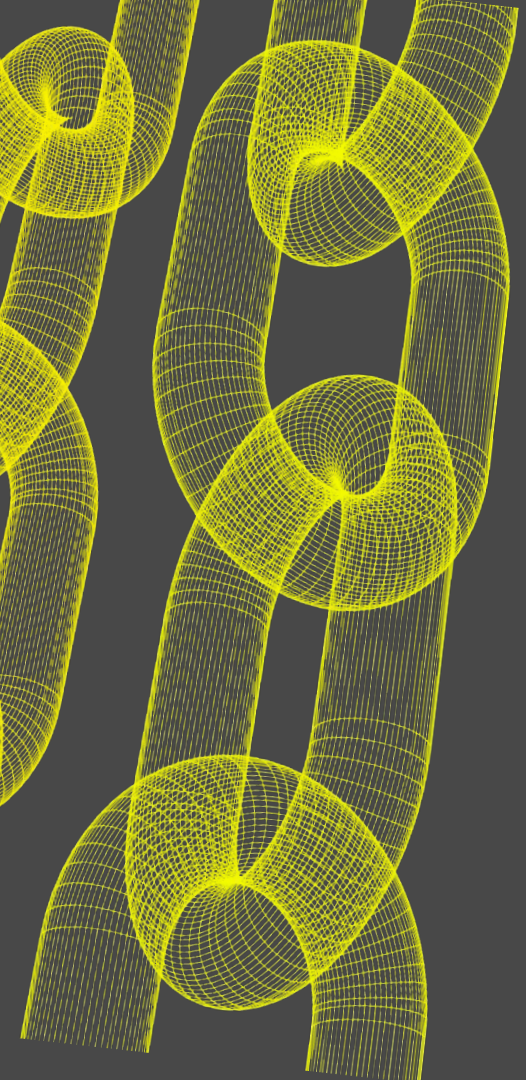


(Casper, Dfinity, Hotstuff, Pili, Pala...)

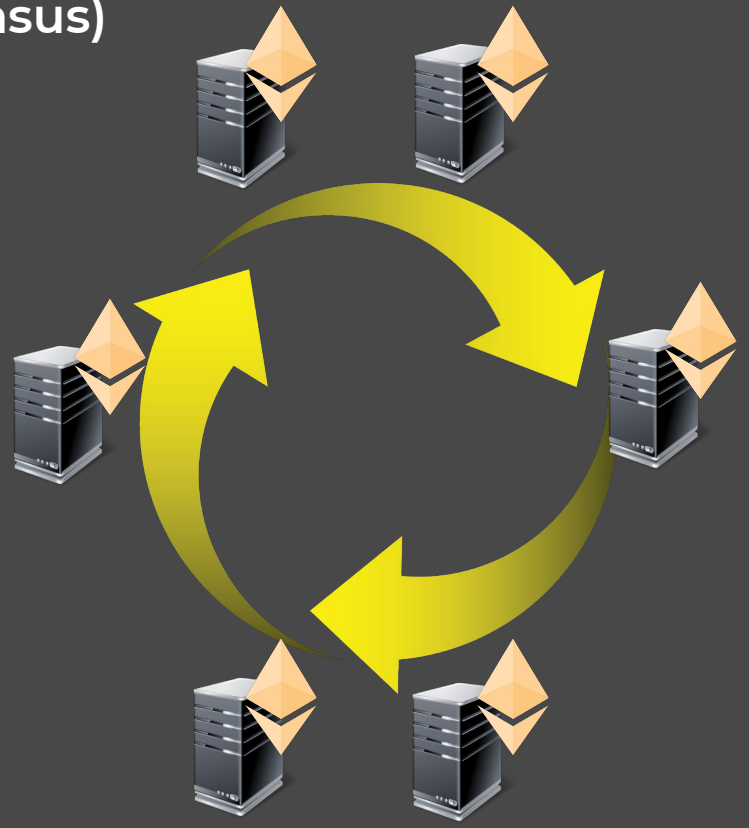
Streamlet:
Textbook streamlined blockchain protocols

Elaine Shi
Cornell

Joint work with Benjamin Chan

Blockchain

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

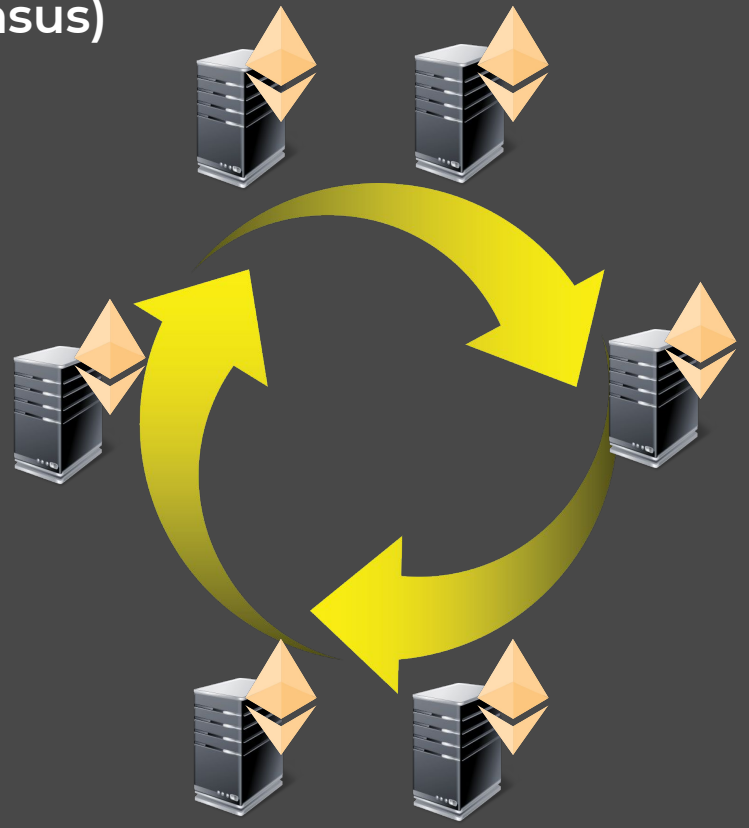


Blockchain

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

Consistency:
Honest nodes agree on log

Liveness:
TXs are incorporated soon



Blockchain: A 30-year-old Problem

YAHOO!

facebook

reddit

NetApp

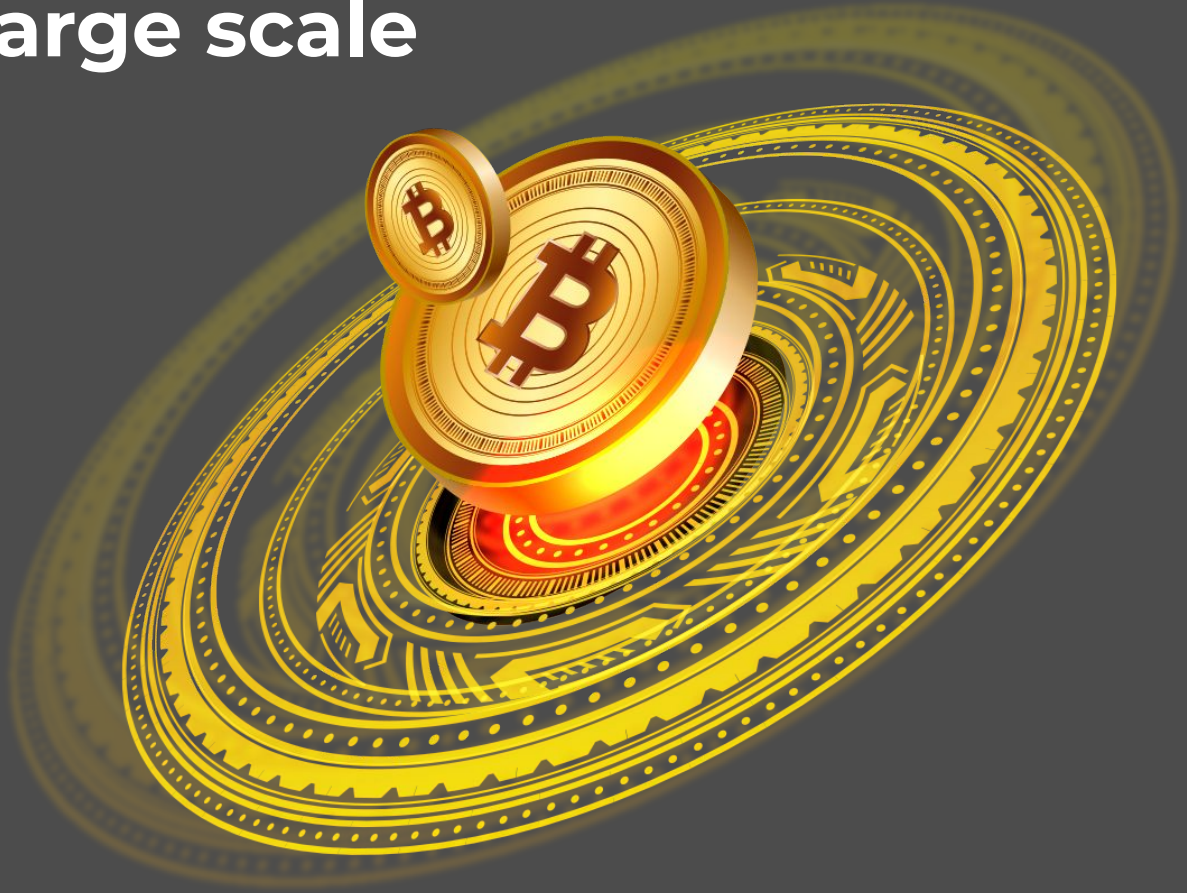
Solr

UBER

ebay

rackspace

Cryptocurrencies brought consensus to a large scale

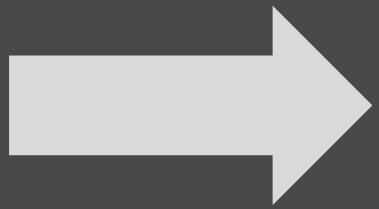


Proof of work

Enables permissionless consensus

Proof of work

Proof of work



Proof of stake

Rely on **permissioned** consensus

Proof of work

Proof of stake

parity

Blockchain

Every round t, node i outputs *longest* final log denoted LOG_i^t

- **Consistency**: for any honest i, j, and t, t',

$$\mathrm{LOG}_i^t \prec \mathrm{LOG}_j^{t'} \quad \text{or} \quad \mathrm{LOG}_j^{t'} \prec \mathrm{LOG}_i^t$$

Holds for 1-negl probability over the choice of execution

Blockchain

Every round t, node i outputs *longest* final log denoted LOG_i^t

- **Consistency**: for any honest i, j, and t, t',

$$\mathrm{LOG}_i^t \prec \mathrm{LOG}_j^{t'} \quad \text{or} \quad \mathrm{LOG}_j^{t'} \prec \mathrm{LOG}_i^t$$

- **Liveness**: if an honest node receives input tx in round t, then in round $t + T(\lambda, n, \Delta)$, any honest node has tx in its LOG

Holds for 1-negl probability over the choice of execution

Blockchain

Single-shot consensus

In PKI setting, equivalent to BA from a feasibility perspective

Blockchain

In PKI setting, equivalent to BA from a feasibility perspective

Is blockchain a meaningful abstraction?

Blockchain: 2 approaches

PODC, CRYPTO community

Sequential composition of BA

SOSP, NDSI, real-world community

Direct blockchain construction

(e.g., pbft, paxos)

Blockchain: 2 approaches

PODC, CRYPTO community

Sequential composition of BA

SOSP, NDSI, real-world community

Direct blockchain construction

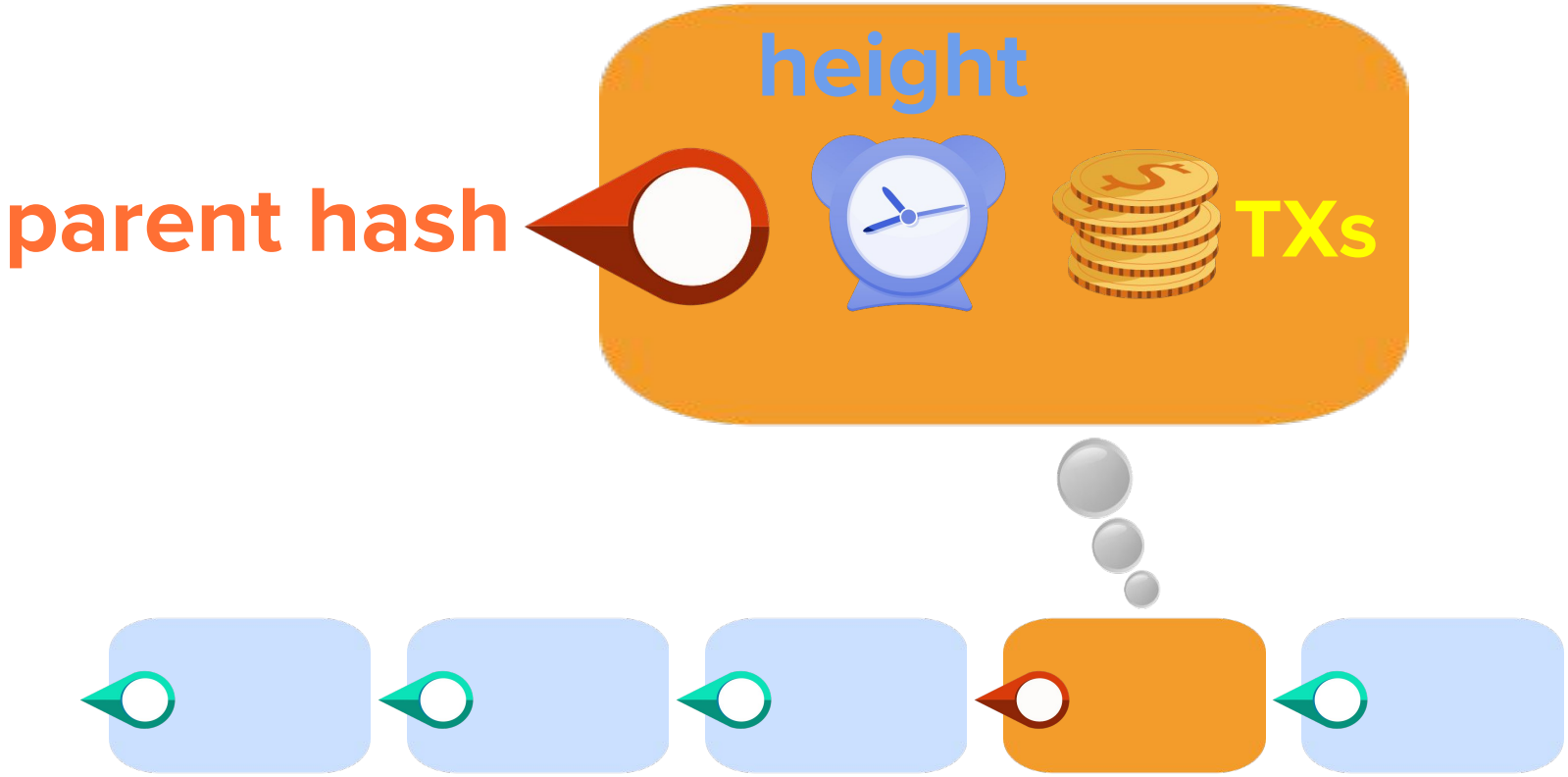
(e.g., pbft, paxos)

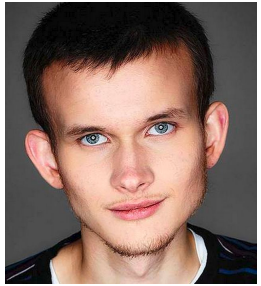
Roadmap

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

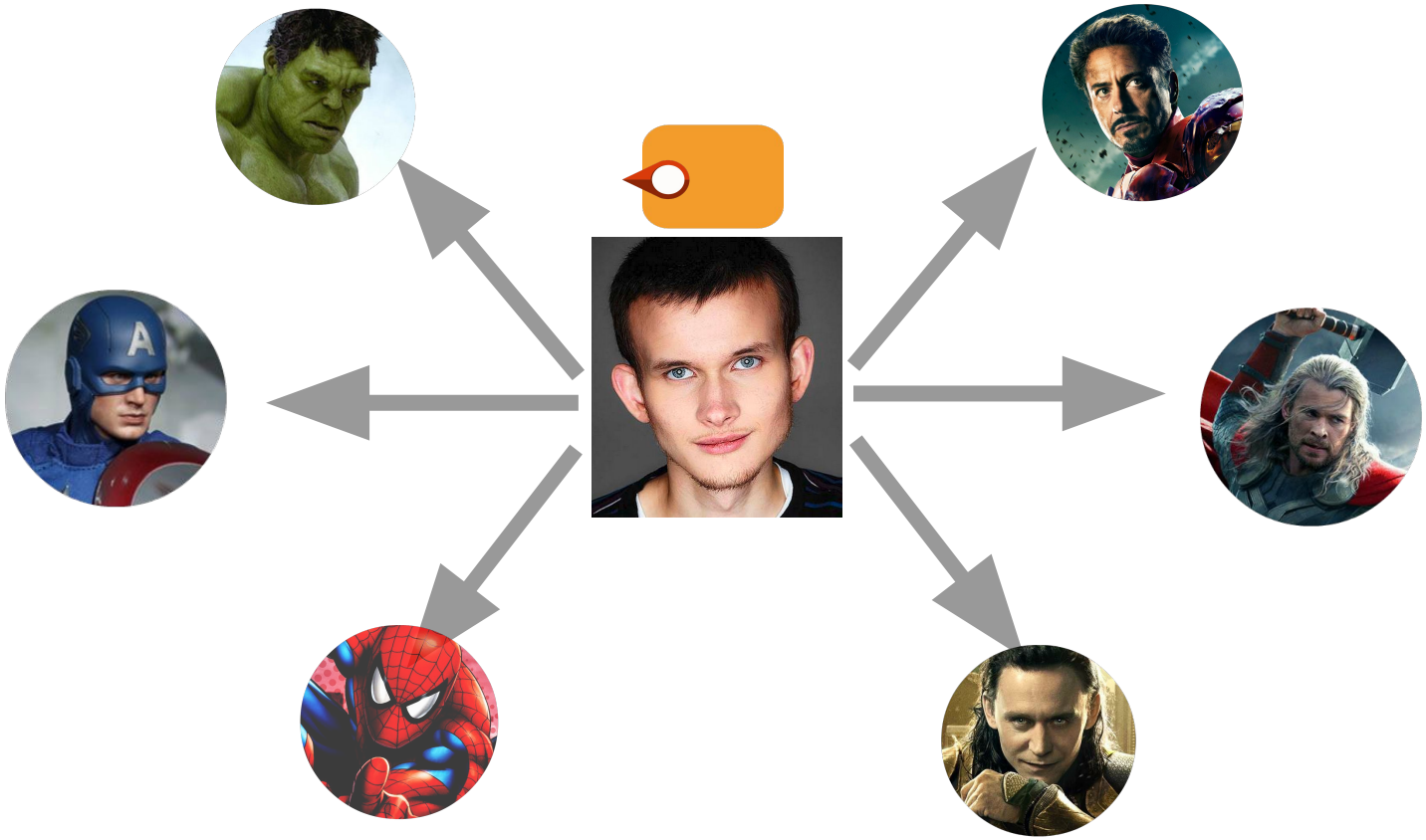
Streamlet: a streamlined blockchain

Block Format

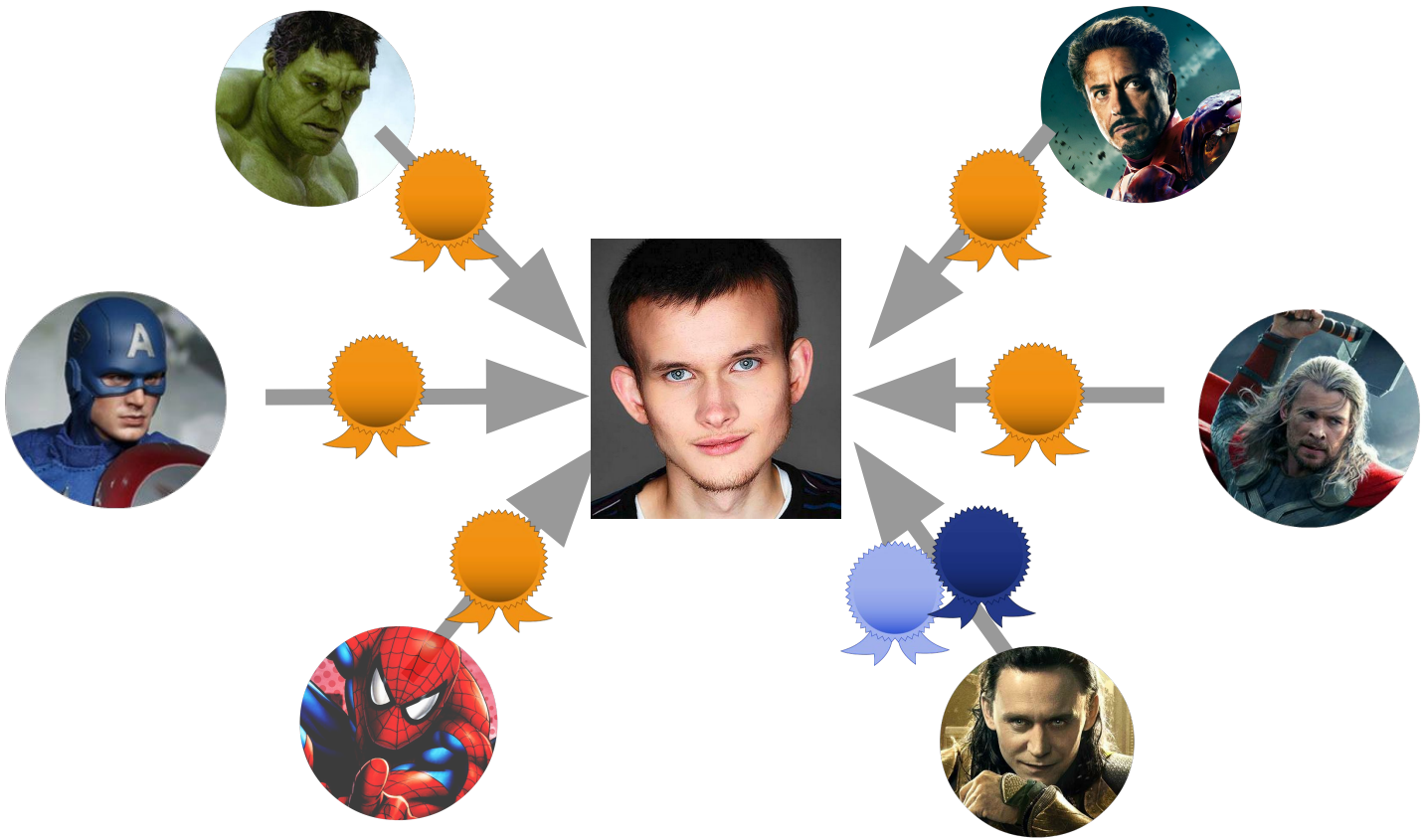




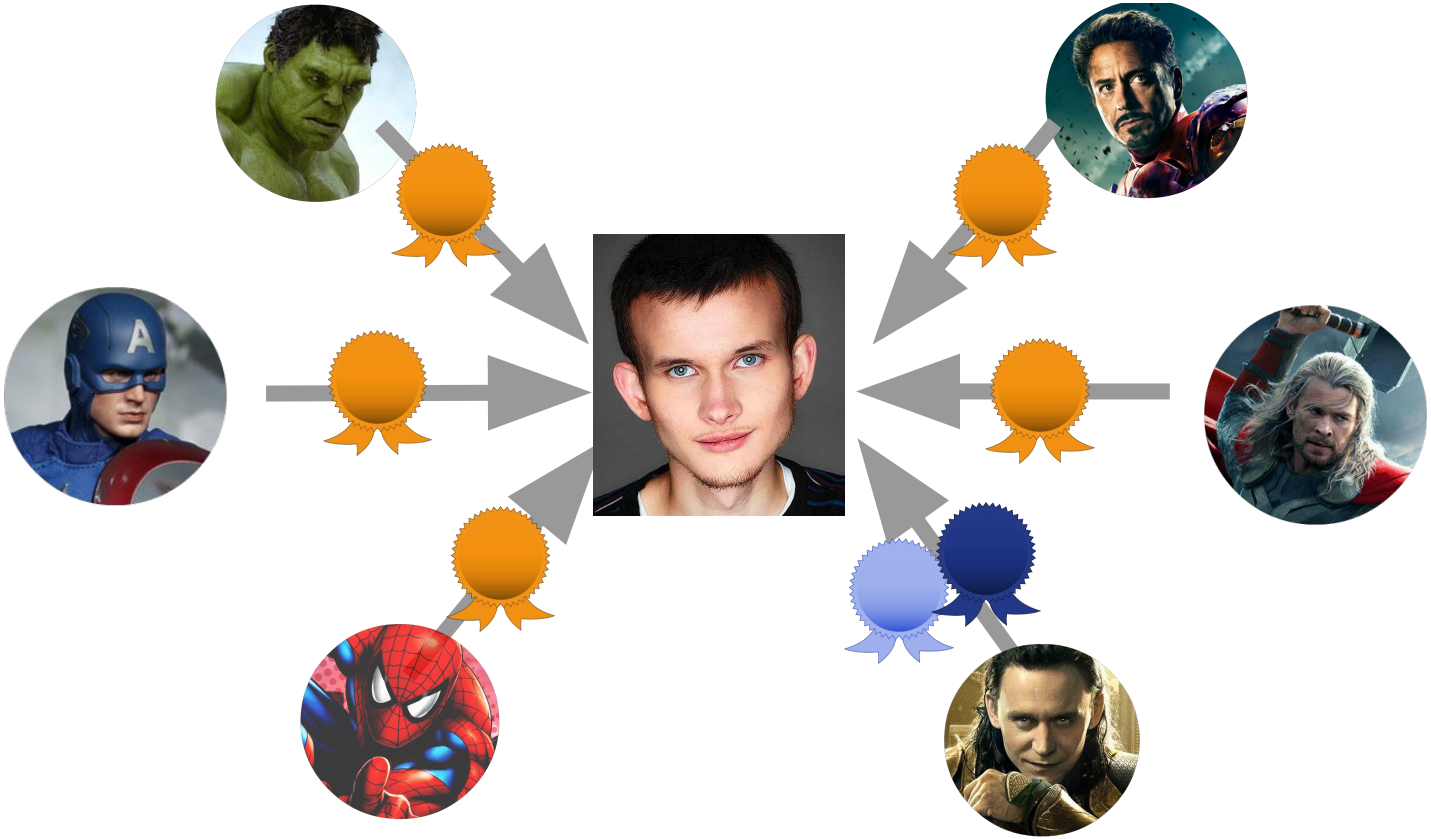
1 Proposer proposes block



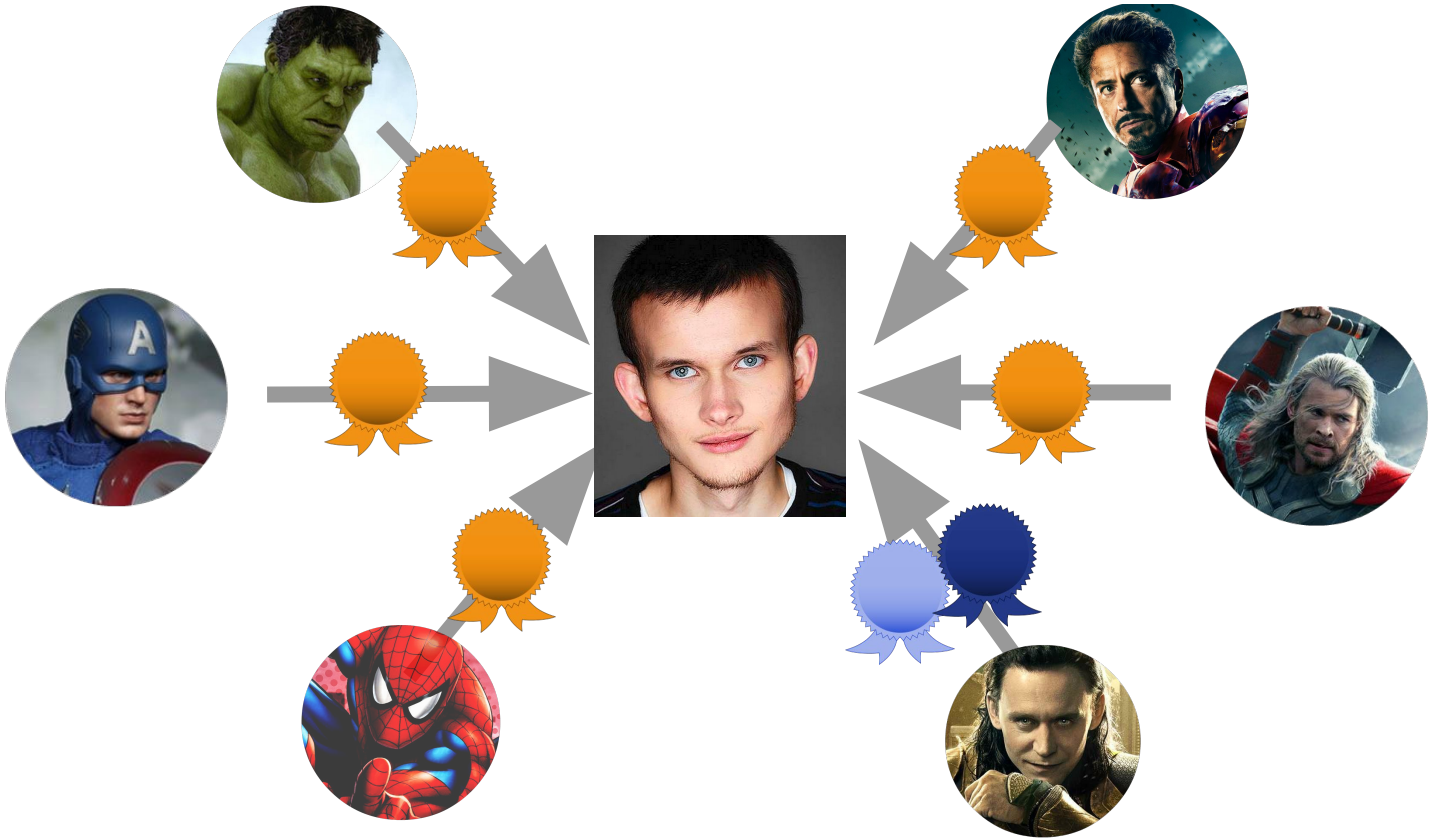
2 Vote



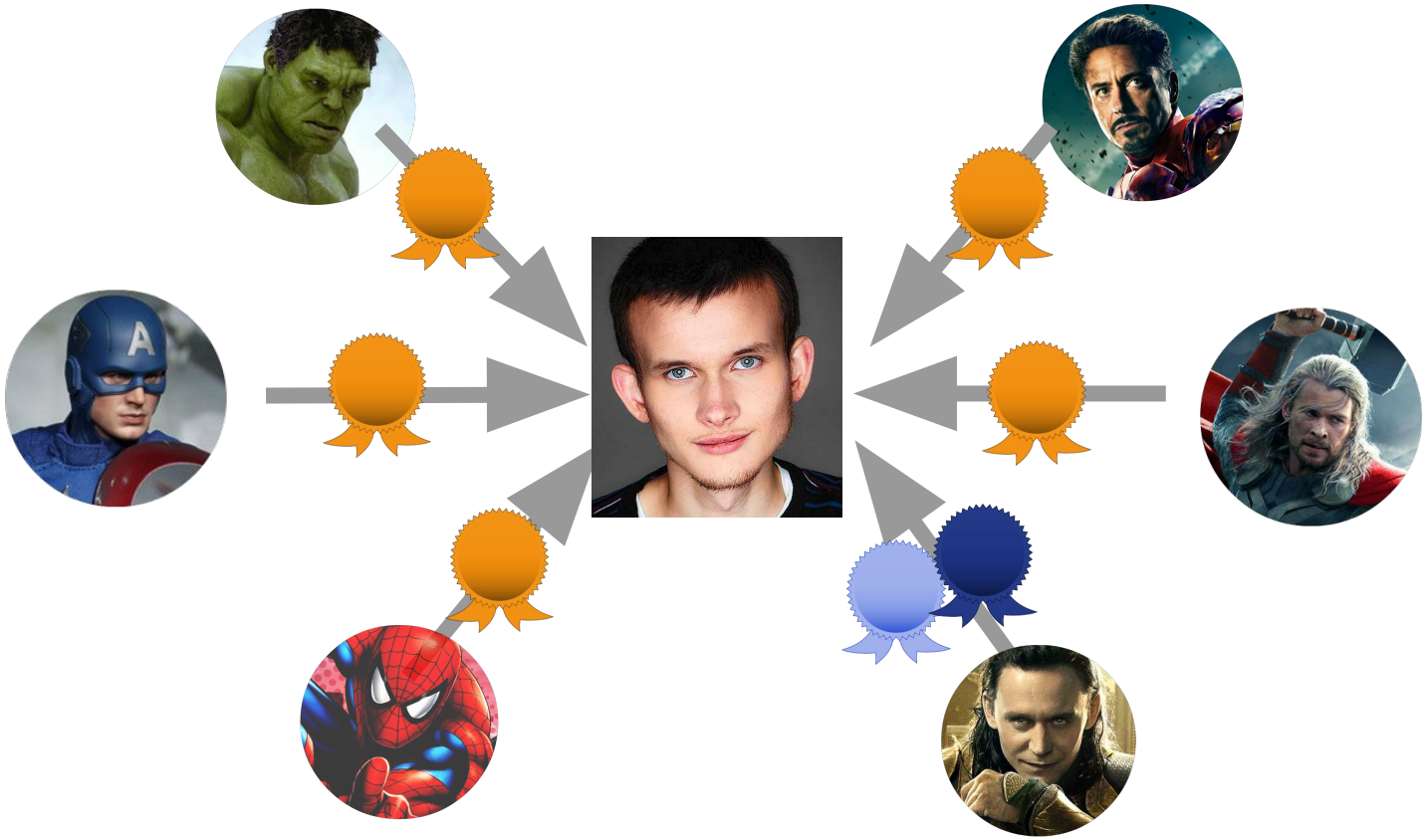
3 Confirm upon ⅔ n votes



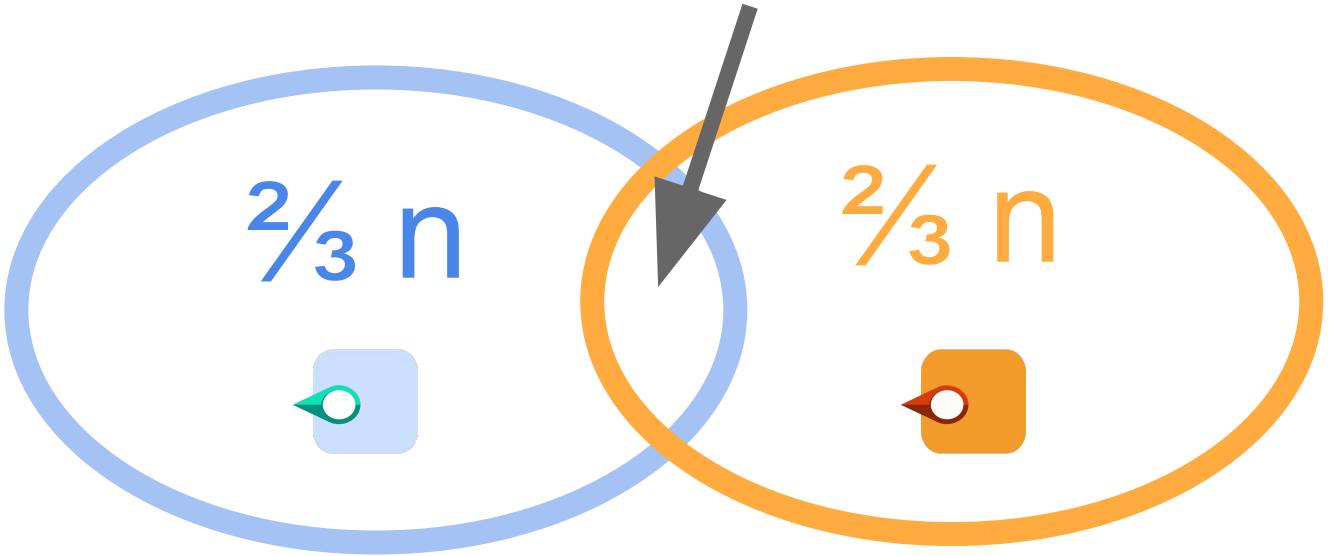
⅔ n votes: notarization



Honest nodes vote **uniquely** each height

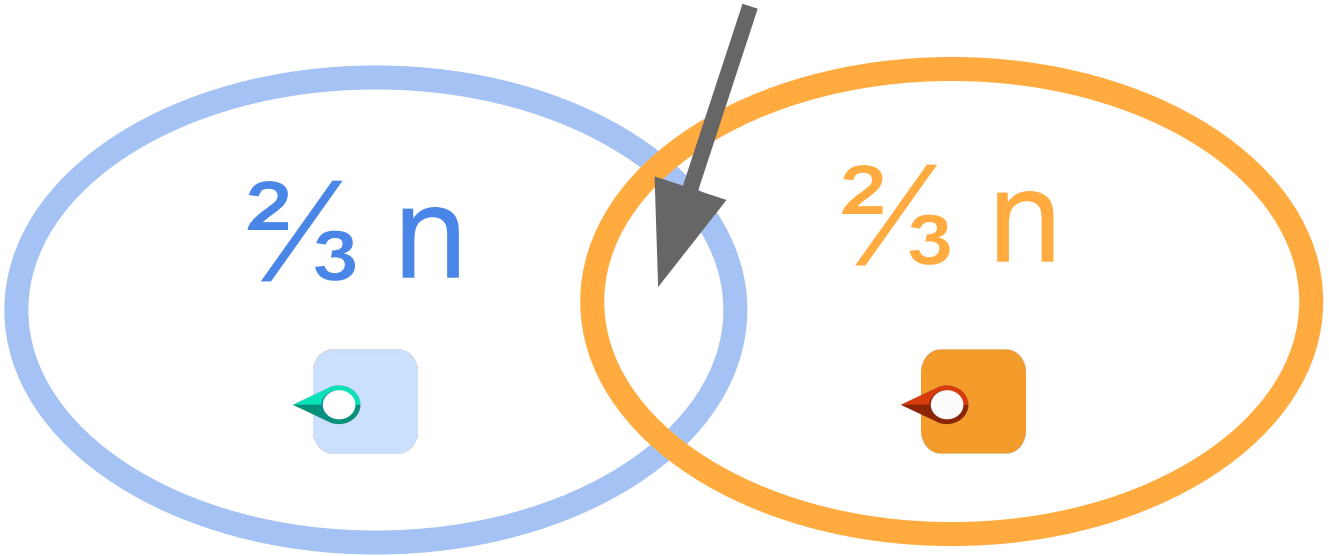


Must intersect at an honest node

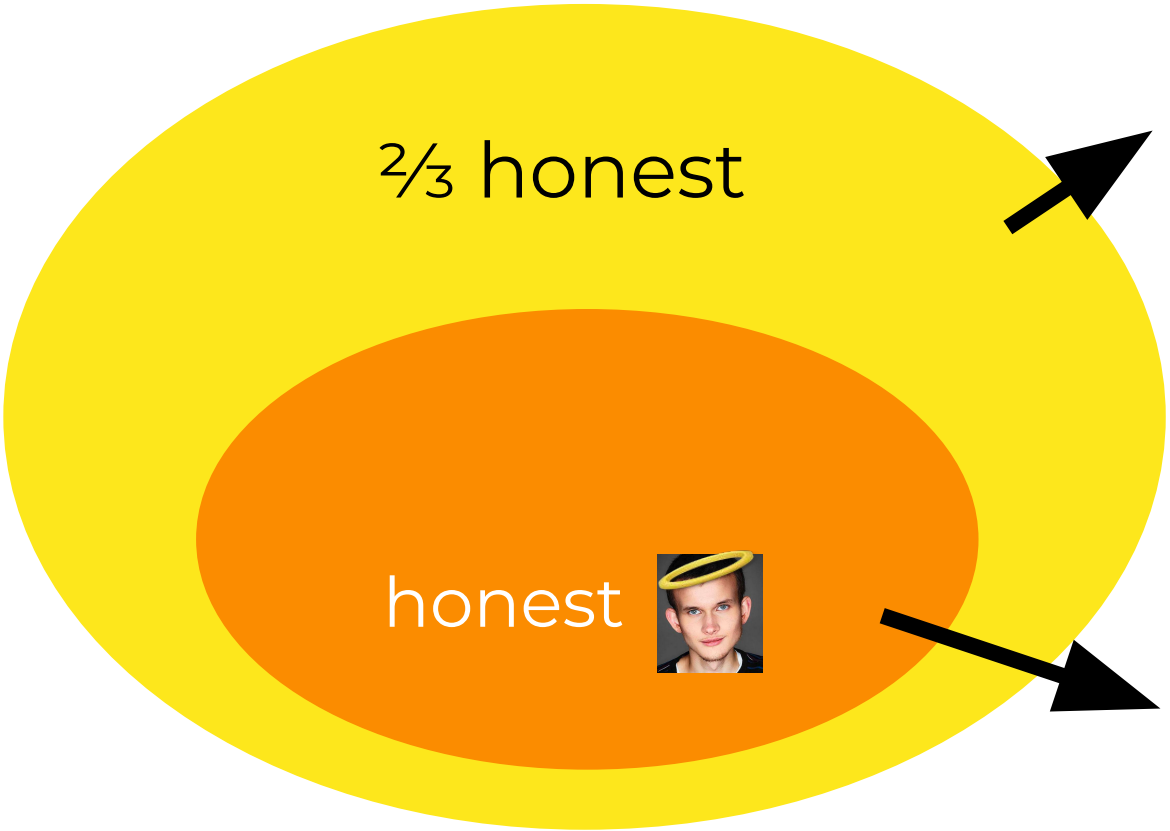


Assume: < ⅓ n corrupt

Must intersect at an honest node

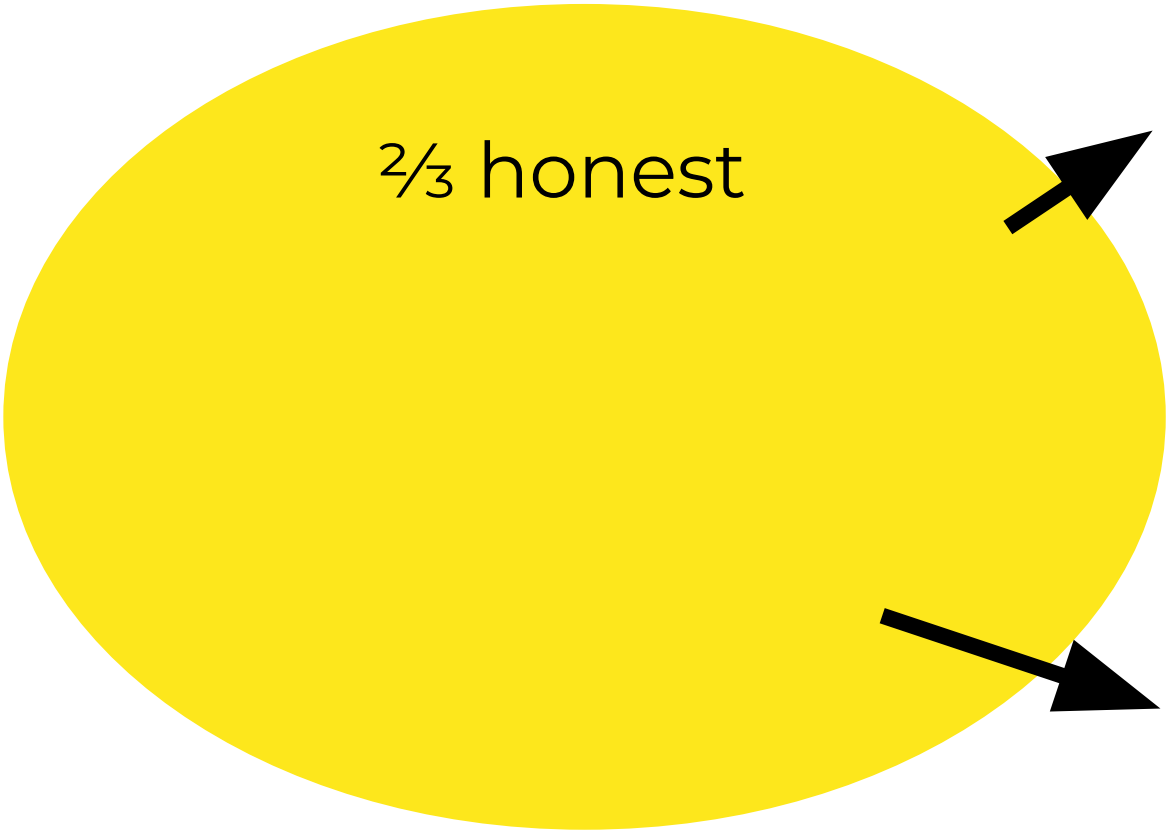


Thus  **=** 



Consistency

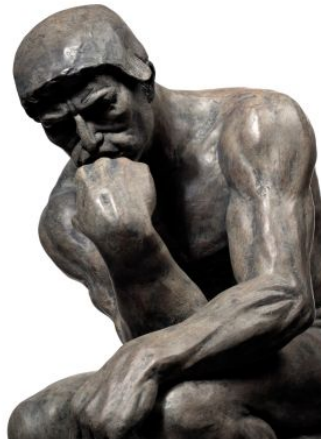
Liveness



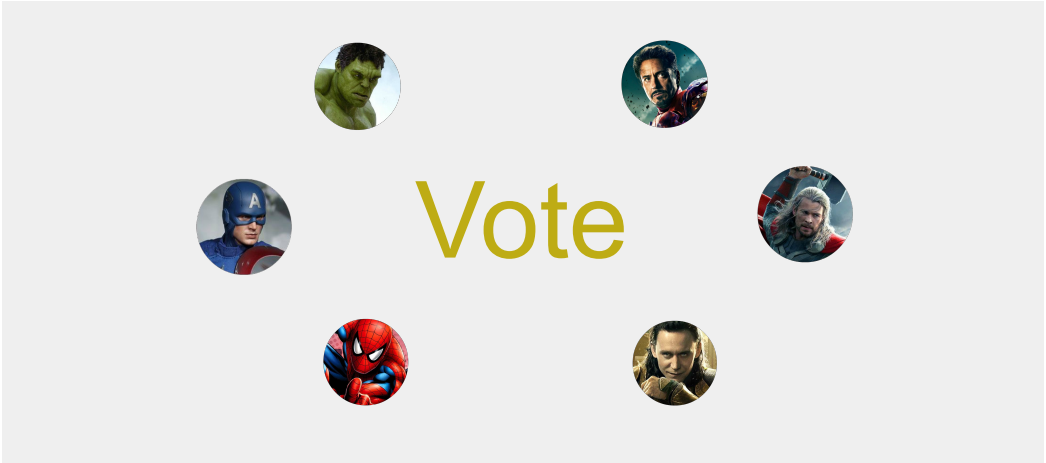
Consistency

Liveness

How do we achieve liveness?



Anatomy of classical consensus



Simple normal path

Complicated recovery path

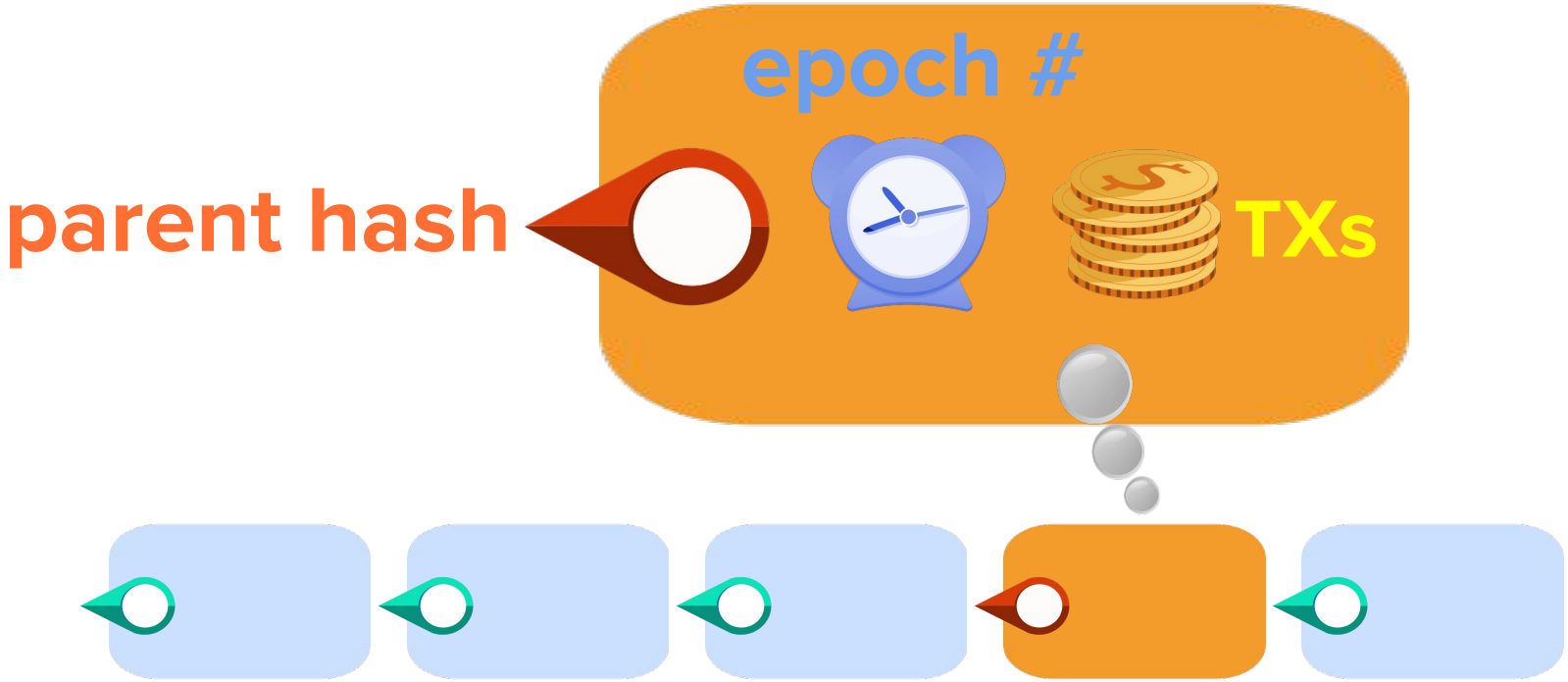
Can we achieve full consensus
(almost) as easily as the normal path?

Roadmap

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

Streamlined blockchains
(Casper, Dfinity, Hotstuff, Pili, Pala, Streamlet)

Assume: epoch = 1 sec ≥ 1 roundtrip



Proposer rotation

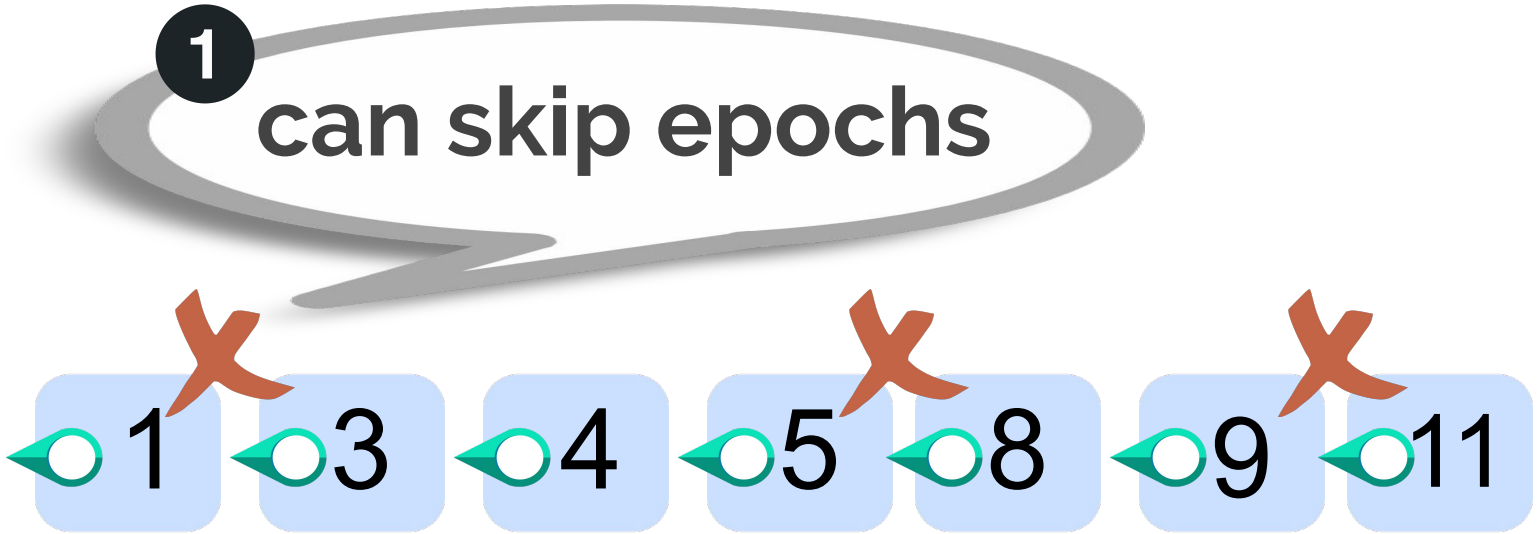
Node H(i) mod n is the proposer in epoch i

Easy to support any other proposer-rotation policy

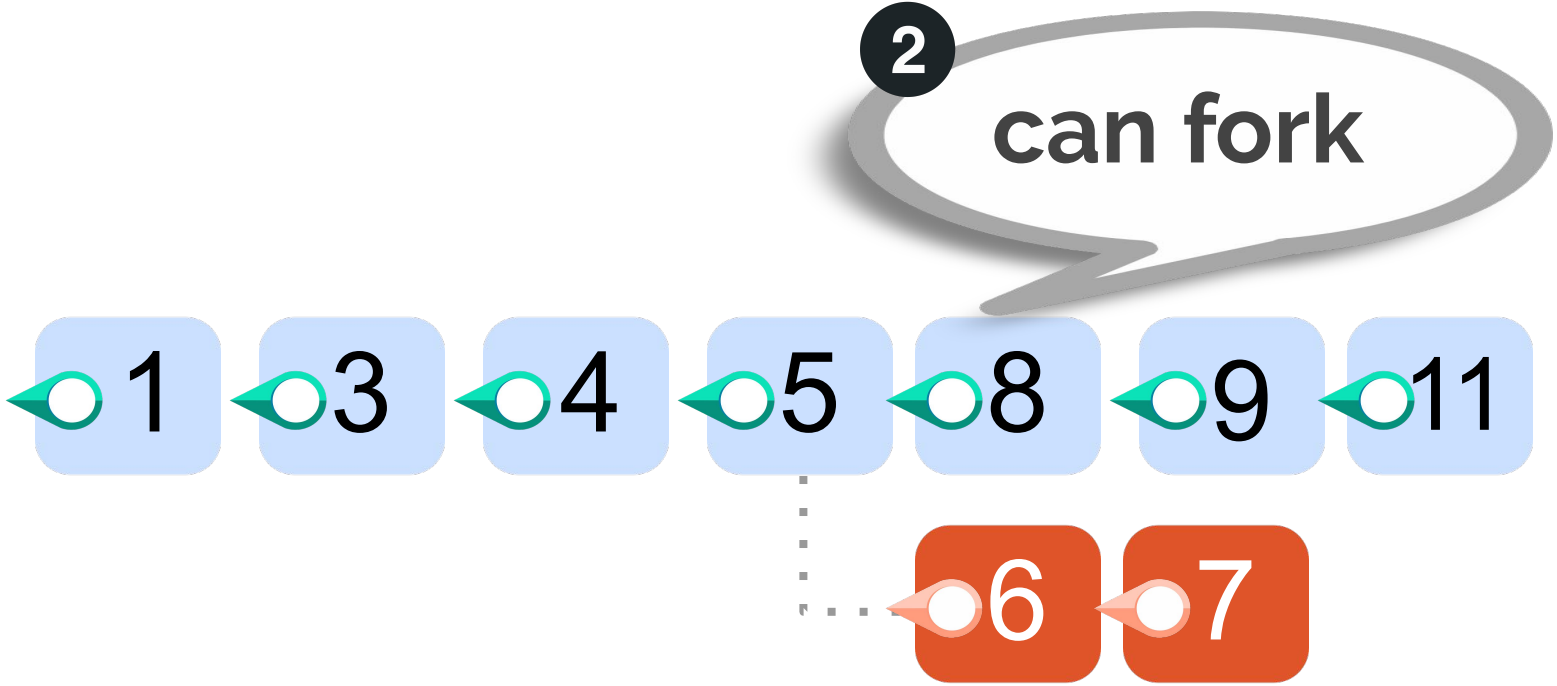
If everyone were honest

1 2 3 4 5

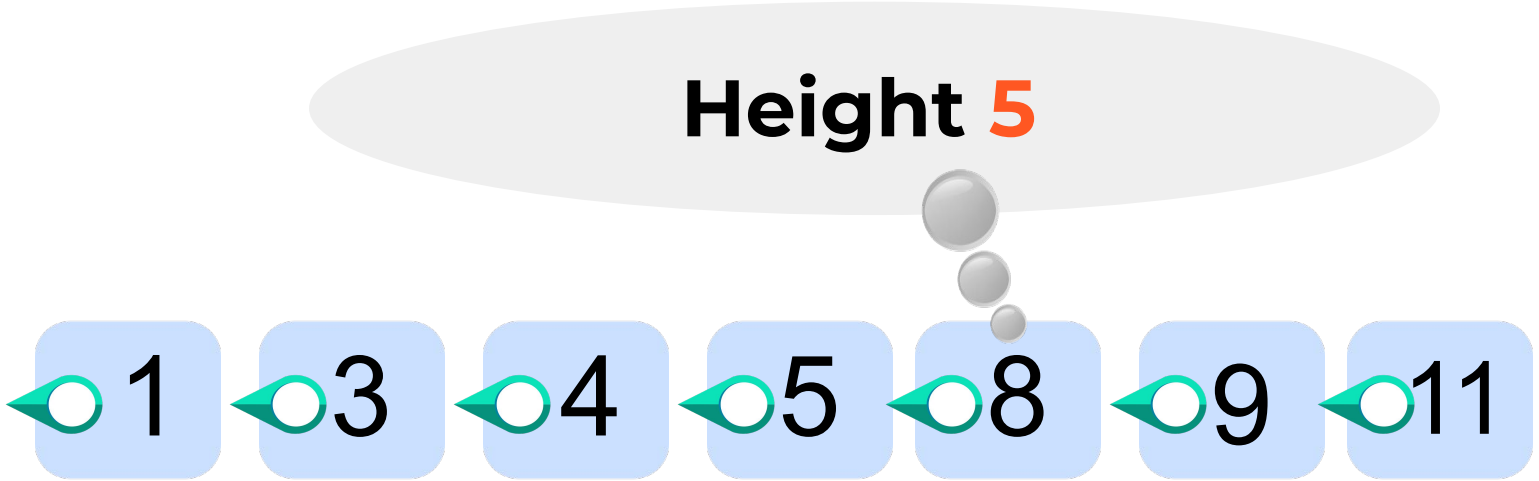
Real world



Real world



Height = “position in chain”



Propose

- extend longest notarized chain

Vote

- no double-vote each epoch
- verify parent block notarized
- no conflicting notr at the height

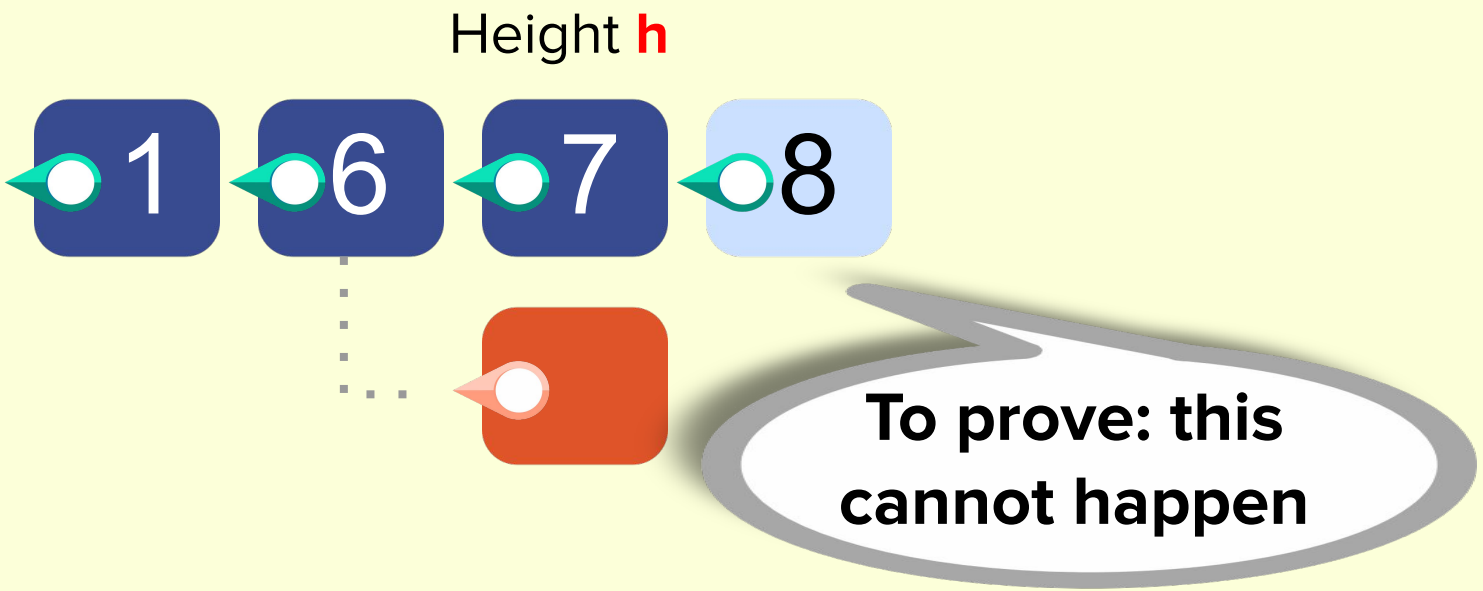
} Every epoch

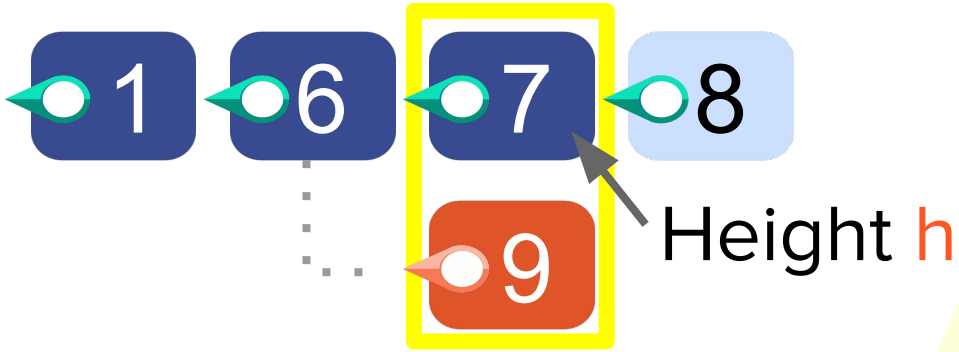
- **Finalization**: height h final if heights h-1, h, h+1 have consecutive epochs & are notarized

1. Consistency Proof

2. Liveness Proof

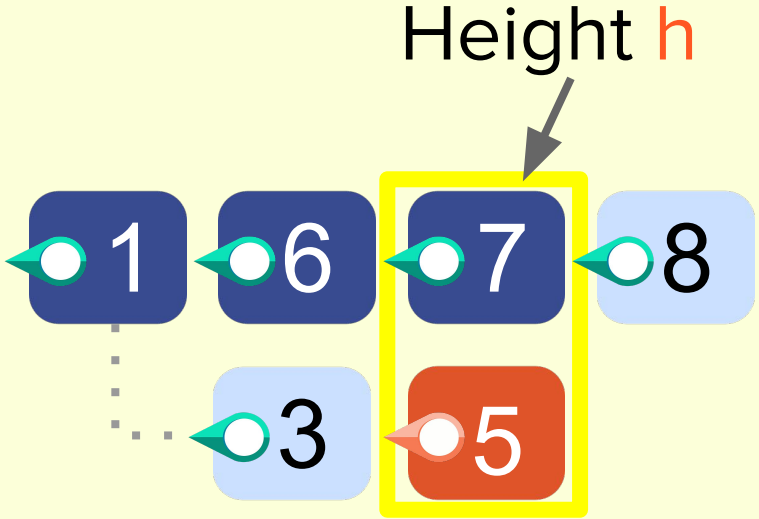
Finalization: height h final if heights h-1, h, h+1 have consecutive epochs & are notarized



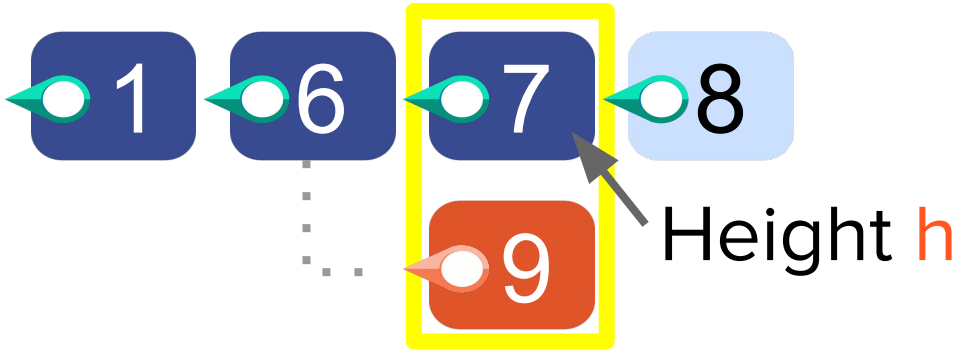


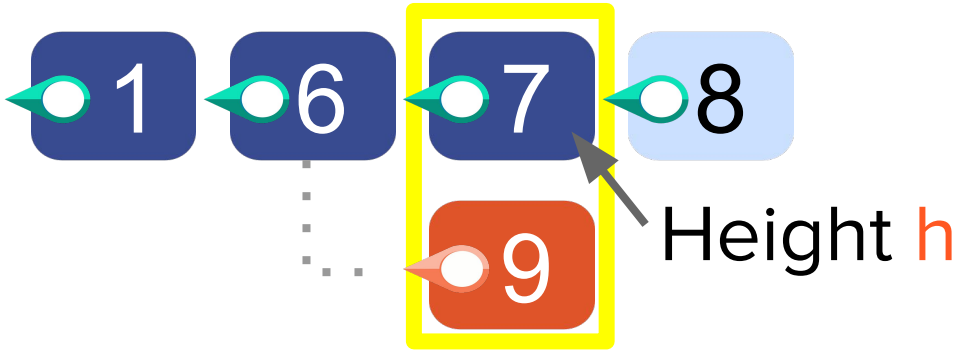
Case 1

Case 2



Lemma: every epoch has at most 1 notarized block.

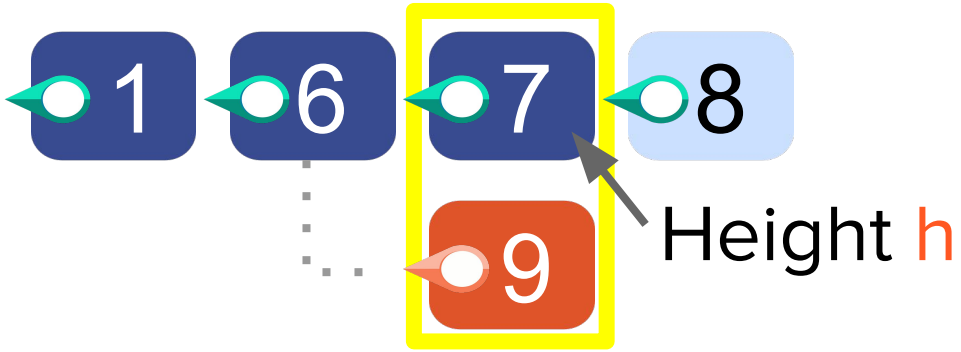

1
6
7
8
9
Height h



“many” = at least n/3 honest

Proof:

many voted for 8 in epoch 8

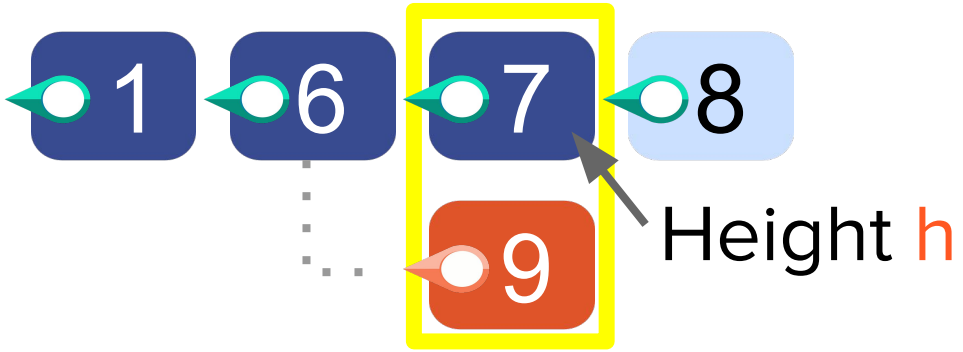


"many" = at least n/3 honest

Proof:

many voted for 8 in epoch 8

--> many saw 7 notarized in epoch 8



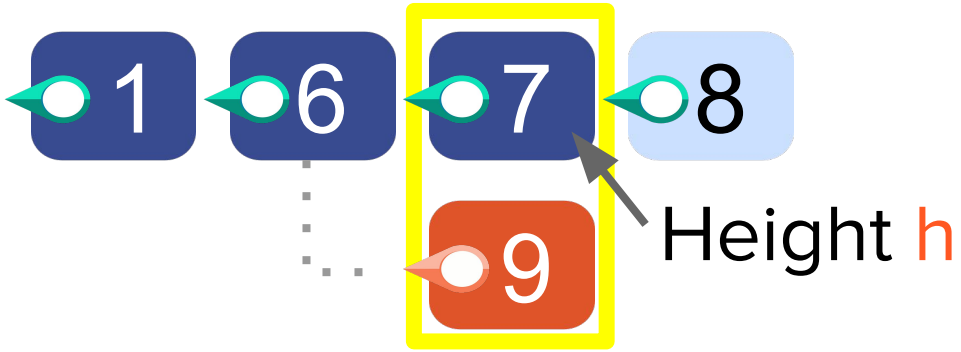
"many" = at least n/3 honest

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” = at least n/3 honest

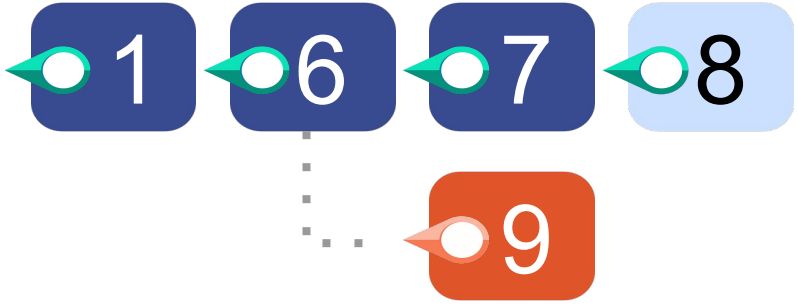
Proof:

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



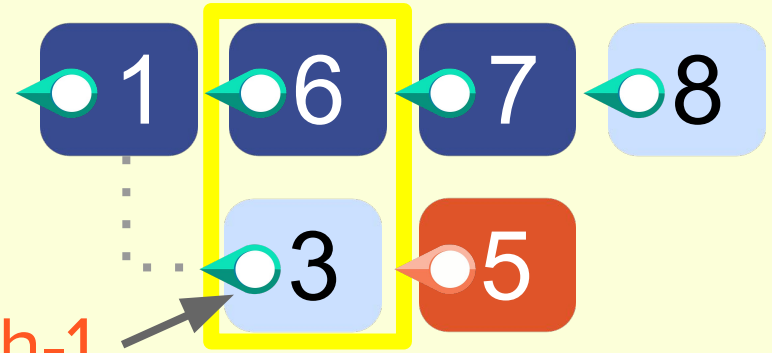
Case 1

Case 2

“many” = at least n/3 honest

Proof:

many voted for 5 in epoch 5

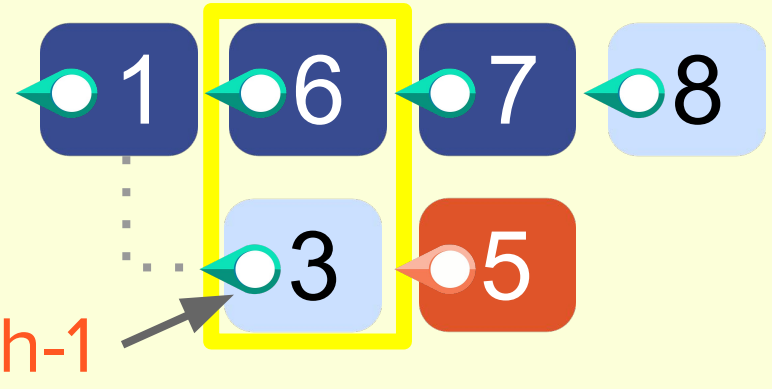


“many” = at least n/3 honest

Proof:

many voted for 5 in epoch 5

--> many saw 3 notarized in epoch 5



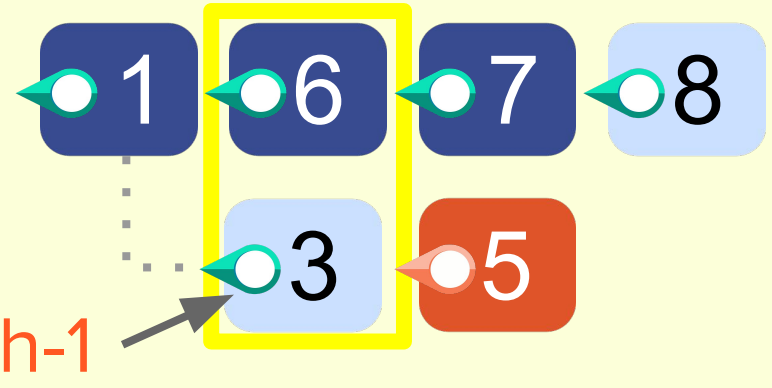
“many” = at least n/3 honest

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” = at least n/3 honest

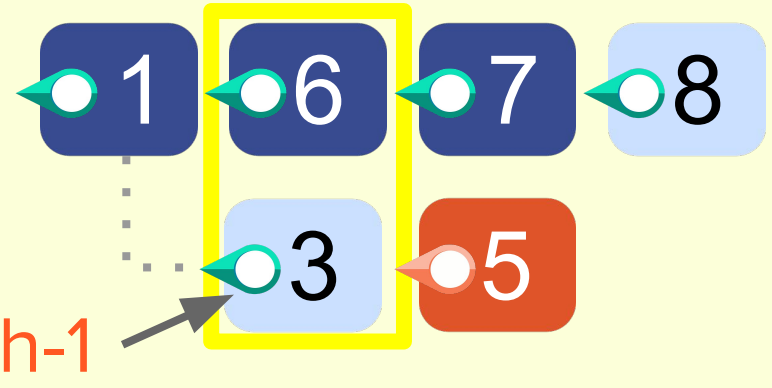
Proof:

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” = at least n/3 honest

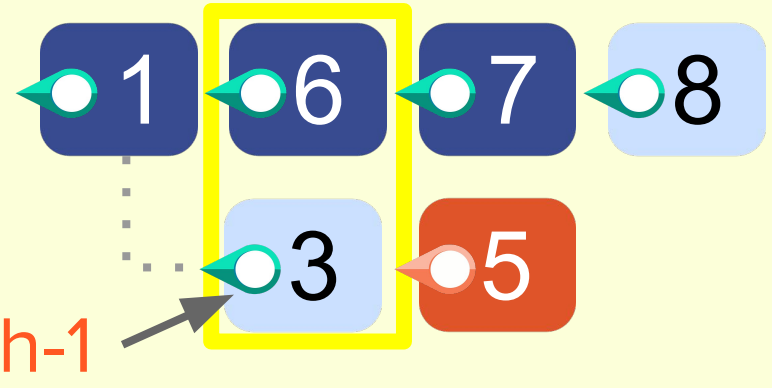
Proof:

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” = at least 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!

Liveness Theorem

During a period of synchrony, honest nodes' finalized chains grow whenever 5 consecutive epochs have honest proposers.

(and moreover the finalized chains grow by honest blocks)

Partial Synchrony [DLS]

- Protocol knows a delay estimate Δ
- Consistency is guaranteed even if actual delay arbitrarily long
- Liveness only during periods of synchrony

Partial Synchrony

[DLS]

Theorem:

Cannot tolerate ⅓ or more corruptions

Summary: streamlined blockchains

- Every epoch allows proposer-switch.
- View change embedded in a unified “propose-vote” paradigm.

Roadmap

½ synchronous

⅓ partially synchronous

Every epoch:

- Proposer proposes a block extending longest notarized chain
- Vote on the first proposal if parent notarized and no other notarized block at same height
- A block with majority votes is notarized

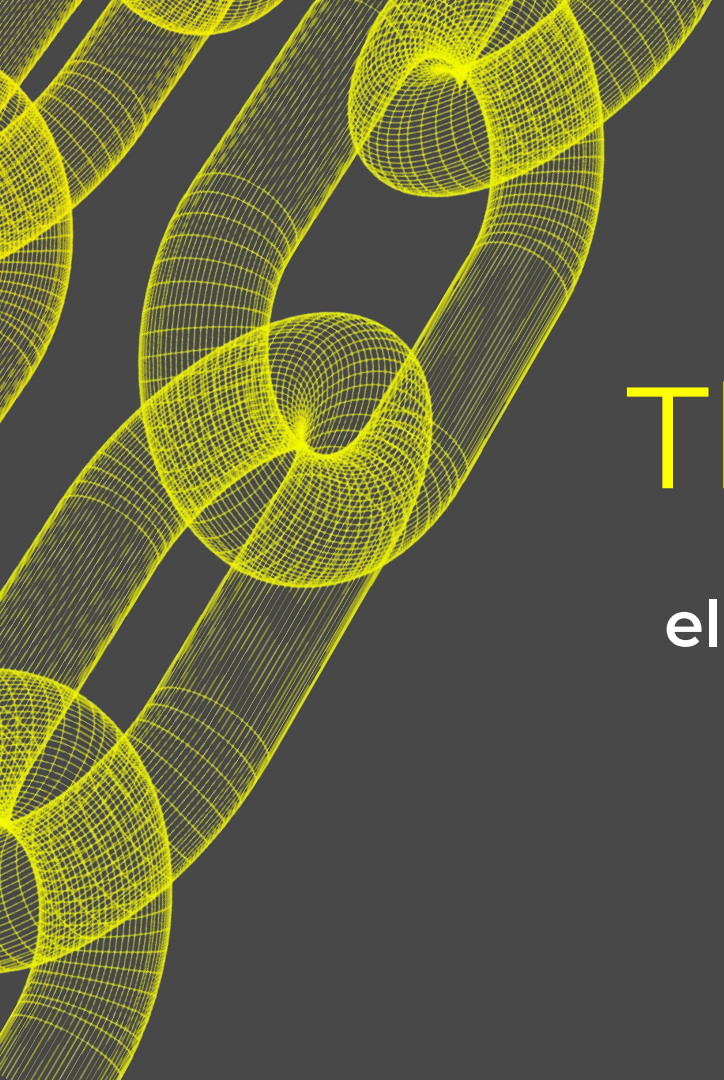
Finalization:

- 6 consecutive at the end, no conflicting notarization, chop off 5

Optimistic Responsiveness

Best-possible partition tolerance

https://eprint.iacr.org/2018/981
https://eprint.iacr.org/2018/980
https://eprint.iacr.org/2019/179



Thank You!

elaine@cs.cornell.edu