Suppose Alice wants to do an atomic exchange with Bob. If she can swap two tokens in a DEX at a certain price, then she atomically reveals sensitive offchain information (e.g. a web2 password) to Bob. If she can't get her price, the password should never be revealed.

Let's have a DEX contract on Aztec with a private → public swap function. The private function creates a note for Bob containing the password, and the public function executes the swap.

As a consequence a private function CANNOT

accept a return value from a public function. (source)

Alice can't dispatch the public function and then

execute the private function based on the results of the public function. Aztec prioritizes the execution of private functions before

public functions, so this can't work.

The other option is for Alice to execute the private function and then dispatch a public function that reverts if Alice doesn't achieve her price, like the L2 access control example.

Be mindful that if part of a transaction is reverting, say the public part of a call, it will revert the entire transaction. Similarly to Ethereum, it might be possible for the block builder to create a block such that your valid transaction reverts because of altered state, e.g., trade incurring too much slippage or the like. (source)

My question is: if the public transaction were to revert, is there any risk of the password getting leaked by Alice having already provided the note hash? And at what point exactly can Bob first discover and decrypt the note?

Malicious sequencer

Could the sequencer include her note hash in the tree, even if it would make the block invalid?

What if Bob were the sequencer? Could he decrypt the note without needing to include it in a valid block?

Would it be better practice to insert a nullifier instead of reverting, or same difference?

L2 reorg

Suppose the public function initially succeeds and were included in block N, which gets proposed and revealed, but not proven. Then, suppose the public function were re-executed, reverted

, and included in block N', which were proven in lieu of block N.

Could Bob decrypt the note when block N gets revealed?

There was some discussion on removing build-ahead and the risk of L2 reorgs, but it's slightly ambiguous from@cooper-aztecLabs's response whether this will be done or not (or if it's even relevant to this question).

L1 reorg

I would need to know more about when Bob is first able to discover and decrypt the note in order to ask an informed question about L1 reorgs.