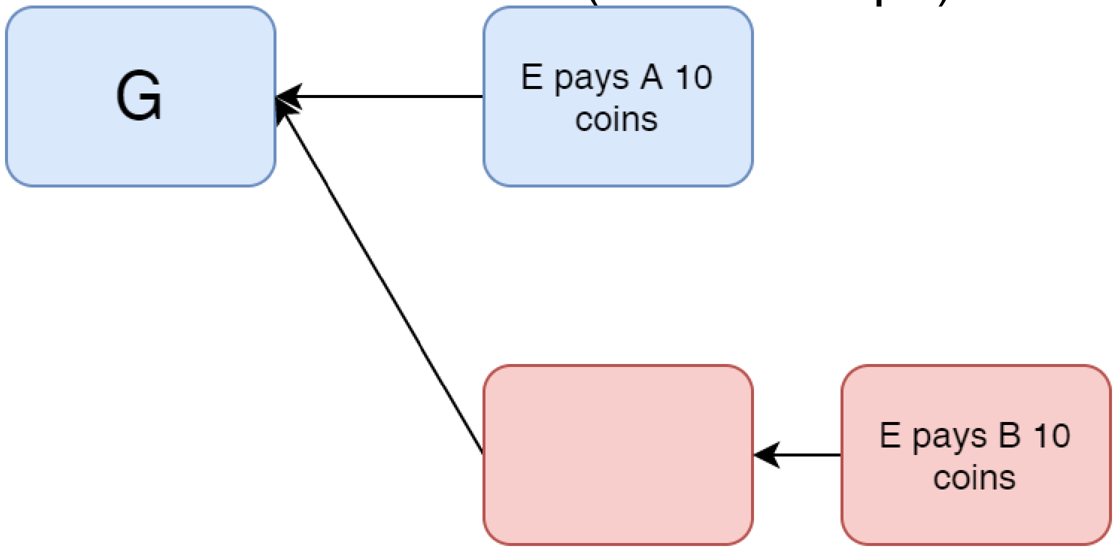
Duplicate transaction inserted

Plausible Deniability

network latency

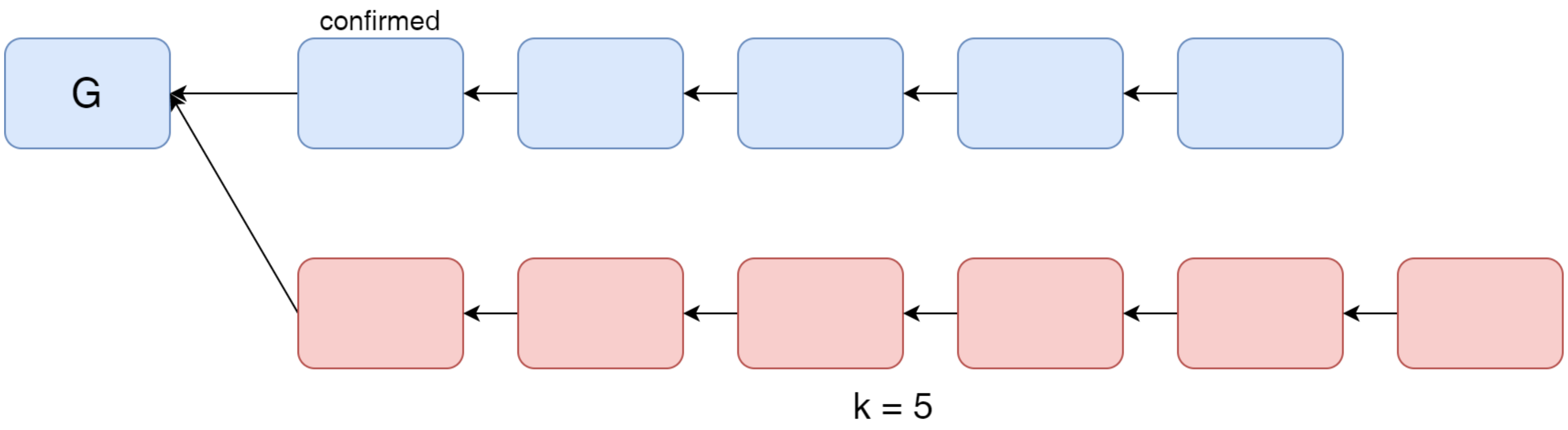
an offline user will not know which block came earlier

blocks have no wall clock reference (time stamps).



k Deep Confirmation Rule

- A block is **confirmed** if it is **buried k-deep in the longest chain**
- An attacker would need more than k blocks to double spend



Mining as a Poisson Process

Time to a successful mining event is an **exponential** random variable

$$T \sim exp(\lambda) \;\; if \;\; \Pr(T \geq t) = e^{-\lambda t}$$

Memoryless:

$$\Pr(T \geq t + t_0 | T \geq t_0) = \frac{\Pr(T \geq t + t_0)}{\Pr(T \geq t_0)} = \frac{e^{-\lambda(t+t_0)}}{e^{-\lambda t_0}} = e^{-\lambda t} = \Pr(T \geq t)$$

Number of mined blocks in time T is a **Poisson** random variable

$$X \sim Poi(\lambda T) \;\; if \;\; \Pr(X = k) = \frac{(\lambda T)^k e^{-\lambda T}}{k!}$$

The mining process is a Poisson process with rate λ, proportional to hash power

Mining as a Poisson Process

Mathematical fact: The sum of multiple independent Poisson processes is still a Poisson process

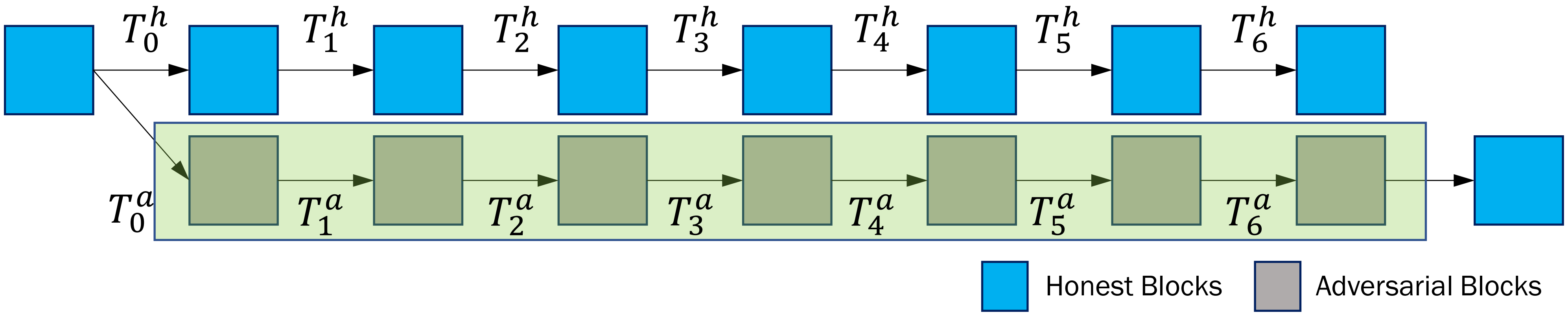
Consequence: the honest/adversarial mining processes are independent Poisson processes with constant mining rate

Honest mining: Poisson process with rate $(1-\beta)\lambda$

Adversarial mining: Poisson process with rate $\beta\lambda$

Private attack

Private Attack



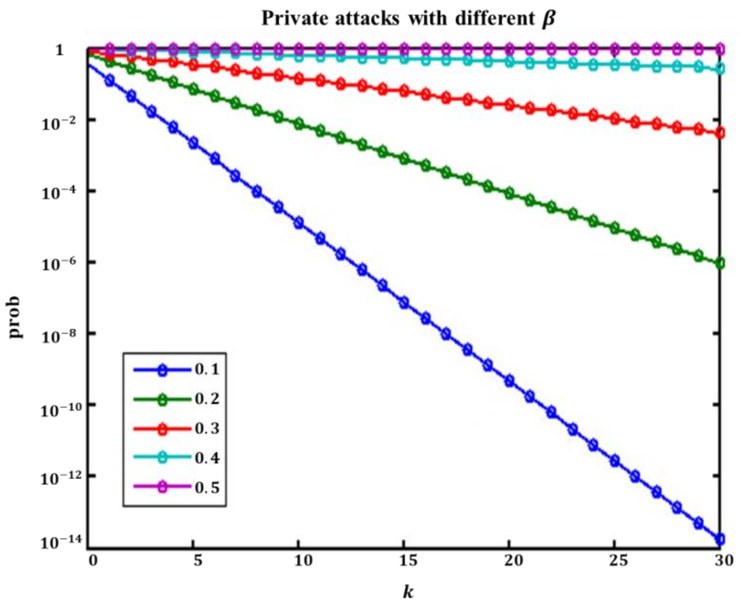
Attack Success

$k \to \infty$

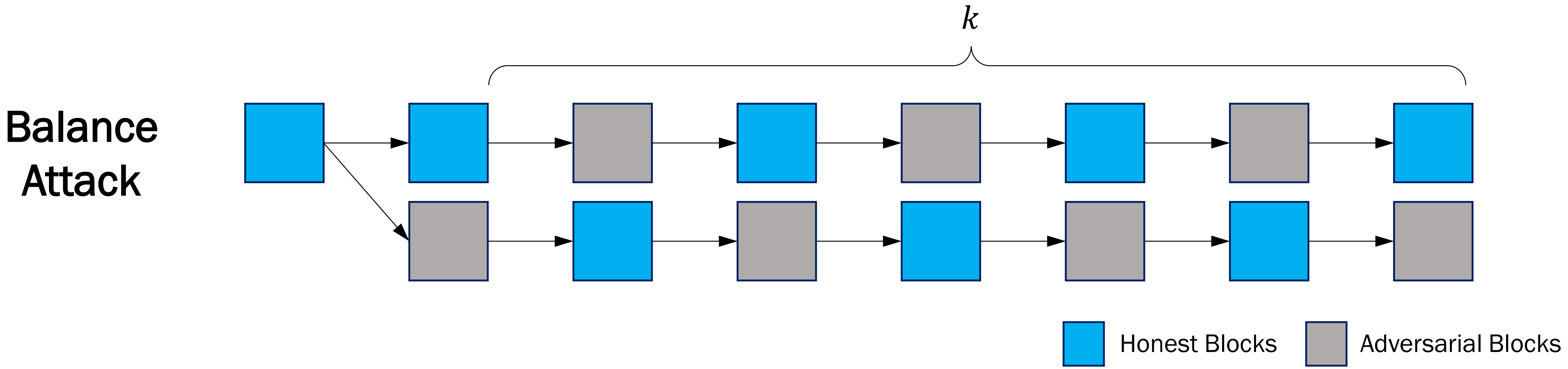
$$\sum_{i=0}^{\infty} T_i^h > \sum_{i=0}^{\infty} T_i^a \to \beta\lambda > (1-\beta)\lambda \to \beta > \frac{1}{2}$$

$k < \infty$

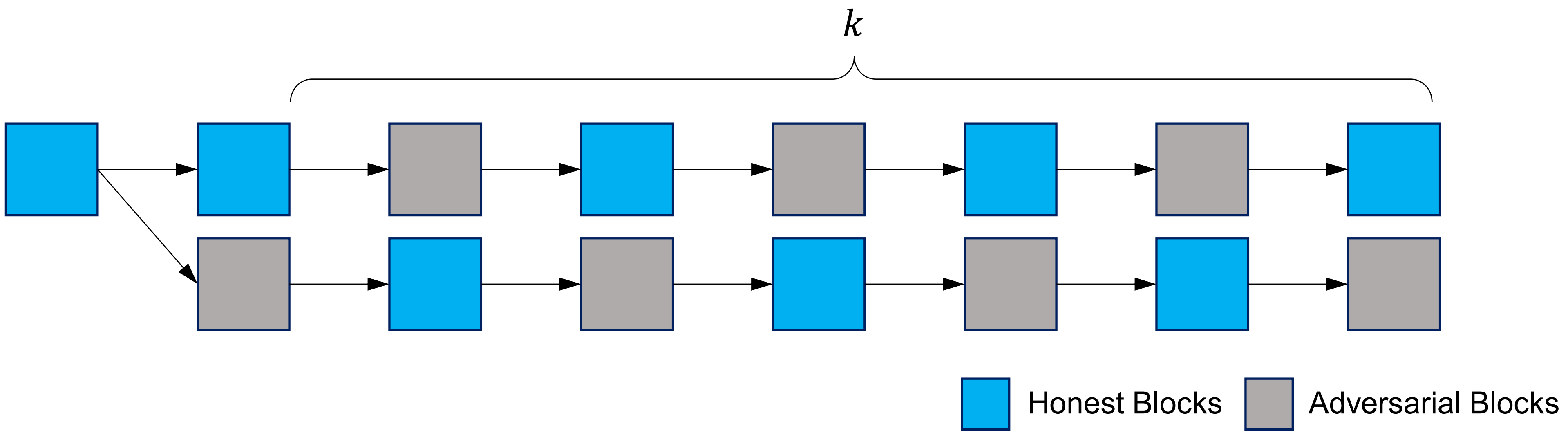
$$p_a = e^{-c(k+1)}$$



Balance attack



Private attack is the worst-case attack



A_k = # adv blocks, H_k = # of honest blocks

$$A_k + H_k \geq 2k + 2$$

$$A_k \geq H_k$$

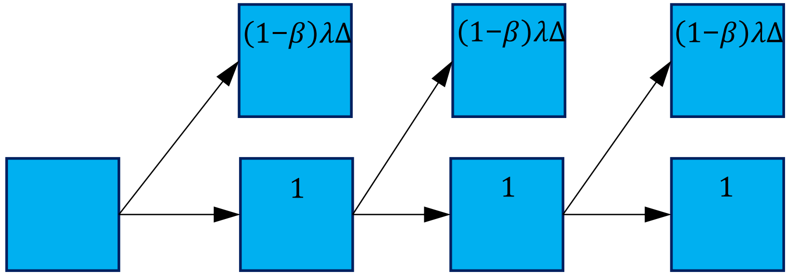
$\Longrightarrow$ $A_k \geq max(k, H_k) + 1$ $\Longrightarrow$ Number of adversarial blocks is enough to launch a private attack

Private Attack (With Honest Forking)

Δ - synchronous network model: network delays bounded by Δ

Natural forking:

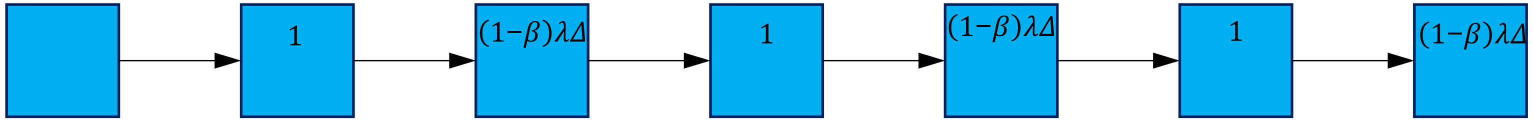
Honest forking:



Reduced honest chain growing rate

$$\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}$$

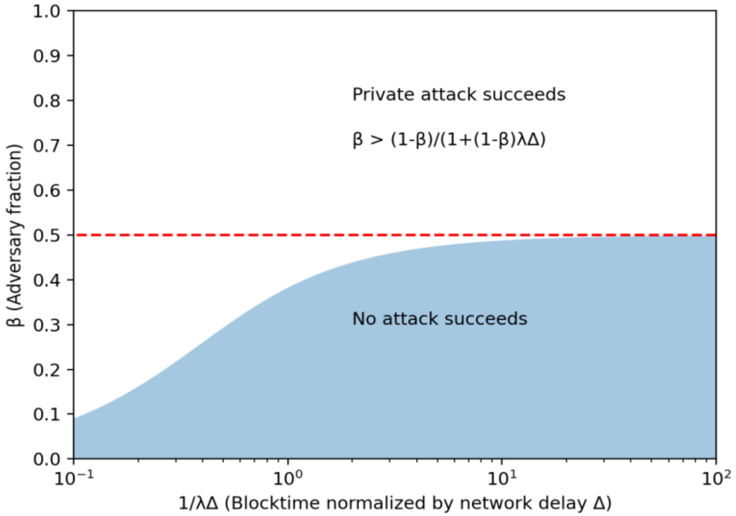
No honest forking:



Attack Success

Δ network delay

$$\beta\lambda > \frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}$$



Summary

- Model Bitcoin mining as Poisson processes
- Analysis against the private attack
- Safety analysis beyond the private attack – all possible protocol attacks