What is Aztec?

Aztec is an L2 that brings programmable privacy to Ethereum.

Private Smart Contracts on Aztec

A smart contract on Aztec is a collection of functions, written as ZK-SNARK circuits. These circuits can have different modes of execution:

1. Private Functions -- can read and write private state, read historical public state, consume or send messages to / from Ethereum, and read Ethereum state. They can call other private functions in the same contract, or other contracts, and can call public functions.
2. Public Functions -- can read and write public state, write private state, consume or send messages to / from Ethereum and read Ethereum state. They can call other public functions on the same or other contracts.
3. Portal Contracts -- these are contracts on Ethereum that can receive messages from Aztec or send messages to Aztec from Ethereum contracts.

Using these different modes of execution, developers can build applications with user privacy, data privacy and code privacy.

- User privacy - transactions may not reveal information about the sender or the recipient.
- Data privacy - transactions may not reveal information about the payload of the transaction, e.g., the asset or value being transacted.
- Code privacy - transactions may not reveal the program logic.

Watch Zac, CEO of Aztec, describe our approach to building a privacy preserving smart contract blockchain.

Private-public Composability

You can watch Mike, Aztec PM, talk about public-private composability in Aztec at Devcon here.

How Aztec is being built

Aztec is being built and launched as a credibly neutral, decentralized network. The protocol is being developed as open source software by Aztec (the company) and our community. Together we are designing, building and auditing much of the software that will be run by network stakeholders such as infrastructure providers in order to create Aztec.

Contributors to Aztec uphold many of the values of the Ethereum community -- building in public, a rigorous commitment to open source and a goal to build a permission-less, censorship resistance system.

Noir

Noir is a domain specific programming language for writing zero-knowledge circuits. On Aztec a smart contract is a collection of circuits that developers write using Noir.

You can find more information and resources for learning about Noir smart contracts on this page .

Cryptography

To support Aztec's rollup, our cryptography team is building Honk , a cutting edge proving system that makes Aztec possible, under the Apache 2.0 License.

Participate

Keep up with the latest discussion and join the conversation in the Aztec forum or Discord server . Edit this page

Previous Welcome Next Vision