Decentralized Messaging Protocol

- White Paper -

Malik Karaoui — contact@wp4f.org — www.wp4f.org

INTRODUCTION

From e-mail to chat to collaborative spaces, digital dialogue has become a fundamental social infrastructure—now essential to our society. In exchange for convenience, many users entrust their conversations to central platforms. This dependency opens the door to content filtering, censorship, and extensive data collection. This document describes a decentralized protocol dedicated to peer-to-peer exchanges, aiming for a simpler framework: communicating freely over the existing internet.

Today, a smartphone is already a small server: permanently connected to the internet, equipped with significant computing power and local storage. The industry has largely steered these capabilities toward capturing attention and monetizing screen time through advertising. This protocol takes the opposite approach: it uses edge computing in service of the user. The time you spend using it works for you — it strengthens peer-to-peer delivery, network resilience, and the confidentiality of your messages.

INSPIRATIONS

The protocol draws inspiration from well-known architectures, pushing their logic to a breaking point:

- Bluetooth Mesh: Proof that a mesh network can transmit without central infrastructure (general idea of decentralization).
- BitChat (Jack Dorsey) – An offline-first Bluetooth mesh approach for extreme situations with no network (outside our current scope).
- Ethereum - “Purge” and lightweight design: keep only what’s essential to remain fast and lean.
- Bitcoin – Remarkably robust, yet its global history is not well-suited for instant messaging.
- Polkadot & Cosmos: Specialized domains linked by bridges; here, we use dedicated sub-networks with modular interconnection.
- Positioning: The intended use is everyday messaging where the internet is available. The protocol does not embed Bluetooth transport and does not use Tor.

CURRENT STATE OF MESSAGING

- High infrastructure costs: servers, maintenance, security, and ever-growing, energy-hungry data centers (optical networks, cooling, carbon footprint).
- Economic centralization: to fund infrastructure, ads, subscriptions, and data exploitation have become the norm.
- Censorship and filtering: beyond outages, the real risk lies in the power of a central actor to block, delist, or throttle messages.

DISCORD

- Reliance on a few control points has shown its limits: pressure on founders, blocked updates, removal of content, or large-scale channel shutdowns—without effective recourse for the affected individuals.
- Lesson from Bitcoin — The BTC white paper addressed a structural abuse: the ability to block and filter.
  Bitcoin also eliminated a precise issue in its domain: the double-spending problem. Without drawing a direct comparison, we retain the guiding principle: a protocol can reduce an abuse through its very design.
  Here, the goal is to curb censorship and the capture of user data.

PROTOCOL PRINCIPLES

1. PEER-TO-PEER OVER THE INTERNET

The transport layer is the everyday internet (mobile data, Wi-Fi). Devices act simultaneously as clients and servers, forming a peer-to-peer overlay. No proprietary servers are required. No volunteer servers or external relays.

Chaining & checkpoints

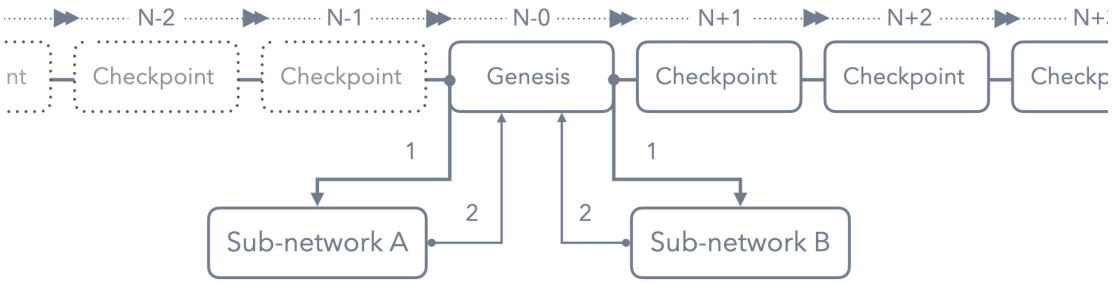

Figure 1 — Periodic chaining highlighting the “Genesis” block and checkpoints.

2. DYNAMIC SUB-NETWORKS

Sub-networks form whenever exchanges become recurrent (family, team, event). Lifecycle: creation → adjustments → merge/fork if needed → idle/purge → extinction (auto-deletion) after prolonged inactivity.

3. DISTINCT SCOPES

Sub-networks remain independent in their operation. A single person can belong to several sub-networks and decide what to relay between them, without duplicating global histories.

4. CONTINUOUS ROUTING & LEARNING

The network learns to favor shorter, more reliable paths (based on observed latency and availability) without becoming dependent on any particular node.

5. PRIVACY BY DEFAULT

End-to-end encryption with locally-held keys. No central collection of metadata. Controlled retention (durations, purging, local export).

UTILITY-DRIVEN ECONOMY

Useful participation — availability, quality of relaying, maintaining a minimal index — can be recognized by the protocol and translated, for each participant, into utility-based yield. The intent is to align individual incentives with the common good: if, over time, value emerges, part of it can be dedicated to a foundation that supports the project and its further development.

Message Delivery via User Relays

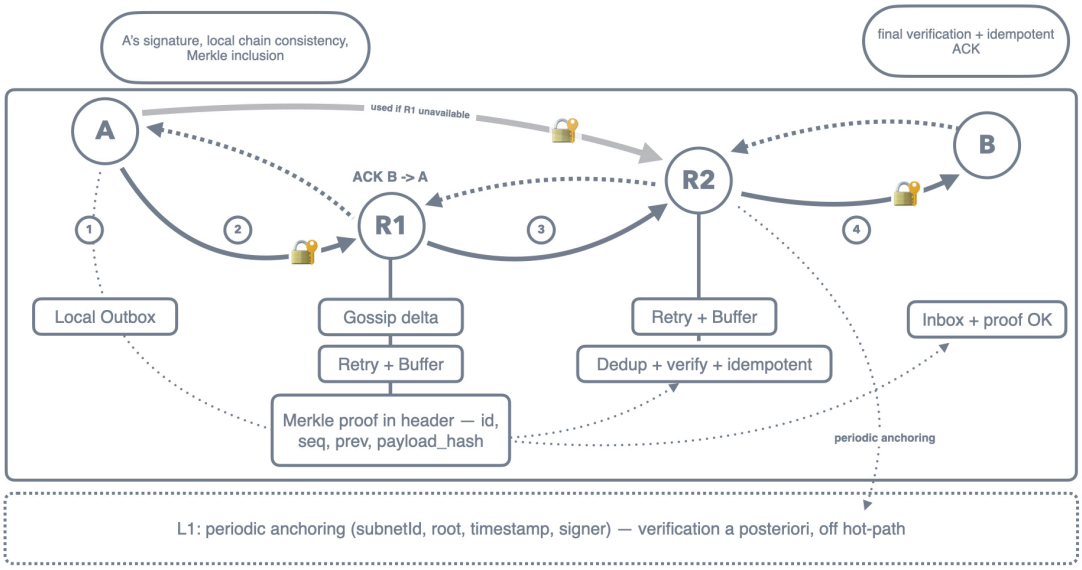

Figure 2 — Sending A → B through relays R1/R2 — network peers. Store-and-forward, verifications, and robust acknowledgments.

ATTACK SURFACE: PROTECTIONS BY DESIGN

- No single point of failure — a DDoS usually targets a specific address or central server. Here, traffic is spread across peers and routes can change on the fly.
- Encrypted traffic — to an external observer, the peer-to-peer flow remains unreadable.
- Purge & lightweightness — less exploitable history means less interest in mass re-analysis.
- Automatic re-routing — in case of local disruption, messages follow alternate paths.
- Reduced economic surface — no central hub to ransom, no single database to steal.

CONCLUSION

Let’s set the record straight: communication should not depend on intermediaries that filter, capture, or charge for the obvious. This peer-to-peer protocol relies on the everyday internet; it is lean, resilient, and truly governed by its users.

No hub to ransom, no massive history to exploit: only peer-to-peer exchanges, encrypted and under user control. As long as it remains useful, the protocol lives — and when its usefulness fades, it erases itself. The world evolves; so should our messaging. Let’s take back control of our conversations.

Stop selling our data for a service that has become essential.