Link to the analysis

At PSE team we've (me, @AtHeartEngineer and @barryWhiteHat ) researched the problem of Ethereum consensus layer validator anonymity in detail as an important problem in general but also as an application for RLN.

The problem itself is sound, as currently ethereum validators are not anonymous andit is easy to map validator IDs to physical IP addresses of beacon nodes (validator nodes and beacon nodes are usually run on the same machine for home stakers) and do DDoS attacks on these nodes in order to destabilise the network. Especially problematic is the current consensus layer design where the block proposers for an epoch are revealed in advance.

Few solutions for providing stronger validator anonymity and avoiding DDoS attacks are being worked on, usually each solving the problem from different angle. One such proposal for a solution is WHISK, which tries to solve the problem at the consensus layer itself.

We've researched a solution that do not do any changes at the consensus layer, but deals with changes at the network layer. The initial reasoning is that network layer changes are easier to accomplish and are less tightly related to the application logic (consensus layer). Additionally the network level changes could be opt-in.

The general idea about the solution is to obfuscate the beacon node through which the message is propagated to the p2p network. This could be done by using various different tools, but we've chosen to experiment with Dandelion++ because of simplicity and low latency purposes (in comparison with other solutions).

The idea is to create a private pre-network which serves for obfuscation, to which only validators could send messages. At a random point (according to the Dandelion++ protocol), the message would get published as a normal consensus layer gossipsub p2p message. Additionally we would add RLN as a spam prevention mechanism for this private pre-network (stronger spam prevention than gossipsub peer scoring and extended validators + rate limiting at protocol level).

However because of latency constraints we've come to a conclusion that this proposal is infeasible for the Ethereum consensus layer (at least not for any strong anonymity guarantees).

Our main conclusion is that network changes are hard, the benefits added are only marginal and the complexity for these benefits is huge. Solutions such as WHISK, which approach the problem at it's root (consensus layer changes) although complicated are most likely the right way of solving this problem long term (except other changes are made at the consensus layer which relax the latency constraint). Additionally there are some other applicable solutions for in the short term, such as leveraging multiple beacon nodes instead of one, etc.

The reasons for this conclusion are the following:

- Ethereum consensus layer latency constraints are very tight and validator reward and penalties are dependent on the latencies (anonymity solutions that add one more second of latency are likely irrelevant, probably even less than that, depending on the network state)
- In order to provide anonymity on network layer, additional steps are needed. This could be extra hops, encryption or some thing else. These extra steps add additional latency and complexity. Dandelion++ + RLN in order to provide sufficient anonymity guarantees add multiple seconds of delay.
- The gossipsub protocol is designed with peer scoring and extended validators in mind. Those can't be completely replaced by RLN for spam prevention, as those are not only used for spam prevention. This would likely require an additional effort to make sure the gossipsub p2p protocol works correctly, and that the implemented changes do not open other vulnerabilities.

The idea in general might not be applicable to the Ethereum consensus layer, but it can be applied to p2p applications that require anonymity and are not latency constrained (the latency added from this solution is acceptable.

Additionally RLN can be used as a spam prevention and rate limiting mechanism for applications that require anonymity. In anonymous environments where rate limiting and frequency-based objective spam prevention is desired, the regular spam prevention rules do not apply and RLN can help a lot in these scenarios.