Streamlet:
Textbook Streamlined Blockchains

Benjamin Chan
Cornell University

Joint work with Elaine Shi

cbr.stanford.edu/sbc20/

“Simplifying Consensus”

Benjamin Chan
Cornell University

Joint work with Elaine Shi

1. Modeling consensus (5min)
2. Motivating simplicity as a goal (a few seconds)
3. Our protocol (20min)

1. Modeling consensus (5min)
2. Motivating simplicity as a goal (a few seconds)
3. Our protocol (20min)

Goal: walk away

1. Modeling consensus (5min)
2. Motivating simplicity as a goal (a few seconds)
3. Our protocol (20min)

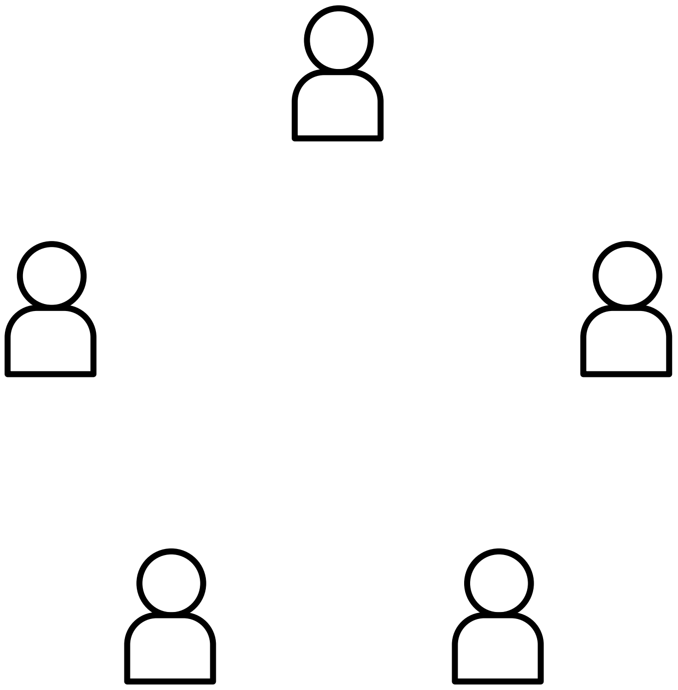
Goal: walk away

and understand a consensus protocol

What is consensus?

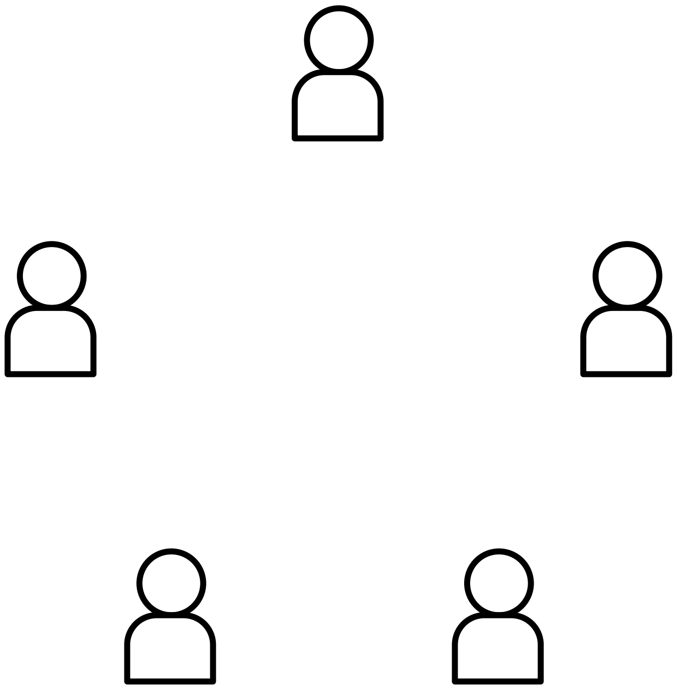
~~What is consensus?~~ Modeling Blockchain

Modeling Blockchain



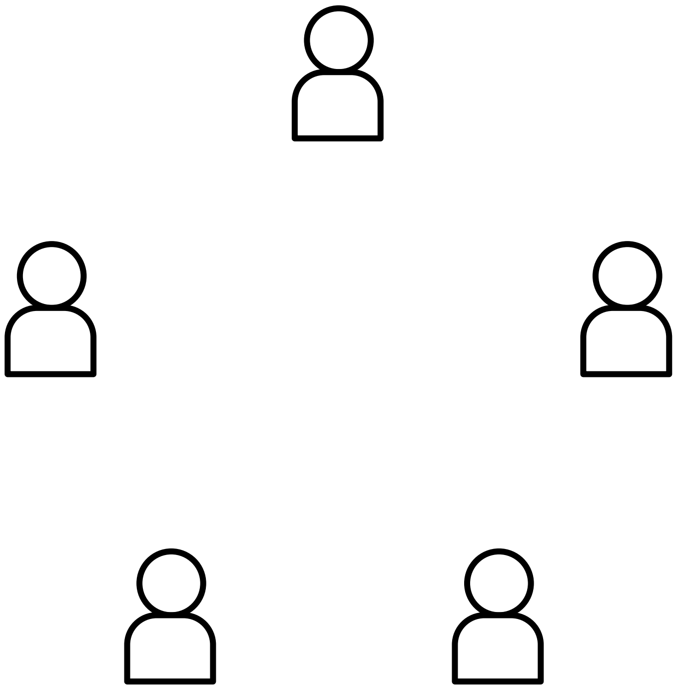
Modeling Blockchain

- Some *known* set of users
    - “permissioned”



Modeling Blockchain

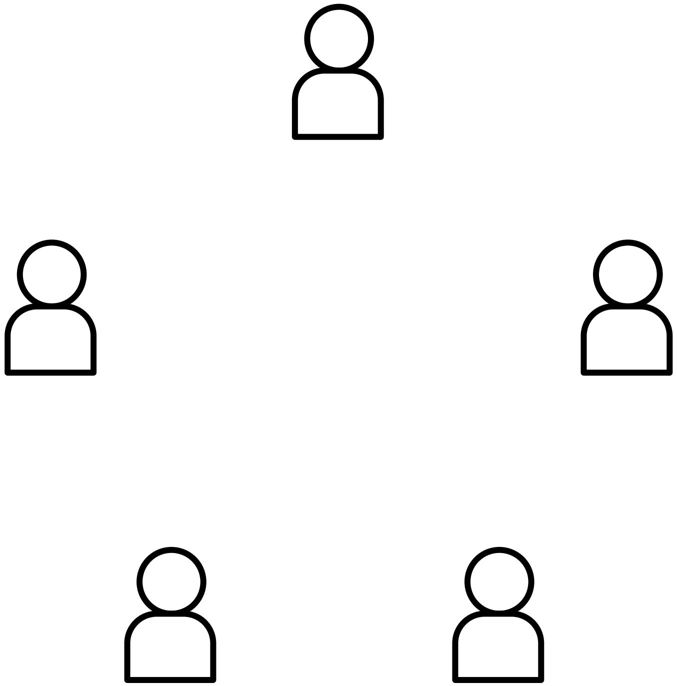
Why the permissioned setting?



Modeling Blockchain

Why the permissioned setting?

Answer: Proof-of-Stake

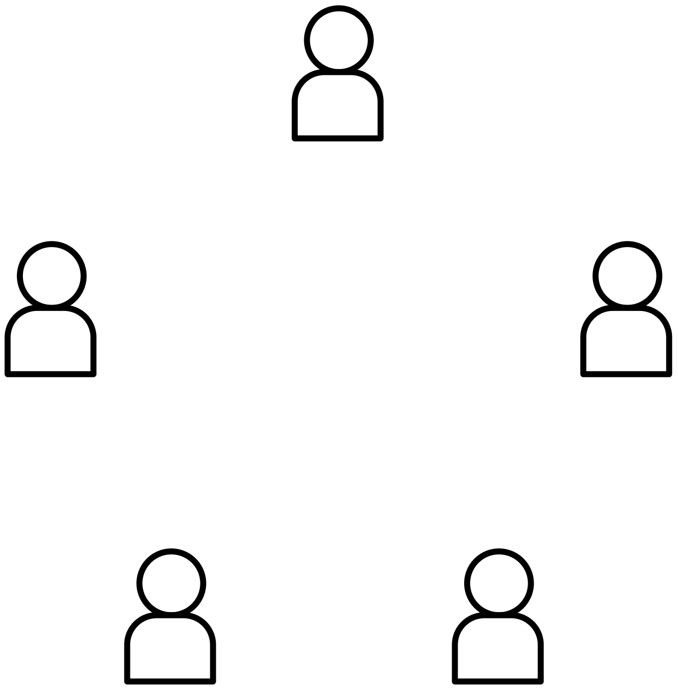


Modeling Blockchain

Why the permissioned setting?

Answer: Proof-of-Stake

Different setting than PoW!!

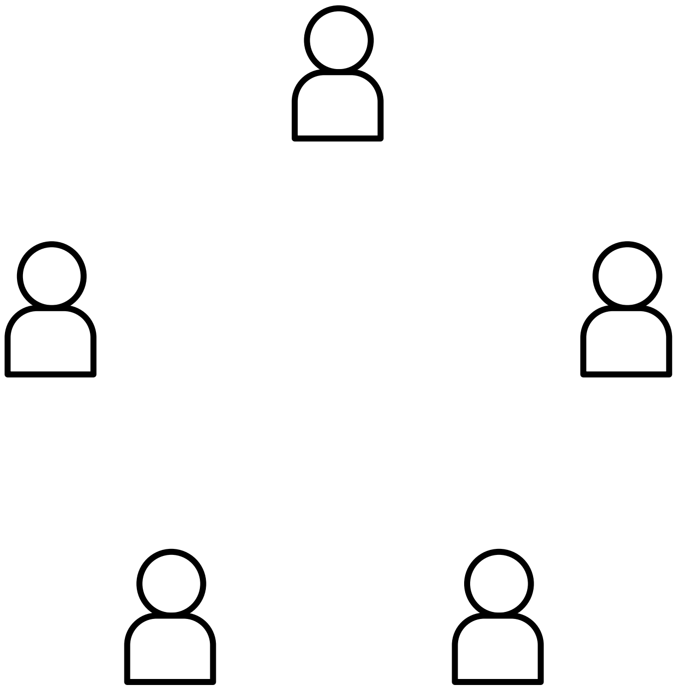


Modeling Blockchain

Why the permissioned setting?

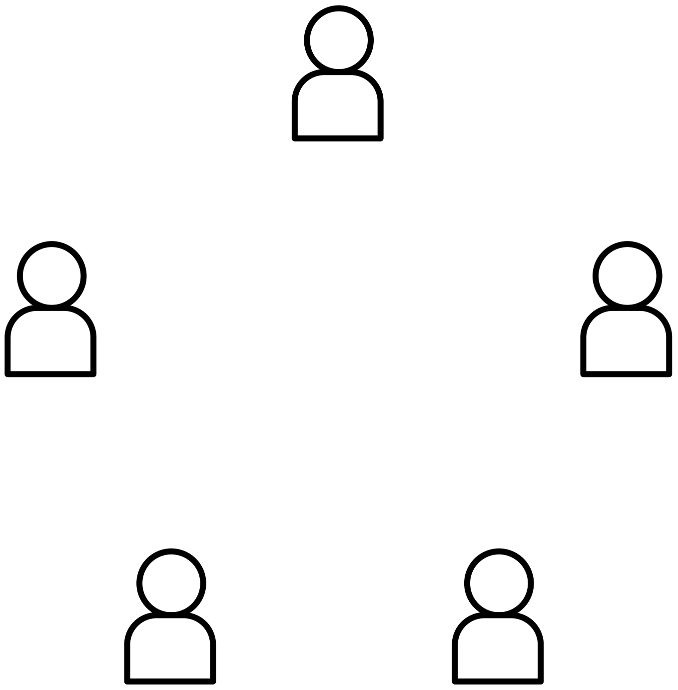
Answer: Proof-of-Stake

Different setting than PoW!! (true finality, speed, partition-resistant)



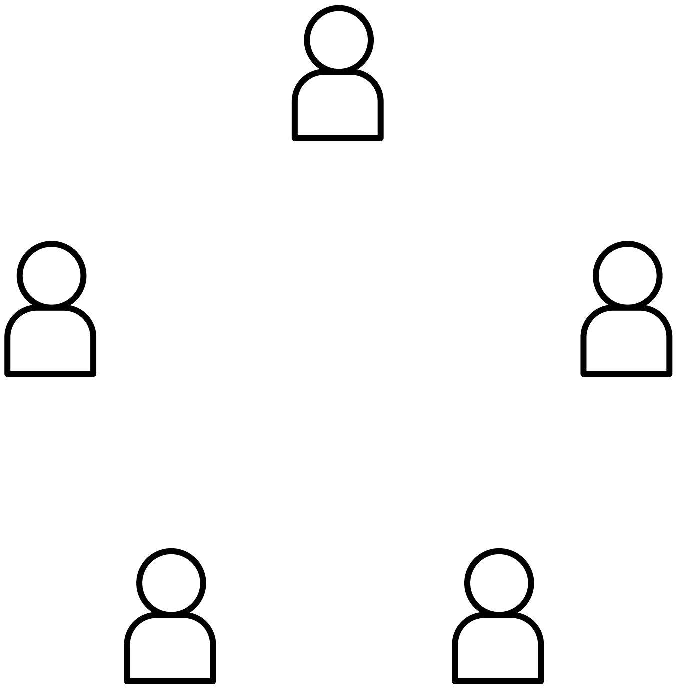
Modeling Blockchain

- Some *known* set of users
  - “permissioned”



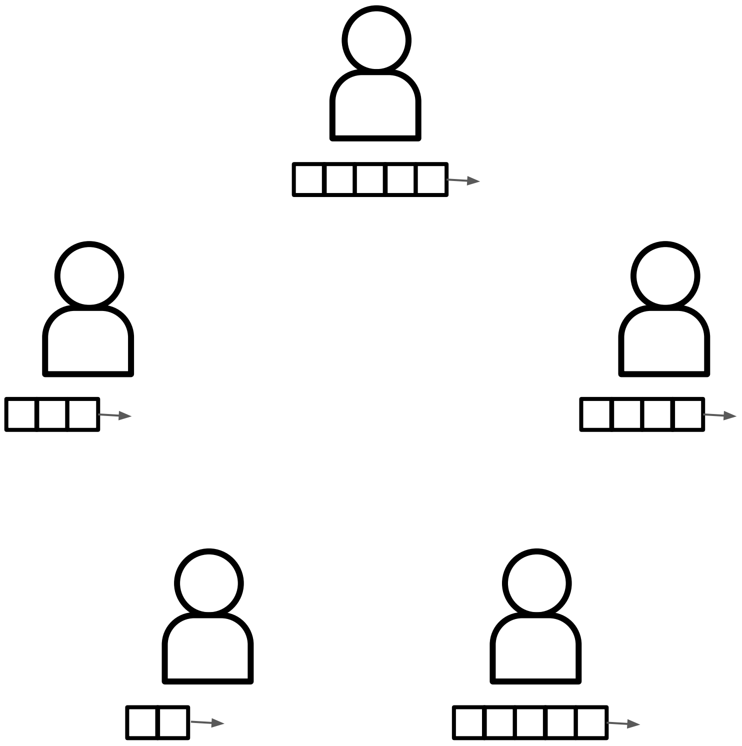
Modeling Blockchain

- Some *known* set of users
  - "permissioned"
- Each user maintains ordered chain of blocks



Modeling Blockchain

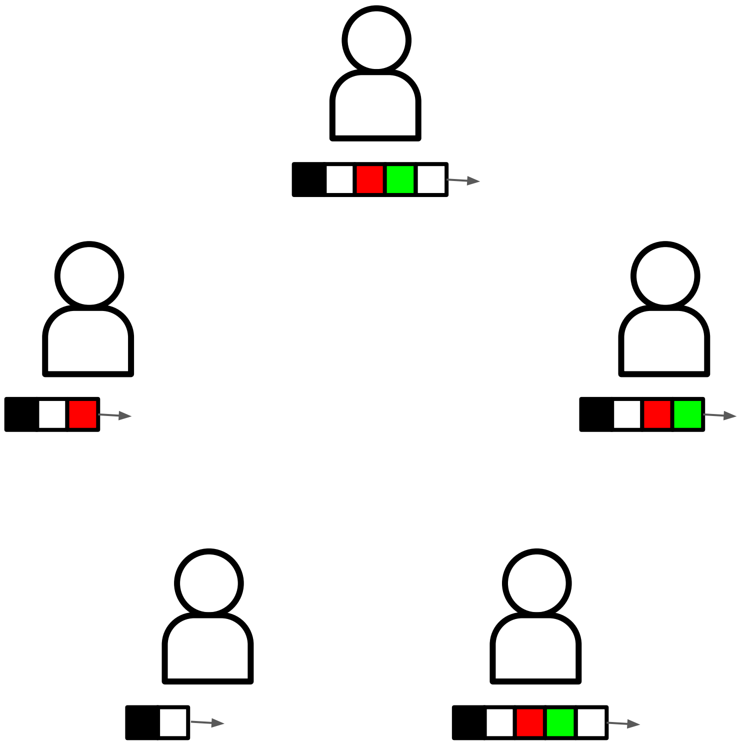
- Some *known* set of users
  - "permissioned"
- Each user maintains ordered chain of blocks



Modeling Blockchain

- Some *known* set of users
  - "permissioned"
- Each user maintains ordered chain of blocks

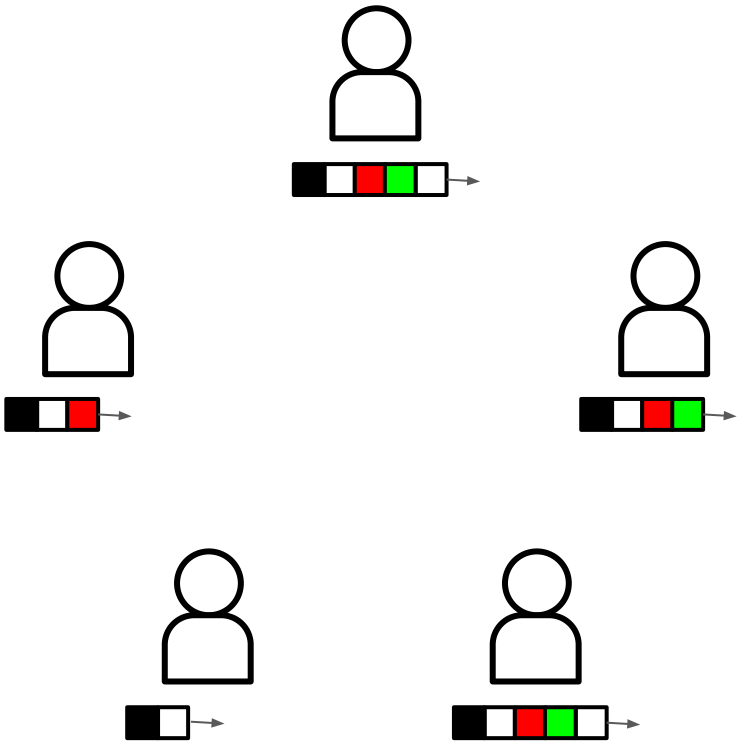
- Consistency: Everyone sees a prefix of the same chain!



Modeling Blockchain

- Some *known* set of users
  - "permissioned"
- Each user maintains ordered chain of blocks

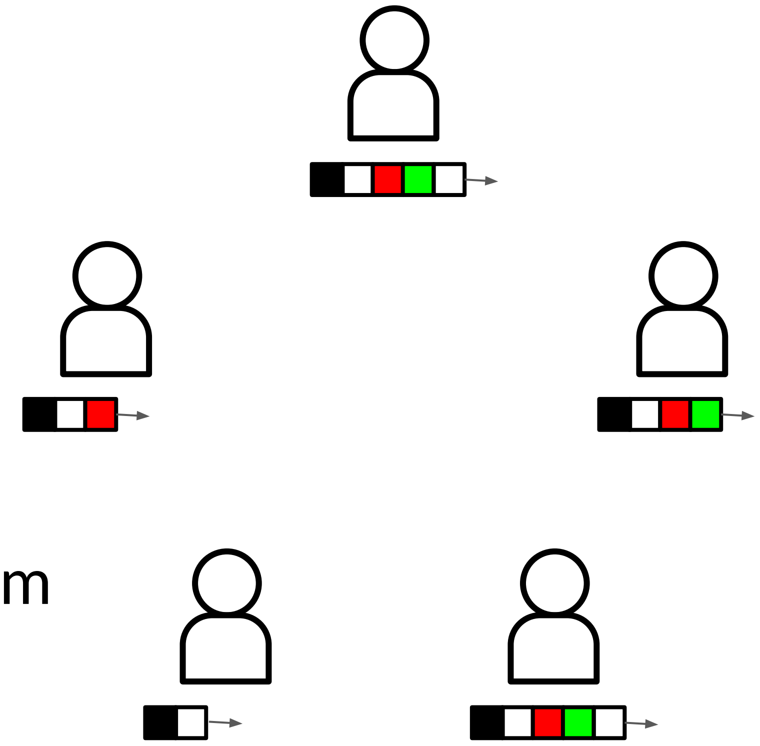
- <u>Consistency</u>
- <u>Liveness</u>



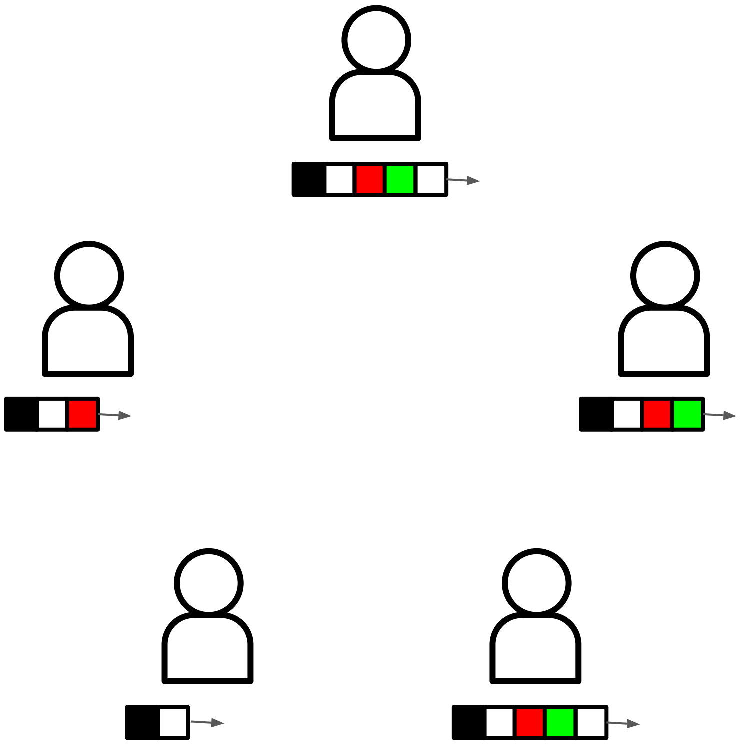
Modeling Blockchain

- Some *known* set of users
  - “permissioned”
- Each user maintains ordered chain of blocks

- <u>Consistency</u>
- <u>Liveness:</u> must be able to confirm new blocks

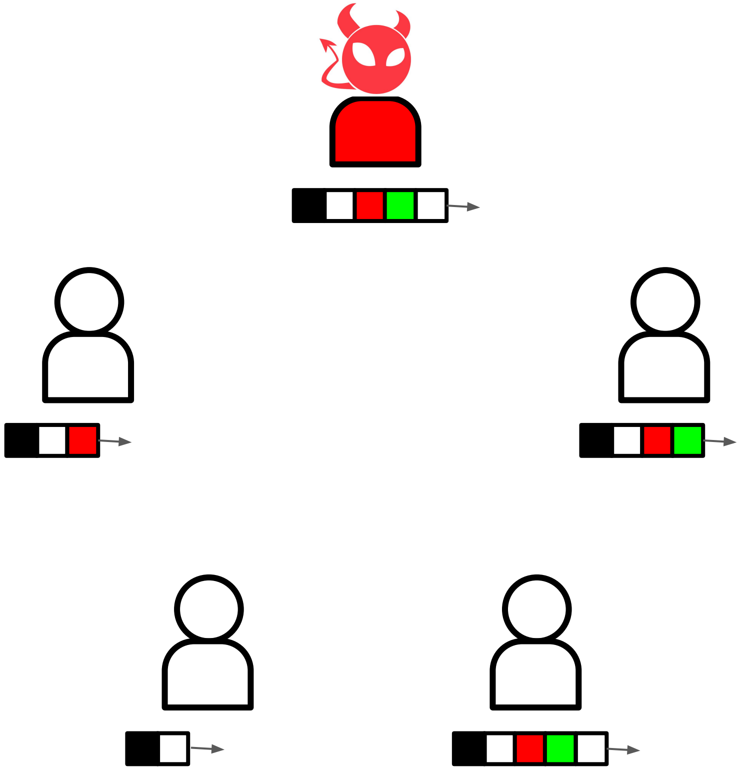


Introducing adversaries



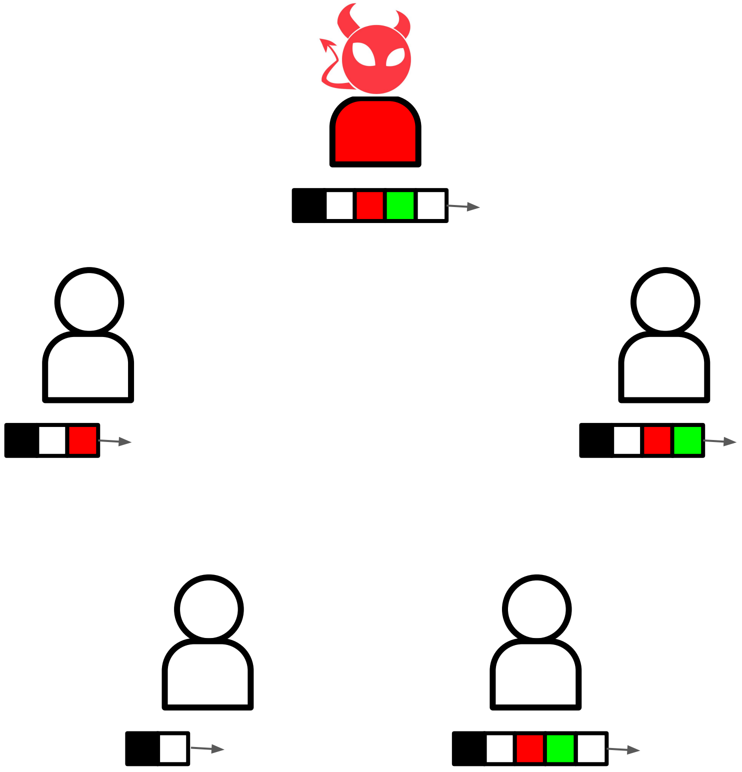
Introducing adversaries

- Malicious users



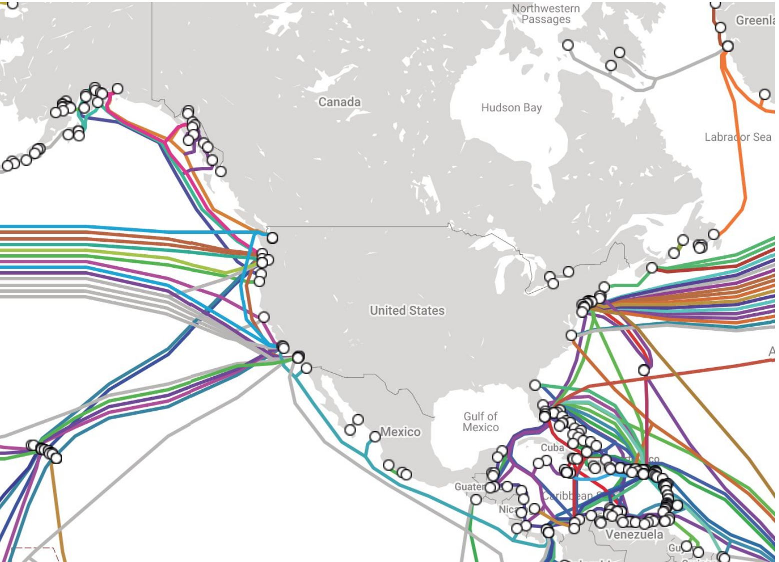
Introducing adversaries

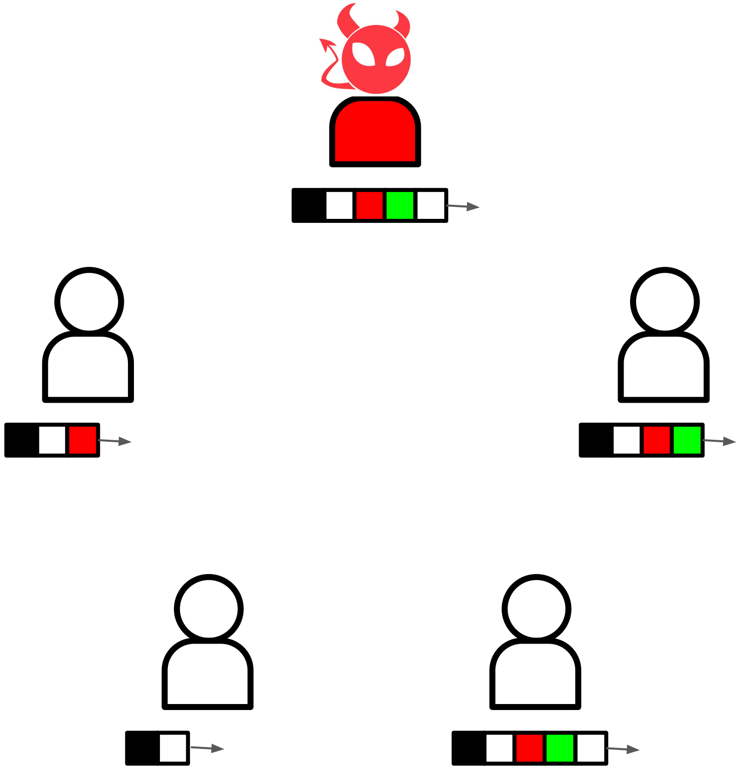
- Malicious users
- Messages may be lost, delayed, reordered

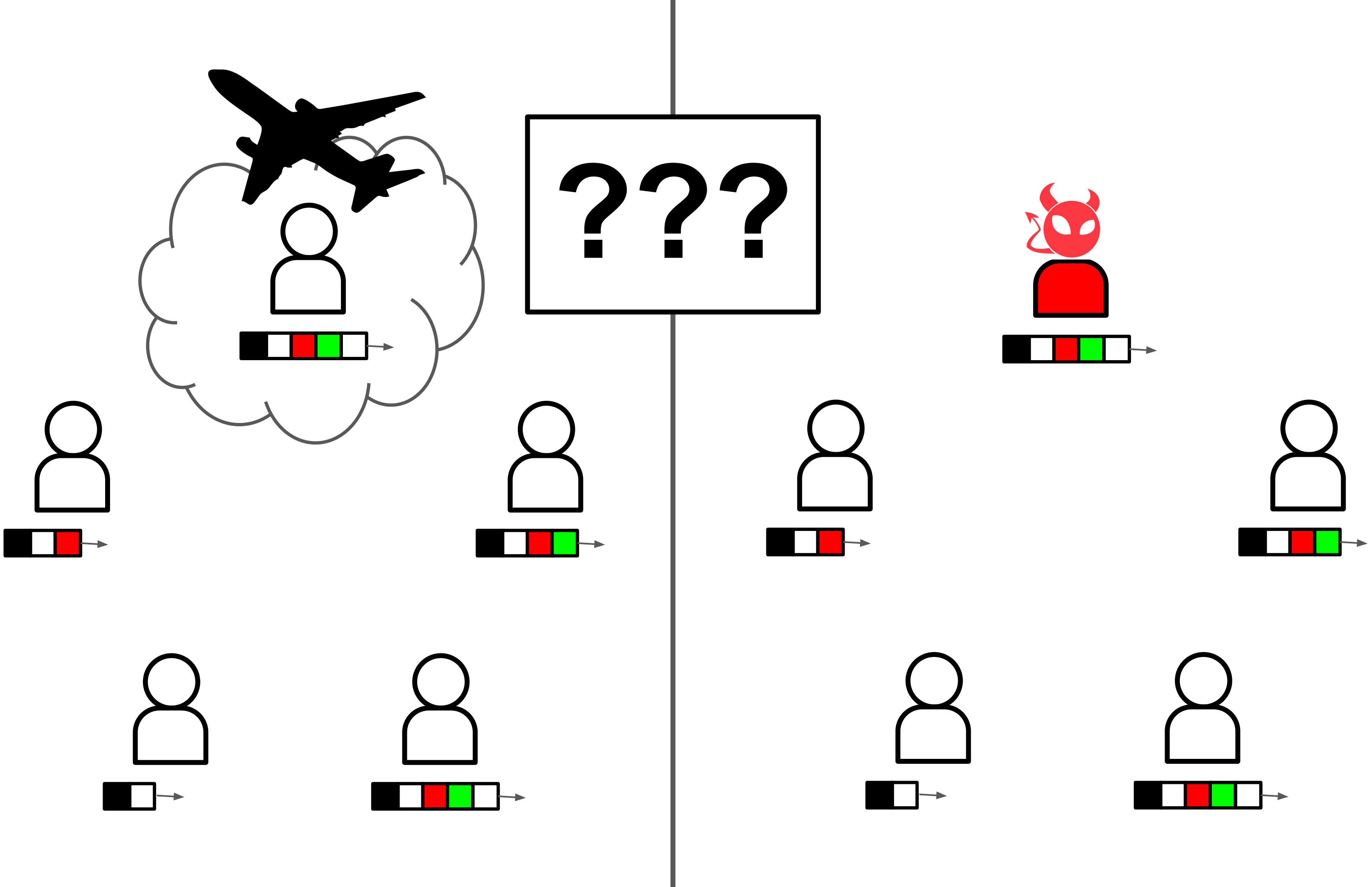


Introducing adversaries

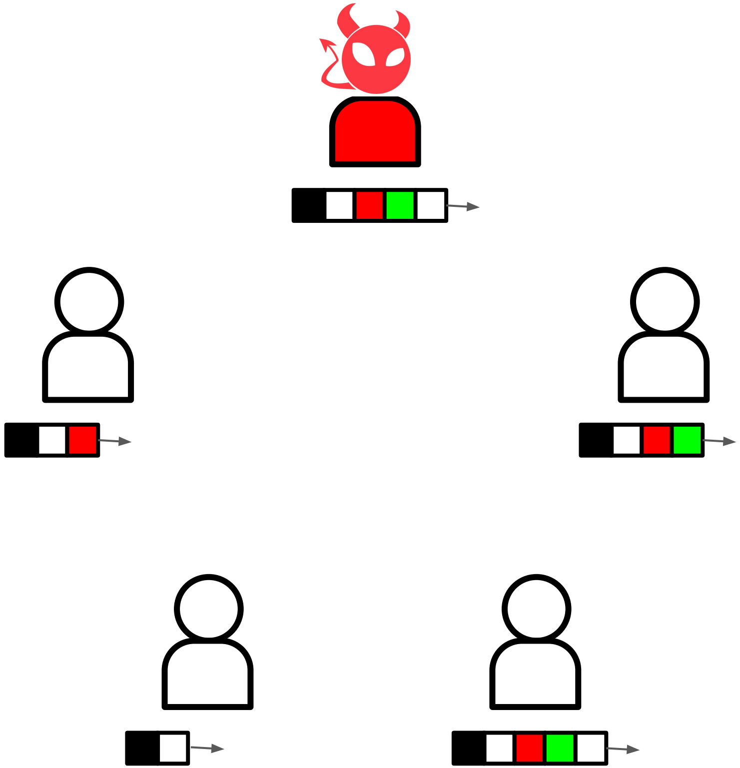
- Malicious users
- Messages may be lost, delayed, reordered







This problem is notoriously hard!



This problem is notoriously hard!

- Paxos (‘70s)
- PBFT (‘99)
- Raft (2014)

This problem is notoriously hard!

- Paxos (‘70s) - “Paxos Made Simple”, “ABCDs of Paxos” (2001)
- PBFT (‘99)
- Raft (2014)

This problem is notoriously hard!

- Paxos (‘70s) - “Paxos Made Simple”, “ABCDs of Paxos” (2001)
- PBFT (‘99) - “Hotstuff” (2018)
- Raft (2014)

This problem is notoriously hard!

- Paxos (‘70s) - “Paxos Made Simple”, “ABCDs of Paxos” (2001)
- PBFT (‘99) - “Hotstuff” (2018)
- Raft (2014) - “Raft Refloated: Do We Have Consensus?” (2014)

This problem is notoriously hard!

- Paxos (‘70s) - “Paxos Made Simple”, “ABCDs of Paxos” (2001)
- PBFT (‘99) - “Hotstuff” (2018)
- Raft (2014) - “Raft Refloated: Do We Have Consensus?” (2014)
- Blockchains (2016+)
  - Dfinity
  - Casper
  - Algorand
  - Hotstuff
  - Pala

This problem is notoriously hard!

- Paxos (‘70s) - “Paxos Made Simple”, “ABCDs of Paxos” (2001)
- PBFT (‘99) - “Hotstuff” (2018)
- Raft (2014) - “Raft Refloated: Do We Have Consensus?” (2014)
- Blockchains (2016+)
    - Dfinity
    - Casper
    - Algorand
    - Hotstuff
    - Pala

New “streamlined” paradigms...

This problem is notoriously hard!

- Paxos ('70s) - "Paxos Made Simple", "ABCDs of Paxos" (2001)
- PBFT ('99) - "Hotstuff" (2018)
- Raft (2014) - "Raft Refloated: Do We Have Consensus?" (2014)
- Blockchains (2016+)
  - Dfinity
  - Casper
  - Algorand
  - Hotstuff
  - Pala

New "streamlined" paradigms...

...but can we eliminate the subtleties?

Motivating Simpler Consensus Protocols

Motivating Simpler Consensus Protocols

- Simpler Implementation

Motivating Simpler Consensus Protocols

- Simpler Implementation
- Fewer Bugs

Motivating Simpler Consensus Protocols

- Simpler Implementation
- Fewer Bugs
- Lower onboarding cost
- Better Open Source

Motivating Simpler Consensus Protocols

- Simpler Implementation
- Fewer Bugs
- Lower onboarding cost
- Better Open Source
- $$$

Motivating Simpler Consensus

- Simpler Implementation
- Fewer Bugs
- Lower onboarding cost
- Better Open Source
- $$$

Motivating Simpler Consensus

- Simpler Implementation
- Fewer Bugs
- Lower onboarding cost
- Better Open Source
- $$$

Motivating Simpler Consensus R

- Simpler Implementation
- Fewer Bugs
- Lower onboarding cost
- Better Open Source
- $$$

Motivating S

- Simpler Im
- Fewer Bugs
- Lower onbo
- Better Ope
- $$$

Images: Encyclopedia Brittanica, greekmythology.com
King of Hearts / Wikimedia Commons

Our Work: Streamlet

Our Work: Streamlet

Goal:
A “Simplest Possible”,
Easy-to-Understand,
Textbook Consensus Protocol

Our Work: Streamlet

Goal:
A "Simplest Possible",
Easy-to-Understand,
Textbook Consensus Protocol (Blockchain)

Our Work: Streamlet

Two Assumptions:

1. **Epochs**
   Processes have local clocks,
   and run in synchronized* epochs of 1 sec each.

Our Work: Streamlet

Two Assumptions:

1. **<u>Epochs</u>**
   Processes have local clocks,
   and run in synchronized* epochs of 1 sec each.
2. **<u>Elect a leader in each epoch, known by all</u>**

Our Work: Streamlet

Two Assumptions:

1. **Epochs**
   Processes have local clocks,
   and run in synchronized* epochs of 1 sec each.
2. **Elect a leader in each epoch, known by all**
   i.e. randomly chosen, given epoch e
   $L_e = H(e) \bmod n$

Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions

Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \text{txs})$

Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$

pointer to parent block

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$

Epoch number in which
block was 'proposed'

Assumptions:

- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$

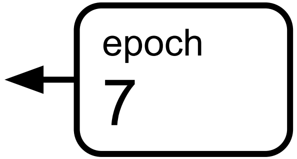
Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

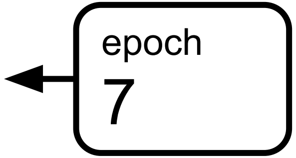


Definitions

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block

Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

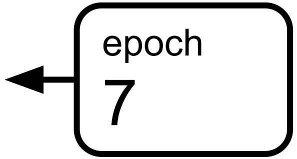


Assumptions:

- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions

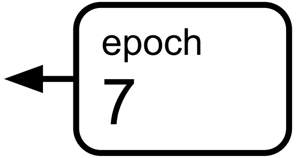
- Block $b = (H(b'), e, \text{txs})$
- Notarized block
  - A block ‘signed’ by ⅔ distinct processes



Definitions

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

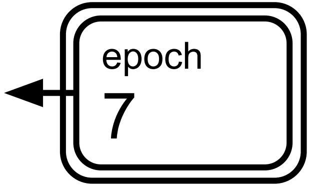
- Block $b = (H(b'), e, \text{txs})$
- Notarized block
    - A block ‘signed’ by ⅔ distinct processes (implies a majority of honest processes have signed it)



Definitions

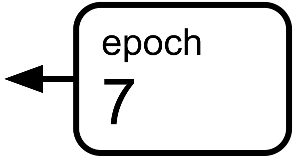
Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
    - A block ‘signed’ by ⅔ distinct processes



Definitions

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
  - A block ‘signed’ by ⅔ distinct processes

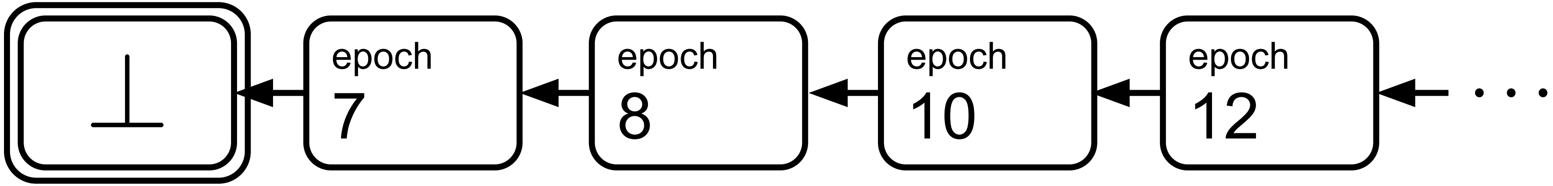


Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
  - A block ‘signed’ by ⅔ distinct processes

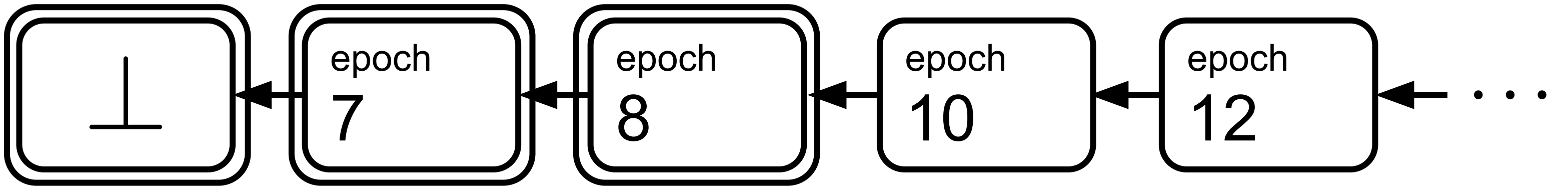
Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader



Definitions

- Block $b = (H(b'), e, \text{txs})$
- Notarized block
  - A block ‘signed’ by ⅔ distinct processes
- Notarized blockchain

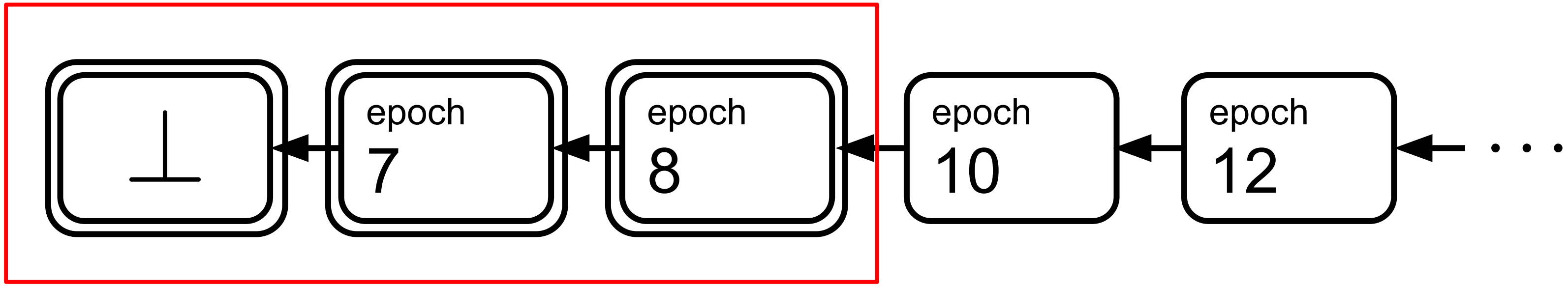
Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader



Definitions

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
  - A block 'signed' by ⅔ distinct processes
- Notarized blockchain

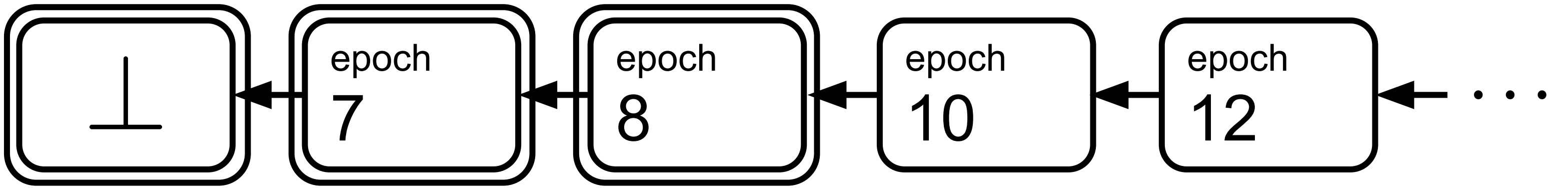
Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader



Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions

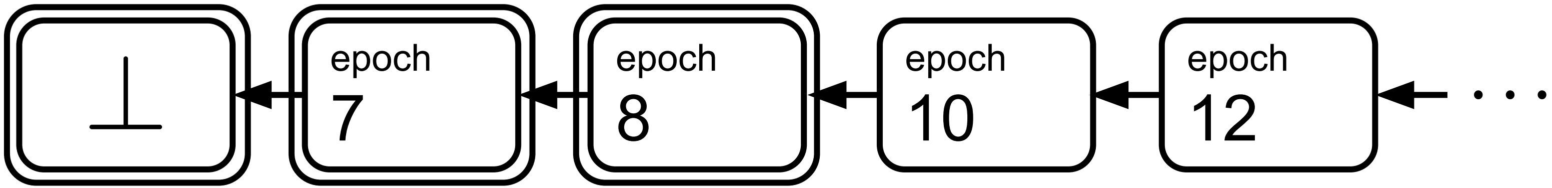
- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
  - A block ‘signed’ by ⅔ distinct processes
- Notarized blockchain



Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block
  - A block 'signed' by ⅔ distinct processes
- Notarized blockchain
- Block "height" ≠ epoch #

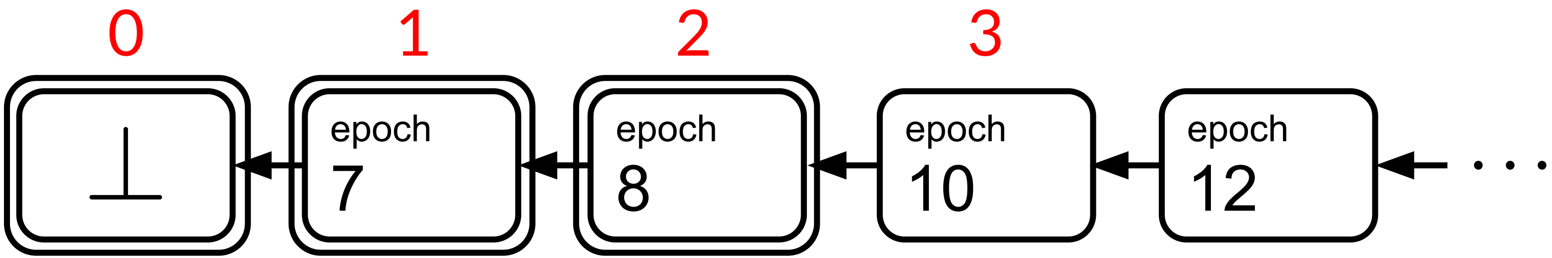


Definitions

- Block $b = (H(b'), e, \text{txs})$
- Notarized block
  - A block 'signed' by ⅔ distinct processes
- Notarized blockchain
- Block "height" ≠ epoch #

Assumptions:

- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader



Assumptions:

- (Synchronized*) epochs of length 1 sec
- Each epoch has random leader

Definitions:

- Block $b = (H(b'), e, \mathrm{txs})$
- Notarized block: signed by 2/3 processes

The Streamlet Protocol

Assumptions:

- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions:

- ❏ Block $b = (H(b'), e, \text{txs})$
- ❏ Notarized block: signed by 2/3 processes

The Streamlet Protocol

In every epoch $e = 1, 2, \ldots$

Assumptions:
- ❑ (Synchronized*) epochs of length 1 sec
- ❑ Each epoch has random leader

Definitions:
- ❑ Block $b = (H(b'), e, \mathrm{txs})$
- ❑ Notarized block: signed by 2/3 processes

The Streamlet Protocol

In every epoch $e = 1, 2, \ldots$

- **leader**,
  creates a new block *b* = (*H*(*b'*), *e*, txs)
  extending longest notarized chain they've seen so far

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions:
- ❏ Block $b = (H(b'), e, \mathrm{txs})$
- ❏ Notarized block: signed by 2/3 processes

The Streamlet Protocol

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions:
- ❏ Block $b = (H(b'), e, \text{txs})$
- ❏ Notarized block: signed by 2/3 processes

In every epoch $e = 1, 2, \ldots$

- **<u>leader</u>**,
  creates a new block *b* = (*H*(*b'*), *e*, txs)
  extending longest notarized chain they've seen so far

- **<u>voters</u>**,
  signs first proposal *b* (from leader, for *e*)
  i.f.f. *b* extends a longest notarized chain seen so far (by voter)

The Streamlet Protocol

Assumptions:
- (Synchronized*) epochs of length 1 sec
- Each epoch has random leader

Definitions:
- Block $b = (H(b'), e, \text{txs})$
- Notarized block: signed by 2/3 processes

<u>**finalization rule**</u>:

The Streamlet Protocol

<u>finalization rule</u>:
take any notarized chain
that ends in 3 consecutive epochs;

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions:
- ❏ Block $b = (H(b'), e, \text{txs})$
- ❏ Notarized block: signed by 2/3 processes

The Streamlet Protocol

Assumptions:
- ❏ (Synchronized*) epochs of length 1 sec
- ❏ Each epoch has random leader

Definitions:
- ❏ Block $b = (H(b'), e, \text{txs})$
- ❏ Notarized block: signed by 2/3 processes

finalization rule:
take any notarized chain
that ends in 3 consecutive epochs;
chop off the last block,
and finalize

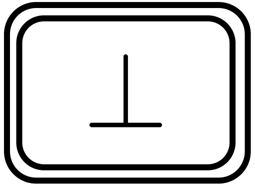
Example

In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

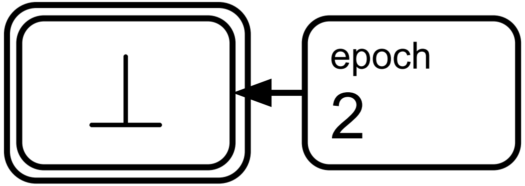


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

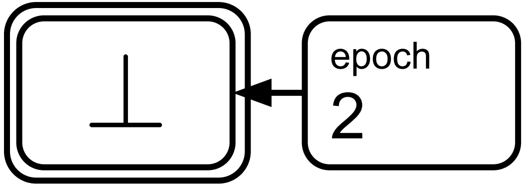


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example (3 honest, 1 malicious)

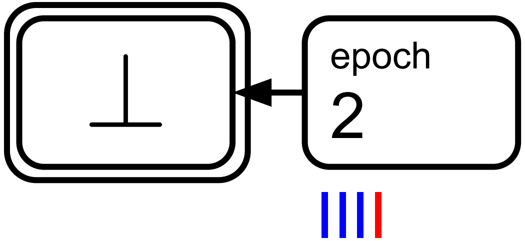


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example (3 honest, 1 malicious)

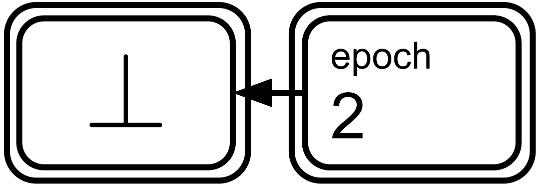


In every epoch $e = 1, 2, ...$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

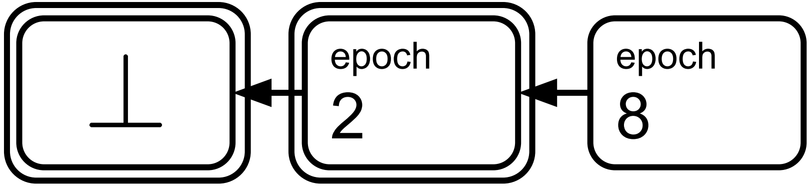


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

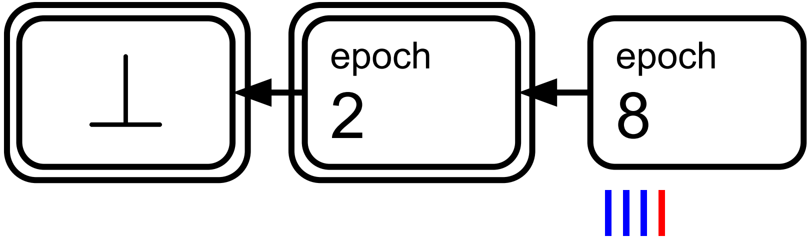


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

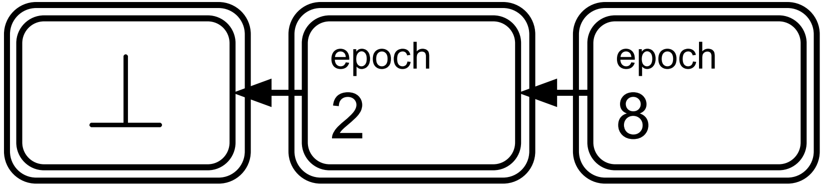


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

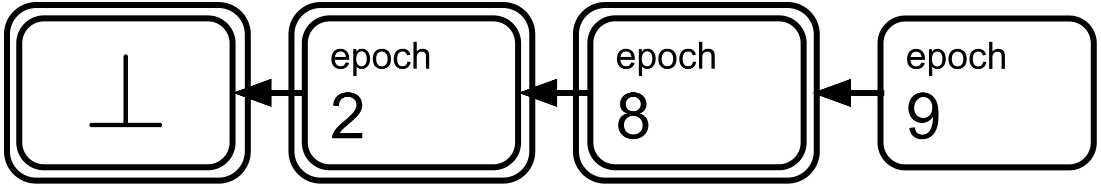


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

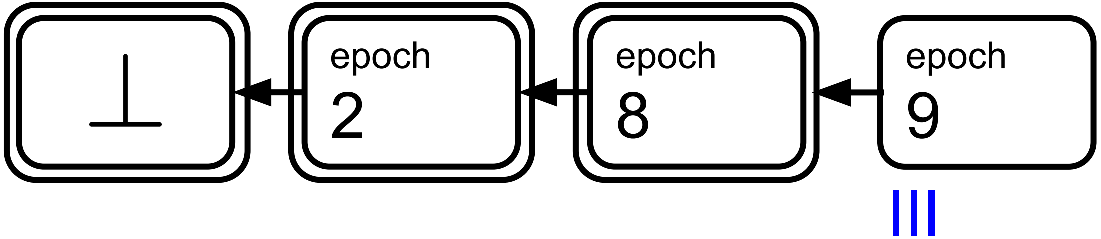


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

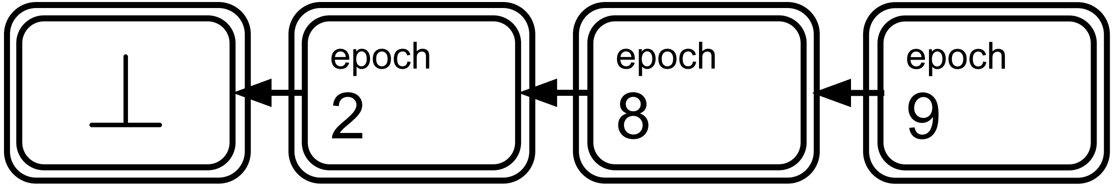


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

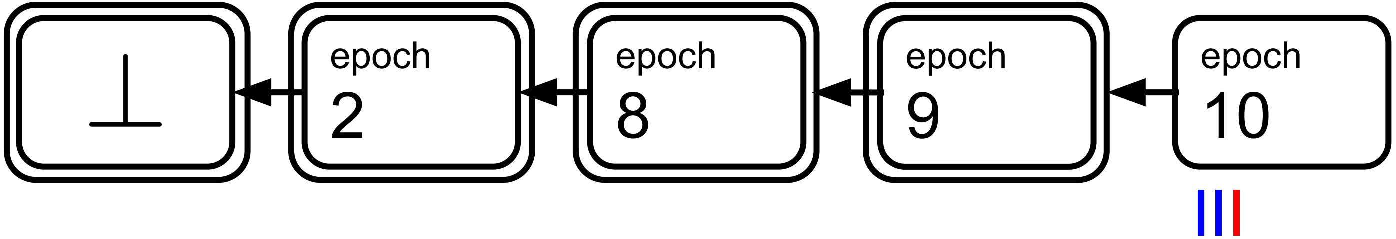


In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example



In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

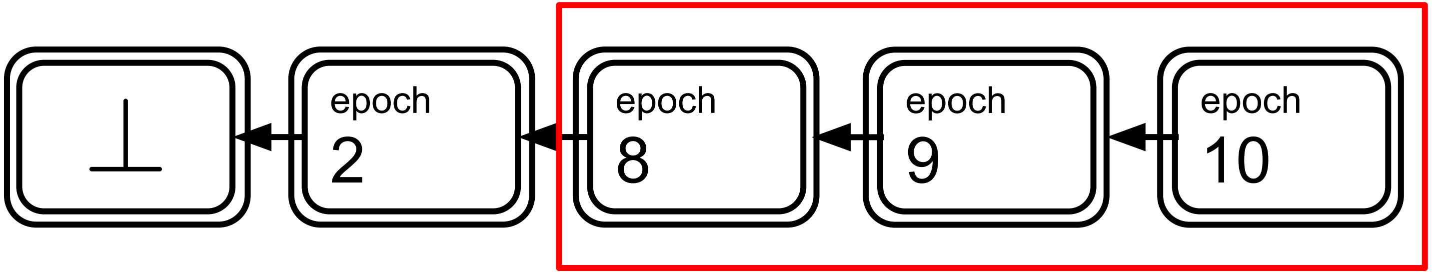
Example

In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

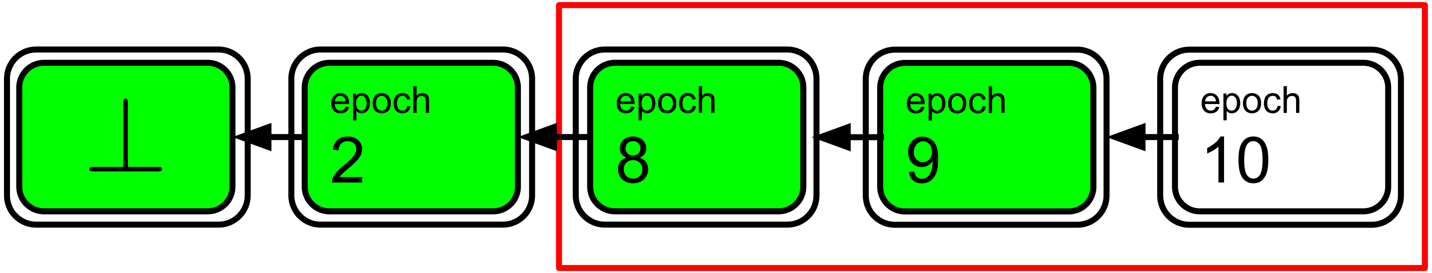


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example



In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Analysis

<u>Consistency</u>: no synchrony assumptions, f < n/3

In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Analysis

Consistency: no synchrony assumptions, f < n/3
Liveness: synchrony assumptions, expected O(1) rounds!

In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Analysis

<u>Consistency</u>: no synchrony assumptions, f < n/3
<u>Liveness</u>: synchrony assumptions, expected O(1) rounds!

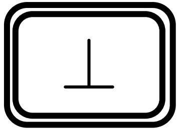
(optimizable)

In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

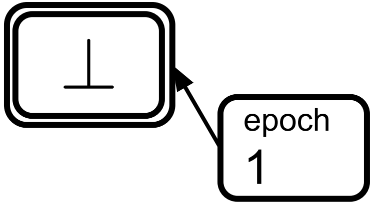


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

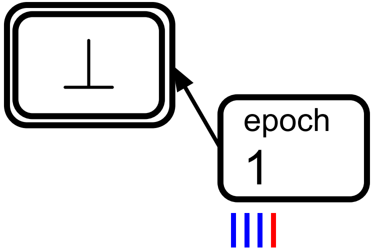


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

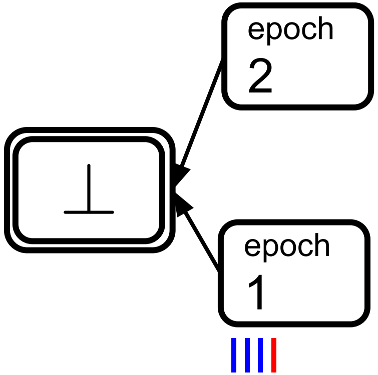


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

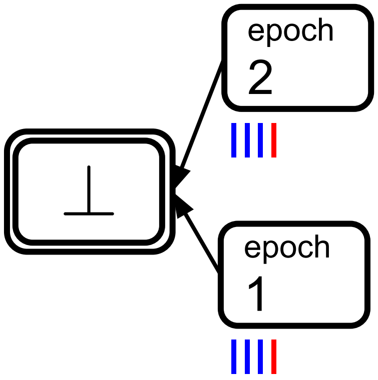


In every epoch $e = 1, 2, ...$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

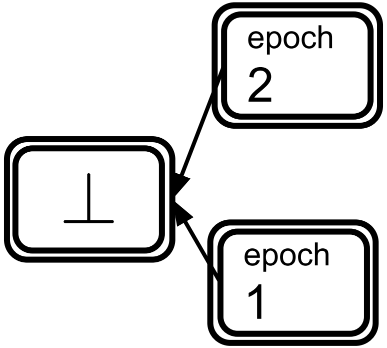


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

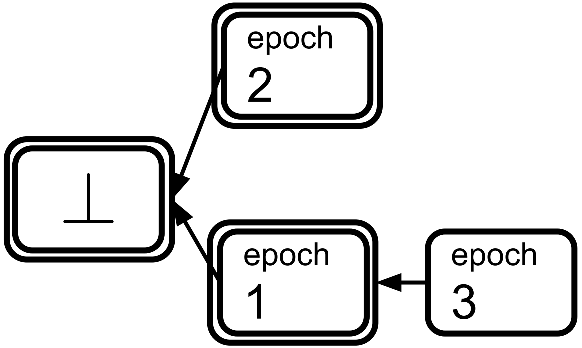


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

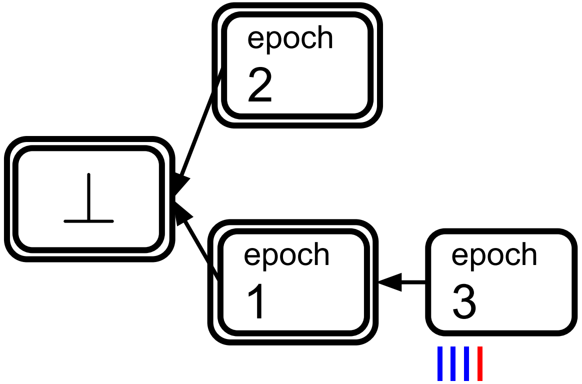


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

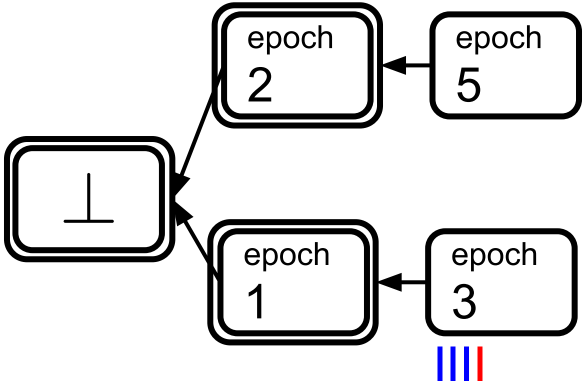


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

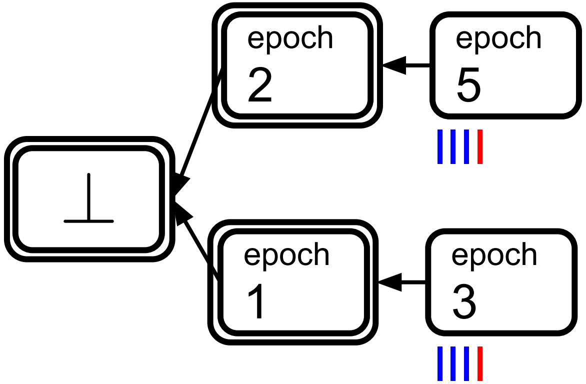


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

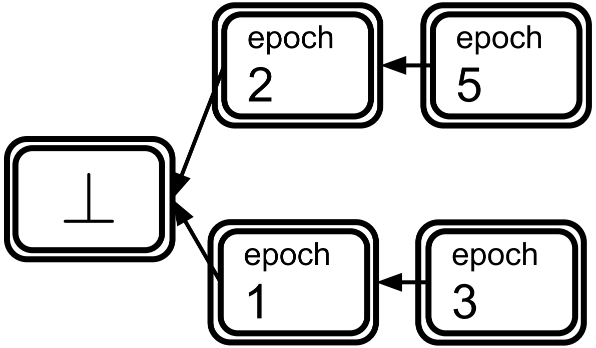


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

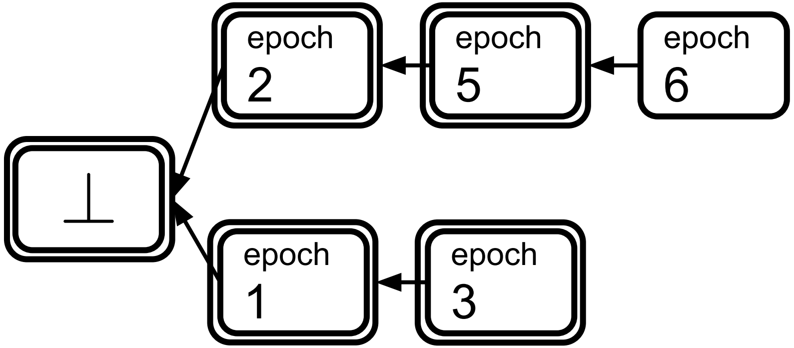


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

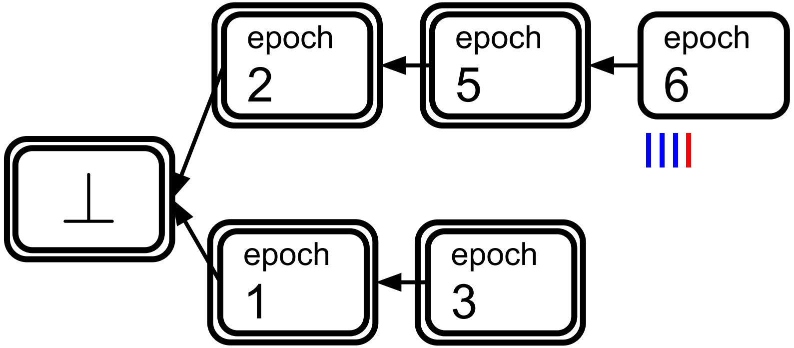


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

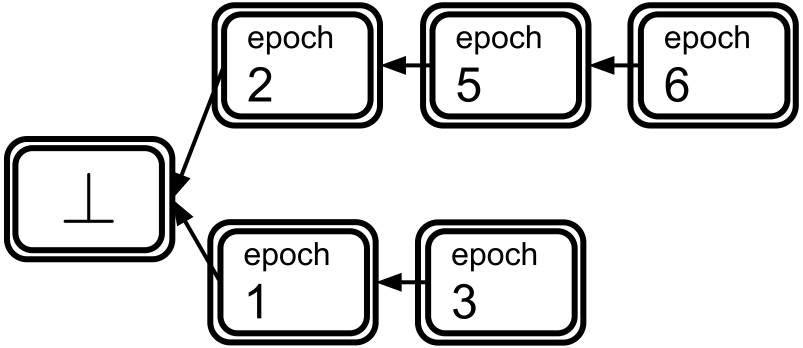


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Example

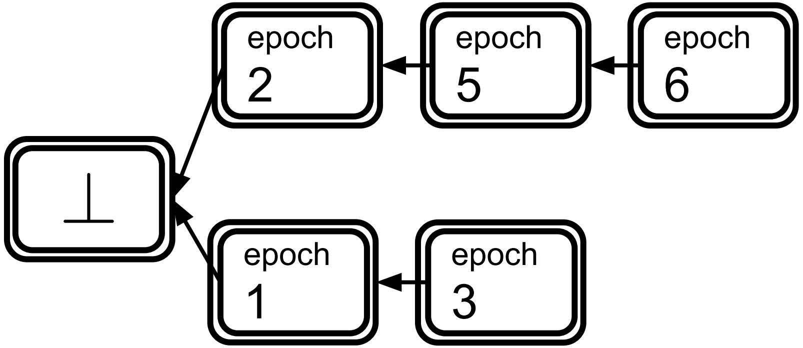


In every epoch $e = 1, 2, \ldots$

- ❏ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Allows two notarized blocks at the same height!

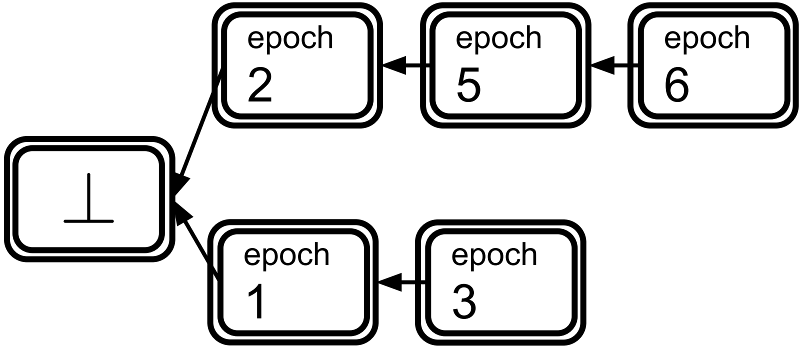


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Allows two notarized blocks at the same height! (usually)

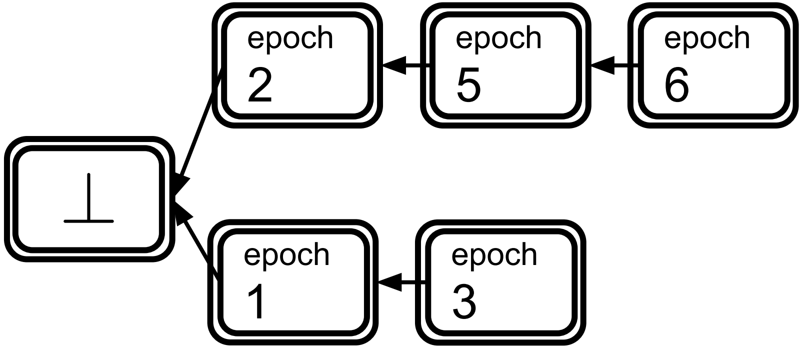


In every epoch $e = 1, 2, \ldots$

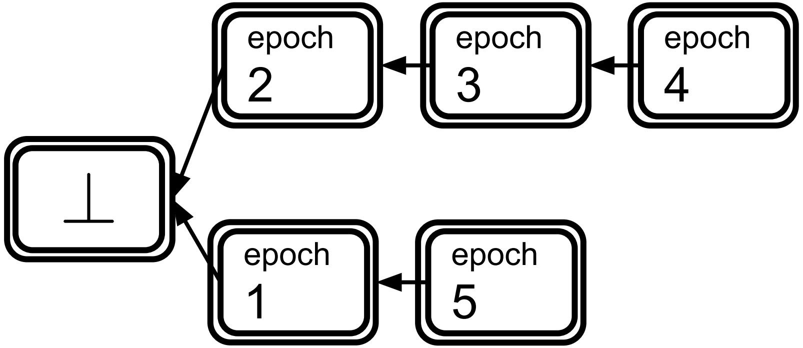
- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Possible



Impossible

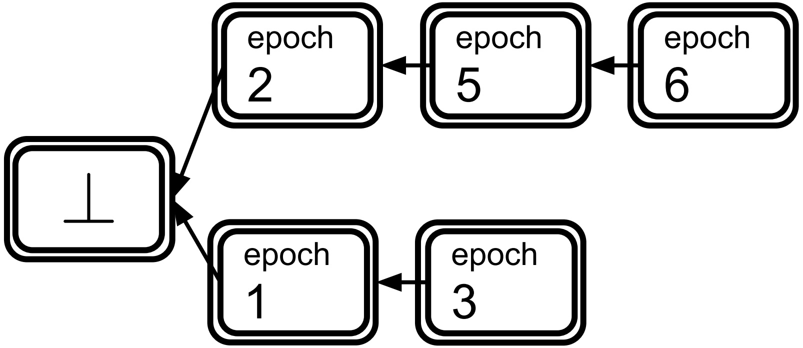


In every epoch $e = 1, 2, \ldots$

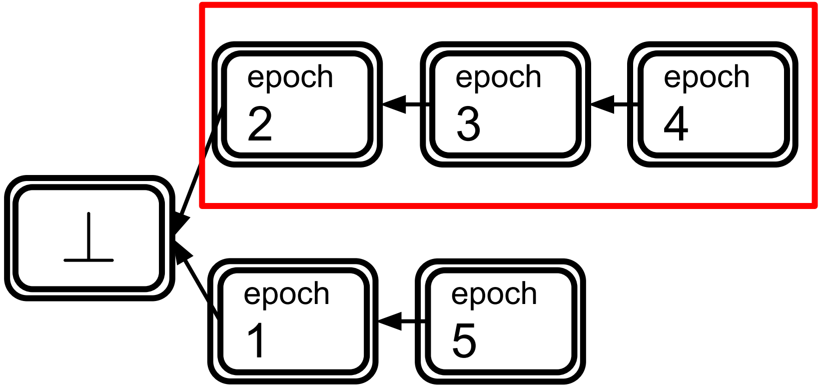
- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Possible



Impossible

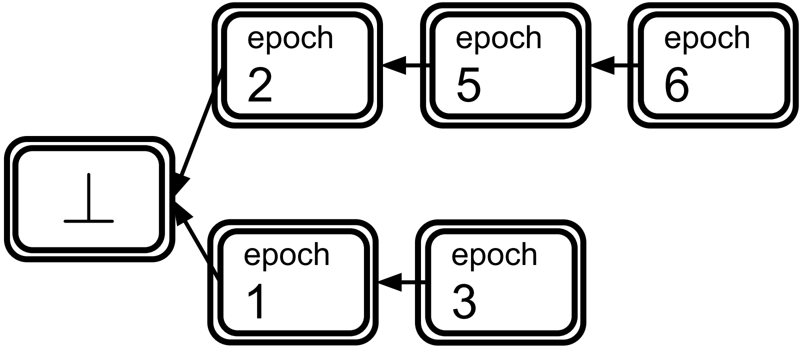


In every epoch $e = 1, 2, \ldots$

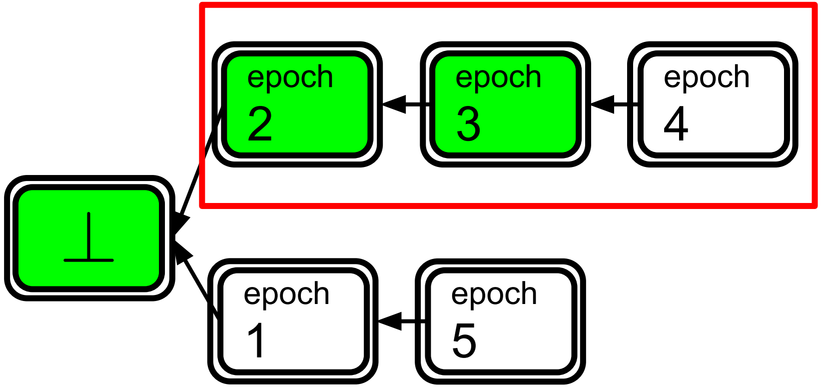
- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Possible



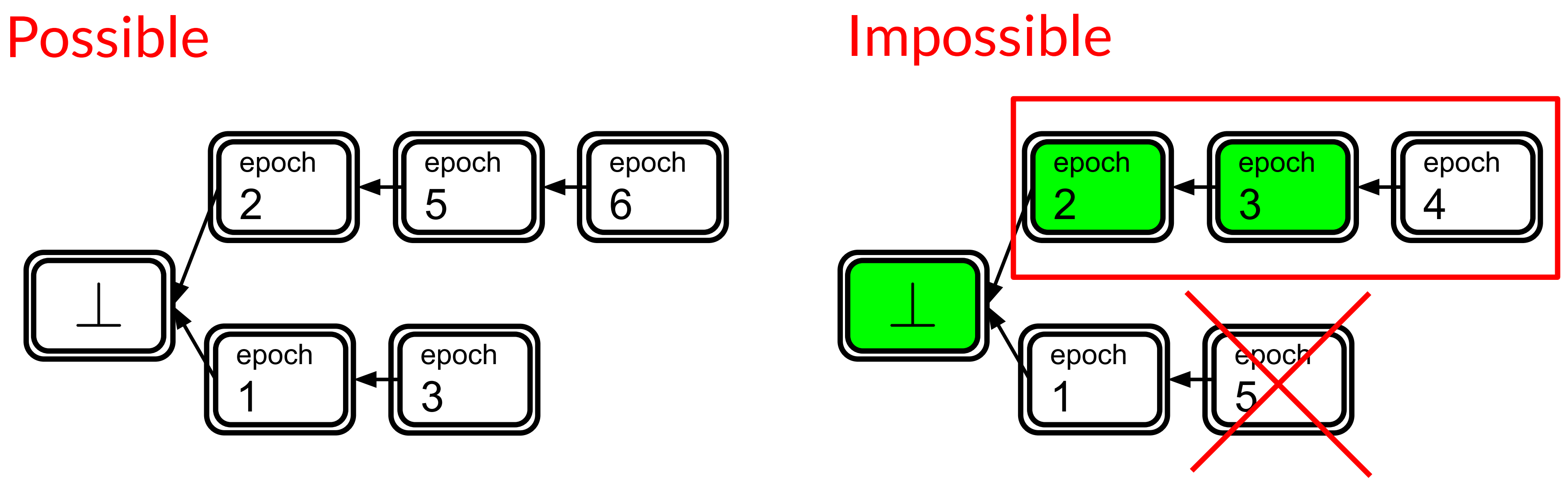
Impossible



In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

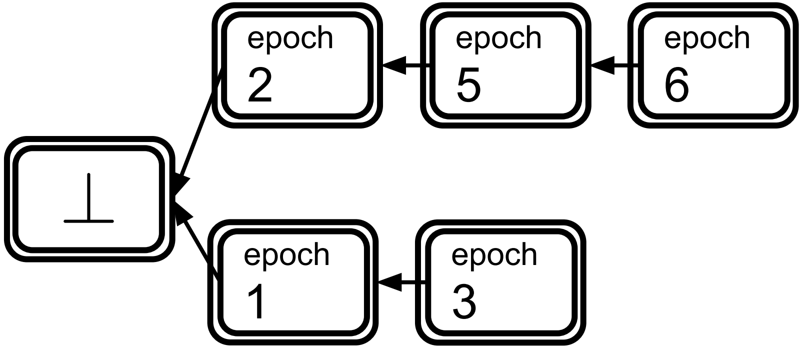


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

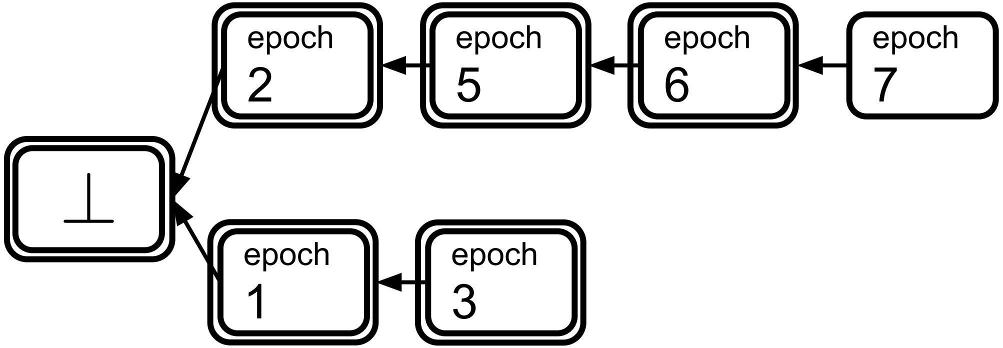


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

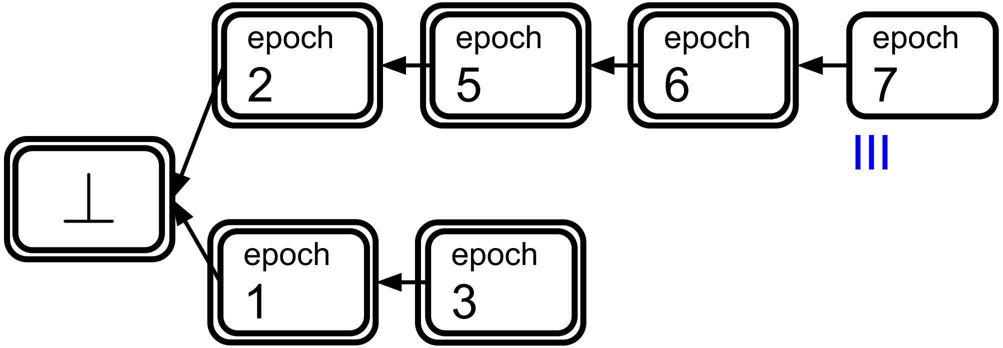


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

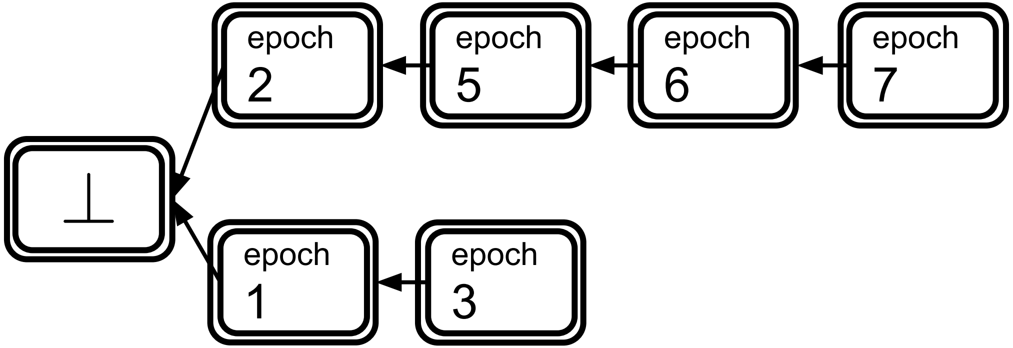


In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

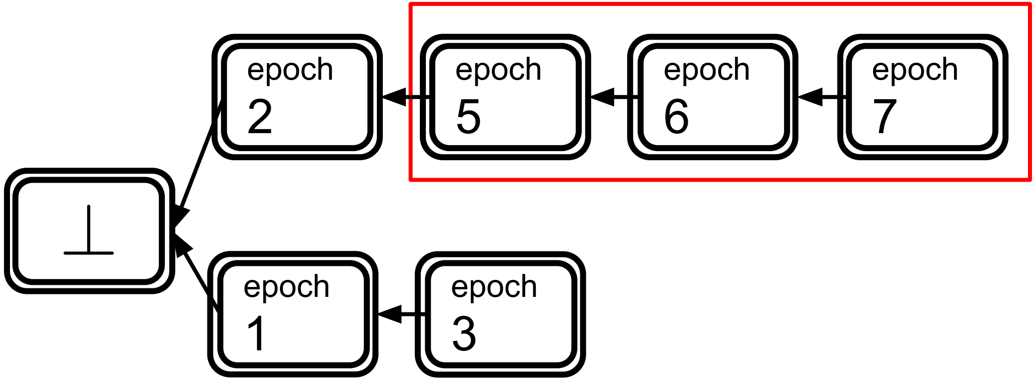


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

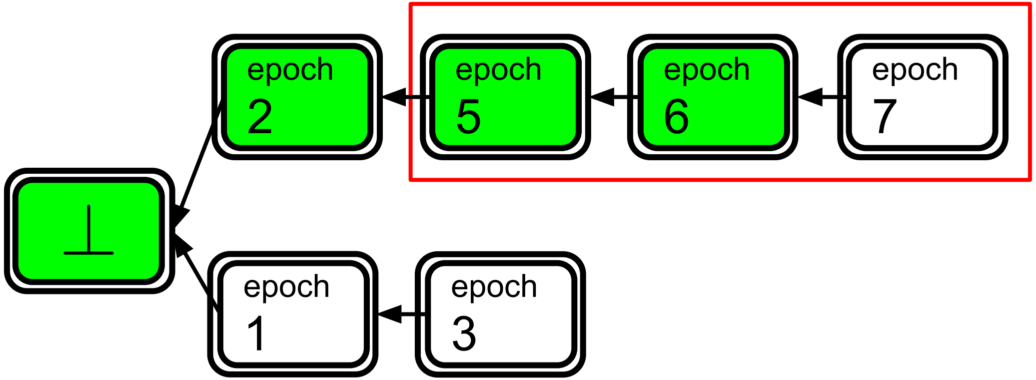


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

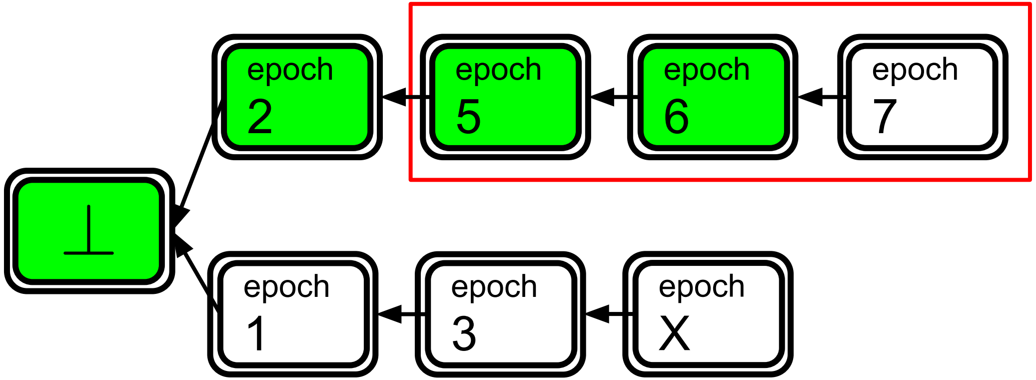


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

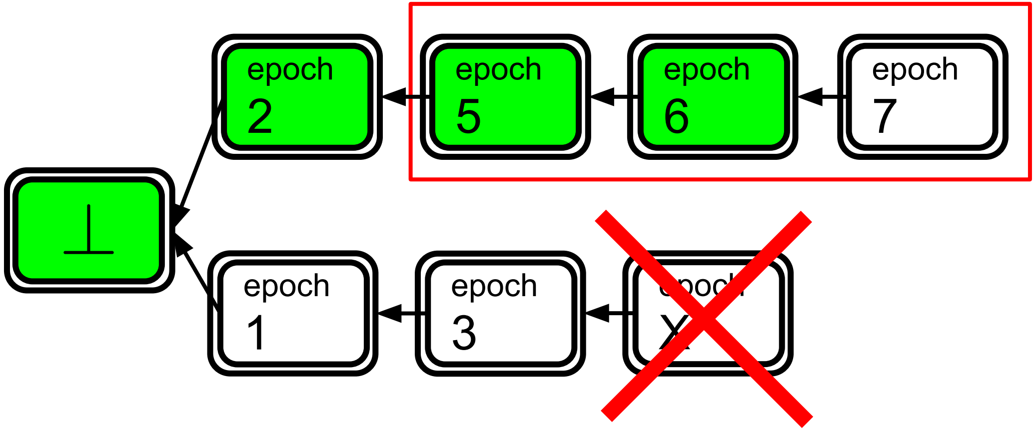


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

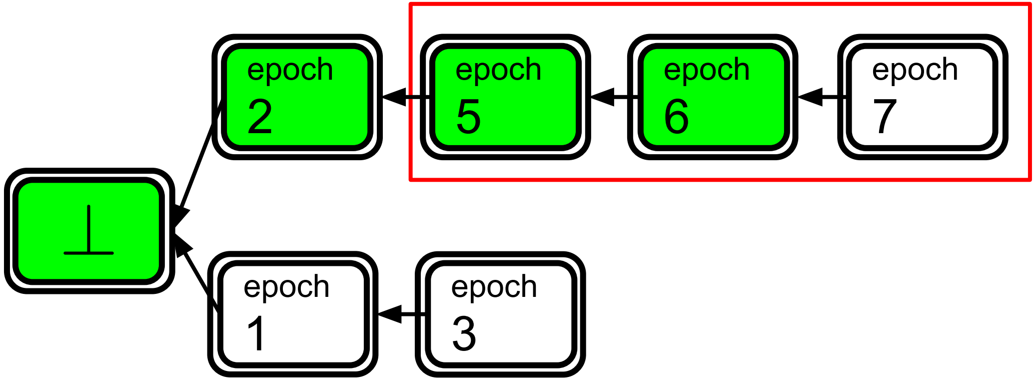


In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

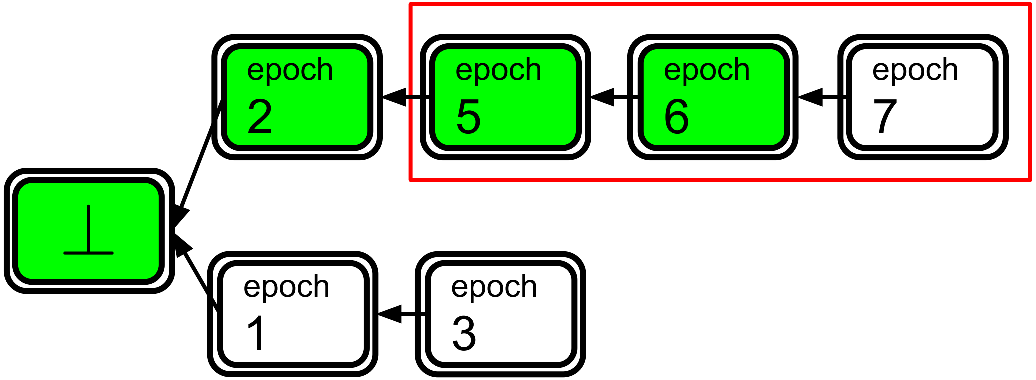


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch



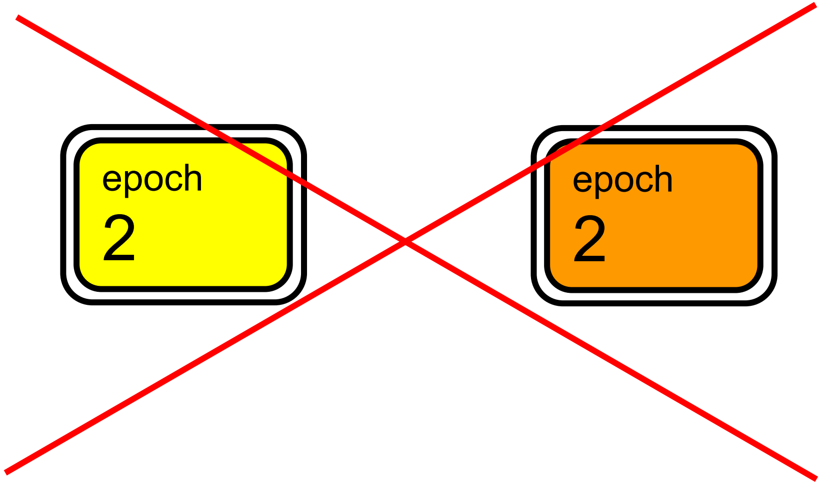
Lemma 1: *Each epoch is associated with at most one notarized block.*

Consistency Sketch

Lemma 1: *Each epoch is associated with at most one notarized block.*

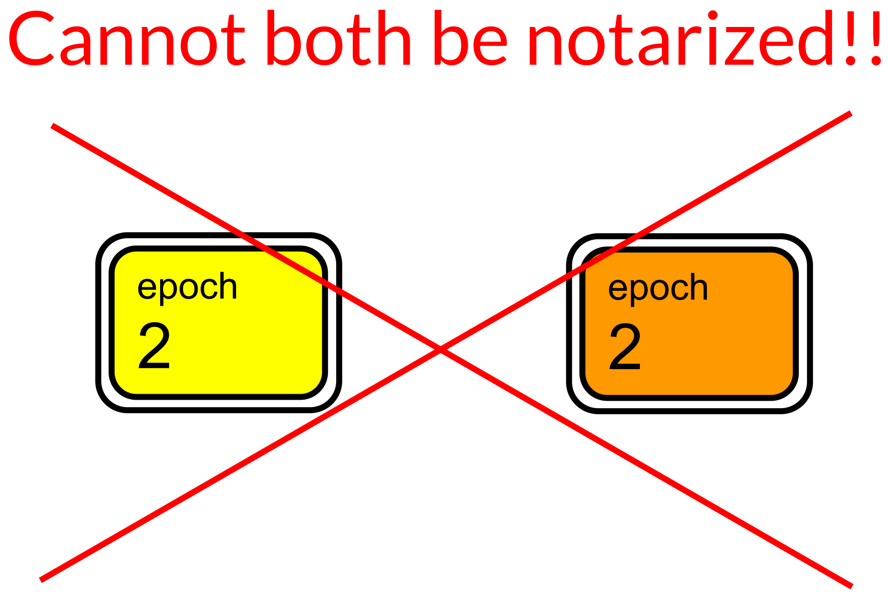
Consistency Sketch

Cannot both be notarized!!



Lemma 1: *Each epoch is associated with at most one notarized block.*

Consistency Sketch



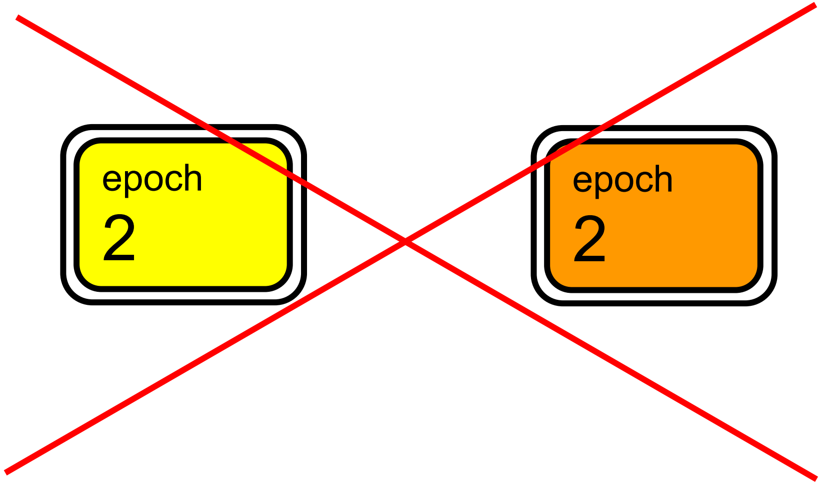
Lemma 1: *Each epoch is associated with at most one notarized block.*

Proof:

- Each honest process votes only once for each epoch.

Consistency Sketch

Cannot both be notarized!!



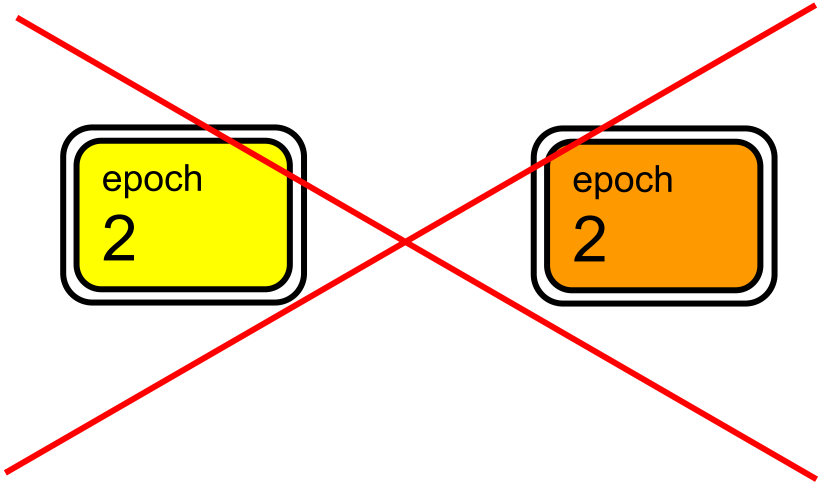
Lemma 1: *Each epoch is associated with at most one notarized block.*

Proof:

- ❏ Each honest process votes only once for each epoch.
- ❏ Each notarized block requires 2n/3 distinct votes.

Consistency Sketch

Cannot both be notarized!!

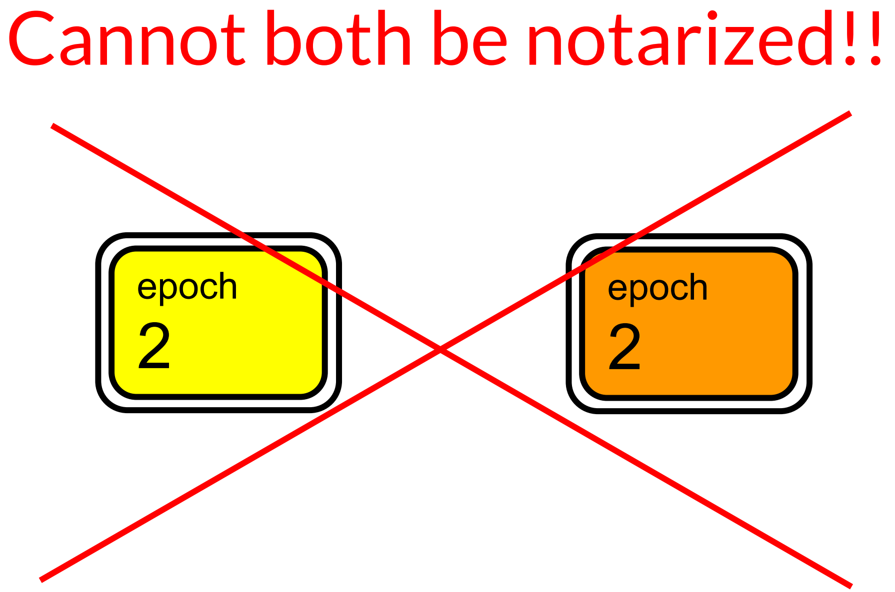


Lemma 1: *Each epoch is associated with at most one notarized block.*

Proof:

- Each honest process votes only once for each epoch.
- Each notarized block requires 2n/3 distinct votes.
- Multiple notarized blocks within epoch
= 4n/3 votes.

Consistency Sketch

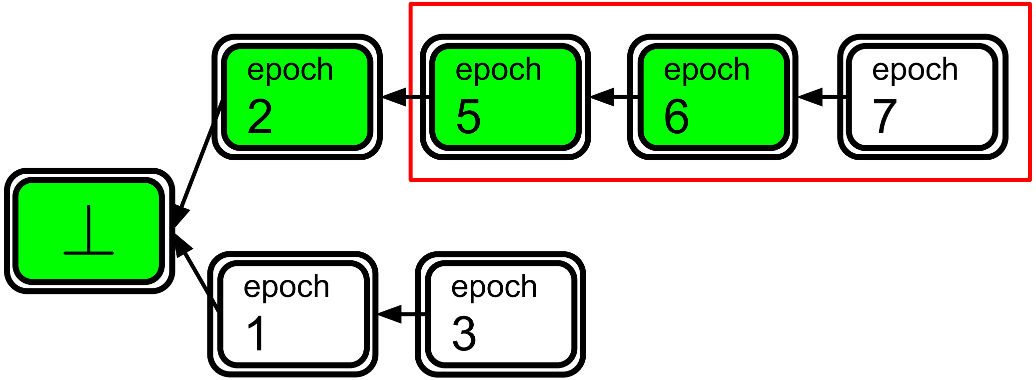


Lemma 1: *Each epoch is associated with at most one notarized block.*

Proof:

- ❏ Each honest process votes only once for each epoch.
- ❏ Each notarized block requires 2n/3 distinct votes.
- ❏ Multiple notarized blocks within epoch = 4n/3 votes.
- ❏ Letting f < n/3, we have (at best) 2n/3 + 2f < 4n/3 votes to go around.

Consistency Sketch



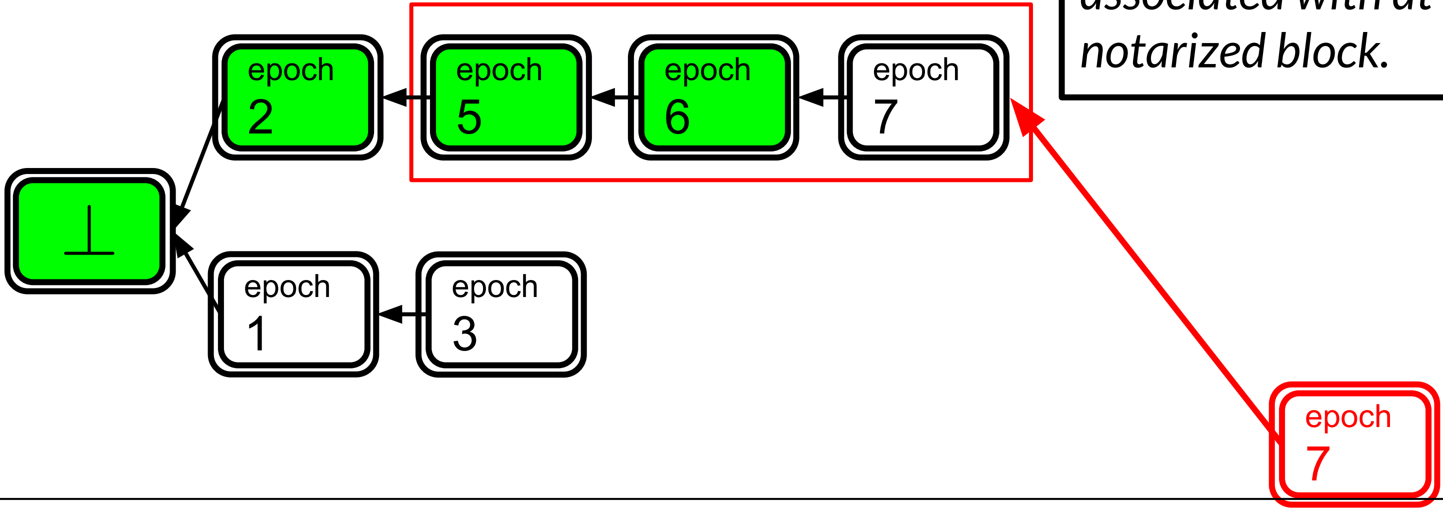
Lemma 1: *Each epoch is associated with at most one notarized block.*

In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch



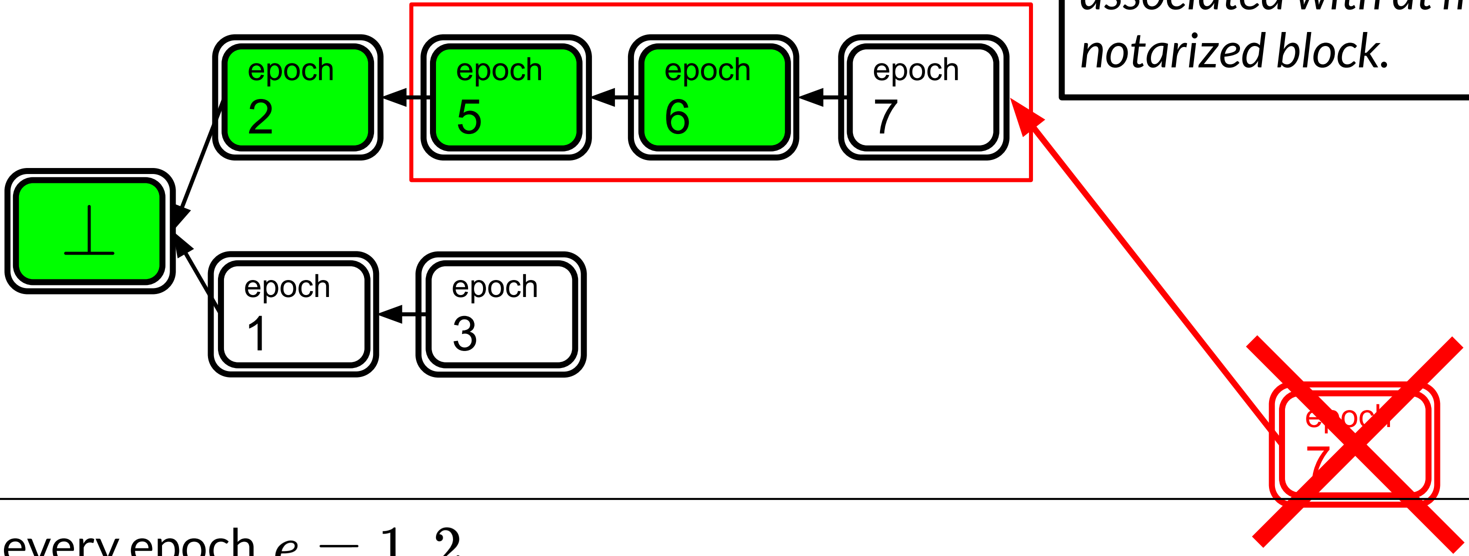
Lemma 1: *Each epoch is associated with at most one notarized block.*

In every epoch $e = 1, 2, \ldots$

- leader proposes b = ($H(b')$, e, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal b,
  but i.f.f. b also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch



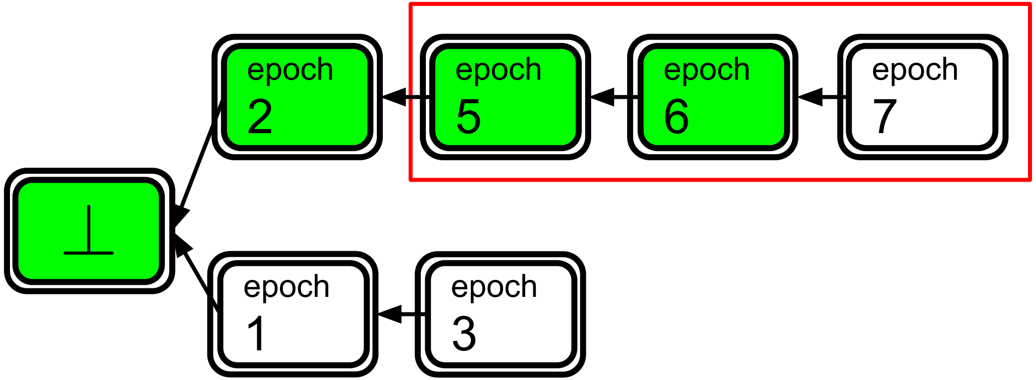
Lemma 1: *Each epoch is associated with at most one notarized block.*

In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

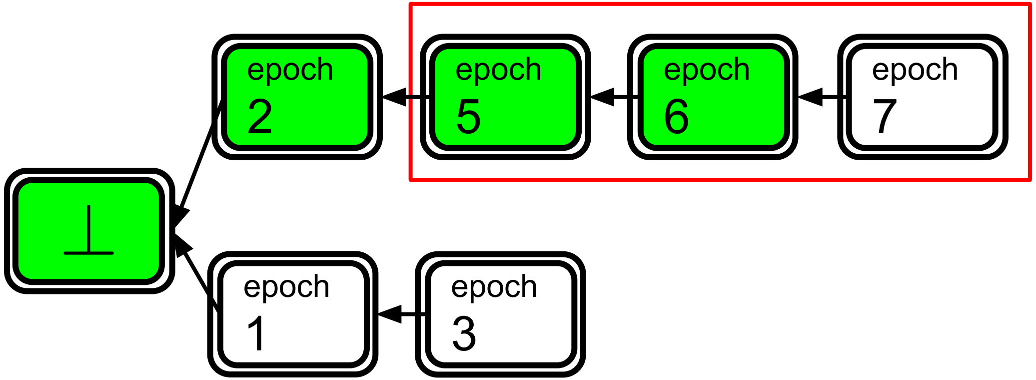


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

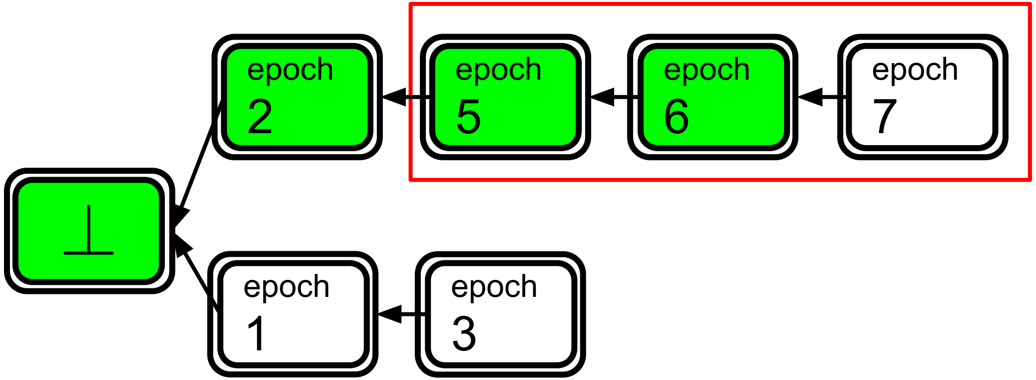
<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch



Now, the main lemma...

Consistency Sketch

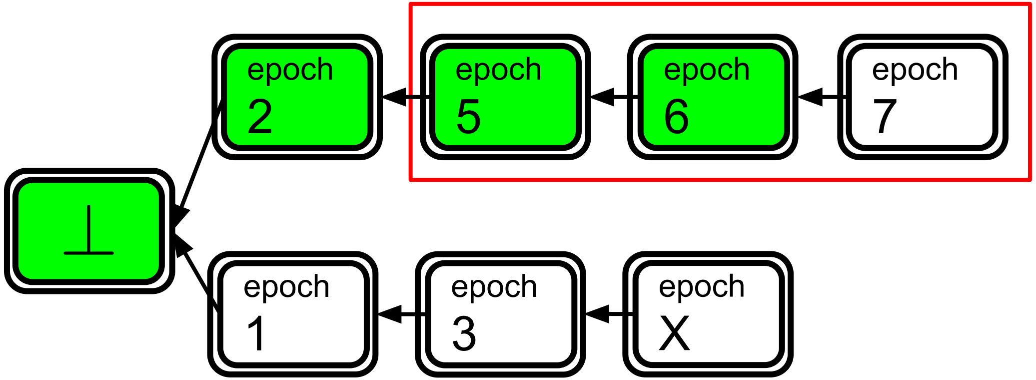


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

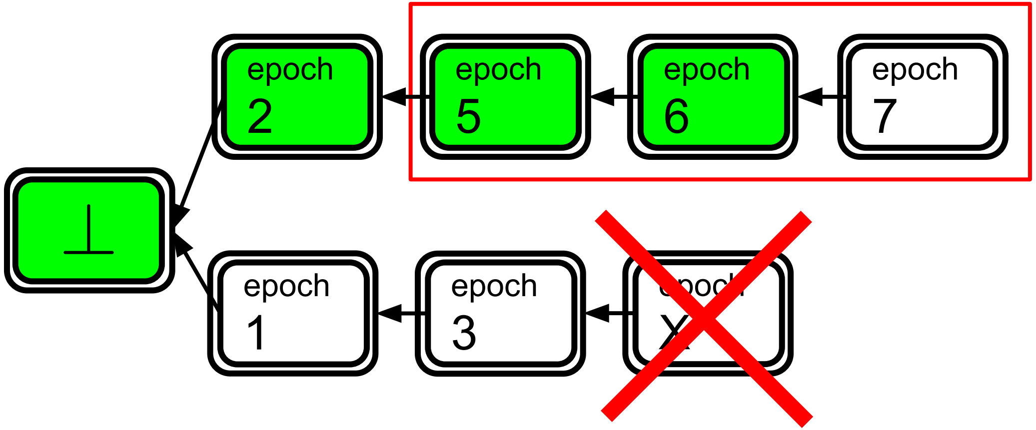


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch

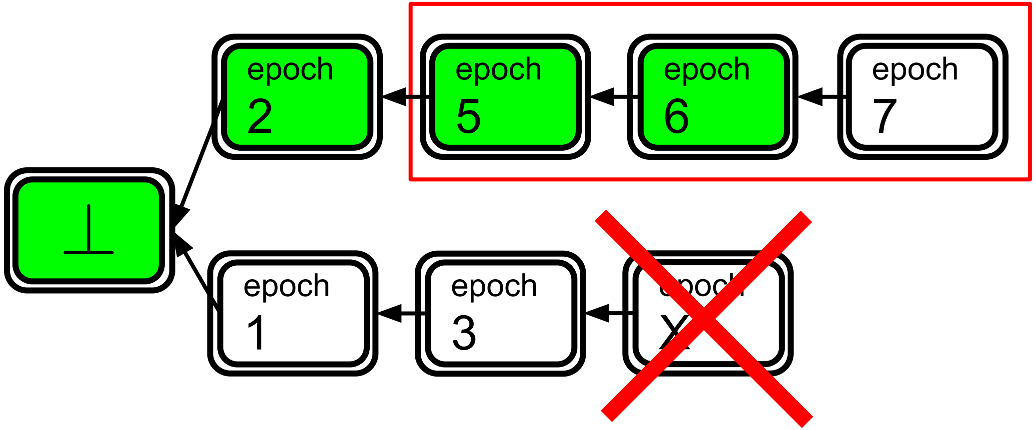


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

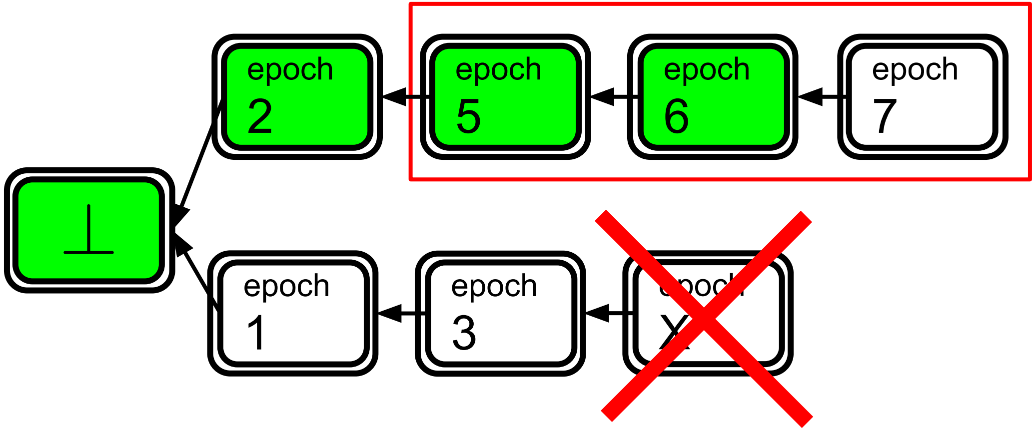
finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Consistency Sketch



Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

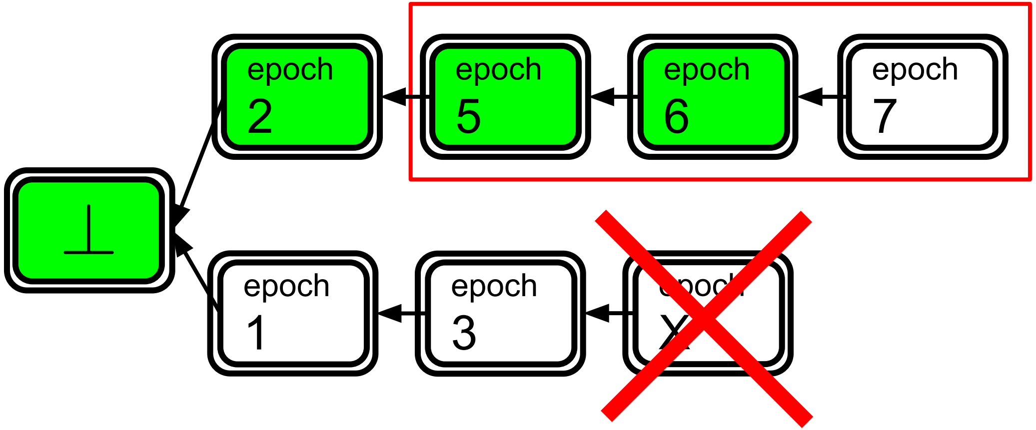
Consistency Sketch



Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Consistency Sketch



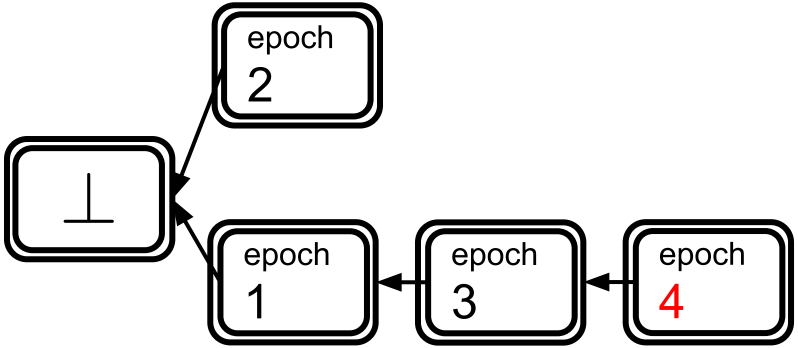
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5:

Case X > 7:

Consistency Sketch



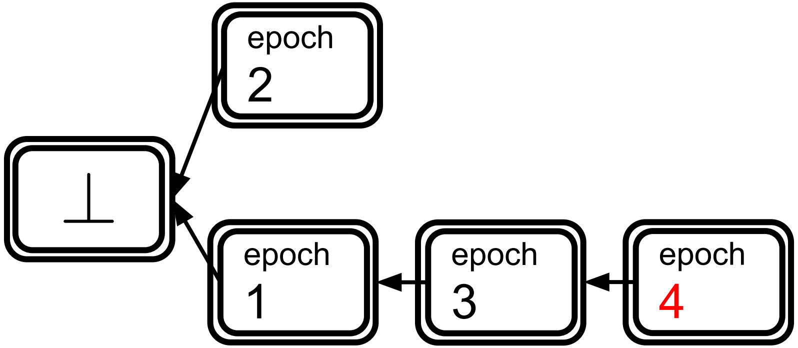
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

<u>**Case X < 5**</u>:

Case X > 7:

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

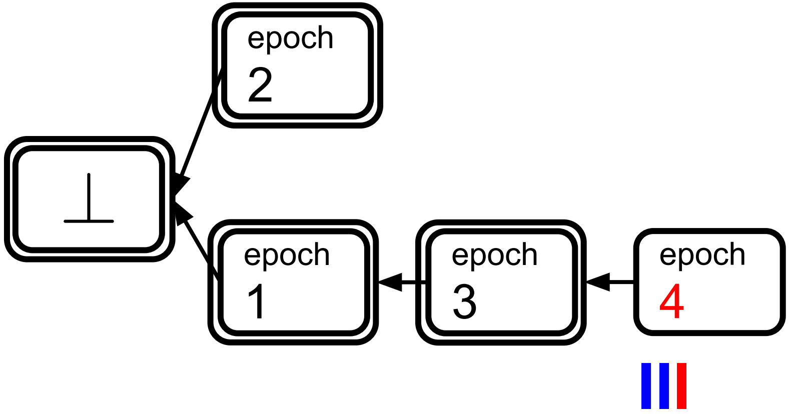
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5:

Case X > 7:

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

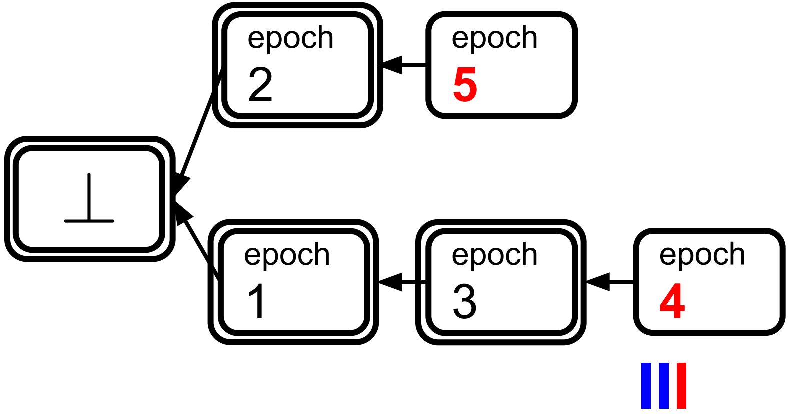
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5:

Case X > 7:

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

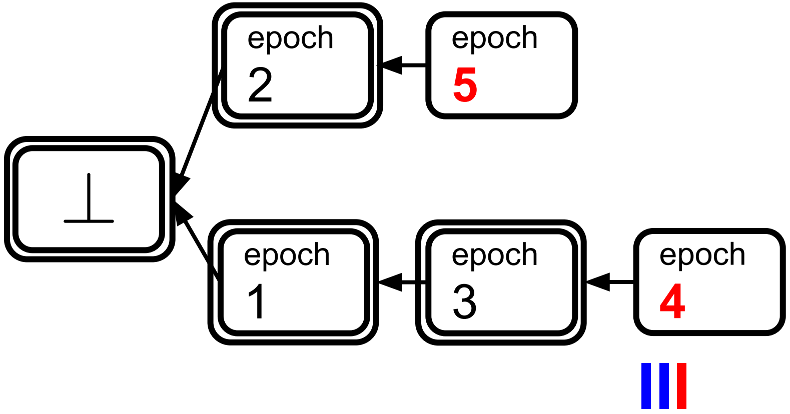
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

<u>Case X < 5</u>:

Case X > 7:

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

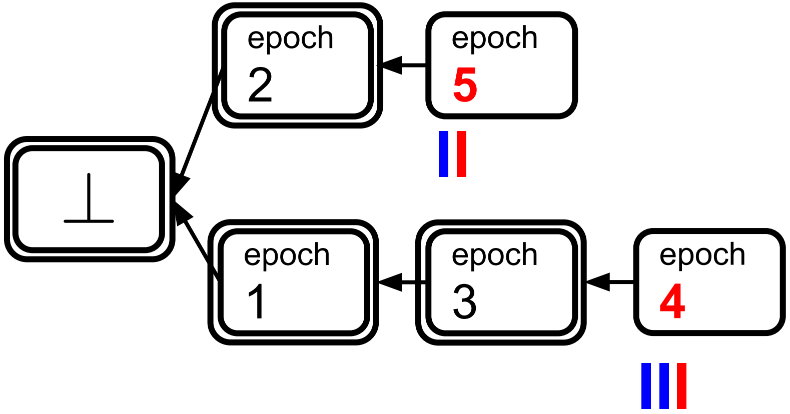
Pf: Assume for contradiction that an epoch X block, with the same height, exists.

<u>Case X < 5</u>:

Case X > 7:

- <u>voters</u> sign the first valid proposal *b*,
  but <u>i.f.f. *b* also extends a longest notarized chain the *voter* has seen</u>

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

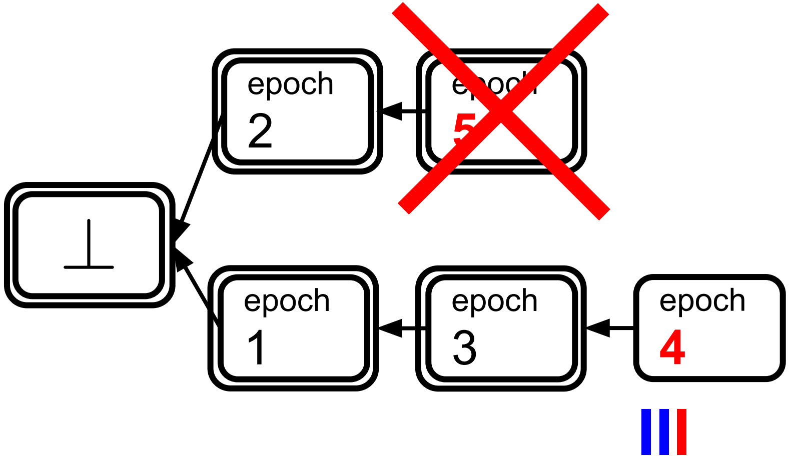
Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5:

Case X > 7:

- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

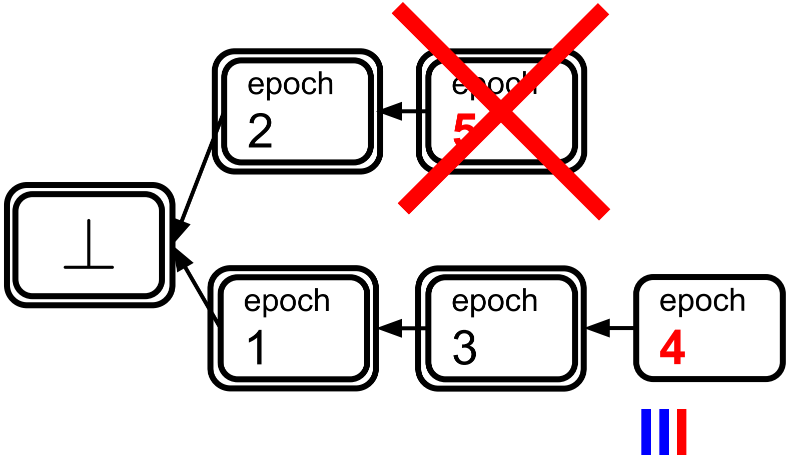
Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5:

Case X > 7:

- voters sign the first valid proposal *b*, but i.f.f. *b* also extends a longest notarized chain the *voter* has seen

Consistency Sketch



4 processes, 3 honest, 1 malicious
Require 3 votes to notarize

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

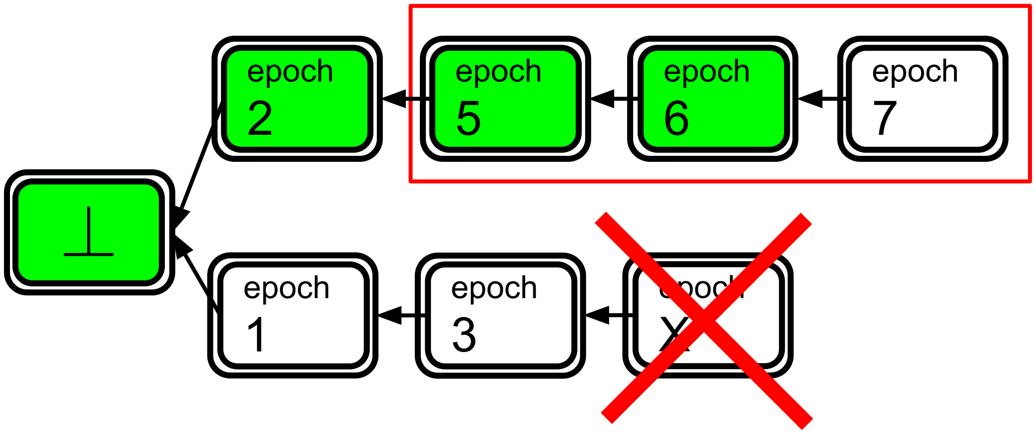
Pf: Assume for contradiction that an epoch X block, with the same height, exists.

<u>Case X < 5</u>: at least one honest process must have signed X, then epoch 5 block -><-

Case X > 7:

- <u>voters</u> sign the first valid proposal *b*,
  but <u>i.f.f. *b* also extends a longest notarized chain the *voter* has seen</u>

Consistency Sketch



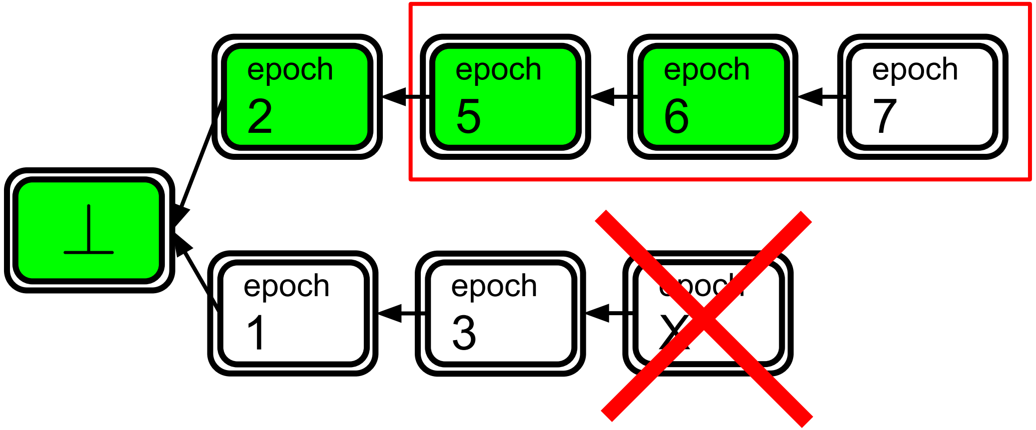
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

Case X > 7:

Consistency Sketch



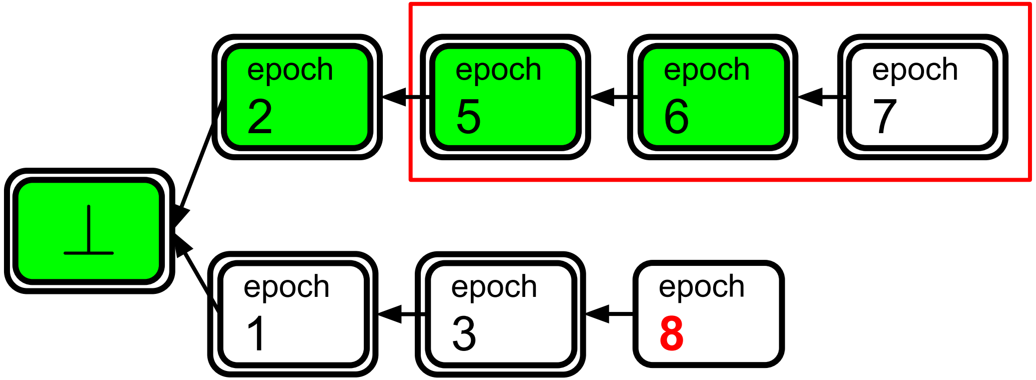
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

Case X > 7:

Consistency Sketch



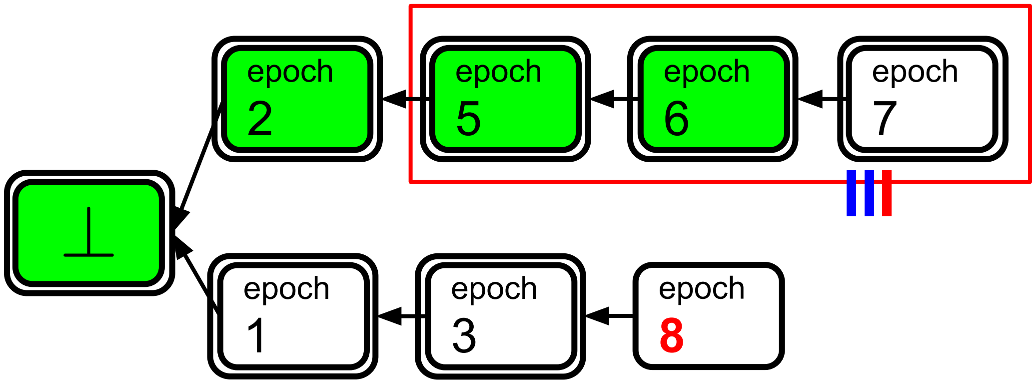
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

Case X > 7:

Consistency Sketch



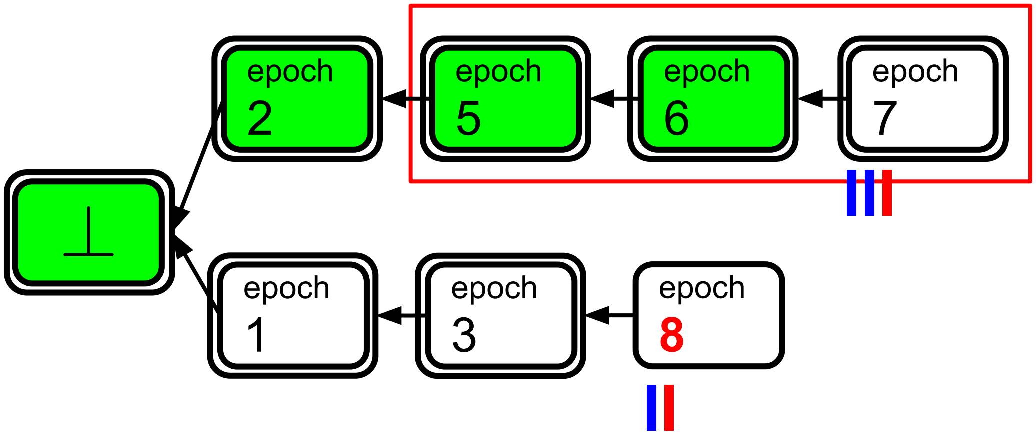
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

<u>Case X > 7</u>:

Consistency Sketch



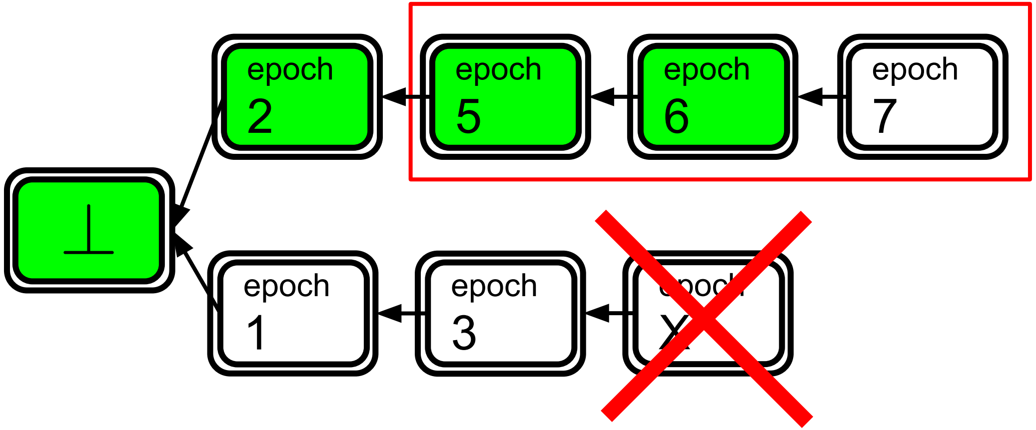
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

<u>Case X > 7</u>:

Consistency Sketch



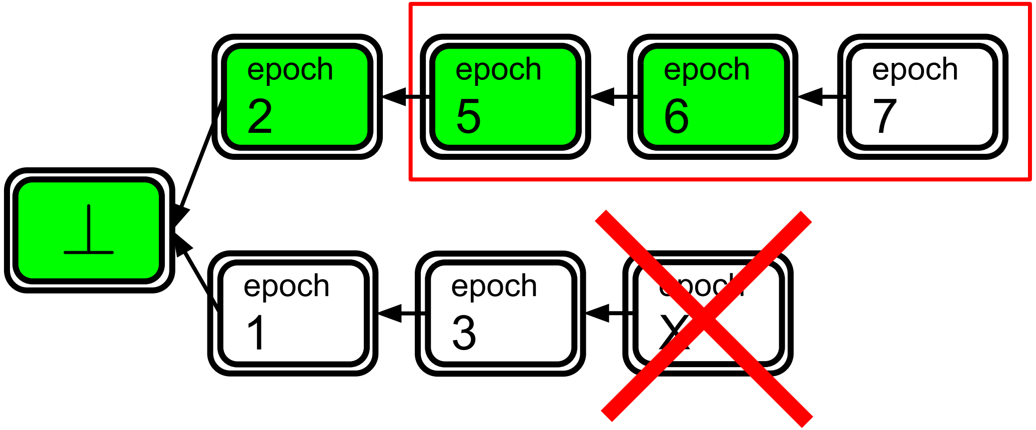
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

Case X > 7: Signed 7, then X -><-

Consistency Sketch



Intuition: Can't rewrite history

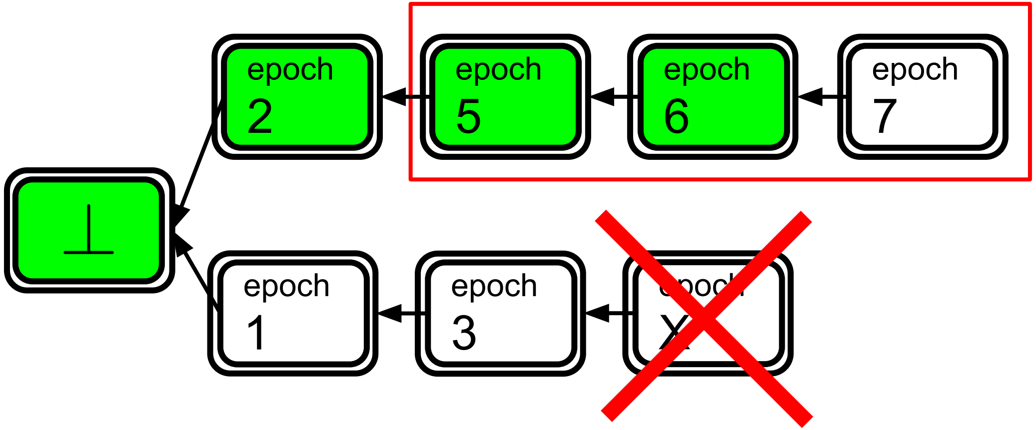
Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

<u>Case X > 7</u>: Signed 7, then X -><-

Consistency Sketch



Intuition: Can't rewrite history

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

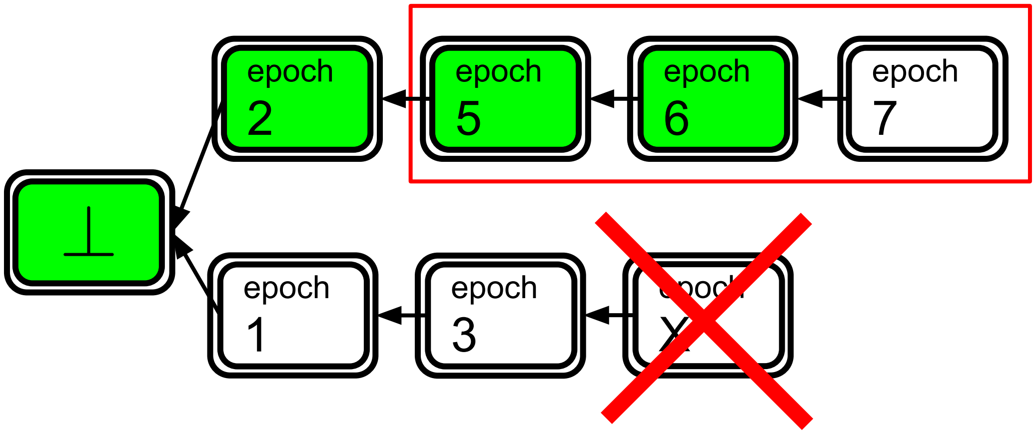
Pf: Assume for contradiction that an epoch X block, with the same height, exists.

Case X < 5: at least one honest process must have signed X, then epoch 5 block -><-

<u>Case X > 7</u>: Signed 7, then X -><-

(can add a new notarized block at the same height as an existing notarized block, but never in the past)

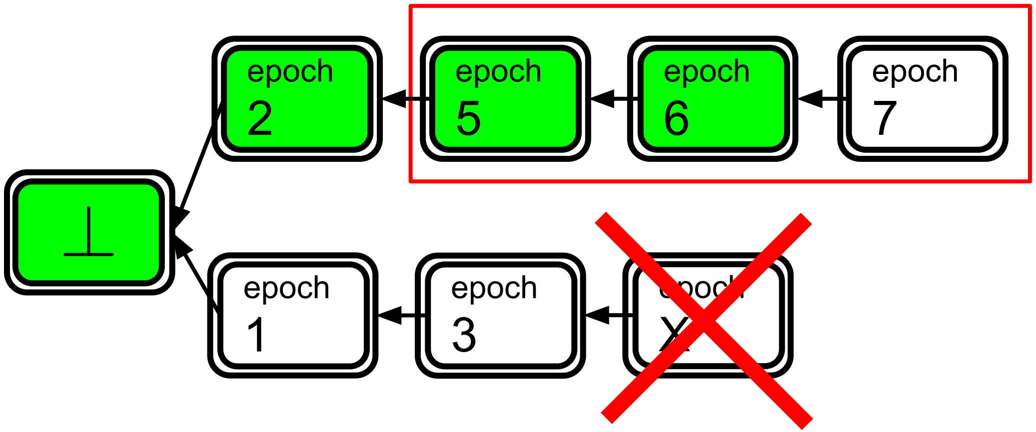
Consistency Sketch



Lemma 1: *Each epoch is associated with at most one notarized block.*

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Consistency Sketch

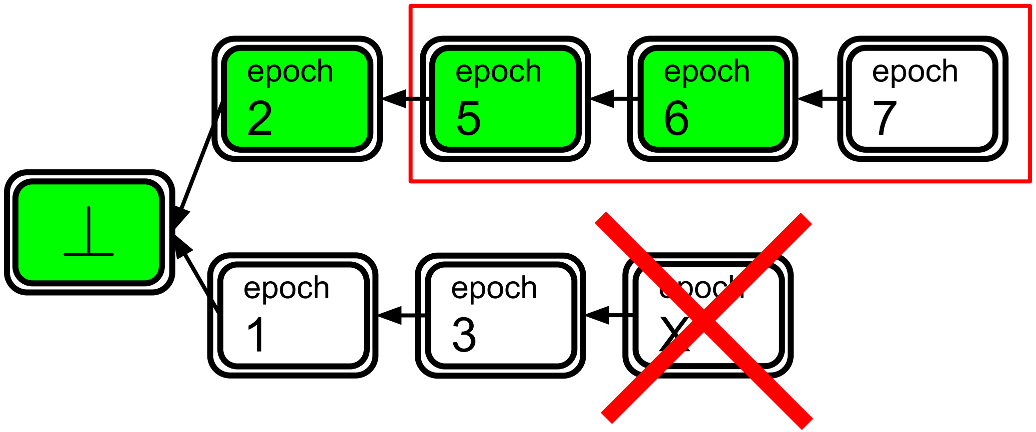


Lemma 1: *Each epoch is associated with at most one notarized block.*

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Lemma 3: *All longer notarized chains, in any view, must extend block 6*

Consistency Sketch

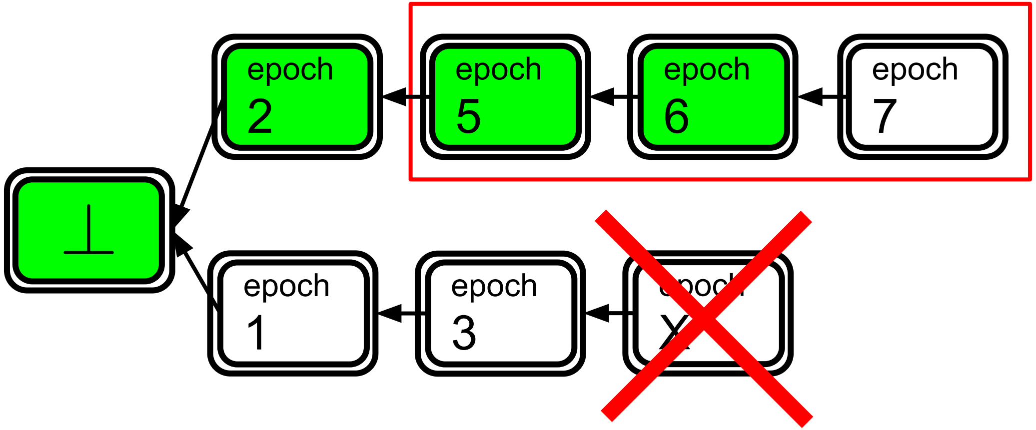


Lemma 1: *Each epoch is associated with at most one notarized block.*

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Lemma 3: *All longer* ***finalized*** *chains, in any view, must extend block 6*

Consistency Sketch



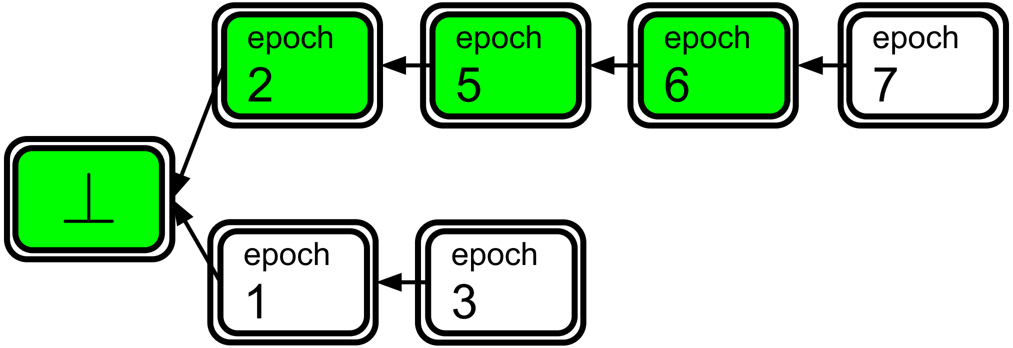
Lemma 1: *Each epoch is associated with at most one notarized block.*

Lemma 2: *No other notarized block, in past or future, can share the same height as block 6*

Lemma 3: *All longer **finalized** chains, in any view, must extend block 6*

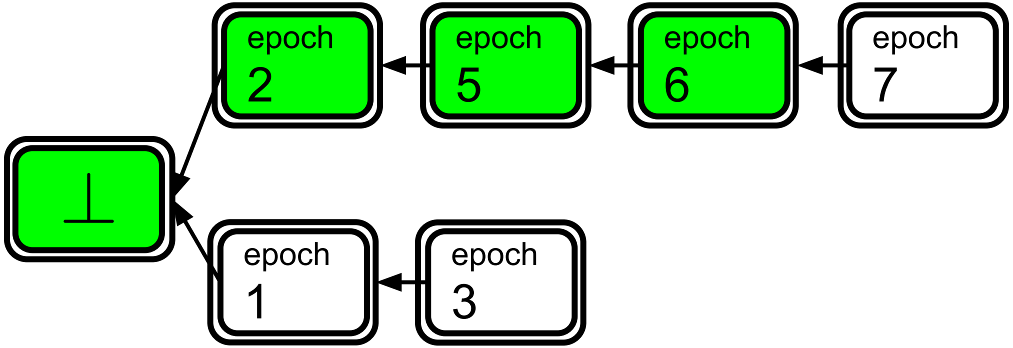
No synchrony assumptions!

Consistency Recap (Intuitive)



1. Can’t rewrite history
2. One block per epoch
3. Demonstrate sudden chain growth

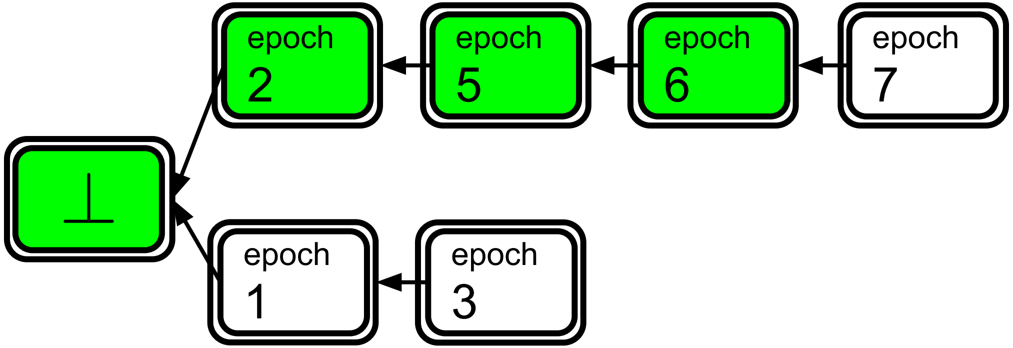
Consistency Recap (Intuitive)



1. Can't rewrite history
2. One block per epoch
3. Demonstrate sudden chain growth

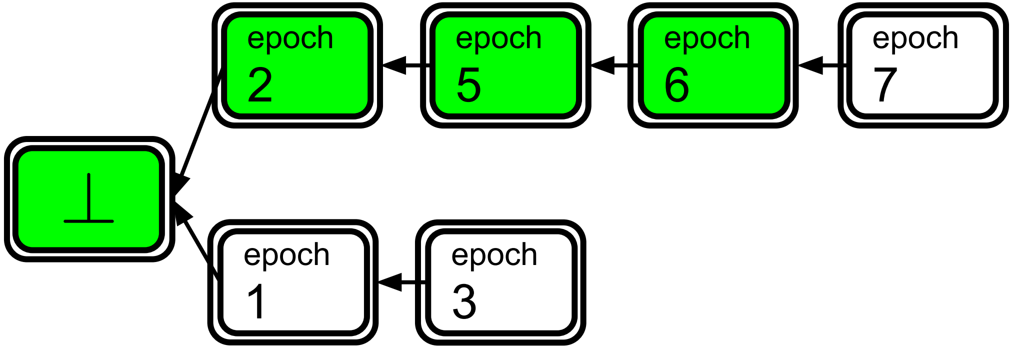
= chain provably longer than competitors

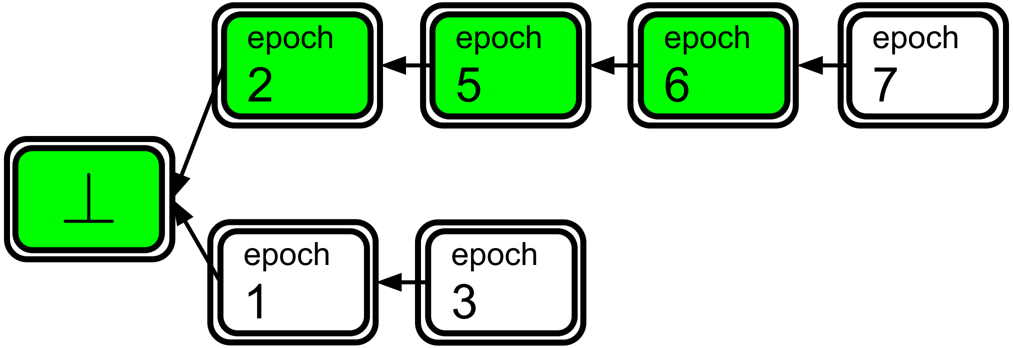
Consistency Recap (Intuitive)



1. Can't rewrite history
2. One block per epoch
3. Demonstrate sudden chain growth (why 3?)

= chain provably longer than competitors


⊥
epoch 2
epoch 5
epoch 6
epoch 7
epoch 1
epoch 3

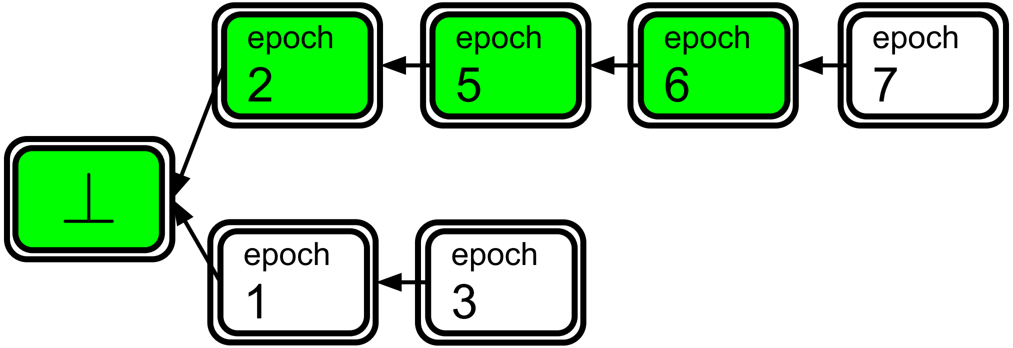


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

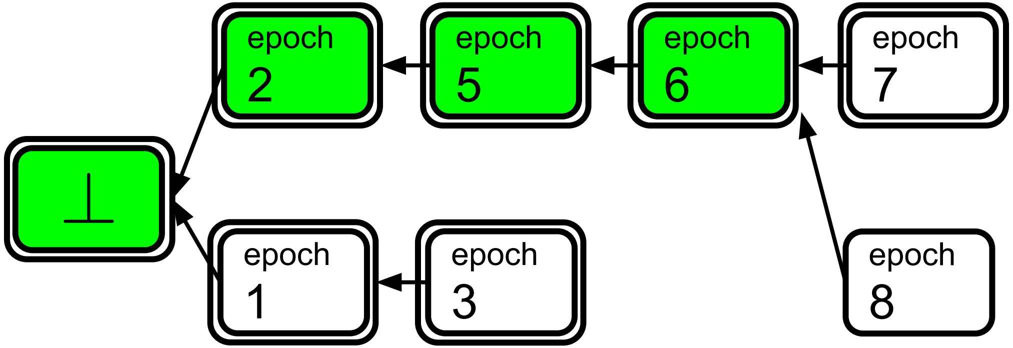


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

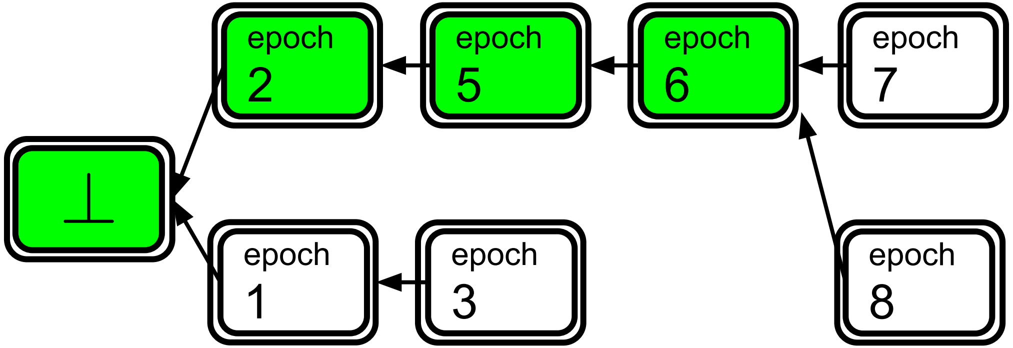


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

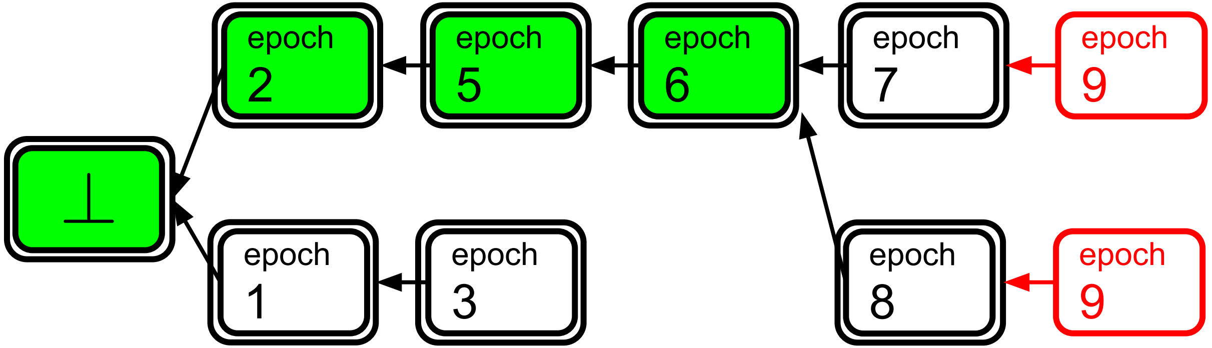


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

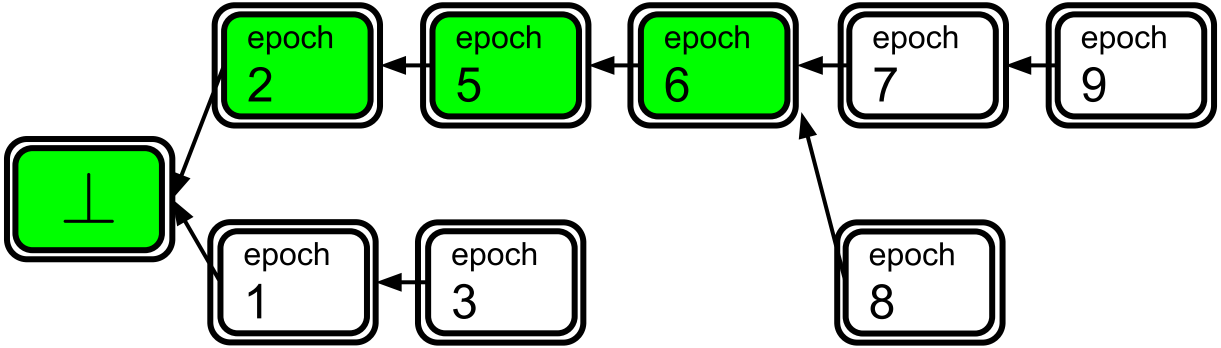


In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

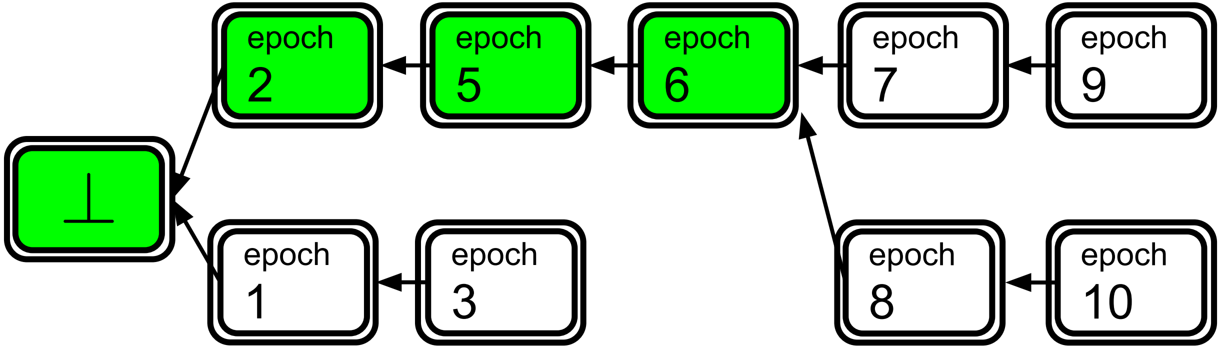


In every epoch $e = 1, 2, \ldots$

- ❏ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

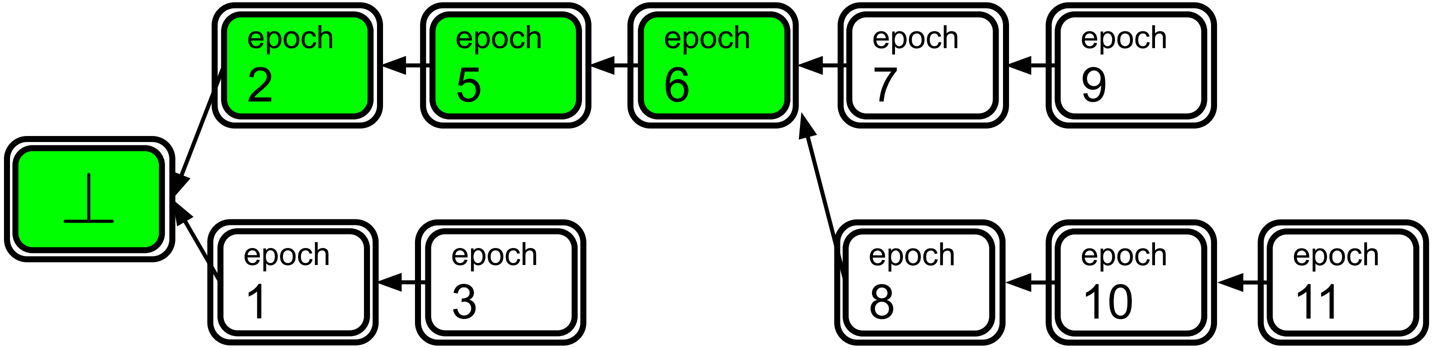


In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

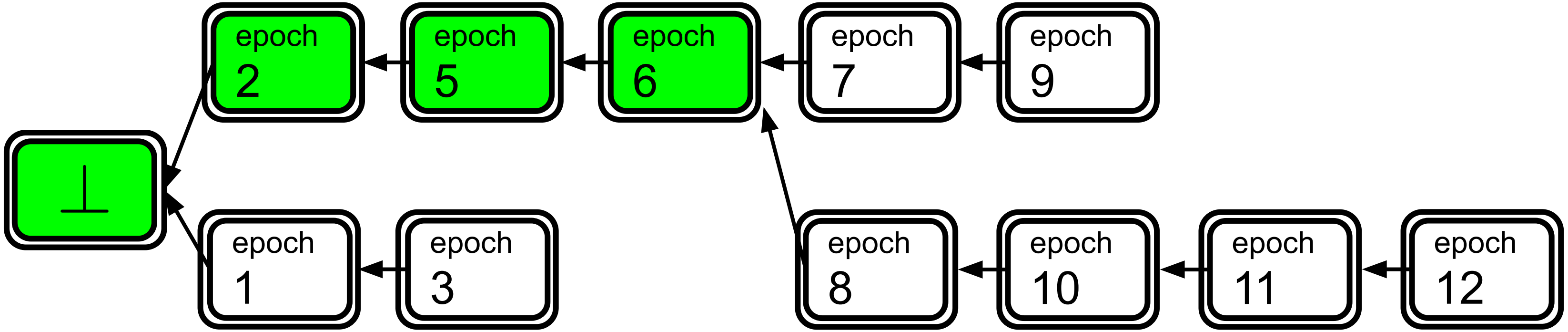


In every epoch $e = 1, 2, \ldots$

- ❏ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❏ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

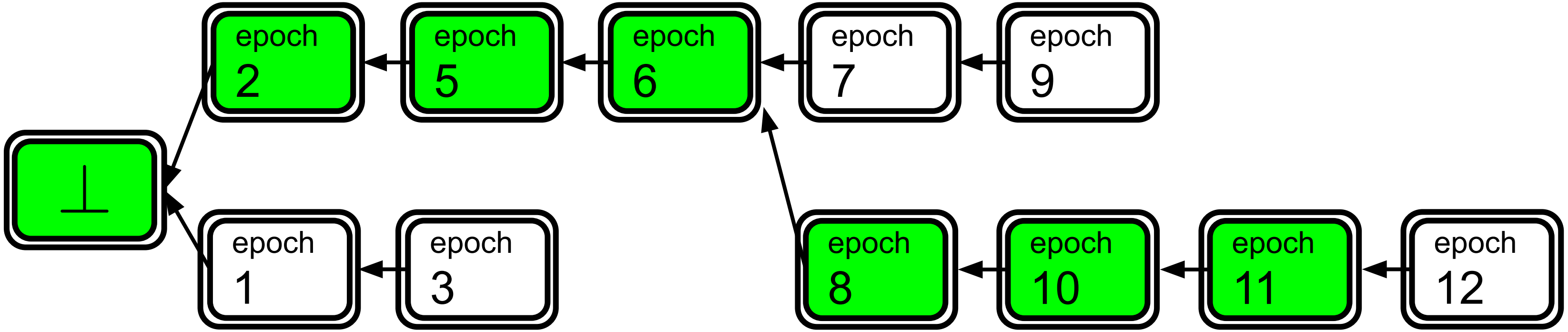


In every epoch $e = 1, 2, \ldots$

- leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?

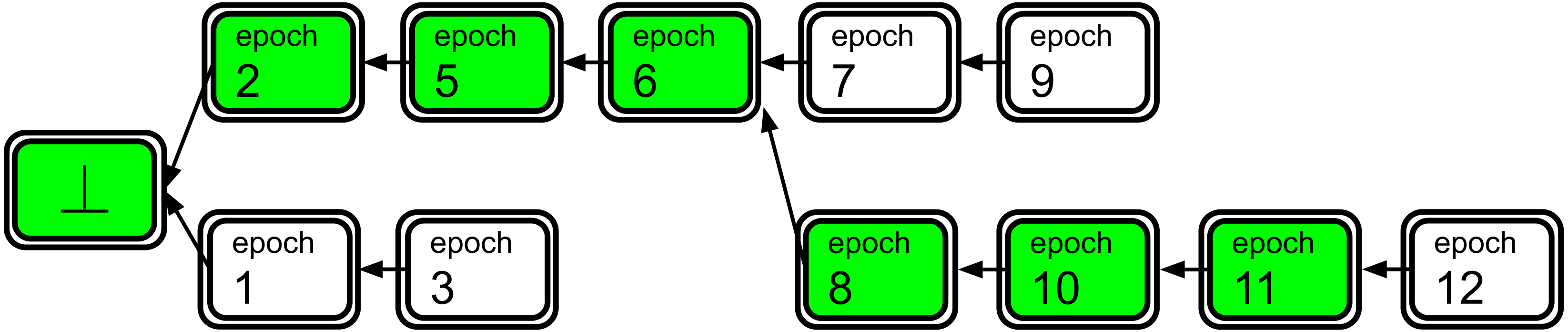


In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

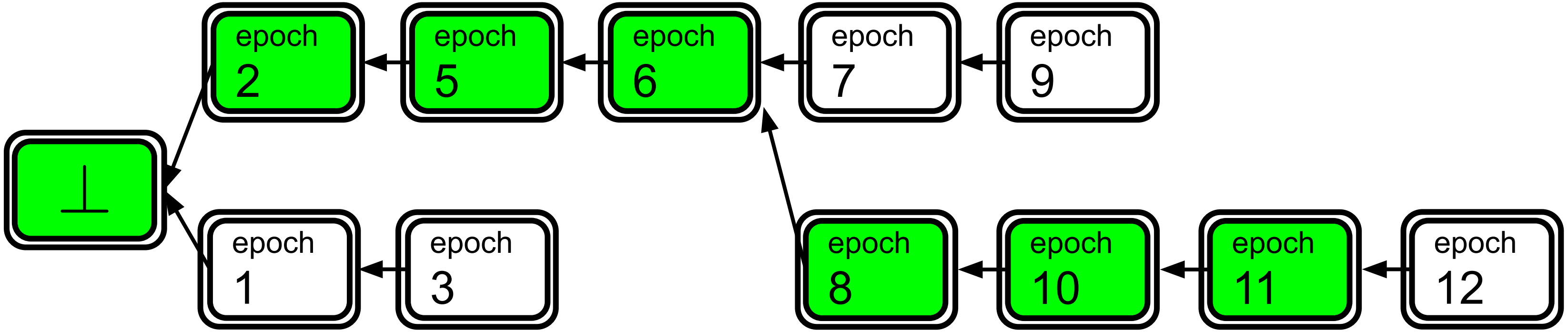
finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Liveness?



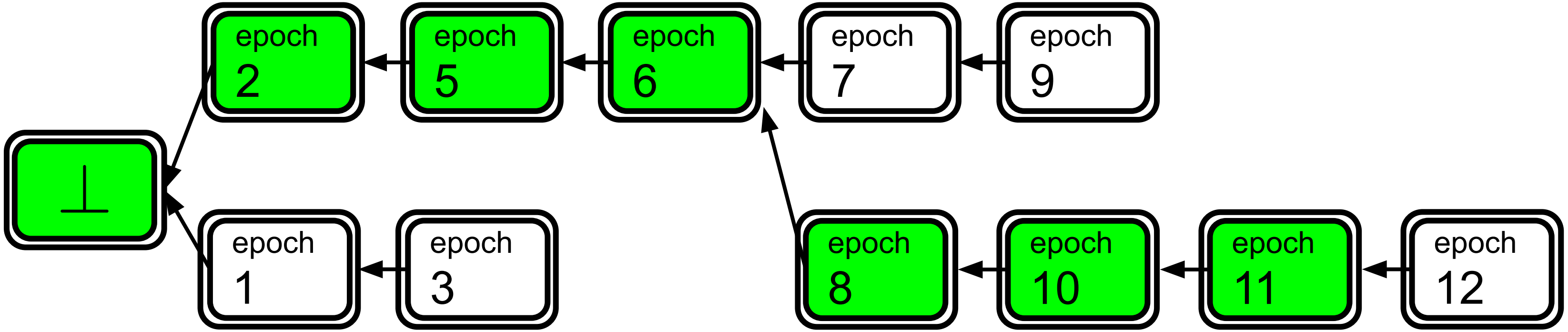
We need many good leaders in a row

Liveness?



We need many good leaders in a row

- Random leaders: get lucky
- Stable leader mechanism
- Not bad!


⊥
epoch 2
epoch 5
epoch 6
epoch 7
epoch 9
epoch 1
epoch 3
epoch 8
epoch 10
epoch 11
epoch 12

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ leader proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ voters sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

finalize any notarized chain ending with 3 consecutive epochs, chopping off last block

Goal: "Simplest-Possible", Drop-in replacement for PBFT

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

<u>Goal</u>: "Simplest-Possible", Drop-in replacement for PBFT
<u>Result</u>: Consensus with a single message type, minimal subtlety

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

<u>Goal</u>: "Simplest-Possible", Drop-in replacement for PBFT

<u>Result</u>: Consensus with a single message type, minimal subtlety

- **<u>Consistency</u>**: f < n/3, no synchrony assumptions!

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

<u>Goal</u>: "Simplest-Possible", Drop-in replacement for PBFT
<u>Result</u>: Consensus with a single message type, minimal subtlety

- **<u>Consistency</u>**: f < n/3, no synchrony assumptions!
- **<u>Liveness</u>**: when network is reliable (GST model)

Recap

In every epoch $e = 1, 2, \ldots$

- ❑ <u>leader</u> proposes *b* = (*H*(*b*'), *e*, txs) extending longest notarized chain they've seen
- ❑ <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

<u>Goal</u>: "Simplest-Possible", Drop-in replacement for PBFT

<u>Result</u>: Consensus with a single message type, minimal subtlety

- **<u>Consistency</u>**: f < n/3, no synchrony assumptions!
- **<u>Liveness</u>**: when network is reliable (GST model)

<u>Eprint</u>: ia.cr/2020/088

Questions?

In every epoch $e = 1, 2, \ldots$

- <u>leader</u> proposes *b* = (*H*(*b'*), *e*, txs) extending longest notarized chain they've seen
- <u>voters</u> sign the first valid proposal *b*,
  but i.f.f. *b* also extends a longest notarized chain the *voter* has seen (notarized=2/3 votes)

<u>finalize</u> any notarized chain ending with 3 consecutive epochs, chopping off last block

<u>Goal</u>: "Simplest-Possible", Drop-in replacement for PBFT
<u>Result</u>: Consensus with a single message type, minimal subtlety
- **<u>Consistency</u>**: f < n/3, no synchrony assumptions!
- **<u>Liveness</u>**: when network is reliable (GST model)

<u>Eprint</u>: ia.cr/2020/088