Core Components

Aztec Labs is building a layer 2 rollup on Ethereum focused on 3 things:

- Data privacy
- Confidentiality
- Trustlessness

Data privacy

Data privacy refers to the ability of Aztec smart contract to have private (encrypted) state. Aztec abstracts away many of the complexities associated with managing private state, providing developers with an interface that feels familiar, but is much more powerful.

Confidentiality

Confidentiality is the ability of Aztec smart contracts to execute private functions and transactions. Aztec provides a secure, private environment for the execution of sensitive operations, ensuring private information and decrypted data are not accessible to unauthorized applications.

When a user sends a private transaction on the network, the only information that an external observer can infer is that a transaction was sent. Transaction data, the sender, and the recipient can all be obfuscated.

Aztec achieved this level of privacy by leveraging a Private eXecution Environment (PXE). This software runs client-side, for example in a browser, and is responsible for managing private keys, encrypting and decrypting data, and executing private functions. The PXE is also responsible for generating proofs of private function execution, which are then sent to the sequencer for inclusion in the rollup.

Trustlessness

Aztec is building a permissionless, censorship resistant, peer-to-peer network. It aims to be credibly neutral, where the same transparent rules apply to everyone, enforced by the protocol.

Aztec will have a network of sequencers that stake tokens to participate in the network. Sequencers are responsible for aggregating transactions into a block, generating proofs of the state updates (or delegating proof generation to the prover network) and posting it to the rollup contract on Ethereum, along with any required public data for data availability.

High level network architecture

An overview of the Aztec network architecture will help contextualize the concepts introduced in this section.

Aztec.js

A user of the Aztec network will interact with the network through Aztec.js. Aztec.js is a library that provides APIs for managing accounts and interacting with smart contracts (including account contracts) on the Aztec network. It communicates with thePrivate eXecution Environment (PXE) through aPXE implementation, allowing developers to easily register new accounts, deploy contracts, view functions, and send transactions.

Private Execution Environment

The PXE provides a secure environment for the execution of sensitive operations, ensuring private information and decrypted data are not accessible to unauthorized applications. It hides the details of thestate model from end users, but the state model is important for Aztec developers to understand as it has implications forprivate/public execution andL1/L2 communication . The PXE also includes theACIR Simulator for private executions and the KeyStore for secure key management.

Procedurally, the PXE sends results of private function execution and requests for public function executions to thesequencer , which will update the state of the rollup.

Sequencer

The sequencer aggregates transactions into a block, generates proofs of the state updates (or delegates proof generate to the prover network) and posts it to the rollup contract on Ethereum, along with any required public data for data availability.

Further Reading

- The state model
- Accounts
- Aztec Smart Contracts
- Transactions
- Communication between network components Edit this page

Previous Vision Next Concepts