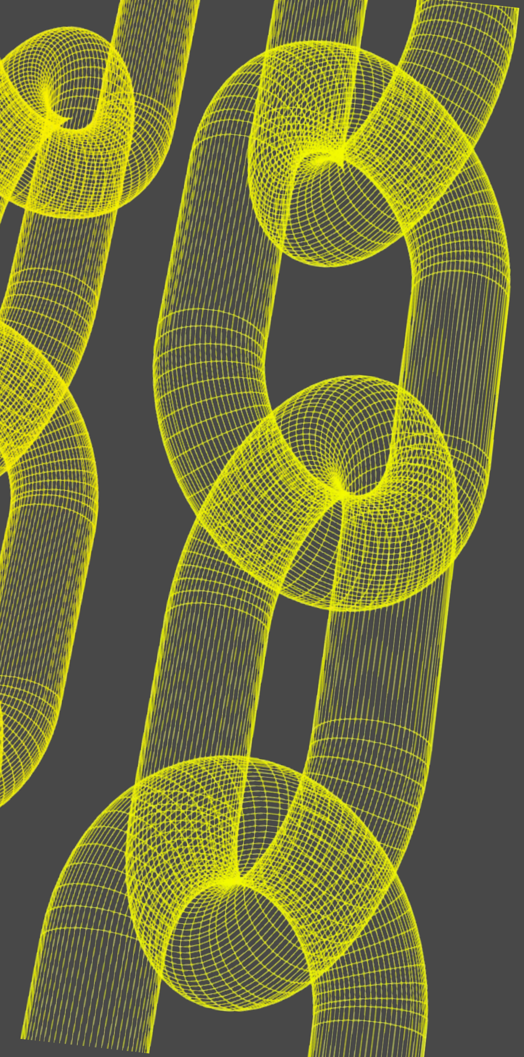


Streamlet:

Textbook streamlined blockchain protocols

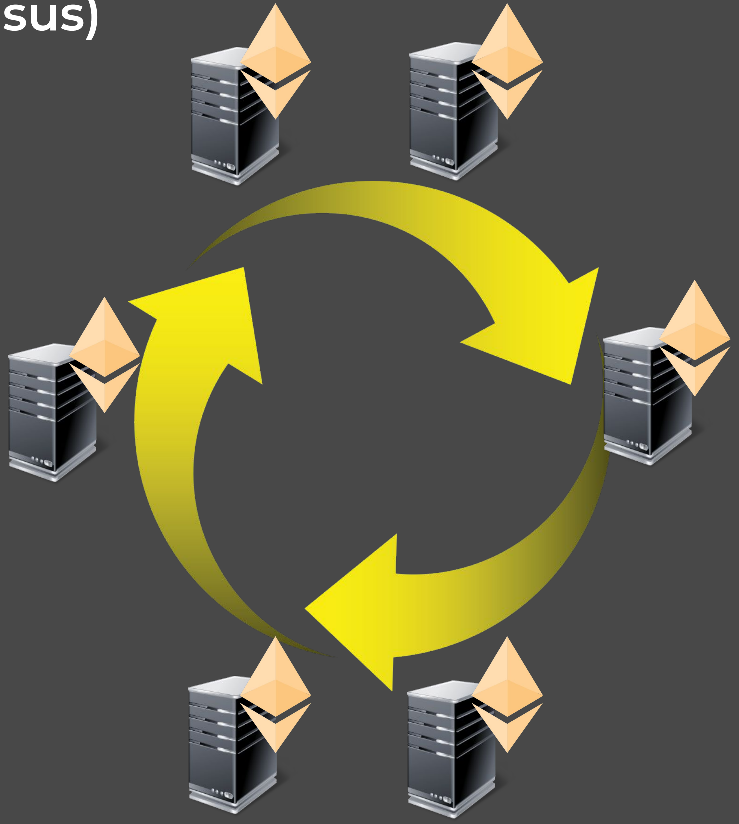
Elaine Shi

Joint work with Benjamin Chan

Streamlet is inspired by Casper, Dfinity, Hotstuff, Pili, Pala...

Blockchain

(a.k.a. state machine replication, consensus)

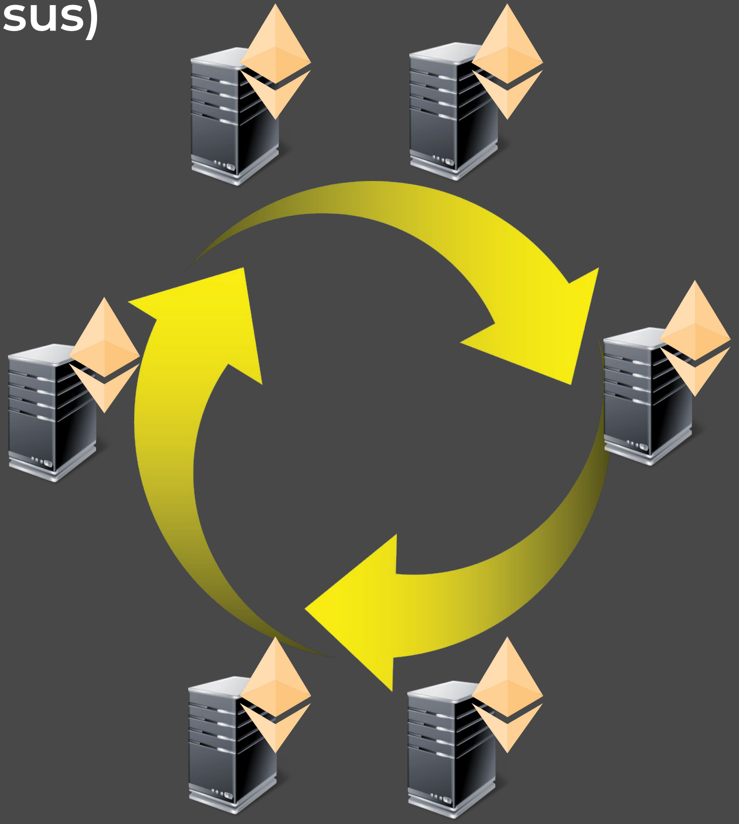


Blockchain

(a.k.a. state machine replication, consensus)

Consistency:
Honest players agree on log

Liveness:
TXs are incorporated soon



Blockchain: A 30-year-old Problem

YAHOO!

facebook

reddit

NetApp

Apache Zookeeper

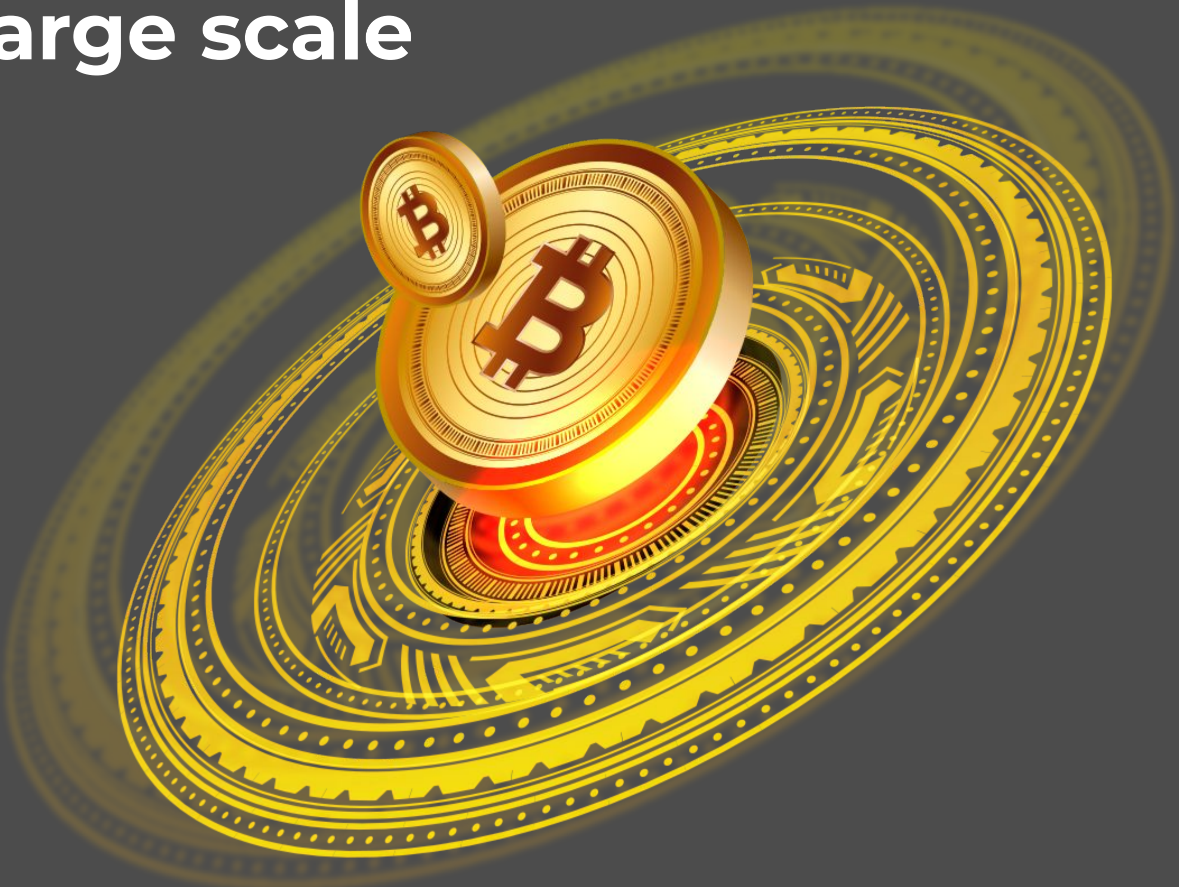
Solr

UBER

ebay

rackspace

Cryptocurrencies brought consensus to a large scale

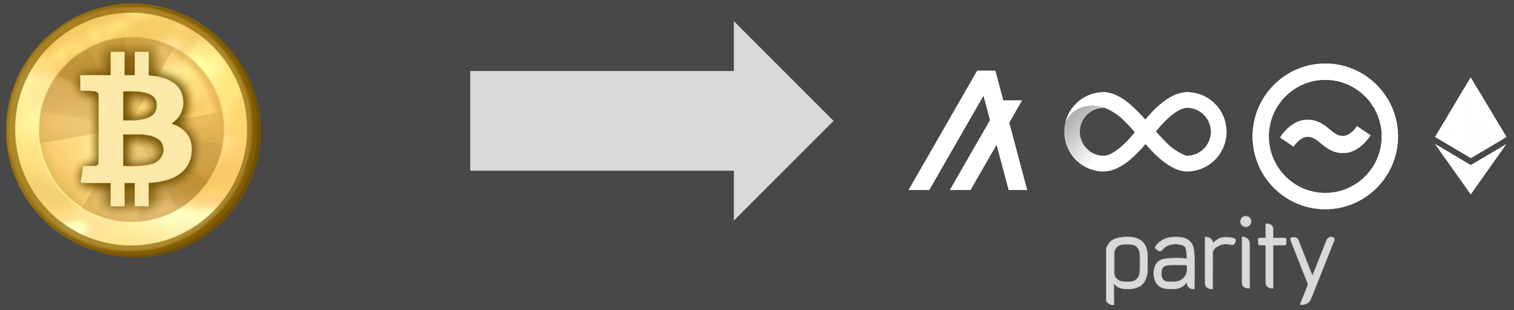


Enables **permissionless** consensus

Proof of work

Proof of work

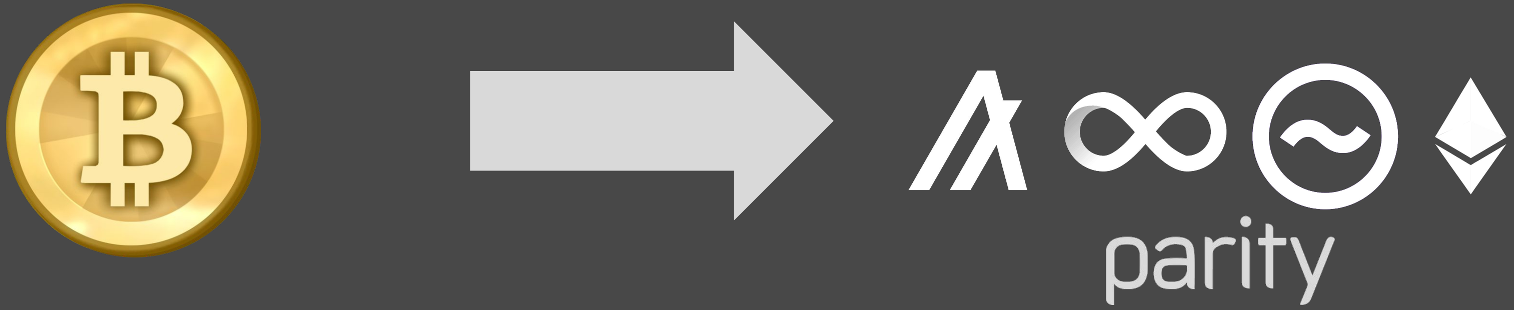
Proof of stake



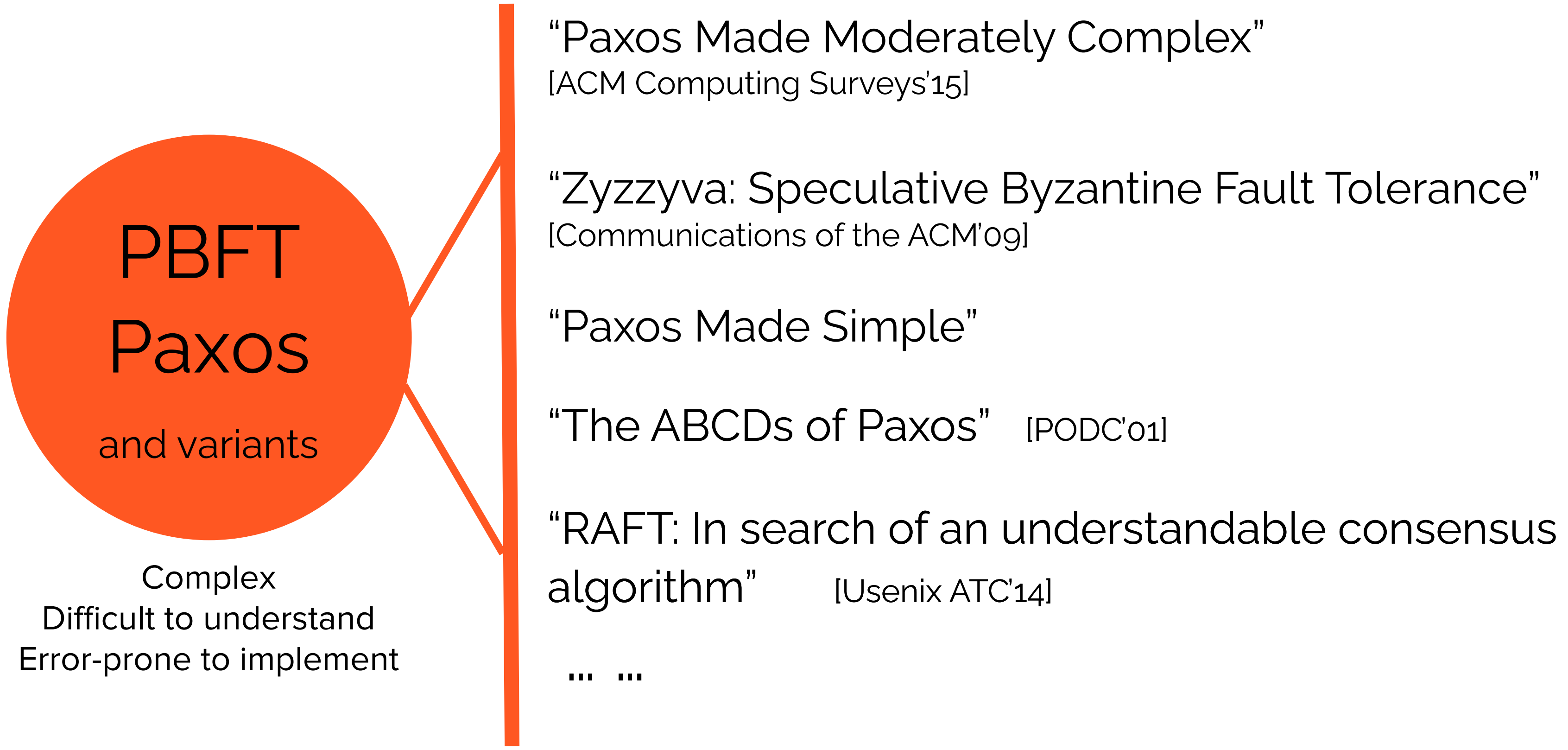
Rely on **permissioned** consensus

Proof of work

Proof of stake



Pursuit of a “Simple” Consensus Protocol



PBFT
Paxos

and variants

Complex
Difficult to understand
Error-prone to implement

“Paxos Made Moderately Complex”
[ACM Computing Surveys’15]

“Zyzzyva: Speculative Byzantine Fault Tolerance”
[Communications of the ACM’09]

“Paxos Made Simple”

“The ABCDs of Paxos” [PODC’01]

“RAFT: In search of an understandable consensus algorithm” [Usenix ATC’14]

… …

Streamlet

👍 Simple

👍 Natural

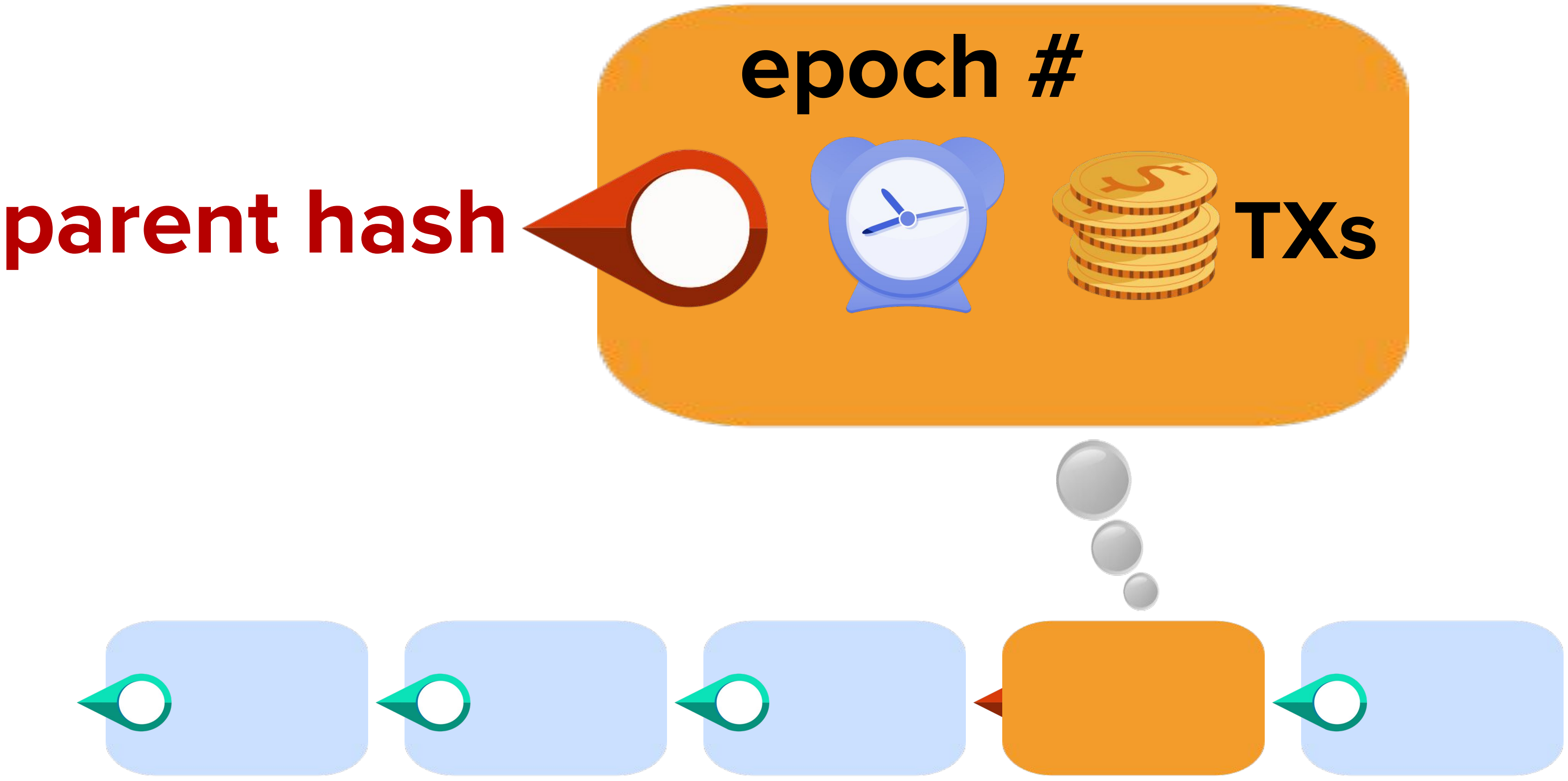
👍 Unified, for pedagogy & implementation

Roadmap

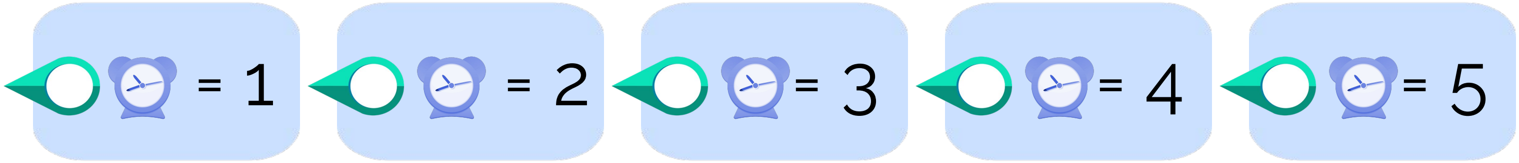
Classical approaches
(e.g., pbft, paxos)

Streamlet: a streamlined blockchain

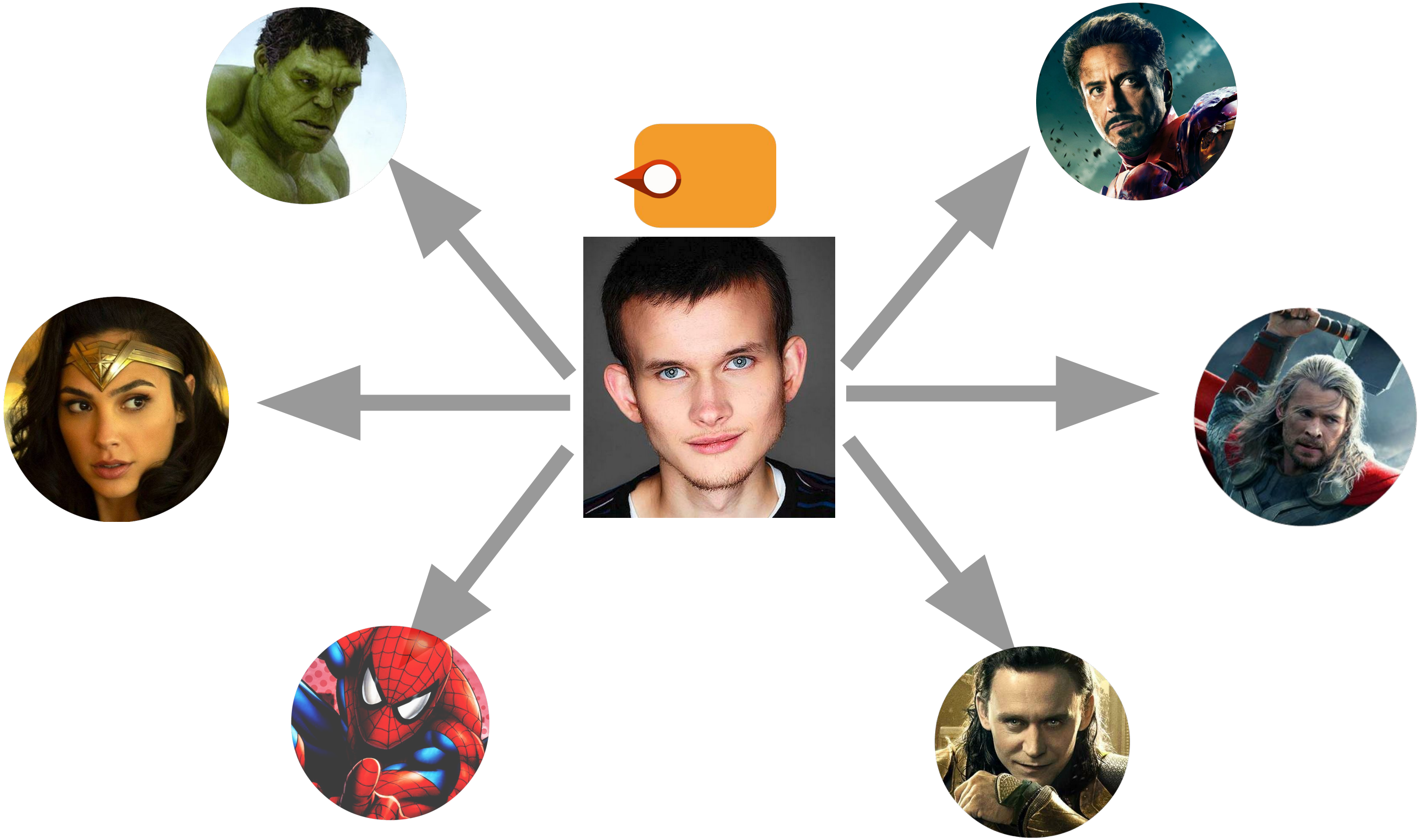
Block Format



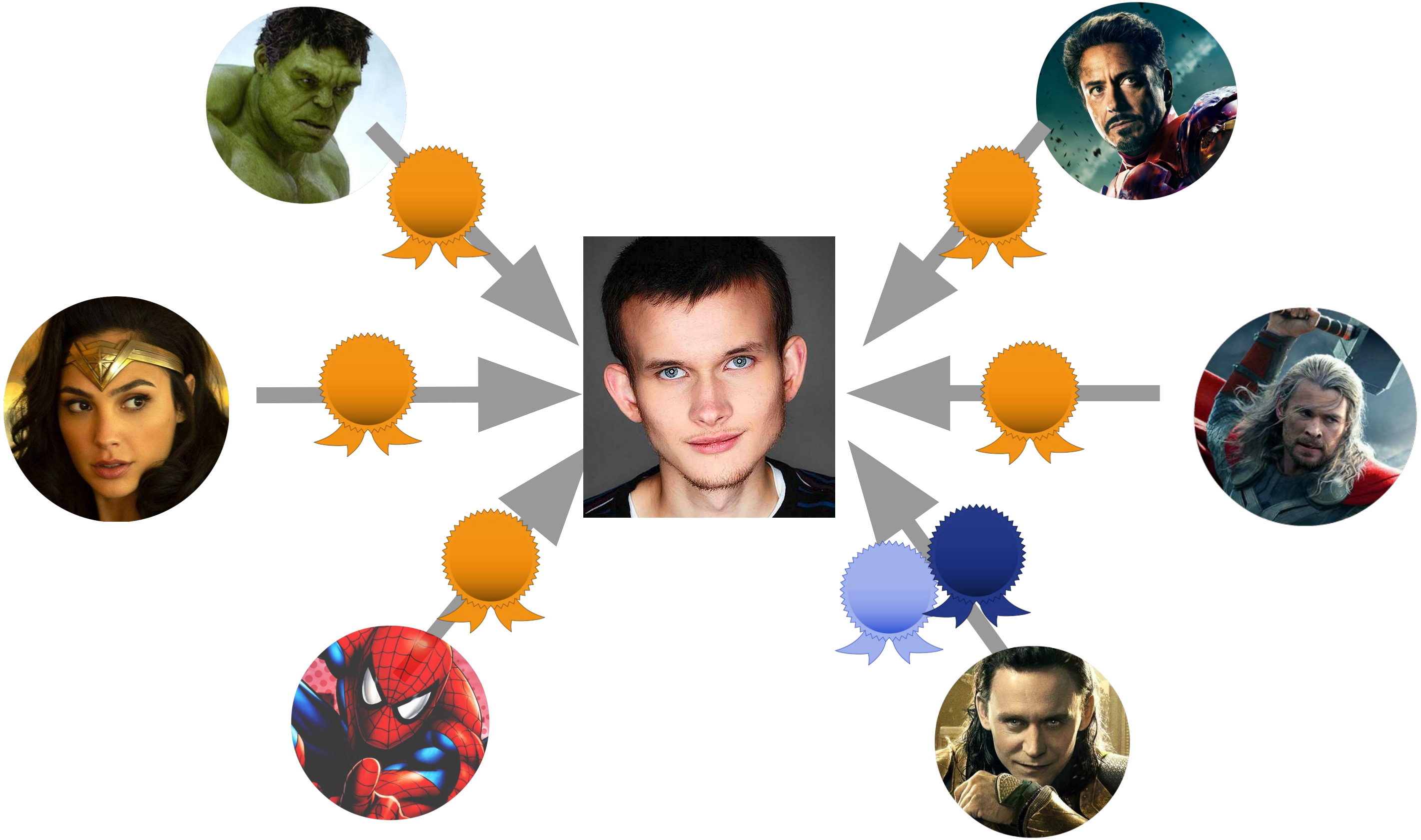
Assume: ⏰s increment in a valid blockchain



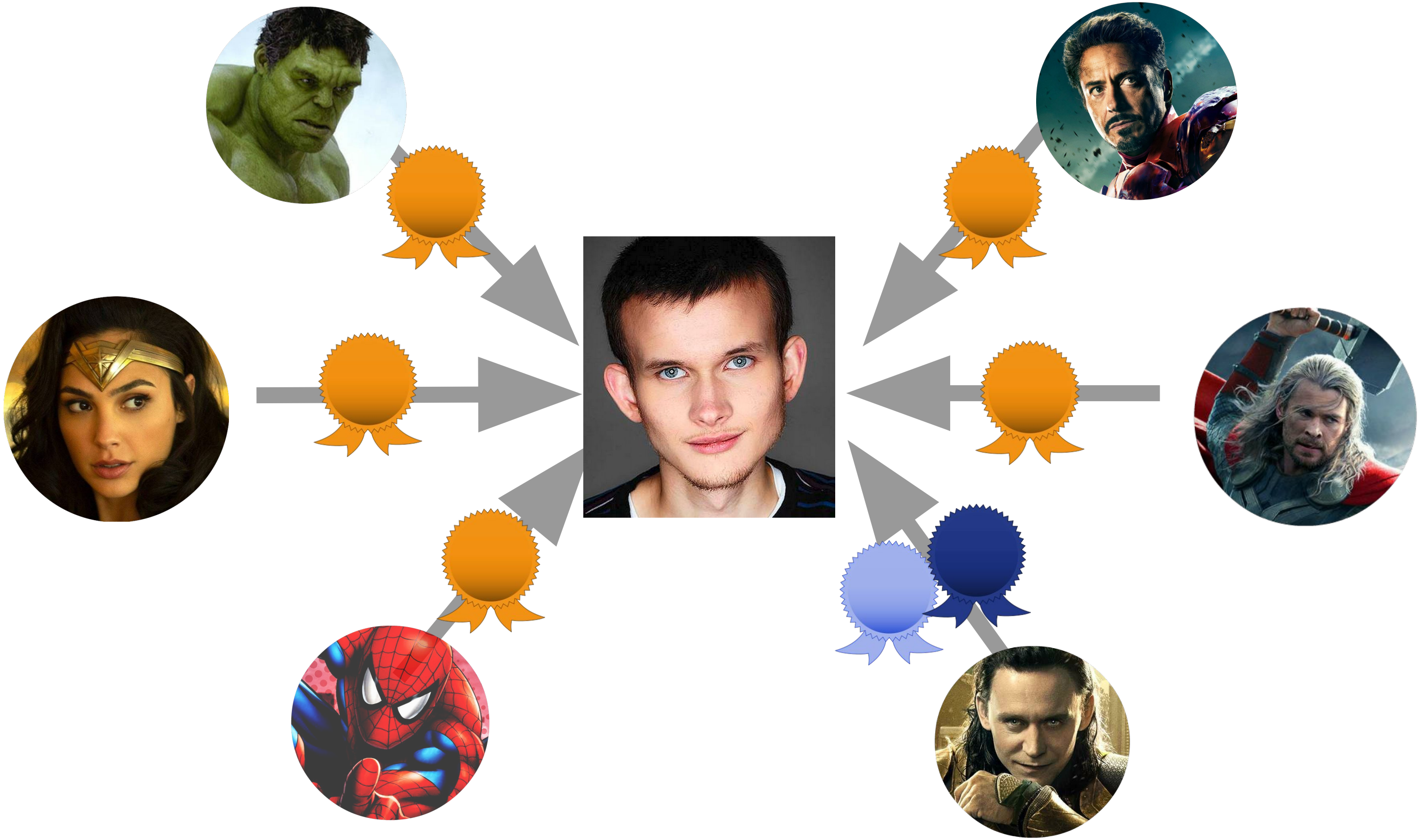
1 Leader proposes block



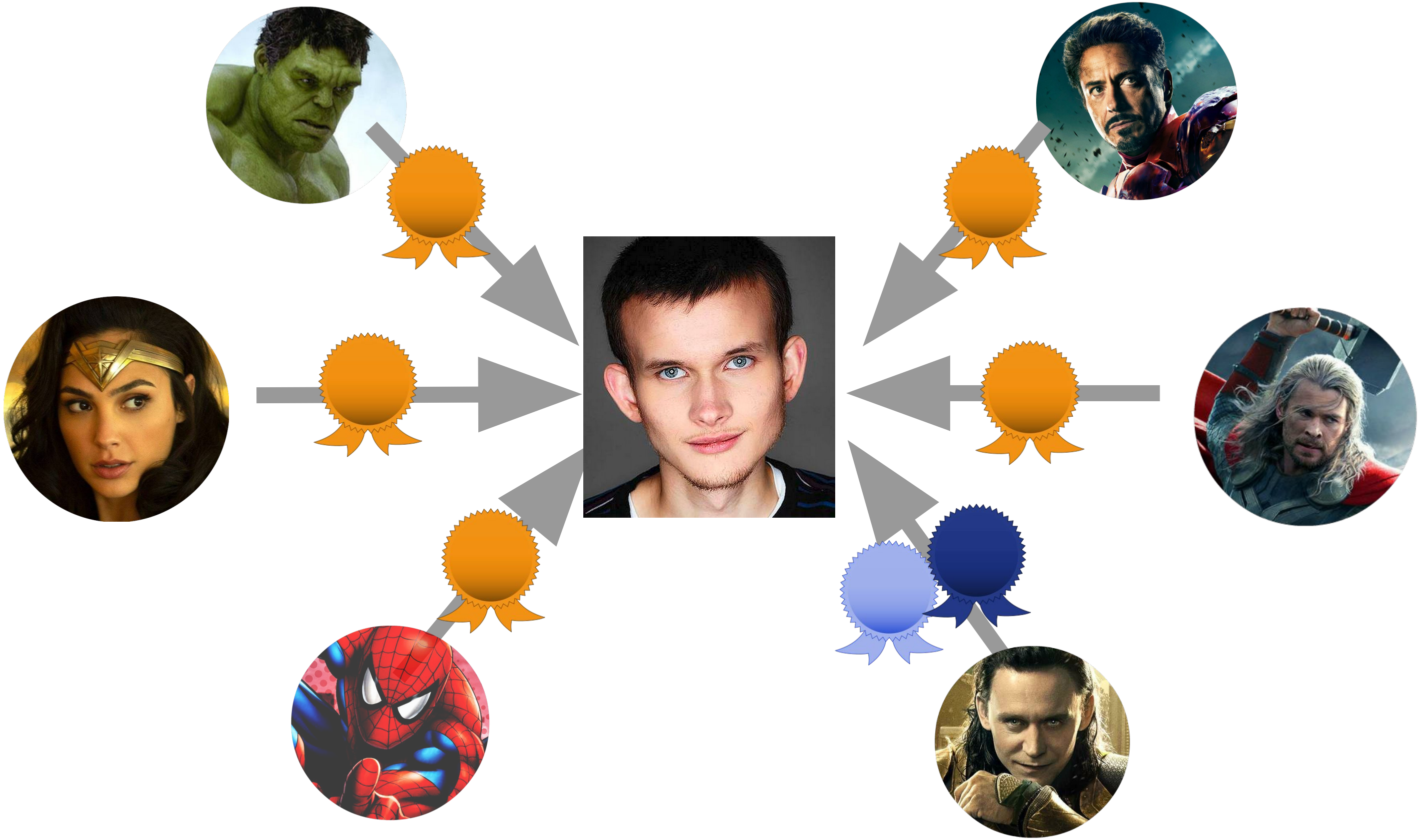
2 Vote



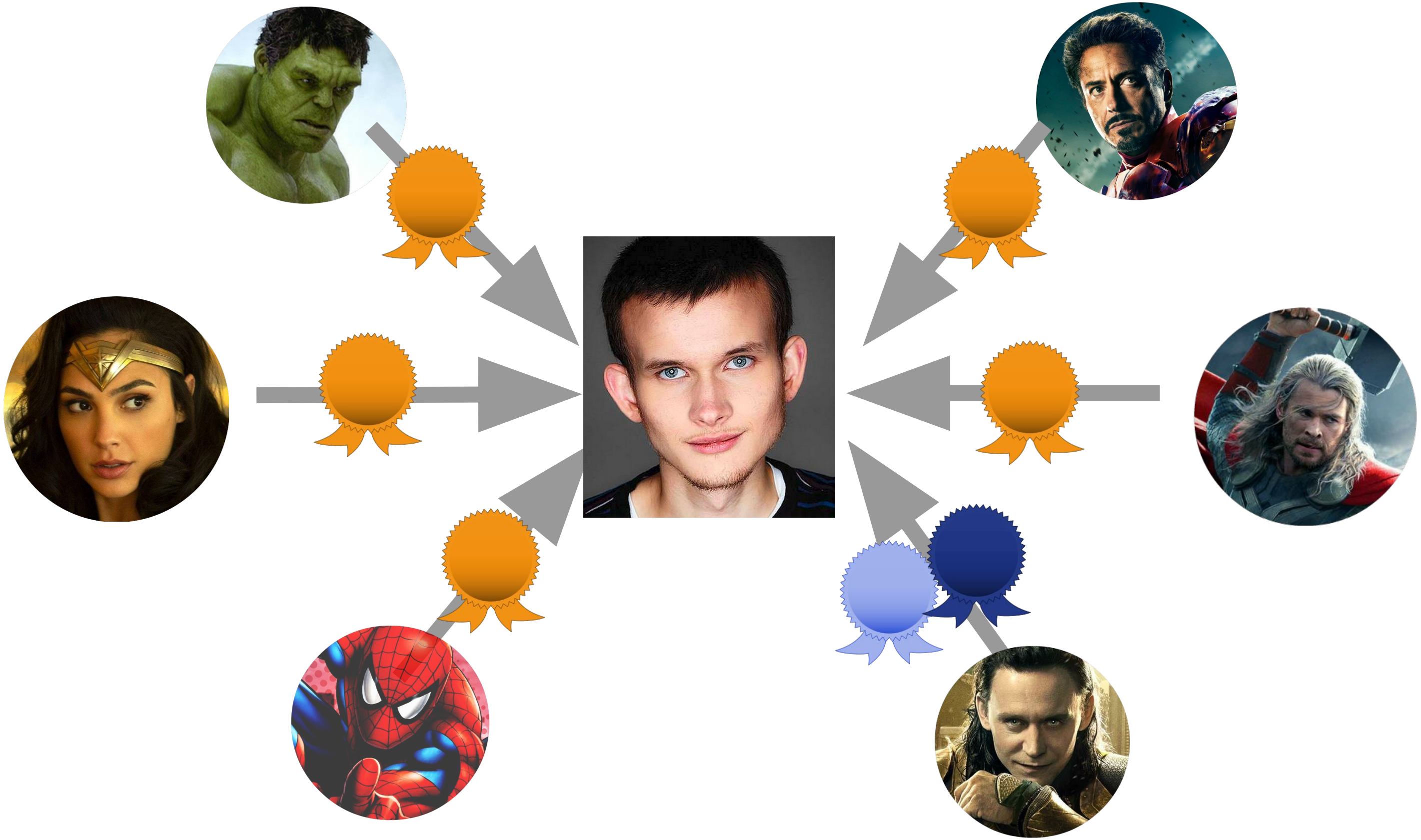
3 Finalize 🟧 upon ⅔ n votes



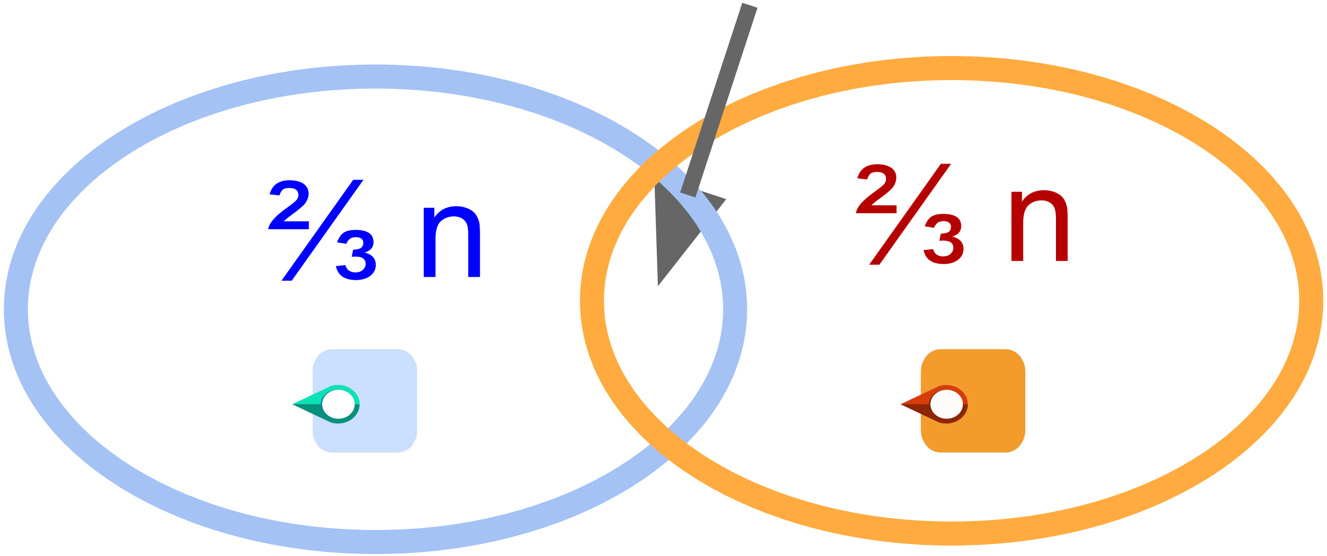
⅔ n votes: notarization



Honest players vote **uniquely** each epoch

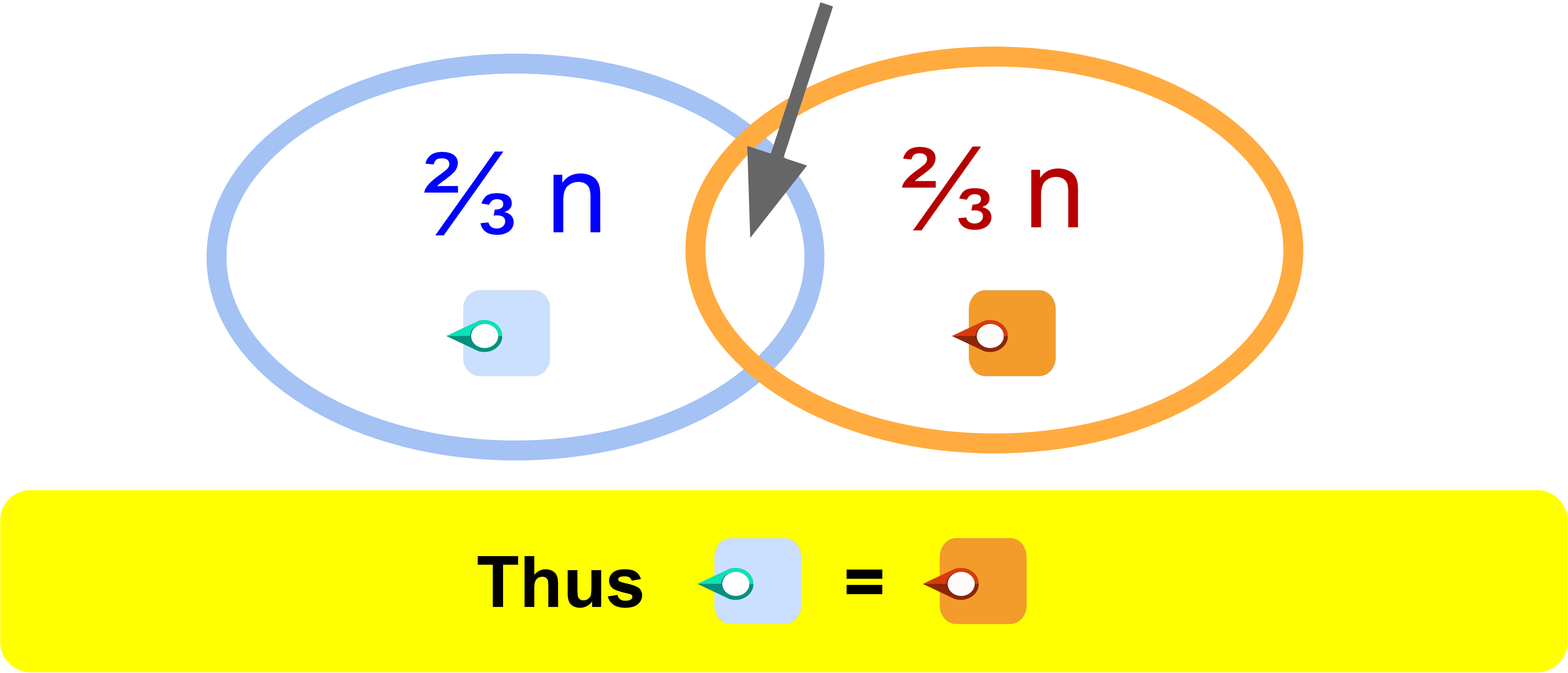


Must intersect at an honest player

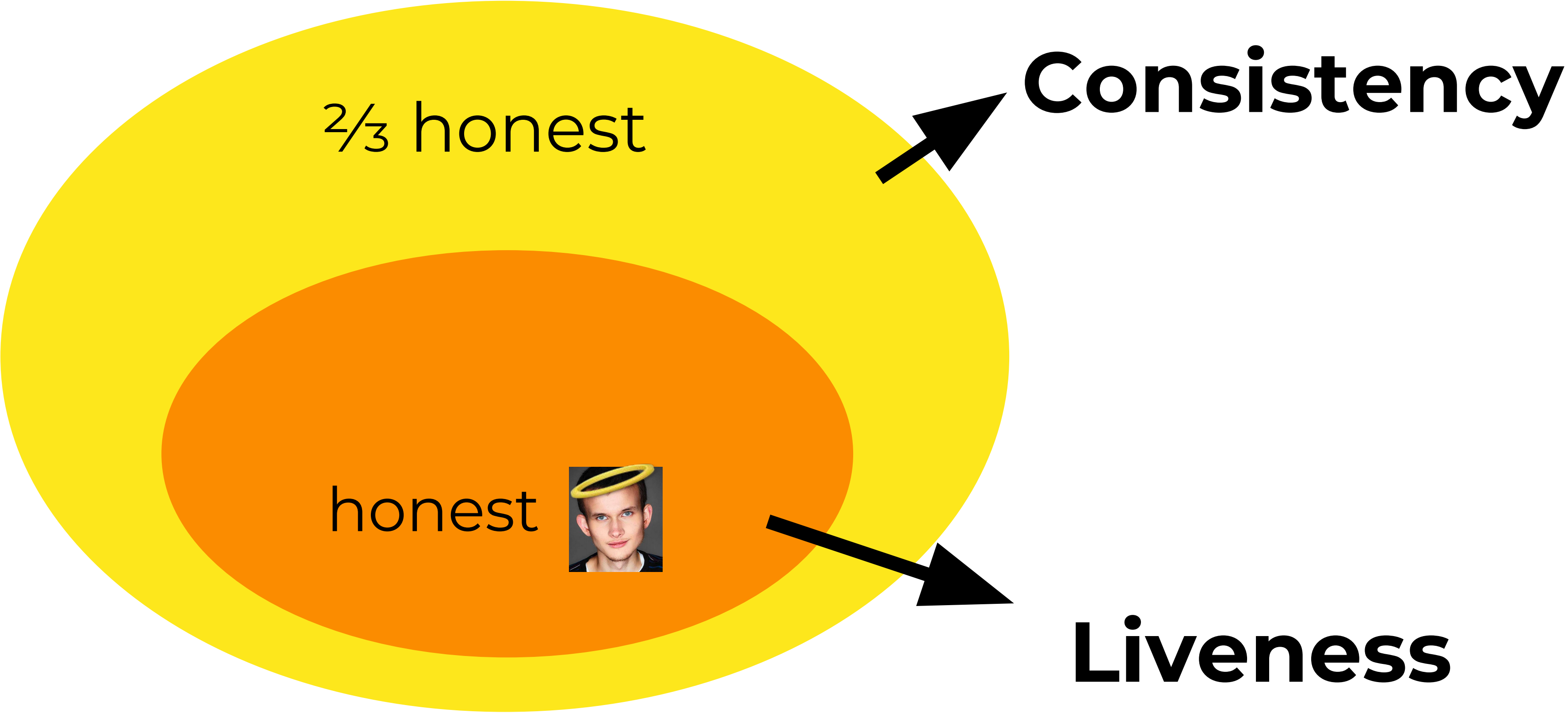


Assume: $< \frac{1}{3}n$ corrupt

Must intersect at an honest player



Thus =

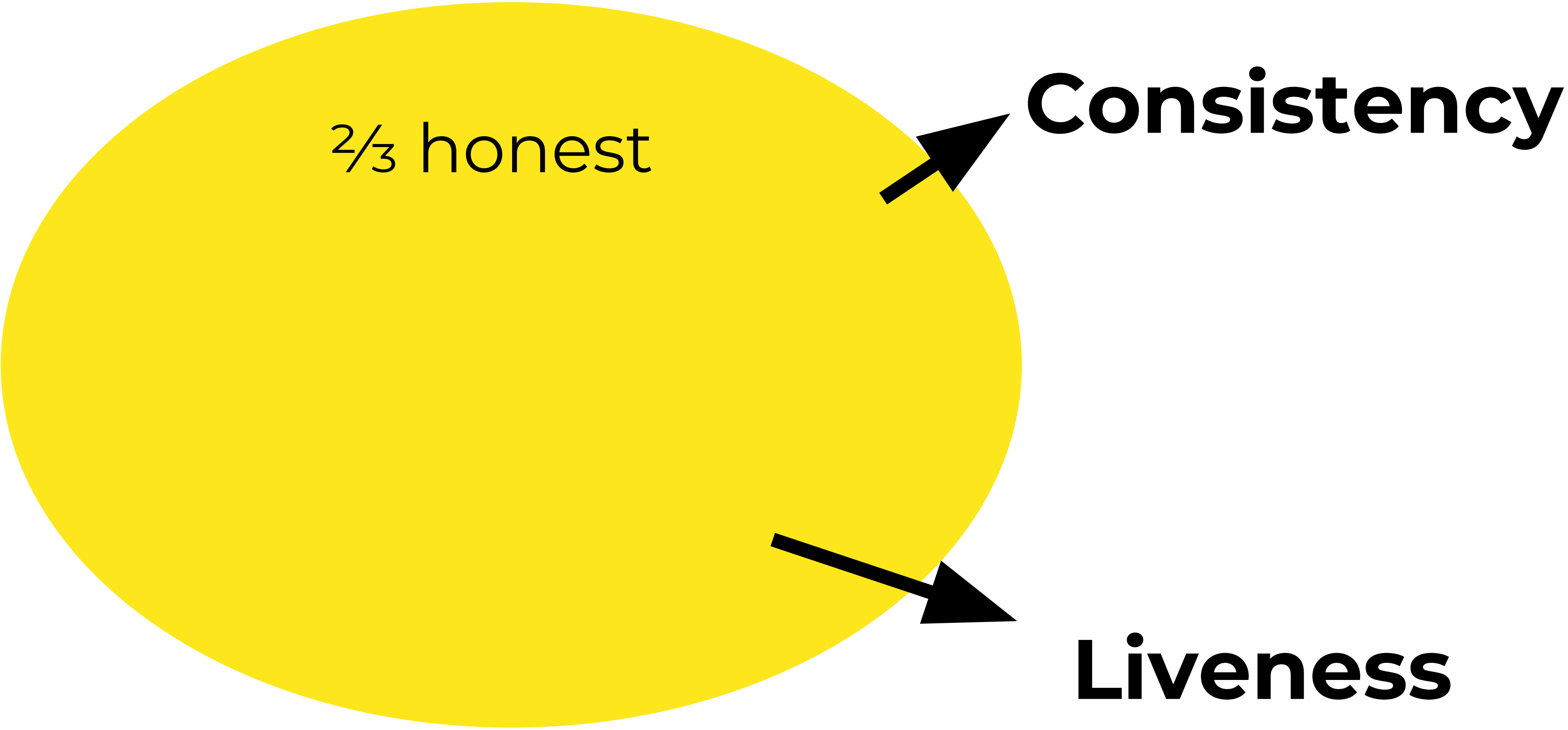


⅔ honest

honest

Consistency

Liveness

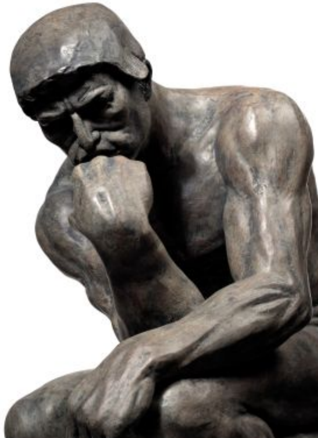


⅔ honest

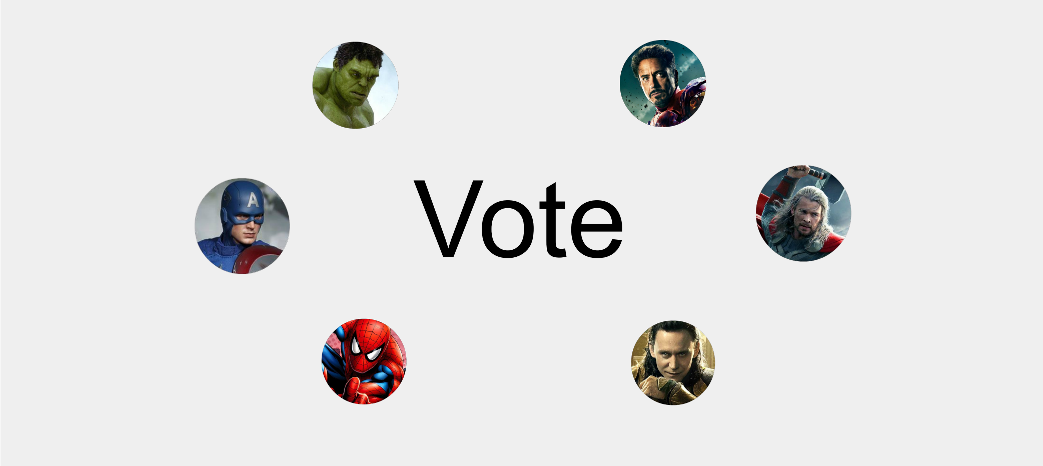
Consistency

Liveness

How do we achieve liveness?



Anatomy of classical consensus



Vote

Simple normal path

Complicated recovery path

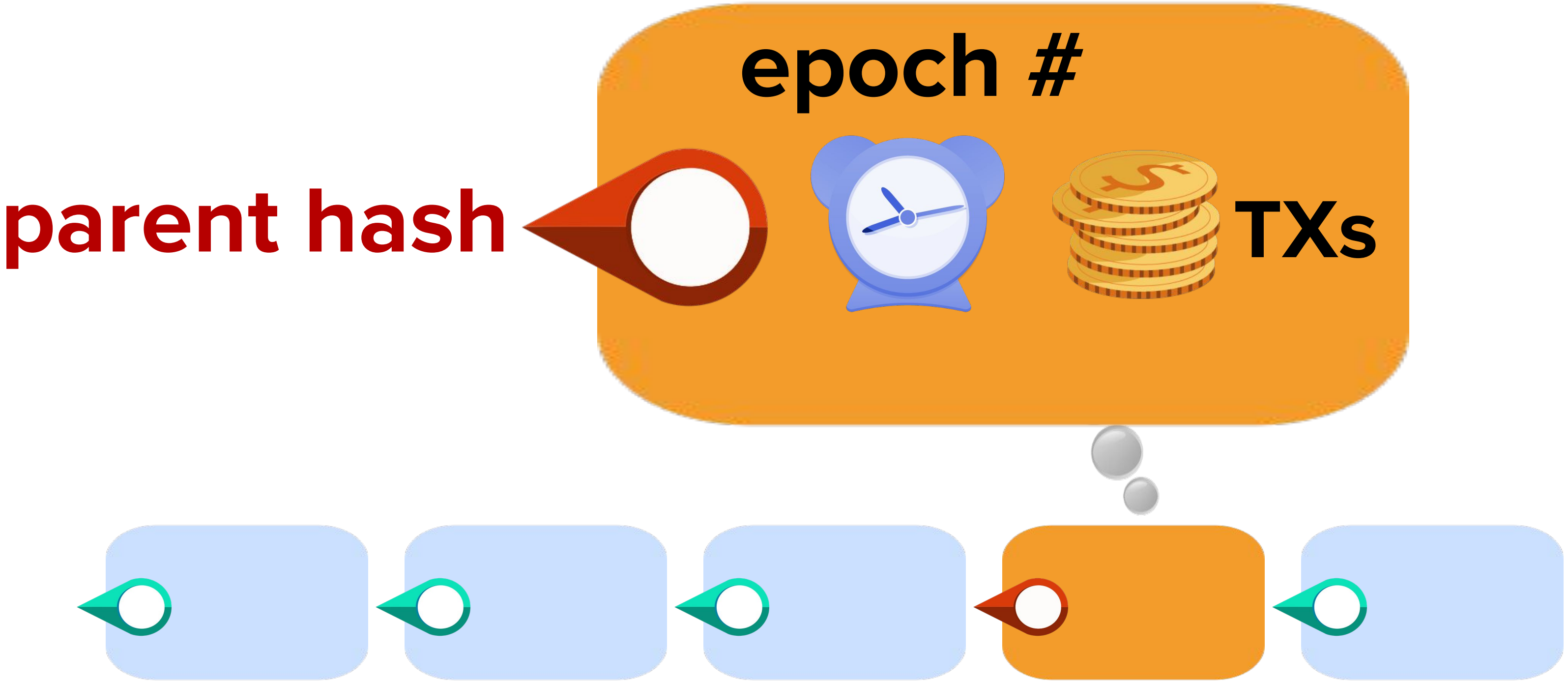
Can we achieve **full** consensus **as simply as the normal path**?

Roadmap

Classical approaches
(e.g., pbft, paxos)

Streamlet

Assume: epoch = 1 sec ≥ 1 roundtrip



Leader rotation

Player $H(i) \bmod n$ is the leader in epoch i

Easy to support any other leader-rotation policy

- **Propose**

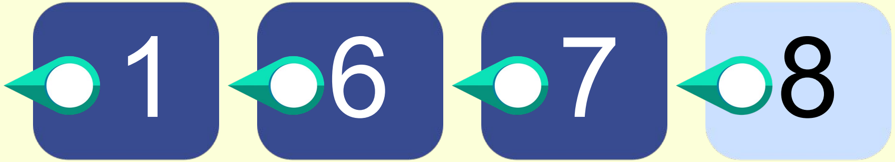
  extend longest notarized chain

- **Vote**

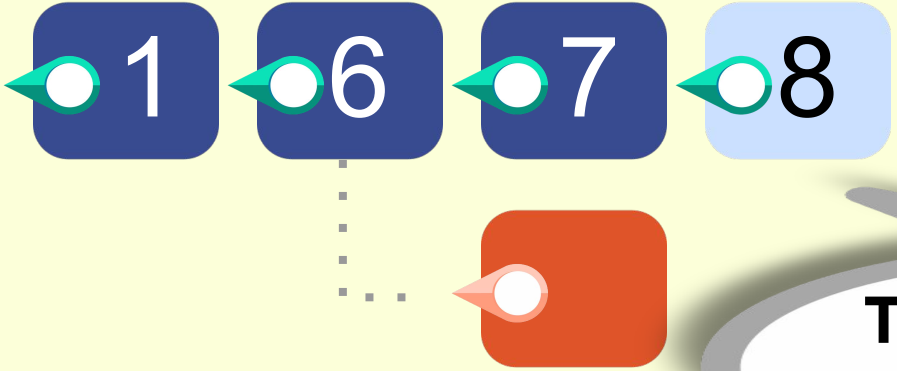
  vote for the 1st proposal from leader iff it extends from one of the longest notarized chains seen

} **Every epoch**

- **Finalization**: 3 consecutive epochs appear together in a notarized chain, all but last final



- **Finalization:** 3 consecutive epochs appear together in notarized chain, all but last final



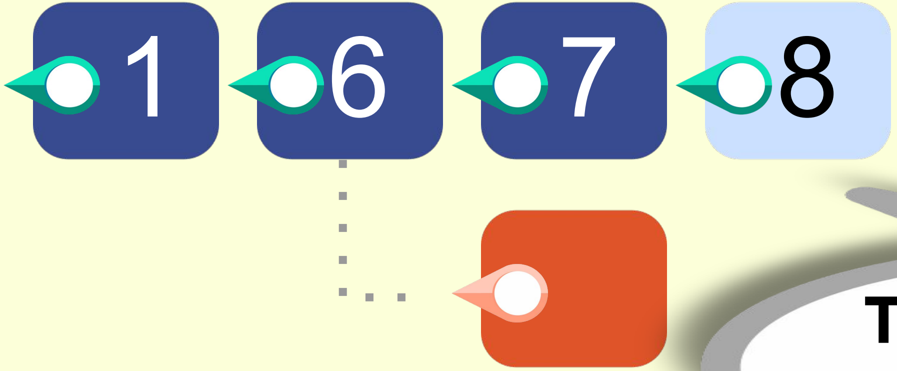
To prove: this cannot happen

This talk

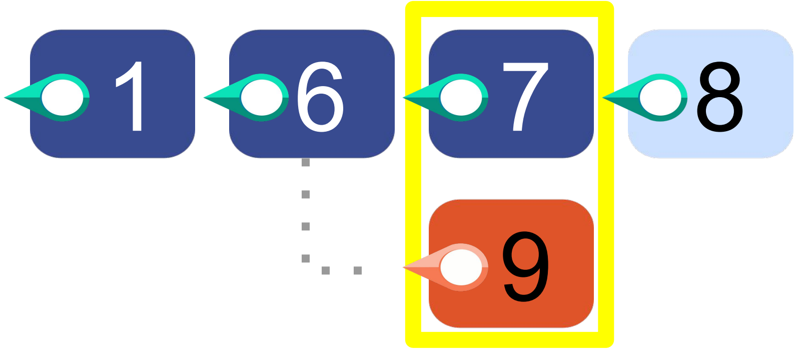
1. Consistency Proof

2. Liveness Proof

- **Finalization:** 3 consecutive epochs in notarized chain, all but last final

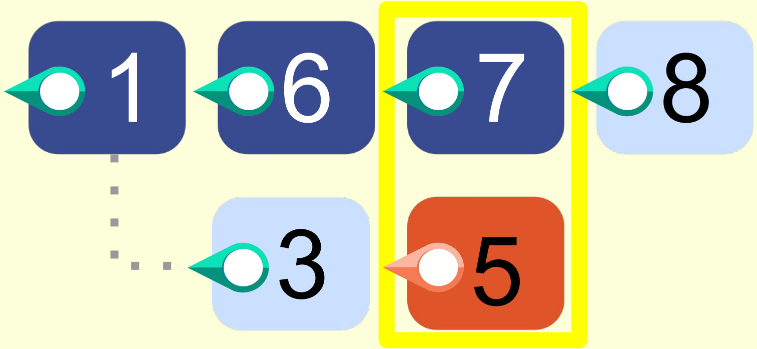


To prove: this cannot happen

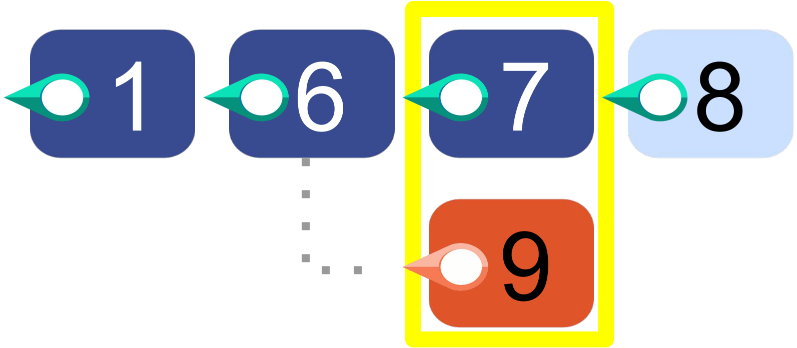


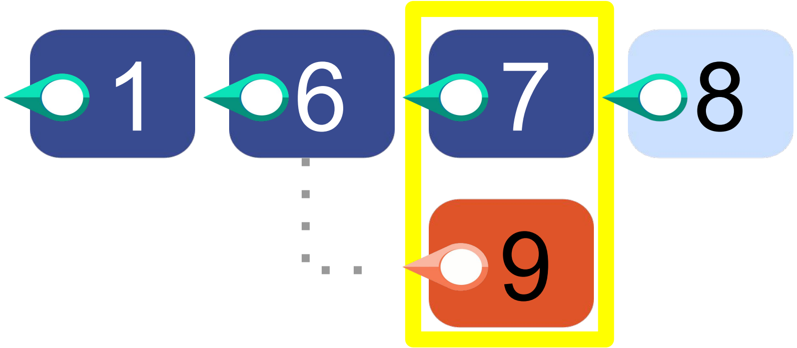
Case 1

Case 2



Lemma: every epoch has at most 1 notarized block.

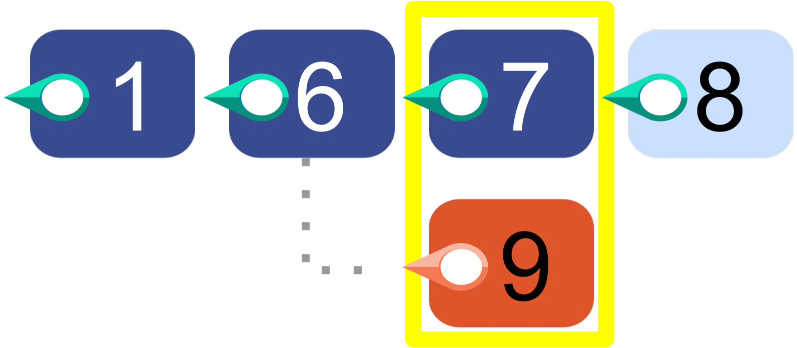

1
6
7
8
9



“many”: > n/3 honest

Proof:

many voted for 8 in epoch 8

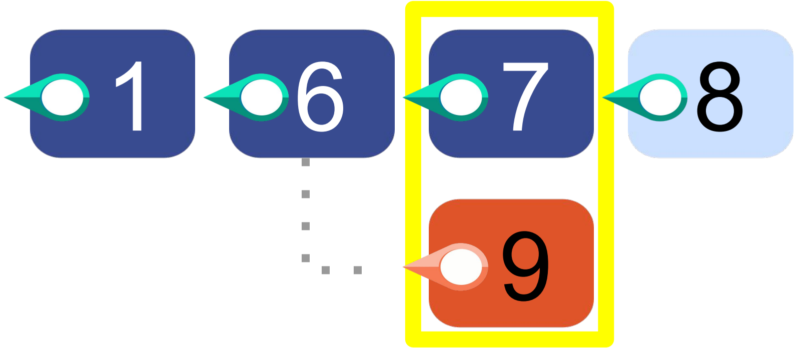


“many”: > n/3 honest

Proof:

many voted for 8 in epoch **8**

--> many saw 7 notarized in epoch **8**



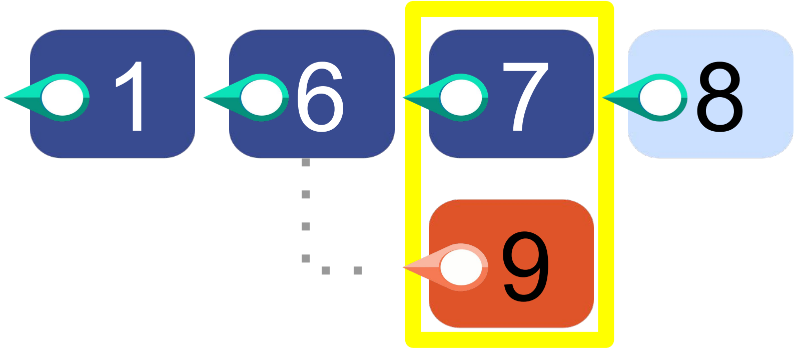
“many”: > n/3 honest

Proof:

many voted for 8 in epoch 8

--> many saw 7 notarized in epoch 8 --

-> they will not vote for 9 in epoch 9



“many”: > n/3 honest

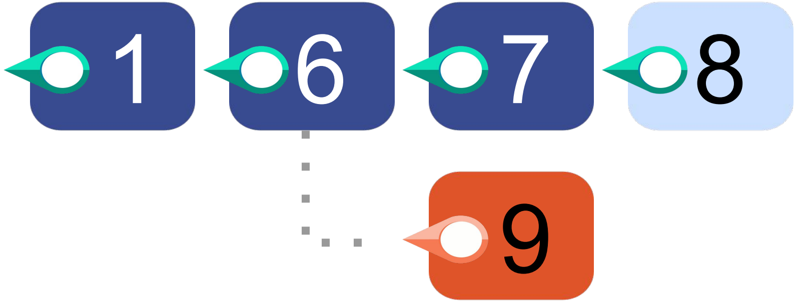
Proof:

many voted for 8 in epoch 8

--> many saw 7 notarized in epoch 8

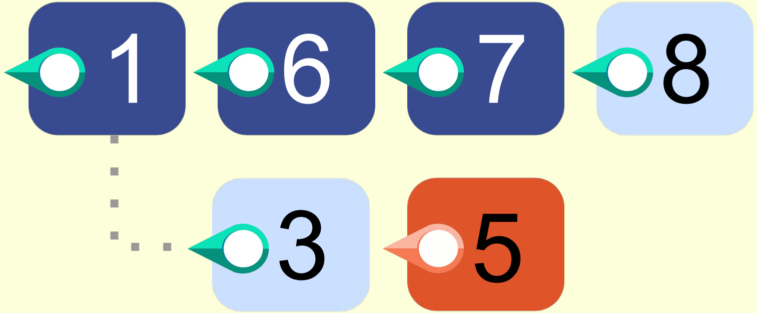
--> they will not vote for 9 in epoch 9

--> 9 cannot gain notarization



Case 1

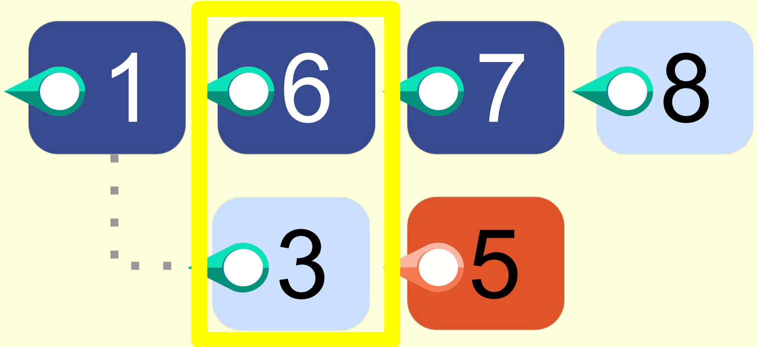
Case 2



“many” : > n/3 honest

Proof:

many voted for 5 in epoch **5**

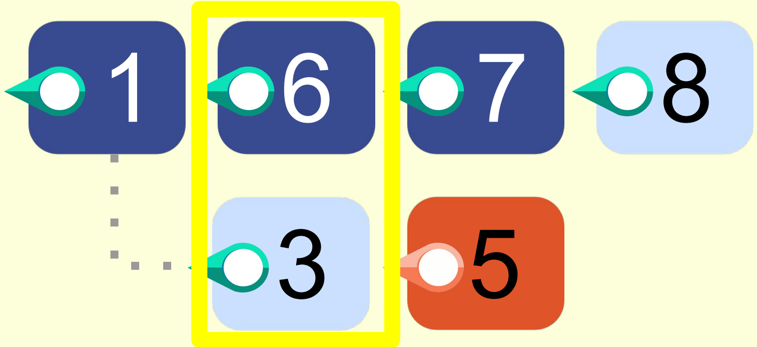


“many” : > n/3 honest

Proof:

many voted for 5 in epoch **5**

--> many saw 3 notarized in epoch **5**



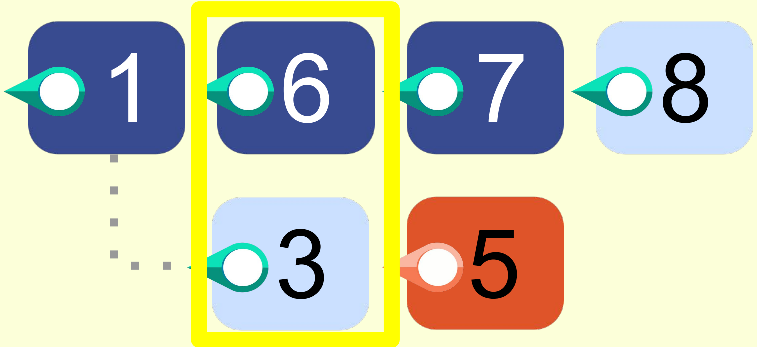
“many” : > n/3 honest

Proof:

many voted for 5 in epoch 5

--> many saw 3 notarized in epoch 5

--> they will not vote for 6 in epoch 6



“many” : > n/3 honest

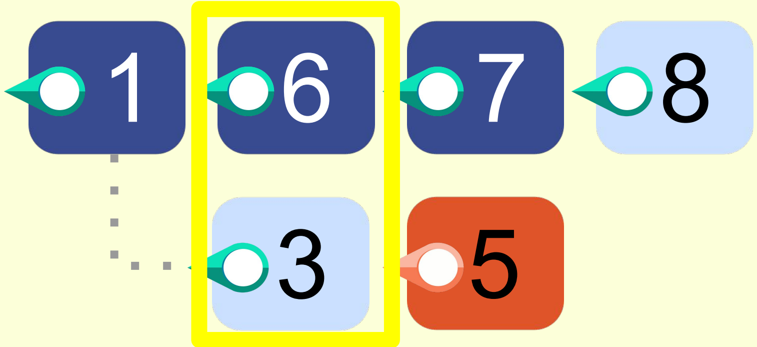
Proof:

many voted for 5 in epoch **5**

--> many saw 3 notarized in epoch **5**

--> they will not vote for 6 in epoch **6**

--> 6 cannot gain notarization



“many” : > n/3 honest

Proof:

many voted for 5 in epoch 5

--> many saw 3 notarized in epoch 5

--> they will not vote for 6 in epoch 6

--> 6 cannot gain notarization

Consistency does not depend on sync. assumptions!

Summary: streamlined blockchains

- Every epoch allows leader-switch.
- View change embedded in a unified "propose-vote" paradigm.

Read after me:

- Propose-vote, propose-vote, propose-vote
- Boom boom boom
- Don’t finalize upon notarization
- 3 consecutive epochs appear together, chop off the last and finalize the prefix

“Foundations of Distributed Consensus and Blockchains”
www.distributedconsensus.net

Thank You!

runting@gmail.com