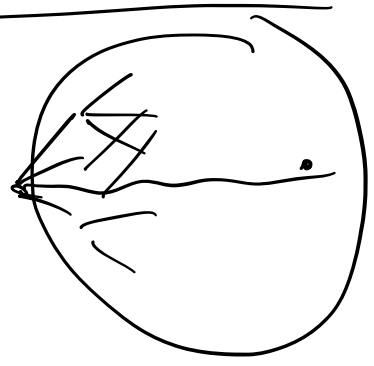
- Formal proof.
- Monetary incentives: → Selfish mining attack. Fruitchains.
- peer-to-peer network

---

longest chain wins rule:



- Mine on longest chain
- Send longest chain to all
- Commit blocks buried k deep.

Goal: Prove Nakamoto's Consensus solves SMR — not shown in Nakamoto's paper

Safety: Honest parties do not commit different blocks at the same height except with $e^{-o(k)}$.

Liveness: Every txn is eventually committed.

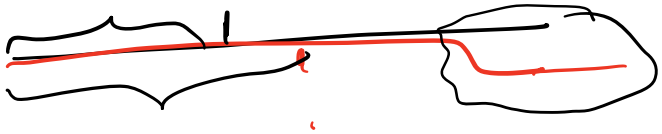
⇓

- (Growth / Quality) Prefix. ⇒ GKL'14 / PSS'16 / Ren'19
- Complex?

Chain growth:

Chain quality: Ratio of honest to malicious.

Chain prefix: Ignoring respective last k blocks any two honest parties have chains s.t. one is a prefix of another.



Model:

- Honest & Byzantine
- Synchronous n/w
  - Delay between $[0, \Delta]$
  - If peer-to-peer, account for diameter.
  - No lock-step.
  - Cannot be partial sync & async.
- Memoryless mining.
  - ↳ Poisson process: #events occuring in a fixed

interval of time if these events have a constant mean rate independent of previous event.

$[0, t]$, we have mean $\lambda t \sim$ 1 block. $\Leftrightarrow$ 10 mins

$Pr[T > t] = e^{-\lambda t}$; T: time to mine next block.

α, β: collective mining rate of honest & Byzantine.

- stable.
- $\alpha > \beta$.

Intuition

Liveness:

Safety: honest power > malicious power

honest chains grow faster, Byzantine cannot keep up.

Plan:

(A) Prove assuming $\Delta = 0$

(B) Reduce Δ-delay case to 0-delay case.

(A)

- Use notion of rounds
  - new round for every mined block.
- Each round has a unique leader.
  - Can two blocks be mined at the same time?
- p: probability of leader being honest $= \frac{\alpha}{\alpha+\beta}$.

  1-p: " " " malicious

Honest

- Always mines on the longest chain. & sends new block to everyone
- Since 0-delay, no two honest mine at the same height.

Malicious: Arbitrary.

Safety: A block committed under k-deep rule is safe except $e^{-O(k)}$ probability.

Proof:

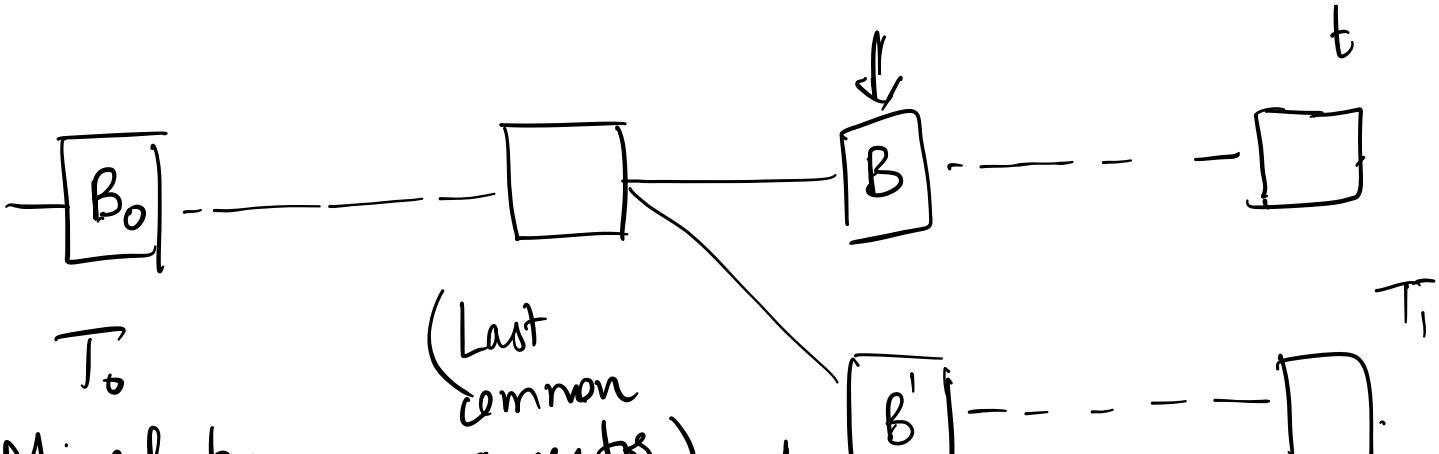
Some honest commits B in round t

B is mined by round t-k.

Can B lose its safety?

Suppose at $T_1 \geq t$, $B' \neq B$ is committed.
(first instance)

$T_0 \leq t-k$.



Mined by honest (Last common honest ancestor)

Both Adopt by honest at T_1 & buy $B_0 > k$

$[T_0, T_1]$: # malicious blocks $\geq$ # honest blocks
(honest blocks do not reside at same height)

Can B lose its safety?

Yes, if $\exists\, T_0 \leq t-k$. & $T_1 \geq t$, we have

malicious blocks $\geq$ # honest blocks.

Using appropriate distributions, happens with probability $e^{-f(k,\rho)}$

Whitepaper : (approximate analysis) :

$\frac{\alpha}{\beta} = 9$, $k = 6$, probability of attack ≈ 0.0009

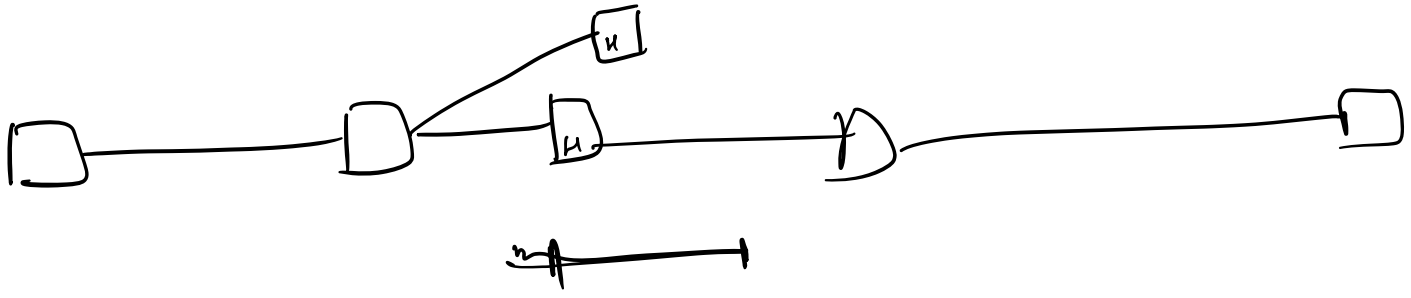
private Mining attack : 0.0018.

(B) Δ-delay case

0-delay: No two honest blocks reside at the same height.

Δ-delay: Honest blocks $> \Delta$ delay apart do not reside at the same height.

Lagger block: no other block mined in the last Δ time.



$$Pr[\text{lagger}] = e^{-(\alpha+\beta)\Delta}$$

(Recall $Pr[T > t] = e^{-\lambda t}$)

$$\Pr[\text{honest lagger}] = e^{-(\alpha+\beta)\Delta} \cdot \frac{\alpha}{\alpha+\beta}$$

Treat honest lagger as good
malicious / non-laggers as malicious.

Invoke 0-delay result with

$$p = e^{-(\alpha+\beta)\Delta} \cdot \frac{\alpha}{(\alpha+\beta)} \quad \left(\text{instead of } \frac{\alpha}{\alpha+\beta}\right)$$

Slow mining vs fast.