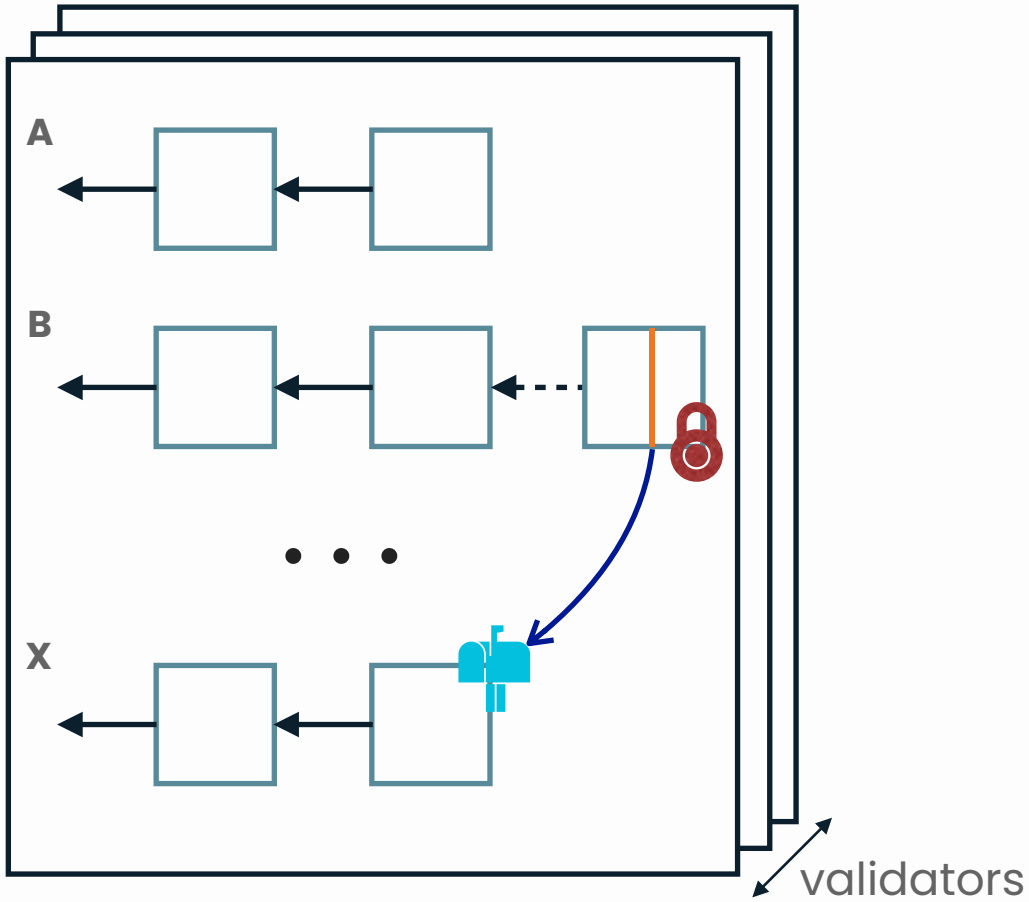
A Low-Latency Blockchain Without a Mempool

Mathieu Baudet

mathieu.baudet@linera.io

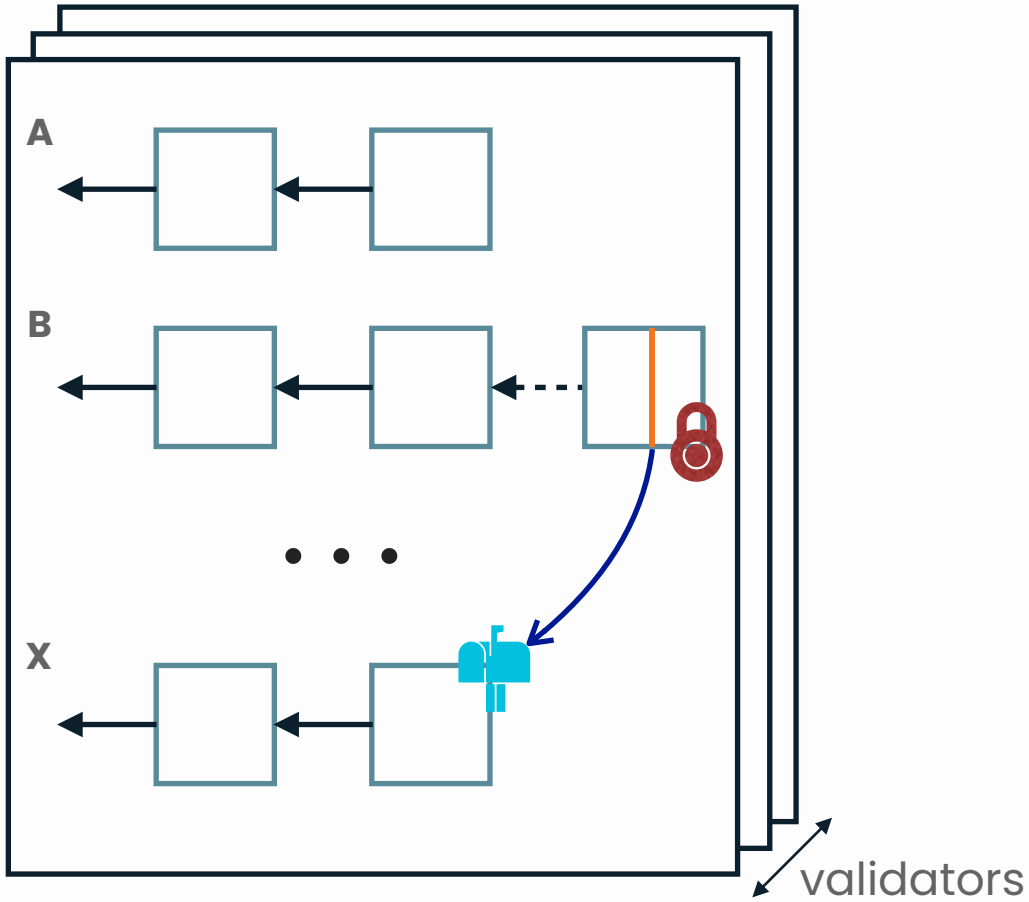
Science of Blockchain Conference 2022

The Linera Protocol (preview)



A new decentralized, multi-chain protocol targeting **low-latency** and **high-throughput** applications.

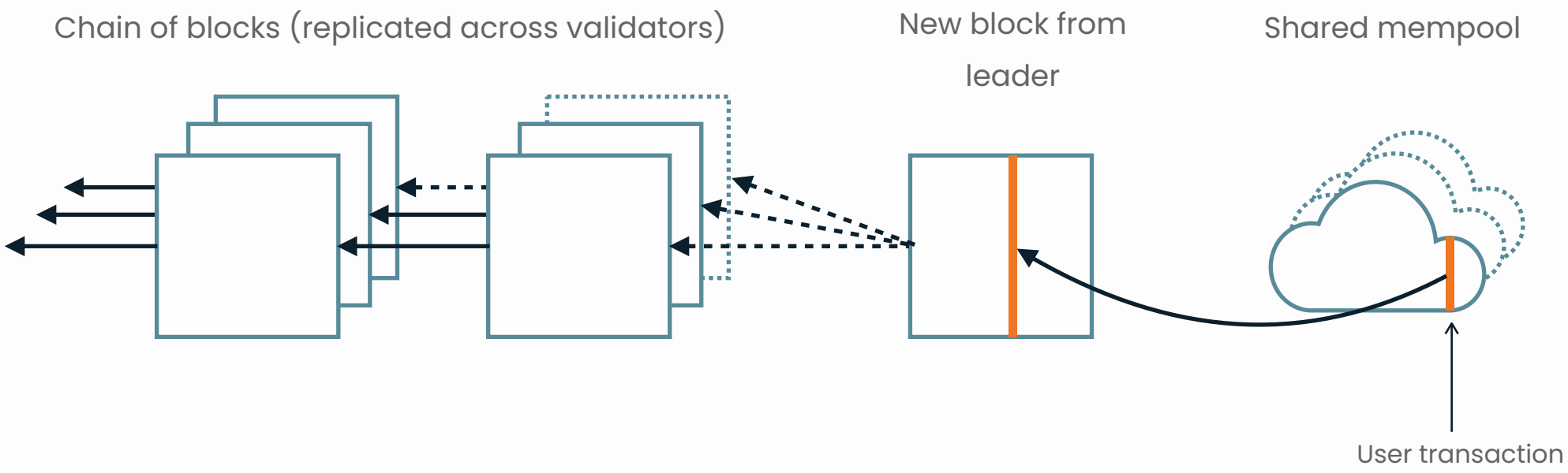
The Linera Protocol (preview)



A new decentralized, multi-chain protocol targeting **low-latency** and **high throughput** applications:

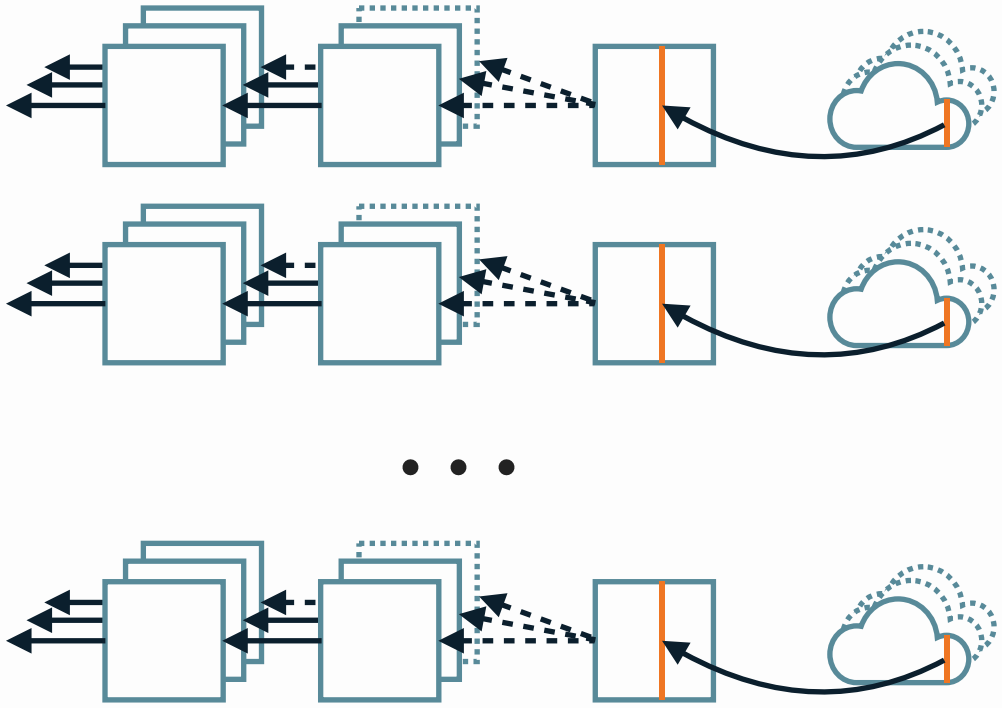
1. Each validator is a web service with all the chains
2. Users are encouraged to operate their own chains (no mempool)

Scalability in a Classical Blockchain

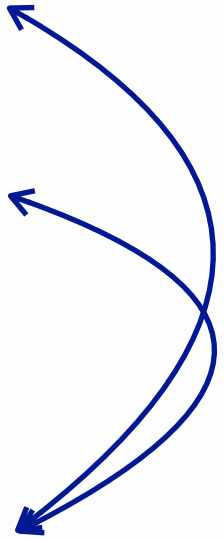


Transaction rate ⩽ single-chain execution rate 😟

Blockchain Sharding



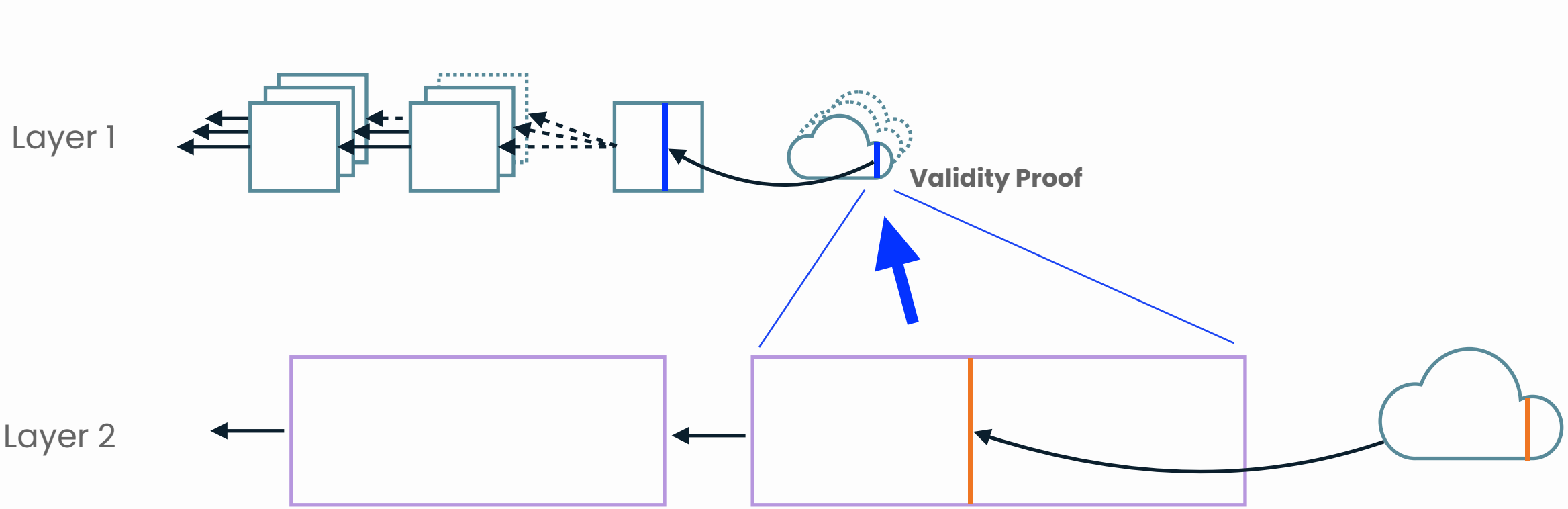
Every shard has its own set of validators



Cross-chain communication overhead

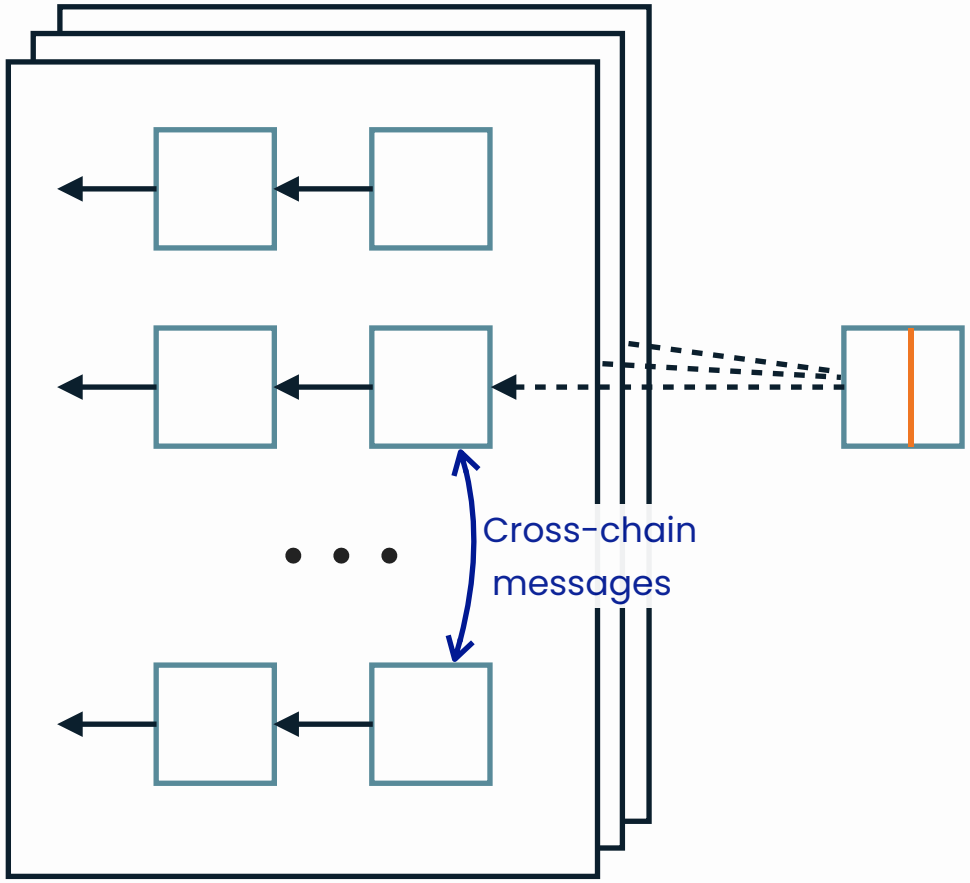
😟

Validity ("ZK") Rollups



Lower L1-gas cost per L2 transaction ⟹ larger L2 blocks ⟹ higher latency 😟

Sharded Validators



Every validator runs every shard

Motivation:

- Efficient cross-chain messages
- web2-like scaling
- Quick block finality

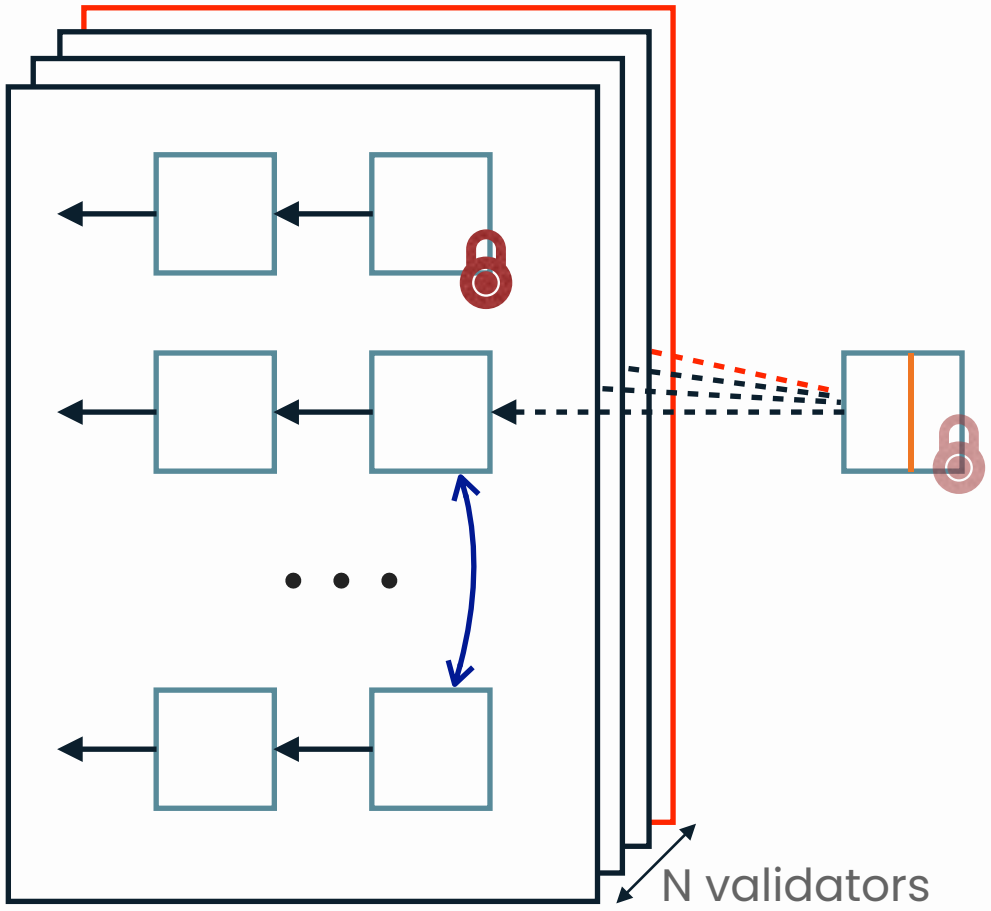
😀

1. Overview of the protocol

2.Cross-chain communication

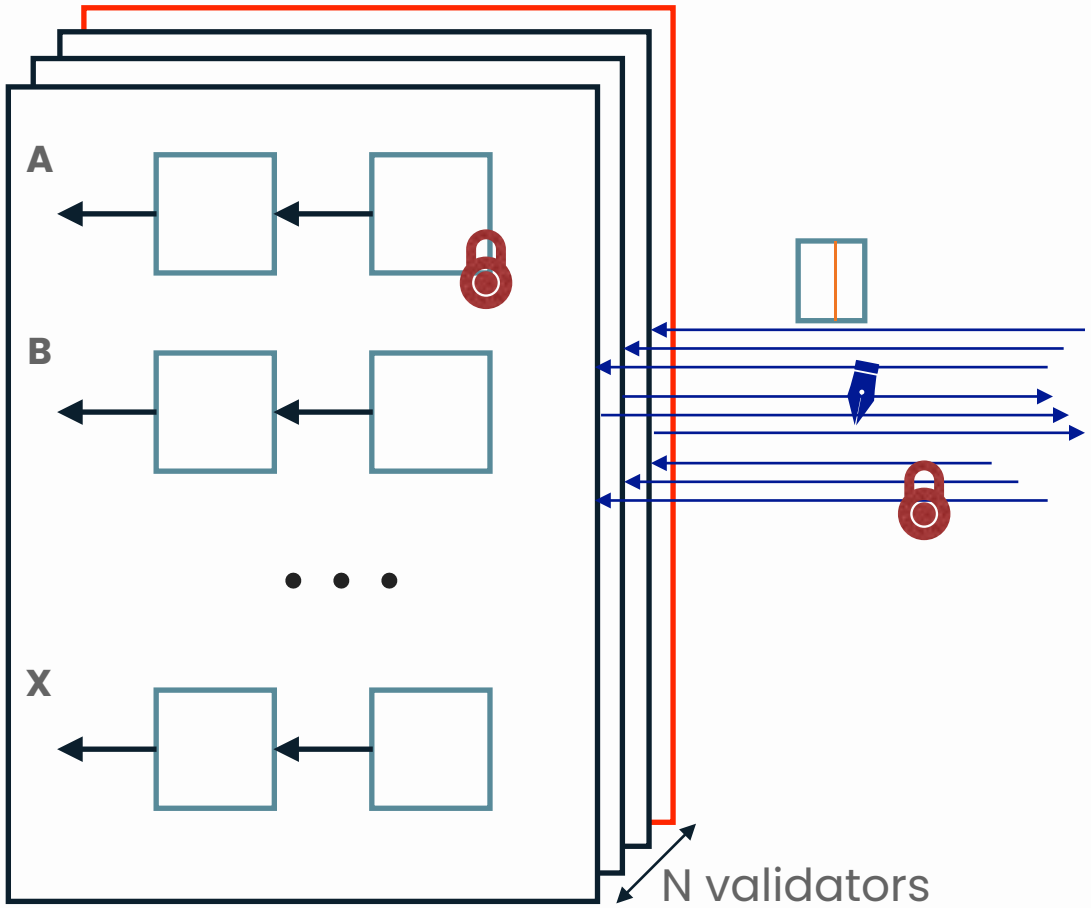
3.Examples of applications

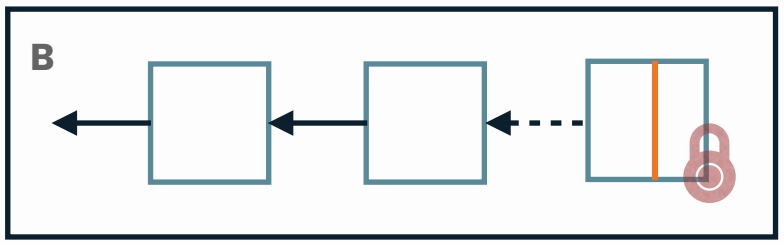
Security Model (BFT + partial synchrony)



- N = 3f + 1 validators
- At most f malicious
- 2f+1 validators may certify a block as final
- Safety doesn't depend on network delays

Client-Validators Interactions





Leader's client

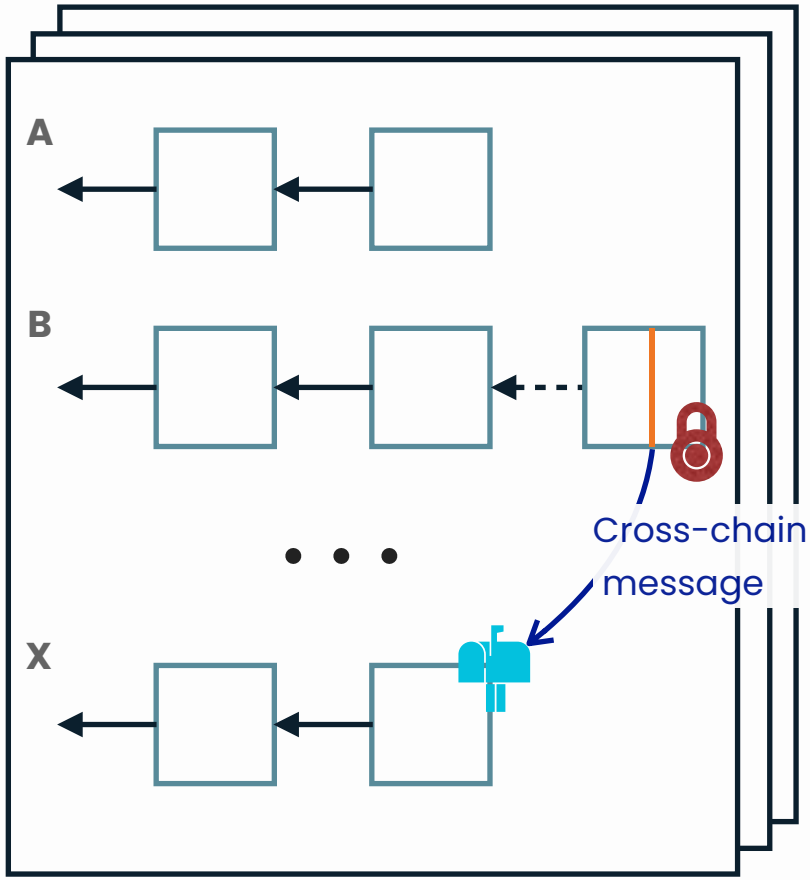
- Blocks proposed by chain leaders.
- Validators sign off if valid
- Only client-to-validator communication

1. Overview of the protocol

2.Cross-chain communication

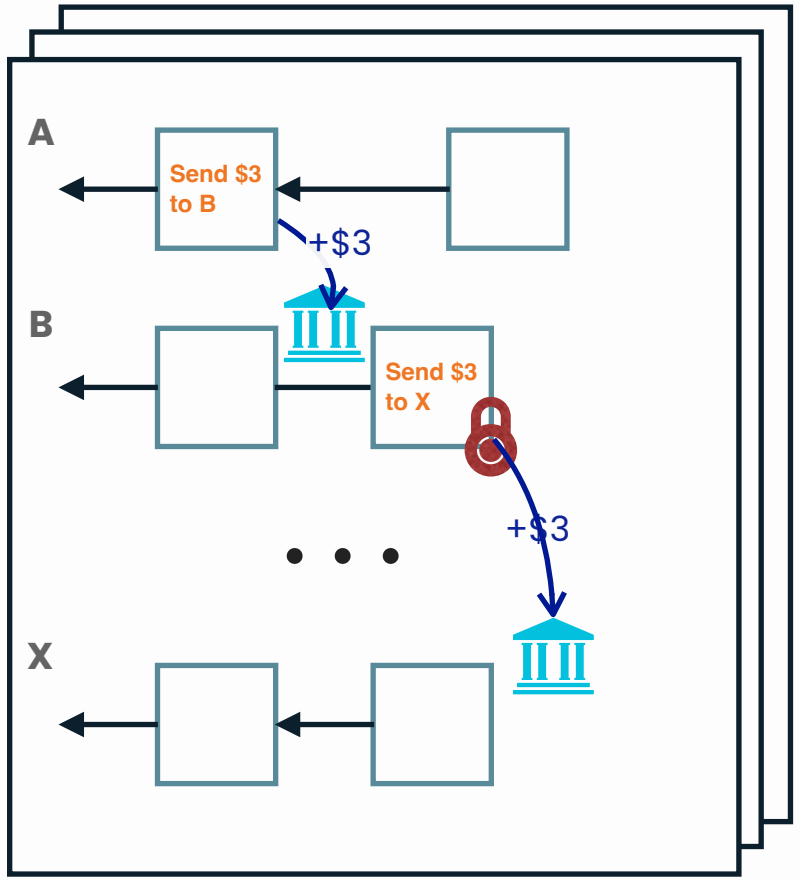
3.Examples of applications

Cross-Chain Messages



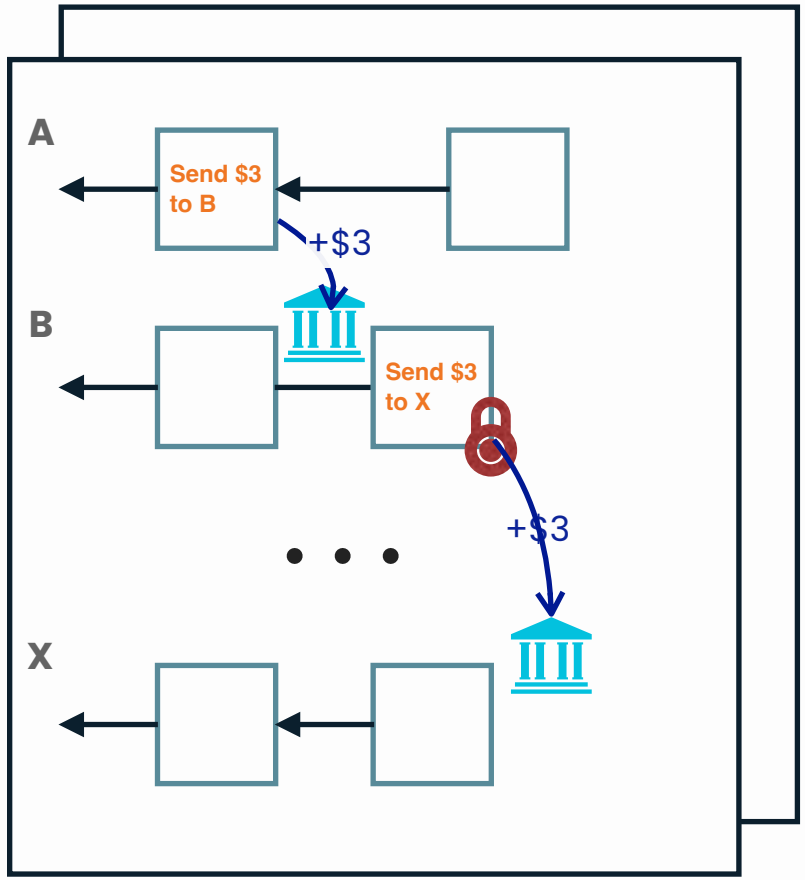
- When executed, certified blocks produce asynchronous messages for other chains.
- Messages are delivered exactly once per validator.
- Validators may schedule messages differently.

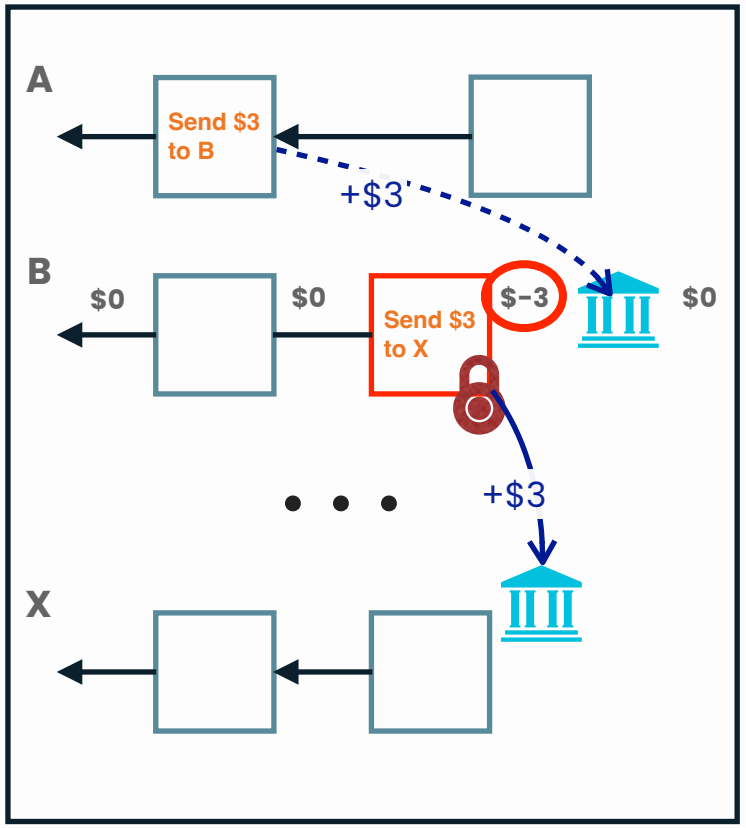
Direct Payments [FastPay, AFT'20]



- Each validator maintain a **balance** for every chain (aka "user account" in FastPay)
- **[Balance-check]** A validator only signs for a proposed block if the resulting balance is non-negative.

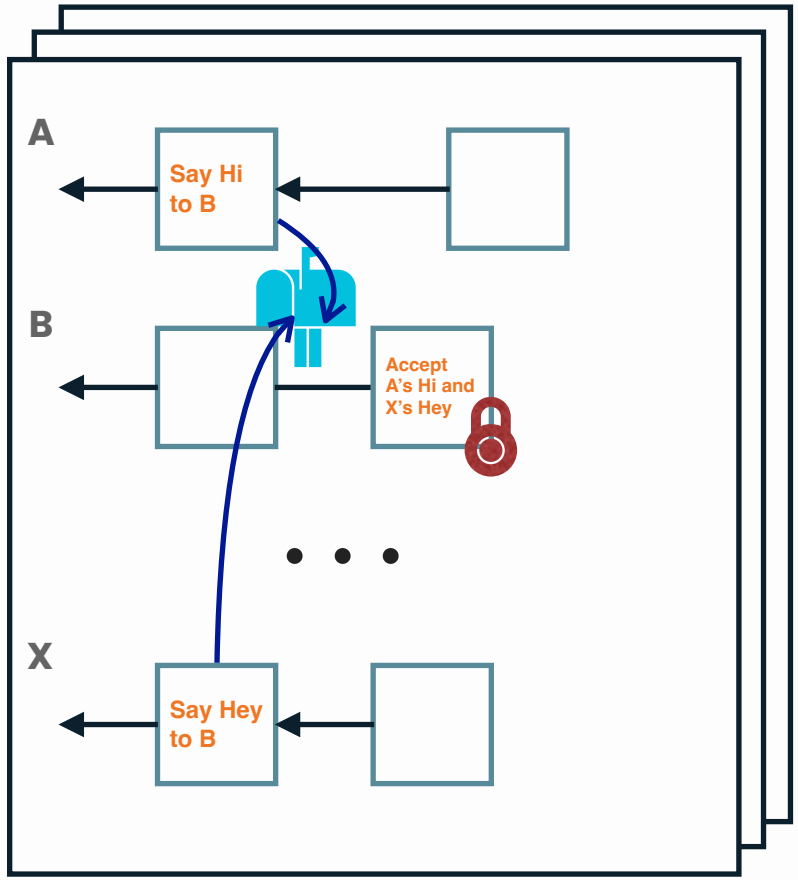
Consistency For Direct Payments





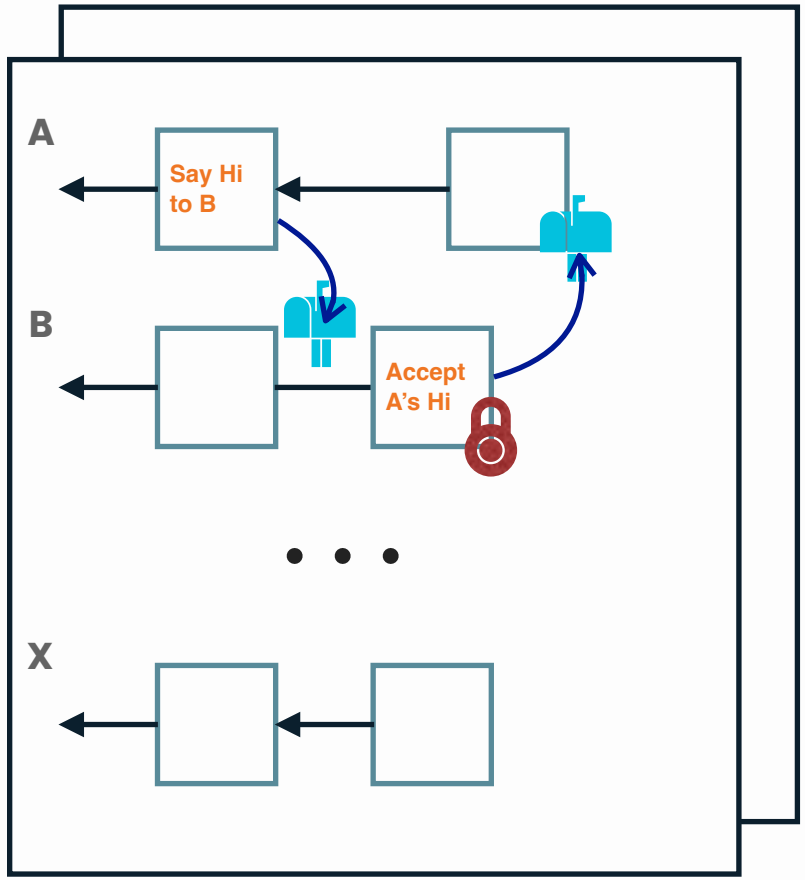
Validators who didn't sign a certified block may temporarily go negative.

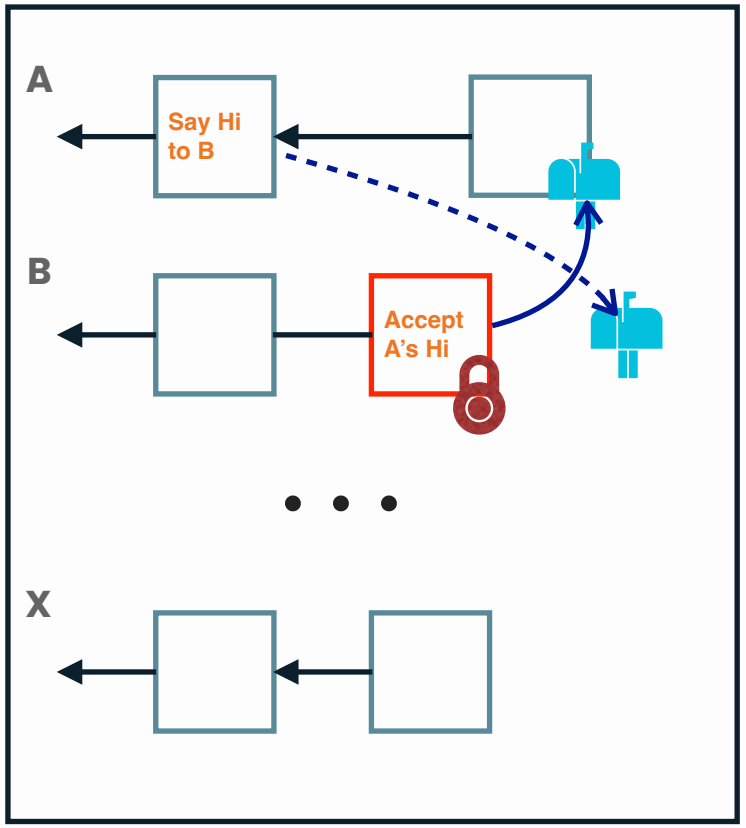
Arbitrary Messages — Intuition



- Messages go to an inbox
- Each block declares ("accepts") an ordered list of received messages to execute.

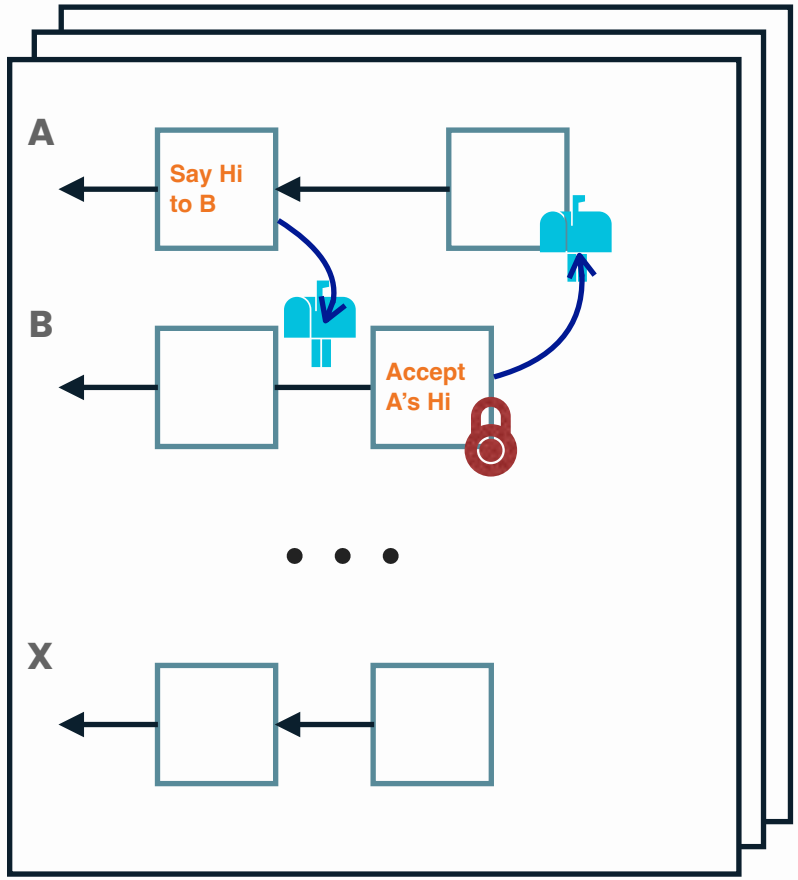
Consistency For Arbitrary Messages





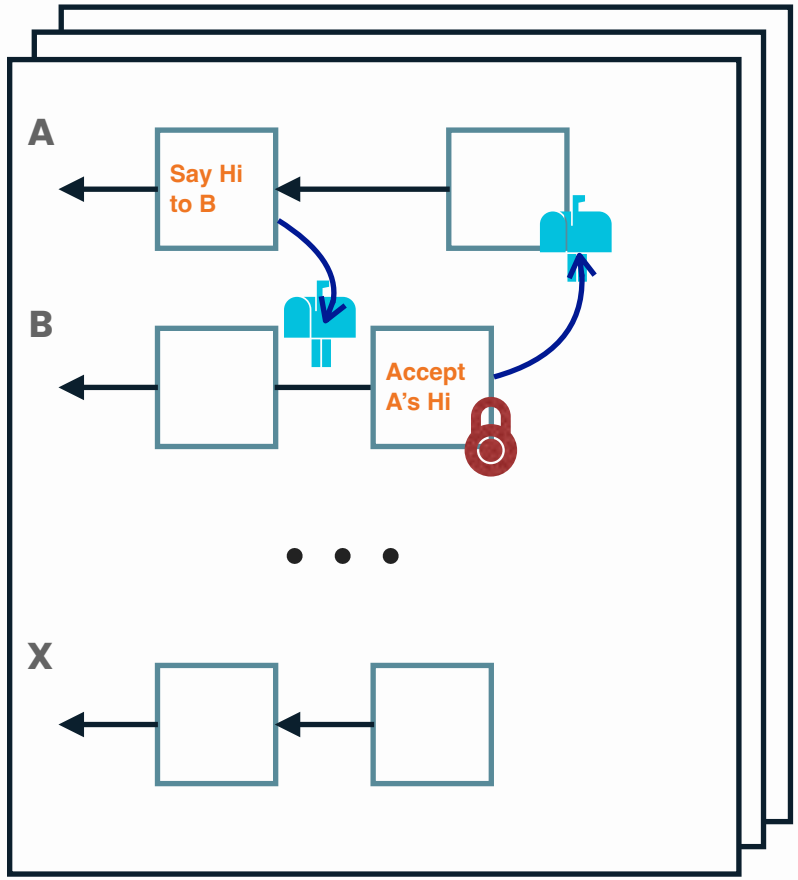
Validators who didn't sign a certified block may execute incoming messages by anticipation.

Arbitrary Messages — Block Validation



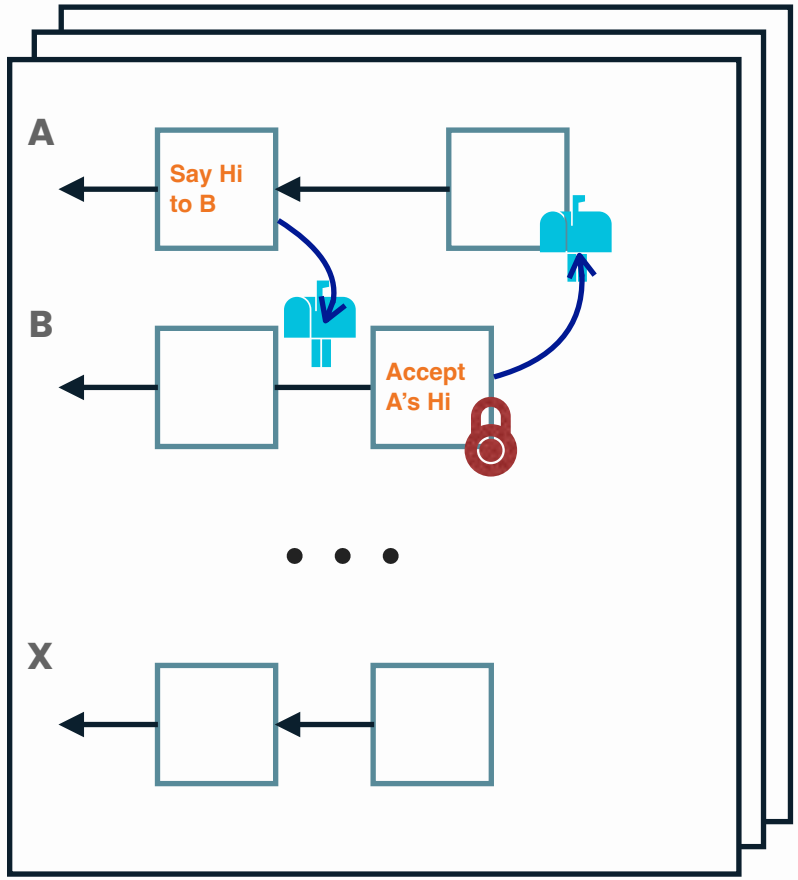
- Every chain has an inbox containing:
  - received messages waiting to be executed
  - messages executed by anticipation
- A validator only signs for a new block if the resulting state has no anticipated messages.

Analysis: Eventual Consistency



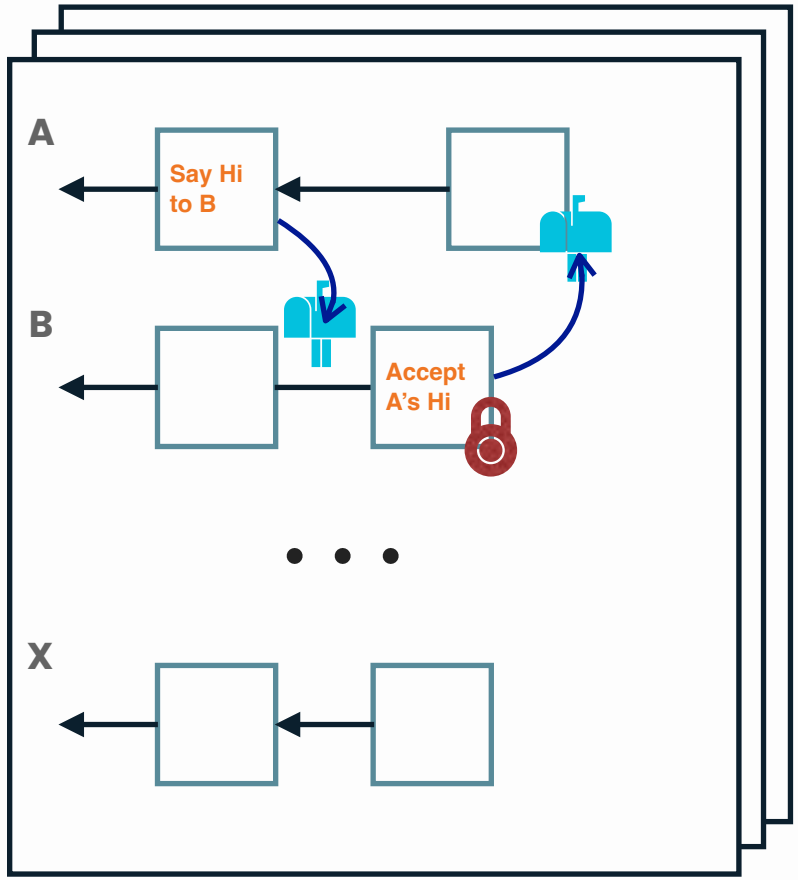
Eventual Consistency : If two (honest) validators have the same heights for every chain and don't accept new blocks, eventually all their inboxes (resp. FastPay balances) are in the same state.

Analysis: Safety



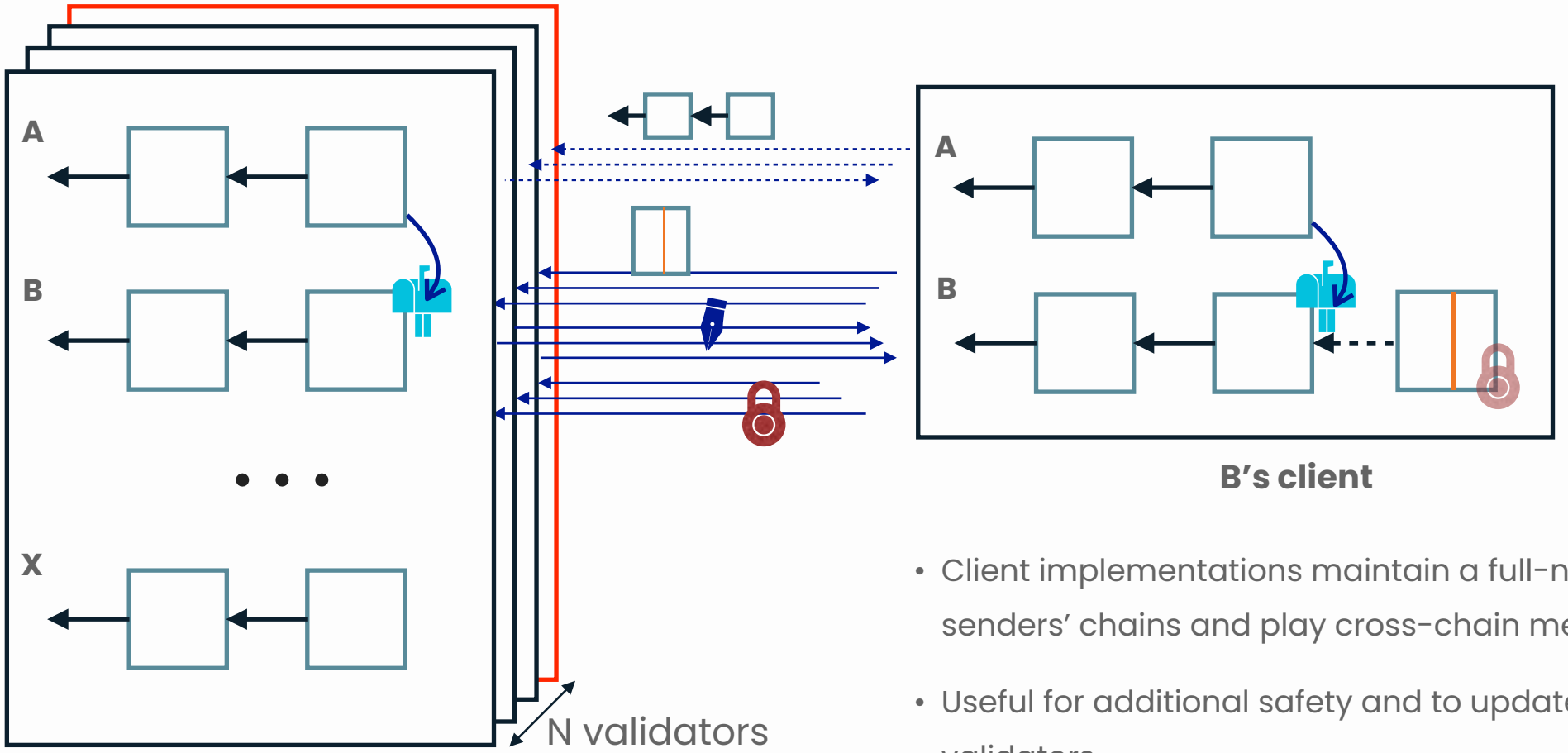
Safety : If an honest validator has signed off for a block at height H for a chain A, then every other validator with equal or longer chains will eventually clear all its anticipated messages for chain A up to height H (resp. have positive FastPay balance at height H).

Analysis: Availability



Availability: when a chain A has executed messages by anticipation, a client can figure out which other chains are too short, then download and forward the missing blocks to unlock A.

Client-Validators Interactions (with Messages)



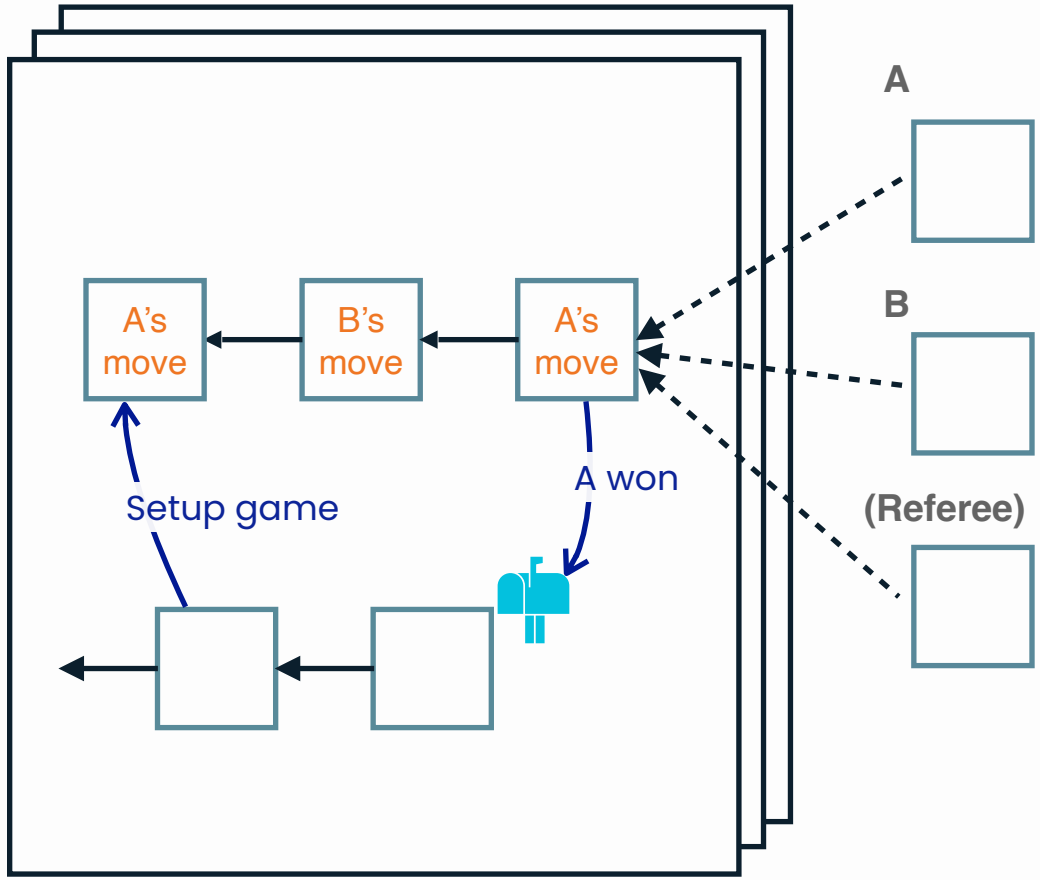
- Client implementations maintain a full-node for senders' chains and play cross-chain messages locally.
- Useful for additional safety and to update lagging validators.

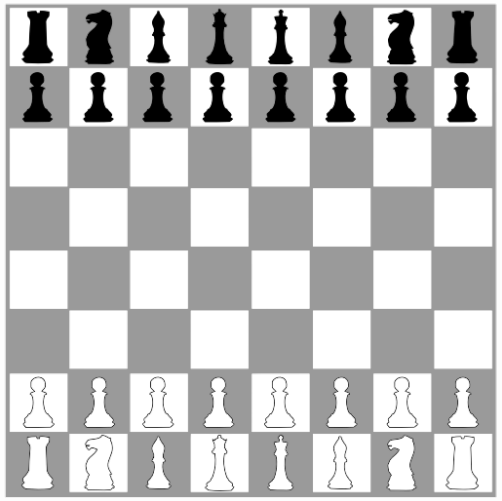
1. Overview of the protocol

2.Cross-chain communication

3.Examples of applications

On-Chain Multi-Player Games at Scale

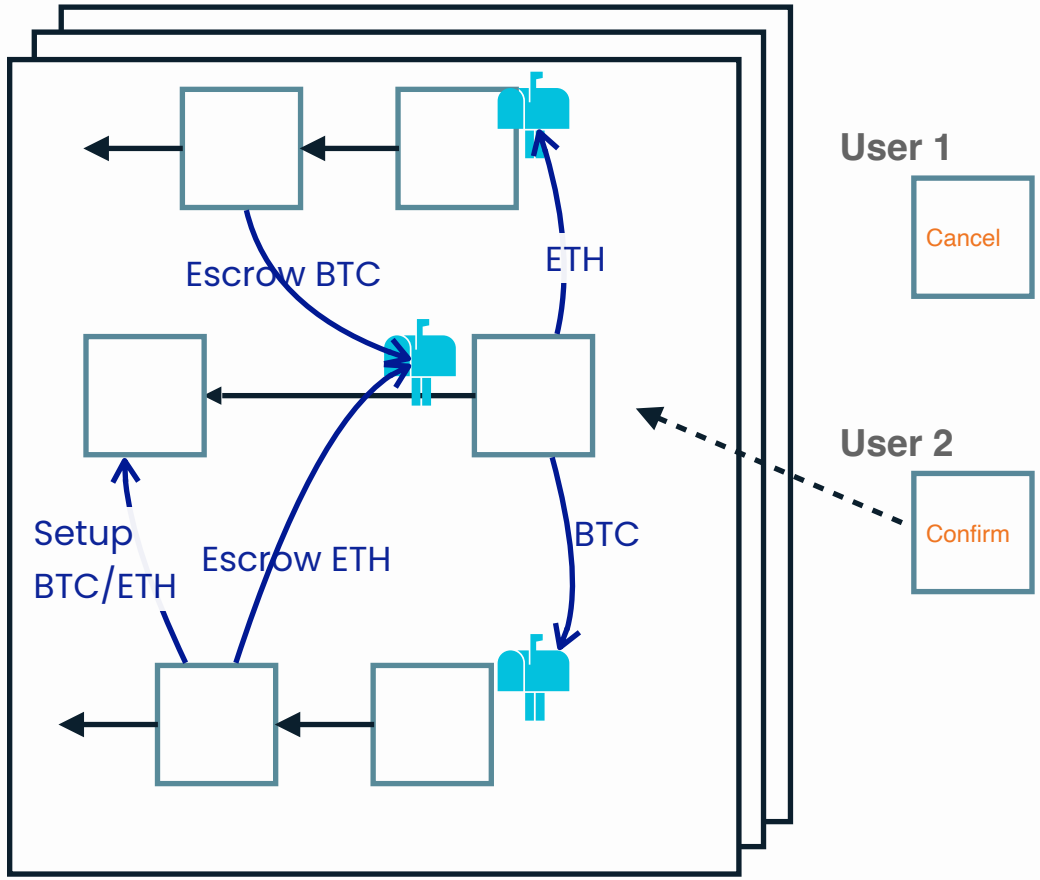




Idea: The state of the temporary chain informs consensus about the expected player

→ Can avoid a full consensus protocol if a referee is trusted to end the game when one player has timed out

Atomic Swaps at Scale

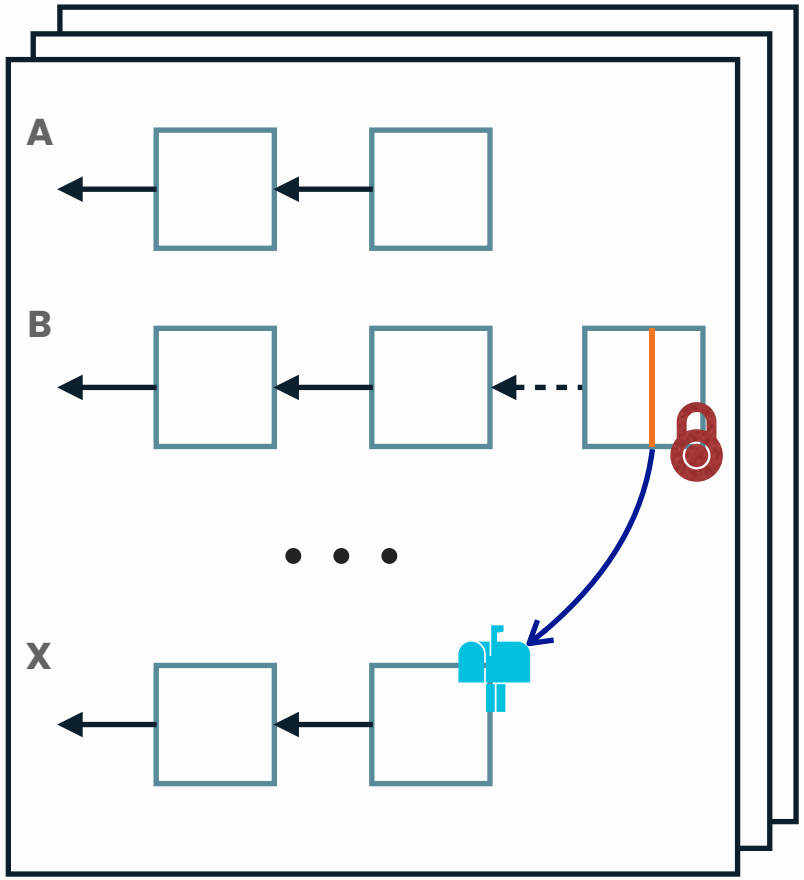


Idea:

- Initiator first sets up a temporary chain (with precise swap parameters)
- The state of the temporary chain informs consensus about the escrowed assets
- "Confirm" requires both assets

→ Can avoid a full consensus protocol if escrow is required to propose a block

Conclusion



- A new kind of **decentralized** protocol where validators are internally sharded → **elastic scaling**
- Easy to create user chains and customized temporary chains → **low latency**
- Generalized FastPay cross-chain messages → **programmable**

This is just the beginning…

We're hiring!

Thank you!

Linera

We’re hiring!

mathieu.baudet@linera.io