Stumbled upon this paper today (Raul Kripalani from Protocol Labs shared it on Twitter).

It’s basically a BFT alternative to DHT-based p2p protocols.

It consists of two components: 1) attack-resilient gossip-based protocol and 2) the component that extracts uniformly random node samples from the stream of node IDs gossiped by the protocol.

The authors show that an attacker cannot create a partition between correct nodes, and prove that each node’s sample converges to an independent uniform one over time (no such properties were proven for a gossip protocol in the past).

I’m not a p2p expert and I don’t have time to check the paper in depth now, but it surely looks interesting, so I’m dropping it here hoping that it will be useful to someone, someday…

cs.technion.ac.il

[

](https://www.cs.technion.ac.il/~gabik/publications/Brahms-COMNET.pdf)

Brahms-COMNET.pdf

1473.64 KB