

I have started to evaluate what is going on with whisper and with secure messaging in ethereum in general.

I found out, that whisper is barely used. Some projects propose to use 3rd party messaging like rabbitMQ, others try develop an own messaging protocol like PSS in Swarm to fit their particular needs. I thought, this is because of missing whisper specification, but the real reason is that whisper does not meet requirements of those projects.

I know six groups working on next generation of ethereum messaging: [Status](#), [EF](#), [W3F](#), [Swarm/PSS](#), [Validity Labs](#) and [CANTO Project \(extending RLPx\)](#). They make amazing work, but developing of an universal secure messaging system is not easy because there are many trade offs to be solved differently depending on requirements. If you would like to see wide spectrum of messaging protocols and trade-offs to be solved, please have a look into this [classic paper](#).

Ethereum become more and more heterogeneous ecosystem: sharding, plasma, state channels, swarm, Tx Relays, oracles, side chains - a lot of different nodes that should be able to communicate to each other.

If we would like to develop an unified secure messaging protocol for ETH2, we must start with collecting requirements.

[Ethresear.ch](#) is a great place for that, because almost any subsystem for ETH2 get discussed and specified here.

Unfortunately I don't see here any discussion about requirements for messaging. All specification efforts are currently going in dev groups internally and probably quite disconnected from demand of projects discussed here. It is not good and I would like to change it.

I would ask all developers working on projects with secure messaging (almost all of them?) to specify requirements for messaging explicitly and make it available here to messaging protocol developers.

Any thoughts?

UPD: [mainframe](#), [uport](#), [NuCypher](#) are building own messaging solutions too.

It is not healthy. We need some unified secure messaging service in ethereum ecosystem.

UPD 2: one project more needs secure messaging: [WalletConnect.org](#) aims to replace their bridge-servers routing transactions to be signed from Dapp to Wallet.