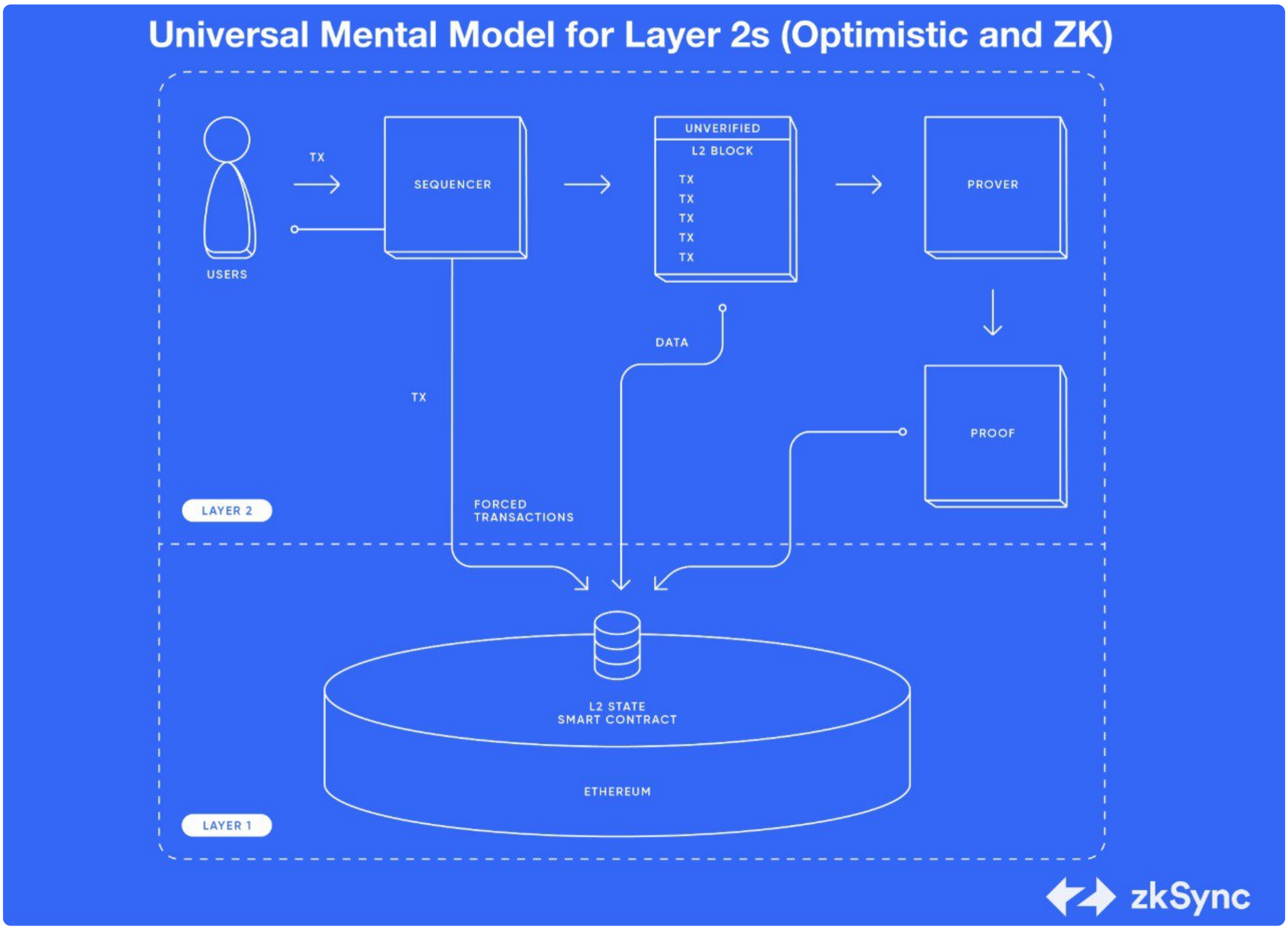
Lesson 8

Week 2

Lesson 5 - Understanding and Analysing Layer 2
Lesson 6 - Agnostic Layer 2 Transaction Lifecycle
Lesson 7 - Optimistic Rollups v ZK Rollups
Lesson 8 -What's next in Layer 2 part 1 : Decentralised Sequencers

A general Article about the future of rollups

Sequencers



From Coin Desk article
"The sequencer is like “the air traffic controller for the specific L2 ecosystem that it serves, so when Alice and Bob attempt to make a transaction at the same time, who comes first? That’s decided by the sequencer.”

Sequencer role

- Collect user transactions: Receive transactions from end users through a mempool.
- Prioritise transactions: Choose transactions from the mempool, arranging them based on a specific set of rules.
- Process transactions by sending them to an executor.
- Initial validation and acceptance, the sequencer can provide some indication of finality for the transaction, see previous notes for more information.
- Send execution results to a prover for validity rollups.
- Batch transactions and send transaction data to the Data Availability Layer

Sequencers and Aggregators

For zkEVMs we may split the functionality into

- transaction batching
- transaction validation

For example in Polygon zkEVM we have

- Sequencer - this will propose transactions batches and submit those.
- Aggregator - this checks the validity of the batches and organises the generation of the proof.

The aggregator role can be permissionless, so that anyone can create a proof.

Problems with centralised sequencers

- Centralisation / Single point of failure / censorship possibilities
- Lack of participation
- MEV
- Lack of trust
- Liveness problems

Advantages of centralised sequencers

- Cost
- Simplicity

Requirements for a sequencer

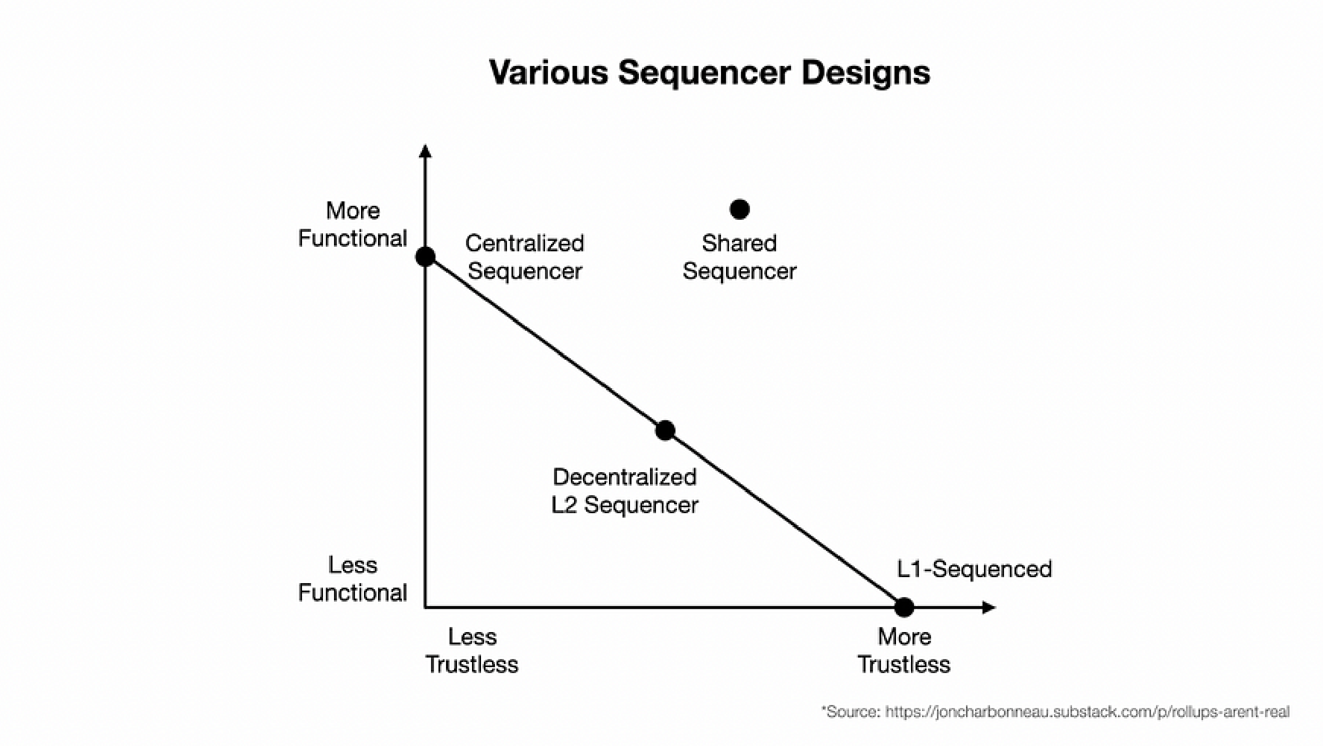
- Sybil resistance mechanism
- Ability to perform the above functions efficiently

Benefits of Decentralised Sequencers

- Improved scalability
    - Reduced latency
- Reduced transaction costs
- Fairness
- Increased participation thanks to economic incentives
- Increased security
- Reduced risk (single point of failure)

Decentralisation Design

From Hacker noon article



Possible approaches to decentralising sequencers

Proof-of-Authority (PoA):

This method involves appointing several specific entities to alternately run sequencers within a PoA framework. While this strategy enhances resistance to censorship and offers the fastest response times, it is not without flaws, primarily the vulnerability to single-point failures.

Base Layer Rollup:

This technique eliminates the need for special sequencers, allowing anyone to present batches to L2. It assigns the tasks of transaction ordering and block proposals to the Data Availability (DA) layer.
Its strength lies in adopting the DA layer's robustness and resistance to censorship.
However, the negatives include

- potential revenue losses to the base layer,
- heightened risk of MEV attacks

- Extended confirmation durations.

Distributed Validator Technology (DVT):

DVT decentralises the role of managing a singular sequencer, spreading it across multiple machines and node operators.
Each operator can provide autonomous attestations with a part of the validator key. While this method can easily integrate with various solutions, it incurs a slight delay.

Shared Sequencing:

This solution enables numerous rollups to utilise a unified, decentralised sequencer network.
This network concurrently processes transactions across multiple chains, ensuring cross-chain interactions, immediate resistance to censorship, and enhanced security at the sequencing level.
Although shared sequencers benefit from serving multiple chains, they remain constrained by the first layer's data processing and transaction ordering capacities.

Initiating New Sequencer Groups:

This strategy involves the formation of a decentralised group of sequencers in a non-permissioned manner, utilising token-based incentives.
Its merit is the enhanced utility of tokens, but it also brings challenges, including increased latency and the complex execution for rollups

In an earlier article about rollups Vitalik also sees the following possibilities

1. Absolute Freedom: This model allows anyone to submit a batch whenever they wish. While being the most straightforward method, it comes with significant downsides. Specifically, the risk of several participants creating and trying to submit batches simultaneously exists, with only one batch ultimately getting accepted. This scenario results in excessive wasted resources in proof generation and unnecessary gas expenditure for batch submissions on the blockchain.
2. Centralised Sequencer: In this approach, a sole sequencer, possesses the exclusive right to submit batches.

An exception exists for withdrawals: typically, a user initiates a withdrawal request, and if the sequencer neglects to include that withdrawal in the forthcoming batch, the user has the right to submit a one-operation batch independently. This method is deemed highly "efficient," yet it hinges on a single entity for ongoing activity.

3. Sequencer Auction: This system involves conducting an auction (perhaps daily) to establish who will hold the sequencer rights for the subsequent period. A notable benefit of this method is its potential to generate funds, possibly managed by a DAO affiliated with the rollup, through mechanisms like MEV auctions.
4. Random Choice from PoS Pool: This method allows anyone to deposit ETH (or possibly a rollup-specific protocol token) into the rollup contract. Batch sequencers are then randomly chosen from among those who have made deposits, with the selection odds being directly proportional to the deposit size. However, a significant disadvantage here is the unnecessary tie-up of vast sums of capital.
5. DPoS Voting: This model operates with a single sequencer chosen through an auction. However, if their performance is subpar, token holders have the privilege to vote them out and initiate a new auction for their replacement. This ensures a balance of power and maintains performance standards.

Further considerations

If a solution relies on L1 interaction as for example the Base rollup idea, this will likely be a bottleneck.
Liveness improvements are dependent on the network configuration and behaviour.

Future directions

Cross-Chain Collaboration:

As an array of blockchains and Layer 2 strategies come into play, the ability for multi-chain collaboration is poised to be a crucial feature of decentralised sequencers. Sequencers of the future could be designed to process transactions on numerous chains in unison, ensuring atomic composability, thereby offering more seamless interactions and enhanced capabilities for users.

Robust MEV Mitigation and Enhanced User Safeguards:

The next generation of sequencers is likely to diminish the effects of MEV and defend against aggressive pricing strategies, safeguarding users more effectively. To achieve this we could use

- Mechanisms for random transaction ordering,
- Equitable fee structures

The role of governance

Increasing participation:

To bolster the integrity and security of decentralised sequencers, upcoming iterations may incorporate more robust governance structures and mechanisms to encourage active involvement.
This enhancement can be realised through initiatives such as

- Token-holder influenced voting,
- Elections for validators, and
- Participant-driven decentralised decision-making processes.

The establishment of more accessible and transparent governance frameworks has the potential to spur community engagement and fuel the system's evolution.

Espresso a sequencer middleware

See article

Espresso functions as middleware between rollups and L1 platforms.
The Espresso Sequencer can be used by both optimistic and validity rollups.
It is also planned to act as an interoperability layer by allowing interaction between an L2 and multiple L1s.