
Vac

Building
privacy-protecting
infrastructure.

Why, what and how?

About

_

Vac builds public good protocols for the decentralized web.

_

vac.dev / @vap2p

oskarth.com / @oskarth

Principles

–

I. Liberty
II. Censorship resistance
III. Security
IV. Privacy
V. Transparency
VI. Openness
VII. Decentralization
VIII. Inclusivity
IX. Continuance
X. Resourcefulness

Why?
_

Privacy is the power to selectively reveal yourself.

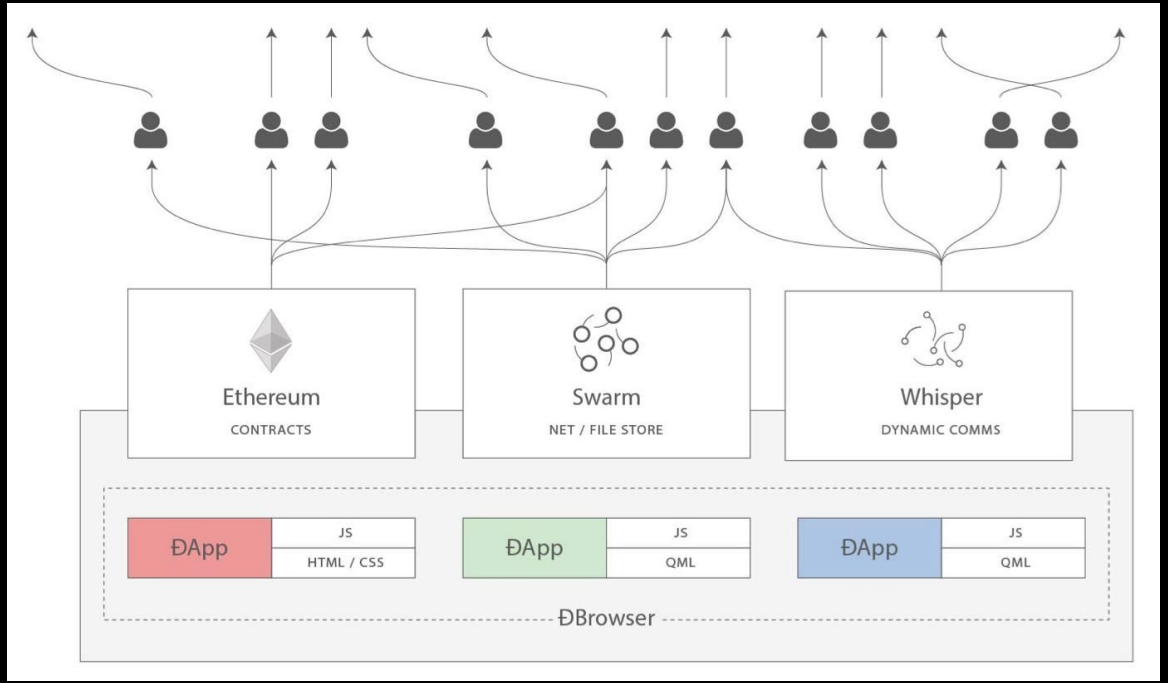
Base layer requirement.

Natural privacy and the Internet.

Building infrastructure.

Web3 Infrastructure

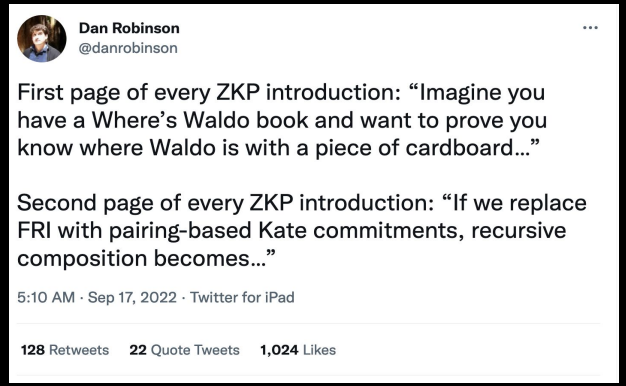
–

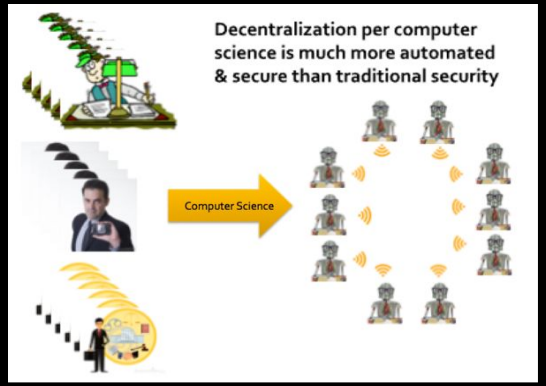


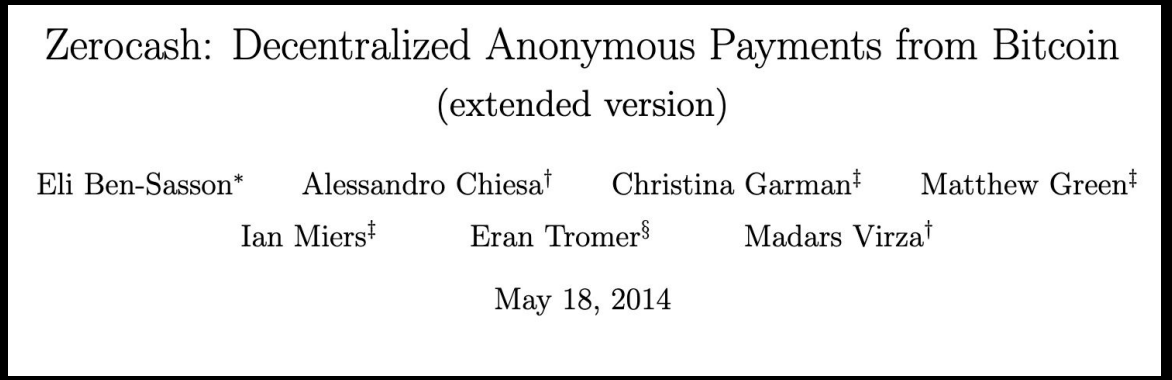
Zero-Knowledge

–

For privacy-protecting infrastructure






Zerocash: Decentralized Anonymous Payments from Bitcoin
(extended version)

Eli Ben-Sasson* Alessandro Chiesa† Christina Garman‡ Matthew Green‡
Ian Miers‡ Eran Tromer§ Madars Virza†

May 18, 2014

Waku
_

Waku is the communication layer for Web3.

Set of modular protocols.

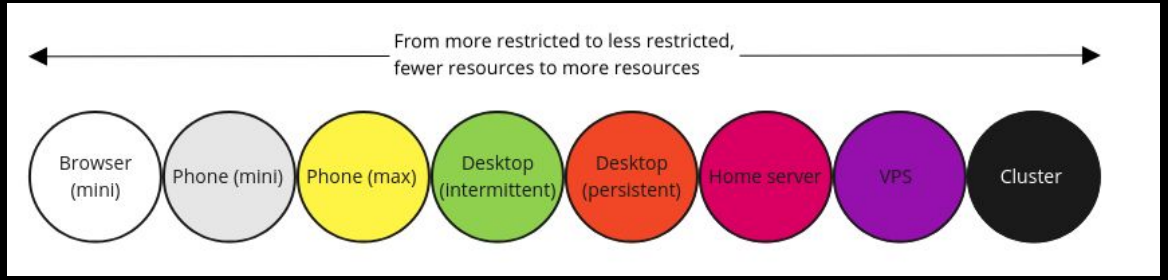
Private, secure, runs anywhere.

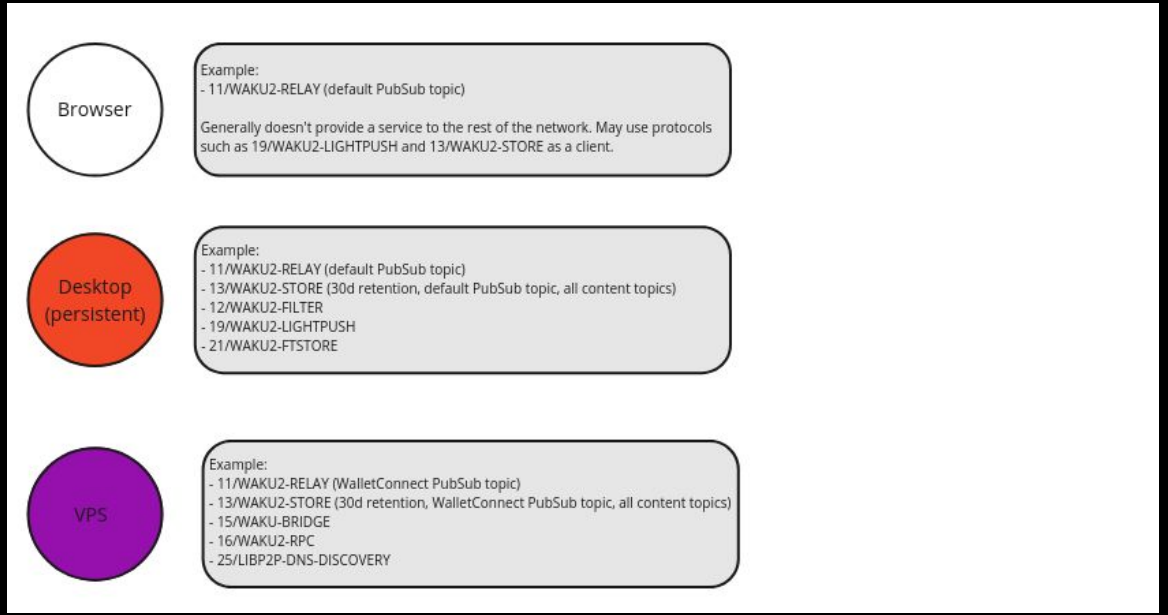
Spiritual successor to Whisper.

Waku

–

Adaptive nodes

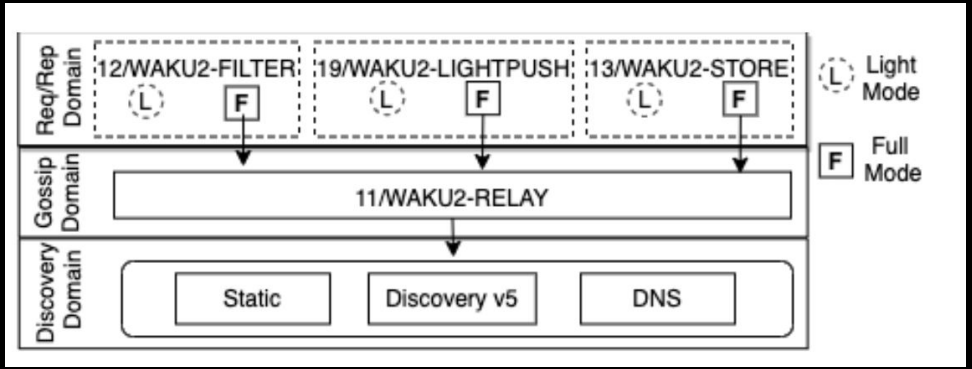


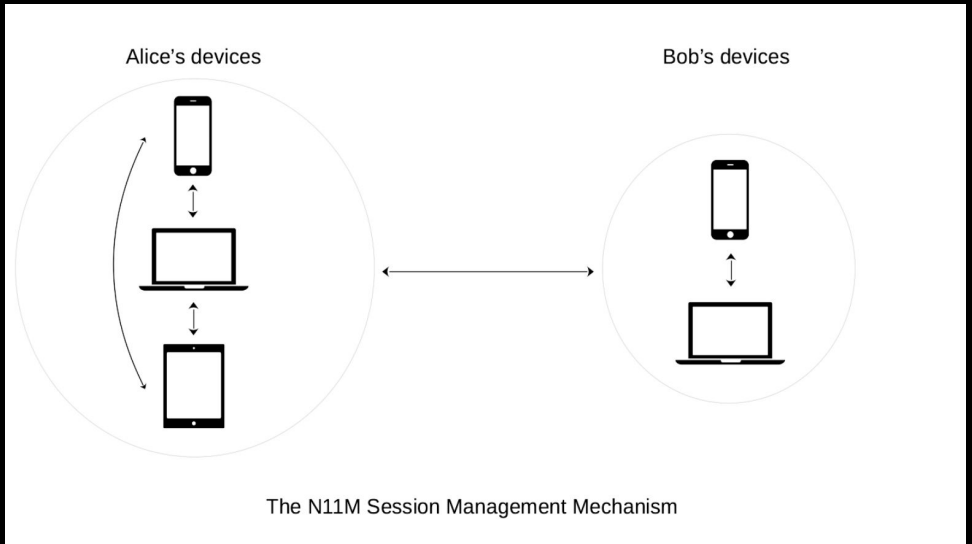


Waku

–

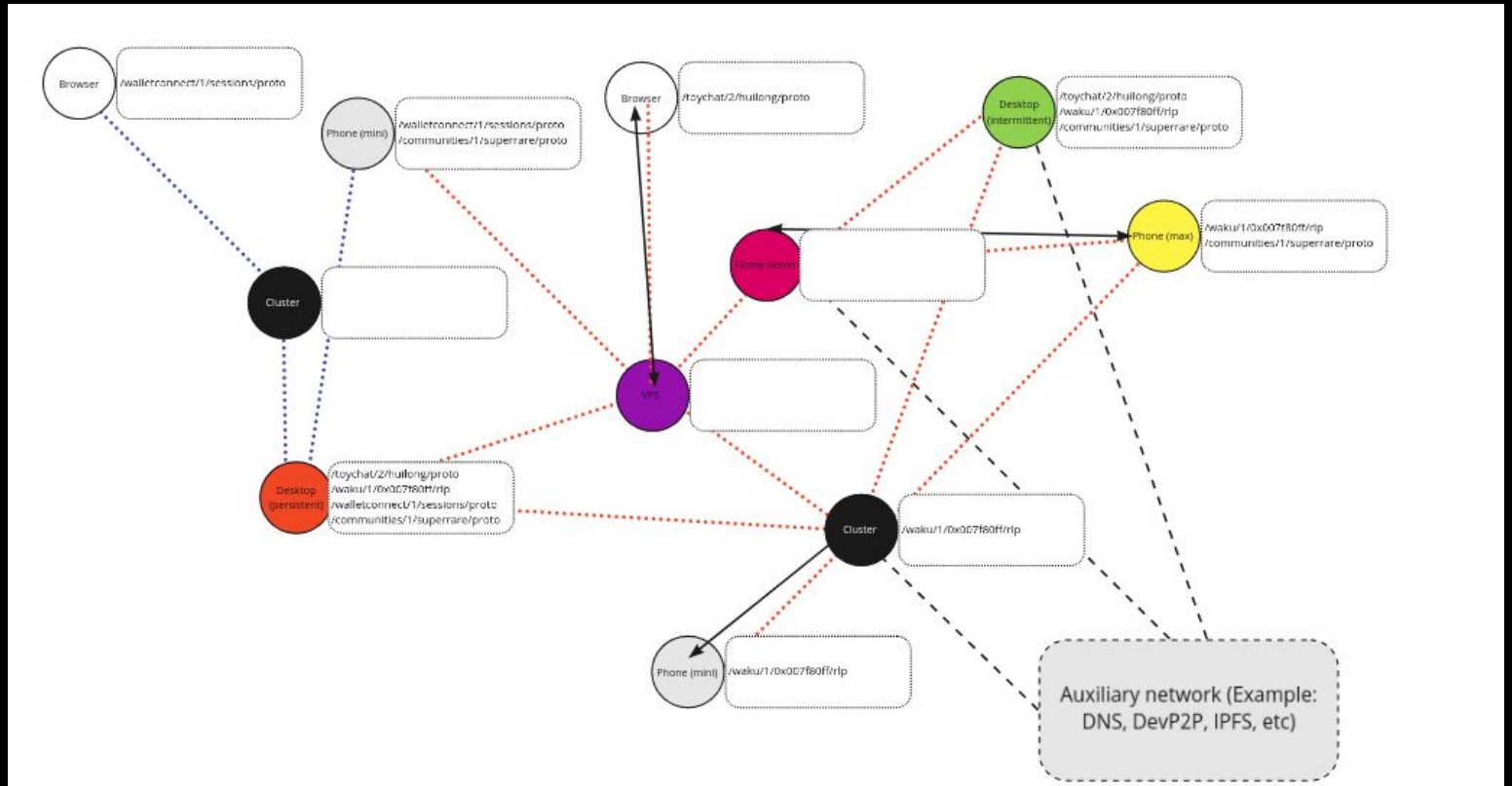
Protocol interactions





Waku Network

–



RLN

–

Motivation

Dealing with network spam.

Phone numbers, PoW, peer scoring.

RLN: Private, economic spam protection using zkSNARKs.

RLN

–

Overview

Rate Limiting Nullifier

Anonymous rate limiting.

Registration, signalling and verification.

RLN

–

Circuit

```
// Private input
signal input identity_secret;
signal input path_elements[n_levels][1];
signal input identity_path_index[n_levels];

// Public input
signal input x; // signal_hash
signal input epoch; // external_nullifier
signal input rln_identifier;

// Circuit output
signal output y;
signal output root;
signal output nullifier;
```

RLN

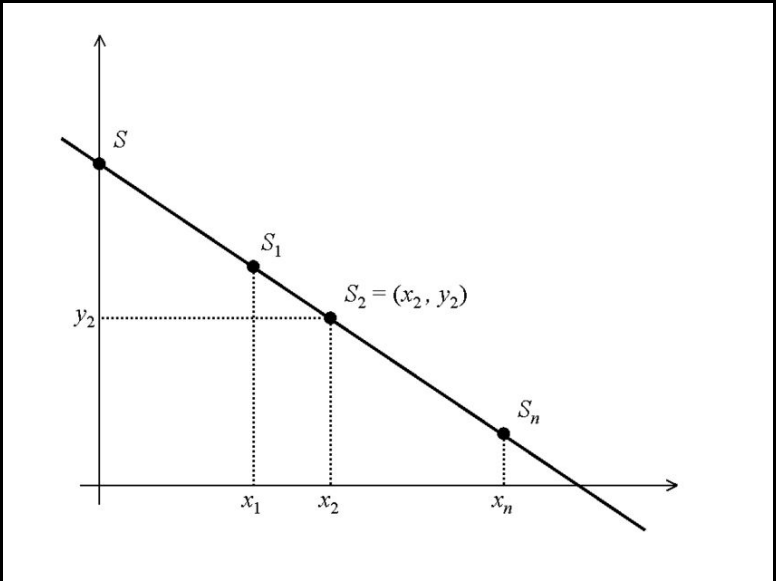
–

Shamir’s secret sharing

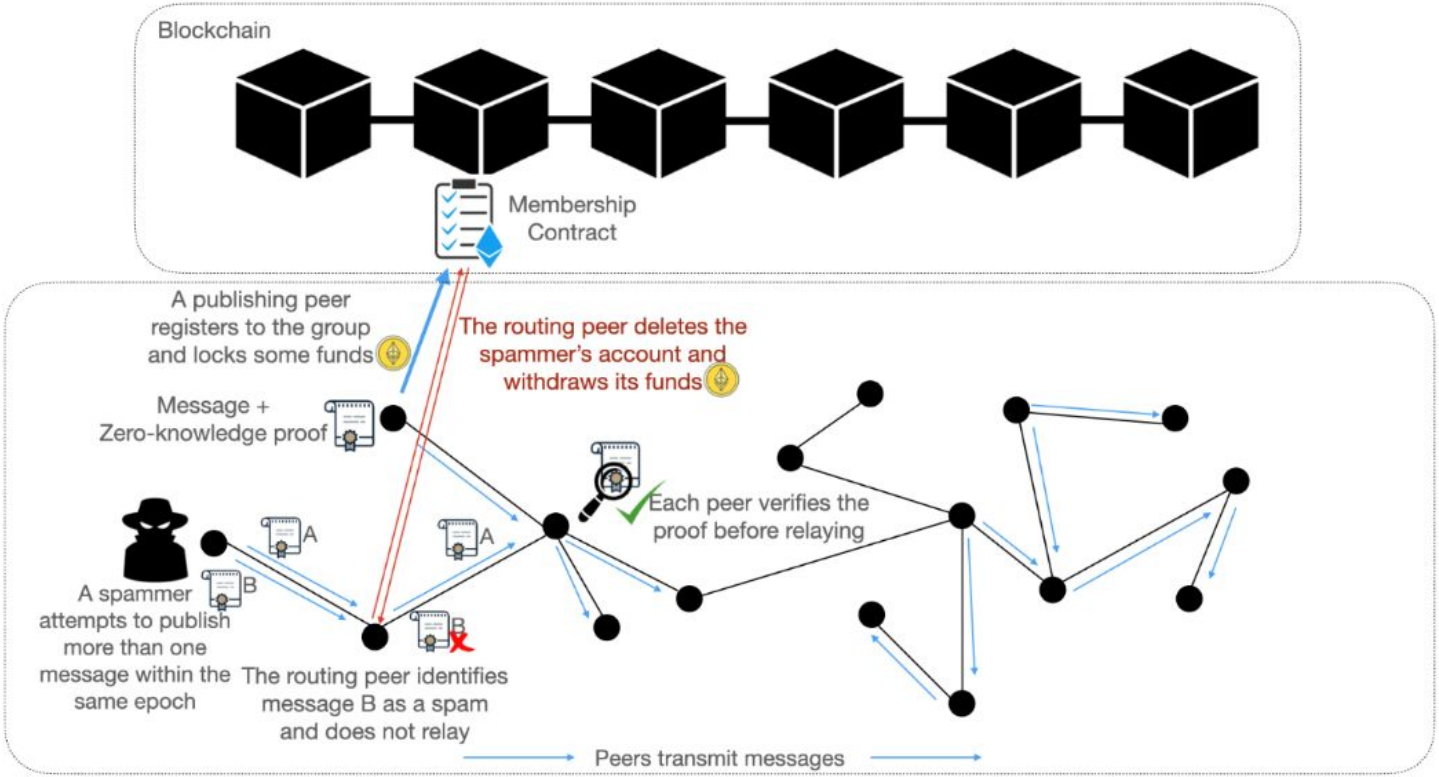
a_0 = identity_secret // secret S
a_1 = poseidonHash([a0, external_nullifier])

y = a_0 + x * a_1

internal_nullifier = poseidonHash([a_1, rln_identifier])



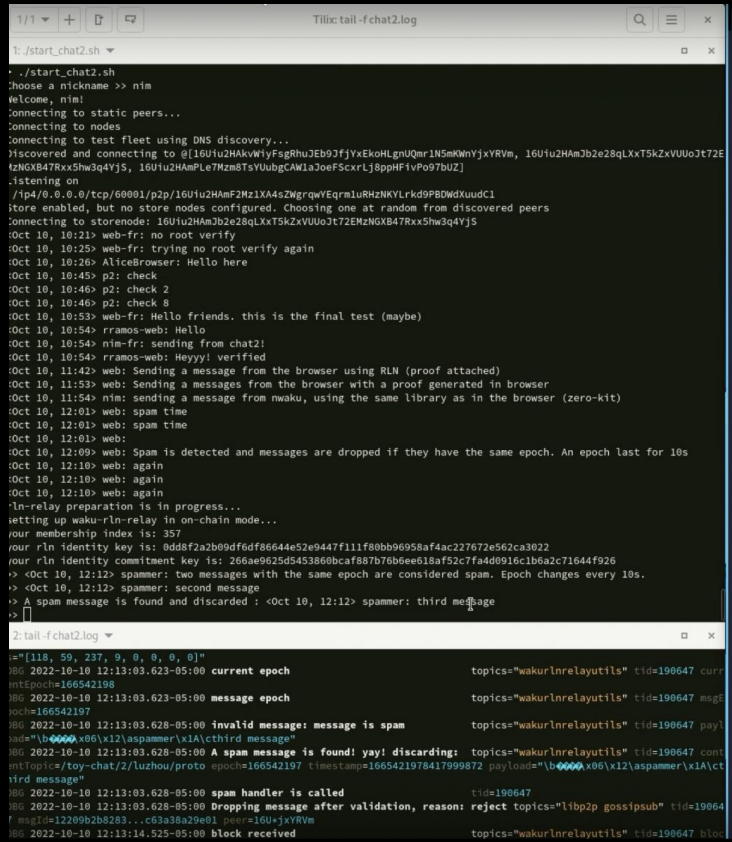
RLN


Blockchain
Membership Contract
A publishing peer registers to the group and locks some funds
The routing peer deletes the spammer's account and withdraws its funds
Message + Zero-knowledge proof
Each peer verifies the proof before relaying
A
A
B
B
A spammer attempts to publish more than one message within the same epoch
The routing peer identifies message B as a spam and does not relay
Peers transmit messages

RLN

–

Cross-client testnet



Service
credentials

–

Service network.

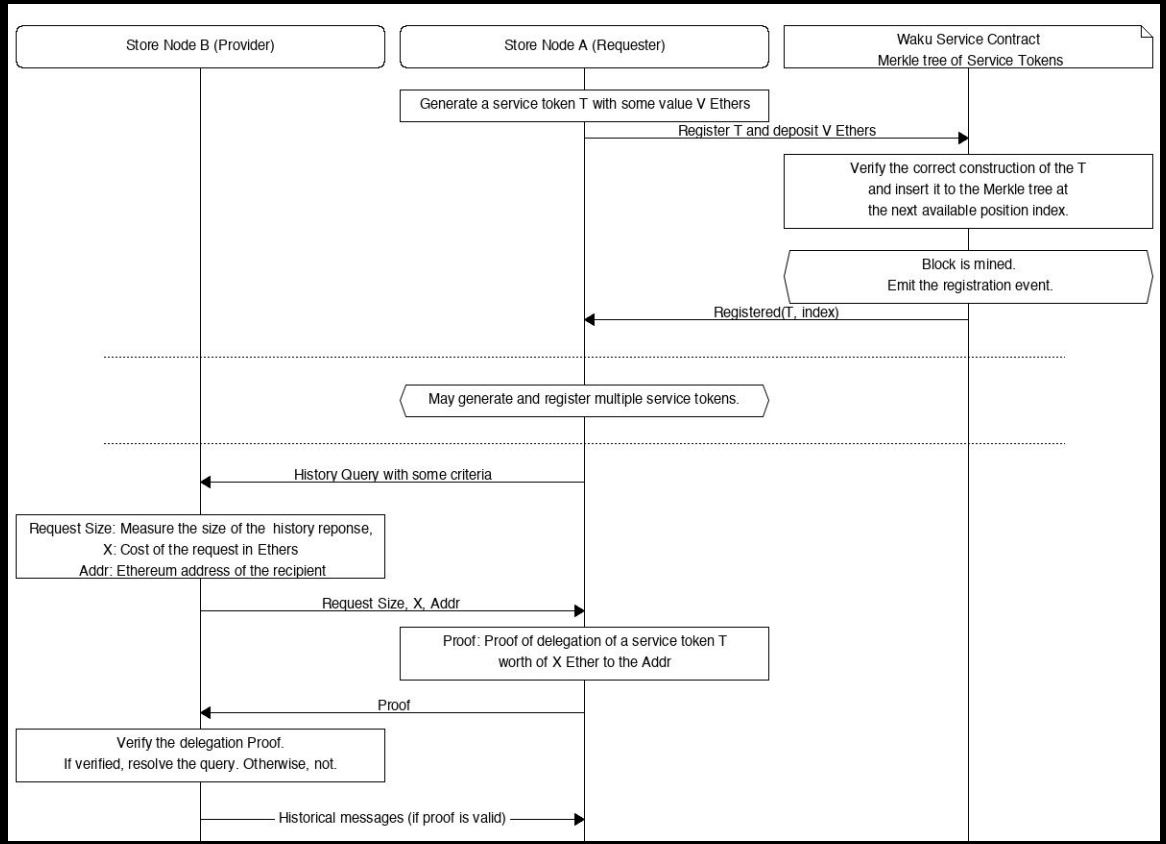
Private settlement.

Byproduct, altruism and incentives.

Req/Resp protocols.

Service credentials

–



Zerokit

Set of ZK modules in Rust.

Circom/Solidity/JS + Rust/ZK Ecosystem.

Expose a Rust, C FFI and WASM API.

RLN module.

Lower barrier to entry.

Other research

–

Specs, papers, device pairing, network privacy

Specs

10/WAKU2

Waku v2

status: draft

- Status: draft
- Editor: Oskar Thorén oskar@status.im
- Contributors: Sanaz Taheri sanaz@status.im , Hanno Cornelius hanno@status.im , Reeshav Khan reeshav@status.im , Daniel Kaiser danielkaiser@status.im

Abstract

Waku v2 is family of modular peer-to-peer protocols for secure communication. The protocols are designed to be secure, privacy-preserving, censorship-resistant and being able to run in resource restricted environments. At a high level, it implements Pub/Sub over libp2p and adds a set of capabilities to it. These capabilities are things such as: (i) retrieving historical messages for mostly-offline devices (ii) adaptive nodes, allowing for heterogeneous nodes to contribute to the network (iii) preserving bandwidth usage for resource-restriced devices

This makes Waku ideal for running a p2p protocol on mobile and in similarly restricted environments.

Device Pairing

The handshake, detailed in next section, can be summarized as:

```
WakuPairing:
a.   <- eB              {H(sB||r), contentTopicParams, messageNametag}
     ...
b.   -> eA, eAeB        {H(sA||s)}   [authcode]
c.   <- sB, eAsB        {r}
d.   -> sA, sAeB, sAsB  {s}

{}: payload,    []: user interaction
```

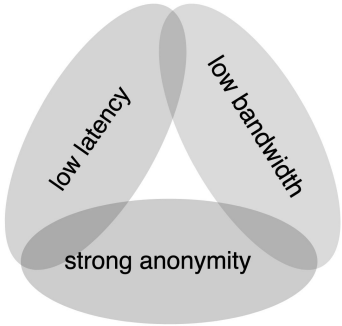
Protocol Flow #

1. The device `B` exposes through a QR code a Base64 serialization of:
   - An ephemeral public key `eB`;
   - The content topic parameters `contentTopicParams = {application-name}, {application-version}, {shard-id}`.
   - A (randomly generated) 16-bytes long `messageNametag`.
   - A commitment `H(sB||r)` for its static key `sB` where `r` is a random fixed-lenght value.
2. The device `A`:
   - scans the QR code;

Network Privacy

Anonymity Trilemma

The Anonymity trilemma states that only two out of *strong anonymity*, *low bandwidth*, and *low latency* can be guaranteed in the global on-net attacker model. Waku's goal, being a modular set of protocols, is to offer any combination of two out of these three properties, as well as blends. An example for blending is an adjustable number of pubsub topics and peers in the respective pubsub topic mesh; this allows tuning the trade-off between anonymity and bandwidth.



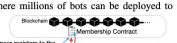
Papers

Privacy-Preserving Spam-Protected Gossip-Based Routing

Sanaz Taheri-Boshrooyeh*†, Oskar Thorén*†, Barry Whitehat‡, Wei Jie Koh§, Onur Kilic¶, and Kobi Gurkan‖
*Vac Research and Development, †Status Research and Development, Singapore, ‡Unaffiliated,
§Independent, ¶Unaffiliated, ‖cLabs
sanaz@status.im, oskar@status.im, barrywhitehat@protonmail.com,
contact@kohweijie.com, onurkilic@protonmail.com, me@kobi.one

***Abstract*—WAKU-RLN-RELAY is an anonymous peer-to-peer gossip-based routing protocol that features a privacy-preserving spam-protection with cryptographically guaranteed economic incentives. While being an anonymous routing protocol where routed messages are not attributable to their origin, it allows**

expensive hence not suitable for resource-constrained devices. The peer scoring is also prone to censorship and inexpensive attacks where millions of bots can be deployed to send bulk



Summary

Privacy-protecting infrastructure is important.

ZK is a fundamental building block.

We can build it.

Come help :)

Links

—

Thanks!

Questions?

- vac.dev / @vacp2p
- waku.org / @waku_org
- oskarth.com / @oskarth

- Hiring for Waku, private computation (zk-WASM), etc
  - Protocol engineers, senior rust engineers, ZK researchers, compiler engineer, production engineers
  - See jobs.status.im