Lecture 8:
Longest-Chain Consensus

(Lecture Series on Foundations of Blockchains)

A Tale of Two Protocol Paradigms

Category #1: BFT-type protocols (e.g., Tendermint)

- canonical tool: multiple rounds of voting to ensure consistency
- ensure consistency, always (assuming < 33% Byzantine)
- very difficult to resolve forks in-protocol
  - ↳ due to software bugs, >33% Byzantine nodes, etc.

→ failure mode under attack: stall!

Category #2: longest-chain protocols (e.g., Bitcoin)

- no explicit voting, embrace forks as normal, resolve ambiguity in-protocol
- favor liveness over consistency during an attack
  - failure mode under attack: big chain reorganizations (e.g., Ethereum Classic)
    - enables double-spend attacks

Longest-Chain Consensus (Abstract)

→ primarily studied in synchronous model (bound Δ on max msg delay)

↳ relevant for: (i) permissioned + PKI (ii) permissionless, proof-of-work (iii) " , proof-of-stake

Pseudocode

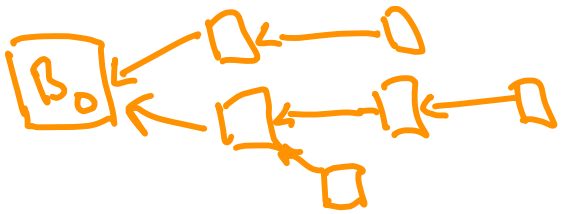
(1) hard-coded "genesis block" B_0

(2) in each "round" $r = 1, 2, 3, \ldots$

(2a) one node chosen as leader

(2b) leader can create a set of round-r blocks, each w/a predecessor block

Note: blocks form an in-tree:



"instant communication model ($\Delta = 0$)"

Assumptions

A1) (trusted setup) B_0 not chosen by or known in advance to Byzantine nodes.

A2) (to be enforced) Round-r leader can prove itself to other nodes. Non-leaders cannot masquerade as leader.

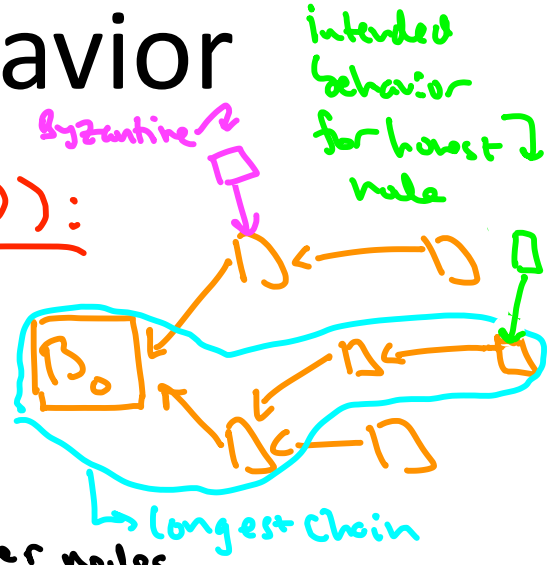
A3) (to be enforced) Nodes cannot manipulate their probability of being chosen as leader in (2a).

A4) (to be enforced) every round-r block's predecessor was created in some previous round.

(consequence: leader can only add one block to any given chain)

A5) (to be related) At all times, all honest nodes about exact same set of blocks.

Honest vs. Dishonest Behavior



Honest node behavior in block proposal step (step ③):

(i) form block $B :=$ all known pending transactions

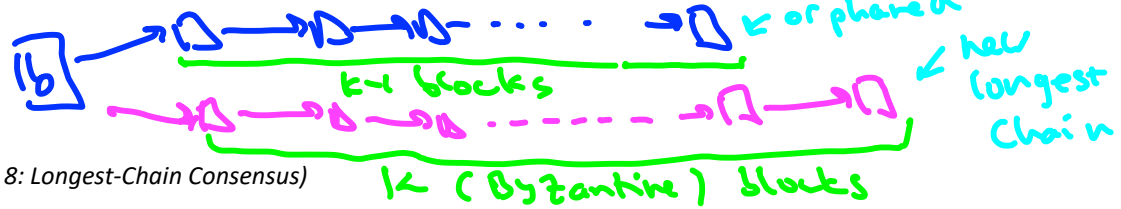
(ii) set predecessor $:=$ end of current longest chain
(break ties among longest chains arbitrarily)

(iii) immediately broadcast B (+ specified predecessor) to all other nodes

Byzantine node: can deviate from any of (i)-(iii), but must commit to B & pred at the time it's selected as a leader.

Note: doomed unless $f < \frac{n}{2}$.

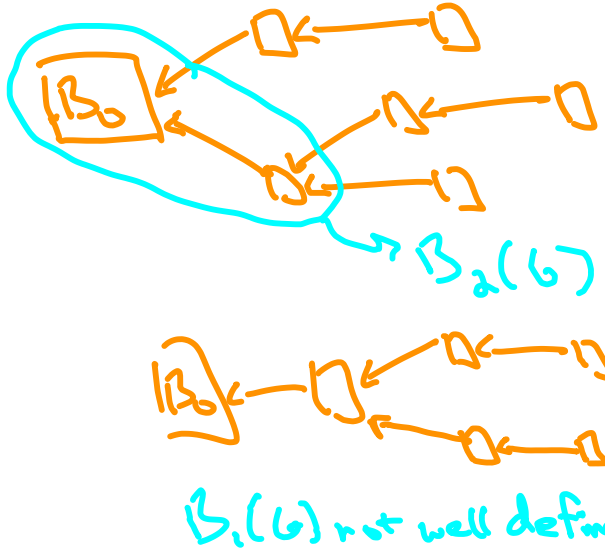
Note: k Byzantine leaders in a row $\Rightarrow$ can "cancel" last $k-1$ blocks



Which Blocks Are Finalized?

Goal: $\forall \langle n \rangle_2 \Rightarrow$ all but last k blocks on longest chain can be (for some k, TBD) considered finalized (i.e., won't be cancelled/rolled back later).

call this $B_k(G)$, where G = current in-tree



Note: k not part of protocol description (up to the user).

Note: not clear $B_k(G)$ is well defined.

honest node
dastardly node

Definition: a sequence $l_1, l_2, \ldots \in \{H, A\}$ is w-balanced if, in every window $l_i, l_{i+1}, \ldots, l_j$ of length at least w, strict majority are honest.

- want w as small as possible (will control time til tx confirmation)
- conceivably holds (for suff. large w) if $\geq 51\%$ honest nodes.

Implications of Balanced Leader Sequences

Assume: "super-synchronous" model, all msgs delivered instantaneously. ($\approx \Delta = 0$)
$\Rightarrow$ trivializes consistency between nodes, but not self-consistency (a.ka. finality)

Fact: all results extend (with some work) to the usual synchronous model.
(see [Garay/Kiayias/Leonardos 15] and [Pass/Seeman/shelat 16])
- need to assume rate of block production slow relative to max msg delay Δ
($\Rightarrow$ inadvertant honest forks rarely occur)

Theorem: if a leader sequence is $2k$-balanced, for every possible sequence $G_0, G_1, G_2, \ldots$

Common prefix property: for all i, $B_k(G_i)$ is well defined;

finality: $B_k(G_0) \subseteq B_k(G_1) \subseteq B_k(G_2) \subseteq B_k(G_3) \subseteq \cdots$ (once confirmed, always confirmed)

liveness: if a tx is known to all honest nodes, will eventually be included in $B_k(G)$.

Random Leaders Are Balanced

Note: # of nodes n plays no role!

Good news: expect randomly chosen leaders to be reasonably balanced.

Bad news: stuck with nonzero (but hopefully astronomically small) failure probability.
⇒ forced to settle for probabilistic guarantees (e.g., probabilistic finality)

Notation: α = fraction of nodes that are Byzantine. (Assume $\alpha < 1/2$.)

Note: for any window of consecutive leaders, expect a $1-\alpha > \frac{1}{2}$ fraction to be honest (on average).

Intuition: bigger window length w ⇒ bigger gap $(1-2\alpha)w$ between expected # of honest vs. Byzantine nodes ⇒ bigger buffer to absorb variation around expectation ⇒ less likely to see ≥ 50% Byzantine nodes.

Math: $\Pr[\text{a given length-}w\text{ window is } \geq 50\% \text{ Byzantine}] \leq e^{-cw}$ (c = some constant)
depend on α

$\Rightarrow \Pr[\text{any window of length} \geq w \text{ is} \geq 50\% \text{ Byzantine}] \leq T^2 e^{-cw}$ (Union bound)

$\Rightarrow$ get failure probability $\leq \delta$ as long as $w \geq c_2(\ln T + \ln 1/\delta)$. ($c_2$ = some constant)

Balanced Leaders → Common Prefix

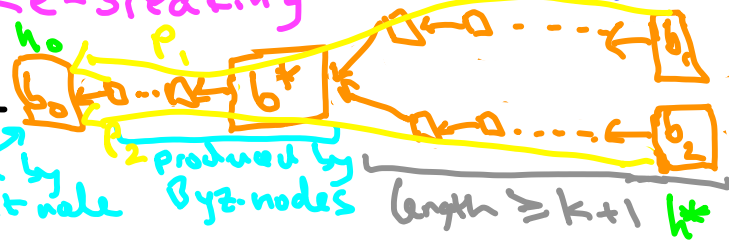
Theorem 1: (common prefix property) if leader sequence is $2k$-balanced, for any possible outcome G, $D_k(G)$ well defined.

pick a longest chain, lop off last k blocks

ranges over Byzantine node strategies + honest tie-breaking

b-balanced = strict majority of honest leaders in all windows of length $\geq w$

Proof: if not, possible that current in-tree G^* looks like



- Let b_0 = first honestly produced ancestor of b^*
- Let r_0 = round in which b_0 created (+announced)
- Let G_0 = in-tree after round r_0, h_0 = b_0's height (ie., # hops from genesis block)

Defn: for H "in between" G_0 & G^*, $\Phi(H) := \min \{$ # of blocks created on ρ_1, # of blocks created on $\rho_2 \}$

[So $\Phi(G_0) = 0$, $\Phi(G^*) = h^* - h_0$] $\geq k+1$

plan: $\geq 50\%$ of leaders between G_0 & G^* Byzantine (contradicts balance)

- note: honest leaders never increase Φ [don't create any blocks on the "stem"; always extend longer of ρ_1, ρ_2]
- note: a Byzantine leader can increase Φ by at most 1 (follows from assumption A4!)

$\Rightarrow$ must have been at least $h^* - h_0$ Byzantine leaders after round r_0 [by A4, b_0 honestly created, announced immediately

- note: at most $h^* - h_0$ honest leaders in this window [why? never have 2 honestly produced blocks at same height] (uses assumption A5)

↳ $\geq 50\%$ Byzantine!

QED!

→ So if leader sequence is balanced with high probability (as in proof-of-work / proof-of-stake) => get finality also w.h.p. ("probabilistic finality")

Balanced Leaders → Finality

Theorem 2: (finality) if leader sequence is $2k$-balanced, for any possible outcome sequence $G_0, G_1, G_2, \ldots$,

ranges over Byzantine node strategies + honest tie-breaking

$$B_k(G_0) \subseteq B_k(G_1) \subseteq B_k(G_2) \subseteq \cdots.$$

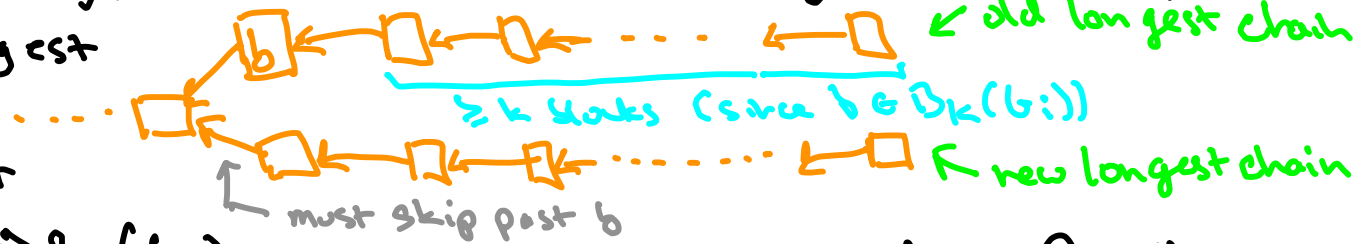
w-balanced = strict majority of honest leaders in all windows of length $\geq w$

Proof: Suppose block b belongs to $B_k(G_i)$ but not $B_k(G_j)$ for some $j > i$.

=> b belongs to every longest chain of G_i (>k blocks deep, even), no longest chain of G_j

=> let $h \in \{i+1, i+2, \ldots, j\}$ be first index such that $\exists$ longest chain in G_h that excludes b:

=> G_h has two longest chains that disagree on last $\geq k+1$ blocks => $B_k(G_h)$ not well defined => contradicts Thm 1.



QED!

Balanced Leaders → Liveness

w-balanced = strict majority of honest leaders in all windows of length ≥ w

Theorem 3: (liveness) if leader sequence is $2k$-balanced, whenever a tx is known to all honest nodes, will eventually be included in $B_k(G)$.

Proof: Define an epoch as $2k$ consecutive rounds (+ their leaders).

[by $2k$-balancedness, $\geq k+1$ honest leaders & $\leq k-1$ Byzantine leaders in each epoch]

- note: every honest leaders add 1 to length of longest chain (since extend longest chain)
- note: each Byzantine leader contributes ≤ 1 block to any given chain (by assumption A4)

$\Rightarrow$ after T epochs, longest chain contains $\geq (k+1)T$ blocks, of which $\leq (k-1)T$ are contributed by Byzantine nodes

$\Rightarrow \geq 2T$ blocks on longest chain produced by honest nodes

$\Rightarrow \geq 2T-k$ of these have been finalized

$\Rightarrow$ honest blocks finalized infinitely often

$\Rightarrow$ a tx known to all honest nodes will eventually be finalized.

QED!

Chain Quality

Note: might have hoped for $1-\alpha$ rather than $\frac{1-2\alpha}{1-\alpha}$. (see Lecture 10 for the full story)

Possible stronger liveness guarantees: (i) assume tx known to only one honest node (⇒ Thm 3 becomes false!) (ii) quantitative bounds on time til finalization (interesting, too for a field) (iii) lower bound fraction of honestly produced blocks on longest chain

Revised analysis of randomly chosen leaders:

$\Pr[\text{Any window of length} \geq w \text{ is } \geq (\alpha+\varepsilon) \text{ fraction Byzantine}] \leq \delta$

as long as $w \geq c(\ln T + \ln \frac{1}{\delta})$ (constant depends on ε)

⇒ i.e., leader sequence is $(w, \alpha+\varepsilon)$-balanced with probability $\geq 1-\delta$

Theorem 3': if leader sequence is $(2k, \alpha+\varepsilon)$-balanced ($\alpha+\varepsilon < 1/2$), then fraction of blocks on longest chain produced by honest leaders $\geq \frac{1-2\alpha-2\varepsilon}{1-\alpha-\varepsilon}$

Thm 3 special case of $\alpha+\varepsilon \approx 1/2$

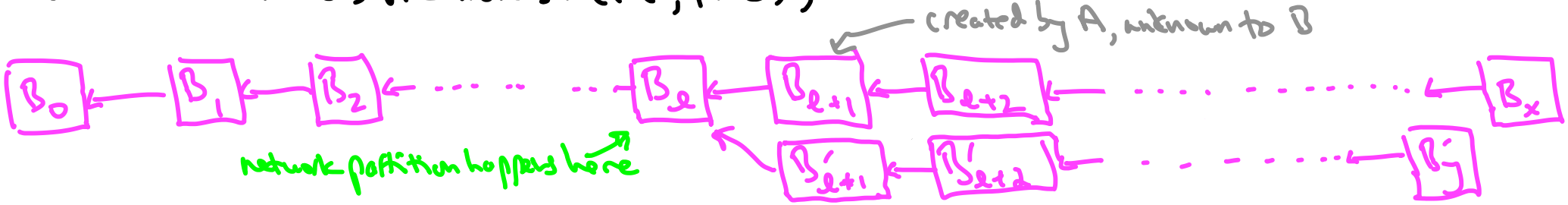
Proof: ⇒ after T epochs, longest chain length $\geq 2k(1-\alpha-\varepsilon)T$, of which $\leq 2k(\alpha+\varepsilon)T$ contributed by Byzantine leaders.

$$\Rightarrow \geq \frac{2k(1-\alpha-\varepsilon)T - 2k(\alpha+\varepsilon)T}{2k(1-\alpha-\varepsilon)T} = \frac{1-2\alpha-2\varepsilon}{1-\alpha-\varepsilon}$$ fraction of blocks honestly produced.

QED!

What About Partial Synchrony?

Note: finality of longest-chain consensus breaks down in partially synchronous model.
(even if all nodes are honest (i.e., $f=0$))



⇒ once branch length exceeds k, lose common prefix property

⇒ once network partition ends, violate finality

network partition

Note: longest-chain consensus still makes progress with a network partition.

⇒ "favors liveness over safety" (fail via reorgs)

(cf. BFT-type protocols which stall under attack (not enough votes))

↳ ⇒ "favors safety over liveness" (fail by stalling)

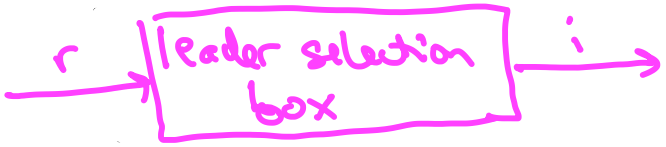
Toward Permissionless Consensus

Pseudocode

(1) hard-coded "genesis block" B_0
[not known in advance to Byz. nodes]

(2) for each "round" $r = 1, 2, 3, \ldots$

(2a) some node i selected as "leader"



(2b) node i specifies set of blocks, each with a predecessor from some previous round

Key takeaways

(1) balanced leader sequence
$\Rightarrow$ consistency + liveness. [taking $k = w/\alpha$]

w-balanced = strict majority of honest leaders in every window of length $\geq w$

[did not use the permissioned assumption]

(2) if in each round r,
$\Pr[\text{round-}r \text{ leader is Byzantine}] \leq \alpha$
for some $\alpha < 1/2$, leader sequences will be balanced with high probability.
[parameter w increases as α tends to $1/2$]