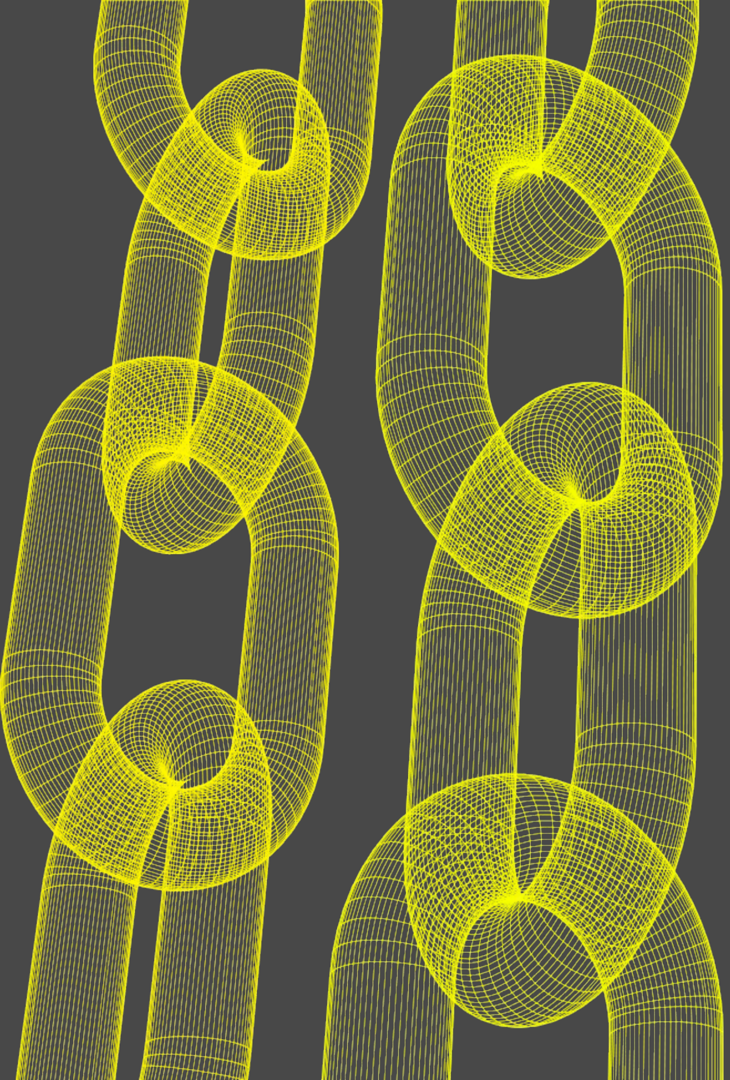
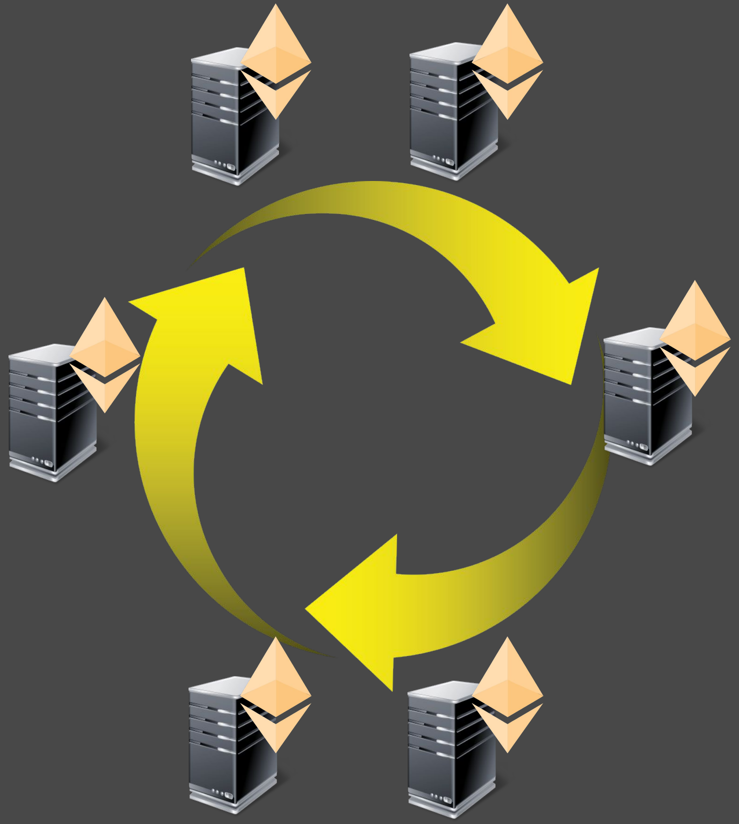


Longest-Chain Consensus Explained

Elaine Shi
Cornell

State-Machine Replication

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

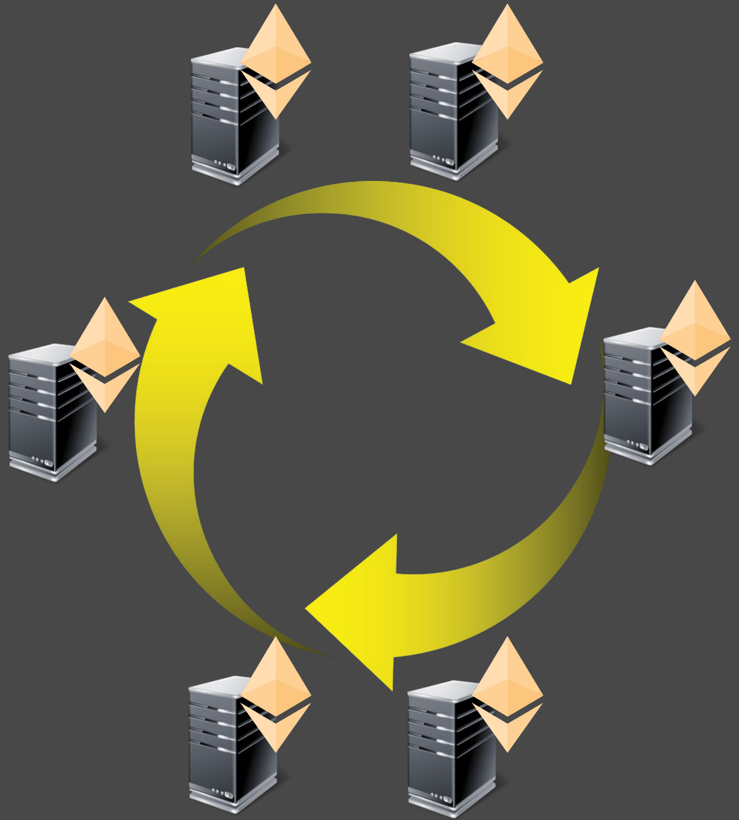


State-Machine Replication

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

Consistency:
Honest nodes agree on log

Liveness:
TXs are incorporated soon



Consensus: A 30-year-old Problem

Apache Zookeeper

YAHOO!

facebook

reddit

NetApp

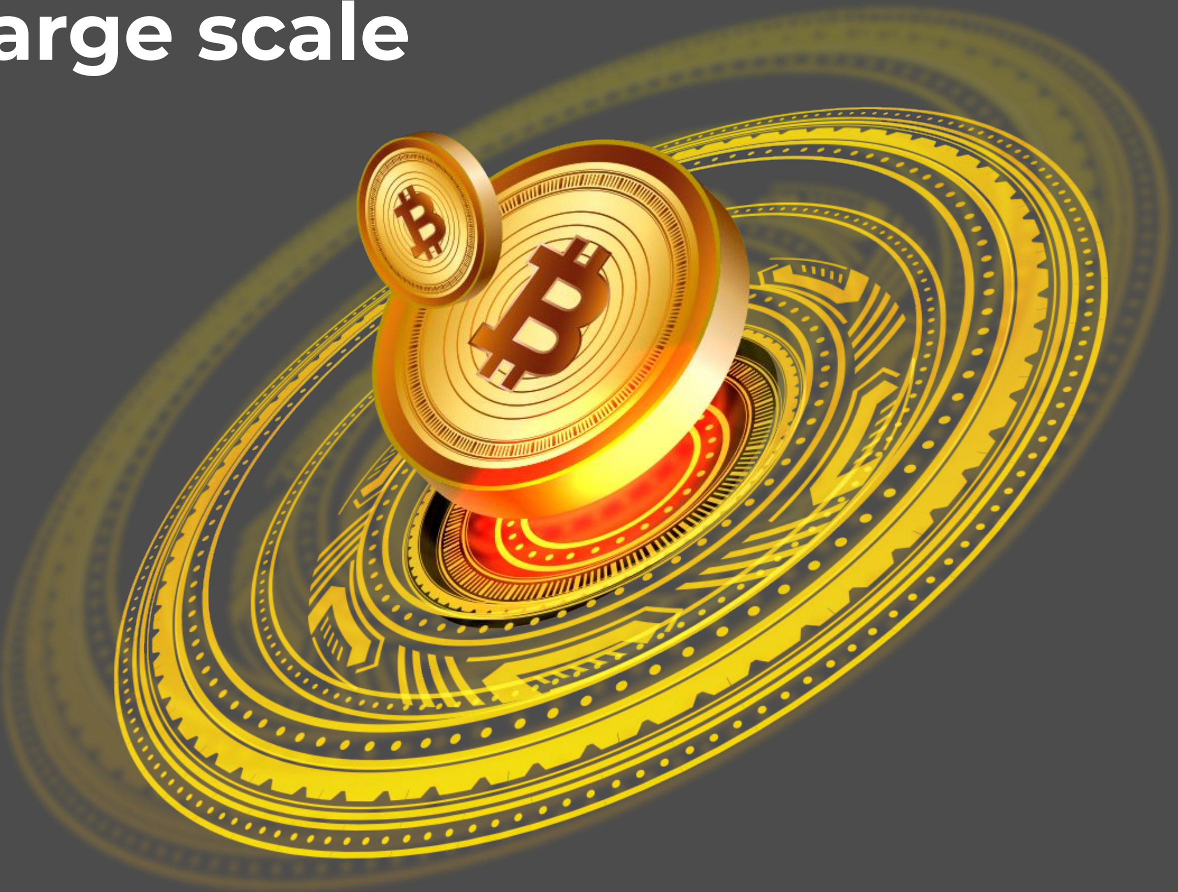
Solr

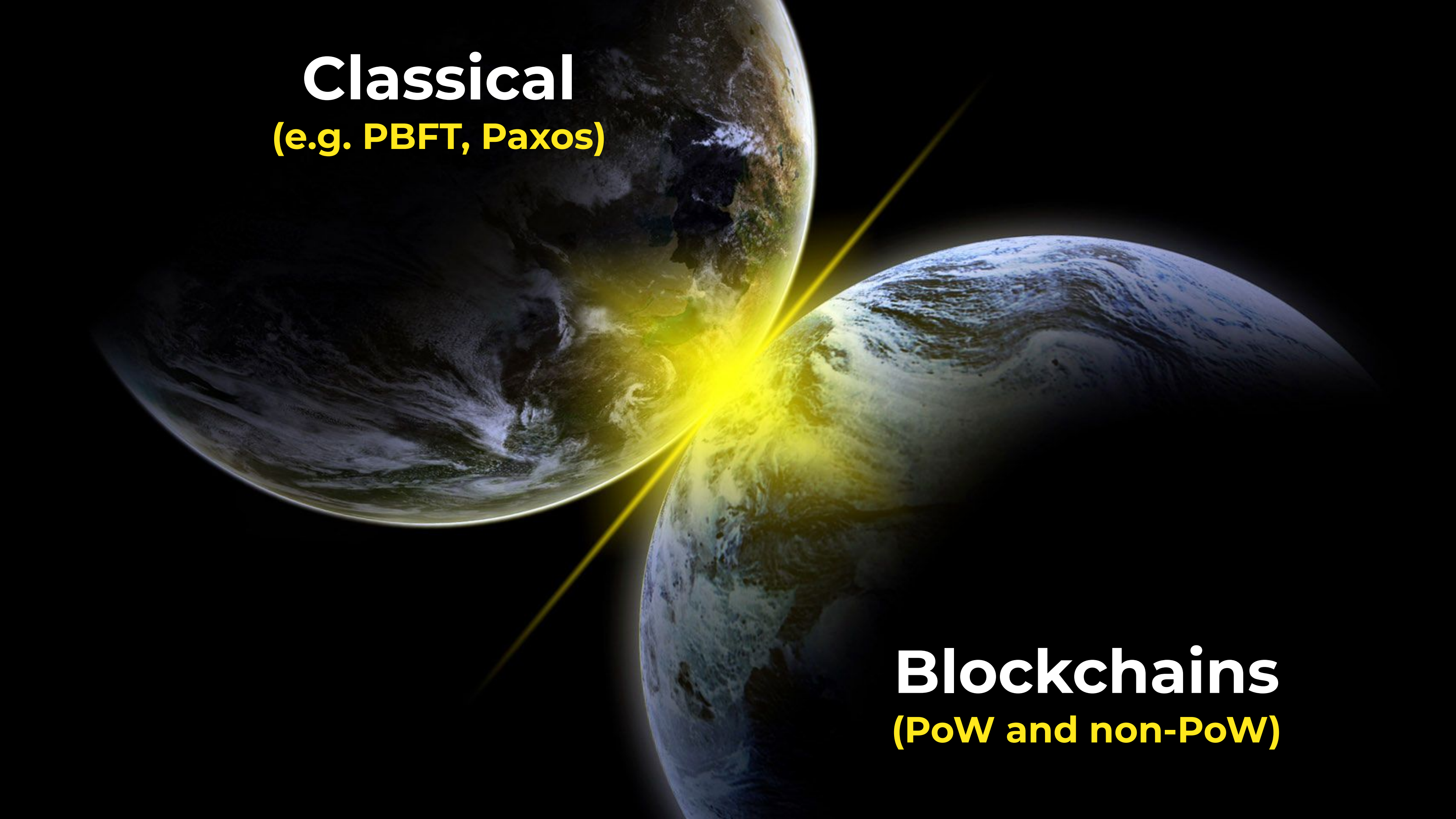
UBER

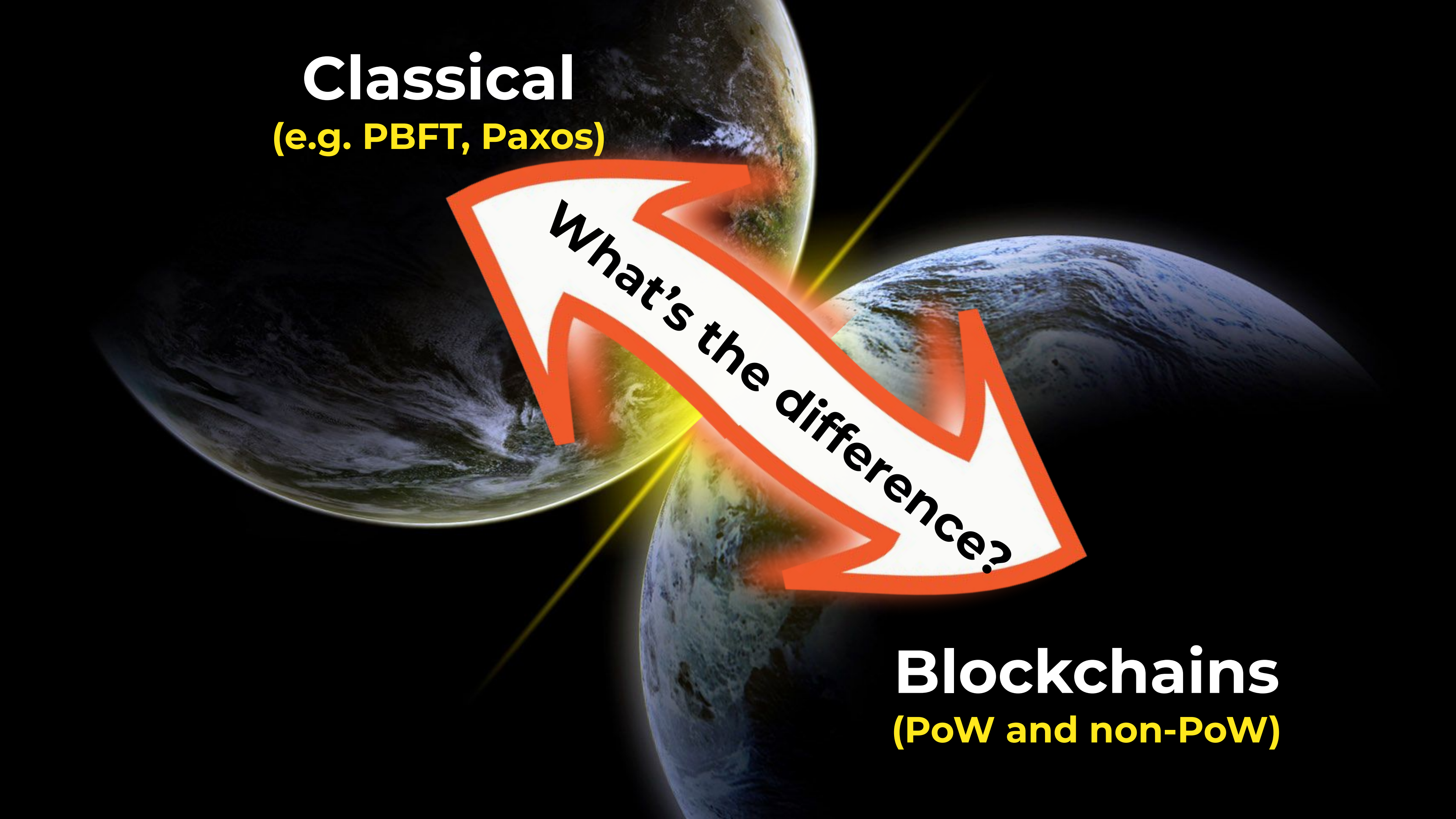
ebay

rackspace

Cryptocurrencies brought consensus to a large scale




Classical
(e.g. PBFT, Paxos)
Blockchains
(PoW and non-PoW)


Classical
(e.g. PBFT, Paxos)
What's the difference?
Blockchains
(PoW and non-PoW)

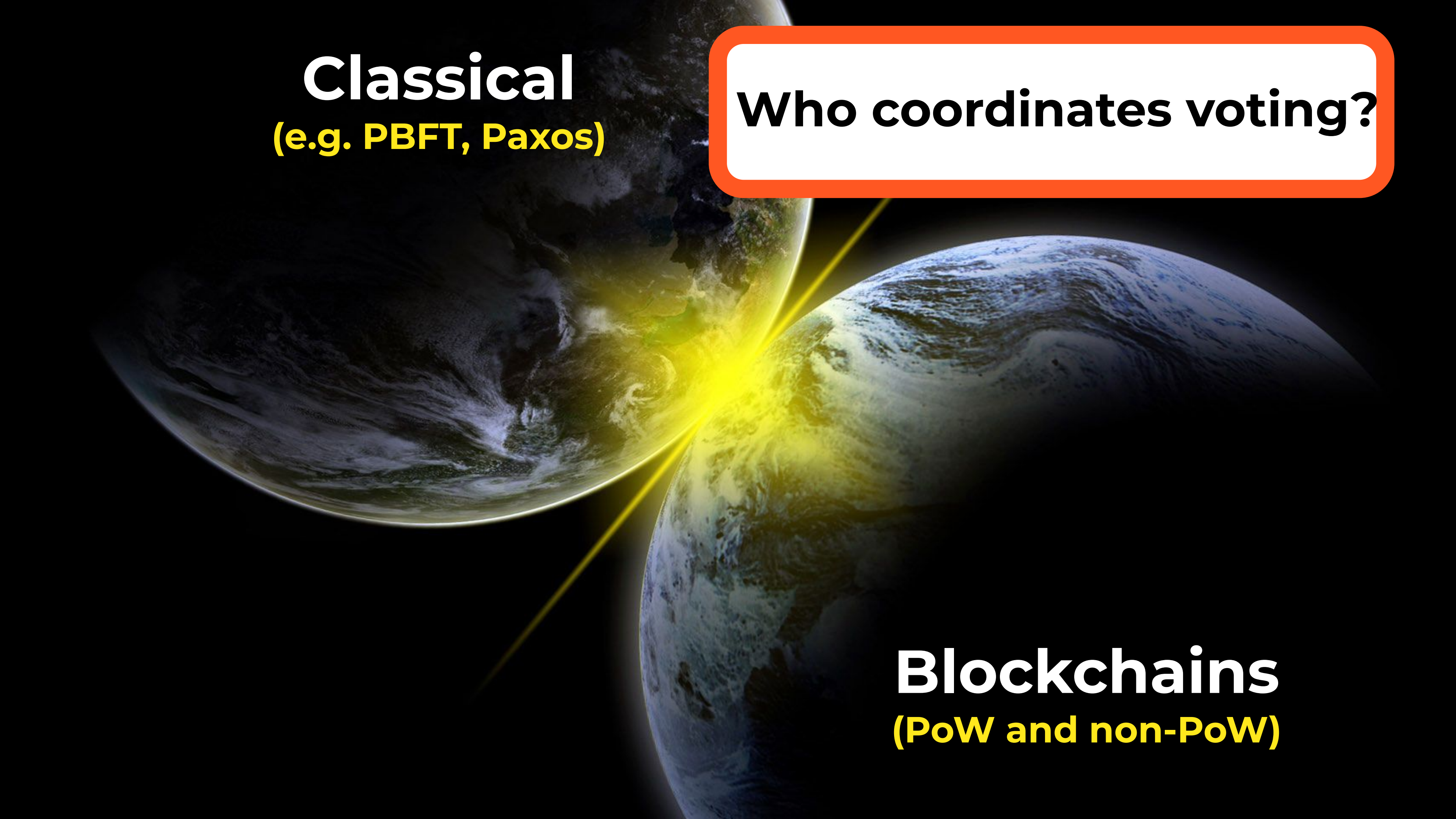
Classical

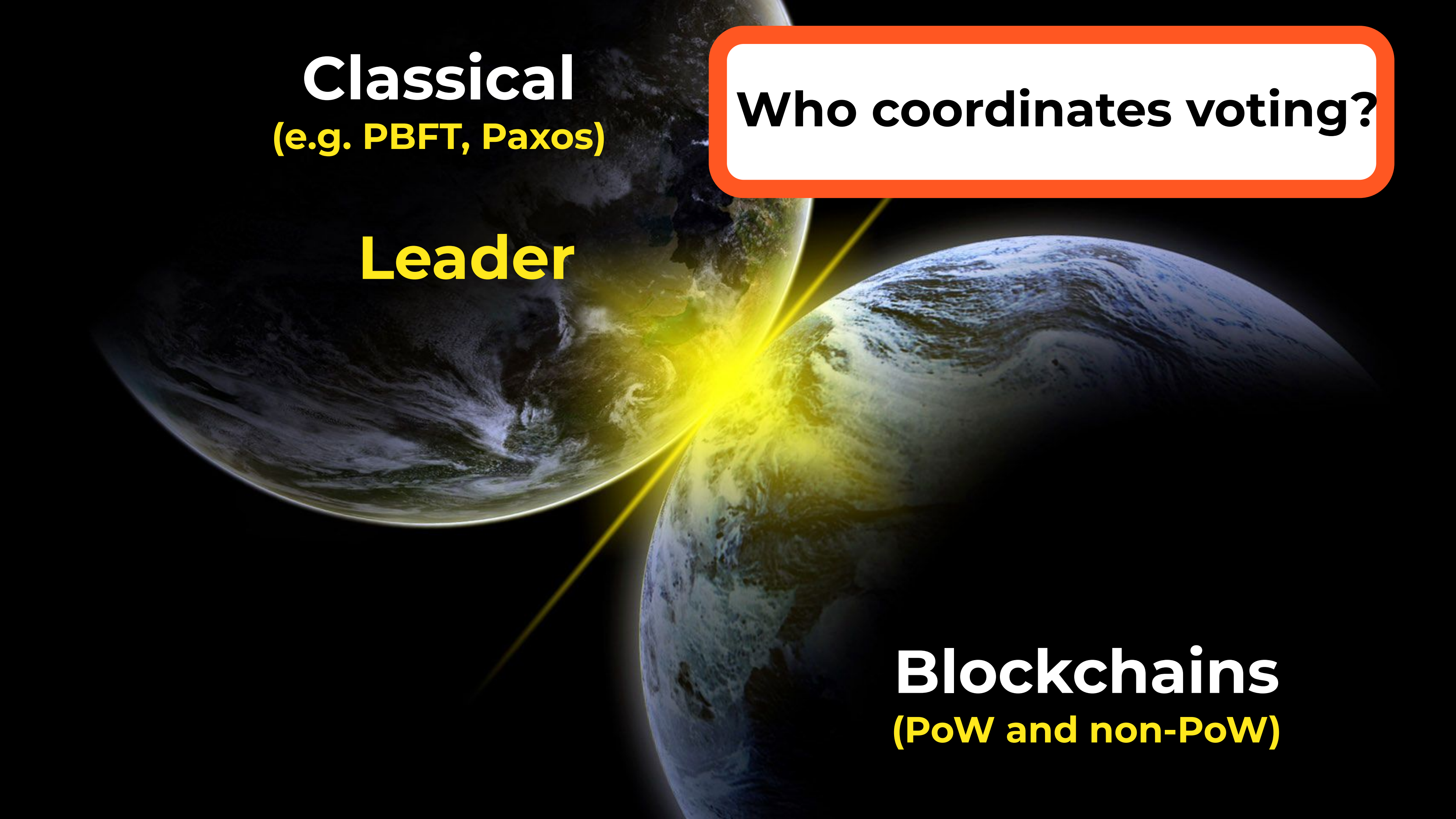
(e.g. PBFT, Paxos)

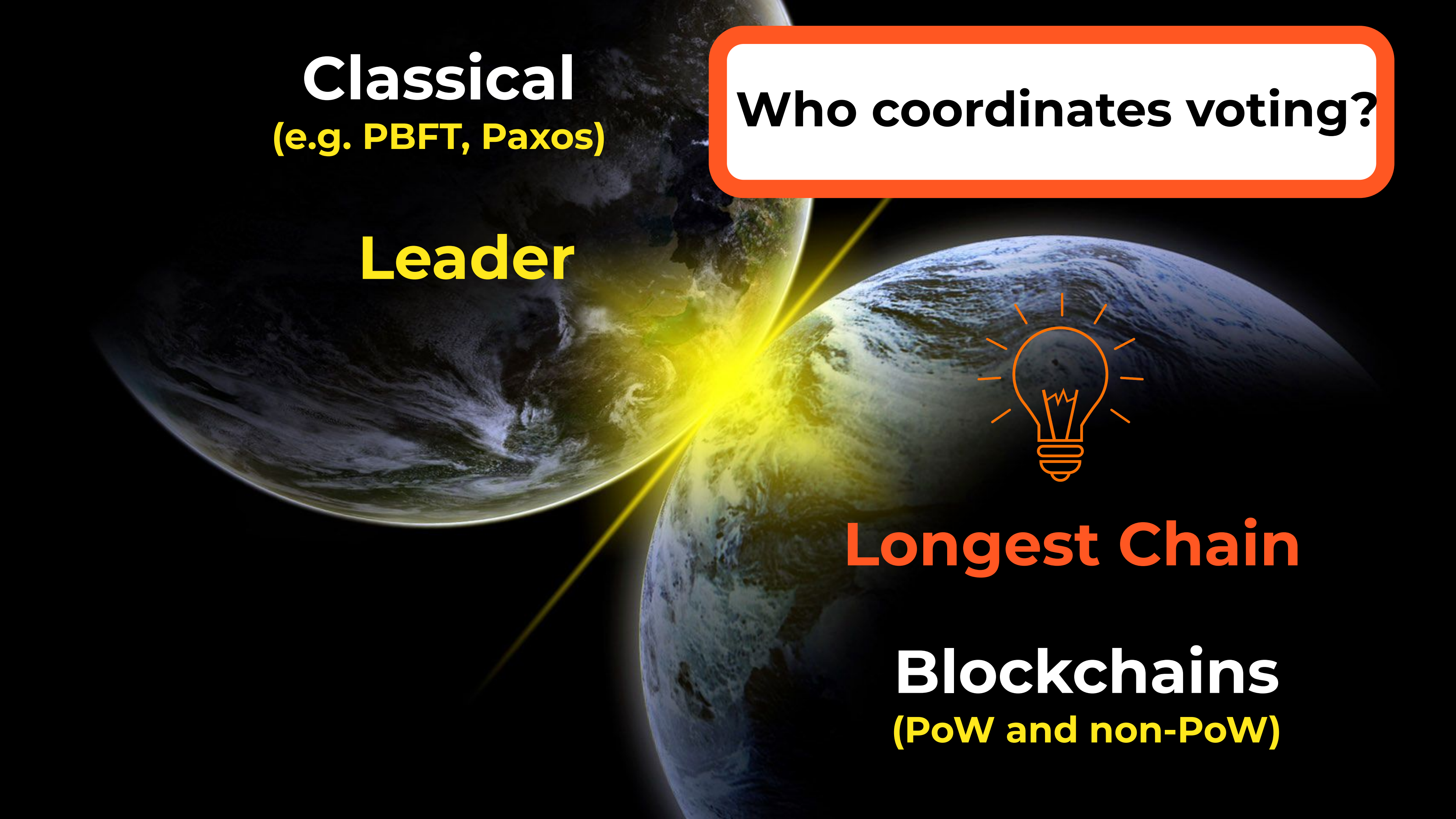
Both reach consensus by voting

Blockchains

(PoW and non-PoW)


Classical
(e.g. PBFT, Paxos)
Who coordinates voting?
Blockchains
(PoW and non-PoW)


Classical
(e.g. PBFT, Paxos)
Who coordinates voting?
Leader
Blockchains
(PoW and non-PoW)


Classical
(e.g. PBFT, Paxos)
Who coordinates voting?
Leader
Longest Chain
Blockchains
(PoW and non-PoW)

This Talk

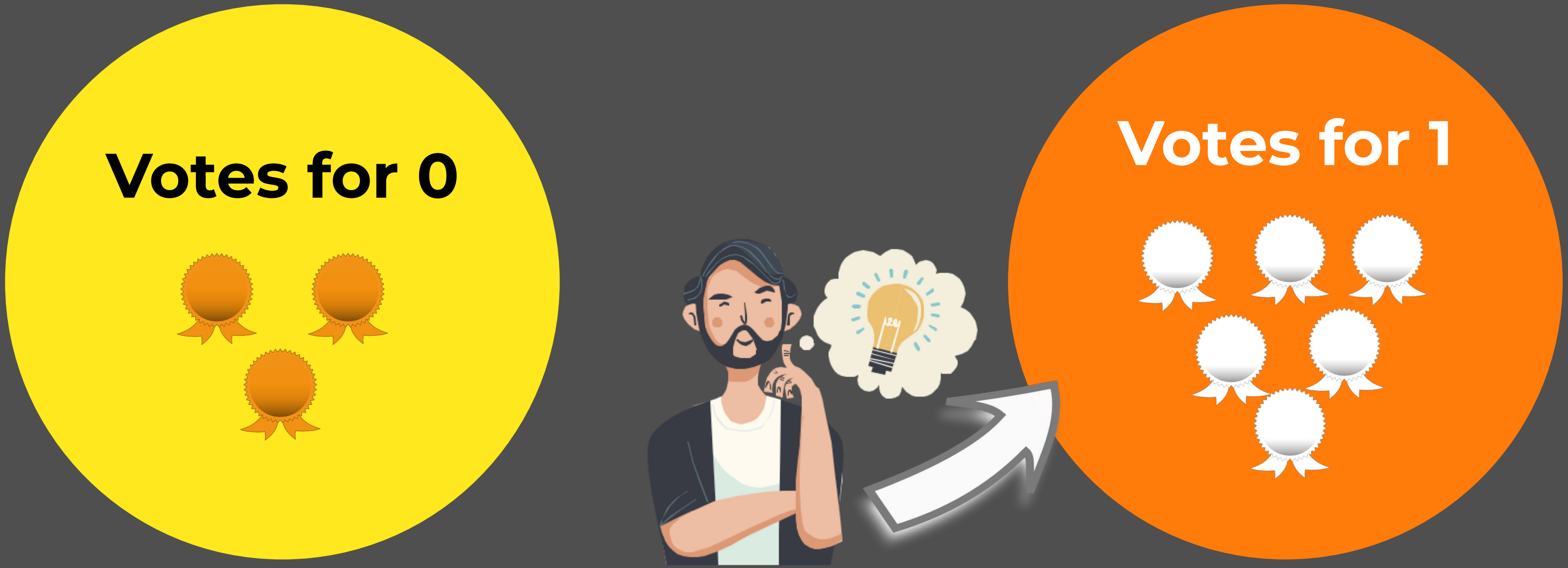
Classical vs longest-chain

Simplest proof for “longest-chain” style protocol

Assume: honest nodes' messages delivered in 1 round.

- In round i, node i mod n is allowed to vote
- Each round i, node i votes for the currently most popular

Assume: honest nodes’ messages delivered in 1 round.



- In round i, node i mod n is allowed to vote
- Each round i, node i votes for the currently most popular

Honest = $\frac{2}{3}n + 1$ Corrupt = $\frac{1}{3}n - 1$

Vote Growth Lemma: by the end of round $T = n$, every honest node's most popular bit has at least $\frac{2}{3}n + 1$ votes

Honest = $\frac{2}{3}$ n + 1 Corrupt = $\frac{1}{3}$ n - 1

Vote Growth Lemma: by the end of round T = n, every honest node's most popular bit has at least $\frac{2}{3}$ n + 1 votes

Proof: every honest-voter round, honest voter signs most popular bit b in its view and shares all votes on b with others

Honest = $\frac{2}{3}n + 1$ Corrupt = $\frac{1}{3}n - 1$

Consistency Theorem: by the end of round $T = n$, it cannot be that both bits have $\geq \frac{2}{3}n + 1$ votes

Honest = $\frac{2}{3}$ n + 1 Corrupt = $\frac{1}{3}$ n - 1

Consistency Theorem: by the end of round $T = n$, it cannot be that both bits have $\geq \frac{2}{3} n + 1$ votes

Proof: an honest-voter round increases total # votes by 1, a corrupt-voter round increases total # votes by at most 2.
Thus by round n,
total # votes $\leq (\frac{2}{3} n + 1) + 2(\frac{1}{3} n - 1) < 4n/3$.

Randomized, longest-chain variant of this achieve security against minority corruption

Nakamoto

PoW-based

Sleepy Consensus
[PS, eprint'16, Asiacrypt'17]

Snow White
[DPS, eprint'16, FC'19]

Ouroboros
[Crypto'17]

PoS-based

c.f. Herding in Economics

[Banarjee'92]

c.f. Herding in Economics

- Everyone has some independent signal about some fundamental W (e.g., W = "is there global warming?")
- Announce their best guess for W one by one
- Update belief based on observations

[Banarjee'92]

c.f. Herding in Economics

- Everyone has some independent signal about some fundamental W (e.g., W = “is there global warming?”)
- Announce their best guess for W one by one
- Update belief based on observations

Cascade: If I originally believe in YES but I hear NO, NO, best to announce NO

[Banarjee’92]

Foolishness of the crowd

- Everyone has some independent signal about some fundamental W (e.g., W = "is there global warming?")
- Announce their best guess for W one by one
- Update belief based on observations

Cascade: If I originally believe in YES but I hear NO, NO, best to announce NO

[Banarjee'92]

This Talk

Classical vs longest-chain

Simplest proof for
“longest-chain” style protocol

Longest-chain consensus

Small amortized **bandwidth**
(one vote per block)

More **decentralized**
See **"sleepy model"** [PS, Asiacrypt' 17]

Deterministic longest-chain protocols in practice

- Parity's Aura protocol
- EOS's DPoS protocol

Thank You!

elaine@cs.cornell.edu