The Waku Network as Infrastructure for dApps

Hanno Cornelius*† Sergei Tikhomirov*† Alvaro Revuelta*† Simon Pierre Vivier*† Aaryamann Challani‡†
*Waku Research, †Institute of Free Technology, Singapore ‡Vac Research and Development
hanno@vac.dev, sergei@status.im, alrevuelta@status.im, simvivier@status.im, aaryamann@vac.dev

***Abstract*—The Waku Network is a decentralized messaging infrastructure designed to provide privacy-preserving, scalable, spam-resistant, and censorship-resistant messaging services for decentralized applications. In this paper, we present the architecture and implementation details of The Waku Network, which leverages Waku protocols to form a global, shared, peer-to-peer messaging infrastructure. We discuss routing and sharding mechanisms, peer discovery methods, rate limiting techniques to prevent denial-of-service (DoS), provided services, as well as incentives for network participation. The Waku Network offers a robust messaging solution suitable for various decentralized applications, with a focus on long-term sustainability.**

***Index Terms*—p2p, privacy, waku, libp2p, infrastructure**

I. Introduction

The Waku Network describes an opinionated deployment of Waku protocols [1], to form a global, shared decentralized messaging infrastructure. This network is an open-access peer-to-peer infrastructure useful for generalized messaging in any decentralized application. It is privacy-preserving, scalable, spam-resistant, censorship-resistant and accessible to heterogeneous nodes, from powerful servers to resource-constrained mobile nodes. As such, it also defines a set of services useful to many messaging applications, such as content filtering, selective message routing, and historical message storage and retrieval. It aims to build a sustainable infrastructure by implementing various monetary and non-monetary ways to incentivize constructive participation in the network. We describe both an extension and implementation of the Waku [2] suite of protocols to create this network.

II. Related Work

Decentralized messaging protocols generally define communication rules between clients and servers, as well as among servers forming federations. Popular examples include ActivityPub [3] and Farcaster [4]. Waku protocols remove the need for servers facilitating message forwarding among users. This allows the deployment of a public Waku Network, the provides general messaging capabilities beyond chat-like applications while ensuring transport privacy, scalability and security.

III. Network Architecture

A. Routing and Sharding

Messages are routed within The Waku Network through the Waku RLN Relay [5] protocol, a publish-subscribe (pub/sub) protocol based on a privacy-preserving application of libp2p [6] GossipSub [7]. It excludes all reference to personally identifiable information (PII), such as signatures, at the GossipSub layer. The main routing innovation is a privacy-preserving method to rate limit publishing, helping protect the network against DoS/spam attacks, based on Rate Limiting Nullifiers (RLN). This is described in Section III-C.

Network scalability is achieved by sharding messaging traffic from all applications into eight pub/sub topics. Every message is published on only one of these eight topics and relayed only by the subset of peers subscribed to this topic. We abstract this routing information away from users of the network by deterministically mapping each application's messages to a specific shard through a process called autosharding. Within autosharding a content identifier provided by the application hashes deterministically and perpetually to one of The Waku Network shards. The network can be scaled beyond these eight shards, by simply increasing the number of shards that messages are mapped to in subsequent network generations.

B. Peer Discovery

Nodes can bootstrap connection to The Waku Network either by statically connecting to any known peer(s) in the network or by retrieving one of several authenticated, published lists of known, long-lived peers. For the latter, Waku nodes will by default use DNS-based discovery as per EIP-1459 [8]. Once connected, Waku nodes use Node Discovery v5 [9] to continuously discover new peers in The Waku Network. This is a decentralized method based on regular random walks through a distributed hash table (DHT) of encoded peer addresses. All discovery methods encode peer information in Ethereum Node Records (ENRs) [10]. Nodes also encode The Waku Network shards they are subscribed to in their discoverable ENRs as per 31/WAKU2-ENR [11]. This information can be used by nodes to filter discovered peers to find the subset subscribed to the same shards as the discovering node.

C. Rate limiting

The Waku Network uses 32/RLN-V1 [11] zero-knowledge proofs to mitigate against spam/DoS attacks by rate limiting publishers. A proof is generated and attached to each message, allowing all relaying nodes to validate in a privacy-preserving manner that [12]:

1) the publisher holds a currently valid membership (without revealing which membership)
2) the pre-agreed rate limit for publishing is not exceeded

The membership set is maintained on-chain and tracked by each node in the network. Only the nodes with a valid membership are allowed to publish messages. The rate limit is currently set to one message per second for each member.

However, a new version of RLN proofs, 58/RLN-V2 [11], is currently being integrated that will allow for more flexible message rates depending on specific application needs.

D. Services

Waku also defines a set of protocols on top of Waku RLN Relay for services generally useful in decentralized applications. The following service protocols are provided in the network:

- **Waku Filter** to allow resource-restricted peers to subscribe to messages matching a specific content filter.
- **Waku Store** to allow other peers to request historical messages from the service provider.
- **Waku Lightpush** to allow resource-restricted peers to request the the service provider to publish a message to the network on their behalf.
- **Waku Peer Exchange** to allow resource-restricted peers to discover more peers in a resource-efficient way.

These services are opt-in, but configured by default on every participating node in the network. We are working on various incentivization vectors to encourage proliferation of high-quality service providers in the network. This is discussed next in Section III-E.

E. Sustainability

Sustainability implies providing long-term incentives for participants to join the network. We consider two aspects, namely, the incentives for Waku nodes to run the Relay protocol (relay messages), and to provide services for resource-restricted clients.

Waku RLN Relay has inherent value for participants. Nodes join the network to get access to its functionality, namely, broadcasting their own messages and receiving messages of interest relayed by others. This is largely in line with non-monetary incentivization of P2P protocols underlying permissionless blockchain.

RLN Relay nodes can provide additional services, such as Store, Filter, and Lightpush (see Section III-D). This activity can be incentivized in a service marketplace, which contains mechanisms for service discovery, price advertisement and negotiation, and privacy-preserving payment. First, a client discover service providers that provide the required service. The client differentiates between service providers based on their offered services, pricing, and reputation. For reputation scoring, a decentralized protocol such as Eigentrust [13] can be used. The client then pays the selected service provider in a privacy-preserving manner and receives the service. These mechanics can be applied not only to Store, Lightpush, and Filter, but also to establish a generalized services marketplace, where third-party providers offer their services using Waku as infrastructure.

IV. Conclusion

In this paper, we presented the design and implementation of The Waku Network, a decentralized messaging infrastructure built upon Waku protocols. We discussed its architecture and scalability, including routing and sharding mechanisms, peer discovery methods, privacy-preserving rate limiting, and services useful to resource-restricted devices. We also considered long-term sustainability of the infrastructure, highlighting monetary and non-monetary incentives for nodes to participate in the network. The Waku Network offers a scalable, privacy-preserving, and censorship-resistant communications solution suitable for various decentralized applications. Future work includes further optimization, integration of new protocols, and enhancement of incentivization mechanisms to ensure the network's long-term sustainability.

References

[1] *10/WAKU2 Waku v2*, en, RFC. [Online]. Available: https://rfc.vac.dev/spec/10/ (visited on 02/15/2024).

[2] O. Thorén, S. Taheri-Boshrooyeh, and H. Cornelius, "Waku: A Family of Modular P2P Protocols For Secure & Censorship-Resistant Communication," in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, ISSN: 2332-5666, Jul. 2022, pp. 86–87. DOI: 10.1109/ICDCSW56584.2022.00024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9951165/ (visited on 02/15/2024).

[3] *Activitypub official website*, https://www.w3.org/TR/activitypub/, Accessed: 2024-02-27, 2024.

[4] *Farcaster official website*, https://docs.farcaster.xyz, Accessed: 2024-02-27, 2024.

[5] S. T. Boshrooyeh, O. Thorén, B. Whitehat, W. J. Koh, O. A. Kilic, and K. Gurkan, "Privacy-preserving spam-protected gossip-based routing," in *ICDCS*, IEEE, 2022, pp. 1286–1287.

[6] *Libp2p specifications*, Feb. 2024. [Online]. Available: https://github.com/libp2p/specs.

[7] D. Vyzovitis, Y. Napora, D. McCormick, D. Dias, and Y. Psaras, "Gossipsub: Attack-resilient message propagation in the filecoin and ETH2.0 networks," *CoRR*, vol. abs/2007.02754, 2020. arXiv: 2007.02754. [Online]. Available: https://arxiv.org/abs/2007.02754.

[8] *Node discovery via dns*, https://eips.ethereum.org/EIPS/eip-1459, Accessed: 2024-02.

[9] *Node discovery protocol version 5.1*, https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md, Accessed: 2024-02.

[10] *Ethereum node records (enr)*, https://eips.ethereum.org/EIPS/eip-778, Accessed: 2024-02.

[11] *Waku specifications*, https://rfc.vac.dev, Accessed: 2024-02.

[12] *Strengthening Anonymous DoS Prevention with Rate Limiting Nullifiers in Waku — Vac Research*, en, Nov. 2023. [Online]. Available: https://vac.dev/rlog/rln-anonymous-dos-prevention (visited on 02/15/2024).

[13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks," in *WWW*, ACM, 2003, pp. 640–651.