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

Up next on our roadmap: Decentralized Prover Coordination Protocols

Below, you will find more information and learn how to get involved.

Overview

Aztec is foundationally built on privacy-preserving, client-side zero knowledge proofs (ZKPs). These client-side ZKPs get aggregated and eventually submitted to Ethereum L1 for verification. This request for proposals is attempting to define which nodes (provers, in this case) within the Aztec Network get to work on which portions of a block. Now that the sequencer selection protocol Fernet is defined, everyone knows who the leader is for a particular slot, and also knows what the block's contents are. Now the goal is to define what's next, in order to complete the lifecycle of block production on Aztec.

Problem Statement

Each transaction in the Aztec Network is submitted to the mempool with a ZKP of correct execution generated by its sender. Transactions may also run through public functions, which are executed by the sequencer in a Public Virtual Machine (VM), and need to be proven as well. These proofs follow a similar structure to private proofs: each function call is individually proven, and these are accumulated by a public kernel circuit. Without going into too many details, it suffices to say that each transaction will require 2N proofs to be generated, where N is the number of public function calls, of which the first N (VM circuit) can be run in parallel and the next N (public kernel circuit) needs to be run sequentially. The end result is that each transaction is represented by a single proof that covers both its private and public execution.

Each of these individual proofs are then aggregated into a binary tree of so-called "rollup" proofs, where each node in the tree proves the correct execution of its children. The root of the tree is then a proof for the correct execution of all transactions in the block. This root is then submitted to and verified on an L1 contract.

Here is one example of what this could look like, from theB52 sequencer selection proposal:

[

image

2948×1338 287 KB

](https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/afeac88872be5131a480e42475aa526324760e04.png)

We are currently targeting a minimum of 1,024 txs per block, and potentially even scaling with available compute/provers (up to, for example, 61,440 txs per block). While there is still more work to do and benchmarks to run, consider that each proof takes roughly 30 seconds to be generated. It is conservatively estimated that the public VM circuit will require no more than 64gb RAM and 32 cores to generate a proof in that time, while the public kernel and rollup circuits will require 16gb RAM and 8 cores. The proof size is at most 32kb.

Note that generating each public execution proof requires the execution trace for that function, along with network state information. Generating the base rollup proofs (i.e., the leaves of the proof tree) requires the individual transaction proofs and potentially the full state of the network. The merge rollup circuits (i.e., the internal nodes of the proof tree) require only their child proofs, and the root rollup circuit requires its child proofs along with network state roots. This means that most provers will need to be stateful network nodes, or need to receive all the information needed from a trusted source.

Given these computing needs, we want to design a prover coordination protocol, compatible with the currentsequencer selection protocol, that will allow the Aztec Network to generate proofs for its blocks in a reliable way.

Further Reading

This post in our forum covers some ideas and tradeoffs when designing a proving network."Decentralized Proving, Proof Markets, and ZK Infrastructure" from Figment Capital is also a good read on the topic. It'd also be useful to become familiar with the Fernet sequencer selection protocol and the design decisions made within.

If you have any questions along the way, please ask in this forum post!

Requirements

1. Compatible with the Fernet sequencer selection protocol

2. Permissionless
3. Anyone can run an Aztec Prover
4. Anyone can run an Aztec Prover
5. Defining who submits the completed work to L1
6. Is a particular node responsible for submitting to L1? The sequencer? Or is it anarchy?
7. Is a particular node responsible for submitting to L1? The sequencer? Or is it anarchy?
8. Ability to verify who generated which proof
9. Could the protocol potentially slash provers who do not do their jobs properly? Or reward them? Alternatively, is it possible to achieve these goals via other means?
10. Could the protocol potentially slash provers who do not do their jobs properly? Or reward them? Alternatively, is it possible to achieve these goals via other means?
11. Graceful recovery
12. If X% of provers stop suddenly, can the network easily get back to “health”?
13. How long does it take?
14. If X% of provers stop suddenly, can the network easily get back to “health”?
15. How long does it take?
16. Graceful reorg resilience
17. In the event of a reorg, can the network keep moving forward/progressing?
18. Can the network reorg without losing Fernet’s preconfirmations?
19. In the event of a reorg, can the network keep moving forward/progressing?
20. Can the network reorg without losing Fernet’s preconfirmations?
21. Flexible for future cryptography improvements
22. Does this enable the network to always use the latest relevant cryptography? At least, as much as the network’s defined upgrade mechanism allows?
23. Does this enable the network to always use the latest relevant cryptography? At least, as much as the network’s defined upgrade mechanism allows?
24. Scaling with available compute
25. If more compute (i.e., provers) is added to the network, can the protocol expand transaction throughput capacity to match?
26. If more compute (i.e., provers) is added to the network, can the protocol expand transaction throughput capacity to match?
27. Clearly articulated incentives for participants
28. Can participants in this proposal be incentived or rewarded for their efforts?
29. Note that it is not expected that the incentives are fully

defined, moreso to ensure that they are feasible to implement.

- Note that it is not expected that the incentives are fully

defined, moreso to ensure that they are feasible to implement.

- Can other participants (e.g., sequencers) be rewarded in the event of a reorg?
- Can participants in this proposal be incentived or rewarded for their efforts?
- Note that it is not expected that the incentives are fully

defined, moreso to ensure that they are feasible to implement.

1. Note that it is not expected that the incentives are fully

defined, moreso to ensure that they are feasible to implement.

1. Can other participants (e.g., sequencers) be rewarded in the event of a reorg?
2. Clearly articulated protocol parameters
3. Are there any design considerations made within the protocol that may want to be changed over time, such as the maximum block size? Minimum number of provers needed? Minimum stake deposit requirements? The time to build each proof, e.g., the duration of the proving phase? etc.
4. Are there any design considerations made within the protocol that may want to be changed over time, such as the maximum block size? Minimum number of provers needed? Minimum stake deposit requirements? The time to build each proof, e.g., the duration of the proving phase? etc.

Potentially nice to have features

1. Privacy for the partipants in the proving protocol
2. Can others identify that I was a prover for a particular block?
3. What about a particular transaction?
4. Does this change ability to slash, or distribute rewards?
5. Can others identify that I was a prover for a particular block?
6. What about a particular transaction?
7. Does this change ability to slash, or distribute rewards?
8. Ability for sequencers to produce proofs by another means
9. As the current sequencer, if the proving network (&/or protocol) is obviously censoring me, can I still produce a rollup?
10. It is unclear if this is fully necessary and therefore a “nice-to-have” that is potentially worth exploring!
11. As the current sequencer, if the proving network (&/or protocol) is obviously censoring me, can I still produce a rollup?
12. It is unclear if this is fully necessary and therefore a “nice-to-have” that is potentially worth exploring!

Submission Format

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

Title:

A concise, descriptive title for your proposal

Summary:

A brief, easy to understand summary of your proposal (about 300 words)

Comparisons:

Explain what makes this solution unique and different from alternative solutions

Details:

Explain the prover coordionation protocol, its components (including parameters), and its functionality

Questions:

Any outstanding questions

Submissions should be created as a new post on this forum, tagged provers and RFP. Once the new post is created, please refer back to this RFP and post the link to your proposal as a comment.

Submission Deadline

The deadline for submissions is Friday November 3rd, 2023.

Grants

Complete proposals may be eligible for a retroactive cash grants and swag.

FAQs

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 post a question in the forum, contact cooper@aztecprotocol.com, or follow us on Twitter (or X…? are we saying that now?) 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 solutions. The selection committee, consisting of Aztec Labs team members and possibly external stakeholders, will determine the winning proposal and share the chosen solution publicly.

Q2. Who can submit proposals?

A2. Anyone!

Q3. May I submit more than one proposal?

A3. Yes, you may submit multiple proposals if you have different ideas for proving coordination protocols.

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.

A note on network incentives & fees

The fee structure for the network is still being designed, but it is safe to assume that each transaction will carry a fee that should cover all its costs, proving included. Inflationary block rewards are also a valid option to consider as part of the proposal.

Acknowledgments

Thank you to Palla for your contributions to this post.

Thank you to Jakob & Jamsheed at BlockScience for your feedback as well.

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.