



Joe Andrews

Cofounder @Aztec
x.com/jaosef

Decentralise your sequencer

A guide for L2s

Agenda

01

Our Journey, why we care, why should you?

02

Why can't we rely on "trust me bro"

03

Forced Inclusion \neq decentralised sequencing

04

Components of a decentralised sequencer

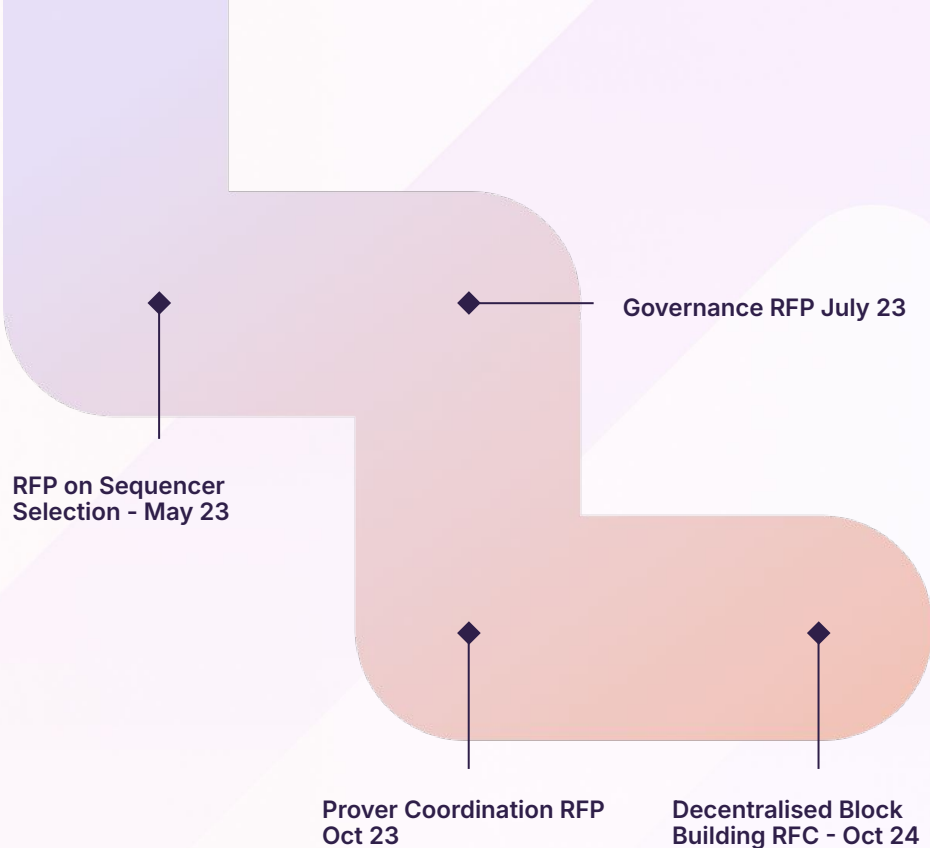
05

Decentralisation is not just about sequencing rights

Our Journey

At Aztec we have spent the last 18 months researching how to decentralise our L2 out of necessity as a privacy rollup.

My goal today is to share some of our learnings with you so we can create a more decentralised set of L2's for users tomorrow



RFP on Sequencer
Selection - May 23

Governance RFP July 23

Prover Coordination RFP
Oct 23

Decentralised Block
Building RFC - Oct 24

Aztec Decentralised Block Production RFC

You can read more about our designs on our forum.

We use random leader election, and L2 committee for pre-confirmations and L1 to verify everything in a zk proof

Head to <https://forum.aztec.network> →



Do L2's care?

All

http

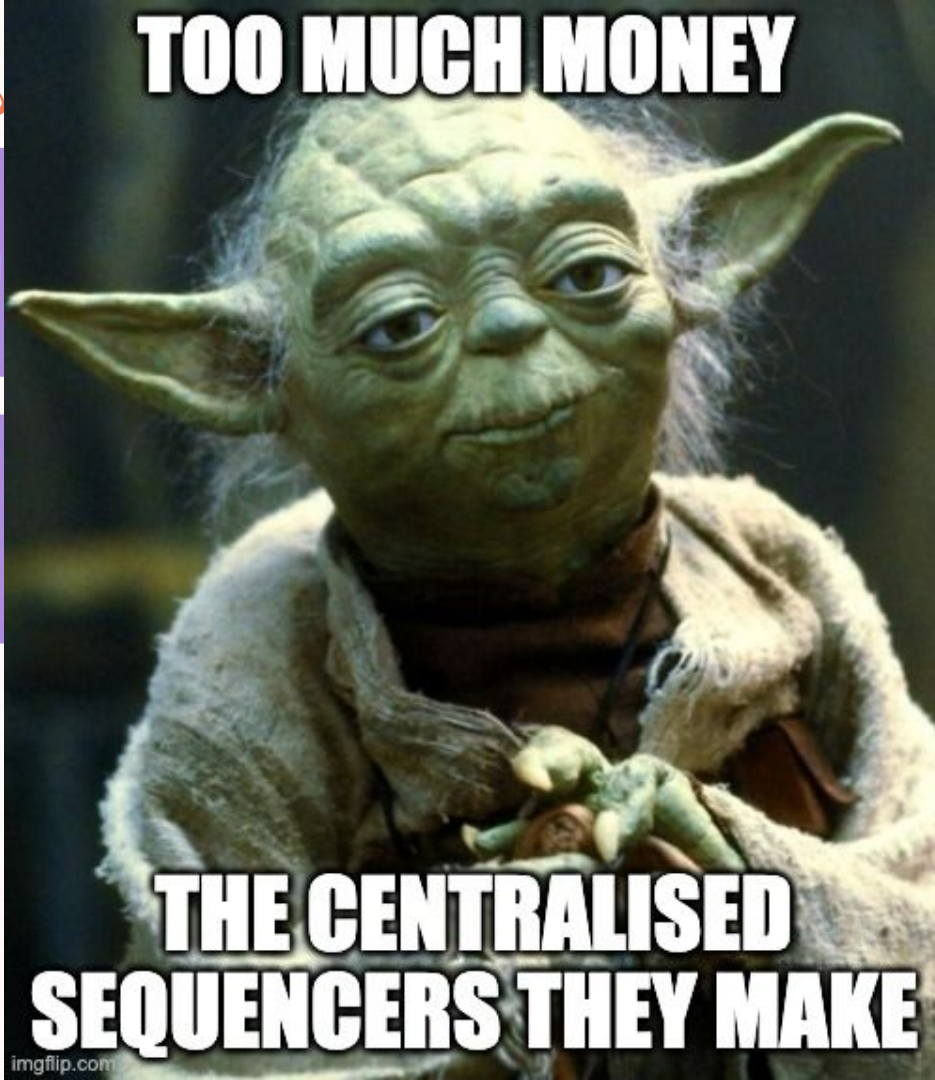
We are working



ARBITRUM

\$20m+

Arbitrum



No comment

k will be
sed....

n+

Linear

Users trust L2's with \$38BN today

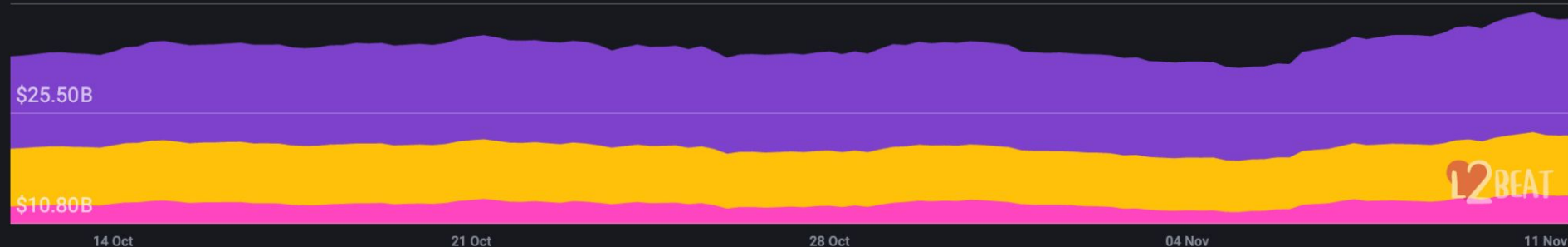
Total value locked stacked by type

2024 Oct 12 — Nov 11

\$38.00B

▲ 15.1% / 30 days

\$40.20B



\$38Bn that **does not** inherit the
liveness and **censorship** properties of
Ethereum

That's \$38Bn that relies on

“Trust me bro”



The **censorship resistance, liveness and “safety”**
of your L2 depend on a decentralised sequencer

Why can't we rely on "trust me bro"?

Centralised sequencers can lie

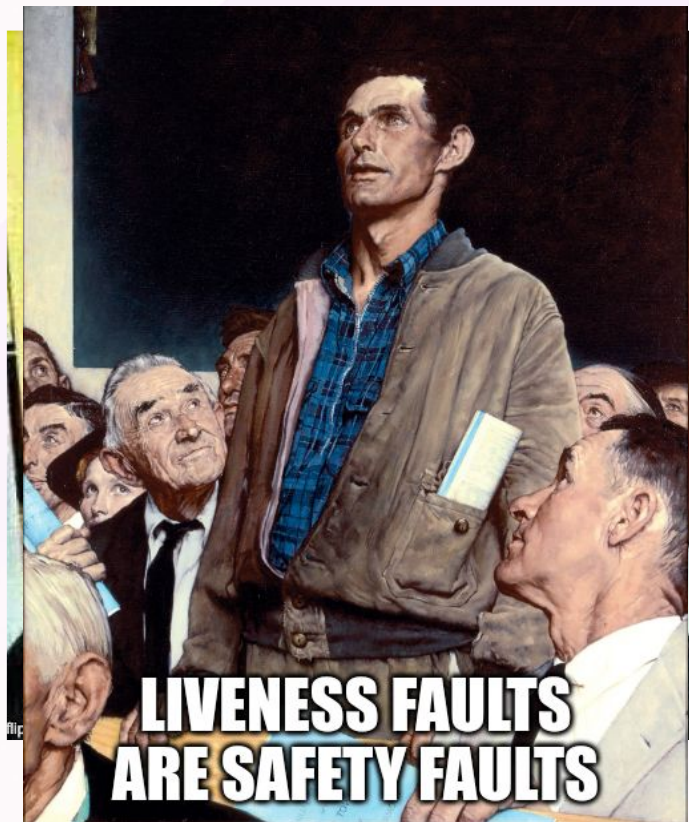
A pre-confirmation from a centralised sequencer is equivalent to "trust me bro". Is the state correct, are the other transactions real?

Censorship in 2024 is real

The world around us is more divisive than ever, the chances of one central entity sharing the ideologies of all are vanishingly small...

A liveness failure is a failure

It is also an attack vector. Maybe not for meme coins or other speculation, but put 20% of the worlds transactions on it and then see who comes knocking...



Forced Inclusion \neq Decentralised Sequencing

The road is technically working – but would you use it to get to work? Maybe to flee a storm as a last resort, but not daily.

1. Forced transactions are second class citizens and only gives a guarantee of eventual inclusion
2. **Decentralised sequencing** is required to give strong liveness and strong censorship properties to all transactions



Forced inclusion = eventual sequencing

So – how do we decentralise?

4 Components of Decentralised Sequencing



Leader Election

Who proposes the next block?

1. Proposal Voting
2. Round Robin
3. Random Shuffle of Sequencers
4. Random shuffle of proposals
5. Random weighted reputation



D/A

How does the next sequencer find out what happened?

1. Data is required to build ahead on the pending chain.
2. Data is required to reconstruct the finalised rollup state

Where is this data published?



Slashing / Incentives

How is sequencer rewarded for work / punished for bad behaviour?

1. Slashing
2. POG?

Who decides?



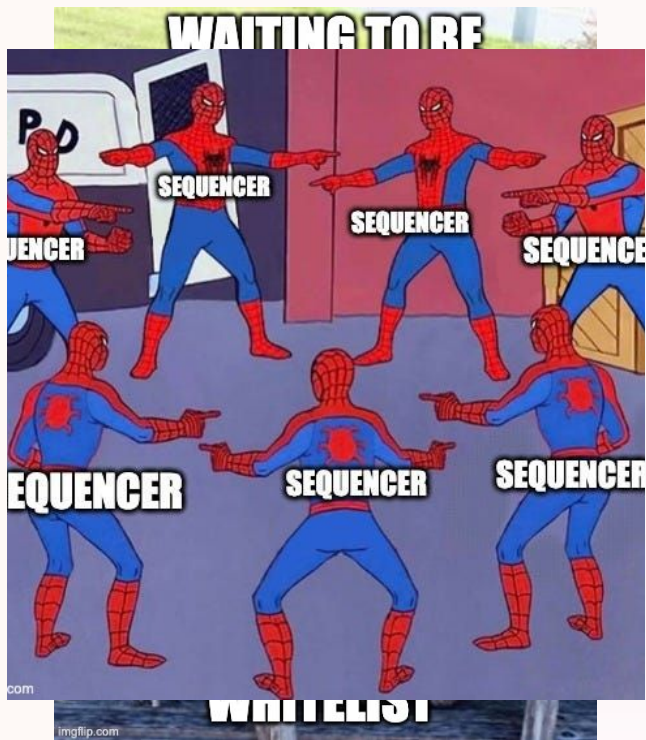
Consensus

How do we verify:

1. The leader election rules were followed?
2. Sufficient data was published
3. Who should be slashed?

Do we use L1, a separate consensus network?
Economics?

Leader Election:



Round Robin

Leaders rotate in a deterministic order through a set, new candidates are added to the back of the set

Random Shuffle

Using a random beacon, usually Randao, either sequencers or proposals are shuffled to pick the next block

Proposal Voting

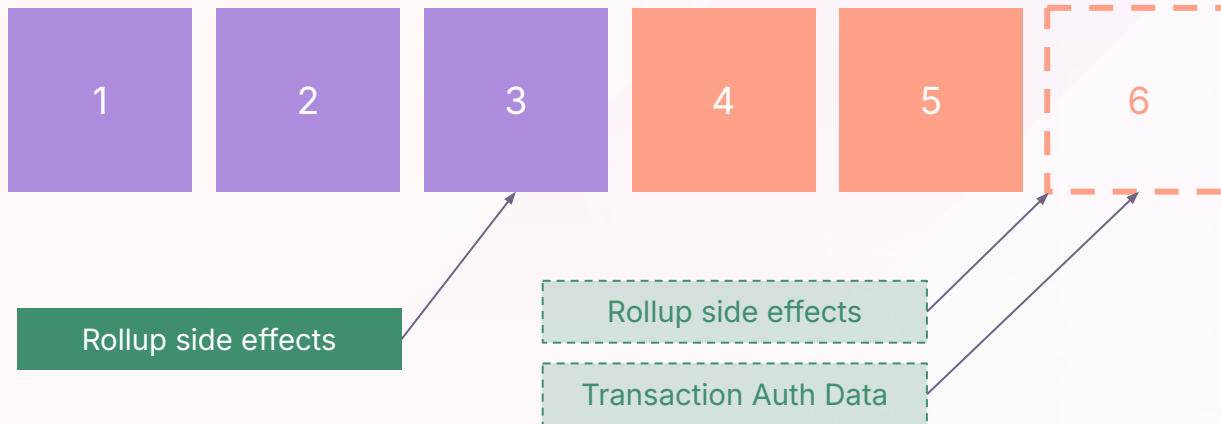
Anyone can make a proposal, stakeholders vote on the “best” proposal to be the next block taking into consideration economics or other factors

Reputation or Stake weighted

Like a random shuffle but weighted by stake or reputation

D/A : What data must a sequencer have to build a block?

- *Blocks finalized on L1, either via expiration of fraud proof window or validity proof*
- *Blocks built ahead on pending chain*



Transaction Auth Data

Public Rollup: TxRequest + Signature (~400 bytes)

Privacy Rollup: TxRequest + Zk Proof(~32-64 kilobytes)

D/A: Comparison

Call Data

Tried and tested since 2013 – required if you want to use the data in an EVM contract

Blobs

More capacity, cheaper, we like this – useful for data that is only needed off-chain, or can be proven in a snark

Payload Timeliness Committee

A dedicated short term L2 committee that attests to sufficient data being available to prove a block

Alt D/A

Celestia, Eigen, Avail lots of capacity, can't use the data on chain, and also can't verify the data exists quickly on L1

Transaction Auth Data	Rollup State	TPS	Security
✗	✓	1	\$\$\$\$
Public Rollups only	✓	10-100	\$\$\$\$
✓	✗	10-100	\$
🤔	✓	100+	\$

Consensus: It's not just about verifying “what”

Who did it?

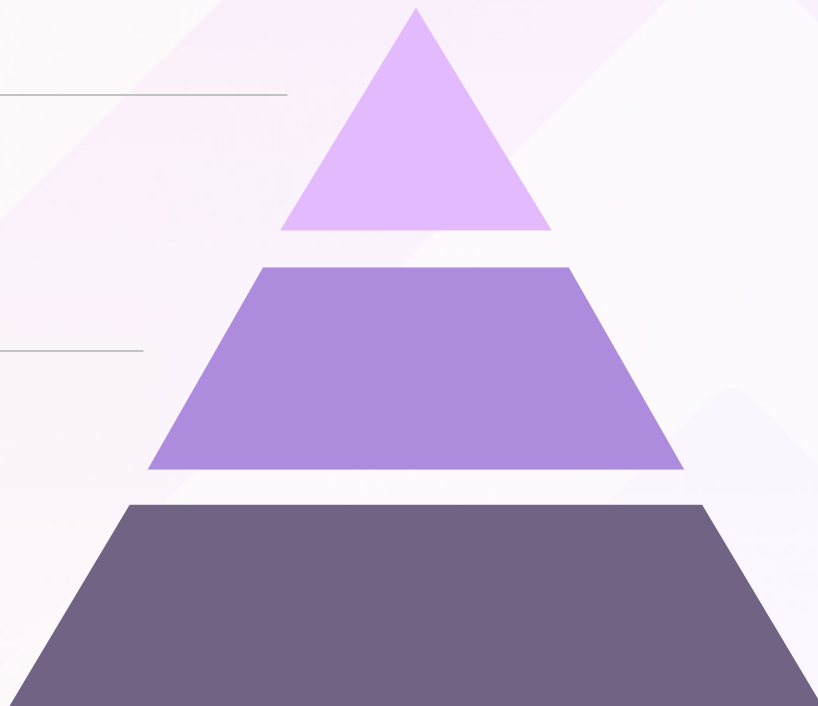
We need to verify the leader election, or it doesn't have any weight for censorship resistance

How can we trust this is correct?

Validity proofs or challenge periods take time.
Is sufficient transaction auth data posted to enable the next sequencer to build?

What happened?

Transactions A,B,C,D produced state X,Y,Z



Consensus: Do we inherit censorship, liveness and safety from L1?

Use L1 (Based)

High latency, and limited throughput, but we inherit everything from L1. Possible for public rollups.

Use L1 + L2 Committee for Transaction Auth D/A

Inherit censorship resistance and liveness, and with good UX as the committee can verify the sufficient data is available to build the next block quickly. Possible for public and private rollups.

Use L1 + Economic Bond for Transaction Auth D/A

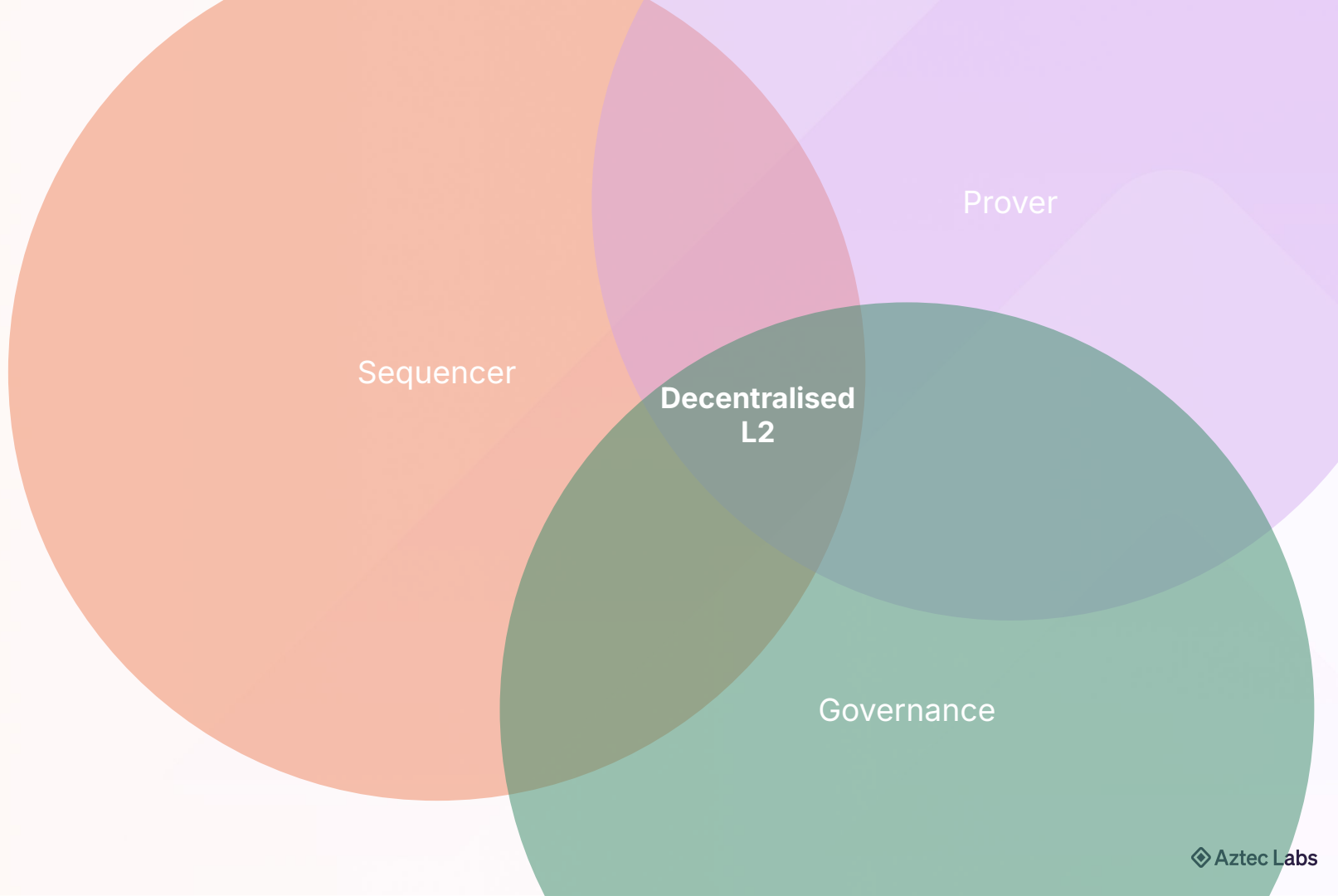
Simple, but requires a centralised actor to put up the entire security of the bond. Possible for public and private rollups

Use separate L2 consensus network

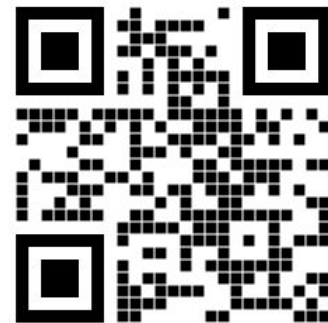
Inherits most properties from its L2 staking set, unless you prove L2 consensus alongside the validity proof on L1. This is hard.

Censorship	Liveness	Safety	Difficulty
✓	✓	✓	
✓	 If committee honesty assumption holds	✓	
✓	 Depends on Bond	✓	
 Inherits from L2 staking set	 Inherits from L2 staking set	 Eventually if side effects are posted to L1, but not for pre-conf	

Decentralising your sequencer is
just the beginning...



Follow me on twitter →



Thank you for listening!

Any questions?

Aztec Forum Posts →

