Working with the CreditScore feedback partner we realized that in the current design of the token contract, I can receive notes, but not know who sent it to me. This becomes important when for example you receive money from friends but aren't sure which ones are yet to pay you back OR in a credit score system, I may want to prove that I indeed got the salary from Aztec and not meme company.

in general:

- from

might want to prove that they sent the note

- to

might want to prove that from

sent them a note

Design 1 - Add from

field in ValueNote

I first thought this made the ValueNote like an NFT since notes become different if they are from different senders. But in our UXTO model, this isn't true as I can spend the value note as long as I am the owner. And I can always combine multiple notes into one and change from

to my address.

However, this increases the cost of publishing the encrypted log to L1 by a Field

element.

Note that, from

can be optional i.e. you can pass a 0x0 if you truly don't want to reveal your address.

However, there is nothing stopping anyone from lying about from

.

Design 2 - Add from

and signature

to ValueNote

You sign the preimage of the note {from, to, amount} with your private key and add this signature as part of the note.

This increases the cost of the encrypted log by yet another field.

Design 3 - Create a new note revealing the from address + a signature

This is nice because it can be strictly optional to create such a note.

But of course, there is a limit on how many notes we can create in a transaction.

Design 4 - Use Emit encrypted log to send sensitive information

If we change how we process events i.e. make it such that emit_encrypted_log works for non-notes too, we could use it as a message-passing mechanism.

This has been discussed in detail in the offsite to enable unencrypted private notes to be added automatically here and involves refactoring events to emit when log is about a note and when it is not.

Any other good designs?

Shoutout to @alexghr for feedback.

third parties who engage with such posts (including, without limitation, by submitting a proposal or responding to posts), (ii) by engaging with any post, the relevant persons are consenting to Aztec Labs' use and publication of such engagement and related information on an open-source basis (and agree that Aztec Labs will not treat such engagement and related information as confidential), and (iii) Aztec Labs is not under any duty to consider any or all engagements, and that consideration of such engagements and any decision to award grants or other rewards for any such engagement is entirely at Aztec Labs' sole discretion. Please do not rely on any information on this forum for any purpose - the development, release, and timing of any products, features or functionality remains subject to change and is currently entirely hypothetical.