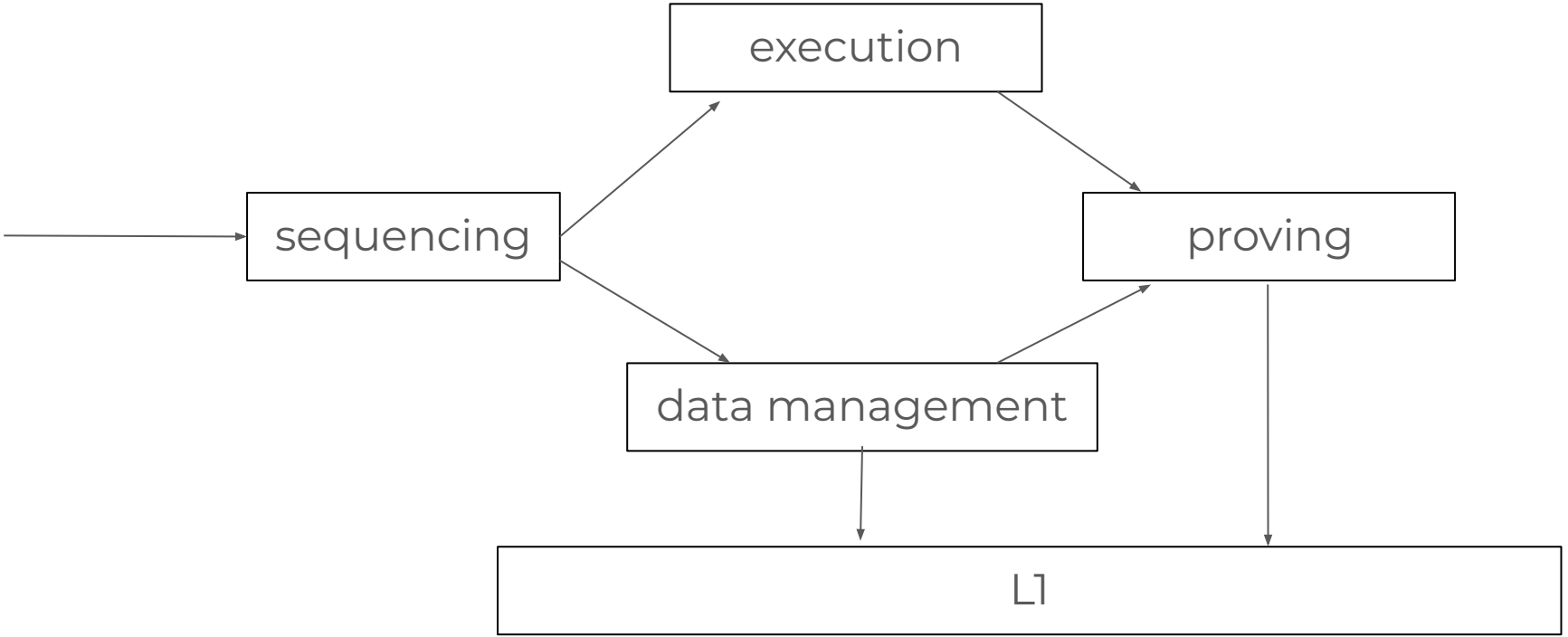
Permissionless Optimistic Validation with BoLD

Ed Felten

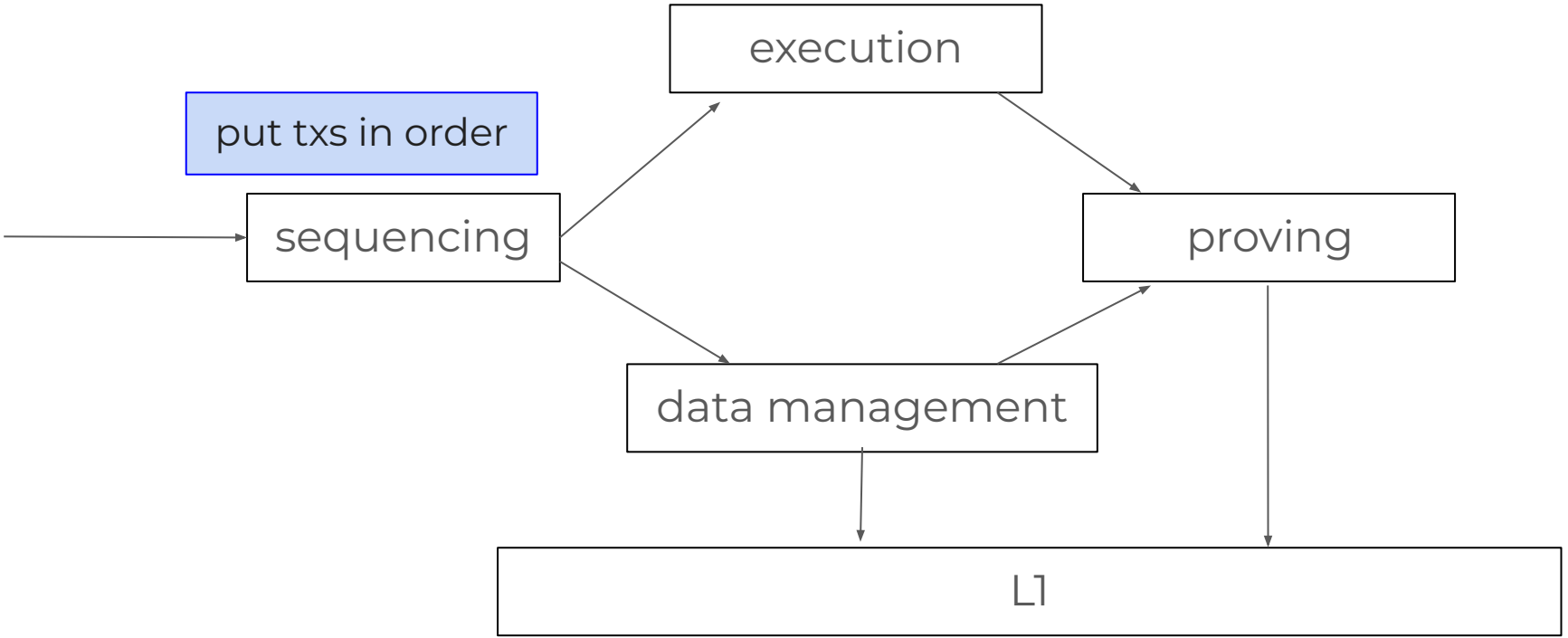
Co-founder and Chief Scientist

OFFCHAIN LABS

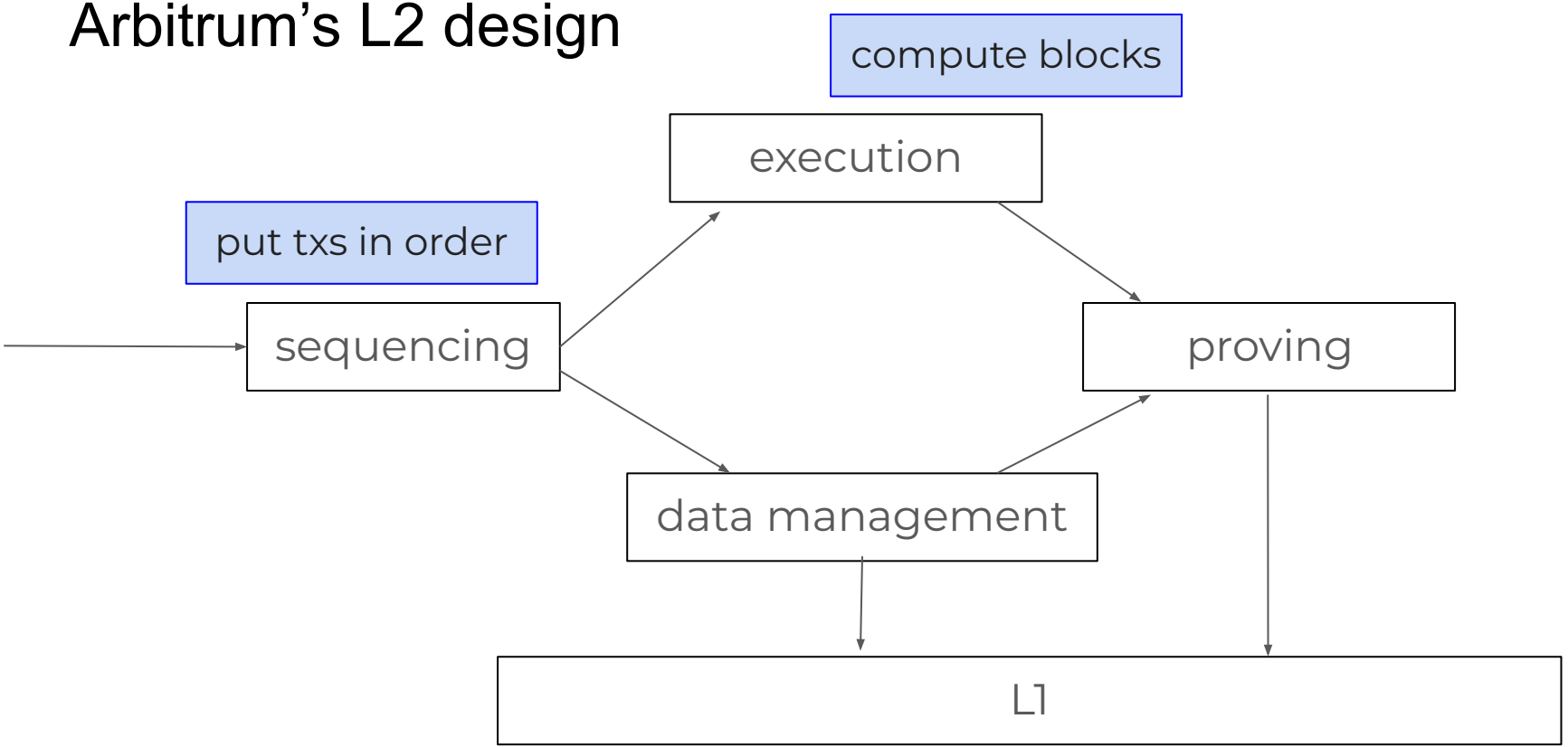
Arbitrum’s L2 design



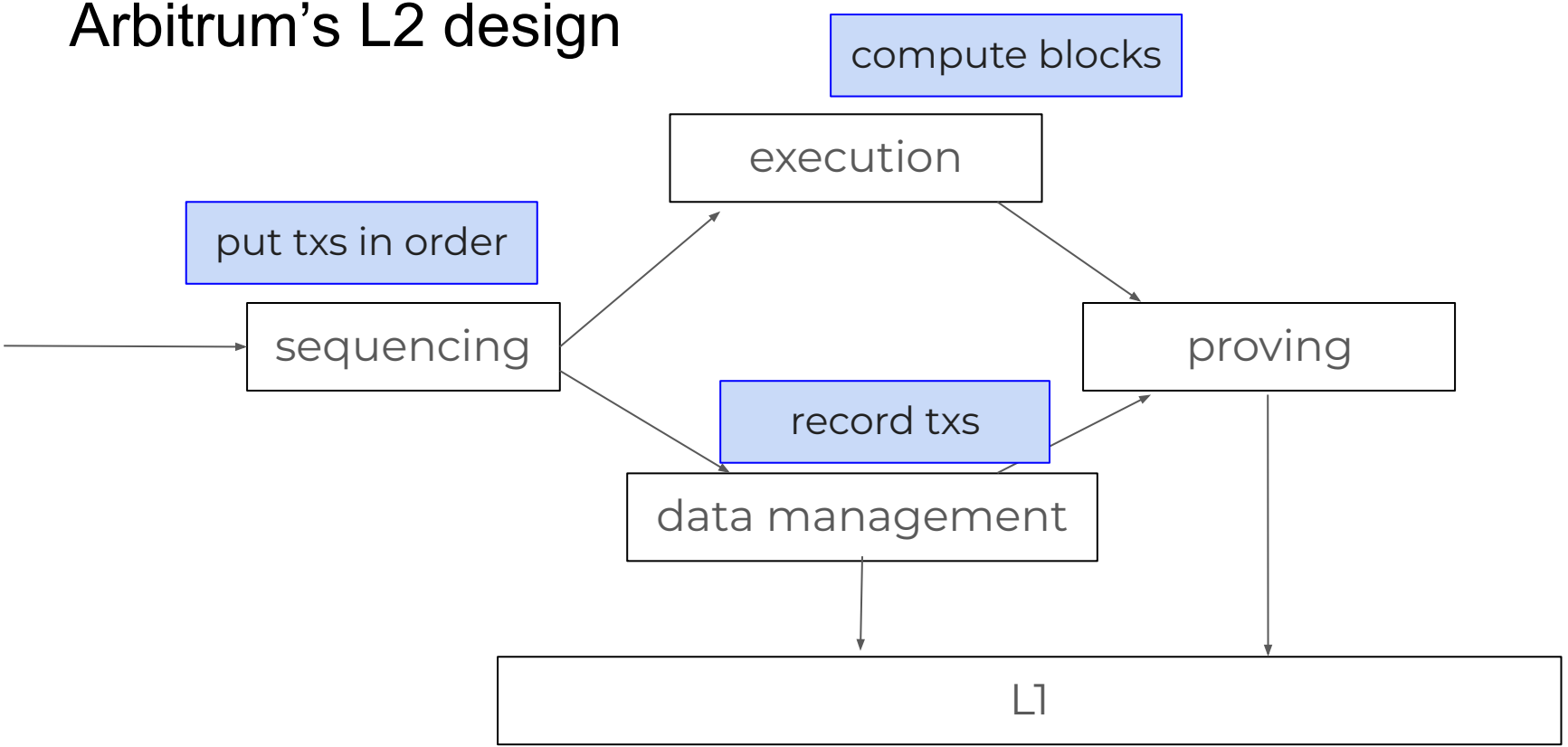
Arbitrum’s L2 design



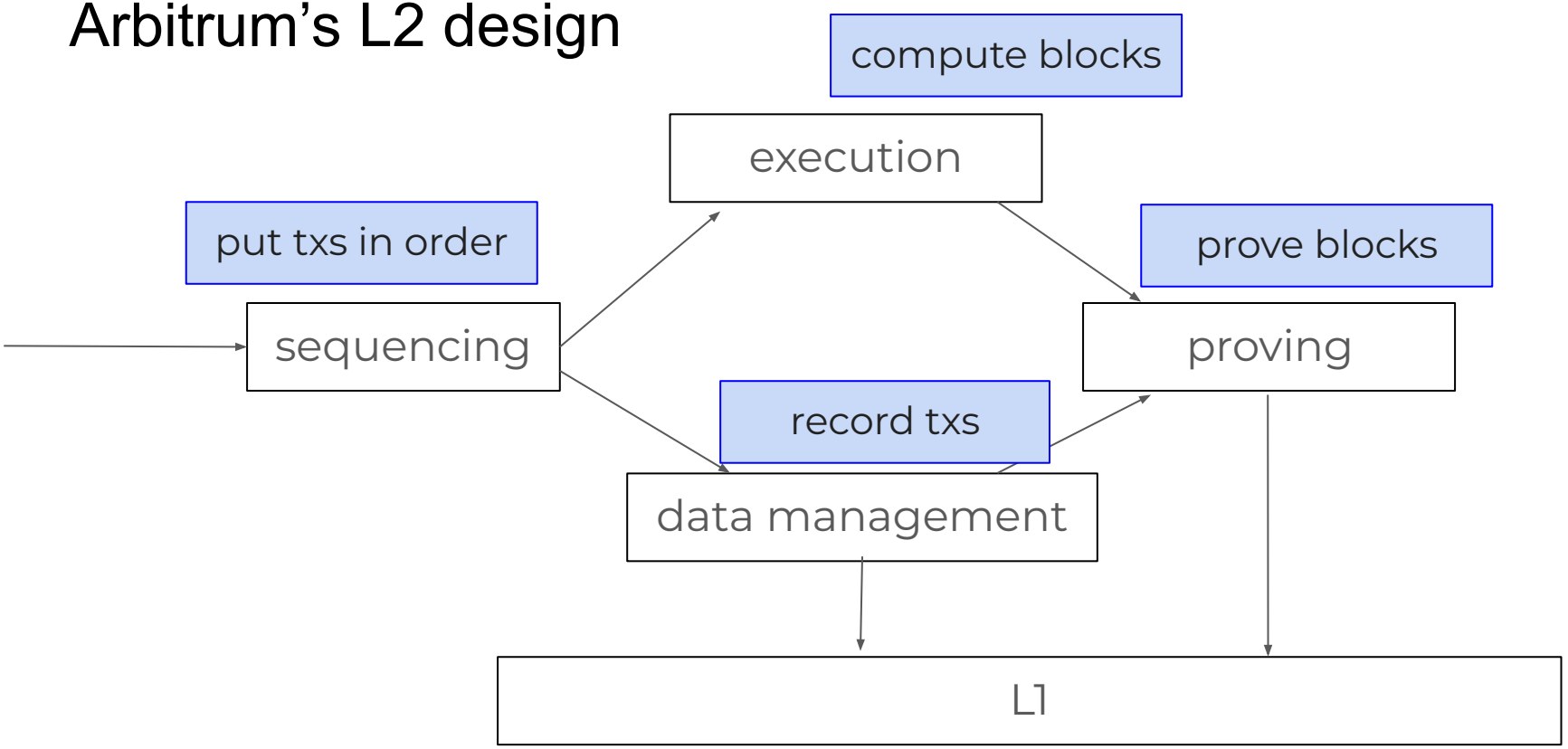
Arbitrum's L2 design



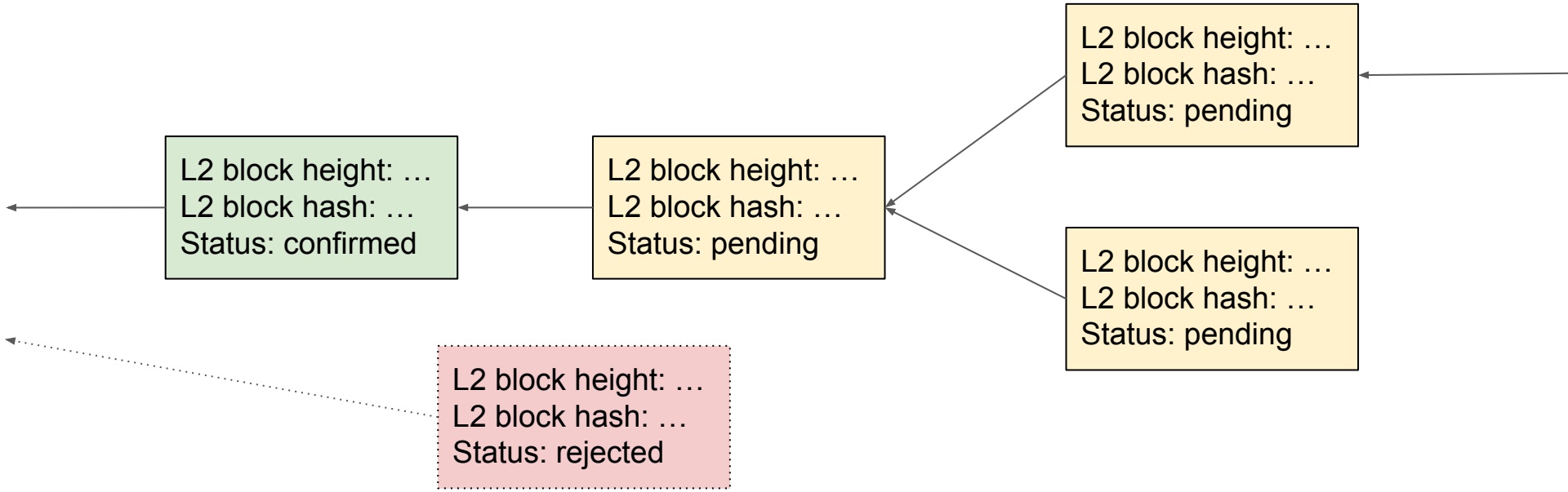
Arbitrum’s L2 design



Arbitrum’s L2 design



Current protocol: assertions



(protocol is managed by L1 contracts)

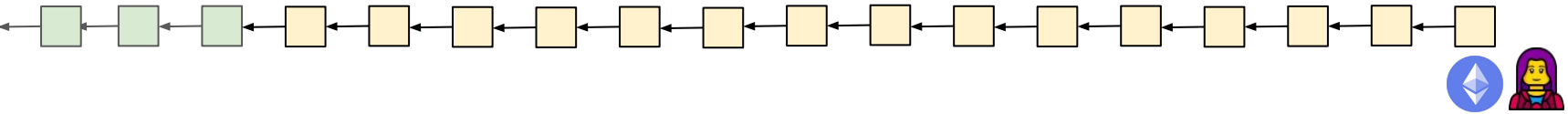
Current protocol: staking

- Any validator can stake on any pending assertion
  - implicitly staking on all pending ancestors as well
  - can move your stake to any successor
  - can recover your stake if assertion you're staked on it confirmed

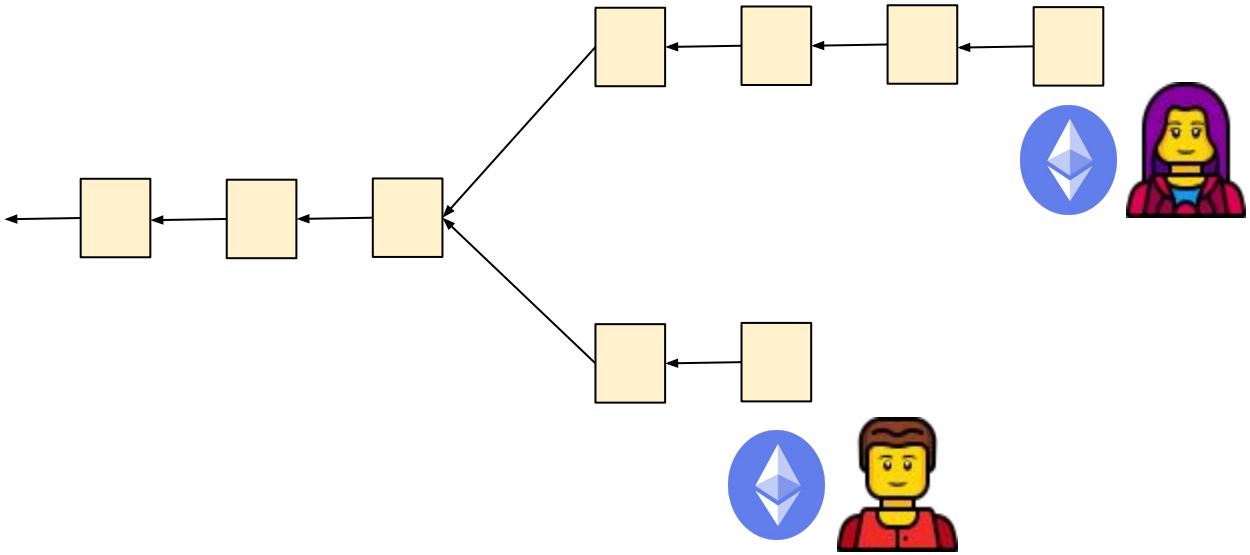
- Every pending leaf will have at least one stake

- If your stake is challenged and you lose, your stake is slashed
  - incentive not to stake dishonestly

Current protocol: normal case



Current protocol: challenges



Properties of current challenge protocol

- Trustless safety: if one honest validator, no bad assertion will be confirmed
- Trustless liveness: if one honest validator, a (good) assertion will be confirmed
- If validators follow incentives, protocol is efficient, minimum time to confirmation
- Malicious validator can cause delays
  - Worst-case: attacker delays confirmation by N challenge periods, by sacrificing N stakes

L1 censorship and the challenge period

Any L2 protocol relies on ability to post transactions on L1 Ethereum.

But Ethereum is subject to censorship attacks.

Current social consensus:

No censorship longer than 7 days on Ethereum without social response.

Censorship: formalizing the threat model

Adversary can censor any Ethereum block(s) of its choice.

But no more than ***C*** censored blocks in total

Adversary controls contents of every block

But every transaction must be included within δ non-censored blocks

BoLD protocol: what changes?

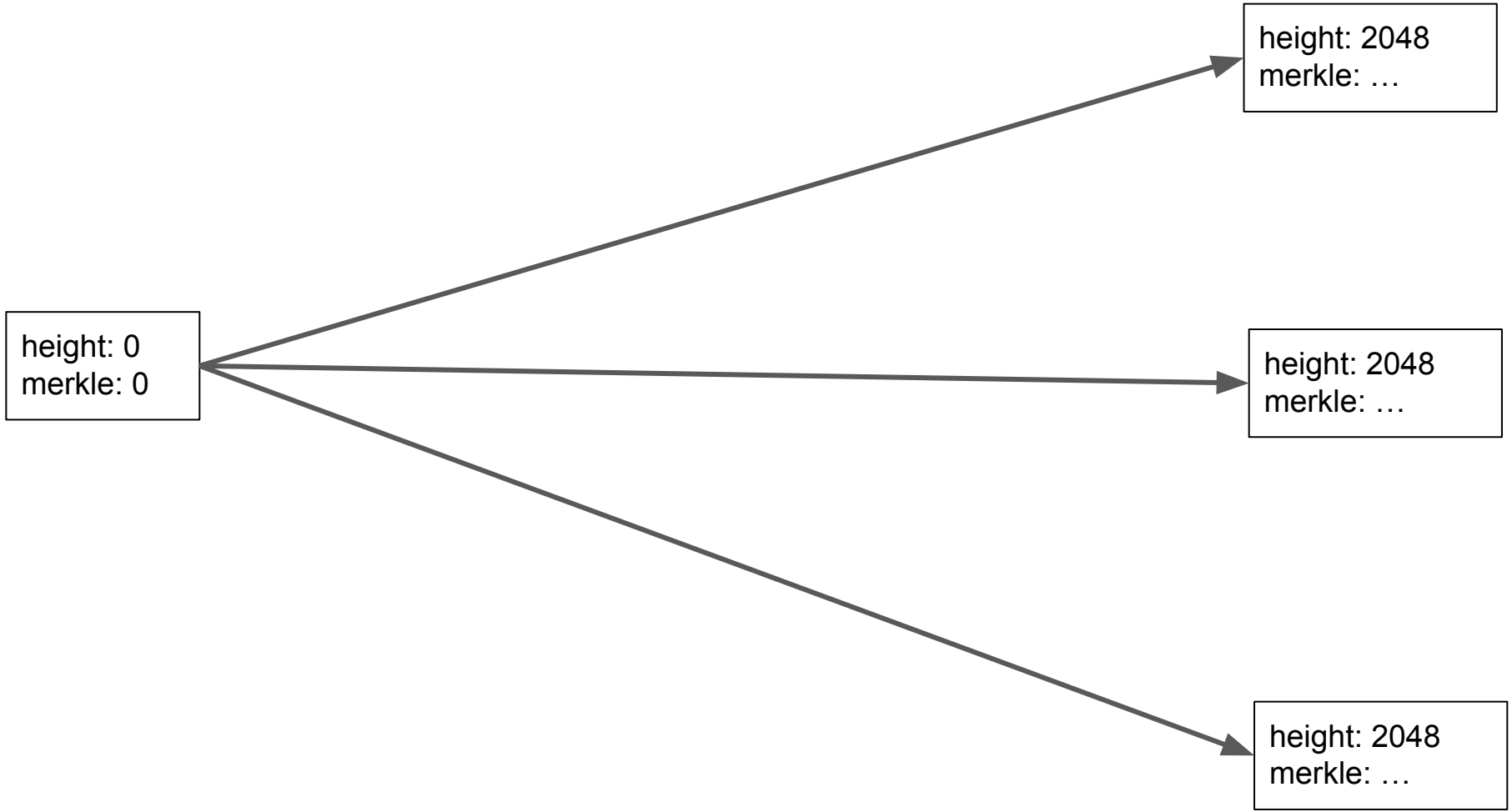
Old protocol	BoLD protocol
one-vs-one challenge	all-vs-all challenge
contestants: stakers	contestants: branches
identify a staker to slash/remove	identify a “winning” branch

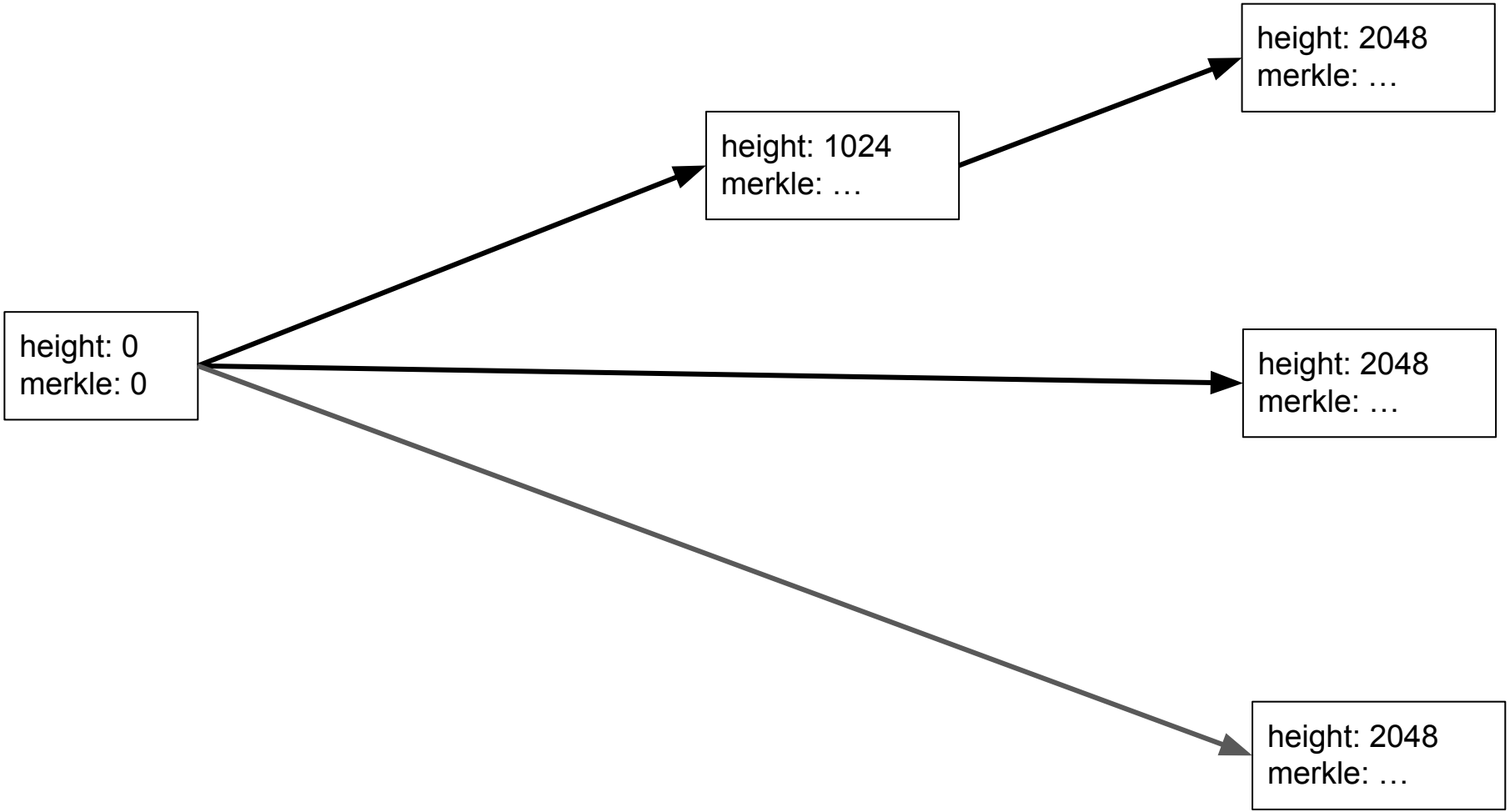
BoLD protocol: what changes?

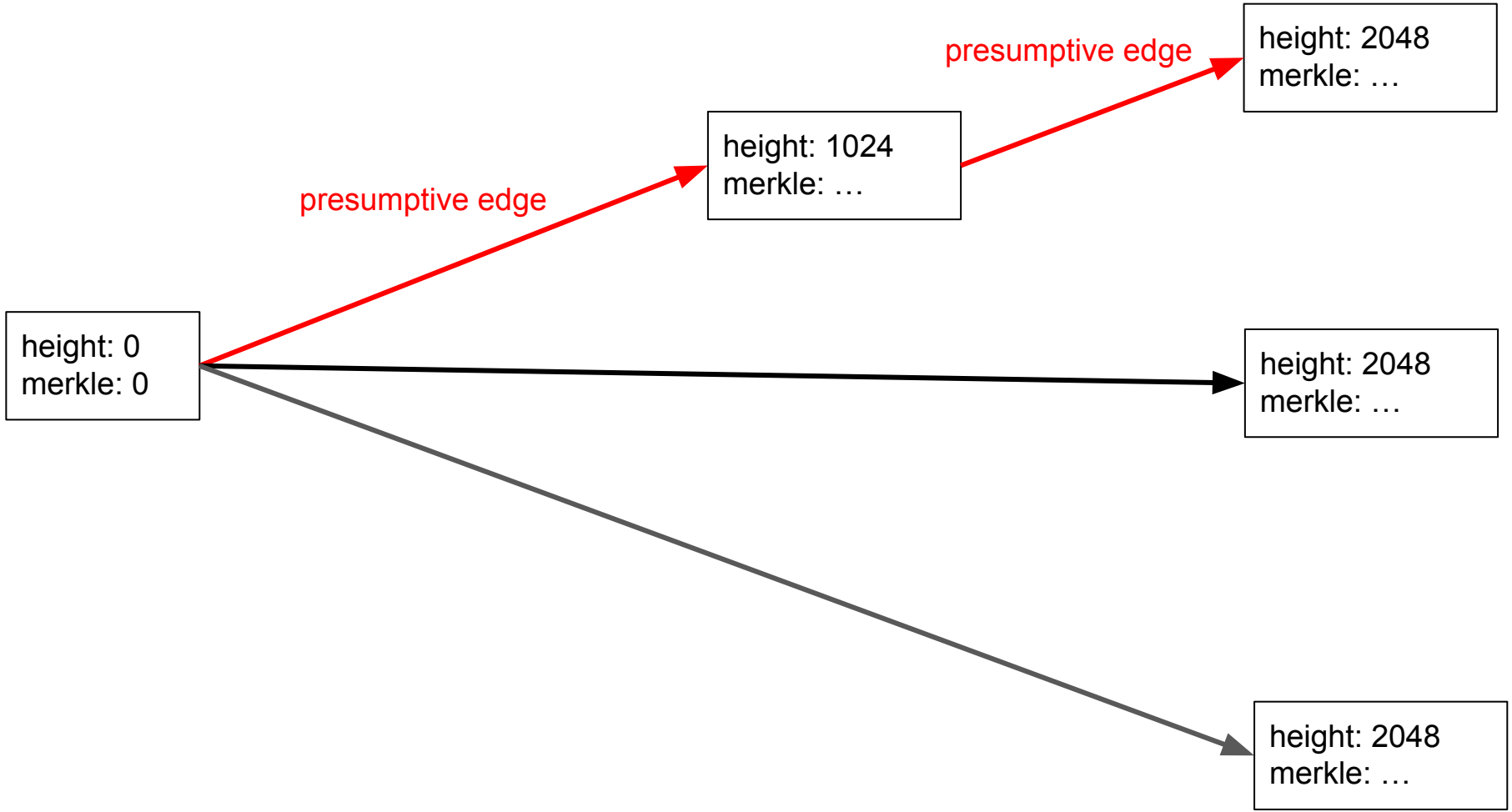
Old protocol	BoLD protocol
one-vs-one challenge	all-vs-all challenge
contestants: stakers	contestants: branches
identify a staker to slash/remove	identify a “winning” branch
each party stakes and fights separately	one party stakes honestly; all honest parties fight as a single decentralized team

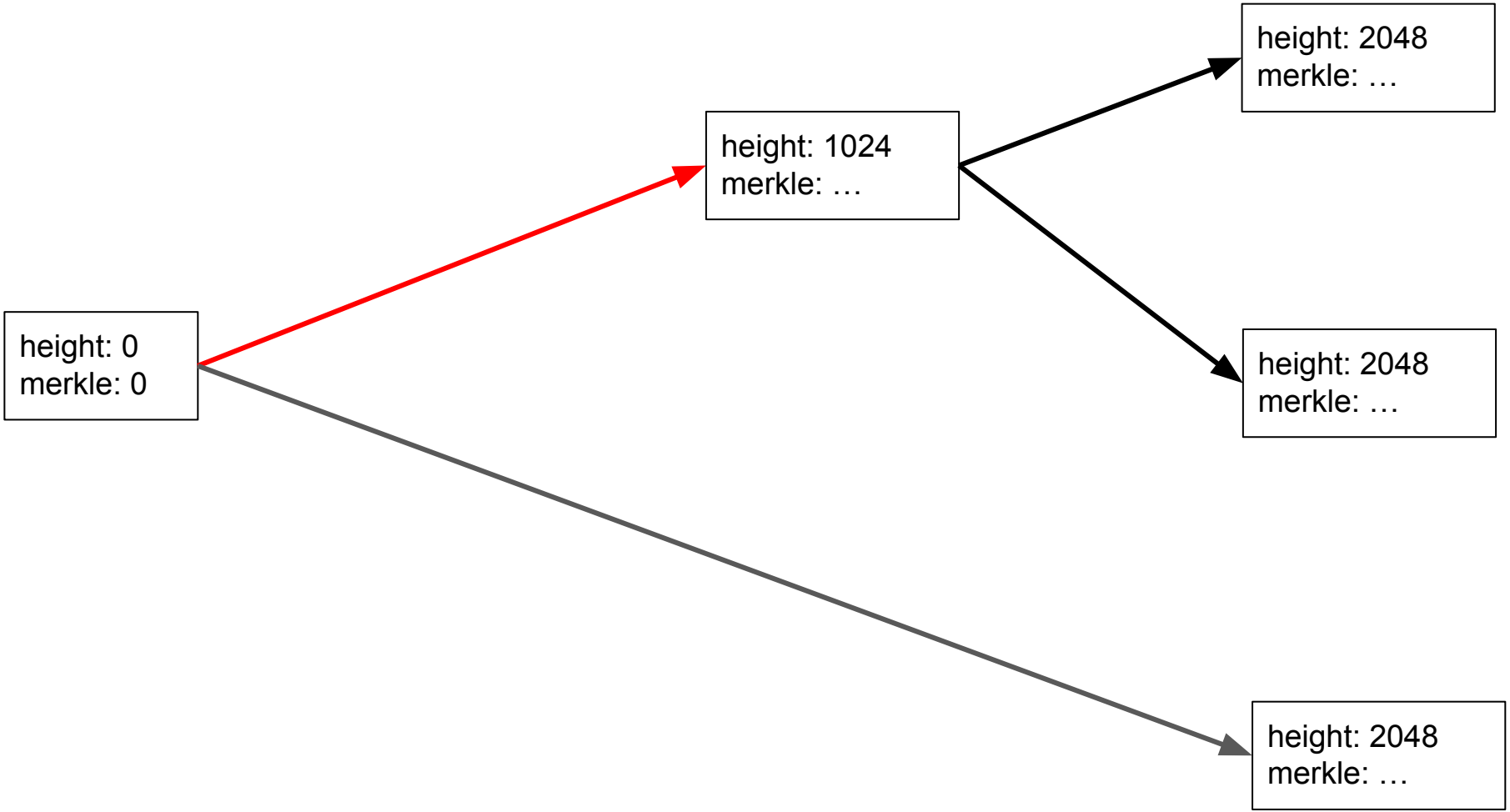
BoLD protocol: what changes?

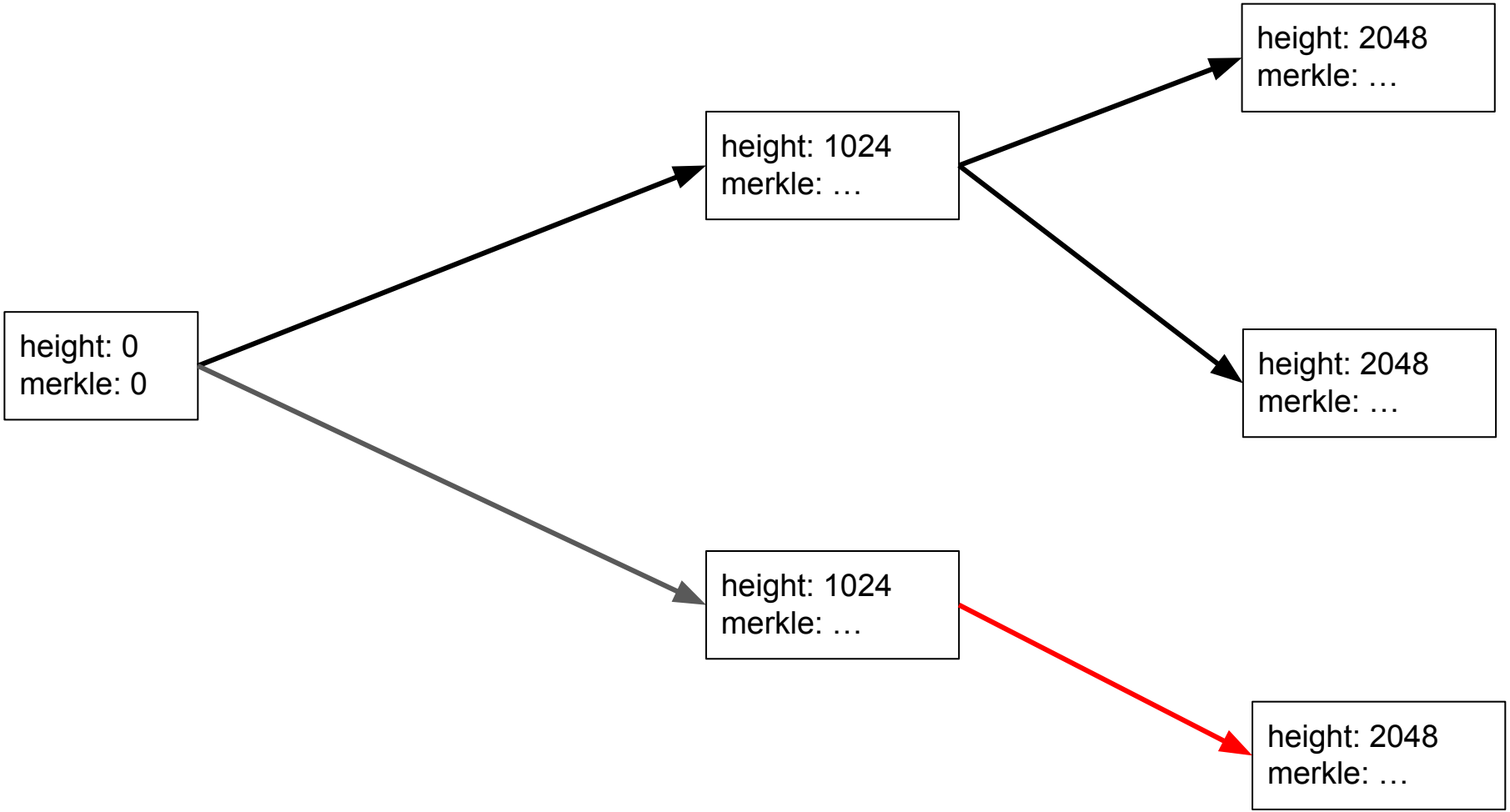
Old protocol	BoLD protocol
one-vs-one challenge	all-vs-all challenge
contestants: stakers	contestants: branches
identify a staker to slash/remove	identify a “winning” branch
each party stakes and fights separately	one party stakes honestly; all honest parties fight as a single decentralized team
adversary can cause N weeks of delay by sacrificing N stakes	adversary can cause one week of delay
honest parties’ total cost proportional to number of honest parties participating	honest parties’ total cost proportional to number of stakes slashed, can reimburse all costs

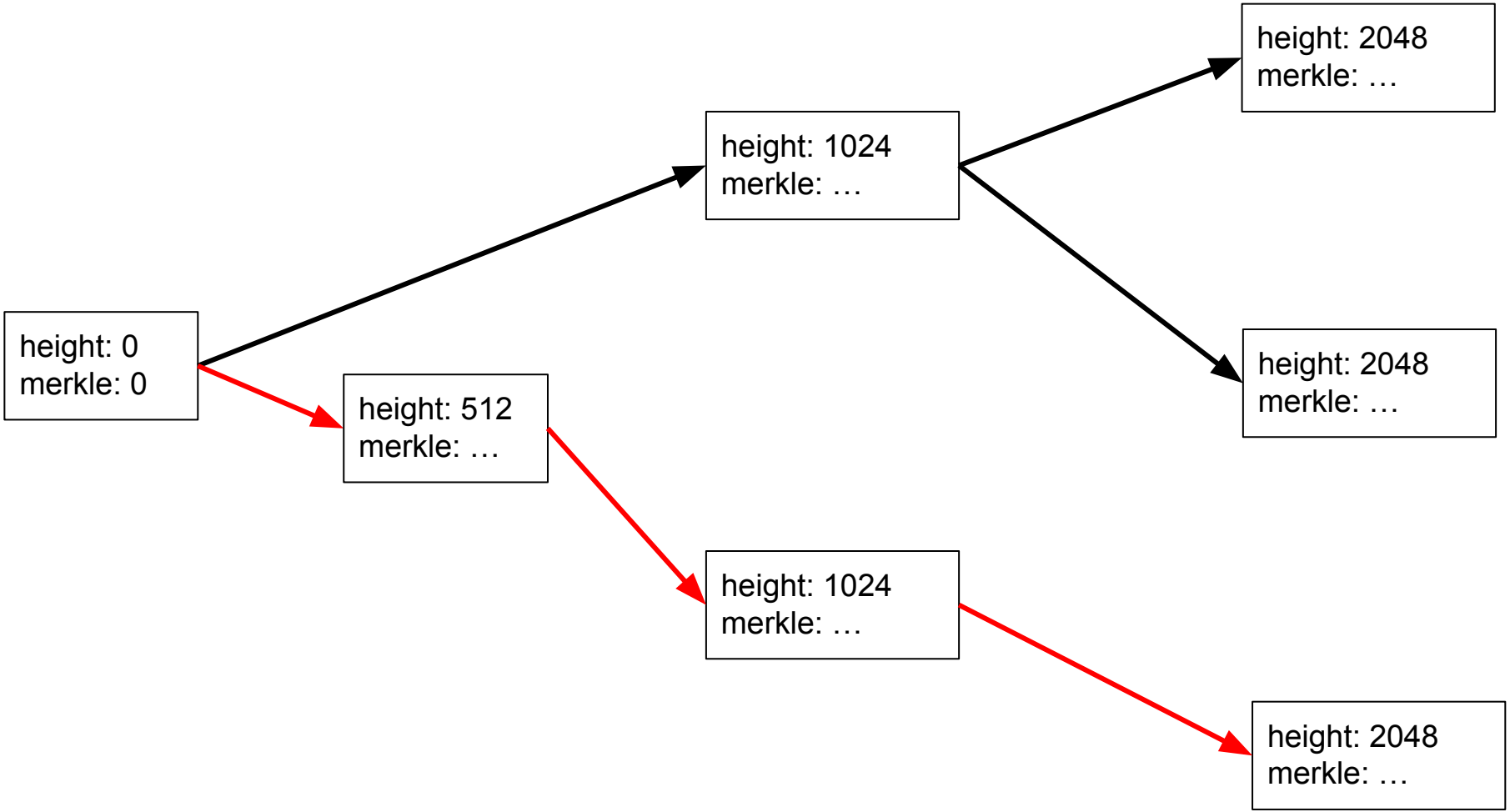

height: 0
merkle: 0
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …

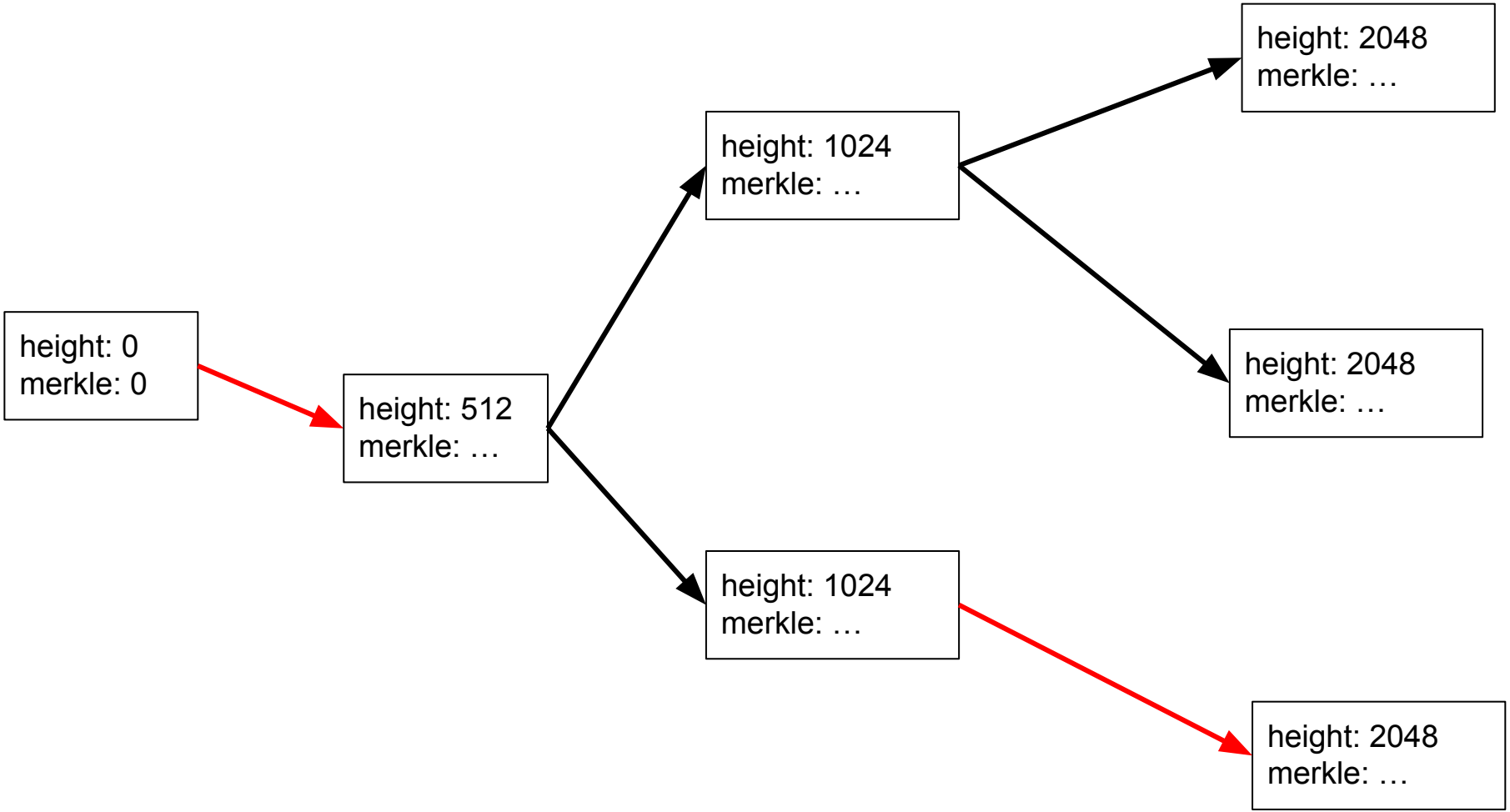

height: 0
merkle: 0
height: 1024
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …

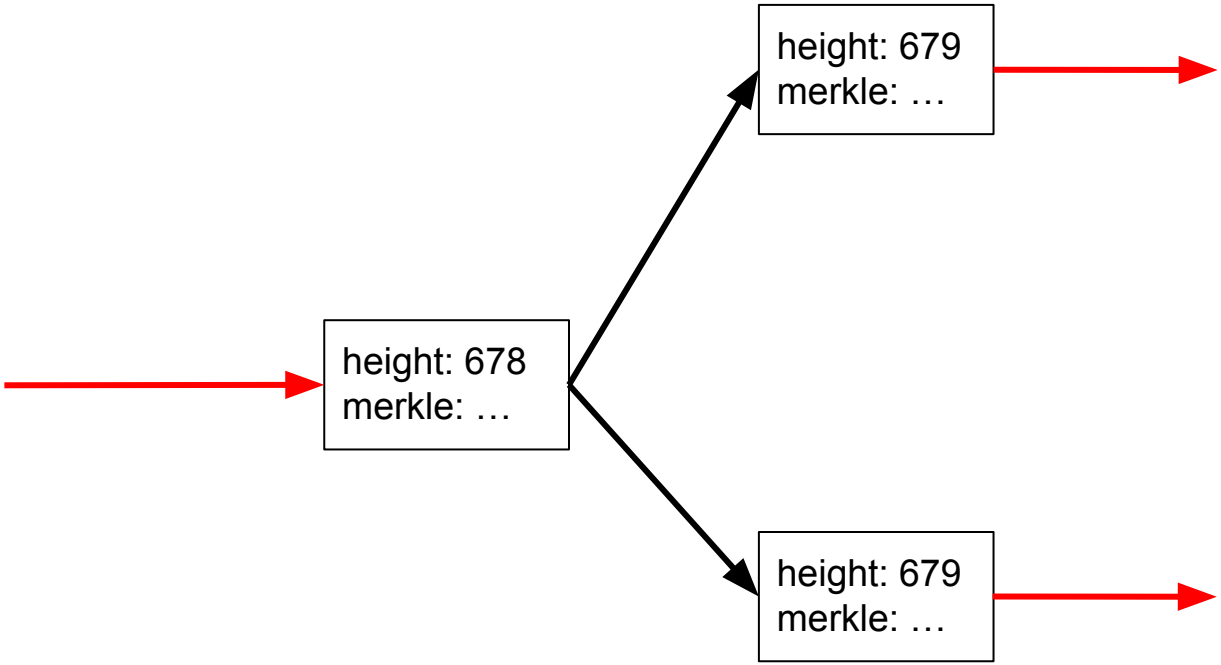

height: 0
merkle: 0
presumptive edge
height: 1024
merkle: …
presumptive edge
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …

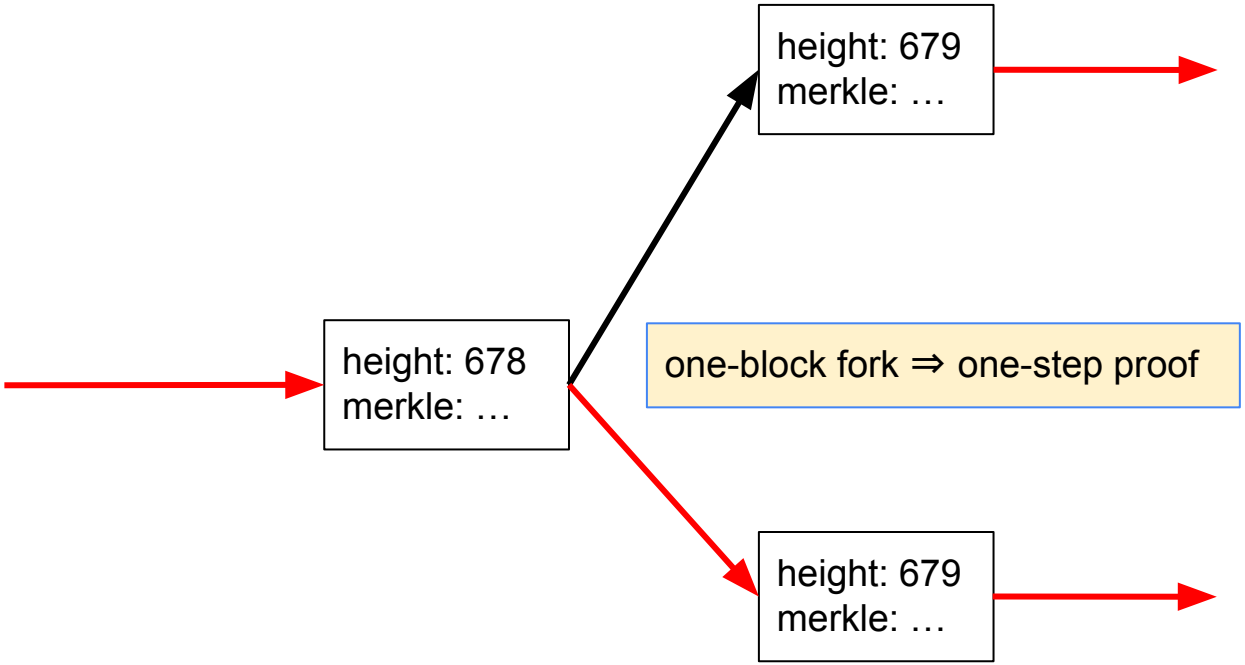

height: 0
merkle: 0
height: 1024
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …


height: 0
merkle: 0
height: 1024
merkle: …
height: 1024
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …


height: 0
merkle: 0
height: 512
merkle: …
height: 1024
merkle: …
height: 1024
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …


height: 0
merkle: 0
height: 512
merkle: …
height: 1024
merkle: …
height: 1024
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …
height: 2048
merkle: …


height: 679
merkle: …
height: 678
merkle: …
height: 679
merkle: …


height: 679
merkle: …
height: 678
merkle: …
one-block fork ⇒ one-step proof
height: 679
merkle: …

Timers

Edge timer: measures how long the edge has been presumptive.

Bottom-up aggregate timer:

edge timer, plus max of aggregate timer over edge’s bisection-children

or infinite, if edge has been one-step proven

Can confirm a top-level edge if its bottom-up timer is at least C+[lower order term]

Honest strategy

1. Make an honest assertion if nobody has.
2. If a top-level edge can be confirmed, confirm it.
3. If an honest edge is not presumptive:
    a. If it is a one-step edge, one-step prove it.
    b. Otherwise, bisect it.

Honest strategy

1. Make an honest assertion if nobody has.
2. If a top-level edge can be confirmed, confirm it.
3. If an honest edge is not presumptive:
    a. If it is a one-step edge, one-step prove it.
    b. Otherwise, bisect it.

Safety Theorem:
If anyone follows honest strategy, no dishonest top-level edge will be confirmed.

Honest strategy

1. Make an honest assertion if nobody has.
2. If a top-level edge can be confirmed, confirm it.
3. If an honest edge is not presumptive:
    a. If it is a one-step edge, one-step prove it.
    b. Otherwise, bisect it.

Safety Theorem:
If anyone follows honest strategy, no dishonest top-level edge will be confirmed.

Completion Theorem:
If anyone follows honest strategy, the protocol will complete
(by confirming an honest top-level edge) within time 2C+[lower order term].

Economic security

- “Delay attack” sacrifices stake(s) to cause delay confirmation.
  - does NOT delay finality, only delays confirmation to the L1 chain

- Must impose a threshold cost on adversary in all delay scenarios.

⇒ don’t give loser’s stake to winner – that incents self-challenges

⇒ one honest staker must stake the threshold amount

Multi-level BoLD

- In practice, might need ~56 levels of bisection.
- Can’t afford to compute the full Merkle tree (2^{56} leaves)

Multi-level BoLD:

- Bisect over blocks in the assertion
- If there’s a one-block dispute, use BoLD recursively to resolve it
    - Recursive bisection is over instructions in the block-building code

Summary: Guarantees

Safety: If any party is following the honest strategy,
no false assertion is confirmed.

Completion: If any party is following the honest strategy,
a (true) assertion is confirmed within 2C+[lower order term]
from the time that the first of the rival assertions was posted.

Economic security: If there's a challenge, malicious posters lose at least one stake.

Status and path forward

Code, paper, and security audit released

- Paper to appear at AFT

Testnet live since April 15

Heading toward DAO vote for adoption on Arbitrum One and Nova

Thanks to teammates!

Mario Alvarez

Pranay Anchuri

Ben Berger

Chris Buckland

Yafah Edelman

Raul Jordan

Mahimna Kelkar

Harry Ng

Victor Shoup

Terence Tsao

Permissionless Optimistic Validation with BoLD

Ed Felten

Co-founder and Chief Scientist

OFFCHAIN LABS