The next version of Aztec will be launched as a fully decentralized network. Community discussion and feedback plays a vital role in decentralization, and one of our goals is to build Aztec as transparently as possible. For key network decisions we will be following a call for proposal method allowing anyone to submit proposals.

Up first on our roadmap: Decentralized Sequencer Selection

We are calling internal and external engineers, researchers, and projects to submit their ideas for discussion. Below you will find more information about how to get involved.

Sequencer Selection Overview

In order to effectively provide sequencer selection proposals and meaningful feedback, it may be valuable to understand the role of the sequencer within the context of Aztec. Here's a basic diagram and brief overview of responsibilities - although we understand your proposal may require some alterations to this list, for example if your proposal includes separating execution from ordering.

[

sequencer selection RFP

2672×1566 284 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/a25dca04bd46b959dba55bc0c75c48dff50e9738.png)

Requirements & Design Considerations

Proposals must meet the following requirements and design considerations. If your proposal doesn't meet all requirements, please call out the missing requirements.

Decentralization:

- Sequencer selection must be sufficiently sybil resistant
- Sequencer selection should not prioritize the best hardware or largest actors
- Hardware requirements for sequencers must be similar to those of Ethereum validators

Liveness:

- Network participants must know in advance who the sequencer is for a given time slot
- A rollup should be created in every given slot to reduce network latency even in periods of low transaction activity

Censorship Resistance:

- Ensure the sequencer selection process is censorship resistant
- Ensure transaction inclusion from a particular sequencer is censorship resistant

Privacy:

- Should allow sequencers the option of anonymity during selection and block submission

Additionally, please consider standard good protocol design principles such as efficiency, complexity, and feasibility of being built within the next 6-12 months.

Responsibilities of the sequencer(s)

Participate in the sequencer selection protocol and if selected execute the following steps:

1. Select pending transactions from the mempool
2. Order transactions into a block
3. Verify all private transaction proofs and execute all public transactions to check their validity
4. Compute the ROLLUP_BLOCK_REQUEST_DATA, which includes: private state database updates, public state updates, and KZG blob commitments (EIP-4844)
5. Compute state updates for messages between L2 & L1 (docs)

6. Broadcast the ROLLUP_BLOCK_REQUEST_DATA to the prover network via the proof pool for parallelizable computation.
7. Build a rollup proof from completed proofs in the proof pool
8. Tag the pending block with an upgrade signal to facilitate forks
9. Publish completed block with proofs to Ethereum as an ETH transaction

For further information please consult the Aztec documentation. It may be worth noting that these are the current responsibilities, and may need to be adjusted based on the proposed solution.

Other Considerations & potential areas of interest

- Compatibility with shared sequencer solutions
- Separating ordering and block building from execution
- Using L1 versus L2 for the sequencer selection protocol
- Proposer-builder separations (refer to this blog post from Vitalik, or Alchemy's explainer)

Submission Format

To ensure consistency and facilitate the review process, kindly adhere to the following submission format:

Title: A concise, descriptive title for your proposal

Summary: A brief summary of your proposal (150-300 words)

Details: Explain the sequencer solution, its components, and its functionality

Comparisons: Explain what makes this solution unique and different from alternative solutions

Feasibility: Explain the ability to implement this solution within the next 6-12 months

Questions: Any outstanding questions

Submissions should be created as a new post on this forum, tagged sequencers

and rfp

. Once the new post is created, please refer back to this RFP and post a short description + link your proposal.

Potentially helpful references

1. Single Secret Leader Election - Dan Boneh & others
2. Leader Election from Randomness Beacons and Other Strategies - a16z
3. SASSAFRAS - polkadot
4. Provable Single Secret Leader Election - Mary Maller
5. Low-overhead secret single-leader election - Justin Drake
6. Secret non-single leader election - Vitalik
7. Endgame - Vitalik
8. Whisk: A practical shuffle-based SSLE protocol for Ethereum - George Kadianakis & others

Grants

Complete proposals may be eligible for a retro-active cash grant and swag.

FAQ

We anticipate that you may have questions regarding the call for proposals. The following frequently asked questions and their corresponding answers should provide some clarification. Otherwise, feel free to contact cooper@aztecprotocol.com, or follow us on Twitter for updates.

Q1. How will a proposal be chosen?

A1. Proposals will be evaluated based on their adherence to the requirements and design considerations, as well as the quality, feasibility, and innovation of the proposed solution. The selection committee, consisting of Aztec Labs employees and possibly external stakeholders, will determine the winning proposal and share the chosen solution publicly.

Q2. Who can submit proposals?

A2. Researchers, developers, and technology enthusiasts with an interest in decentralized sequencer solutions are encouraged to submit their proposals.

Q3. Can I submit more than one proposal?

A3. Yes, you can submit multiple proposals if you have different ideas for sequencer solutions.

Q4. What if my proposal does not fully meet the requirements?

A4. We still encourage you to submit your proposal and participate in the discussion, as your ideas could contribute valuable insights and help shape the final solution.

Questions & clarifications (post publication)

- Due to the nature of UTXO based privacy, and Aztec's use of a nullifier tree, each block must be built from the last confirmed block, with a valid zk proof proving the state transition. If this is not the case, the nullifier non membership proofs would not be valid.

DISCLAIMER

The information set out herein is only conceptual and describes Aztec's future development goals. In particular, the network roadmap is being shared in order to outline some of the plans for Aztec and is provided solely for informational purposes only and does not constitute any binding commitment. Please do not rely on this information for any purpose - the development, release, and timing of any products, features or functionality remains subject to change.