In Aztec3, private state will be wrapped in a commitment

, which looks something like:

h(contract_address, h(storage_slot, value, owner, salt, nonce))

The value

itself might also be a hash of data. For example if it represents a struct, it'll be a hash of the struct's data members.

We need a way of transmitting the preimage of the commitment

, and the preimage of the value

, to the owner

of the private state.

Questions:

- Do we broadcast an encryption of the preimage?
- How would we broadcast the data? L1? Nym? Other DA solution?
- Which encryption scheme to use?
- Do we enable devs to control which encryption scheme to use?
- If so, we'd need to inject custom decryption code into the Private Client on a per contract

basis.

- If so, we'd need to inject custom decryption code into the Private Client on a per contract

basis.

- Encrypted preimages of struct / array data will be variable in length, which will leak information about the function that's been executed. Can we pad that data?
- Do the preimages of commitments always follow the default layout as prescribed by Noir++?
- Or, do we enable devs to design their own commitment preimages?

- Or, do we enable devs to design their own commitment preimages?

- Do we emit the encrypted data as public inputs of the circuit?
- Do we add constraints within the circuit to verify correct encryption?
- Perhaps it's actually always in the tx sender's interest to provide the preimage data to the owner?
- For example, in Aztec Connect, if the sender doesn't provide a preimage to the recipient of value, it can be interpreted by the recipient that they were never paid.
- If so, maybe we can trust that they transmit it somehow, and the protocol doesn't need to expose a rigid way of transmitting the data.

- For example, in Aztec Connect, if the sender doesn't provide a preimage to the recipient of value, it can be interpreted by the recipient that they were never paid.
- If so, maybe we can trust that they transmit it somehow, and the protocol doesn't need to expose a rigid way of transmitting the data.