Overview

I’ve been playing around with the idea of bridging data between a side chain and the ethereum mainnet.

The setup is 2 parallel chains, ethereum mainnet and some other chain where it’s actors are bonded on the ethereum mainnet.

The challenge is how to approve the un-bonding on the side chain but actually withdraw the bond on mainnet.

Details

- A contract on the ethereum chain will have an “admin” pubkey which can perform a restricted action like releasing a bonded actor.
- The admin key is generated via DKG by a random committee with 2/3 threshold.
- Committee size and selection is similar to eth2 spec (size and RANDAO).
- Bonded actors on the side chain will randomly get selected to a committee to sign restricted actions.
- The committee from Epoch E-1 will publish a signed pub admin key which was generated by a future committee at epoch E. That signed pub key will switch the admin key for epoch E.
- To un-bond an actor, he will request to be un-bonded on the side chain. If the committee at that epoch agrees on the validity of his request it will sign it.
- The bonded actor will publish to the ethereum chain the signature along with the request.
- The bond is released if the signature verifies against that epoch’s admin pub key.
- Using BLS signatures, the verification will require 2 pairing operations.
- Aggregating signatures as part of a shared secret is easily implementable.
- Switching the admin key between epochs should only be done on a finalised state on the side chain, in case of a re-org.

Instead of restricting ourselves to a simple use-case, the state root of the side chain can be published via the committee which can expand the restricted operations possible on the mainnet via Merkle proofs.