

Building privacy-protecting infrastructure.

Why, what and how?

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?

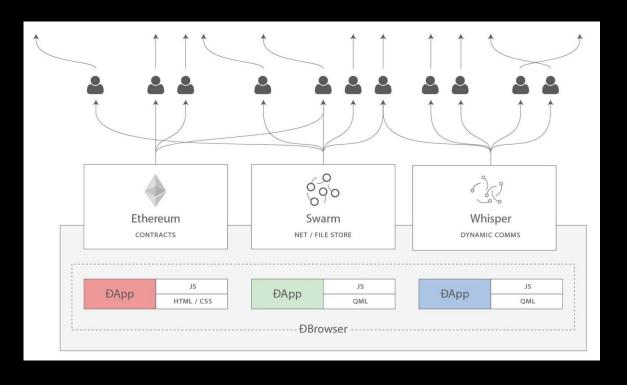
Privacy is the power to selectively reveal yourself.

Base layer requirement.

Natural privacy and the Internet.

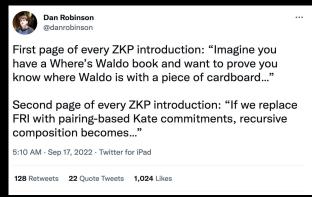
Building infrastructure.

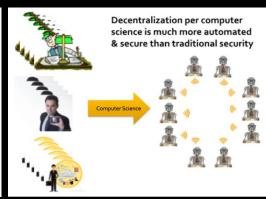
Web3 Infrastructure



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.

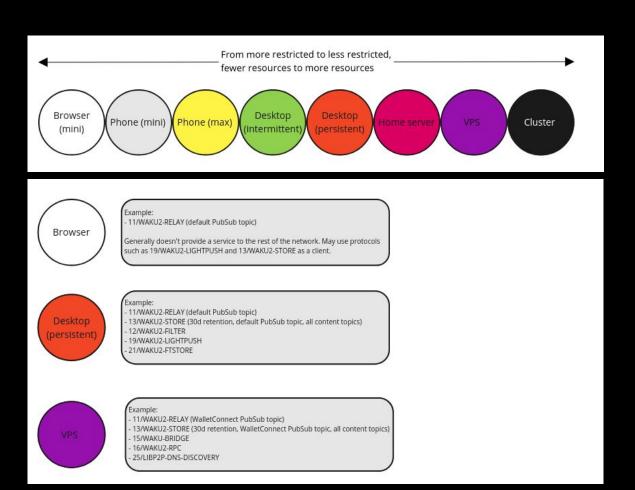
Set of modular protocols.

Private, secure, runs anywhere.

Spiritual successor to Whisper.

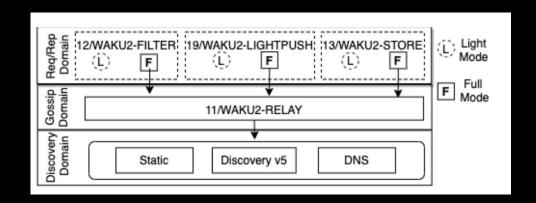
Waku

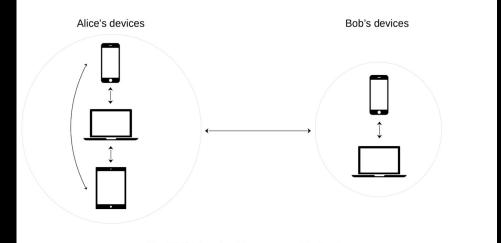
Adaptive nodes



Waku

Protocol interactions

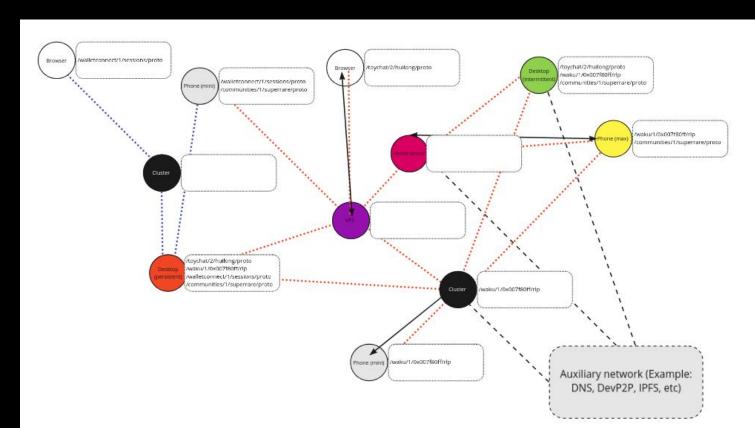




The N11M Session Management Mechanism

Waku Network







Dealing with network spam.

Motivation

Phone numbers, PoW, peer scoring.

RLN: Private, economic spam protection using zkSNARKs.

Rate Limiting Nullifier

Overview

Anonymous rate limiting.

Registration, signalling and verification.



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;

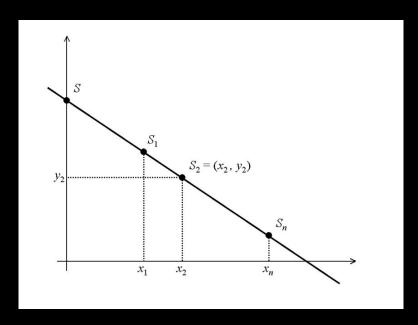
// Circuit output
signal output y;
signal output root;
signal output nullifier;

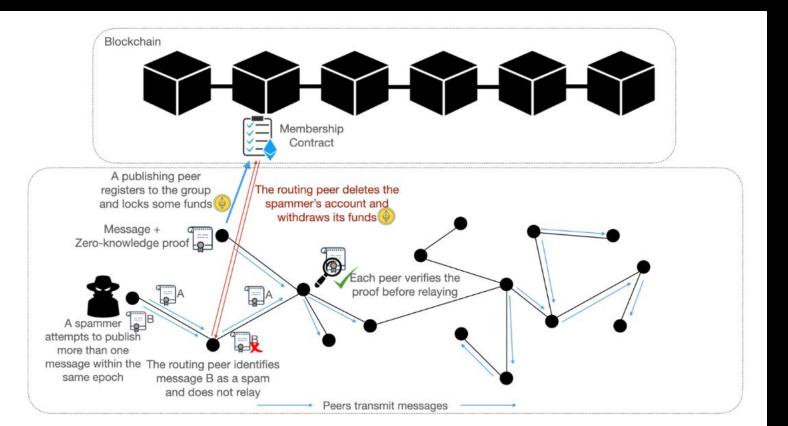
Shamir's secret sharing

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])









Cross-client testnet

1/1 + + R Q a examples.waku.org/rln-js/ < | 👽 🛕 * 3 :/start chat2.sh 🔻 · ./start_chat2.sh RLN Commitment Key (hex string): Choose a nickname >> nim Velcome, nim! b48871f92fca9cfc4d568920 Connecting to static peers... Connecting to nodes Import RLN Credentials Connecting to test fleet using DNS discovery... discovered and connecting to @[16Uiu2HAkvWijvFsgRhuJEb9JfjYxEkoHLgnUQmr1N5mKWnYjxYRVm, 16Ui<u>u2HAmJb2e28qLXxT5kZxVUUo</u>Jt72E (zNGXB47Rxx5hw3q4YiS, 16Uiu2HAmPLe7Mzm8TsYUubgCAW1aJoeFScxrLi8ppHFivPo97bUZ] istening on /ip4/0.0.0.0/tcp/60001/p2p/16Uiu2HAmF2Mz1XA4sZWgrqwYEqrmluRHzNKYLrkd9PBDWdXuudC1 store enabled, but no store nodes configured. Choosing one at random from discovered peers Connecting to storenode: 16Uiu2HAmJb2e28qLXxT5kZxVUUoJt72EMzNGXB47Rxx5hw3q4YjS 365 Membership id :Oct 10, 10:21> web-fr: no root verify Oct 10, 10:25> web-fr: trying no root verify again Oct 10, 10:26> AliceBrowser: Hello here 021fa709cd2c9cff7df00a2a688babaebea370236a89ebe8cb5cd6d90fb45527 Oct 10, 10:45> p2: check Key Oct 10, 10:46> p2: check 2 Oct 10, 10:46> p2: check 8 b48871f92fca9cfc4d568920c3d5d98d5d83a7b9c6a8d713d6481ec44e650023 Oct 10, 10:53> web-fr: Hello friends. this is the final test (maybe) Commitment :Oct 10, 10:54> rramos-web: Hello :Oct 10, 10:54> nim-fr: sending from chat2! Oct 10, 10:54> rramos-web: Heyvy! verified Oct 10, 11:42> web: Sending a message from the browser using RLN (proof attached) Oct 10, 11:53> web: Sending a messages from the browser with a proof generated in browser Oct 10, 11:54> nim: sending a message from nwaku, using the same library as in the browser (zero-kit) Oct 10, 12:01> web: spam time Waku Oct 10, 12:01> web: spam time Oct 10, 12:01> web: Oct 10, 12:09> web: Spam is detected and messages are dropped if they have the same epoch. An epoch last for 10s Oct 10, 12:10> web: again Waku node subscribed. Oct 10, 12:10> web: again Oct 10, 12:10> web: again setting up waku-rln-relay in on-chain mode... Remote peer's multiaddr your membership index is: 357 our rln identity key is: 0dd8f2a2b09df6df86644e52e9447f111f80bb96958af4ac227672e562ca3022 /dns4/node-01.ac-cn-hongkong-c.wakuv2.test.statusim.net/tcp/443/wss/p2p/16Uiu2HAkv Dial our rln identity commitment key is: 266ae9625d5453860bcaf887b76b6ee618af52c7fa4d0916c1b6a2c71644f926 >> <Oct 10, 12:12> spammer: two messages with the same epoch are considered spam. Epoch changes every 10s. >> <Oct 10, 12:12> spammer: second message Your nickname >> A spam message is found and discarded : <Oct 10, 12:12> spammer: third me∯sage spammer 2: tail -f chat2.log 🔻 0 × Message text topics="wakurlnrelayutils" tid=190647 c)86 2022-10-10 12:13:03.623-05:00 current epoch)BG 2022-10-10 12:13:03.623-05:00 message epoch Send message using Light Push)86 2022-10-10 12:13:03.628-05:00 invalid message: message is spam topics="wakurlnrelayutils" tid=198647 page 198647 pad="\been x06\x12\aspammer\x1A\cthird message 086 2022-10-10 12:13:03.628-05:00 **A spam message is found! yay! discarding:** topics="wakurlnrelayutils" tid=190647 c ntTopic=/toy-chat/2/luzhou/proto epoch=166542197 timestamp=1665421978417999872 payload="\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred"\beentarred Messages)BG 2022-10-10 12:13:03.628-05:00 spam handler is called • (spammer) two messages with the same epoch are considered spam. Epoch changes every 10s. [2022-10-086 2022-10-10 12:13:03.628-05:00 Dropping message after validation, reason: reject topics="libp2p gossipsub" tid=19064 10T17:12:42.000Z] - [epoch: 166542196, proof: verified.] BG 2022-10-10 12:13:14.525-05:00 block received (spammer) second message [2022-10-10717:12:50 00071 - [epoch: 166542197 proof: verified]



Service credentials

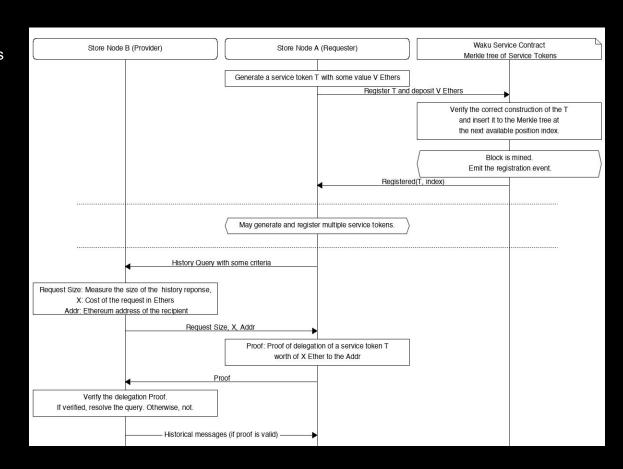
Service network.

Private settlement.

Byproduct, altruism and incentives.

Req/Resp protocols.

Service credentials



Zerokit

Set of ZK modules in Rust.

Expose a Rust, C FFI and WASM API.

Circom/Solidity/JS + Rust/ZK Ecosystem.

RLN module.

Lower barrier to entry.

/ac October 2022 Devcon Bogota Building privacy-protecting infrastructure

Other research

Specs, papers, device pairing, network privacy

Specs

10/WAKU2 Motivation and goals Waku v2 Gossip domain Direct use of libp2p proto · Editor: Oskar Thorén oskar@status.im Request/Reply domain . Contributors: Sanaz Taheri sanaz@status.im . Hanno Cornelius hanno@status.im . Reeshav Overview of protocol interaction Khan reeshav@status.im , Daniel Kaiser danielkaiser@status.im Appendix A: Upgradability and Compatibility with Waku v1 Abstract Primary Adversarial Model Security Features 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 Anonymity / Unlinkability 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 Data confidentiality, Integrity, and Authenticity mostly-offline devices (ii) adaptive nodes, allowing for heterogeneous nodes to contribute to the network (iii) preserving bandwidth usage for resource-restriced devices Security Considerations This makes Waku ideal for running a p2p protocol on mobile and in similarly restricted Implementation Matrix

Device Pairing

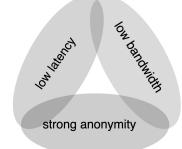
The handshake, detailed in next section, can be summarized as:

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.
 - o A commitment H(sB||r) for its static key sB where r is a random fixed-lenght value.
- 2. The device A:
 - ecane the OP 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 ofer any combination of two out of these three properties, as well as blonds. An example for briefland is an adjustate 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, ¹Status Research and Development, Singapore, [‡]Unaffiliated,
[‡]Independent, [†]Unaffiliated, [‡]Labs

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:)

Vac October 2022 Devoon Bogota Building privacy-protecting infrastructure

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

