Web8- Decentralized Verified Domain System (DVDS)

Web8: Decentralized Verified Domain System (DVDS)

Executive Summary

The Web8 (Decentralized Verified Domain System (DVDS)) also known as **“New Internet”** is a blueprint for a high-integrity, community-powered DNS alternative. Unlike traditional DNS, which relies on a hierarchical chain of trust, or blockchain-based DNS, which requires expensive gas fees, DVDS utilizes a Centralized Registry with Decentralized Verification.

By combining a Merkle Tree "Source of Truth" with a peer-to-peer (P2P) mesh of volunteer nodes, the network provides fast, cryptographically proven domain resolution while rewarding contributors with a proprietary Virtual Coin—all without the complexity of a blockchain.

The Problem

Traditional DNS (Domain Name System) is vulnerable to "cache poisoning" and "man-in-the-middle" attacks where a malicious actor can redirect a user to a fake website. Existing decentralized solutions often require users to interact with complex crypto wallets or pay high fees to register a simple name. There is a need for a system that is easy for the end-user (phone settings only) but trustless in its execution.

System Architecture

The network operates through three distinct layers: the Registry, the Volunteer Mesh, and the User Gateway.

Phase 1: The Registry (The "Source of Truth")

The Registry serves as the ultimate authority for domain-to-IP mappings.

- **The Table**: A simple database of domain pairs (e.g., mysite.www > 17.253.144.10).
- **The Merkle Tree:** To avoid sending the entire database to every user, the Registry compiles all pairs into a Merkle Tree.
- **The Root Hash:** A unique, 32-byte "Global Fingerprint" is generated. This hash is published at a static, public URL.

Phase 2: The Volunteer Mesh (The "Workers")

Volunteers provide the infrastructure. They run a Python-based node that performs three functions:

- **Synchronization:** Downloads the domain list and recreates the Merkle Tree locally.
- **P2P Communication:** Uses libp2p to "gossip" with other volunteers, ensuring data is available even if the Registry goes offline.
- **Proof Generation:** When a request comes in, the volunteer doesn't just send the IP they send a Merkle Proof (a path of sibling hashes) that proves the IP belongs to the Root Hash.

Phase 3: The User Experience

The beauty of DVDS is its simplicity for the consumer.

- **Zero-Install:** The user does not need an app. They simply update their phone's "Private DNS" or "DNS Server" setting to the IP of a Master Volunteer (VPS).
- **Standard Query:** The phone sends a standard UDP/TCP request on Port 53.

Verification & Security (The "Light Client")

To ensure volunteers aren't redirecting users to phishing sites, the Master Volunteer acts as a Judge. When a volunteer provides an IP, the Master Volunteer runs a cryptographic check if the Calculated Hash matches the Global Root Hash published by the Registry, the data is verified. The user is then safely directed to the correct website.

Economic Model: The Virtual Coin

To incentivize uptime and honest behavior, the system employs a reward mechanism.

- **The Receipt:** Upon successful verification of a domain, the Master Volunteer signs a digital receipt.
- **The Mint:** This receipt is uploaded to the Registry's "Bank".
- **Ledger Update:** The Registry increments the volunteer's balance: Volunteer_Balance += 1 VC.
- **Redemption:** While not a cryptocurrency, these Virtual Coins can be used for leaderboard ranking, premium features, or internal ecosystem rewards.

Implementation Roadmap

To bring this white paper to life, development is categorized into three core scripts:

- **The "Bank" Script:** Merkle Root generation and receipt validation.
- **The "Volunteer" Script:** libp2p mesh networking and proof generation.
- **The "Proxy" Script:** DNS request handling and Light Client verification.

Reference

- Camarillo, G. (Ed.). (2010). Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability. IETF. RFC 5694. https://www.rfc-editor.org/rfc/rfc5694.html
- Jeon, J., & Park, S. (2024). Setonix: Blockchain-Based Hierarchy Domain Name System for Web3. Applied Sciences, 14(23), 11213. https://doi.org/10.3390/app142311213
- Merkle, R. C. (1987). A Digital Signature Based on Entity Names. In: Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg.
- Mockapetris, P. (1987). Domain Names - Implementation and Specification. IETF. RFC 1035. https://www.rfc-editor.org/rfc/rfc1035.html
- Protocol Labs. (2024). libp2p: A modular network stack. libp2p.io. https://libp2p.io/spec/
- Yang, G., et al. (2025). Decentralized Domain Name System (DDNS): Analysis of Zero-Trust Verification. UC Berkeley School of Information.
- Zhu, X., et al. (2023). An Efficient Decentralized Identity Management System Based on Range Proof for Social Networks. IEEE Open Journal of the Computer Society, 4, 84-96. https://doi.org/10.1109/ojcs.2023.3258188

Note: *This Idea was my but the white paper is written by AI, because I don't know how to write a white paper so I shared the idea with AI to make this paper so it may contain some typos, mistakes or misinformations. Also this Idea is still in development and may change in future.*

Thank you

Published on 27 February 2026
sanagkerkar45@gmail.com