EE 374: Fundamentals of Blockchain Infrastructure **Stanford, Spring 2025**

Lecture 7: Security Tradeoffs and from PoW to PoS

April 21, 2025

Lecturer: Prof. David Tse Scribe: Yuxiang Liu

1 Latency and Throughput vs. Security

Recapping from the previous lecture:

- Network delay is denoted as Δ, typically ranging from fractions of a second to a few seconds for Bitcoin.
- Latency is defined as: latency $= k \cdot \frac{1}{\lambda}$.
- Throughput is given by: throughput $= B \cdot \lambda$.

Note that when λ increases, latency decreases and throughput increases. However, increasing λ does not simply lead to a proportional increase in the chain growth.

Moreover, security takes a hit. When two blocks are mined in quick successions because of a large λ, a fork can take place, and because one of the forked blocks would be eliminated, chain growth is diminished by the fork:

$$\text{chain growth} = \frac{\lambda}{1+\lambda\Delta}$$

Here, $\lambda\Delta$ represents the forking rate, resulting in wasted energy during forks, thereby reducing security.

Security depends on the comparative mining rates of honest miners (λ_h) and adversarial miners (λ_a). Typically, security is ensured if $\lambda_a < \lambda_h$. However, due to forks, the effective rate becomes:

$$\lambda \to \frac{\lambda}{1+\lambda\Delta}$$

and thus the condition becomes:

$$\lambda_a < \frac{\lambda_h}{1+\lambda_h\Delta}$$

Defining β as the adversarial ratio where $\lambda_a = \beta\lambda$ and $\lambda_h = (1-\beta)\lambda$, we derive the security threshold condition:

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

Thus, the maximum adversarial ratio β_{max} ensuring network security is:

$$\beta_{max} = \frac{1-\beta_{max}}{1+(1-\beta_{max})\lambda\Delta}$$

We can also plot β_{max} as a function of $\lambda\Delta$ in Figure 1 below:

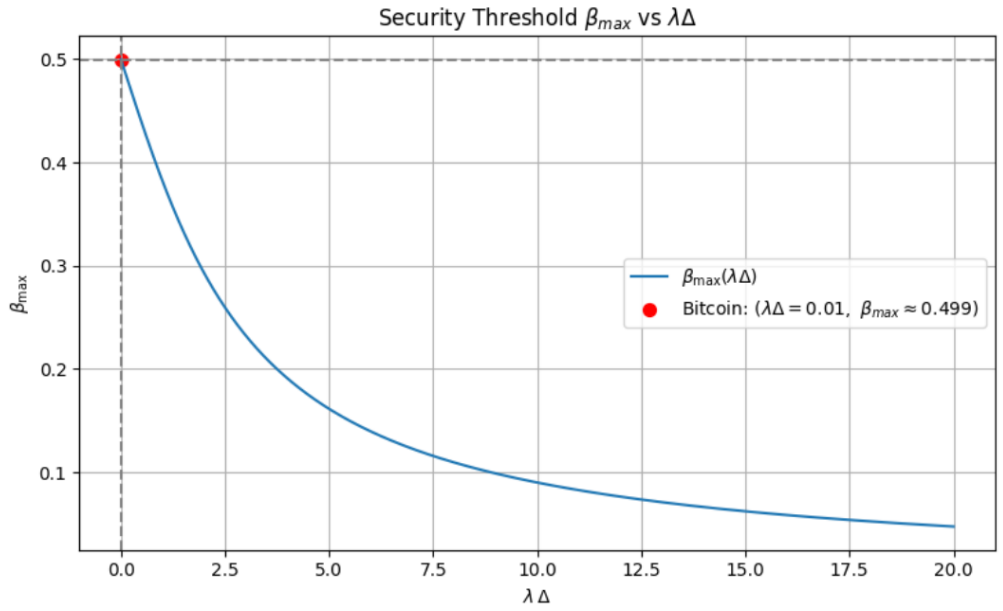

Figure 1: Security threshold (β_{max}) as a function of $\lambda\Delta$.

For Bitcoin, the product $\lambda\Delta \approx 0.01$, which yields $\beta_{max} \approx 49.9\%$, demonstrating Nakamoto's strong emphasis on security.

1.1 Security Tradeoffs

We can also demonstrate the Security-Throughput tradeoff and the Security-Latency tradeoff as follows:

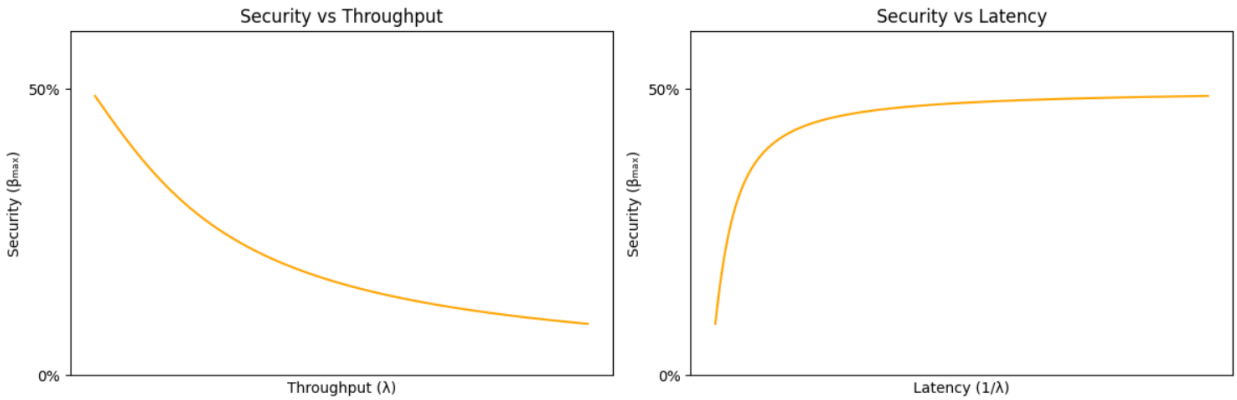

Figure 2: Security-Throughput and Security-Latency tradeoffs.

1.2 Adjusting k and B

Given that we cannot easily adjust λ without giving up security and the equations:

$$\text{latency} = k \cdot \frac{1}{\lambda}, \qquad \text{throughput} = B \cdot \lambda,$$

We may ask, can we choose k or B to optimize latency and throughput?

- k **(confirmation depth):** In Nakamoto's security analysis (see his table), k is chosen to drive the double-spend probability down to an acceptably small level. In practice, clients with different risk tolerances can choose smaller or larger k; however reducing k directly reduces security. Thus, latency should not be reduced by reducing k as this sacrifices security.
- B **(block size):** Recall Δ (network delay) depends on
  1. *Propagation delay* Δ_c, dominated by speed-of-light c, roughly 0.1 s.
  2. *Processing delay* Δ_B, since each node must check and process blocks to avoid DDoS attacks, this processing delay scales linearly with block size B.

  Hence $\Delta = \Delta_c + \Delta_B$, where $\Delta_B \propto B$. However, since $\Delta_c \propto 1/c << \Delta_B$, $\Delta \propto B$. If we increase B to raise throughput ($B\lambda$), we also increase Δ, which in turn raises the forking rate $\lambda\,\Delta$ and thus lowers the security threshold. Consequently, Bitcoin cannot increase B without sacrificing security.

2 From PoW to PoS

We compare Proof-of-Work (PoW) with Proof-of-Stake (PoS):

Property	**Proof-of-Work (PoW)**	**Proof-of-Stake (PoS)**
Energy consumption	×	✓
Latency	×	✓ (sub-1-second latency achievable)
Accountability	×	✓ (can provably identify malicious actors)
Resistant to long-range attacks	✓	×