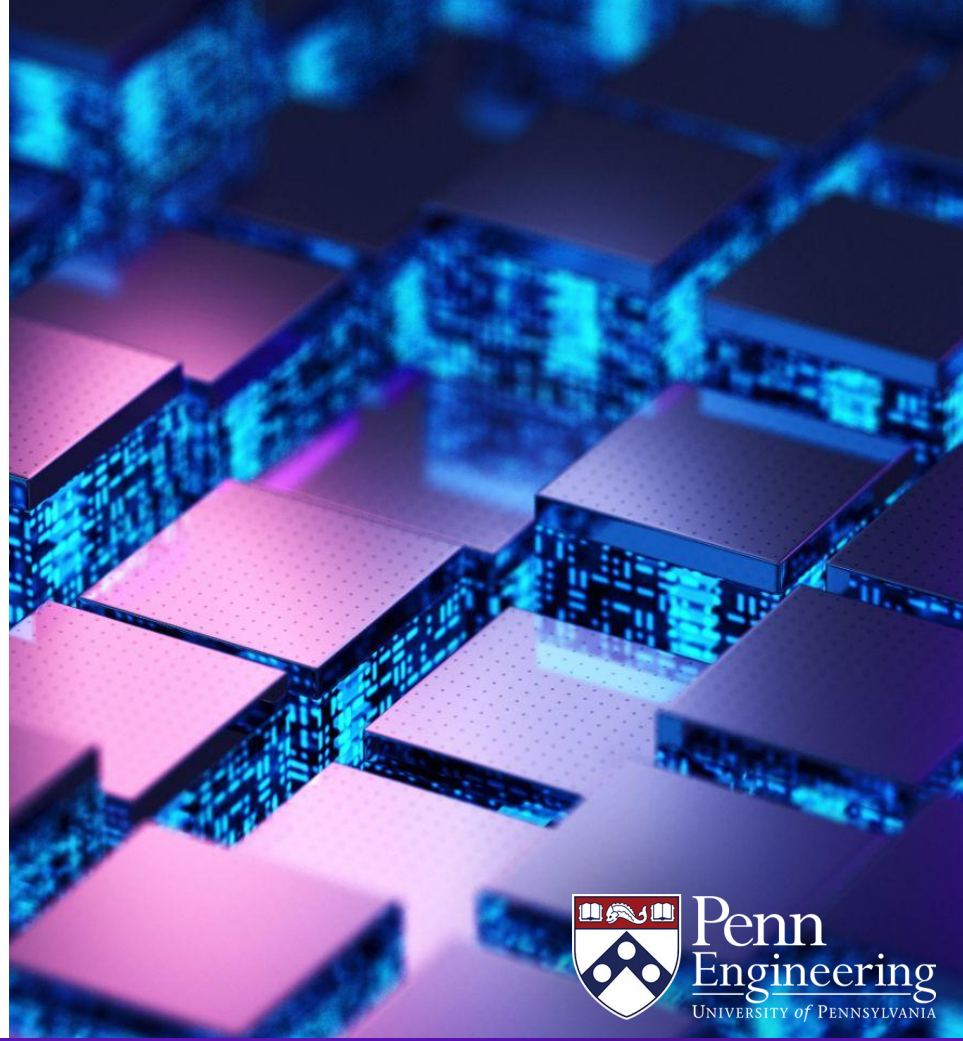
EAS 5830: BLOCKCHAINS

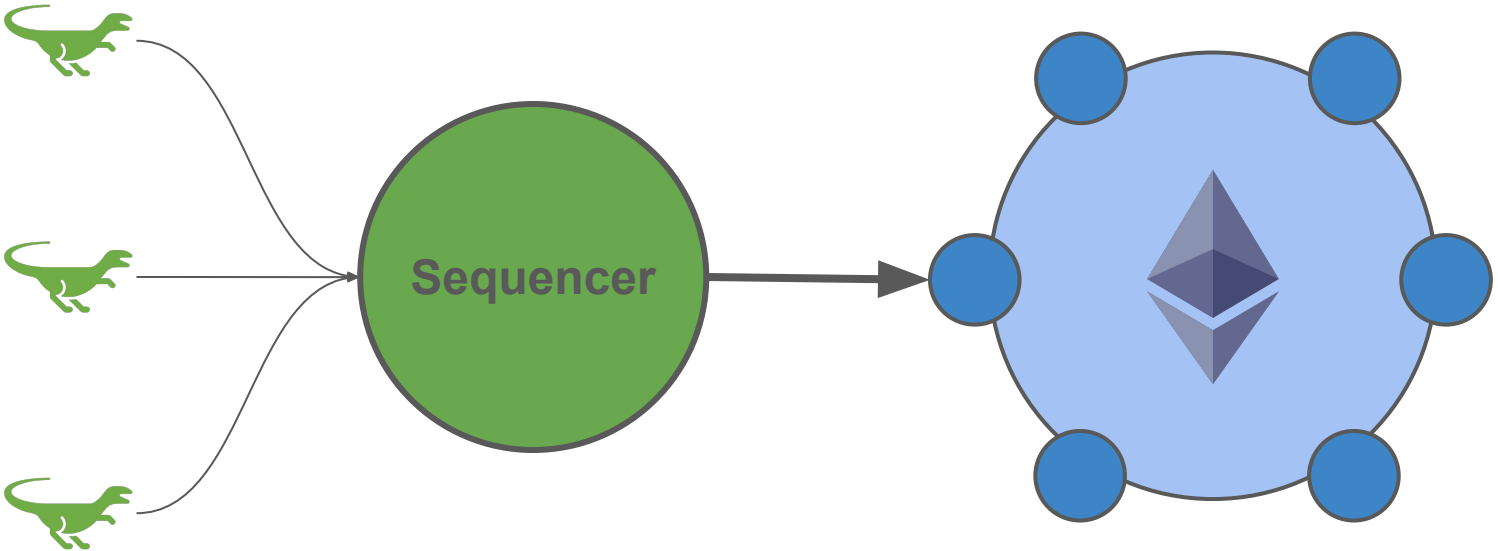
Optimistic Rollups

Professor Brett Hemenway Falk




OP

Optimistic Rollups



Rollup users

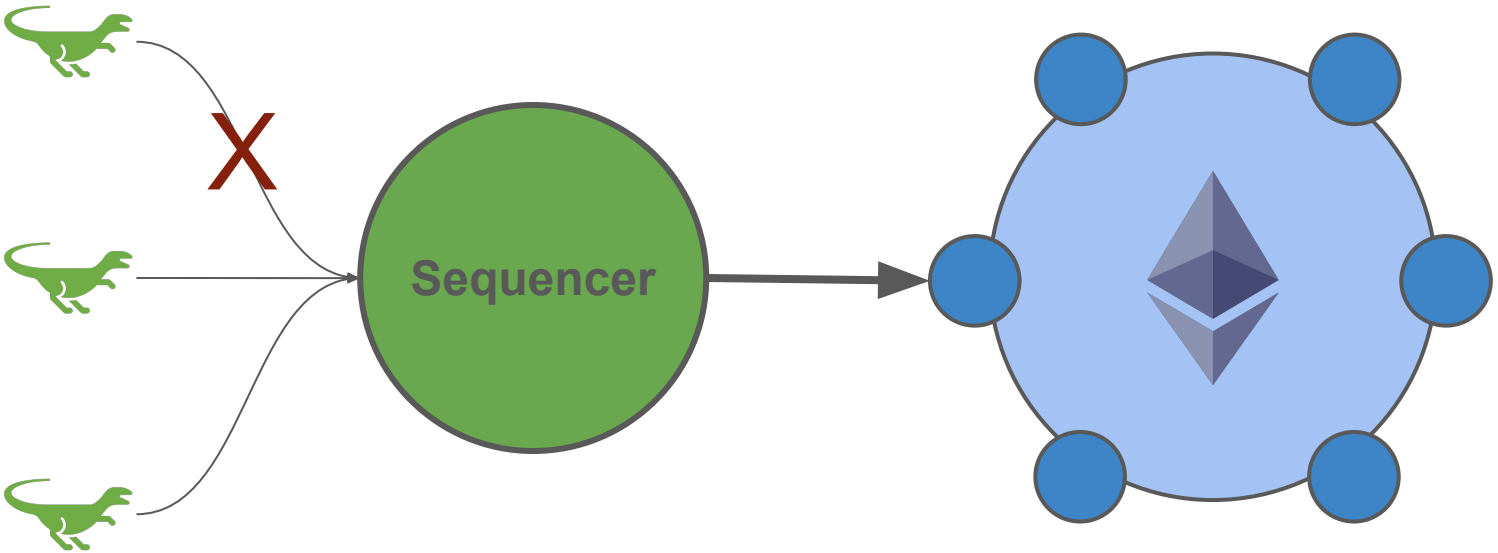
What can the sequencer do?

- Censor transactions
  - Refuse to include user transactions
- Invalid state updates
  - E.g. lower your balance without a signed transaction
- MEV
  - Reorder transactions
  - Add their own transactions

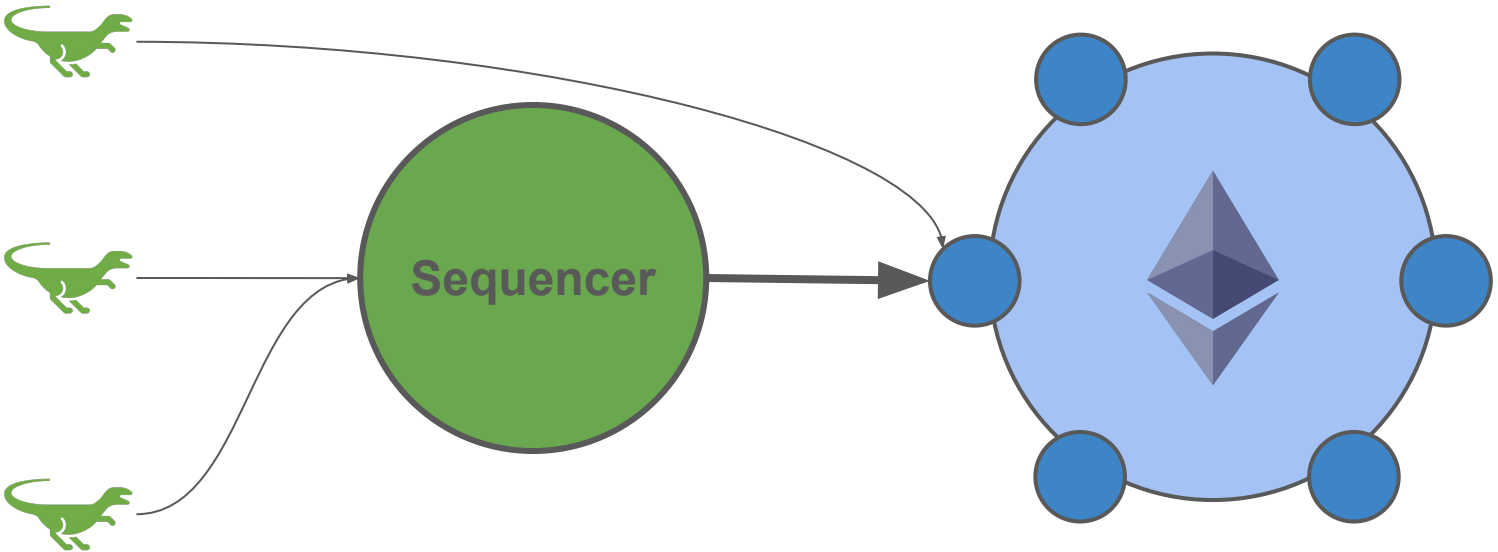
What can the sequencer do?

- **Censor transactions**
  - Refuse to include user transactions
- **Invalid state updates**
  - E.g. lower your balance without a signed transaction
- MEV
  - Reorder transactions
  - Add their own transactions

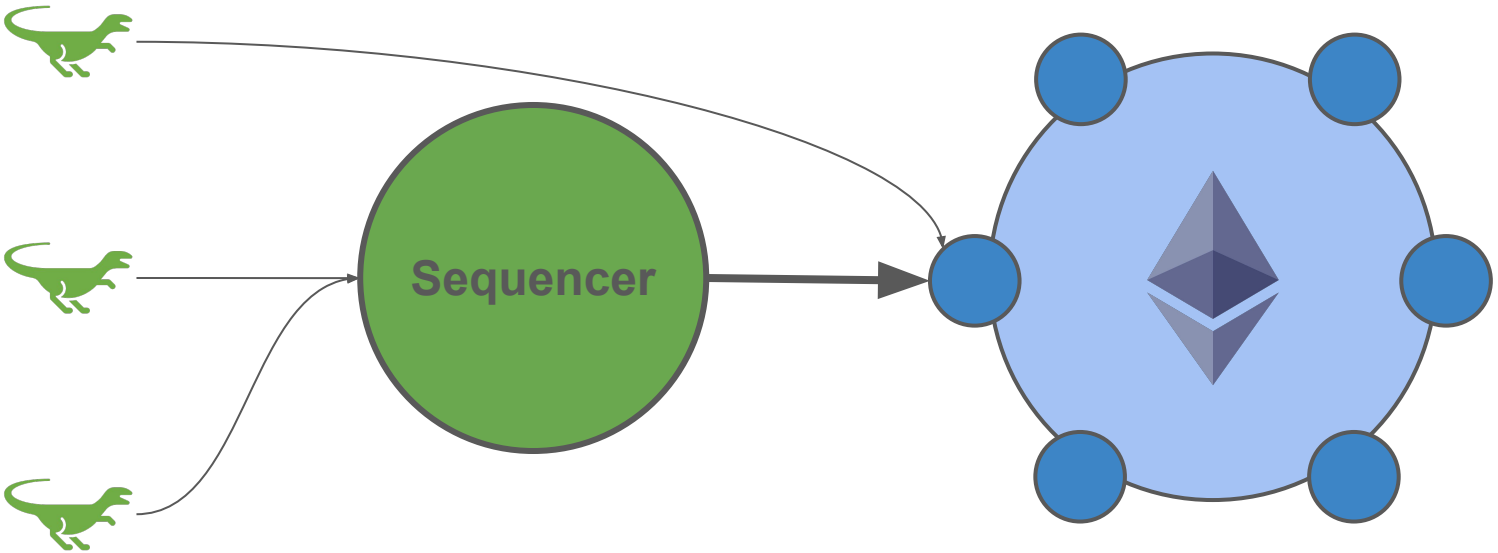
Censoring transactions



Censoring transactions



Censoring transactions



In Arbitrum this is done by calling the forceInclusion function in the Inbox contract

Invalid State Updates

- Sequencer (or validator) posts a new L2 state to the L1 chain
- The L1 does **not** execute all the L2 transactions that led to the new state
  - This is where the cost savings comes from!
- Fraud Proofs
  - 7 day window in Arbitrum and Optimism

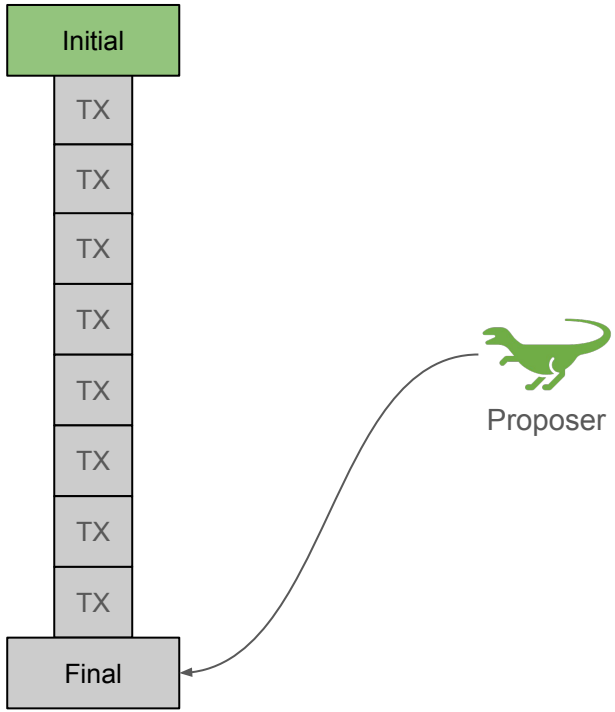
Fraud proofs

- L1 has
  - Old state
  - New state
  - Hash of all transactions in the update
- Fraud proof
  - Users can submit a “challenge”
  - Put up some stake
  - Challenge is resolved on L1
    - e.g. simulate all the L2 txs on the L1 and checking the resulting state
    - This is really slow and expensive, but it should never happen

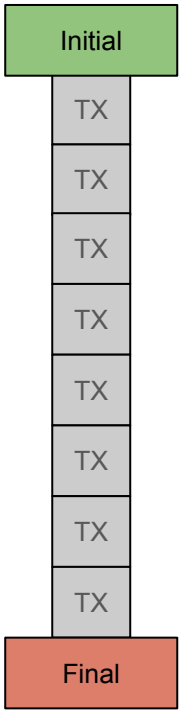
Interactive Fraud Proofs

- Problem:
  - When someone claims fraud, re-executing all the transactions on L1 can be expensive
- Solution:
  - Arbitrum's solution: don't re-execute all the transactions
  - Identify where the problem is

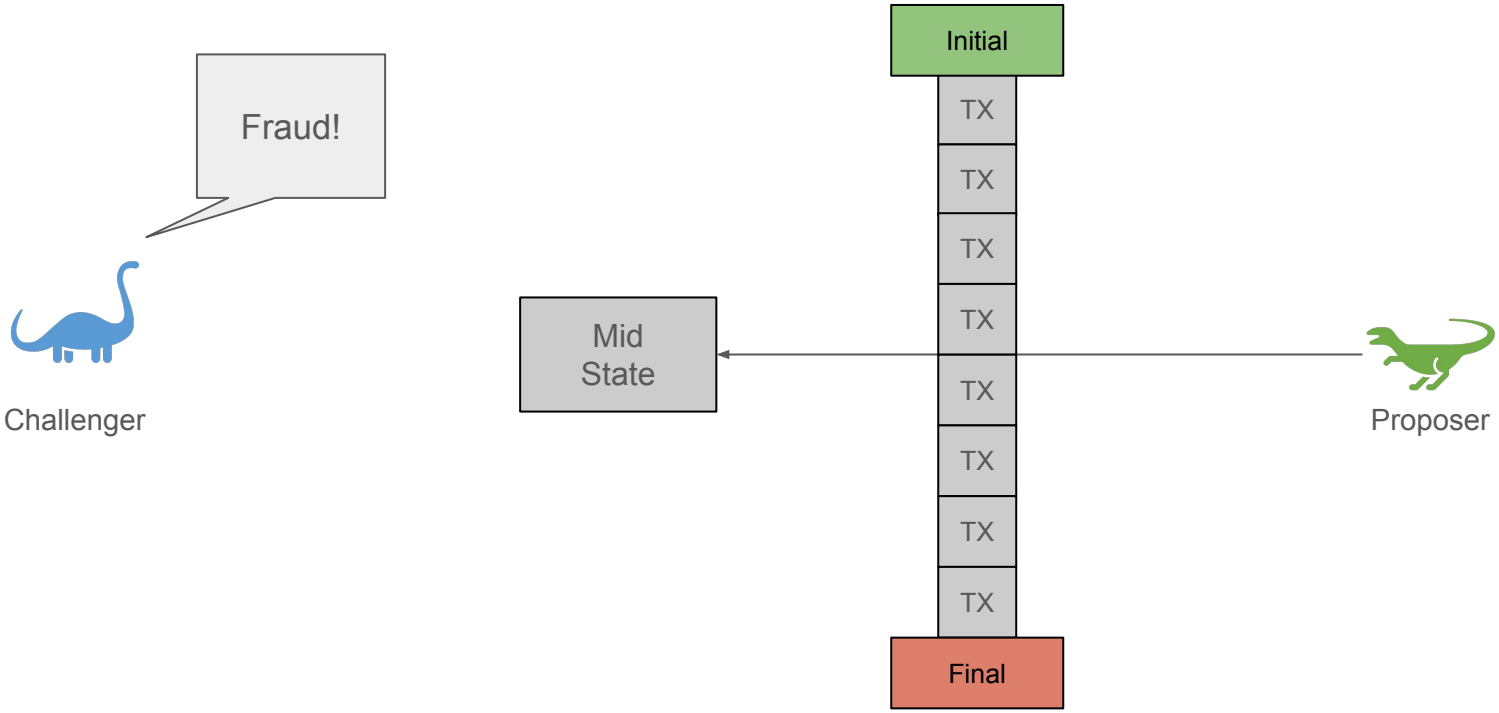
Arbitrum's bisection protocol



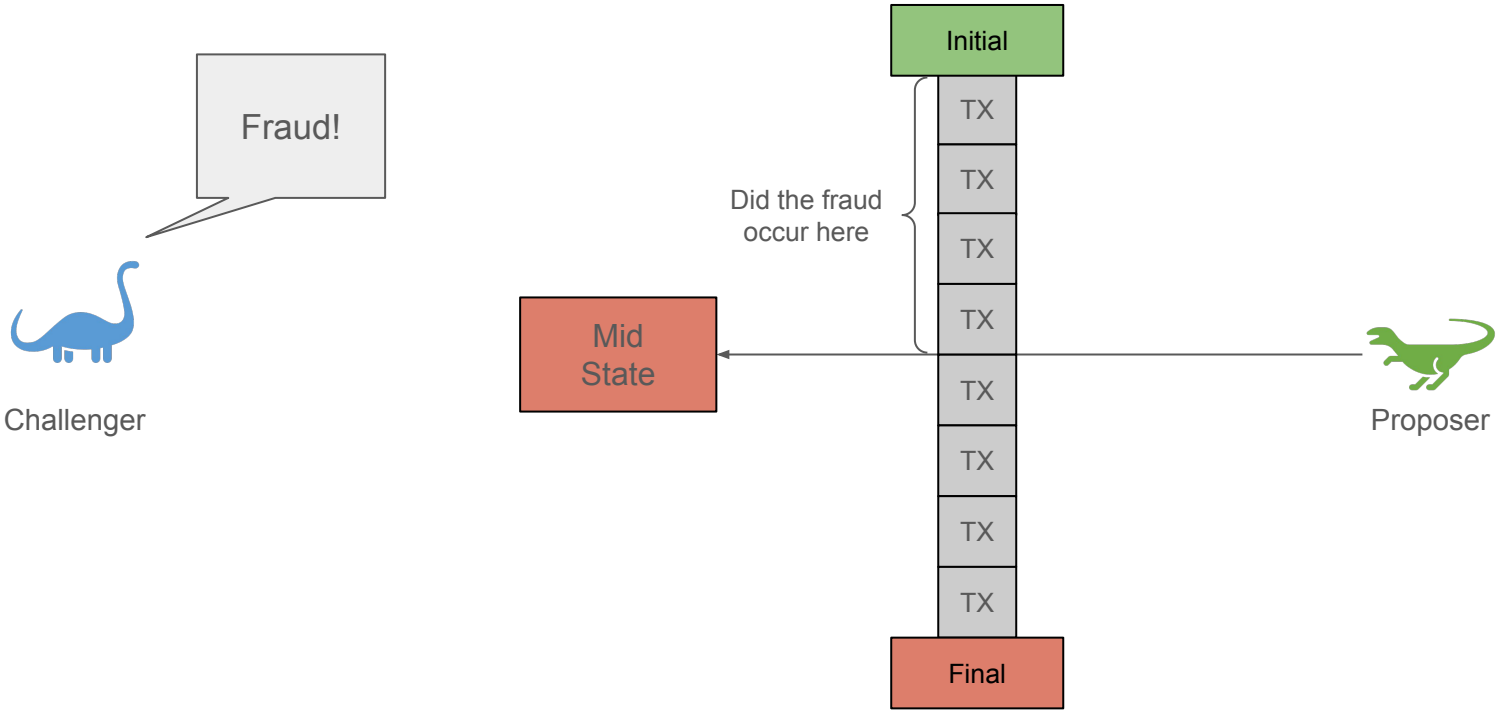
Arbitrum's bisection protocol



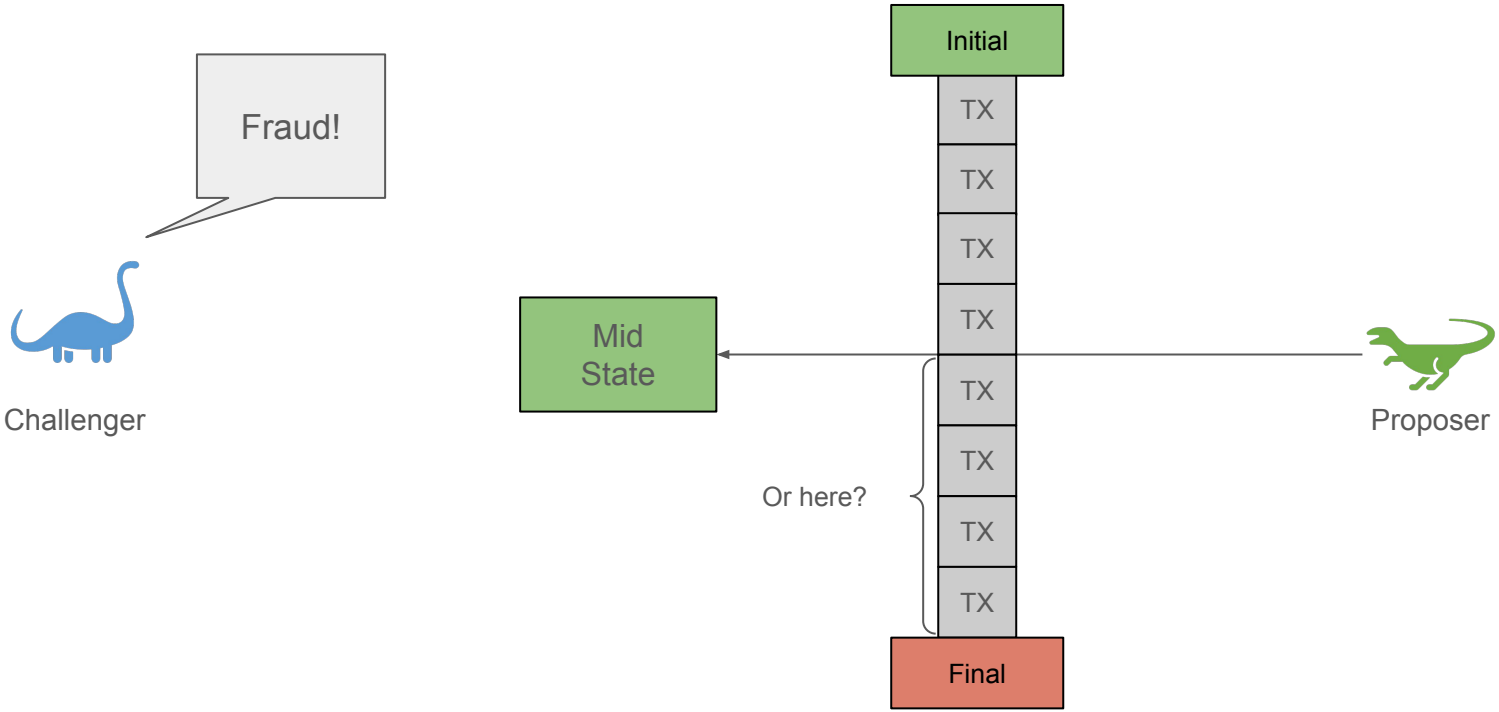
Arbitrum's bisection protocol



Arbitrum's bisection protocol



Arbitrum's bisection protocol



BRAYDEN LINDREA

SEP 11, 2023

Arbitrum’s fraud proofs haven’t been used in the two years since it launched

“the most important code that should never run”

Near's Rainbow Bridge Blocks Another Attack, Costing Hackers 5 Ethereum

The Rainbow Bridge hack over the weekend saw funds returned in 31 seconds with no harm to users, but the attackers lost 5 Ethereum in the process.

By Emily Tonelli

Aug 23, 2022

3 min read

Where does the data live?

On the L1

- L2 TXs are stored on the L1 as “calldata”
- Not executed on the L1
- But still expensive

On a “data-availability layer”

- Celestia
- Avail
- Arbitrum’s AnyTrust

Soft Confirmations

- Full confirmation:
  - Rollup transactions are not confirmed until the fraud proof window expires (7 days)
- Soft confirmation:
  - Trust the sequencer
    - Sequencer can confirm transactions instantly (even before a block is posted to the L1)
- Local confirmation:
  - When a block is posted to the L1, you don't need to wait for the fraud proof window, you can validate the transactions yourself
    - "Watchtower mode" in Arbitrum

Centralization

- Optimism and Arbitrum launched with a single, centralized sequencers
- Optimism launched with fraud proofs disabled
- At Launch, Arbitrum only allowed fraud proofs from AllowListed entities
- Optimism's and Arbitrum's contracts are upgradeable
  - Address with upgrade authority can change the state of the rollup!
  - Initially, developers had upgrade keys
  - Eventually, upgrades controlled by DAO governance