Tl;dr:

Instead of using one network per shard, use a single network, but limit propagation of messages between nodes interested in different shards.

Problem

A single p2p network in which all messages are broadcasted to everyone is obviously unsuitable for sharding, as it's opposed to the goal of distributing workload. However, the alternative of having one network per shard has the disadvantage that notaries, whenever they are assigned to a shard, need to connect to a new network. At least with the current devp2p protocol, this takes a long time and thus lower bounds the period length as well as the lookahead length. libp2p might bring improvements here, but this is untested and reconnecting won't be free either.

In order to connect to a new shard network more quickly, notaries might rely on bootstrapping nodes. This is dangerous though as those would be an easy target for DoS attacks that could temporarily stop notarization for a specific shard.

A separate issue may be that the behavior of rapidly reconnecting to new networks whenever a new period starts is a way to identify notaries, making them a target for DoS attacks aiming to, for instance, censor certain proposals.

As a result of above points, notaries benefit from being constantly well connected to all shard networks. This is a centralization risk as participating in many networks is quite costly bandwidth-wise, likely requiring notaries to be run in data centers.

Proposed solution

A solution to these problems could look like this: Use a single network in which nodes are placed on the surface of a torus. A node's ID defines the "poloidal" (red circle in the Wikipedia illustration below), the shard id the "toroidal" angle. All messages are transmitted as usual in the poloidal direction as the nodes on the ring care about the same shard. In the toroidal direction however, only messages of interest to notaries are relayed (mainly new collations, but not, for instance, transactions). In addition, those toroidal messages are transmitted only across a certain number of shards (say, 5).

[

Toroidal_coord.png

1024×768 121 KB

](https://ethresear.ch/uploads/default/original/2X/e/e3471d1a35550fcec2f426983e330c8687da5c20.png)

Discussion

Compared to the naive single network approach, this type of network has the advantage of only increasing the bandwidth requirements of each node by a little (essentially, only by some collations of neighboring shards which neither have to be validated nor stored permanently). Compared to the one-network-per-shard apprach, this allows notaries to require less reconnections as it's possible to be close to a shard (instead of either being connected or not) and being close leads to receiving collations (albeit with higher latency).

Another tweak one could add is making the notary sampling mechanism give "hints" for future samples: Notaries could get bits of information like "if I get sampled at all then I get sampled for some shard in the range 25 to 45", possibly narrowing it down over time. This would allow notaries to make sure that they are propably close to the right shard prior to actually being sampled.