Ligita ˶li8ita″: A Serverless, Privacy-Preserving, Peer-to-Peer Geolocation Lookup Protocol

Abstract *Ligita is a fully peer-to-peer, serverless geolocation lookup protocol that enables users and applications to discover nearby entities (devices, users, or items) without revealing their raw GPS coordinates to any centralized service. No cloud backend, no gateway collectors, no central identity services, and no third-party location storage exist in the system. All proximity computation occurs client-side or through direct peer-to-peer encrypted messages. This publication discloses the architecture, hashing mechanisms, message formats, security model, lookup algorithm, and protocol flows to establish this system as prior art.*

1. Background & Prior Art Most location-based services rely on centralized servers to collect, index, and store user geolocation data. Examples include mobile check-in services, fleet tracking platforms, advertising systems, and real-time location systems (RTLS). Some prior research explores mesh networks and offline Bluetooth discovery, while others explore server-coordinated private set intersection (PSI) for matching locations. Blockchain-based proof-of-location models require cryptographic verifiers or validators acting similarly to servers. Ligita differs fundamentally: - No server, validator, gateway, or coordinator exists. - No global or central index stores location.

2. Problem Statement Users need to discover “What or who is near me?” without exposing raw GPS, history, or identity to any central service. Traditional systems either break privacy (central servers) or lack scalability (offline Bluetooth-only mesh). The problem: How can proximity discovery work globally, in real-time, without a backend or data aggregation? Ligita solves this.

3. System Overview - Devices periodically compute a neighbouring net and geospatial hash for their GPS coordinates. - All communication is end-to-end encrypted. - No persistent logs or server storage exist.

8. Security & Privacy Model - No central servers → nothing to hack or subpoena - No storage of historical location - Full end-to-end encrypted sessions between consenting peers - No IP-level correlation stored

9. Implementation Notes Ligita can be implemented over: - Any P2P overlay with DHT capabilities Works with: - Mobile apps (Android/iOS) - Desktop clients - IoT devices

10. Claims-Like Disclosure 1. A method to perform proximity discovery without servers, No storage of raw GPS or identity in any central system.

12. Novelty No known system combines: - Real-time proximity - Serverless routing - DHT geographic lookup - Internet-based P2P (not offline mesh)

This document establishes public prior art as of its publication date.