Waku: decentralized and privacy-preserving communication for Web3 applications

Sergei Tikhomirov

Protocol Research Engineer, Waku

d/acc Berlin, 2025-06-11

Web3 communication is not private

- (d)apps rely on centralized services (RPCs etc)
- Users generally don’t want to run nodes

Web3 needs a secure communication layer - also needed for d/acc vision!

Swarm

Ethereum

Whisper

Ethereum as part of a broader technological vision

In 2014, Gavin Wood introduced Ethereum as one of a suite of tools that can be built, the other two being Whisper (decentralized messaging) and Swarm (decentralized storage). The former was heavily emphasized, but with the turn toward financialization around 2017 the latter were unfortunately given much less love and attention. That said, Whisper continues to exist as Waku, and is being actively used by projects like the decentralized messenger Status. Swarm continues to be developed, and now we also have IPFS, which is used to host and serve this blog.

https://vitalik.eth.limo/general/2023/12/28/cypherpunk.html

Introduction to Waku

Waku is a family of open-source, modular P2P communication protocols that are:

- permissionless
- decentralized
- privacy-preserving
- censorship-resistant

Waku is used by Status, Railgun, and The Graph, among others.

What can Waku be used for?

- Chats and messengers (eg. Status)
- Voting, Q&A
- Signing coordination for multisig wallets
- …and more

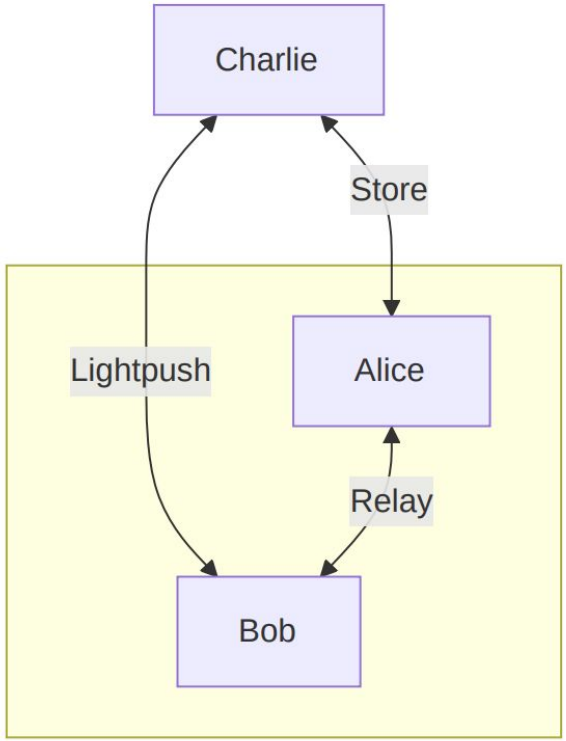
See ideas.waku.org for more ideas!

Waku Network Architecture

Waku nodes choose which protocols to run:

- Relay, the backbone of the network (libp2p-based);

- Light protocols suited for resource-restricted devices:
  - Filter: subscribe to a subset of relayed messages;
  - Lightpush: publish a message to the network;
  - Store: query historic messages.


Charlie
Store
Lightpush
Alice
Relay
Bob

Rate Limiting Nullifiers (RLN)

Waku defends against DoS attacks using ZK-based Rate Limiting Nullifiers (RLN).

RLN works as follows:

- Users register a membership in a smart contract;
- Users attach a proof of membership to each message;
- Relay nodes only propagate messages with valid proofs.

Waku implementations

Multiple interoperating implementations exist:

- nwaku in Nim
- go-waku in Go
- js-waku in Javascript

+ SDKs in various languages (check out docs.waku.org)

The Waku Network

An opinionated deployment of the Waku protocol stack launched in 2023:

- Sharding by topic for scalability;
- Privacy-preserving rate limiting via RLN.

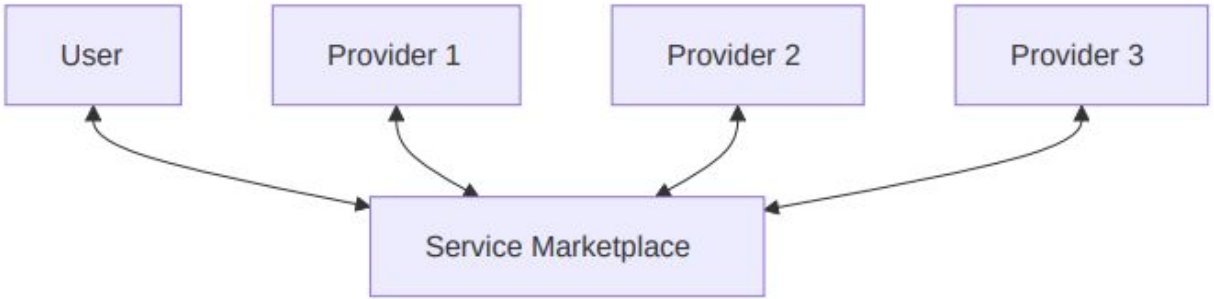
Fully permissionless, anyone can join!

Research direction: incentivization

Currently, Waku is altruistic.

Research is ongoing to incentivize service provision in the Waku network.

I'll give a talk on one aspect of this at Protocol Berg tomorrow (2025-06-12) - keyword "Waku Service Marketplace".



Learn more about Waku

Check out waku.org to learn more (scan QR code). Thank you!