Questions

Xun Zhang Bingsheng Zhang
Zhejiang University, CHN
22221024@zju.edu.cn bingsheng@zju.edu.cn

March 19, 2024

1 Questions about zkBridge

- Q: Does blkH_r-1 contain a Merkle tree of the public keys used to verify the signatures in the proof for blkH_r? This would allow us to keep everything succinct.

  A: **YES**(according to Cosmos code).

  "In Cosmos, each block header contains about 128 EdDSA signatures (on Curve25519), Merkle roots for transactions and states, along with other metadata, where 32 top signatures are required to achieve super-majority stakes."(sec. 6.1)

  See it in tendermint pkg: code

  ValidatorsHash tmbytes.HexBytes ‘json : "validators_hash"‘ validatorsforthecurrentblock
  NextValidatorsHash tmbytes.HexBytes ‘json : "next_validators$_{h}$ash"‘ validatorsforthenextblock

- Q: Should we reuse existing building blocks or do we want to design our own scheme?

  A: I think it depends on the blockchains we want to bridge. Since there are many blockchains use diverse signature schemes, the performance requirements for the ZK-SNARK are also different. Even in some scenarios, such as bridging from Ethereum to other EVM-compatible blockchains, there is no need to use zksnark(see sec. 6.4).