Oracle Functions

This page goes over what oracles are in Aztec and how they work.

Looking for a hands-on guide? You can learn how to use oracles in a smart contrachere .

An oracle is something that allows us to get data from the outside world into our contracts. The most widely-known types of oracles in blockchain systems are probably Chainlink price feeds, which allow us to get the price of an asset in USD taking non-blockchain data into account.

While this is one type of oracle, the more general oracle, allows us to get any data into the contract. In the context of oracle functions or oracle calls in Aztec, it can essentially be seen as user-provided arguments, that can be fetched at any point in the circuit, and don't need to be an input parameter.

Why is this useful? Why don't just pass them as input parameters? In the world of EVM, you would just read the values directly from storage and call it a day. However, when we are working with circuits for private execution, this becomes more tricky as you cannot just read the storage directly from your state tree, because there are only commitments (e.g. hashes) there. The pre-images (content) of your commitments need to be provided to the function to prove that you actually allowed to modify them.

If we fetch the notes using an oracle call, we can keep the function signature independent of the underlying data and make it easier to use. A similar idea, applied to the authentication mechanism is used for the Authentication Witnesses that allow us to have a single function signature for any wallet implementation, seeAuthWit for more information on this.

Oracles introducenon-determinism into a circuit, and thus areunconstrained . It is important that any information that is injected into a circuit through an oracle is later constrained for correctness. Otherwise, the circuit will beunder-constrained and potentially insecure!

Aztec.nr has a module dedicated to its oracles. If you are interested, you can view them by following the link below:

oracles-module /// Oracles moduleSource code: noir-projects/aztec-nr/aztec/src/oracle.nr#L1-L3 Edit this page

Previous How to emit an eventNext Inbuilt Oracles