Request for integration: Provers

For additional context please see the slides and recording from the July 31st Aztec Proving Ecosystem Community Call.

We are inviting zero-knowledge proving infrastructure providers who wish to integrate with the upcoming Aztec Network to respond to the following request for integration. As a validity rollup, Aztec submits zero-knowledge proofs to L1 to verify the state transition after the execution of the transactions in a sequence of blocks. As a fully decentralized network Aztec will depend on a decentralized fleet of provers, which could range from independent infrastructure providers to established proving marketplaces, to generate proofs. Coordination amongst provers will eventually be conducted via a proof-boost-like model using the Sidecar protocol, as was defined by thecorresponding RFP for decentralized prover coordination.

As part of the development process, we are opening up a permissioned testnet for provers interested in generating proofs for the Aztec Network, incentivized via a contest that will reward the participants based on the rate and speed of blocks proven.

Scope of the integration

During this initial integration phase, we will not

be testing the Sidecar sequencer-prover coordination mechanism. Instead, we will focus on ensuring that infrastructure providers can successfully generate proofs for the network when called upon.

To do this, we will spin up a permissioned version of the Aztec network on top of an Ethereum mainnet fork, where any whitelisted prover can prove any block, and any block can be proven an arbitrary number of times. Each proof will include an identifier of the entity that generated the proof, so we will be able to track who has proven each block and when. Aztec will run a centralized sequencer that will post small 4-transaction blocks at regular intervals of 1 minute to an L1 fork (details subject to change) to be proven. Provers will download and process these blocks, and upload the resulting rollup proofs back to the L1 fork.

Constructing a rollup proof

For a more in-depth explanation of Aztec circuits please seethe docs.

Creating a rollup proof for Aztec involves running multiple circuits. Each Aztec transaction carries a client-generated proof using the ClientIVC proving scheme, which is converted to a Honk proof via a tube

circuit once picked up by a prover. In addition, each transaction may involve public functions to be executed, which require one or more iterations of the Aztec Virtual Machine

and public kernel

circuits to be run.

Then, transactions in a sequence of blocks are aggregated into a tree-like structure, composed of base

, merge

, block root

, block merge

, and root rollup

circuits. This means that each rollup proof requires multiple inner proofs, some of which can be run in parallel, while others must be recursively aggregated.

For this first prover test network, the block root and block merge circuits will not be used. Each block will be individually proven: one proof will prove the validity of a single block.

Aztec’s prover node

The Aztec Network client can be configured to run as a prover node

, which as it stands today will automatically monitor L1 for unproven blocks, re-execute their transactions using its local state, orchestrate their proving into a single root rollup proof, and upload the proof to L1. This software is open source and we will make it available to all participants, along with documentation on how to run it.

[

image

2370×1455 247 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aztec/original/2X/9/9342d464c6a29aa96da107cb7b2ab7369e019707.png)

The prover node relies on an internal prover orchestrator

module that breaks down a given block into all the inner proofs that need to be generated in order to arrive at a root rollup proof, following the structure described in the previous section. The orchestrator fans out individual proving jobs to external prover agents

. Prover agents are stateless processes that poll the prover node for job definitions, and return the resulting proof. Prover agents use Aztec's ACVM to generate partial witnesses, and the barretenberg cryptographic library via its CLI interface for generating proofs under the hood.

Integrating with existing infrastructure

For more information on the prover node and potential integration, check outthis guide.

While it is possible to simply run Aztec's prover node software for generating proofs for the protocol, we expect already-established provers to integrate the prover node with their existing tech stack to ensure reliability. The integration contest will include a category exclusive for prover networks who have built custom integrations with their infrastructure

.

For custom integrations, we recommend leveraging the interface between the prover orchestrator

and prover agent

for integration. Infrastructure providers can rely on Aztec's prover node for coordination and orchestration, and develop custom prover agents that pull job definitions from the prover node's HTTP interface and execute them by calling into the ACVM and Barretenberg. The existing prover agent can act as a reference implementation.

Alternatively, integrations can replace the prover orchestrator

within the prover node with a custom implementation that builds on top of existing infrastructure. While this interface is not as clearly cut out as the prover agent's, we'll be happy to provide support to those who want to take this route.

As the network matures, we expect fully custom solutions to be developed in parallel with Aztec's prover node software, in order to leverage the differentiating aspects of the different proving service providers, and have structured this contest to enable a diverse set of entrants.

Hardware requirements

Initial estimates for hardware requirements based on our internal benchmarks show that a prover node can run on a 2-core 4gb RAM machine. Prover agents, on the other hand, require more powerful hardware since they perform the actual proving. Proving is CPU-bound and memory-hungry, and we are currently working with 16-32 core machines with 96-128 gb RAM.

We expect to share more up-to-date benchmarks, which include running times for proving each circuit, in the upcoming weeks.

Timeline and contest

The dates below are subject to change. Any modifications will be communicated in this thread.

- August 9th : Registration Closes
- Week of August 12th: Testing environment live
- Week of September 2nd: Contest runs for the week
- Week of September 9th: Winners announced

How to participate

Given this initial integration phase will be permissioned, we ask for everyone interested in participating to pleasefill in this

form.

Fill in this form to express interest in participation before August 9th.

We'll include all participants in a telegram group for internal coordination and sharing information about the test network they can connect to. Note that we may limit the total number of participants for this initial integration phase should we receive more applications than we can manage, but we'll open the pool for future networks.

On the week of August 12th participants can expect a permissioned network to be available for them to start testing their respective integrations. During this period, we'll share more documentation on running and extending Aztec's prover node, and provide support to integrators via telegram and this forum.

After having time to test their integrations, the contest will officially start on September 2nd, when we'll monitor the number of blocks produced by each team, as well as how fast they arrive at L1 after the pending block is proposed.

The contest period will last until September 6th. Based on the results, Aztec will announce winners in two categories

: one for infrastructure providers running Aztec's prover agents without modifications, and another for those who have built custom integrations and modified the code to their network.

To be eligible for the second category, we will require that a github repository is shared with Aztec Labs containing the custom integration.

Winners will be judged based on the number of blocks produced within a 20 minute timeout from the block being proposed, though the L1 contract will accept proofs without a time restriction.

In the event of a tie, the prover with the fastest overall proving time will win. Note that, in the event of a disruption caused by a bug in Aztec network software itself, we may remove certain time windows from consideration for the contest at our discretion.

Winners will receive a $5,000 cash prize, and bragging rights for helping decentralize the world's first privacy focussed L2. Aztec Labs reserves the right to appoint more winners if desired.

Next Steps

Further test networks will be announced after September 20th. Stay tuned for more details.

We welcome all participants and new entrants to contribute to these networks as we roll out incremental upgrades to the Aztec network over the rest of the year.

EDIT: We ask that all interested participants fill outthis form rather than commenting on this post.

Disclaimer

The information set out herein is for discussion purposes only and does not represent any binding indication or commitment by Aztec Labs and its employees to take any action whatsoever, including relating to the structure and/or any potential operation of the Aztec protocol or the protocol roadmap. In particular: (i) nothing in these posts is intended to create any contractual or other form of legal relationship with Aztec Labs or third parties who engage with such posts (including, without limitation, by submitting a proposal or responding to posts), (ii) by engaging with any post, the relevant persons are consenting to Aztec Labs' use and publication of such engagement and related information on an open-source basis (and agree that Aztec Labs will not treat such engagement and related information as confidential), and (iii) Aztec Labs is not under any duty to consider any or all engagements, and that consideration of such engagements and any decision to award grants or other rewards for any such engagement is entirely at Aztec Labs' sole discretion. Please do not rely on any information on this forum for any purpose - the development, release, and timing of any products, features or functionality remains subject to change and is currently entirely hypothetical. Nothing on this forum should be treated as an offer to sell any security or any other asset by Aztec Labs or its affiliates, and you should not rely on any forum posts or content for advice of any kind, including legal, investment, financial, tax or other professional advice.