The Future of Light Clients

Noah Citron

Ethereum’s light client ecosystem

Ethereum L1 has multiple light clients!

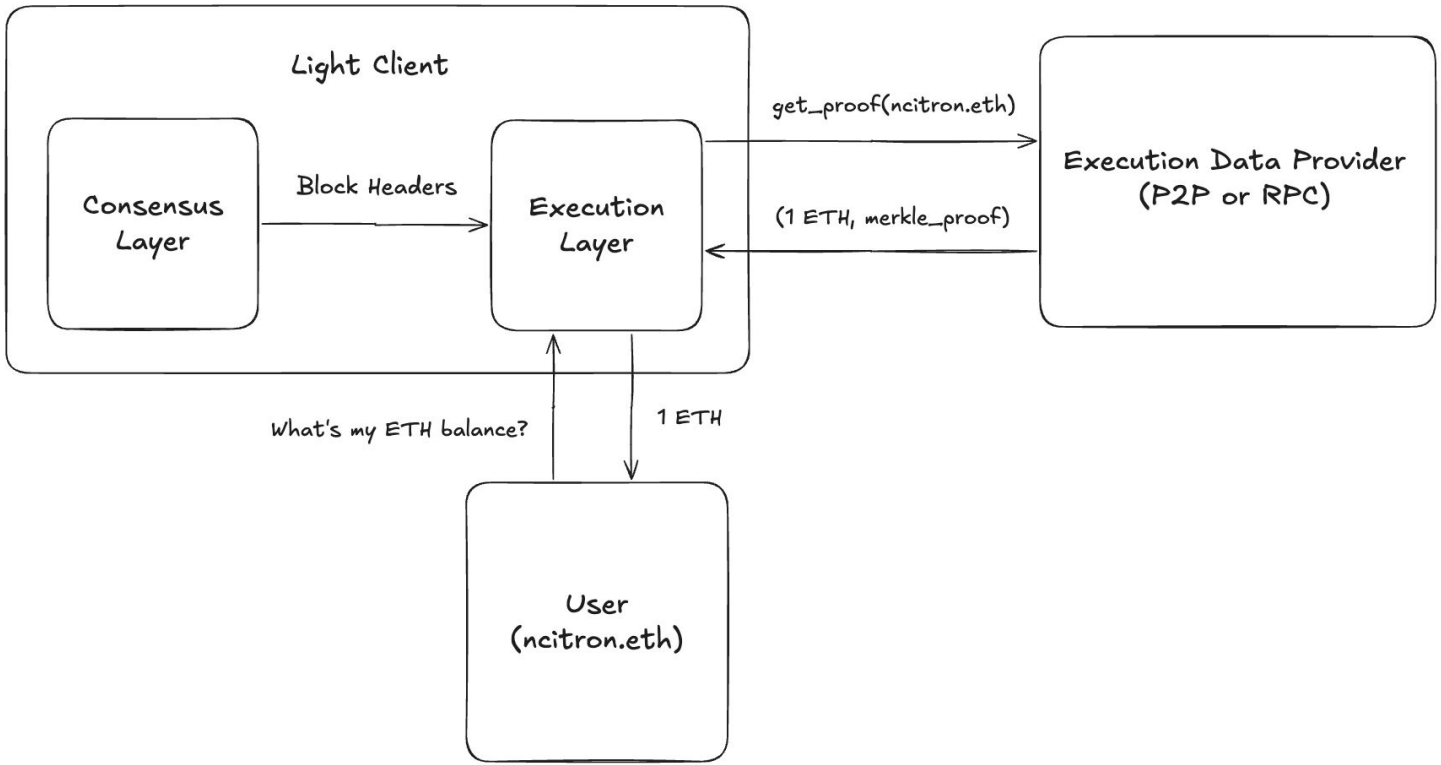
Ethereum’s L2 light client ecosystem

Users are moving to L2!

We have fewer options when it comes to L2 light clients…

We want to change that!

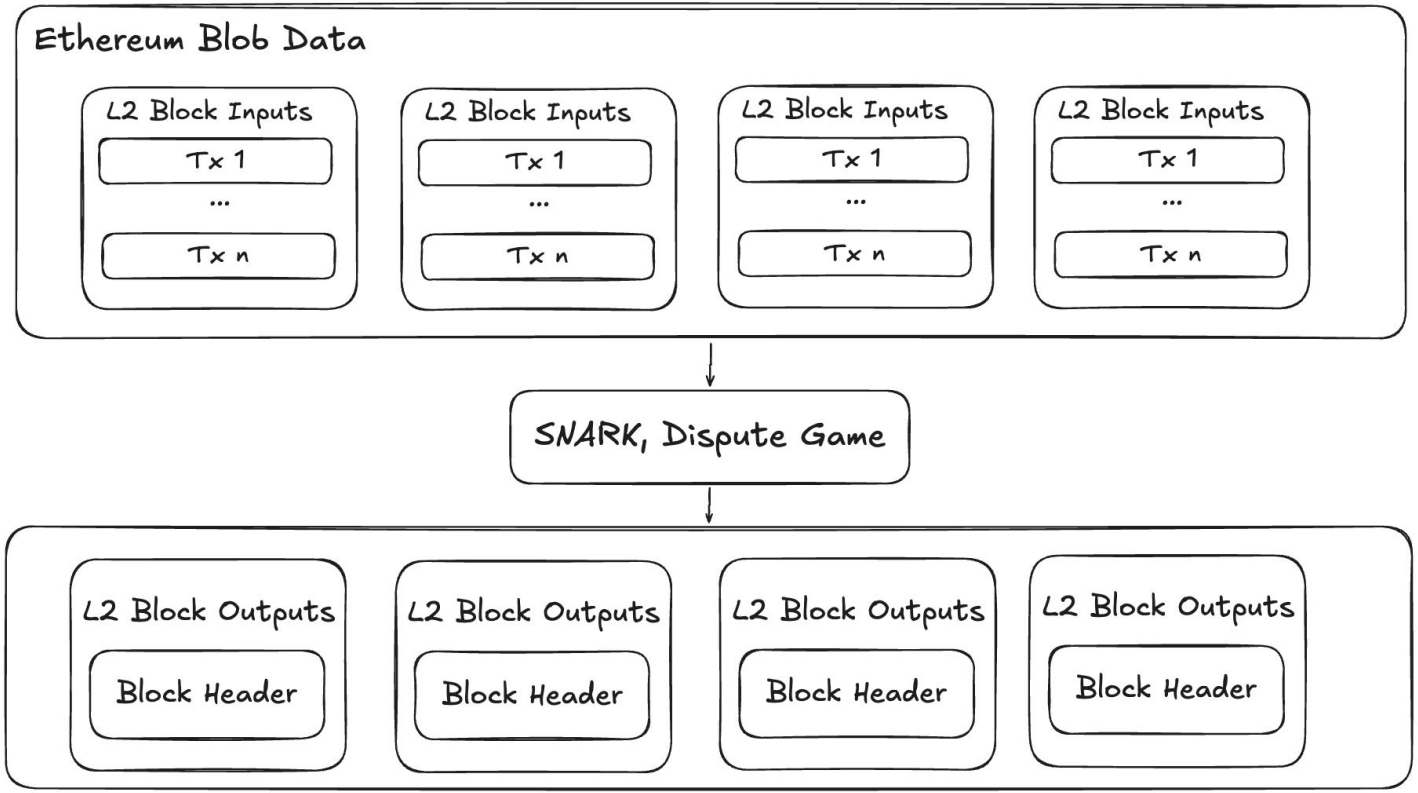
How light clients work



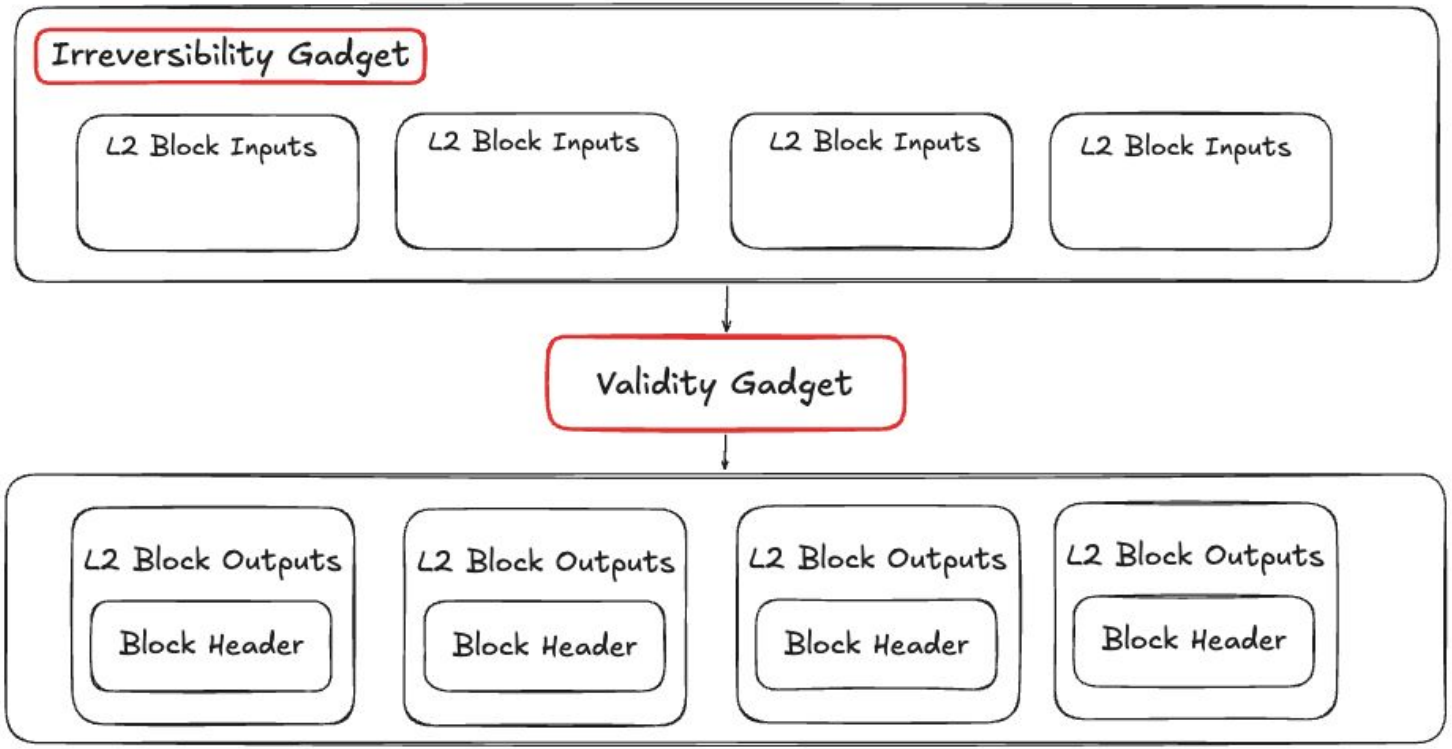
How to build the consensus layer

- Ethereum L1
  - Use the Altair light client sync protocol
  - Uses the trust of the Ethereum validators signing block headers
  - Implemented by light clients today
- L2
  - Validators can’t help us
  - Need a different mechanism to validate the block headers

A model of L2s



A generic model of L2s



The gadgets

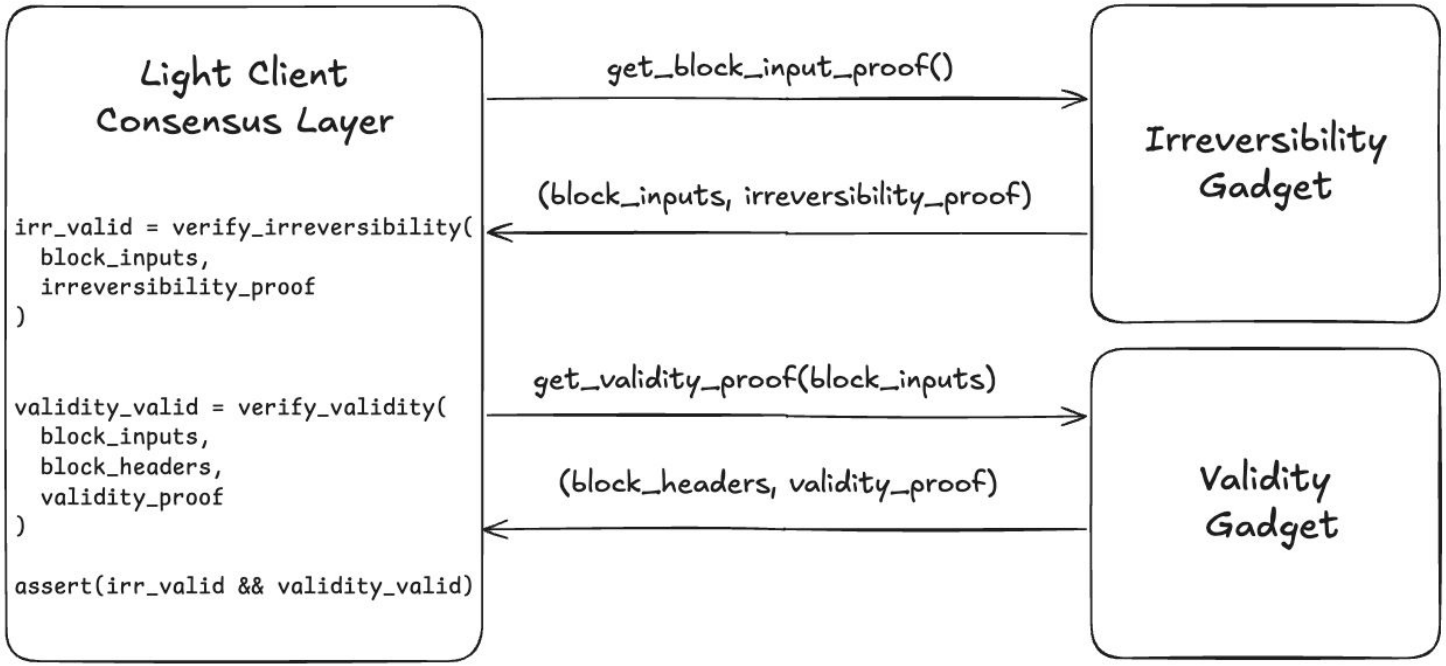
Irreversibility Gadget

- Convinces a verifier about what the L2 block input data is
- Example: block input data posted to L1 and we use the Altair sync protocol to fetch it

Validity Gadget

- Convinces a verifier about what the the L2 block output (header) is given an L2 block input
- Example: SNARKs implementing the rollup state transition function

Generic L2 light client



Generic L2 Light Client: Security

C_i = cost to break irreversibility gadget

C_v = cost to break validity gadget

C_{LC} = cost to break light client

$$C_{LC} = \min(C_i , C_v)$$

A first attempt at instantiating the light client

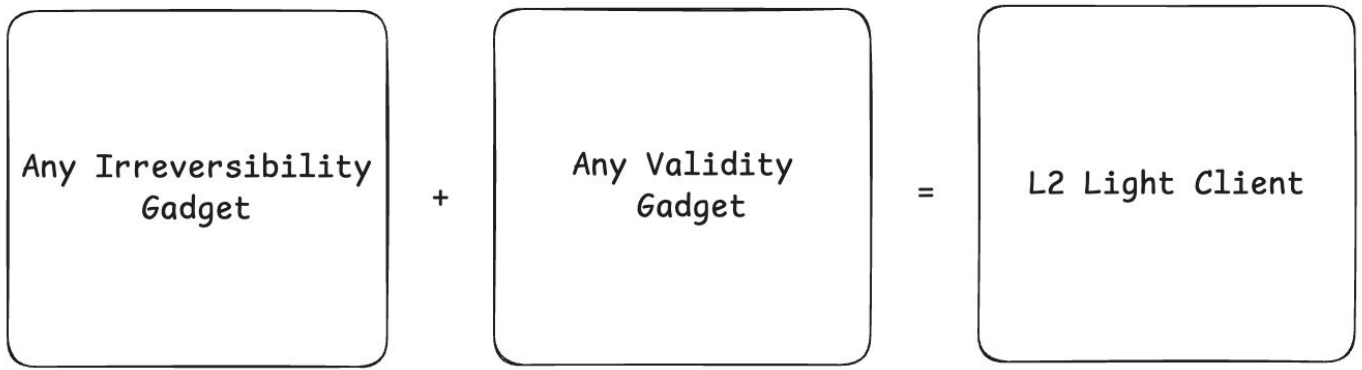
- Irreversibility gadget: Ethereum Altair light client
  - L2s use L1 as their primary irreversibility gadget (by posting data to L1 via blobs)
  - Sync the Ethereum light client and fetch L2 block inputs from the blobs (maybe fetch just the blob commitments to save bandwidth)
  - We now have access to the L2 block inputs in our light client!
- Validity gadget: SNARKs
  - Use a SNARK (potentially the snark generated for the L2 bridge) to verify that the execution of the block inputs yields some given block output
  - We now have access to the L2 block outputs (headers) in our light client!
- Problem: latency
  - Rollups tend to post data to L1 only every few minutes
  - This data takes 13 - 19.5 additional minutes to finalize
  - SNARK generation or dispute games may take even longer
  - Our light client runs way to far behind the tip of the chain!

The light client superpower

Balance security with latency and performance!

The light client superpower

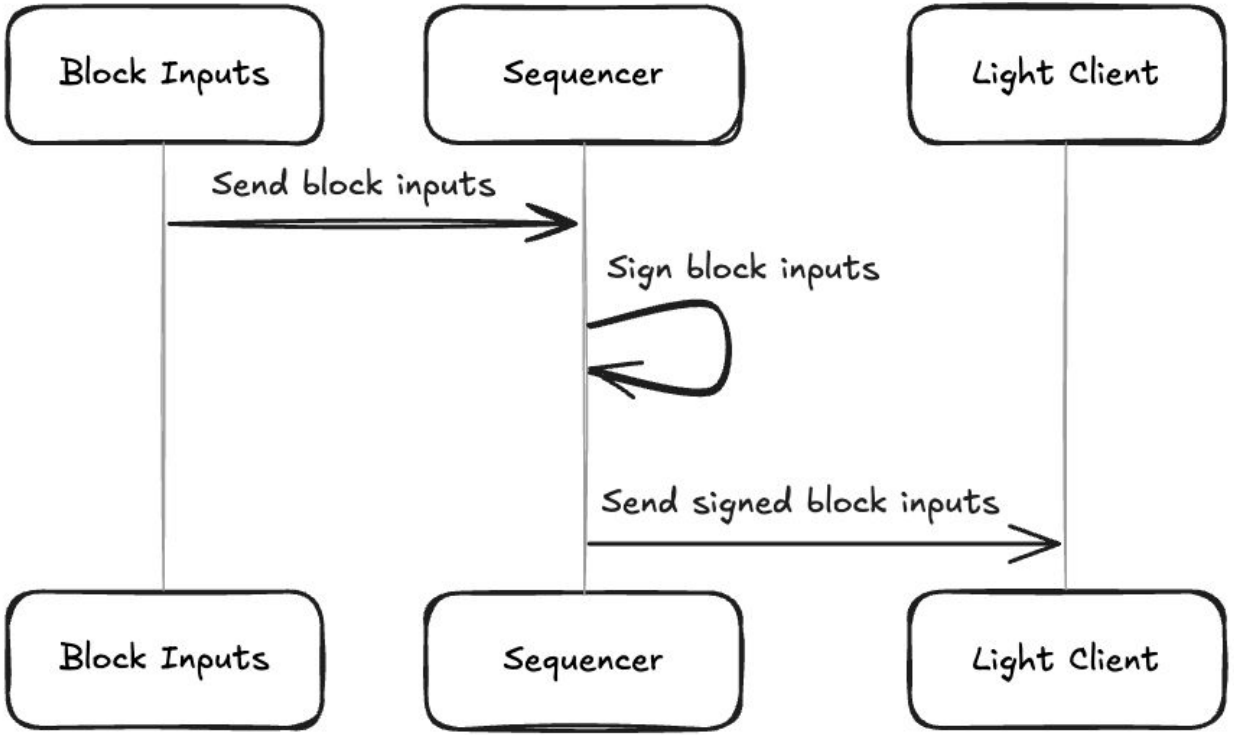
Let’s choose irreversibility gadgets and validity gadgets that offer lesser security guarantees, but much lower latency and higher performance!



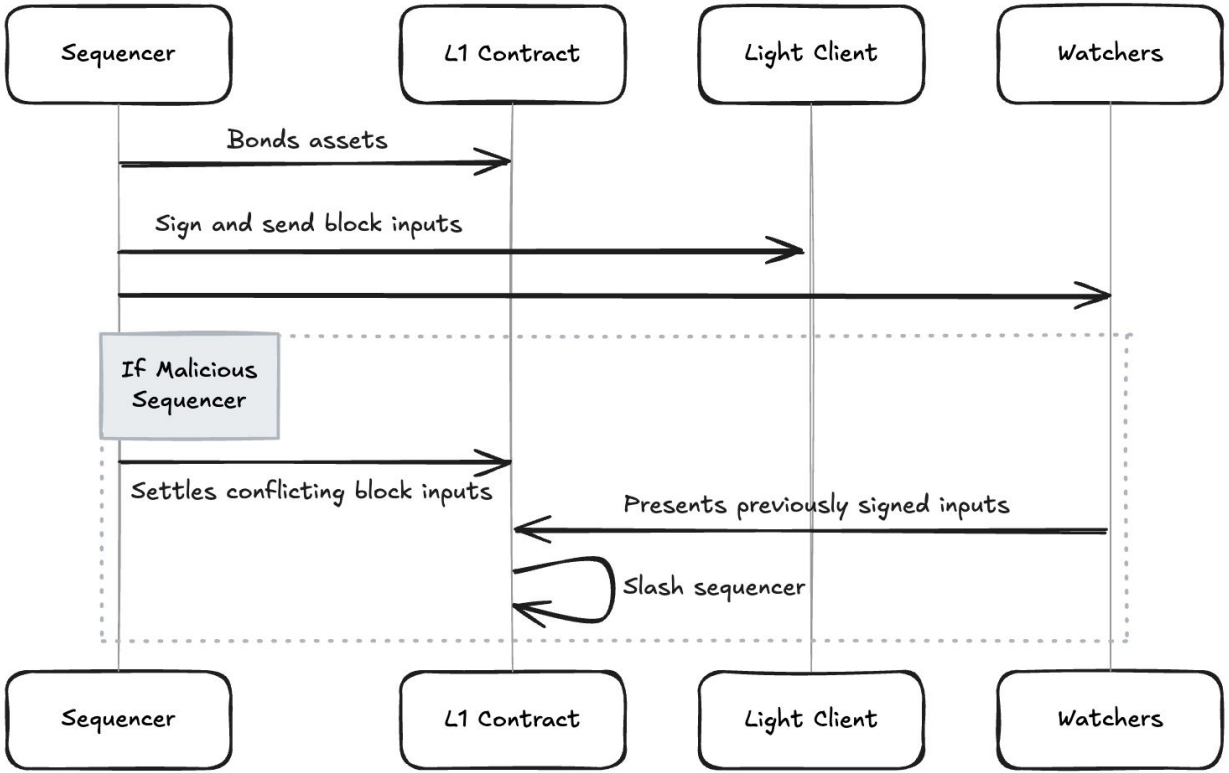
Example irreversibility gadgets

Irreversibility Gadget	Latency	Security	Complexity
Sequencer Commitment	Low	Low	Low
Bonded Sequencer	Low	Medium	Medium
Fast Finality Committee	Low	Medium	Medium
Ethereum Finality	Very High (for now)	Very High	Low

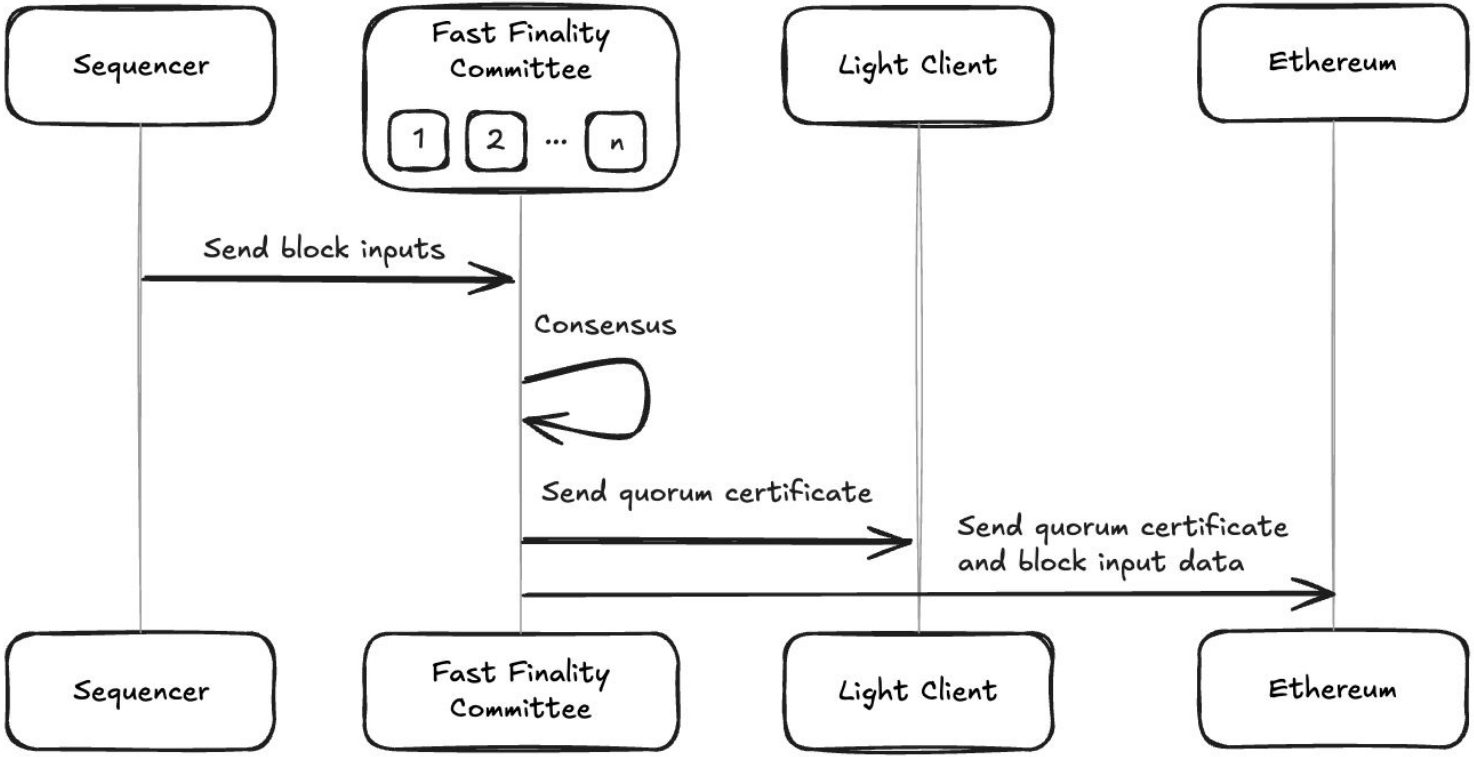
Low latency irreversibility gadgets: sequencer commitment



Low latency irreversibility gadgets: bonded sequencer



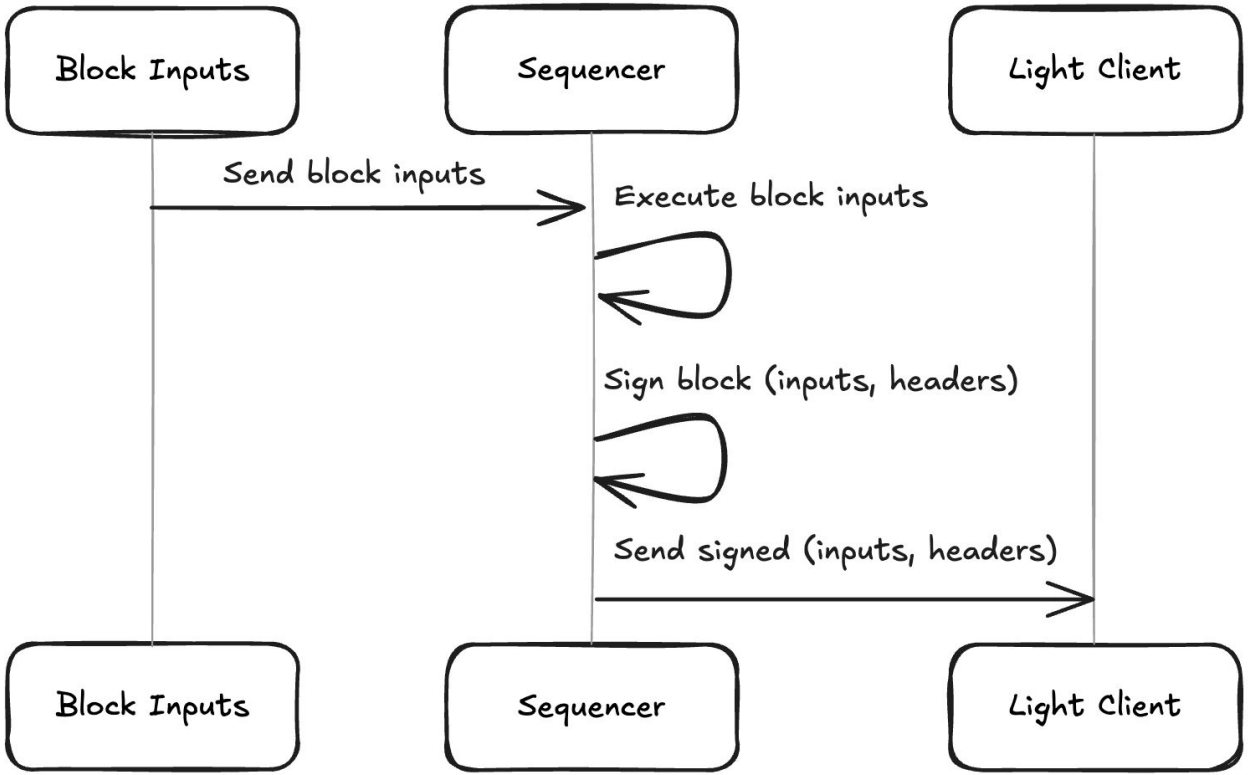
Low latency irreversibility gadgets: fast finality committee



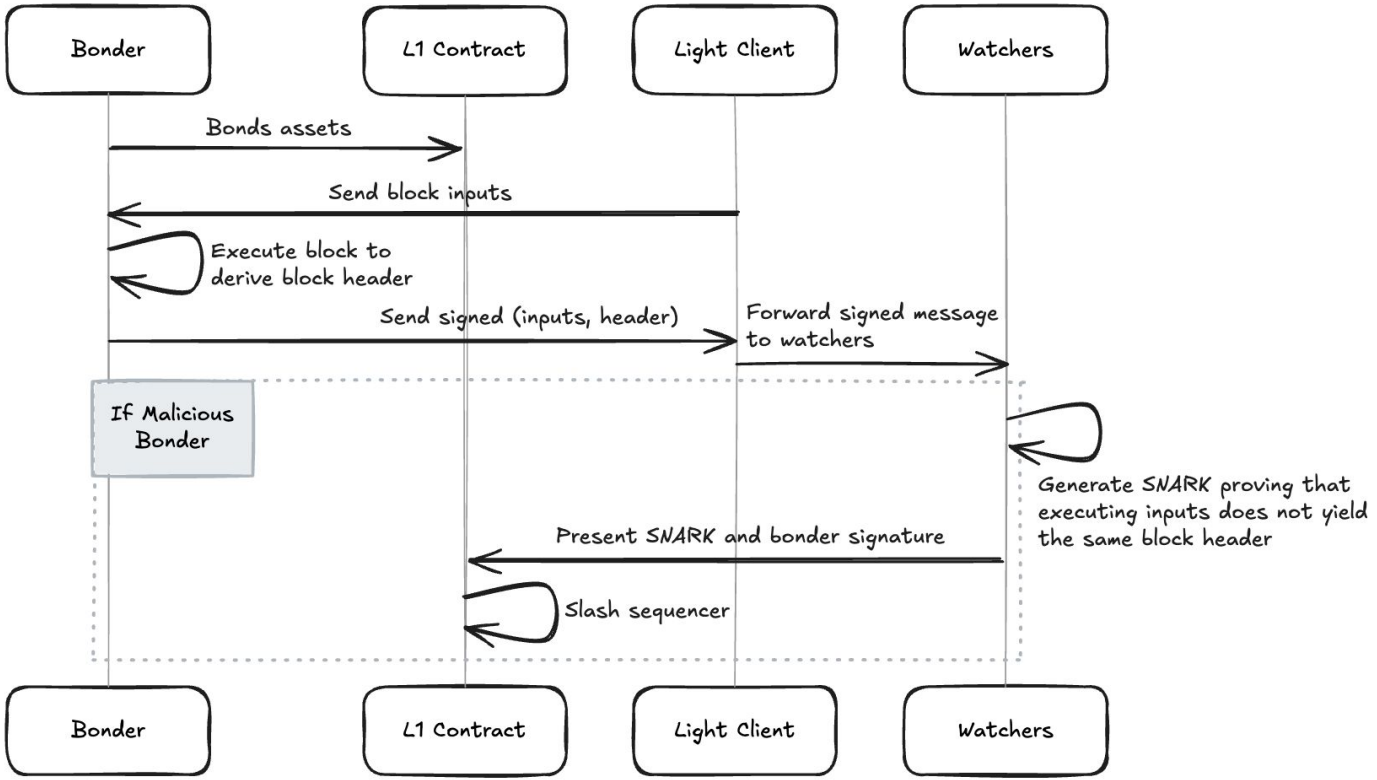
Low latency validity gadgets

Validity Gadget	Latency	Security	Complexity
Sequencer Commitment	Low	Low	Low
Bonded Commitment	Low	Medium	Medium
TEE Execution	Low	Medium	Medium
Offchain Dispute	Medium	High	High
SNARK	High (for now)	Very High	Very High

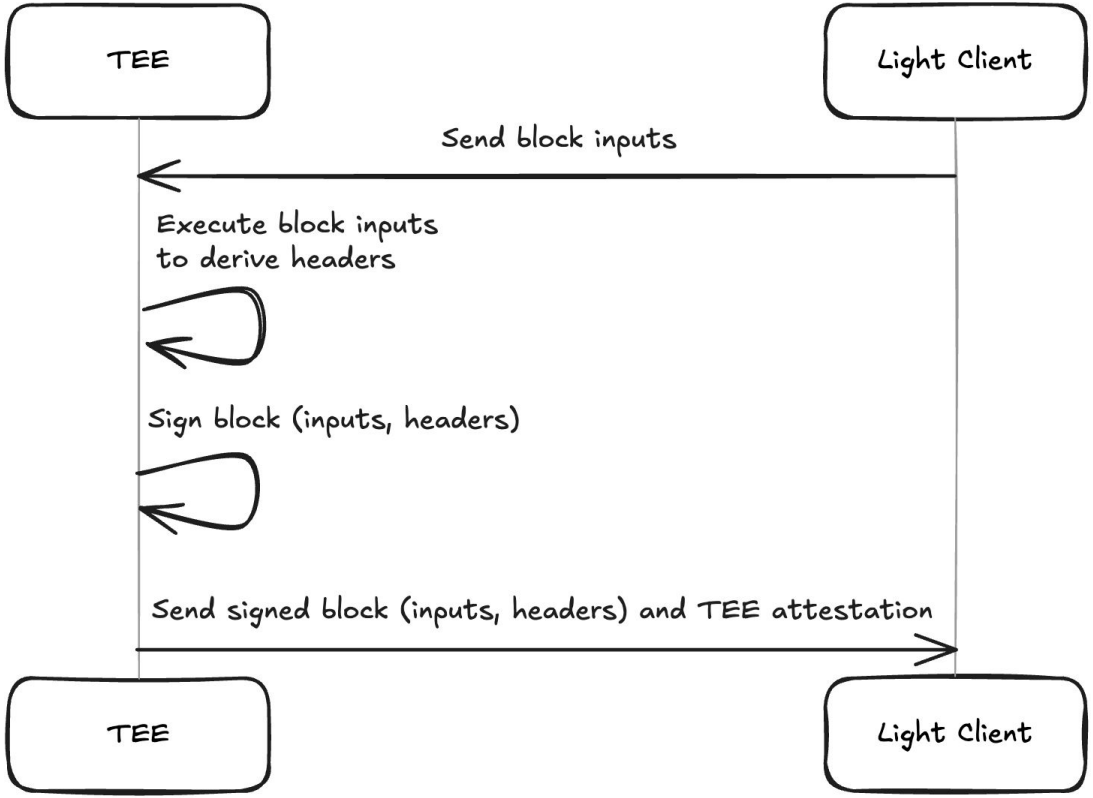
Low latency validity gadgets: sequencer commitments



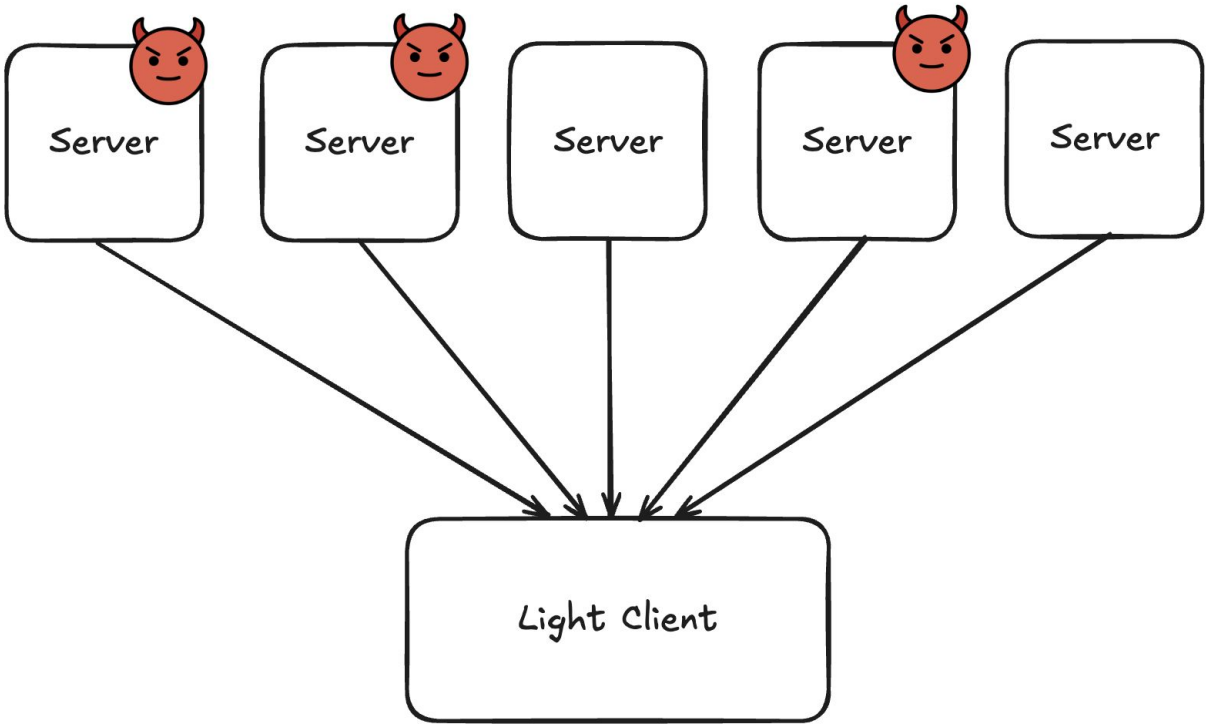
Low latency validity gadgets: bonded commitments



Low latency validity gadgets: TEEs



Low latency validity gadgets: offchain dispute games



The light client security-latency trade-off matrix

Irreversibility Gadget	Latency	Security	Complexity
Sequencer Commitment	Low	Low	Low
Bonded Sequencer	Low	Medium	Medium
Fast Finality Committee	Low	Medium	Medium
Ethereum Finality	Very High (for now)	Very High	Low

X

Validity Gadget	Latency	Security	Complexity
Sequencer Commitment	Low	Low	Low
Bonded Commitment	Low	Medium	Medium
TEE Execution	Low	Medium	Medium
Offchain Dispute	Medium	High	High
SNARK	High (for now)	Very High	Very High

Recap

- We have a new way of thinking about L2 light clients!
- To build better L2 light clients we need to implement
  - Better irreversibility gadgets
  - Better validity gadgets

Helios: all the L2s and all the gadgets!

- Helios now supports the OP Stack
  - Uses sequencer commitments for both irreversibility and validity
  - You can now use Helios on OP Mainnet, Base, Zora, Worldchain, and everything else built on the stock OP Stack!
- What's next
  - More L2s
  - More validity gadgets
  - More irreversibility gadgets (we need L2 buy in for some of them)
- Want to help?
  - Reach out to me on Telegram (@ncitron)
  - We're always looking for more people to help build the future of light clients!