Authors and attributions

Blagoj and Barry WhiteHat.

Onur implemented the RLN construct.

Thanks to Thore for reviewing and suggestions.

Introduction

Currently validators in the ETH2 network are public and although their IP addresses are not explicitly known, it is easy to obtain with metadata analysis.

Intorducing a private p2p network in ETH2 would lead to massive DoS attacks against validators. Because in private p2p networks it's not clear who to block in response to spam. In transparent p2p networks, IP based blocking is enough to mitigate most spam attacks.

RLN (Rate limiting nullfier) is a construct based on zero-knowledge proofs that allows for private p2p networks that are spam resistant.

In RLN users sign up with public key. Every message they send also reveals a small portion of their private key. If they send too many messages per epoch their private key is revealed. At the end of every epoch their private key shares are updated.

You can read more about RLNhere.

Description

This messaging service imlements the gossipsub-rln protocol for the p2p pubsub networking layer, and is separate from the gossipsub-v1.1 pubsub protocol that ETH2 validator clients use for consensus message propagation.

The ETH2 validators will have two connections for two different pubsub protocols, one for the default gossipsub v1.1 for consensus message propagation and one for gossipsub-rln for the private messaging.

The private message channel should use the same underlying discovery service (discv5) as the consensus message propagation service (the native gossip domain) as it provides additional security (we can add add additional key:value pairs for the ENR for extra security and validation, if we need to).

Using gossipsub-rln will also enable spam/DDoS protection for the private messaging channel.

Rationale

The implementation consist of three parts:

- Smart contract which serves as a registry, and is only used for storage and data availability (i.e LazyLedger approach)
- Private, spam resistant PubSub protocol on a p2p network - gossipsub-rln, which is used for private message propagation part between the validators of the RLN group.
- REST API with a single endpoint which provides list of removed members private keys - used for correctly reconstructing the membership trees of the later joining participants

The blockchain serves only as a data availability layer. It is only used to register an account. Each registeration contains:

1. A signature from ETH2 validator
2. RLN public key

The nodes watch this smart contract, for each validator who signs up, they check:

1. The BLS signature is correct
2. The user has not already signed up
3. If so they insert them into the RLN group.

If a user is spamming, their private key can be revealed. This is gossiped to other peers who remove the spammer from their local membership tree.

Conclusion

Here we proposed a private ETH2 p2p layer that allows for both privacy and spam resistance. It requires on chain interaction only for registration which means its scalable.

One possible concern is having to come to conesnsus on slashed users.

Implementation draft

We provide implementation draft for this idea, which can be found here:https://hackmd.io/@blagoj/ryGyO8C-Y