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

Lecture 6: Selfish Mining, Latency and Throughput

April 16, 2025

Lecturer: Prof. David Tse Scribe: Billy Gao

1 Mining Pools

Bitcoin's hash power is aggregated into large pools, e.g. FoundryUSA, AntPool and F2Pool, so that individual miners can trade uncertain payouts for a steady share of rewards. Without pooling, a miner with a low hash rate might wait years between blocks; in a pool it is paid in proportion to contributed shares. Each mined block pays a fixed block reward of 3.125 BTC, as well as the sum of transaction fees.

Every four years the reward halves until the asymptotic cap of 21×10^6 BTC is reached. Whether fees alone can maintain enough hash power is an open question.

Even though aggregate hash power has grown, the protocol still produces one block every ≈ 10 minutes. Every 2016 blocks the target hash is recalculated by effectively adding or removing leading zeros; so that the expected inter-block interval stays close to 600s.

2 Latency and Throughput

Let λ [blocks $\times$ s^{-1}] be the raw mining rate and B [tx $\times$ block^{-1}] the average block occupancy.

$$\text{Throughput} = B\lambda, \qquad \text{Latency}(k) = \frac{k}{\lambda},$$

with $\lambda = \frac{1}{600}$ and $k = 6$ giving ≈ 60 minutes for finality. Empirically $B \approx 2000$, so Bitcoin settles only $3-4$ tps versus Visa's $\sim 30\,000$ tps.

Nakamoto chose a very low λ so that the worst-case network delay Δ (seconds) is negligible in comparison to λ^{-1}.

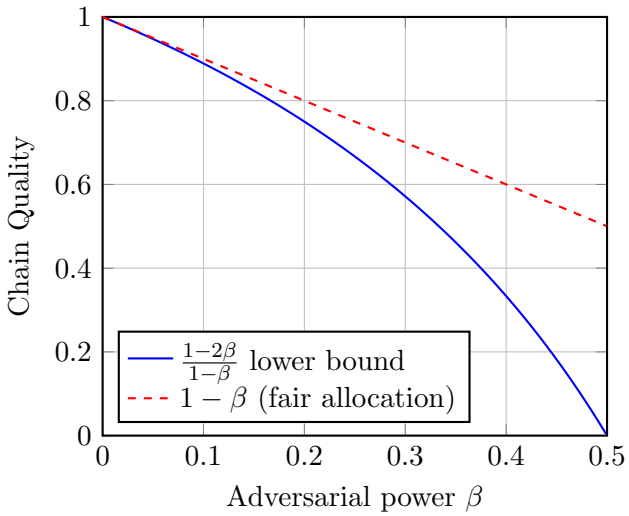
3 Chain Quality and Fair Allocation

Chain Quality (CQ) is the long-run fraction of blocks in the main chain that are mined by honest parties.

For adversarial power β

$$\text{CQ} \;\geq\; \frac{1-2\beta}{1-\beta} \;=\; 1 - \frac{\lambda_A}{\lambda_H},$$

producing the convex curve sketched in class that drops to 0 at $\beta = 0.5$. The straight line $1 - \beta$ represents fair allocation where hash share = block share.



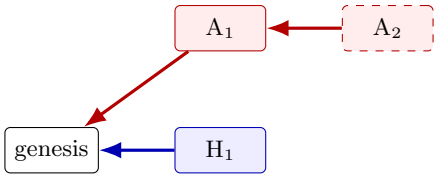
4 Selfish Mining (Eyal & Sirer)

Under the selfish-mining/greedy witholding strategy the attacker maintains a private fork and publishes it opportunistically.

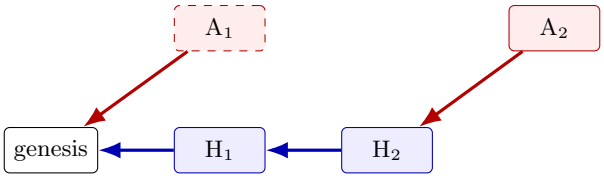
The attacker mines on its private tip, withholding newly-found blocks and increasing its lead. The attacker publishes exactly one block when an honest block appears while the lead is positive, creating a tie that honest miners resolve in the attacker's favour.

When the honest chain catches up before the attacker can extend its fork, the attacker abandons its private fork and immediately starts mining on top of the new honest block. This happens occasionally and ensures the attacker never commits effort to a branch that will certainly be orphaned. Therefore, the attacker never wastes a block, because every block it eventually reveals ends up on the main chain.

This strategy pushes CQ all the way down to the lower-bound curve, granting the attacker more than its hash-power share of rewards and providing a powerful economic incentive for pools to merge. At exactly $\beta = 0.5$ the attacker captures all rewards despite controlling only half the total hash power.



(a) Attacker withholds A_1; when honest block H_1 appears, it publishes A_1 to win the tie.



(b) If honest miners pull ahead, the attacker discards its fork and mines on the new public tip.

5 Latency and Throughput with Network Delay

Let Δ be worst-case message delay. Only miners who have received the latest block can extend the chain, so the effective growth rate is

$$\lambda_{\text{eff}} = \frac{\lambda}{1 + \lambda\Delta}.$$

As such,

$$\text{Latency}(k) \;=\; k\,\frac{1+\lambda\Delta}{\lambda}, \qquad \text{Throughput} \;=\; B\,\frac{\lambda}{1+\lambda\Delta}.$$

If $\lambda\Delta \ll 1$ (Bitcoin's current regime) these collapse to the earlier formulas.

6 Summary

Bitcoin's security model trades performance for robustness. Difficulty-adjusted PoW stabilises a 10-minute cadence, but leaves latency and throughput below modern expectations.