zkConfidentialBridge

Concepts

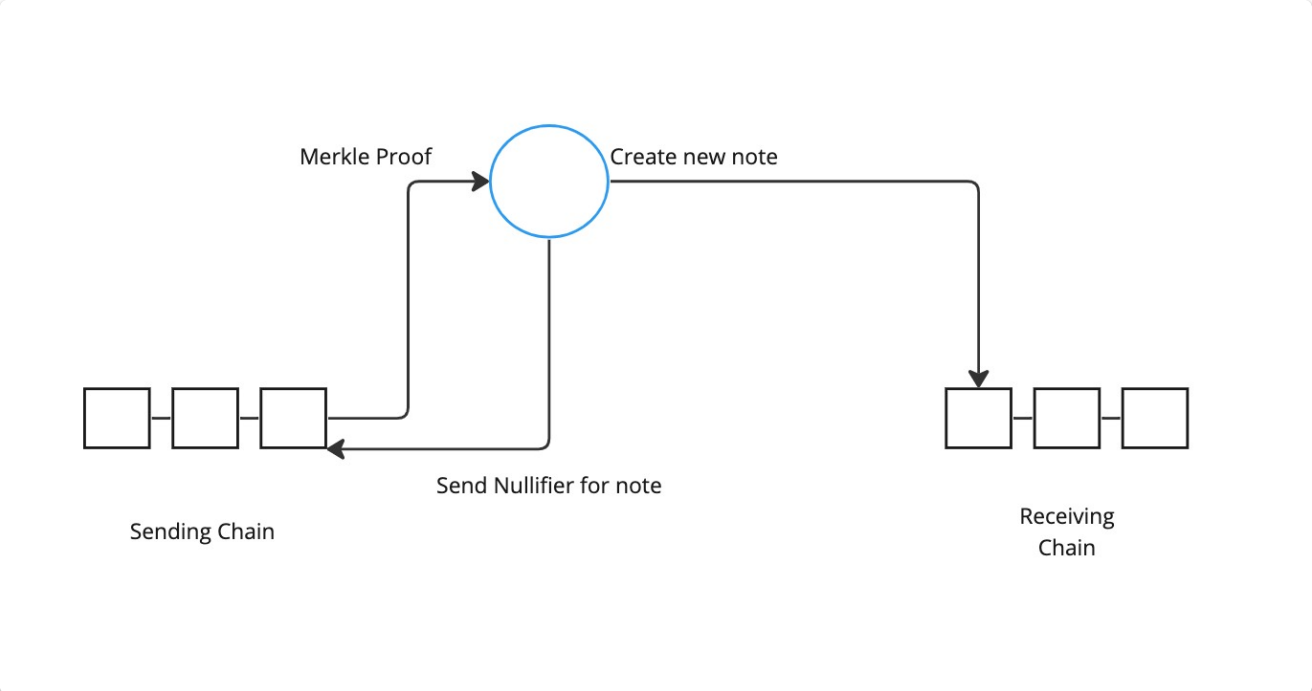
Tokens involved

The tokens involved are zkERC20 tokens following the proposed confidential token standard EIP-1724

Token Transfer

Tokens are spent on the sending chain and a new note is created on the receiving chain

The process is carried out by an operator.



The operator will receive the note fron a note commitment tree on the sending chain and (if the authorisation is correct) will issue a nullifier on the sending chain and create a new note of equivalent value on the receiving chain. The authorisation can be set up via a confidential approve function on the zkERC20.

Operator incentivisation

The operator is rewarded for maintaining the bridge by taking fees (and perhaps MEV) , but they are required to supply a stake If they fail to transfer a token their stake will be slashed.

Proofs needed.

Token transfer
The operator will create a proof that the process of
1. Nullifying the note on the sending chain
2. Creating a new note on the receiving chain
has been carried out correctly

This is in addition to the proofs needed for general confidential token transfer.
Merkle proofs are also needed to check set membership for the notes and the nullifiers.

Merkle trees

A tree of note commitments and a tree of nullifiers is needed.
It is possible that this could be an off chain data structure that is replicated by the operators.