ACIR Simulator

The ACIR Simulator is responsible for simulation Aztec smart contract function execution. This component helps with correct execution of Aztec transactions.

Simulating a function implies generating the partial witness and the public inputs of the function, as well as collecting all the data (such as created notes or nullifiers, or state changes) that are necessary for components upstream.

Simulating functions

It simulates three types of functions:

Private Functions

Private functions are simulated and proved client-side, and verified client-side in the private kernel circuit.

They are run with the assistance of a DB oracle that provides any private data requested by the function. You can read more about oracle functions in the smart contract sectionhere .

Private functions can call other private functions and can request to call a public function. The public function execution will be performed by the sequencer asynchronously, so private functions don't have direct access to the return values of public functions.

Public Functions

Public functions are simulated and proved on thesequencer side, and verified by thepublic kernel circuit .

They are run with the assistance of an oracle that provides any value read from the public state tree.

Public functions can call other public functions as well as private functions. Public function composability can happen atomically, but public to private function calls happen asynchronously (the private function call must happen in a future block).

Unconstrained Functions

Unconstrained functions are used to extract useful data for users, such as the user balance. They are not proved, and are simulated client-side.

They are run with the assistance of a DB oracle that provides any private data requested by the function.

At the moment, unconstrained functions cannot call any other function. It is not possible for them to call constrained functions, but it is on the roadmap to allow them to call other unconstrained functions. Edit this page

Previous Private Execution Environment (PXE) Next Circuits