

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

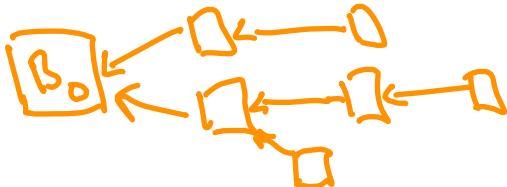
(bound Δ on max msg delay)

↳ 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" $r=1, 2, 3, \dots$
 - ②a one node chosen as leader
 - ②b leader can create a set of round- r blocks, each w/o 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)

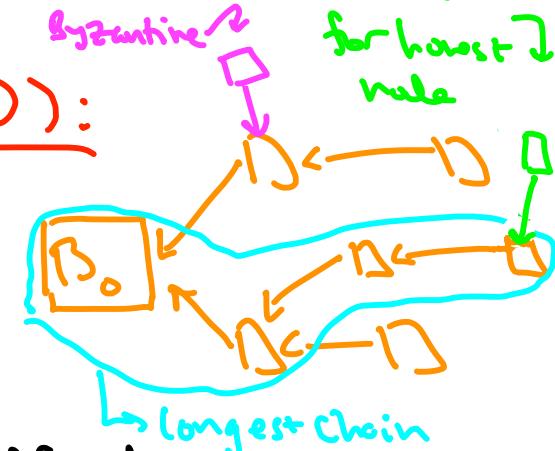
(iii) immediately broadcast B (+specified predecessor) to all other nodes

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

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



intended behavior for honest node



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

Which Blocks Are Finalized?

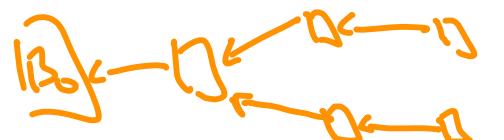
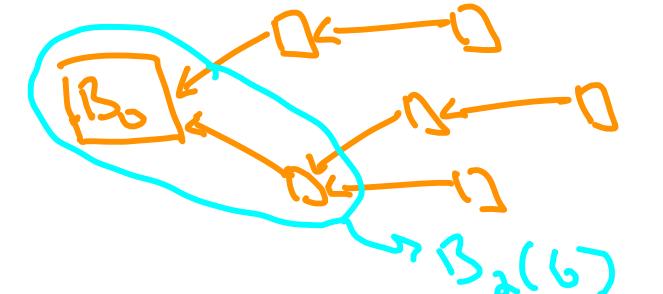
Goal: $f < n/2 \Rightarrow$ all but last k blocks on longest chain can be (for some k, TBD) considered finalized (i.e., won't be cancelled/rolled back later).
Call this $B_{k\ell}(G)$, where $G = \text{current in-tree}$

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

Note: not clear $B_{k\ell}(G)$ is well defined.

Definition: A sequence $l_1, l_2, \dots \in \{H, A\}^*$ is w -balanced if, in every window l_i, l_{i+1}, \dots, 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.



$B_{k\ell}(G)$ not well defined

Implications of Balanced Leader Sequences

Assume: "super-synchronous" model, all msgs delivered instantaneously. ($\tilde{\Delta} = 0$)
⇒ trivializes consistency between nodes, but not self-consistency (a.k.a. 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
(⇒ inadvertent honest forks rarely occur)

holds
in PoW
setting

will prove under assumption (A4')
(holds also under (A4), via stronger balancedness assumption)

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

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

(once confirmed,
always confirmed)

finality: $B_k(G_0) \subseteq B_k(G_1) \subseteq B_k(G_2) \subseteq B_k(G_3) \subseteq \dots$

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

which
holds w.h.p.
for random
leaders

Note: # of nodes n plays no role!

Random Leaders Are Balanced

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 $w \Rightarrow$ bigger gap $((1-\alpha)\omega)$ between expected # of honest vs. Byzantine nodes ⇒ bigger buffer to absorb variation around expectation ⇒ less likely to see $\geq 50\%$ Byzantine nodes.

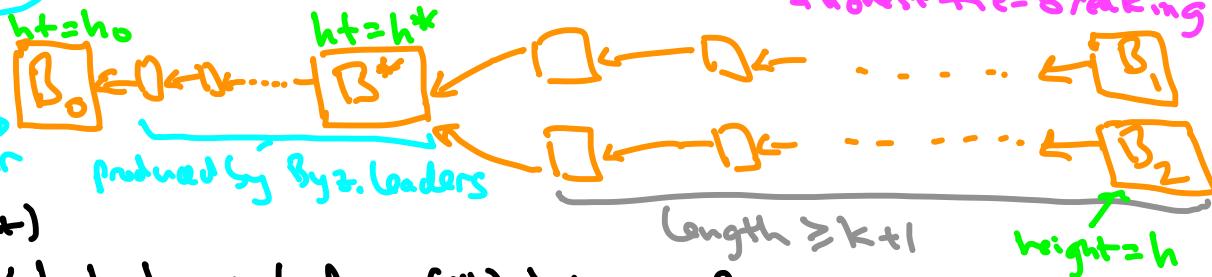
Math: $\Pr\{\text{a given length-}w\text{ window is } \geq 50\%\text{ Byzantine}\} \leq e^{-c_1 w}$ (c_1 = some constant)
 $\Rightarrow \Pr\{\text{any window of length } \geq w \text{ is } \geq 50\%\text{ Byzantine}\} \leq T^2 e^{-c_1 w}$ (Union Bound)
 \Rightarrow get failure probability $\leq \delta$ as long as $w \geq c_2(\ln T + \ln \frac{1}{\delta})$. (c_2 = some constant)

Balanced Leaders → Common Prefix

pick alongst chain,
top off lost k blocks

Theorem 1: (common prefix property) if leader sequence is $(2k+2)$ -balanced + assumptions (A1), (A1t'), (AS) hold, for any possible in-tree (known to (all) honest nodes), $B_k(w)$ is well defined. ranges over Byzantine node strategies + honest tie-breaking
 (uses assumption (AS))

Proof: if not, current in-tree could be exists by (A1)! → produced by honest leader



r_0 = round of B_0 's creation (announcement)

Claim: (i) $\geq 2k+2$ leaders after r_0 (ii) $\leq h-h_0$ honest leaders (iii) $\geq h-h_0$ Byzantine leaders

all orange blocks produced after round r_0 , $\geq 2k+2$ such blocks, done by (A4')

all produce blocks of heights h_0+1, \dots, h , at most one per height

* orange blocks produced by Byz. leaders

$$\geq (h^*-h_0) + (h-h^*)$$

by defn of B_0

by 'Proposition'

⇒ by (A4'), $\geq h-h_0$ distinct Byz. leaders

Tim Roughgarden

QED!

Proposition: the heights of honestly produced blocks strictly increase over time. (uses assumption (AS))

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

Balanced Leaders \rightarrow Finality

Theorem 2: (finality): if leader sequence is $2k$ -balanced,
for any possible outcome sequence G_0, G_1, G_2, \dots ,
 ranges over Byzantine node strategies + honest tie-breaking
 $B_k(G_0) \subseteq B_k(G_1) \subseteq B_k(G_2) \subseteq \dots$

Unbalanced =
 strict majority of
 honest leaders in all
 windows of length $\geq n$

Proof: Suppose block b belongs to $B_k(G_i)$ but not $B_k(G_j)$ for some $j > i$.
 $\Rightarrow b$ belongs to every longest chain of G_i ($> k$ blocks deep, even), no longest chain of G_j
 \Rightarrow let $h \in \{i+1, i+2, \dots, j\}$ be first index such that longest chain in G_h that excludes b :
 $\Rightarrow G_h$ has two longest chains that disagree on last $\geq k$ blocks (since $b \in B_k(G_i)$)
 $\Rightarrow k+1$ blocks $\Rightarrow B_{k+1}(G_h)$ not well defined \Rightarrow contradicts Thm 1.

Balanced Leaders \rightarrow Liveness

Theorem 3: (Liveness) if leader sequence is $2k$ -balanced,

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

w-balanced =

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

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

[By $2k$ -balancedness, $\geq k+1$ honest leaders $\in \leq k-1$ 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

$\Rightarrow \geq 2T$ blocks on longest chain produced by honest nodes contributed by Byzantine 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 (\Rightarrow Thm 3 becomes false!)
 - (ii) quantitative bounds on time til finalization (interesting, too far afield)
 - (iii) lower bound fraction of honestly produced blocks on longest chain

Revised analysis of randomly chosen leaders:

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

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

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

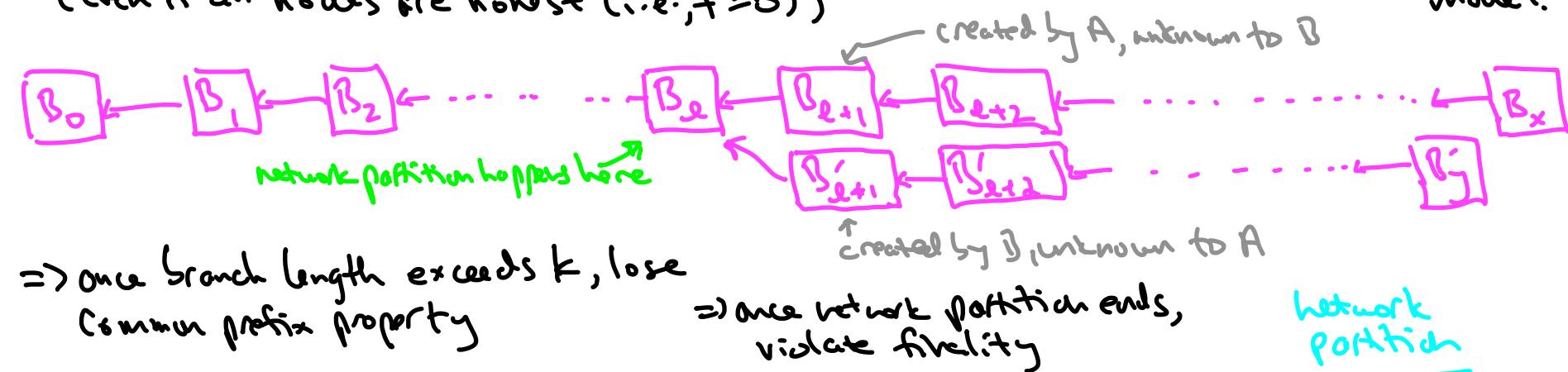
Proof: \Rightarrow after T epochs, longest chain length $\geq 2k(1-\alpha-\varepsilon)T$, of which $\leq 2k(\alpha+\varepsilon)T$

$$\Rightarrow \frac{2k((1-\alpha-\varepsilon)T - 2k(\alpha+\varepsilon)T)}{2k((1-\alpha-\varepsilon)T)} = \frac{1-2\alpha-2\varepsilon}{1-\alpha-\varepsilon} \text{ fraction of blocks contributed by Byzantine leaders.}$$

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., $f=0$))



network partition

Note: longest-chain consensus still makes progress with a network partition.
 \Rightarrow "favors liveness over safety" (fail via reorgs)
(cf. GFT-type protocols which stall under attack (not enough votes))
 $\hookrightarrow \Rightarrow$ "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" $r = 1, 2, 3, \dots$
- ②a some node i selected as "leader"


A pink-bordered box labeled "Leader selection box". An arrow labeled "r" points to the top edge of the box. An arrow labeled "i" points from the bottom right corner of the box.
- ②b node i specifies set of blocks,
each with a predecessor from some previous
round

Key takeaways

- ① balanced leader sequence
⇒ consistency + liveness. [taking $k = w/a$]
[did not use the permissioned assumption]
- ② if in each round r ,
 $\Pr[\text{round-}r \text{ leader is Byzantine}] \leq \alpha$
for some $\alpha < \frac{1}{2}$, leader sequences will be
balanced with high probability.
[parameter w increases as α tends to $\frac{1}{2}$]

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