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

Ethereum
CONTRACTS

Swarm
NET / FILE STORE

Whisper
DYNAMIC COMMS

DApp
JS
HTML / CSS

DApp
JS
QML

DApp
JS
QML

DBrowser
Zero-Knowledge

For privacy-protecting infrastructure

---

First page of every ZKP introduction: “Imagine you have a Where’s Waldo book and want to prove you know where Waldo is with a piece of cardboard...”

Second page of every ZKP introduction: “If we replace FRI with pairing-based Kate commitments, recursive composition becomes...”

---

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 is the communication layer for Web3.

Set of modular protocols.

Private, secure, runs anywhere.

Spiritual successor to Whisper.
Waku

Adaptive nodes

From more restricted to less restricted, fewer resources to more resources

- **Browser (mini)**
  - Example: 11/WAKU2-RELAY (default PubSub topic)
  - Generally doesn't provide a service to the rest of the network. May use protocols such as 19/WAKU2-LIGHTPUSH and 13/WAKU2-STORE as a client.

- **Desktop (persistent)**
  - Example: 11/WAKU2-RELAY (default PubSub topic)
    - 13/WAKU2-STORE (60d retention, default PubSub topic, all content topics)
    - 12/WAKU2-FILTER
    - 19/WAKU2-LIGHTPUSH
    - 21/WAKU2-STORE

- **VPS**
  - Example: 11/WAKU2-RELAY (WalletConnect PubSub topic)
    - 13/WAKU2-STORE (30d retention, WalletConnect PubSub topic, all content topics)
    - 15/WAKU2-BRIDGE
    - 16/WAKU2-RPC
    - 25/LBP3P-DNS-RECOVERY
Waku

Protocol interactions
Waku Network
Motivation

Dealing with network spam.

Phone numbers, PoW, peer scoring.

RLN: Private, economic spam protection using zkSNARKs.
Rate Limiting Nullifier

Anonymous rate limiting.

Registration, signalling and verification.
// 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

\[ a_0 = \text{identity\_secret} // \text{secret } S \]

\[ a_1 = \text{poseidonHash([}a_0, \text{external\_nullifier}]) \]

\[ y = a_0 + x \times a_1 \]

\[ \text{internal\_nullifier} = \text{poseidonHash([}a_1, \text{rln\_identifier}]) \]
Vac Building privacy-protecting infrastructure - October 2022 - Devcon Bogota

RLN
RLN

Cross-client testnet

Building privacy-protecting infrastructure

Devcon Bogota

October 2022

Vac Building privacy-protecting infrastructure

Review of network data

Connecting to test fleet using DMS discovery

Connecting to static peers...

Connecting to nodes

Connecting to test fleet using DMS discovery...

Connecting to static peers...

Connecting to nodes

Connecting to test fleet using DMS discovery...

Connecting to static peers...

Connecting to nodes

Membership ID

Key

Commitment

Waku

Waku node subscribed.

Remote peer’s multiaddr

Your nickname

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages

• spammer

Message text

Type your message here

Send message using Light Push

Messages
Service network.

Private settlement.

Byproduct, altruism and incentives.

Req/Resp protocols.
Service credentials

Vac

- Building privacy-protecting infrastructure

- October 2022

- Devcon Bogota

- Service credentials

Store Node B (Provider)

Store Node A (Requester)

Waku Service Contract

Merkle tree of Service Tokens

Generate a service token $T$ with some value $V$ Ethers

Register $T$ and deposit $V$ Ethers

Verify the correct construction of the $T$

and insert it to the Merkle tree at

the next available position index.

Block is mined

Emit the registration event.

May generate and register multiple service tokens.

History Query with some criteria

Request Size: Measure the size of the history response,

$X$: Cost of the request in Ethers

Addr: Ethereum address of the recipient

Request Size, $X$, Addr

Proof: Proof of delegation of a service token $T$

worth of $X$ Ether to the Addr

Proof

Verify the delegation Proof.

If verified, resolve the query. Otherwise, not.

Historical messages (if proof is valid)
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/WAKUZ**

**Waku v2**

**Authors**

- Status: draft
- Editors: Takeshi Tanaka, r@status.im
- Contributors: Saez Taheri, s@status.im, Hanso Cornelius, h@status.im, Reshef Klein, r@status.im, Daniel Klein, d@status.im

**Abstract**

Waku is a family of modular peer-to-peer protocols for secure communication. These protocols are designed to be secure, privacy-preserving, privacy-resistant, and being able to run in resource-constrained environments, as low-level, implements Protocol over low (IoT) and static set of capabilities 3. These capabilities are things such as 1) networking historical messages for mostly of this device's (that is a) device's node, allowing for heterogeneous nodes to contribute to the network (s) processing bandwidth usage for resource-constrained 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 *->* b : (H(a||b), contentTopicParams, messageNameTag) ...
  - b *->* a : (H(a||s) [authcode] )
  - c *->* a : (H(a||r) )
  - d *->* a : (H(a||x) [authcode] )

(): 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), (share-id);
   - A (randomly generated) 16 bytes long messageNameTag;
   - A commitment H(a||r) for its static key a; where r is a random fixed-length value.

2. The device a:*
   - scans the QR code;
Summary

Privacy-protecting infrastructure is important.

ZK is a fundamental building block.

We can build it.

Come help :)
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