Blockchains & Cryptocurrencies

Scaling

www.securitities.io

Instructor: Abhishek Jain
Johns Hopkins University - Spring 2021

Recap: The Problem

- Bitcoin transaction rate: 5-7 tx/sec
    - Bounded by block size, TX size
    - All transactions must be globally verified, stored
- Ethereum: 15 transactions per second if they're small
- Visa: 24,000/sec peak (150M/day globally)
- WeChat 256,000/sec peak

Can we do better?

- **Current ideas**:
  - "Off-chain" transactions
  - New consensus algorithms
  - "Sharding"

Agenda

- **Last Time**: Lightning Network
- **Today**: Thunderella Blockchain (fast optimistic consensus with slow fallback)

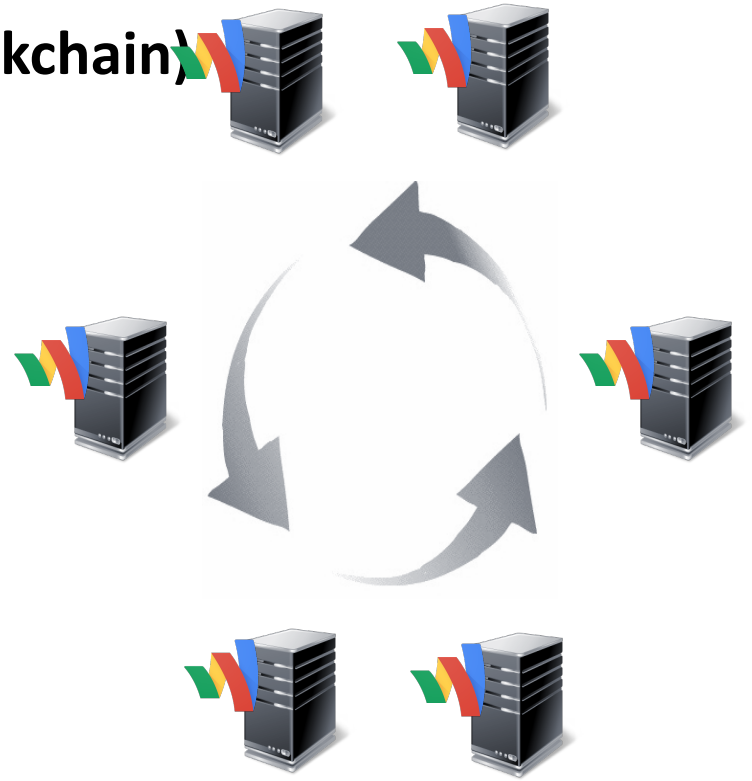
Thunderella

Rafael Pass, Elaine Shi (Thunder Research/Cornell)

Slides credit: Rafael Pass

State-machine replication

(a.k.a. linearly ordered log, consensus, blockchain)

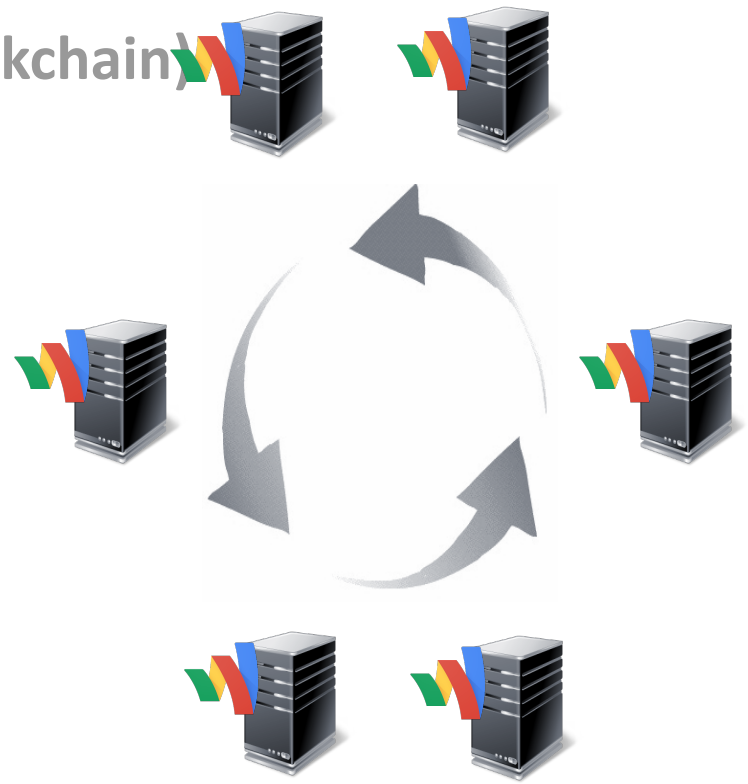


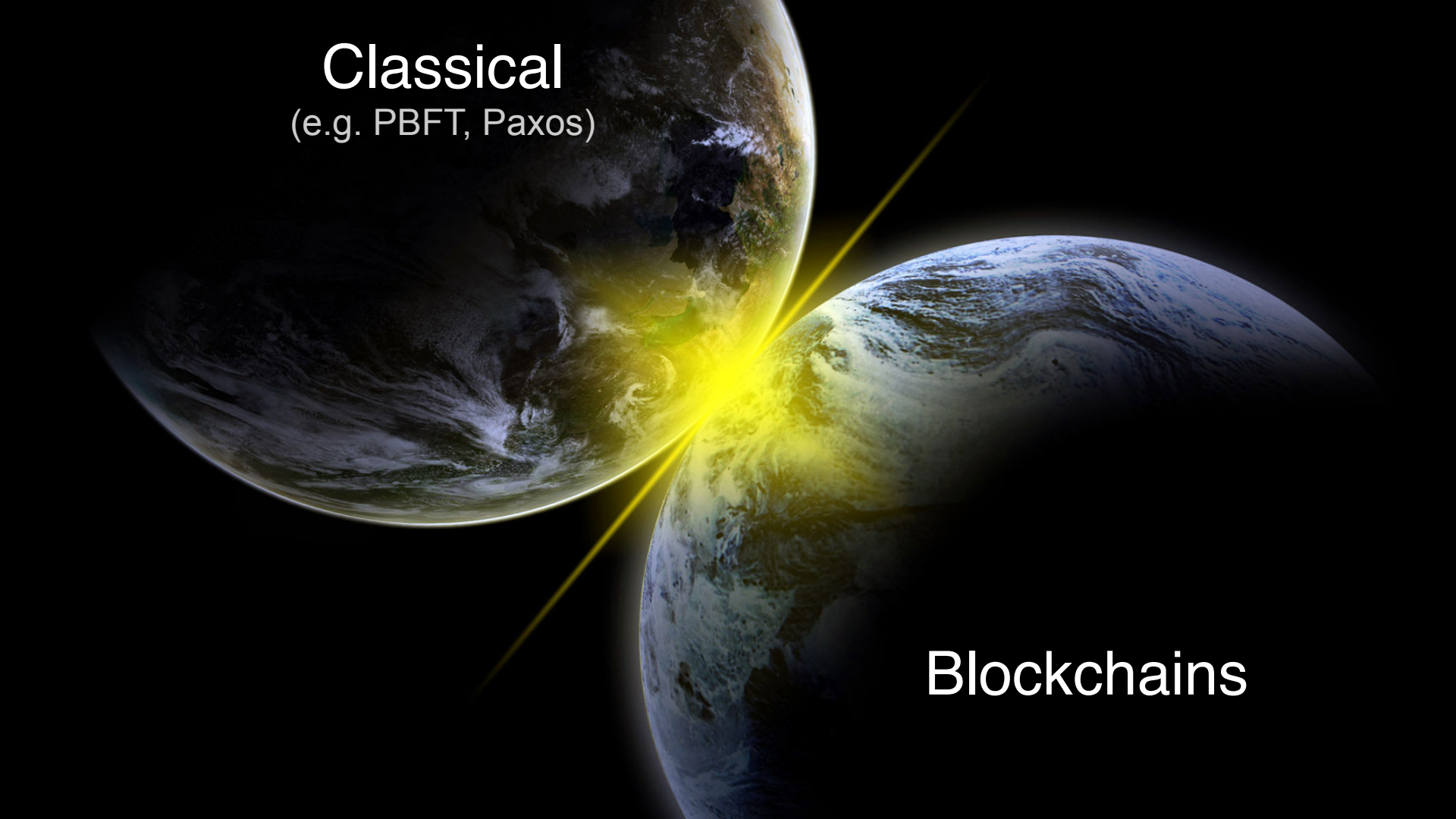
State-machine replication

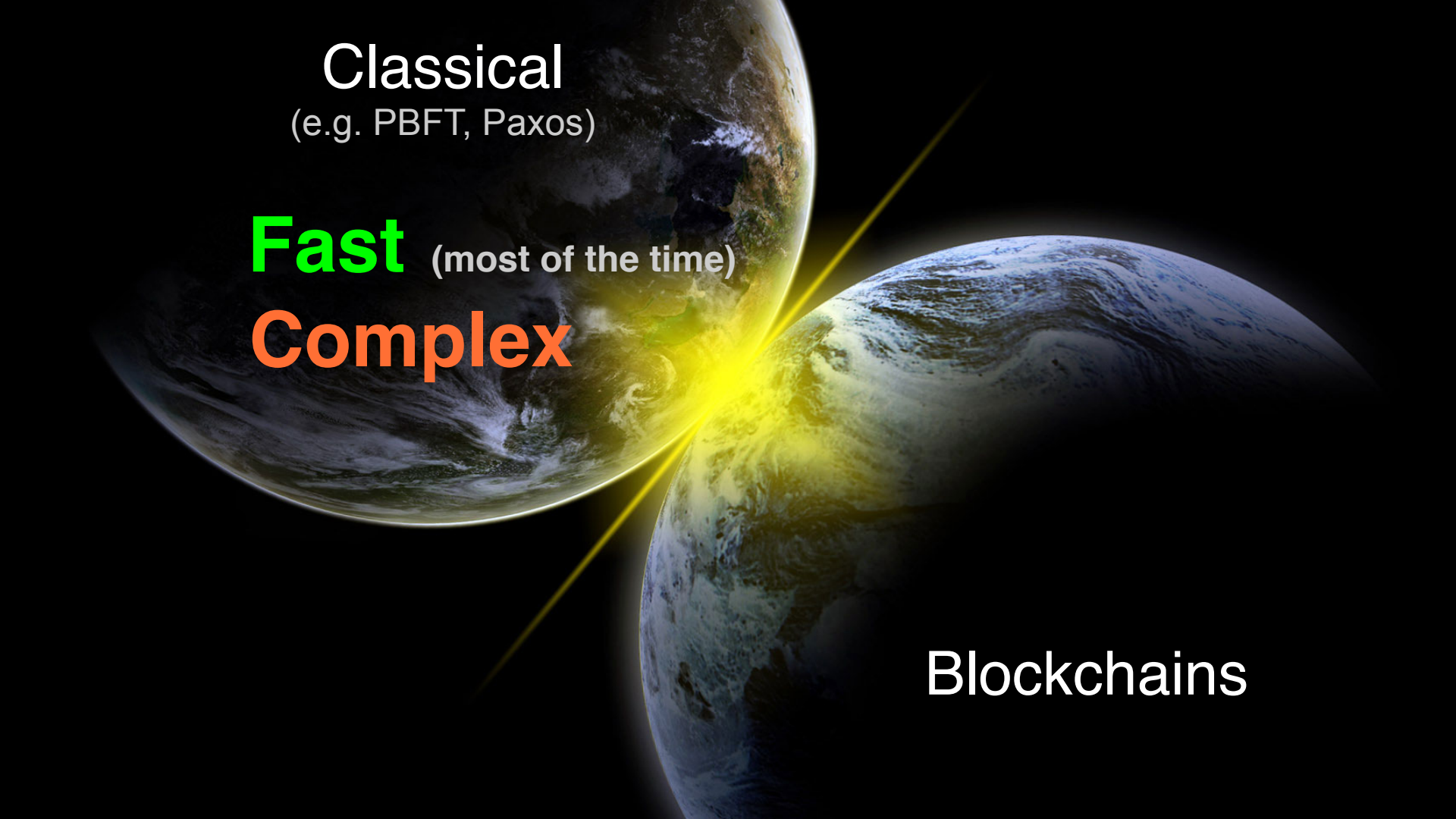
(a.k.a. linearly ordered log, consensus, blockchain)

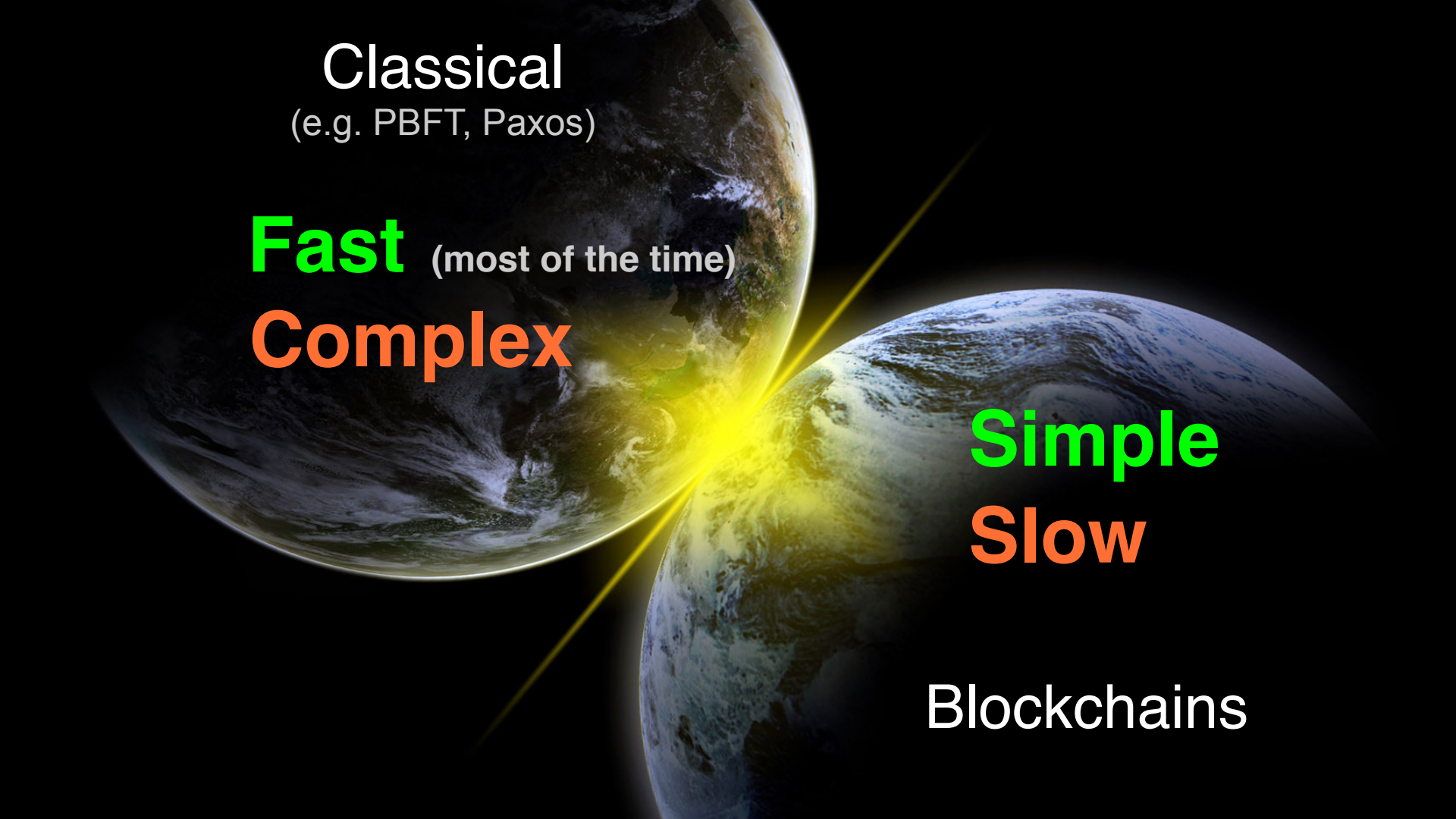
Consistency:
honest nodes agree on log

Liveness:
TXs are incorporated soon



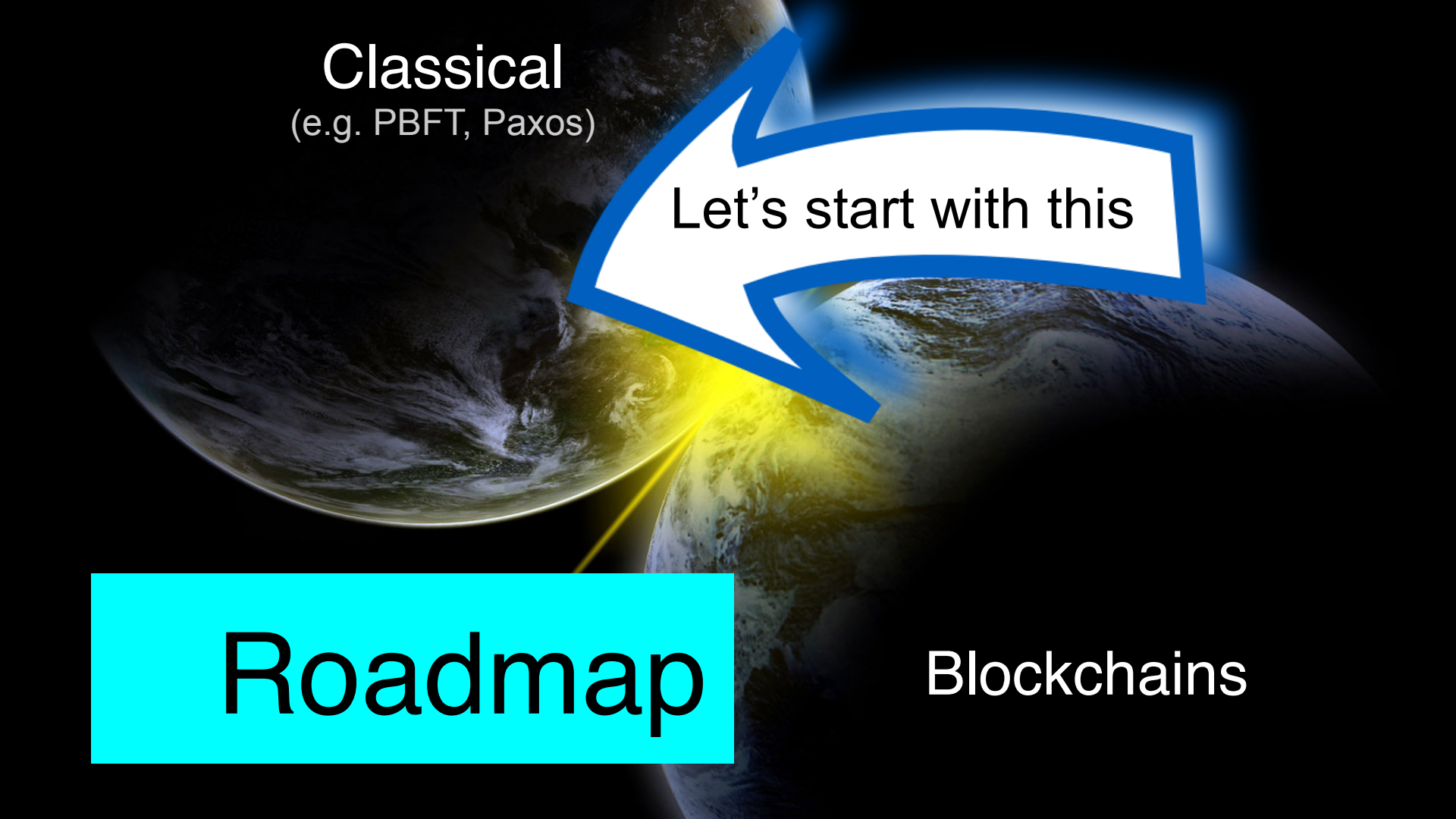

Classical
(e.g. PBFT, Paxos)
Blockchains

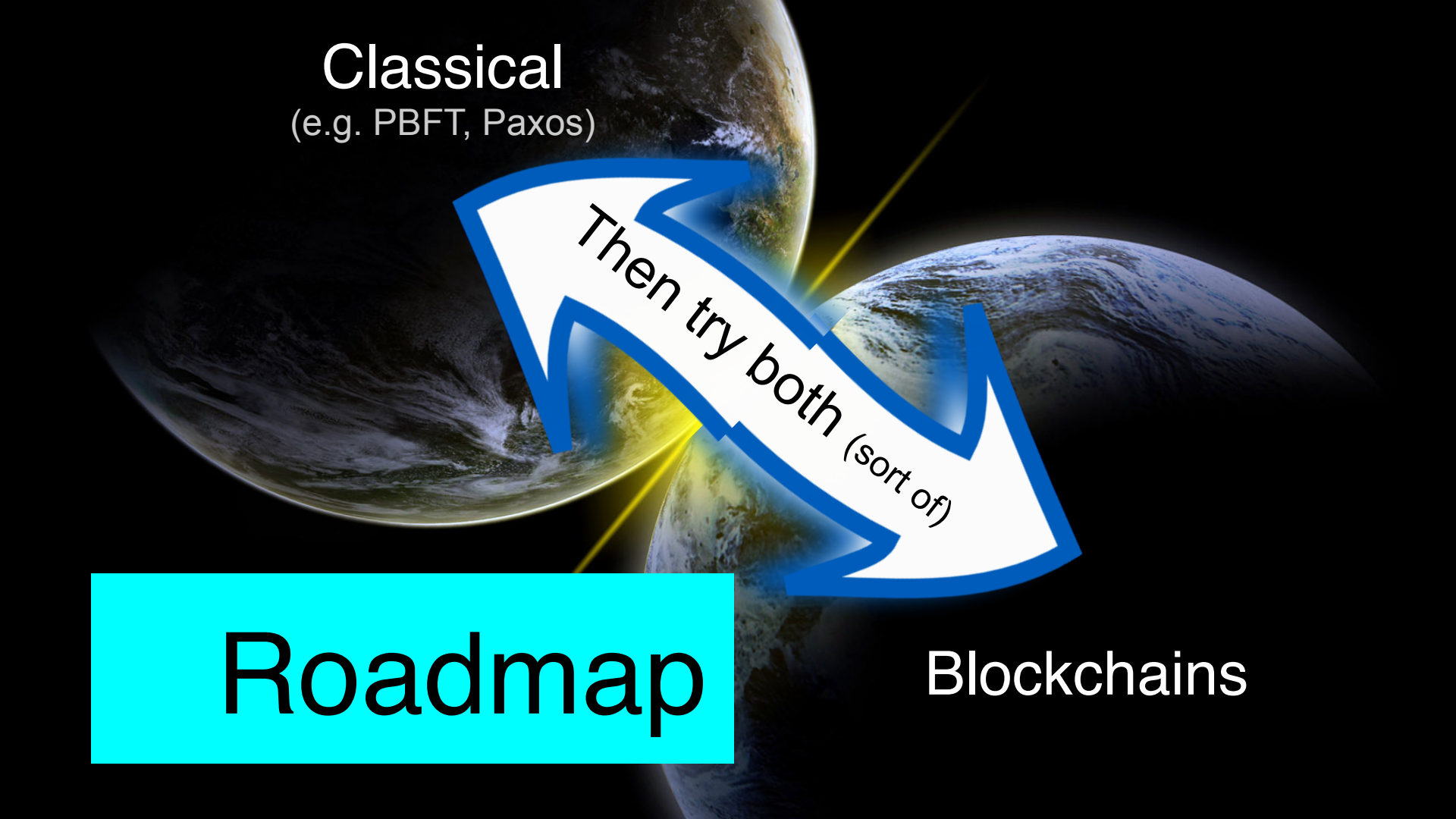

Classical
(e.g. PBFT, Paxos)
Fast (most of the time)
Complex
Blockchains


Classical
(e.g. PBFT, Paxos)
Fast (most of the time)
Complex
Simple
Slow
Blockchains

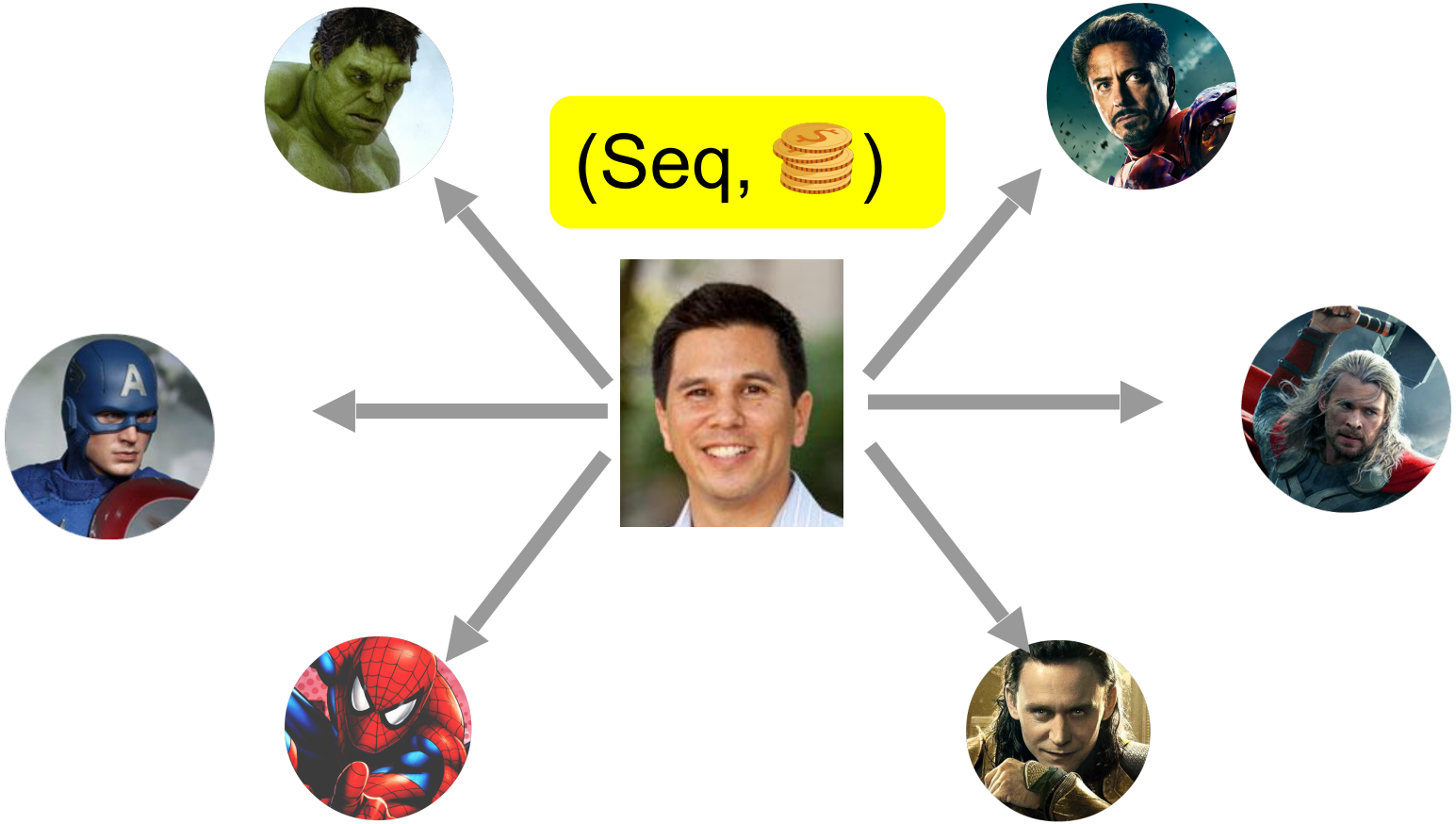
Thunderella [PS'18]

- **As simple as blockchains**
- **"Optimistic case": *Very fast!***
- **If things "go bad", fall back to slow blockchain**

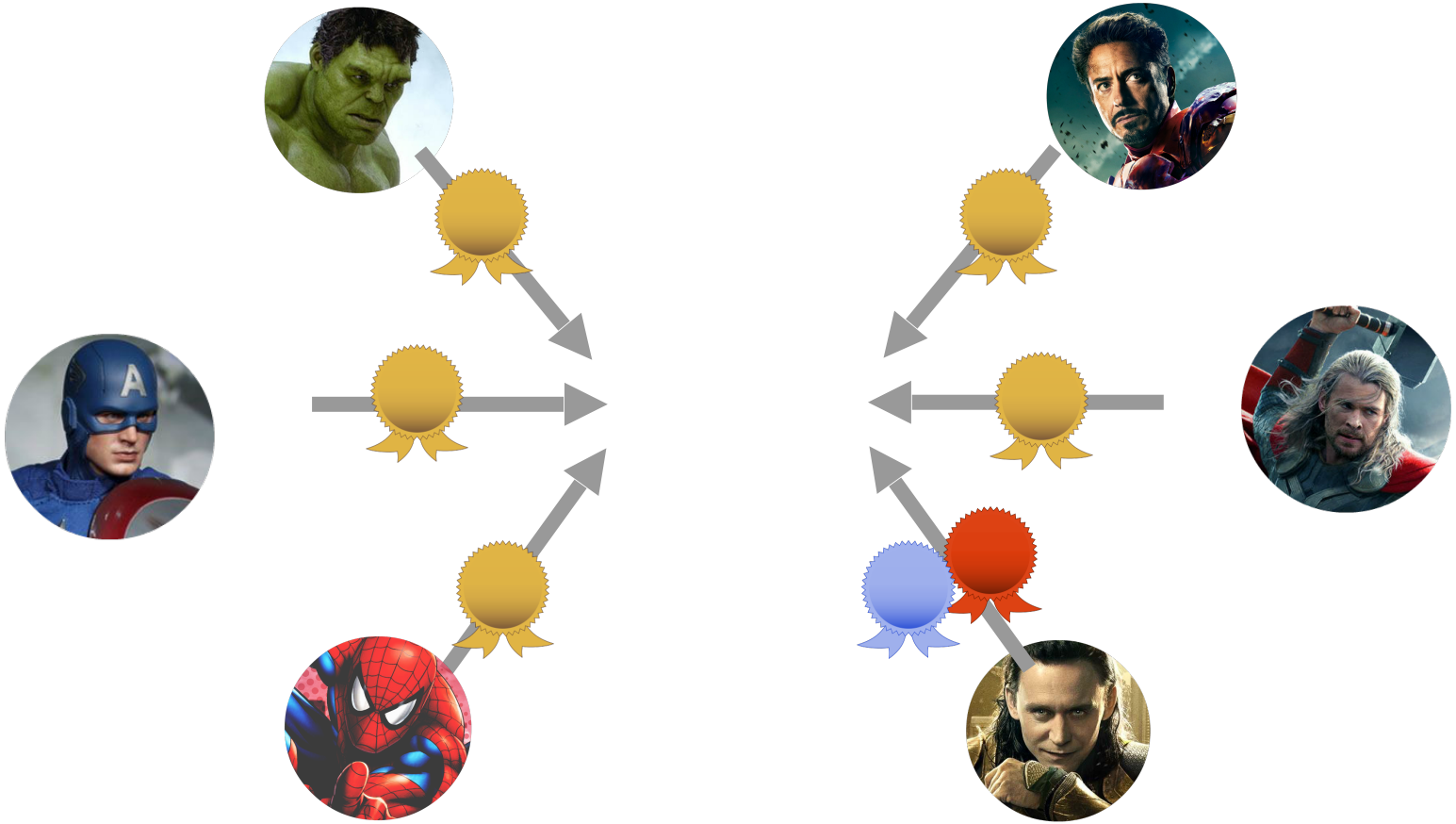

Classical
(e.g. PBFT, Paxos)
Let's start with this
Roadmap
Blockchains


Classical
(e.g. PBFT, Paxos)
Then try both (sort of)
Roadmap
Blockchains

❶ Leader proposes transaction



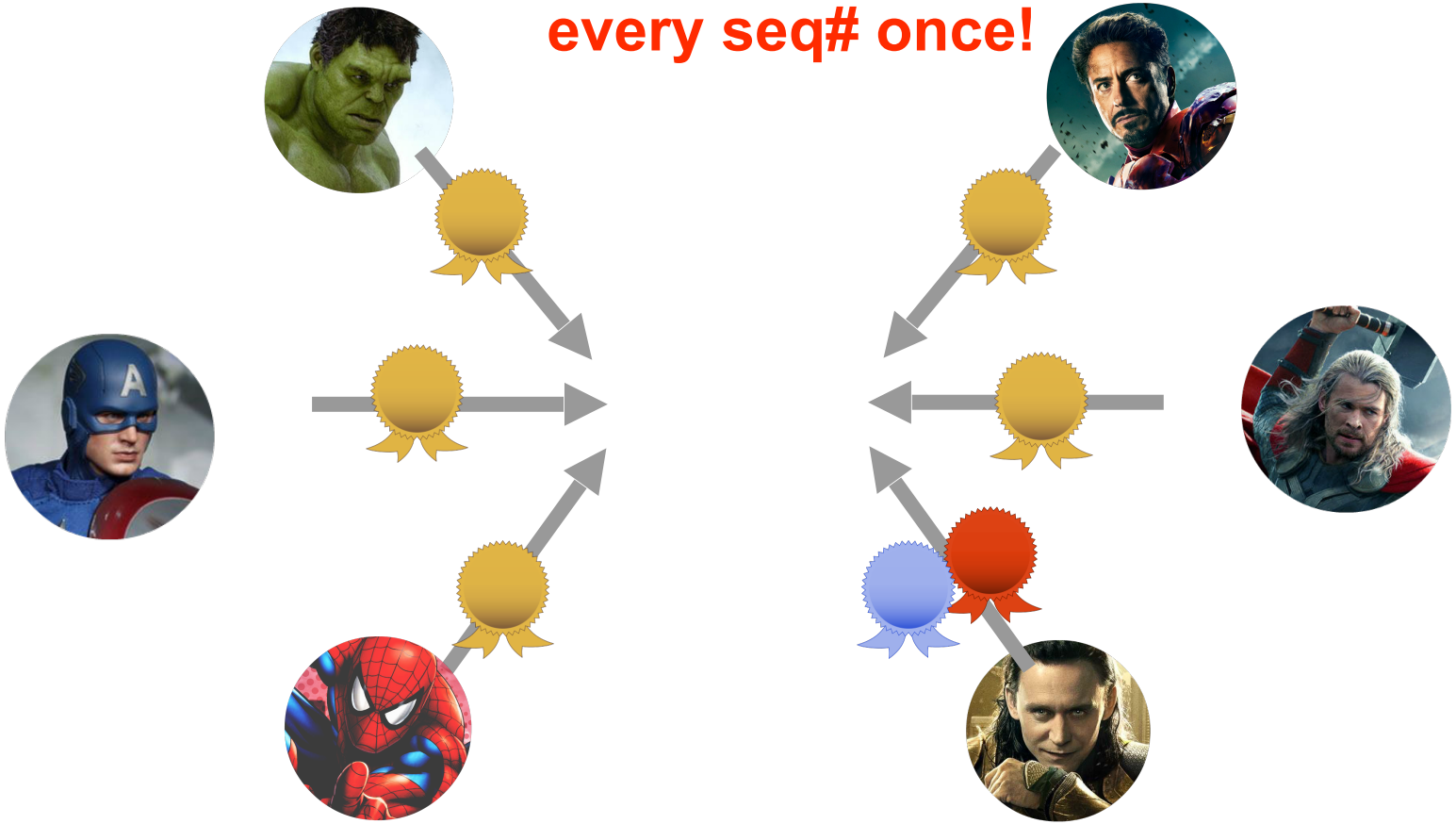
2 Everyone “ack’s”



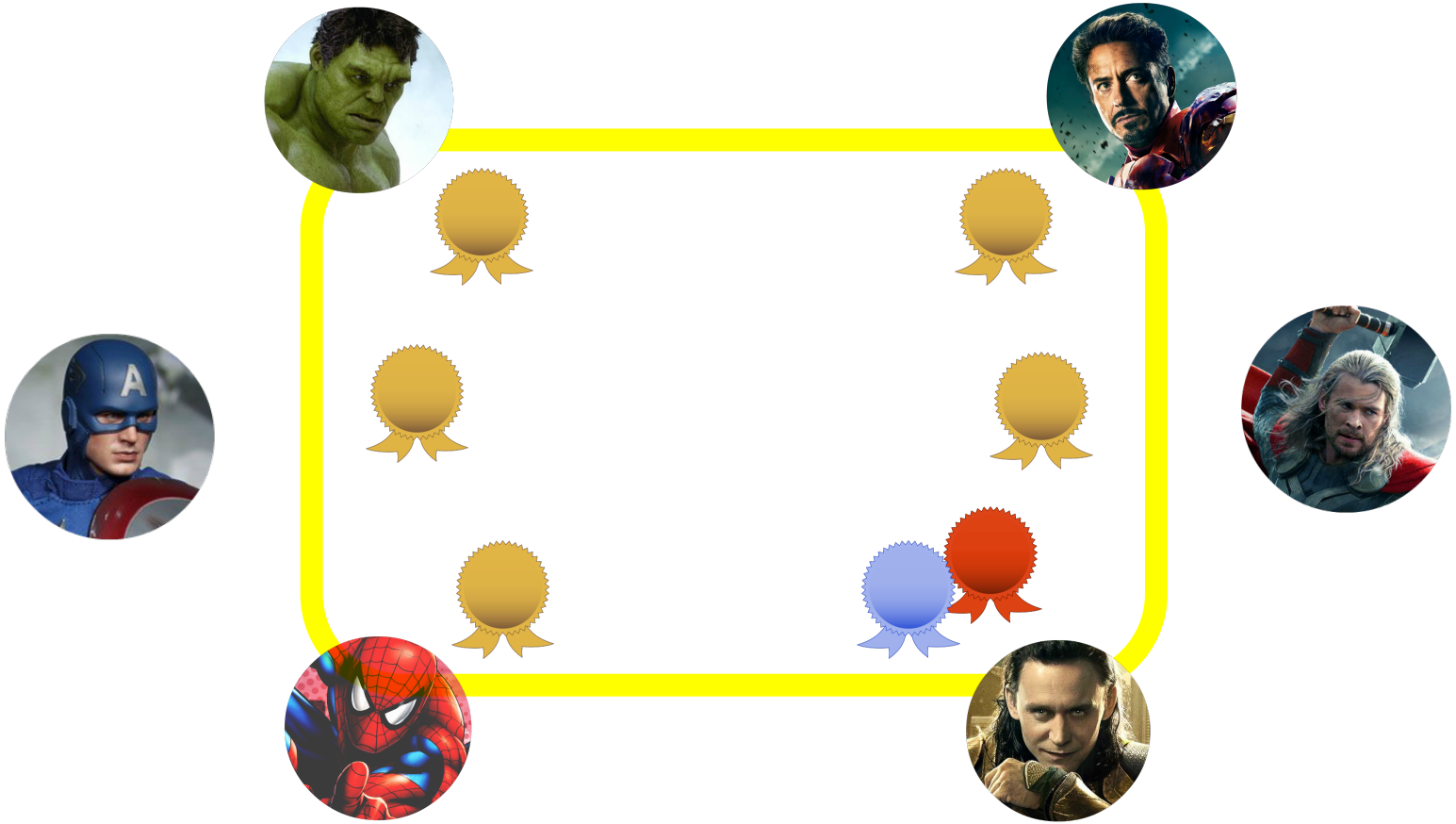
2

Everyone “ack’s”

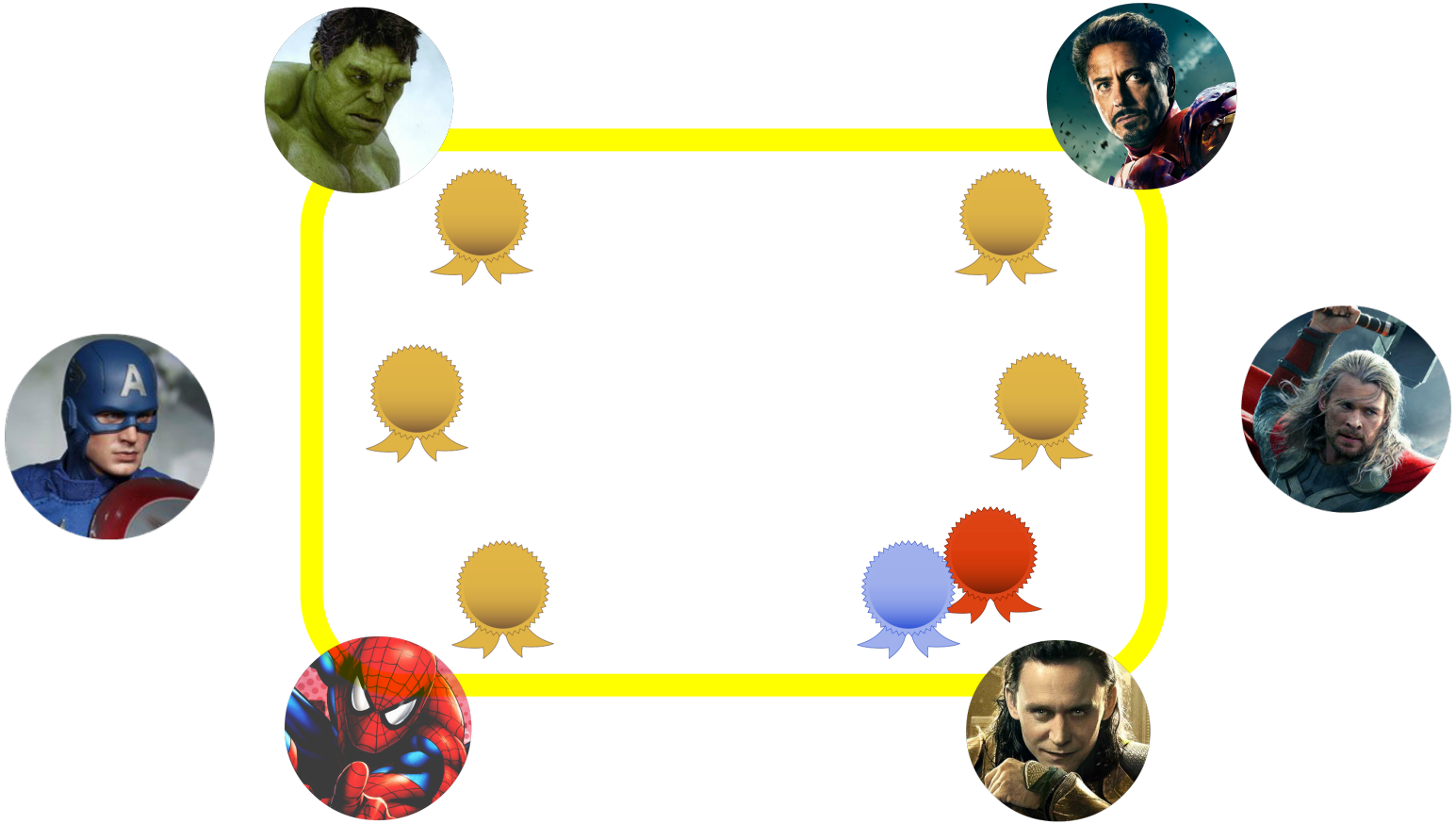
every seq# once!



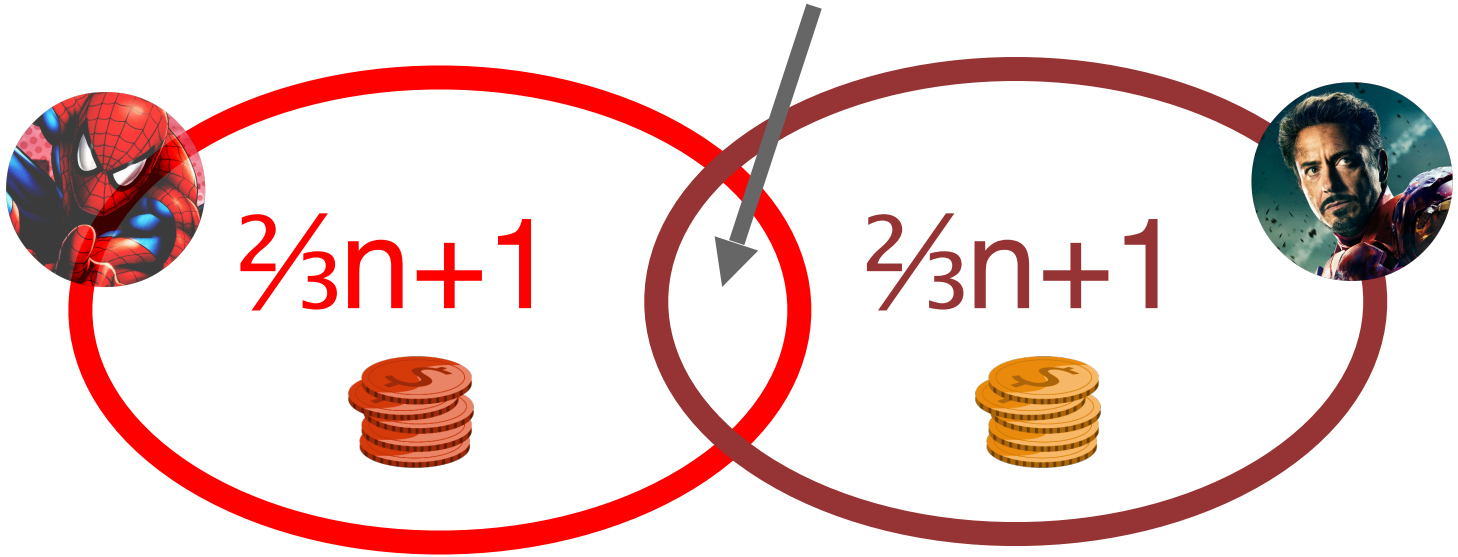
3 Confirm upon “enough” acks



E.g.: Assume ⅔n+1 honest; wait for ⅔n+1 acks

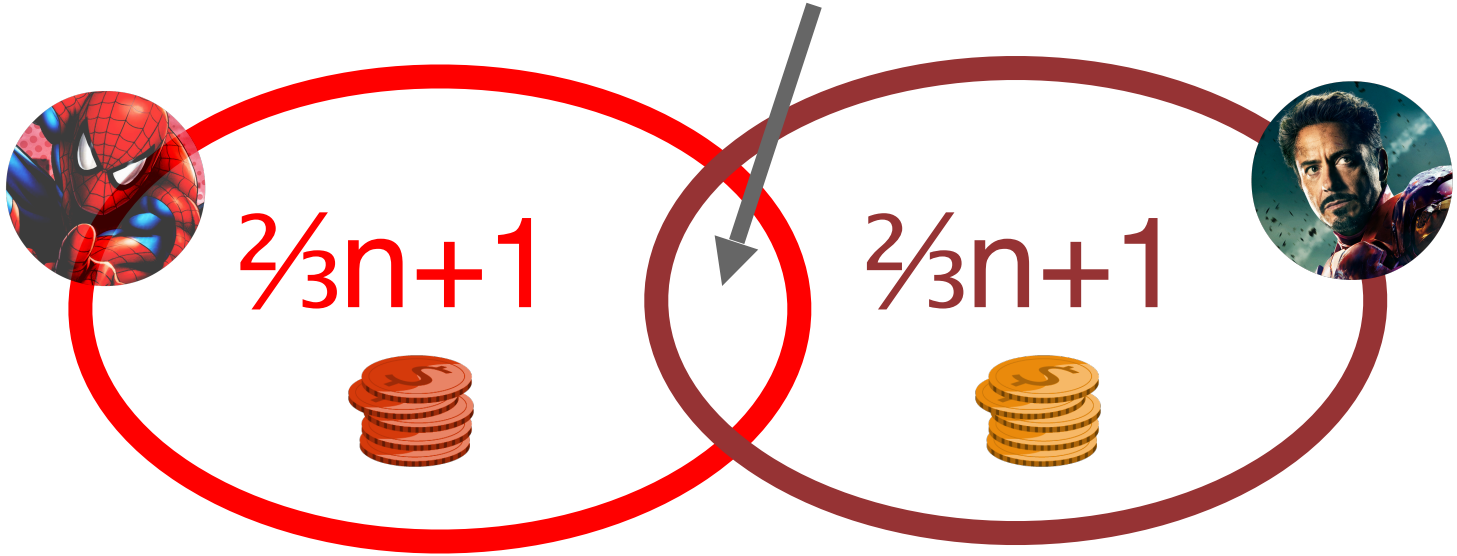


Must intersect at an honest node



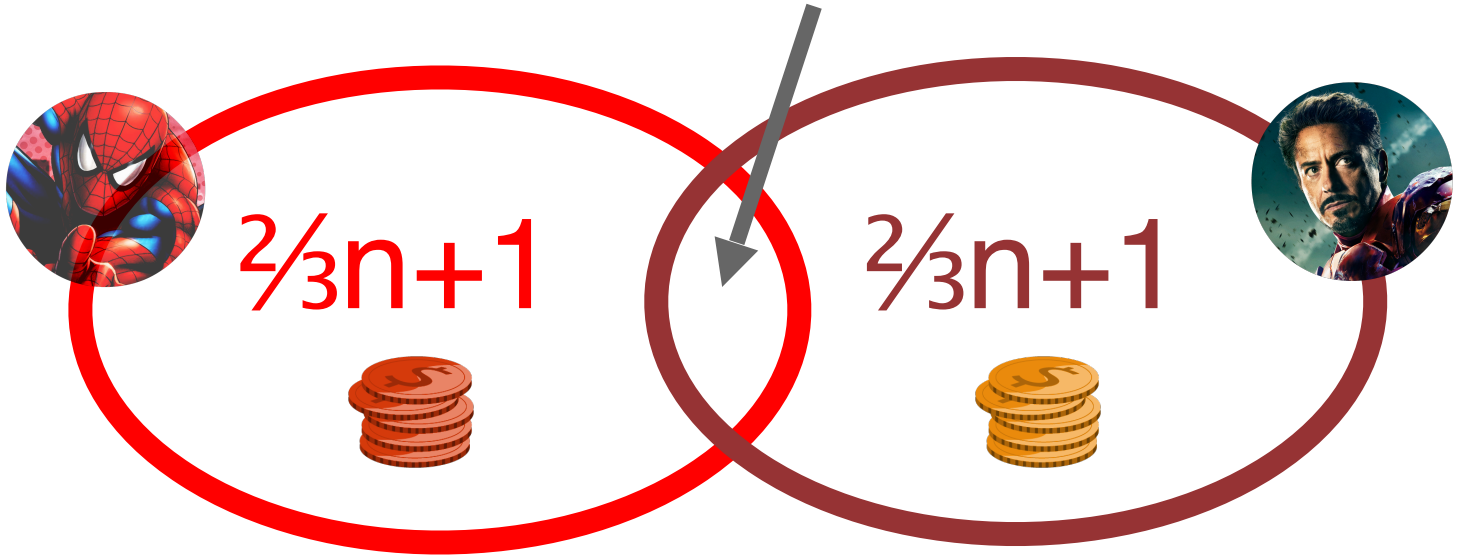
Assume ⅔n+1 honest

Must intersect at an honest node



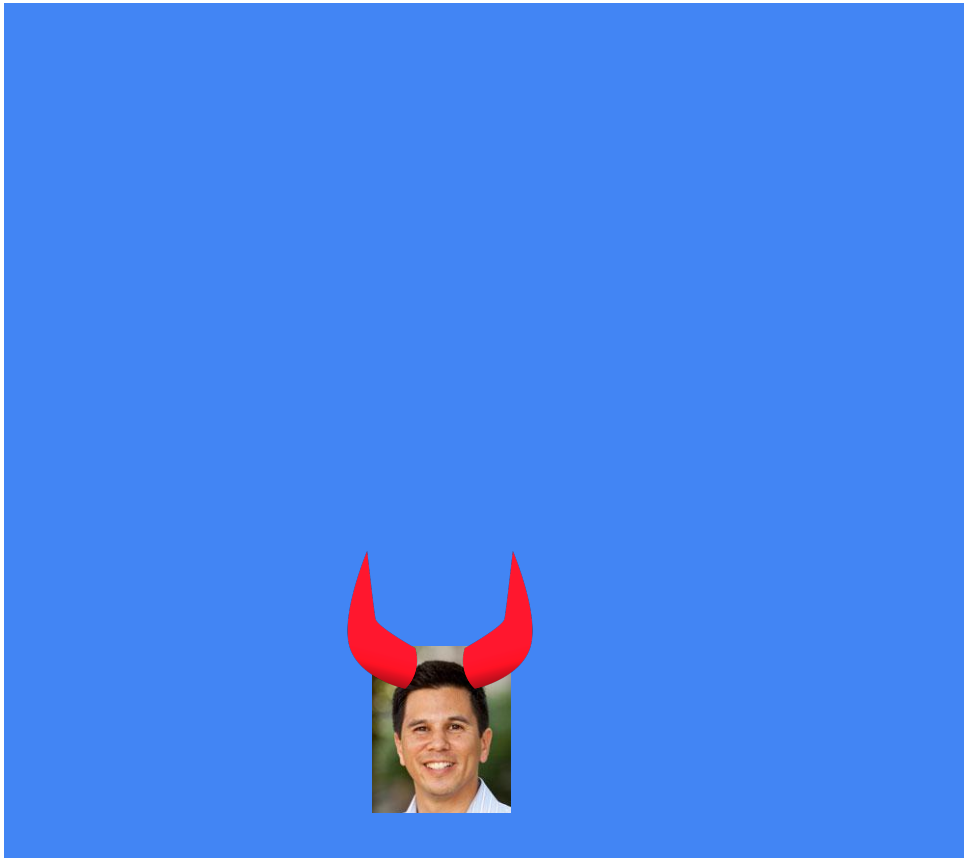
Assume 1/3n malicious

Must intersect at an honest node



Thus  **=** 

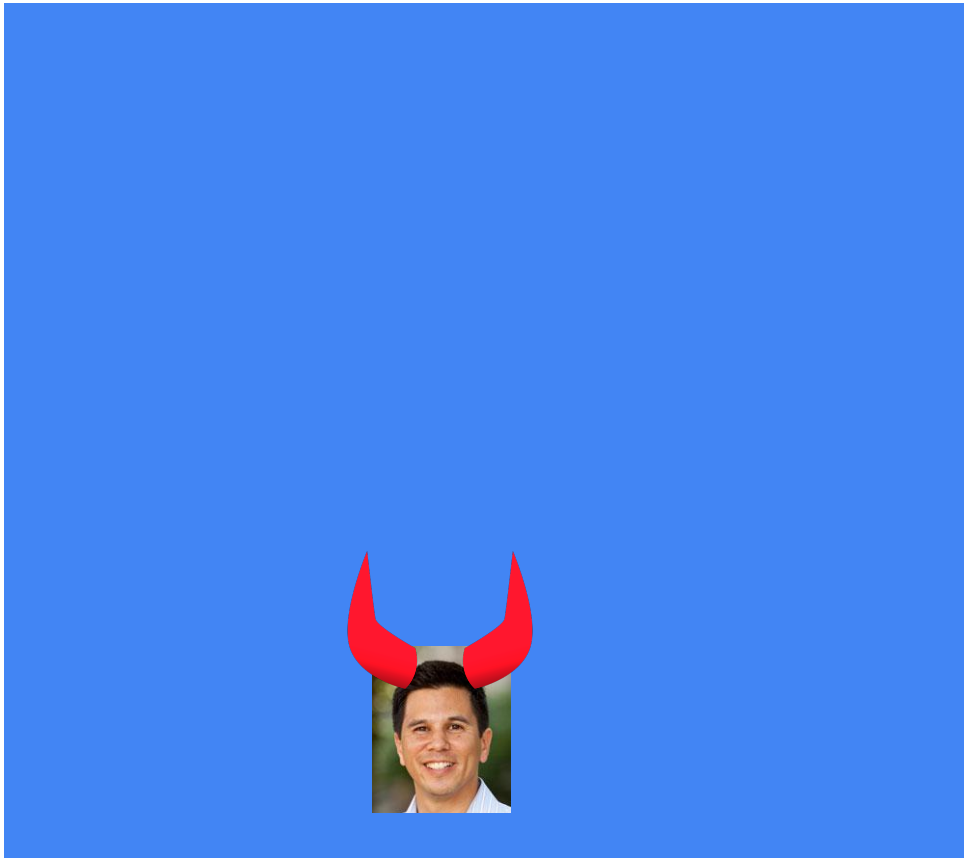
Assume ⅔ honest and online



Assume ⅔ honest and online

✓ **Consistency**

✓ **Liveness**



Assume ⅔ honest and online

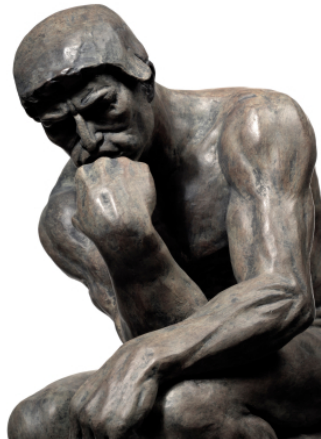
✓ **Consistency**

✓ **Liveness**

✓ **Consistency**

✗ **No liveness**

How do we achieve liveness?

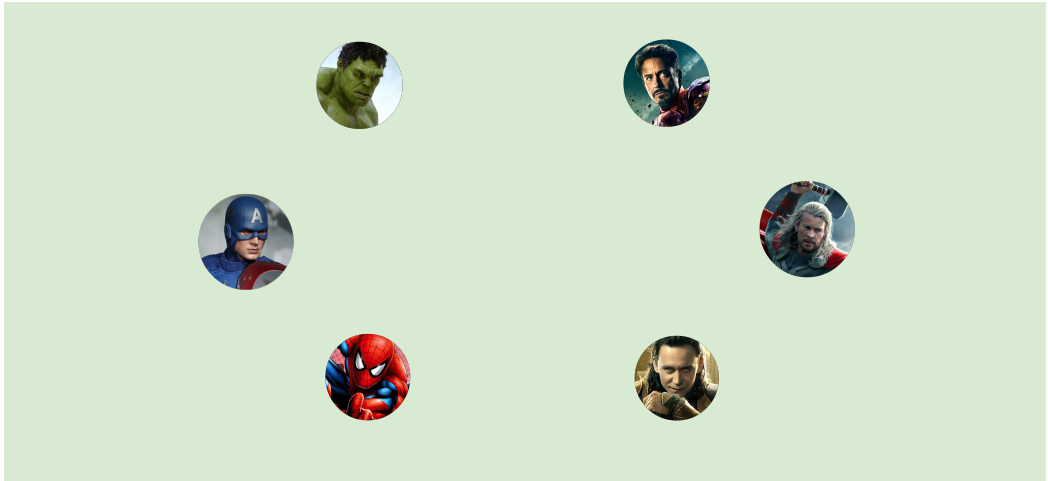


How do we achieve liveness?

You don’t want to know …

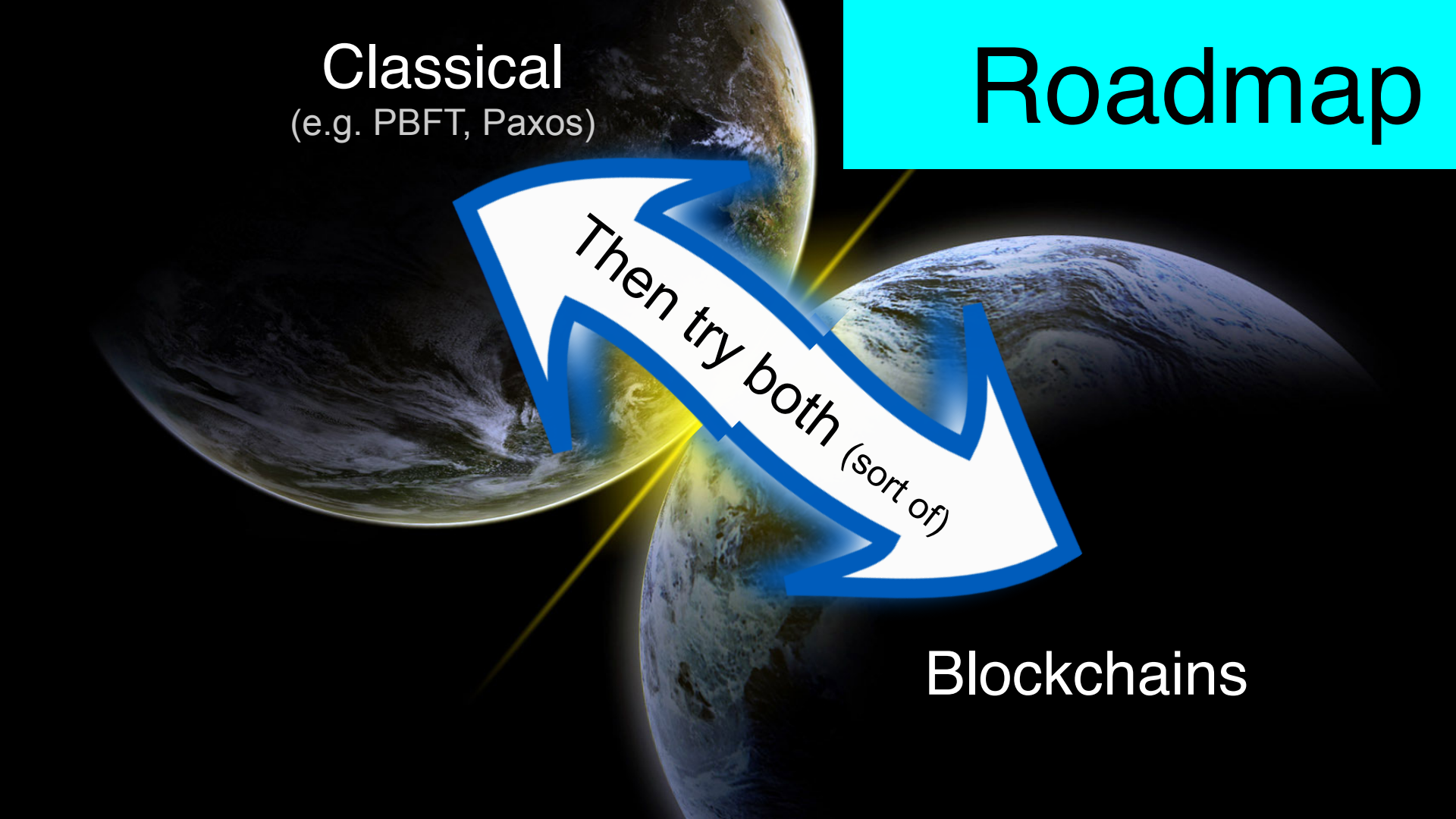
[PBFT, Paxos...]

Anatomy of classical consensus

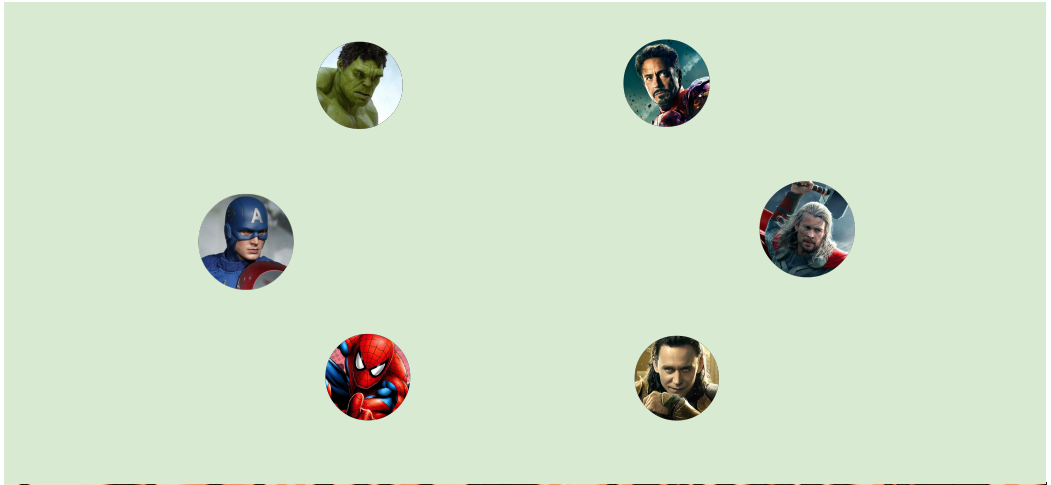


Simple normal path

Complicated recovery path


Classical
(e.g. PBFT, Paxos)
Roadmap
Then try both (sort of)
Blockchains

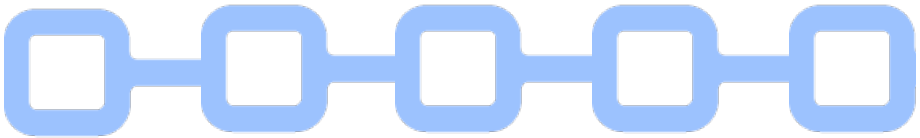
Thunderella



Leader (a.k.a. accelerator)

Committee

(e.g., recent miners or "stakeholders”)



blockchain miners

“Optimistic” mode: **Instant confirmation**

honest and online

majority honest

3/4 fraction honest and **online**

But, still **SECURE** as long as:

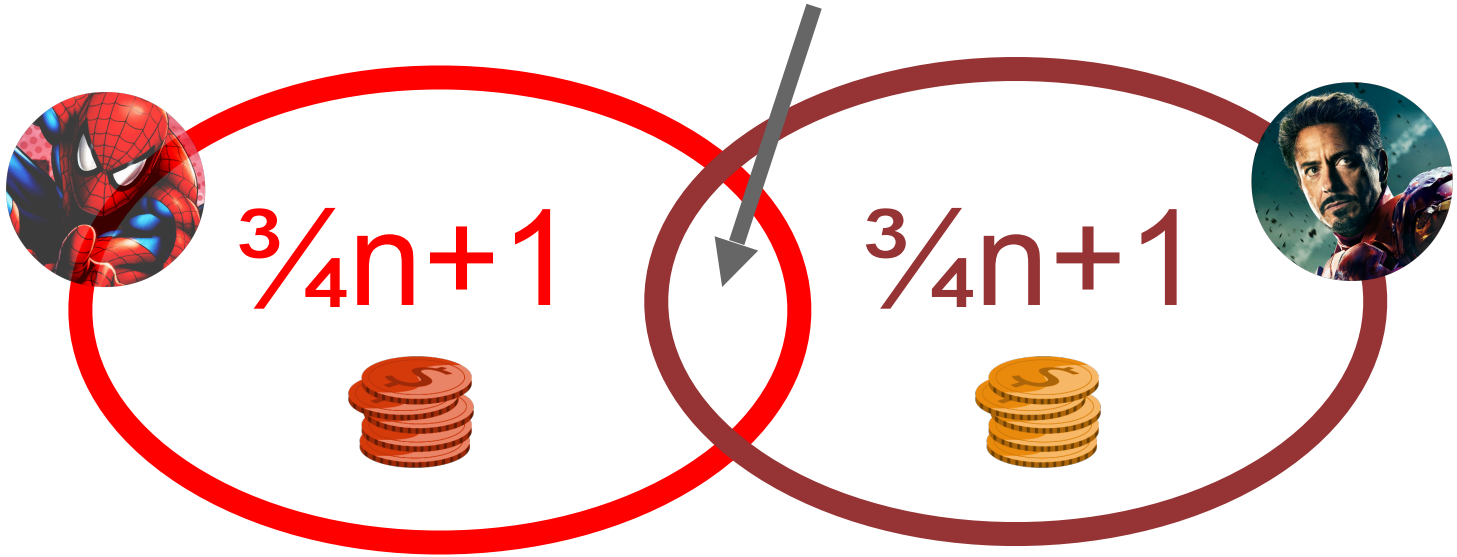
Arbitrary deviation!

majority honest

(but need not be online)

majority honest

Must intersect at an honest node



Assume < ½n malicious

Propose (seq,)

Ack

Propose (seq, )

Ack

1 2 3 4 5 6

¾ acks:
notarized

notarized

Confirm maximal "lucky" sequence

No liveness when

notarized

Confirm maximal “lucky” sequence

blockchain collects evidence of

blockchain collects evidence of

What evidence do we collect?

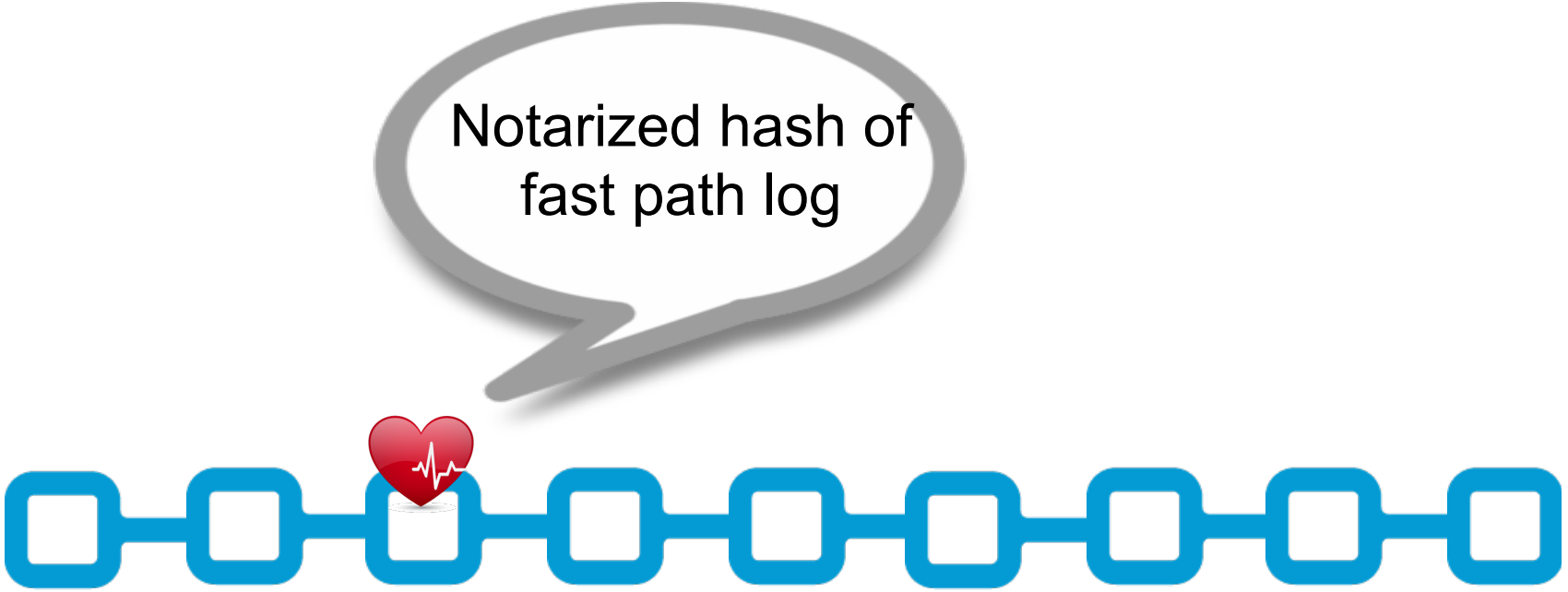
Need: faulty nodes cannot implicate honest leader

Evidence and Recovery

- Miners use blockchain (aka "slowchain") as a complaint/yelling channel
    - Post transactions that haven't been notarized
- Leader must confirm those transactions within a "window"
- If not, then it constitutes as evidence that something is wrong
- We then transition to "slow mode" (but after a "grace period" to agree on longest chain so far)
- Once in slow mode, elect new leader and restart "fast path" after recovery

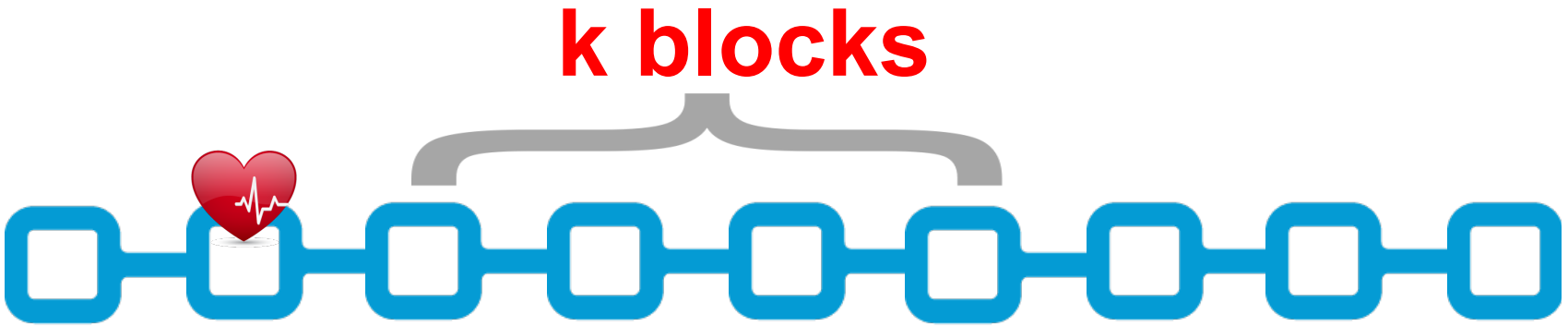
Accelerator posts heartbeats to slowchain

Committee only signs if Acc has confirmed all recent transactions posted to “slowchain”



Accelerator posts heartbeats to slowchain

k blocks without a heartbeat



blockchain collects evidence of

2

Now enter slow mode

Need: agree on log before entering slow mode

1 2 3 4 5 6

1 2 3 4 5 6

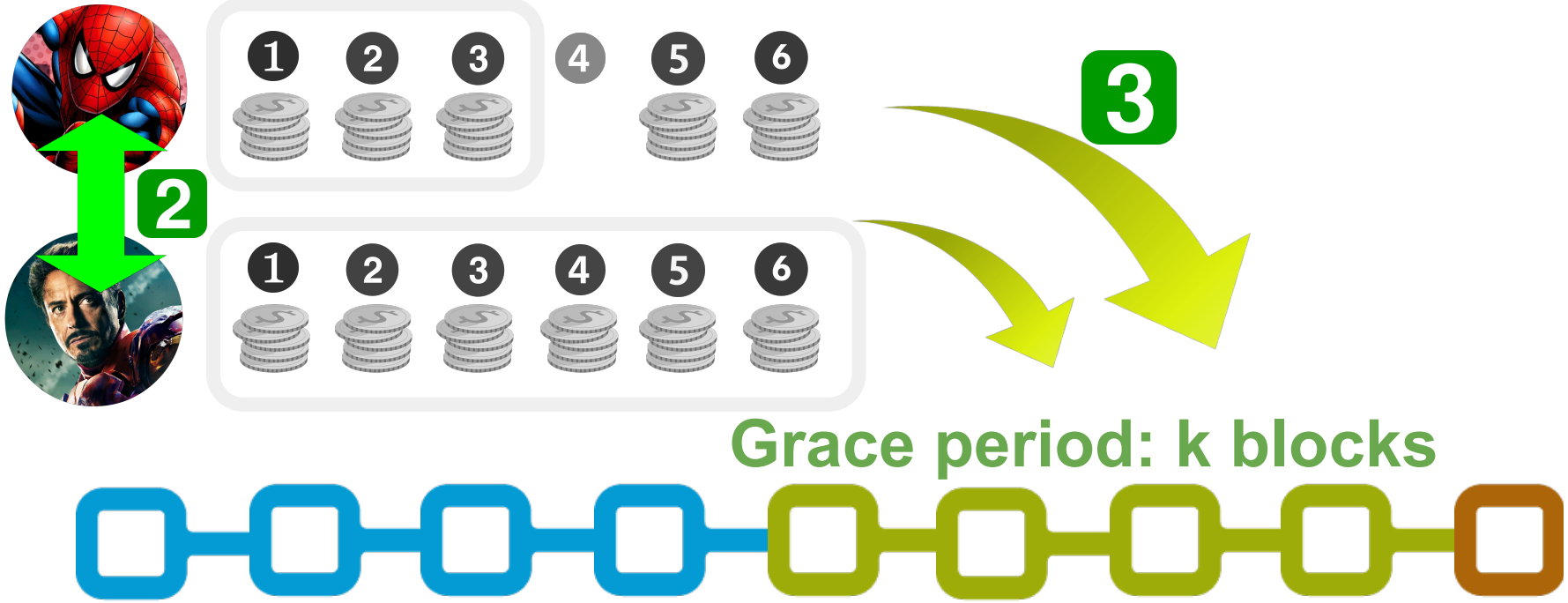
Now enter slow mode

Need: agree on log before entering slow mode

This is an agreement problem in itself.

Use the slowchain for “fallback”

1. Stop participating in fast path
2. Tell others what you know
3. Post notarized but uncheckpointed TXs to slowchain



Summary

Final Remarks

- Incentives for honest behavior?

- Miners might have different incentives. E.g., maybe want to go to slow mode