Special thanks to @adlerjohn and @liangcc for comments and feedback

Abstract

: We explore how a hybrid p2p and client-server network might improve validator privacy in ETH2.0. We go through considerations for implementation and the tradeoffs in validator UX.

Motivation

ETH2.0 is a P2P network built on top of Libp2p. It uses a gossip-based pubsub algorithm to propagate messages between peers in the network and uses Discv5 for peer discovery. At the time of this writing, there are no provisions for validator privacy. As such, all network-level activities of the validators in ETH2.0 are public and susceptible to a wide range of both network-level attacks and out-of-band attacks such as bribery attacks. Further, many of the better anonymous networking protocol designs all assume a client-server architecture. Those that have a P2P architecture are less studied and offer less security against a well-resourced adversary such as a global passive adversary.

Hybrid P2P Networking Structure

A possible way to remedy this disconnect between state of the art anonymous networking protocols based on a client-server architecture and ETH2.0's P2P architecture is to consider a hybrid architecture in which ETH2.0 has both client-server and P2P elements. In the past, hybrid architectures have had applications such as data storage, more efficient querying and network bootstrapping. In this particular instance, we consider an application of such an architecture to increase the anonymity of peers in the ETH2.0 network.

Assumptions

In both ideas, we assume the existence of some PKI infrastructure for managing the nodes in their respective ACN design. Note that in any practical deployment, PKI infrastructure needs to be carefully considered and not glossed over.

Approach 1: Onion Routing

The first approach we consider is one based on onion routing. In onion routing, encrypted messages are sent through a series of proxies and are decrypted (hence onion) at each step. The nodes along the path don't know who the original sender of the message is, just the nodes that are adjacent to it in the path.

A hybrid architecture with this approach would be as follows:

1. Have nodes in the ETH2.0 network that serve as the onion routers (these nodes could be validators themselves)
2. Validators would first send then the messages (attestations, proposals, etc) to these nodes
3. These nodes would operate as per a predefined onion routing protocol similar to Tor.
4. The final node in the onion routing would broadcast it to the rest of the network.

This design enables the privacy notion of sender-message unlinkability. In other words, an adversary cannot tell which validator sent a message.

Problems

There are several problems with this approach. First, this increases the latency of a given validator's message propagation. Given that ETH2.0 has fixed time slots for epochs, this can affect a validator's ability to properly participate in ETH2.0 consensus. Second, this technique also increases the bandwidth a given validator might need if it decides to be both a validator and a node in this specialized onion routing network. This may not be an issue for a node whose sole purpose it to be a onion routing node. Another issue that arises is that as described, nodes in this onion routing network are altruistic. This may become a problem as the network scales and given that Sybil attacks have been observed on real world onion routing networks in the past. Potentially having incentives (rewards and penalties) for maintaining the quality of service of the network is to be determined. Finally, this scheme is not metadata resistant and is thus not secure against a global passive adversary. This means that validators can still be de-anonymized through traffic analysis, correlation attacks, etc.

Approach 2: Mixnets

The second approach we consider is based on mix networks, namely the Loopix design. In the Loopix design, there's 3 components to the mixnet: clients, a PKI system and the mix nodes. For ease of exposition, we will forgo going into detail about the PKI and will only explain the relationship between clients and mix nodes. Further, there is a separate category of mix nodes that are called providers that provide extra services for clients depending on the application. The mix nodes are in a stratified topology. Path selection for messages are created independently and streams of messages are sent according to an exponential distribution.

A hybrid architecture incorporating a Loopix-based approach is as follows:

1. Have nodes in the network that would serve as mix nodes
2. Validators would send their messages through the mixnet
3. The providers at the edges of the mixnet would propagate the message to the other validator nodes

This scheme's privacy notions are

- Sender-Receiver Third Party Unlinkability: The sender and receiver are unlinkable by any unauthorized party.
- Sender Unobservability: An adversary can't tell if a sender sent a message or not
- Receiver Unobserability: An adversary can't tell whether a receiver received a particular message

Problems

The main issue with this approach is the increased latency needed to send messages, and the need for cover traffic which affects scalability. Although the Loopix design provides a tunable tradeoff between latency and cover traffic, the tradeoff needs to take into account the fact that validators need to be timely in their delivery of messages to other peers in the network. Second, the number of mix nodes in the mixnet is dependent on various parameters for which it is difficult to dynamically tune. This means that one would have to reassess the current number of mix nodes throughout the lifetime of the mixnet in order to adjust to increased activity.

Conclusions and Future work

We looked at hybrid networking architectures for increasing validator privacy in ETH2.0. First, we looked at an approach that tries to combine onion routing and p2p networking. Then, we looked at another approach that attempts to combine mixnets with p2p networking. We looked at the issues in both ideas. Future work would be to attempt an implementation and determine whether these networks would benefit from in-protocol incentivization for proper quality of service.

References

- Loopix Anonymity System
- On Privacy Notions
- Tor: The second generation onion router

If you want to chat about Mixnets or more generally anonymous communication networks, join our Riot chathere