香港科技大學
THE HONG KONG
UNIVERSITY OF SCIENCE
AND TECHNOLOGY

DDNS: Web3.0 Data Decentralized Infrastructure

Institute of Web3.0 HK

May 2025

Zhang Jingyang

Contents

1 Objective

This report aims to analyze the Decentralized Domain Name System (DDNS) in the Web3.0 ecosystem, based on Professor James Lei's research. The objective is to understand how DDNS transforms data asset addressing and ownership, enabling a paradigm shift from platform-controlled data (Web2.0) to user-owned digital assets (Web3.0).

2 Problem Description

The current Web2.0 architecture presents several fundamental problems:

- Asymmetric value extraction where platforms own and control user data
- Centralized storage systems that create single points of failure
- Users have limited sovereignty over their digital assets
- Data producers rarely receive compensation for the value they create
- Traditional DNS relies on centralized authorities, compromising censorship resistance

DDNS addresses these issues by reimagining how data assets are identified, accessed, and controlled in a decentralized environment.

3 Technical Architecture

3.1 Core Components

DDNS implements a multi-layered architecture that distributes naming resolution and data control across a decentralized network:

3.1.1 DDNS Chain Nodes

The system deploys nodes across various environments:

- Cloud environments (financial institutions, service providers, data centers)

- Edge infrastructure (telecom networks, mobile systems)
- Business environments (API integration points)
- Home environments (AI Agent Boxes, consumer devices)

These nodes form a resilient network that validates name registrations and updates through consensus mechanisms.

3.1.2 Data Wallet Integration

The DDNS architecture includes:

- Cryptographic binding between user identities and data assets
- Smart contracts that point to user data wallets
- Granular permission controls for asset access

3.1.3 Addressing Format

DDNS employs a unique addressing format (e.g., Web3.0://mind33762/peter/HKUST/NT/HK) that connects directly to user-owned data wallets, replacing traditional DNS formats.

3.1.4 Token Function Calls

The system implements token function calls structured as:

$$\text{Token\_Function\_Call}(\text{App\_Para} \text{ —— } \text{Chain\_Para}) \tag{1}$$

This structure bridges application parameters with blockchain parameters, enabling programmatic access to tokenized assets.

3.2 Protocol Layers

3.2.1 Name Resolution Layer

This layer handles:

- Translation of human-readable names to cryptographic addresses

- Caching mechanisms to improve performance
- Fallback systems for network resilience

3.2.2 Data Rights Layer

The rights management layer:

- Encodes ownership and access rights as ”packetized digital rights objects”
- Implements time-bound, context-sensitive permissions
- Maintains auditable access logs on-chain

3.2.3 Value Exchange Layer

This layer facilitates:

- Tokenized compensation for data sharing
- Micro-payment channels for continuous data access
- Value distribution mechanisms for multi-party data contributions

4 Security and Privacy Considerations

4.1 Threat Models

The DDNS system must address various security threats:

4.1.1 Name Squatting

- Risk: Malicious registration of valuable or trademarked names
- Mitigation: Reputation systems, name registration fees, challenge periods

4.1.2 Eclipse Attacks

- Risk: Isolating a user by surrounding them with malicious nodes
- Mitigation: Randomized node selection, node diversity requirements

4.1.3 Smart Contract Vulnerabilities

- Risk: Bugs in permission logic leading to unauthorized access
- Mitigation: Formal verification, code audits, upgradeable contracts

4.1.4 Key Management Risks

- Risk: Private key theft leading to unauthorized data access
- Mitigation: Multi-signature requirements, social recovery options, hardware security

4.2 Privacy Enhancements

DDNS incorporates advanced privacy technologies:

4.2.1 Zero-Knowledge Proofs

These cryptographic methods verify data properties without revealing the data itself, supporting selective disclosure of information.

4.2.2 Homomorphic Encryption

This enables computation on encrypted data, allowing AI processing without exposing raw data.

4.2.3 Data Minimization

The system grants access only to specific data fields required for a function and implements temporal access limitations with automatic expiration.

5 Scalability and Extensibility

5.1 Performance Considerations

DDNS addresses scalability through multiple approaches:

5.1.1 Hierarchical Resolution

- Localized resolution for faster response times
- Multi-level caching strategies

5.1.2 Sharding Approaches

- Horizontal partitioning of the naming space
- Domain-specific subchains for specialized use cases

5.1.3 Layer 2 Solutions

- Off-chain resolution with periodic on-chain anchoring
- State channels for high-frequency updates

5.2 Interoperability

The system ensures compatibility across different ecosystems:

5.2.1 Cross-Chain Compatibility

- Bridge protocols to existing blockchain ecosystems
- Universal resolvers for multi-chain asset addressing

5.2.2 Legacy System Integration

- DNS-to-DDNS gateways
- API compatibility layers for Web2 applications

5.2.3 Standards Compliance

- Alignment with W3C DID specifications
- Compatibility with emerging data sovereignty frameworks

5.3 Future Directions

DDNS development roadmap includes:

5.3.1 AI-Enhanced Resolution

- Context-aware name resolution based on user behavior
- Predictive caching of frequently accessed assets

5.3.2 IoT Integration

- Addressing schemes for billions of connected devices
- Lightweight client implementations for resource-constrained devices

5.3.3 Governance Evolution

- DAO-based protocol management
- Token-weighted voting on technical parameters and feature additions

6 Conclusions

DDNS represents a fundamental evolution in how we conceptualize digital asset ownership and addressing in the Web3.0 era. The system transforms the internet architecture from a platform-centric model to a user-centric data ecosystem where:

- Users maintain sovereignty over their digital assets
- Data producers directly receive value for their contributions
- Decentralized infrastructure reduces platform dependency
- Peer-to-peer trading of storage and network resources becomes possible

By implementing a robust naming system with granular permission controls, DDNS enables the Web3.0 vision of a more equitable digital economy. The architecture supports the evolution from passive web consumers to active ”data prosumers” who both produce and consume digital assets.

Future work should focus on:

- Improving resolution speed without compromising security
- Simplifying the user experience for non-technical adopters
- Developing standardized interfaces for application developers
- Expanding the ecosystem of compatible services and tools

DDNS has the potential to revolutionize various sectors by creating trustworthy data asset networking with AI computing capabilities across home, business, edge, and cloud environments. This transition represents not just a technical evolution but a fundamental reimagining of the relationship between users and their digital footprint.