By Nobitex Labs (@keyvank, @ostadgeorge et al)

We are thrilled to introduce our proof-of-concept implementation of EIP-7503, Burnth, which simply is an ERC-20 smart-contract that can be minted by providing proofs-of-burn. We are using Circom/SnarkJS for implementing our circuits and building zk-proofs.

Our circuit simply checks if there is an account with an unspendable address in the stateRoot of a block, by verifying a Merkle-Patricia-Trie proof inside a R1CS circuit. We use a modified version of MPT proof verifier which significantly reduces the number of constraints needed. We are also not verifying the entire MPT proof in a single circuit, but we are chaining some subcircuits together by commiting into intermediary layers, and checking if the commitments (Which are fed as public-inputs) are chained together. This results in two Groth16 circuits, with parameter files of size around 500MB, and it takes around 1 minute to generate a private-proof-of-burn on a laptop.

You can find the codes here:GitHub - nobitex/burnth: Ether, but burnt

For more info on EIP-7503 itself:https://eip7503.org