Private Kernel Circuit

This circuit is executed by the user, on their own device. This is to ensure private inputs to the circuit remain private!

- Verifies a user's signature.
- Hides the user's address.
- Verifies an app's proof - i.e. a proof which has been output after the execution of some function in an Aztec.nr Contract.
- Performs private state reads and writes.
- Exposes (forwards) the following data to the next recursive circuit:* new note hashes;
  - new nullifiers;
  - new messages to L1 contracts;
  - private call stacks: hashes representing calls to other private functions;
  - public call stacks: hashes representing calls to other public functions;
  - events;
  - all data accumulated by all previous private kernel circuit recursions of this tx;
- Hides which private function has been executed, by performing a zero-knowledge proof of membership against thecontract tree
- .
- Ensures the entire stack trace of private functions (for a particular tx) adheres to function execution rules.
- Verifies a previous 'Private Kernel Proof', recursively, when verifying transactions which are composed of many private function calls.
- Optionally candeploy
- a new private contract.

Note:This is the only core protocol circuit which actually needs to be "zk" (zero-knowledge)!!! That's because this is the only core protocol circuit which handles private data, and hence the only circuit for which proofs must not leak any information about witnesses! (The private data being handled includes: details of the Aztec.nr Contract function which has been executed; the address of the user who executed the function; the intelligible inputs and outputs of that function). This is a really interesting point. Most so-called "zk-Rollups" do not make use of this "zero-knowledge" property. Their snarks are "snarks"; with no need for zero-knowledge, because they don't seek privacy; they only seek the 'succinct' computation-compression properties of snarks. Aztec's "zk-Rollup" actually makes use of "zero-knowledge" snarks. That's why we sometimes call it a "zk-zk-Rollup", or "actual zk-Rollup". Edit this page

Previous Circuits Next Public Kernel Circuit