Blockchain-Based Decentralized Domain Name System

Guang Yang, Peter Trinh, Alma Nkemla,
Amuru Serikyaku, Edward Tatchim, Osman Sharaf
{guangyang19, trinhp, almankemla, amuru, edwardtatchim, sharafosman}@berkeley.edu
University of California, Berkeley

***Abstract*—The current Domain Name System (DNS) infrastructure faces critical vulnerabilities including poisoning attacks, censorship mechanisms, and centralized points of failure that compromise internet freedom and security. Recent incidents such as the APT Group StormBamboo DNS poisoning attacks on ISP customers demonstrate the urgent need for resilient alternatives. This paper presents a novel blockchain-based Decentralized Domain Name System (DDNS). We designed a specialized Proof-of-Work blockchain to maximize support for DNS-related protocols and achieve node decentralization. The system integrates our blockchain with IPFS for distributed storage, implements cryptographic primitives for end-to-end trust signatures, achieving Never Trust, Always Verify zero-trust verification. Our implementation achieves 15-second domain record propagation times, supports 20 standard DNS record types, and provides perpetual free .ddns domains. The system has been deployed across distributed infrastructure in San Jose, Los Angeles, and Orange County, demonstrating practical scalability and resistance to traditional DNS manipulation techniques. Performance evaluation shows the system can handle up to Max Theor. TPS 1,111.1 tx/s (minimal transactions) / Max Theor. TPS 266.7 tx/s (regular transactions) for domain operations while maintaining sub-second query resolution through intelligent caching mechanisms.**

***Index Terms*—Blockchain, Decentralized DNS, Proof of Work, UTXO Model, Anti-Censorship, Cryptographic Verification, IPFS, Domain Name System**

I. Introduction

A. Problem Statement

The modern internet's Domain Name System (DNS) represents a critical infrastructure vulnerability that undermines both security and freedom of information. Two primary categories of threats have emerged as systemic challenges:

DNS Security Vulnerabilities: The centralized architecture of traditional DNS systems creates attractive targets for sophisticated attacks. Recent evidence includes the APT Group StormBamboo attacks, which compromised ISP-level DNS infrastructure to redirect legitimate traffic to malicious endpoints [1]. These poisoning attacks exploit the inherent trust relationships in hierarchical DNS resolution, demonstrating how centralized control points become systemic weaknesses [35], [36].

Censorship and Access Restrictions: Authoritarian regimes and restrictive governments increasingly employ DNS-based censorship as a mechanism for information control. Large-scale DNS record manipulation and selective blocking of domain resolution violate fundamental principles of information freedom and democratic access to knowledge. This systematic interference with DNS infrastructure represents a technological assault on human rights to free expression and access to information.

The mathematical formulation of these problems can be expressed as single points of failure in the DNS resolution chain:

$$P_{failure} = 1 - \prod_{i=1}^{n}(1 - p_i) \tag{1}$$

where p_i represents the failure probability of the i-th centralized component in the DNS hierarchy, and n is the number of critical control points.

B. Motivation

Traditional DNS systems operate under a trust model that is susceptible to single point of failure problems and prone to security and availability risks. The hierarchical structure creates dependencies on centralized authorities (root servers, top-level domain registrars, ISPs) that can be compromised, coerced, or corrupted. This centralization enables attacks that violate the CIA (Confidentiality, Integrity, Availability) security principles:

- **Single Point of Failure Attacks:** Compromising availability (Availability), where compromise of authoritative servers can affect millions of domains simultaneously
- **State-Level Censorship:** Compromising confidentiality (Confidentiality), where governments can mandate DNS filtering at ISP or national levels
- **Commercial Manipulation:** Compromising availability (Availability), where domain registrars can unilaterally suspend or transfer domains
- **Data Integrity Violations:** Compromising integrity (Integrity), where DNS responses lack cryptographic verification, enabling man-in-the-middle attacks

The proliferation of these attacks necessitates a paradigm shift toward cryptographically secured, decentralized domain name zero-trust resolution that ensures confidentiality and integrity. This paradigm eliminates central points of control, thereby ensuring performance and availability.

C. Our Contribution

This paper presents a comprehensive blockchain-based decentralized DNS system (hereinafter referred to as DDNS) that addresses these fundamental limitations through:

1) **DDNS Blockchain Infrastructure:** The project codename is Phicoin, representing an acronym for Proof of

Work High-performance Infrastructure, aimed at building a fully decentralized blockchain network using PoW mechanism. A purpose-built Proof-of-Work blockchain optimized for domain asset management using modified UTXO model with enhanced transaction throughput (4MB blocks, 15-second intervals)

2) **Cryptographic Trust Chain:** End-to-end verification using elliptic curve digital signatures (ECDSA) for domain registration and modification, eliminating reliance on third-party trust
3) **Distributed Storage Integration:** IPFS-based domain control file storage with content-addressable hashing for tamper-evident record management
4) **Anti-Censorship Architecture:** Mesh network communication patterns and distributed resolver infrastructure that circumvents traditional blocking mechanisms
5) **Cross-chain Integration:** We developed cross-chain bridges capable of connecting the DDNS blockchain to other smart contract-enabled blockchains such as Solana and Ethereum. We have deployed smart contracts on Solana, enabling the 15 million monthly active users (MAU) of Solana to directly utilize DDNS services for domain registration and updates without downloading node clients.
6) **Edge DDNS Resolution Services:** We developed edge DDNS servers that enable DDNS resolution within organizations without relying on public DDNS services, while maintaining compatibility with traditional DNS resolution. This requires only deploying edge DDNS services within the organization and configuring them as the organization's network DNS servers.
7) **Decentralized Web Protocol (D-WEB):** We implemented a decentralized D-WEB protocol based on DDNS TXT records, which leverages IPFS's capability to resolve static directories, using TXT records to resolve website IPFS hashes, enabling decentralized archiving/access of traditional websites.

II. Related Work

Existing decentralized naming systems have made significant contributions to addressing DNS centralization, but each suffers from fundamental limitations that prevent widespread adoption [2]. Recent surveys on blockchain consensus mechanisms provide comprehensive frameworks for evaluating different approaches to decentralized systems [33], [34].

Ethereum Name Service (ENS): Utilizes Ethereum's smart contract infrastructure for .eth domain management [3]. While innovative, ENS faces scalability constraints due to Ethereum's throughput limitations (Max Theor. TPS 119.1 tx/s) and high transaction costs (gas fees often exceeding $50 per operation). Additionally, ENS domains are not compatible with traditional DNS infrastructure, limiting their utility [48].

Namecoin: The first blockchain-based naming system, forked from Bitcoin to support .bit domains [4]. Namecoin suffers from slow block times (10 minutes), limited throughput, and lack of modern DNS record type support. The system's security relies on merge-mining with Bitcoin, creating potential centralization risks [49].

Handshake: Implements a novel approach using proof-of-work to manage top-level domain auctions [5]. However, Handshake focuses primarily on TLD ownership rather than practical DNS resolution, and its auction mechanism creates significant barriers to entry for users.

While these systems represent important advances in decentralized naming, they each exhibit fundamental trade-offs between security, scalability, and usability that limit their practical deployment. Recent research in blockchain consensus mechanisms has shown that achieving optimal balance between these properties requires careful design of the underlying consensus protocol.

Our system advances the state-of-the-art by combining: - High throughput blockchain infrastructure (Max Theor. TPS 1,111.1 tx/s vs. Max Theor. TPS 119.1 tx/s for Ethereum) - Universal DNS compatibility (supports all standard record types) - Zero-cost operation for .ddns domains - Production-ready resolver infrastructure

TABLE I
Comparison of Decentralized DNS Solutions

Feature	DDNS	ENS	Namecoin	Handshake	Traditional DNS
Decentralized	Yes	Partial	Yes	Yes	No
DNS Compatible	Yes	No	Limited	Limited	Yes
Block Time	15s	12s	10min	10min	N/A
Transaction Cost	Free	$10-50	$0.01	$1-10	$10-100/year
Throughput (TPS)	1,111.1/266.7	119.1	7	7	250 [10]
Record Types	20	Limited	Limited	Limited	20 [9]
Censorship Resist	High	Medium	High	High	Low

III. System Architecture

A. High-Level Design

The DDNS system implements a layered architecture that separates concerns while maintaining cryptographic security guarantees throughout the stack. The design follows the principle of *cryptographic minimalism*, where trust assumptions are explicitly modeled and minimized.

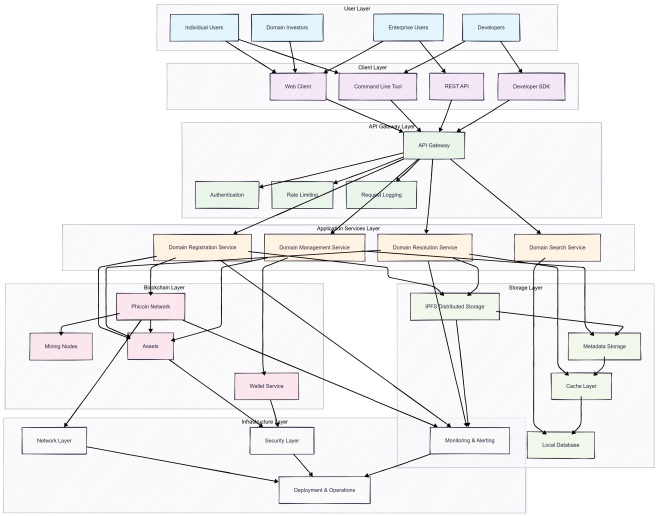


Fig. 1. DDNS System High-Level Architecture

The architecture consists of six primary layers:

User Layer: Supports diverse stakeholders including individual users, enterprises, developers, and domain investors with varying technical requirements and economic models.

Client Layer: Provides multiple interfaces (Web UI, CLI tools, REST APIs, SDKs) for different integration patterns and user preferences.

API Gateway Layer: Implements authentication, rate limiting, and request logging with horizontal scaling capabilities.

Application Services Layer: Core business logic for domain registration, resolution, management, and search with high-availability design.

Blockchain Layer: DDNS network providing cryptographic consensus, asset management, wallet services, and mining infrastructure.

Storage Layer: Distributed storage using IPFS, metadata management, intelligent caching, and local database optimization.

B. Functional Components

The system architecture comprises multiple specialized functional components that work together to provide comprehensive domain management and resolution services.

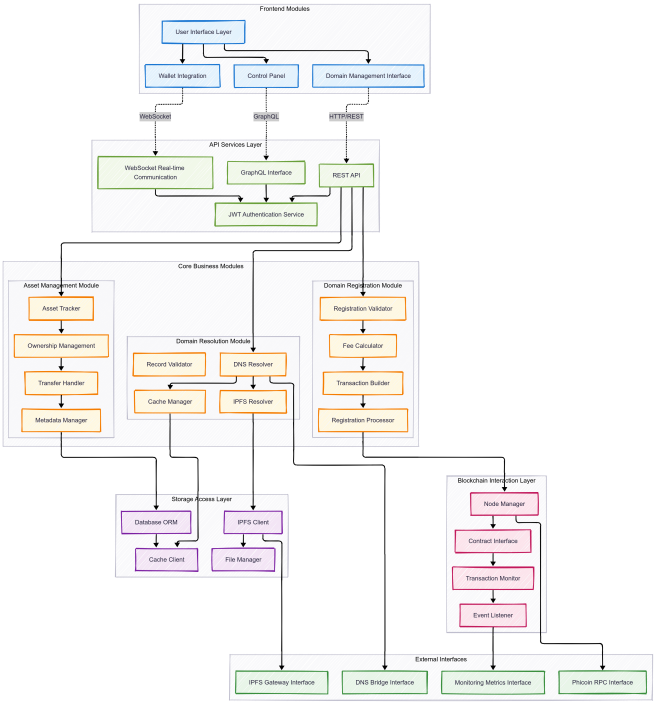


Fig. 2. DDNS Functional Components and Module Interactions

The functional architecture includes core business modules (Asset Management, Domain Registration), domain resolution modules (DNS Resolver, Cache Manager, IPFS Resolver), blockchain integration components (Node Manager, Contract Interface), and storage access layers (Database ORM, IPFS Client, File Manager). The frontend modules provide user interfaces through REST APIs, WebSocket real-time communication, and GraphQL interfaces for advanced querying capabilities.

C. Use Case Analysis

The system supports diverse user personas with varying technical expertise and usage patterns, from individual users seeking simple domain registration to enterprise users requiring bulk domain management capabilities.

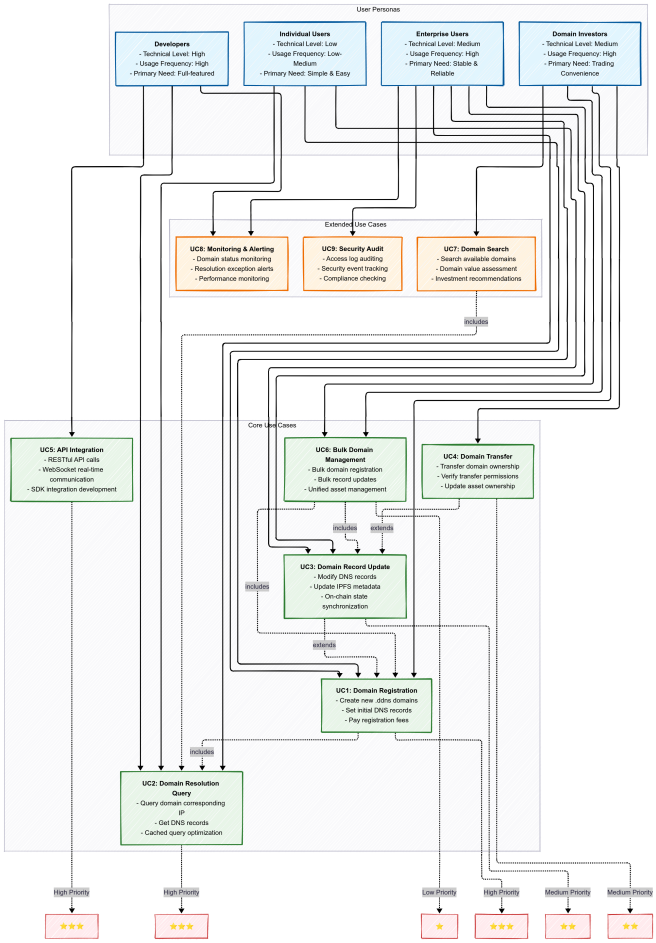


Fig. 3. DDNS Use Case Diagram and User Interactions

The use case diagram illustrates core functionalities including domain registration, record updates, domain resolution queries, bulk domain management, domain transfers, and monitoring/alerting services. Each use case is prioritized based on user needs and technical complexity, with high-priority cases including domain registration and resolution queries that form the foundation of the system.

D. Technology Stack

The DDNS implementation leverages a modern, scalable technology stack designed for high-performance blockchain and distributed systems operations.

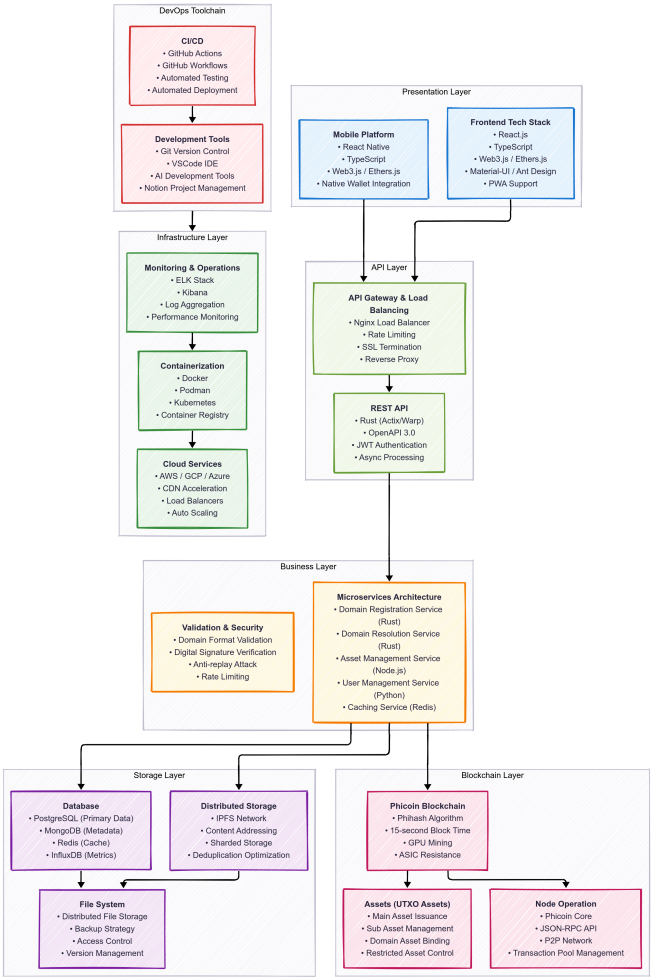


Fig. 4. DDNS Technology Stack and Infrastructure Components

The technology stack spans multiple layers: the presentation layer utilizes React.js for frontend development and React Native for mobile platforms; the API layer implements load balancing with Nginx and RESTful services; the business layer employs microservices architecture with domain-specific services in Rust and Node.js; the storage layer combines distributed storage (IPFS), traditional databases (PostgreSQL, MongoDB), and Redis for caching; the blockchain layer features the custom DDNS blockchain with UTXO asset management; and the infrastructure layer provides containerization with Docker/Kubernetes, monitoring with ELK stack, and DevOps automation.

E. Cryptographic Primitives

The system employs well-established cryptographic primitives to ensure security:

Digital Signatures: Domain operations utilize ECDSA with secp256k1 curve (identical to Bitcoin) for signing transactions. The signature verification process follows:

$$\text{Verify}(m, \sigma, pk) = e(\sigma, G) \stackrel{?}{=} e(H(m) + r \cdot pk, G) \quad (2)$$

where m is the message (domain operation), σ is the signature, pk is the public key, and H is SHA-256 hash function.

Content Addressing: IPFS uses SHA-256 hash function for content addressing:

$$\begin{aligned}\text{IPFS_Hash} = \text{Base58}(\text{SHA256}(\\ \text{ProtoBuf}(\text{Domain_Record})))\end{aligned} \quad (3)$$

This ensures tamper-evident storage where any modification to domain records results in a different hash value.

F. DDNS Blockchain Infrastructure

The DDNS blockchain represents a purpose-built blockchain optimized for domain name service requirements. Key technical specifications include:

Consensus Algorithm: Proof-of-Work using PhihashV2, an ASIC-resistant algorithm designed to prevent network hash power centralization that leads to centralization risks [6], [37]. Additionally, we optimized the DAG structure to enable cache files to run on integrated graphics cards, allowing tens of millions of devices worldwide equipped with integrated graphics to join the mining network at any time, enabling broader network participation and larger-scale decentralized networks. This approach addresses the well-documented mining centralization concerns in PoW systems [39], [40].

Block Parameters: - Block time: 15 seconds (optimized for DNS update responsiveness) - Block size: 4MB Weight Units (WU) = 4,000,000 WU (enabling high transaction throughput) - Difficulty adjustment: Enhanced Dark Gravity Wave algorithm for rapid response

Transaction Throughput: The system achieves theoretical maximum throughput using Weight Units calculation method [6]:

General TPS calculation formula (applicable only to DDNS Blockchain: 4M WU):

$$TPS = \frac{4,000,000}{\text{Average Weight Units per Transaction}} \div 15 \quad (4)$$

Different transaction types yield the following results:

1) Minimal transactions (bare transfers, typically 60 bytes = 240 WU):

$$TPS_{minimal} = \frac{4,000,000}{240} \div 15 \approx 1,111.1 \quad (5)$$

2) Regular transactions (≈ 250 bytes = 1,000 WU):

$$TPS_{regular} = \frac{4,000,000}{1,000} \div 15 = 266.7 \quad (6)$$

Final Results Summary (4M WU):

TABLE II
TRANSACTION TYPES AND THEORETICAL MAXIMUM TPS

Transaction Type	Average Size (WU)	TPS (Theoretical Max)
Minimal Transaction	240 WU	≈ 1,111.1
Regular Transaction	1,000 WU	≈ 266.7

Network Security: Empirical analysis of mainnet performance from block heights 92,594 to 143,669 shows orphan rate of 0.0176% (9 orphaned blocks out of 51,075 total) [8], demonstrating network stability.

G. Domain Asset Model

The system implements a modified UTXO model specifically designed for domain asset management. Each domain is represented as a unique asset with the following properties:

```
{
  "asset_name": "DDNS/EXAMPLE",
  "quantity": 1,
  "units": 1,
  "reissuable": false,
  "has_ipfs": true,
  "ipfs_hash": "QmX7M8RxZ...",
  "owner_address": "PhiCoinAddress123..."
}
```

Listing 1. Domain Asset Structure

Asset Naming Convention: Domains follow hierarchical naming: `ROOT_TLD/DOMAIN_NAME` where ROOT_TLD represents the top-level domain asset (e.g., "DDNS") and DOMAIN_NAME represents the specific domain.

Economic Model: Domain registration requires minimal fees (0.1 PHI ≈ $0.00001) with no recurring costs, implementing true digital asset ownership rather than lease-based models used by traditional DNS. Additionally, we subsidize the gas fees for domain registration. For .DDNS domain registration, we cover all gas fees, thereby achieving permanently free domain services.

H. IPFS Integration and Domain Control Files

Domain records are stored in JSON-formatted control files on IPFS, enabling flexible schema evolution and comprehensive DNS record type support [28]. The control file structure follows RFC-compliant specifications:

```
{
  "version": "2.0",
  "domain": "example.ddns",
  "records": {
    "@": {
      "A": [{"address": "192.168.1.100", "ttl": 3600}]
    },
    "www": {
      "CNAME": [{"target": "example.ddns", "ttl": 3600}]
    },
    "mail": {
      "MX": [{"server": "mail.example.ddns", "priority": 10}]
    }
  }
}
```

Listing 2. Domain Control File Example

This design provides several advantages: - **Schema Flexibility:** JSON format allows arbitrary record types without blockchain protocol changes - **Efficient Storage:** Only IPFS hash stored on-chain, enabling large record sets without blockchain bloat - **Content Verification:** IPFS content addressing ensures data integrity

I. Supported DNS Record Types

The DDNS system provides comprehensive support for 20 different DNS record types, ensuring compatibility with modern internet infrastructure requirements and enabling diverse use cases from simple web hosting to complex service architectures. We have implemented 76 types of domain resolution and control files enumerated in RFC documents. However, we also referenced Cloudflare's protocol resolution settings and selected the 20 most commonly used domain resolution records. The aforementioned control file code and scripts are open-sourced in the ddnsd service, allowing users to configure according to their specific needs.

Core Address Records:

- **A Records [14]:** IPv4 address mapping for standard web services and applications
- **AAAA Records [15]:** IPv6 address mapping supporting next-generation internet protocols
- **CNAME Records [14]:** Canonical name aliases enabling flexible domain management and CDN integration

Mail and Communication Records:

- **MX Records [14]:** Mail exchange server specifications with priority-based routing
- **TXT Records [14]:** Arbitrary text data for SPF, DKIM, domain verification, and custom metadata
- **SPF Records [16]:** Sender Policy Framework for email authentication and anti-spam protection
- **DKIM Records [17]:** DomainKeys Identified Mail cryptographic signatures for email integrity
- **DMARC Records [18]:** Domain-based Message Authentication for comprehensive email security policies

Service Discovery Records:

- **SRV Records [19]:** Service location records defining port and priority for specific services
- **NS Records [14]:** Name server delegation for subdomain management and distributed authority
- **PTR Records [14]:** Reverse DNS lookups enabling IP-to-domain resolution
- **SOA Records [14]:** Start of Authority defining zone management parameters and refresh intervals

Advanced and Specialized Records:

- **CAA Records [20]:** Certificate Authority Authorization controlling SSL/TLS certificate issuance
- **TLSA Records [21]:** Transport Layer Security Authentication for DNS-based certificate pinning
- **SSHFP Records [22]:** SSH Key Fingerprints for secure shell authentication verification
- **URI Records [23]:** Uniform Resource Identifier mapping for advanced service location
- **NAPTR Records [24]:** Naming Authority Pointer for complex protocol transformations
- **LOC Records [25]:** Geographic location information for physical server positioning
- **HINFO Records [14]:** Host information describing system architecture and operating system

- **RP Records [26]:** Responsible Person contact information for domain administration

Record Type Validation: Each record type implements RFC-compliant validation ensuring data integrity and standards compliance. The system performs real-time validation during record updates, preventing malformed entries and maintaining DNS protocol compatibility.

Performance Optimization: Record resolution is optimized through intelligent caching with type-specific TTL policies, reducing resolution latency for frequently accessed record types while maintaining accuracy for dynamic records.

IV. Implementation

A. Blockchain Infrastructure Components

The DDNS network consists of multiple specialized components working in concert:

Core Node Software: Full blockchain nodes implementing the DDNS protocol, maintaining complete transaction history, and participating in consensus.

Mining Infrastructure: Distributed mining pools supporting the PhihashV2 algorithm, with specialized mining software optimized for GPU hardware [7].

Network Discovery: Seeder servers providing initial peer discovery and network health monitoring.

DDNSD Public DDNS Resolution Servers: Distributed public resolution infrastructure providing high-availability domain name resolution services.

DDoH Public DDNS over HTTPS Resolution Servers: Secure DNS resolution services implementing DNS-over-HTTPS protocol for enhanced privacy and censorship resistance.

Cross-Chain Bridge: Smart contract infrastructure on Solana enabling PHI token trading and liquidity provision, creating economic incentives for network participation.

Sustainable Infrastructure: The DDNS network operates on environmentally sustainable infrastructure, including solar-powered data centers that provide carbon-neutral blockchain operations. Our San Jose facility demonstrates the feasibility of renewable energy-powered PoW cryptocurrency block perpetual generation node operations.



Fig. 5. Solar-Powered Data Center Infrastructure in San Jose

The solar infrastructure includes high-efficiency photovoltaic panels, battery storage systems, and optimized cooling solutions that enable 24/7 blockchain node operation with minimal environmental impact. This sustainable approach to blockchain infrastructure addresses growing concerns about cryptocurrency energy consumption while maintaining network security and performance.

B. Domain Registration and Modification Process

The domain lifecycle follows a cryptographically secured process:

Registration Flow:

1) User generates key pair (sk, pk) where sk is private key and $pk = sk \cdot G$ is corresponding public key
2) Create domain control file with initial DNS records
3) Upload control file to IPFS, obtaining hash h_{ipfs}
4) Construct blockchain transaction $tx = \{domain_name, h_{ipfs}, pk\}$
5) Sign transaction: $\sigma = \text{ECDSA_Sign}(sk, H(tx))$
6) Broadcast signed transaction to DDNS network
7) Miners validate signature and include in next block

Modification Flow: Domain updates follow identical process but reference existing asset, ensuring only authorized private key holder can modify records.

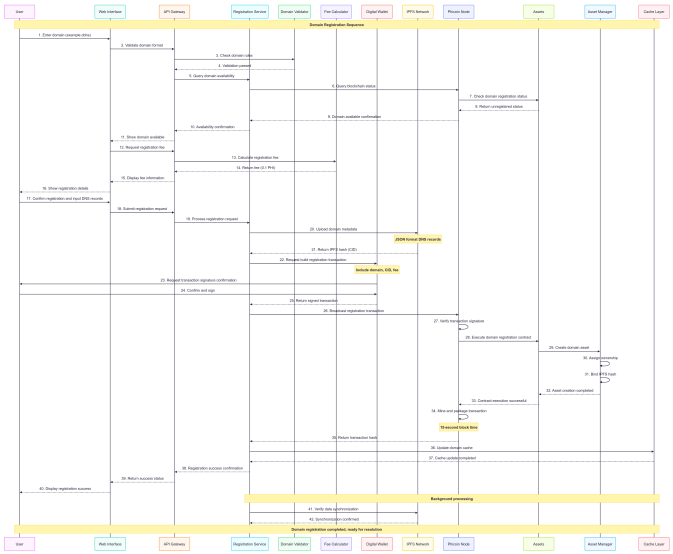


Fig. 6. Domain Registration Sequence Diagram

The domain registration sequence demonstrates the complete end-to-end flow from user initiation through blockchain confirmation. The process involves multiple system components including the Web Interface, API Gateway, Registration Service, Domain Validator, Fee Calculator, Digital Wallet, IPFS Network, DDNS Node, and Asset Manager. Key steps include domain validation, fee calculation, IPFS metadata upload, blockchain transaction creation and signing, and final asset creation with ownership assignment. The sequence emphasizes the cryptographic security at each step and the 15-second block time for rapid confirmation.

C. DNS Resolution Process

The resolution system implements a hybrid approach combining blockchain verification with traditional DNS performance requirements:

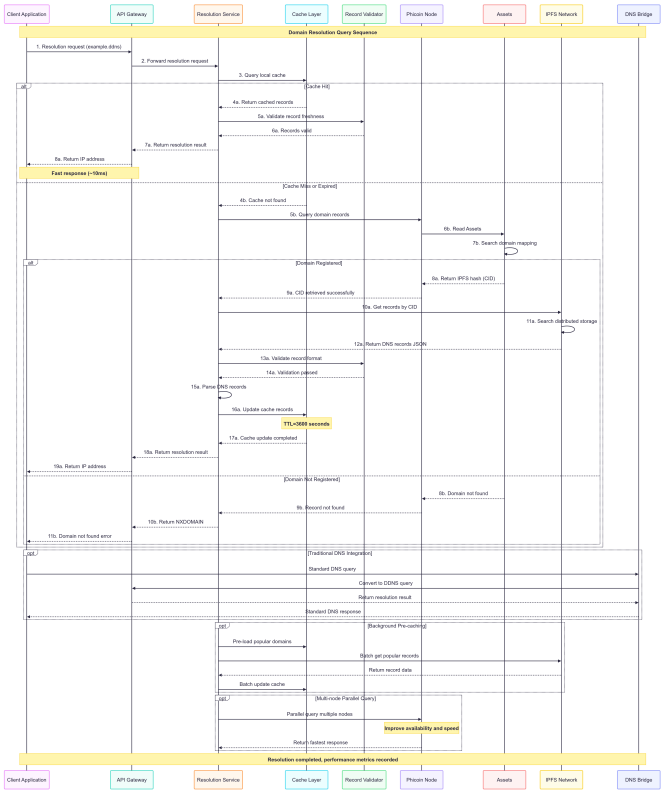


Fig. 7. DDNS Domain Resolution Sequence

Resolution Algorithm:

1) Client queries local DDNSD resolver for domain
2) Resolver checks multi-tier cache (memory $\rightarrow$ file $\rightarrow$ blockchain)
3) If cache miss, query DDNS RPC for domain asset
4) Extract IPFS hash from blockchain record
5) Retrieve domain control file from IPFS
6) Verify $H(\text{control_file}) = h_{ipfs}$ for integrity
7) Parse requested record type and return response
8) Cache result with appropriate TTL

Performance Optimization: The system implements intelligent caching with the following hierarchy: - **L1 Cache:** In-memory LRU cache (50,000 entries, 15-second TTL) - **L2 Cache:** Persistent file cache with longer TTL - **L3 Cache:** Blockchain verification cache for domain ownership

Production Domain Registration and Resolution: To demonstrate the practical functionality and performance characteristics of the DDNS system, we conducted a comprehensive end-to-end evaluation using the production DDNS infrastructure. The evaluation encompasses domain registration, DNS record configuration, resolution performance analysis, and accessibility demonstration.

Domain Registration Process: Using the DDNS web interface at https://d.phicoin.net/, we registered the domain `test01.ddns` and configured TXT records for testing purposes. Figure 8 illustrates the user-friendly domain registration interface, which provides comprehensive DNS record management capabilities including support for A, AAAA, CNAME, MX, TXT, and other standard record types.

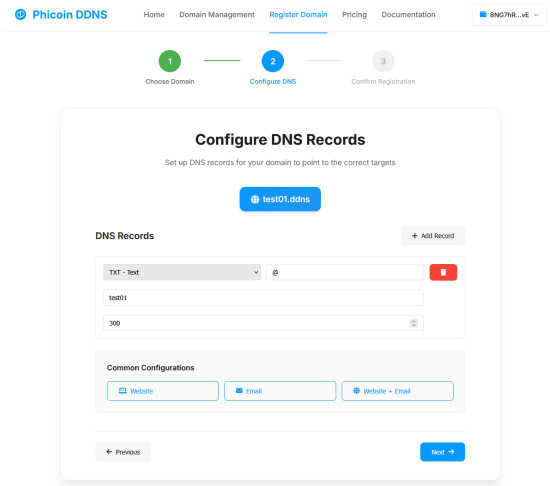


Fig. 8. DDNS Domain Registration and DNS Configuration Interface

DNS Resolution Performance Analysis: To evaluate the system's resolution performance and caching efficiency, we conducted repeated DNS queries using the `dig` utility against the DDNS public resolver at `138.2.235.218`. The performance evaluation demonstrates significant improvements in query response times through intelligent caching mechanisms.

Figure 9 shows the initial DNS query for `test01.ddns TXT`, which required blockchain verification and IPFS retrieval, resulting in a response time of 183 milliseconds. The subsequent query, illustrated in Figure 10, demonstrates the effectiveness of the multi-tier caching system with a dramatically reduced response time of 19 milliseconds, representing a 89.6% performance improvement.

```
(base) ubuntu@[redacted]:~$ dig @138.2.235.218 test01.ddns TXT

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @138.2.235.218 test01.ddns TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42987
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;test01.ddns.                   IN      TXT

;; ANSWER SECTION:
test01.ddns.            0       IN      TXT     "test01"

;; Query time: 183 msec
;; SERVER: 138.2.235.218#53(138.2.235.218) (UDP)
;; WHEN: Tue Jul 29 04:36:17 PDT 2025
;; MSG SIZE  rcvd: 48

(base) ubuntu@[redacted]:~$ dig @138.2.235.218 test01.ddns TXT

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @138.2.235.218 test01.ddns TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10096
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;test01.ddns.                   IN      TXT

;; ANSWER SECTION:
test01.ddns.            0       IN      TXT     "test01"

;; Query time: 19 msec
;; SERVER: 138.2.235.218#53(138.2.235.218) (UDP)
;; WHEN: Tue Jul 29 04:36:27 PDT 2025
;; MSG SIZE  rcvd: 48
```

Fig. 9. Initial DNS Query with Full Blockchain Resolution (183ms)

```
(base) ubuntu@D[redacted]:~$ dig @138.2.235.218 explorer.phi

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @138.2.235.218 explorer.phi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23817
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;explorer.phi.                  IN      A

;; ANSWER SECTION:
explorer.phi.           0       IN      A       138.2.235.218

;; Query time: 84 msec
;; SERVER: 138.2.235.218#53(138.2.235.218) (UDP)
;; WHEN: Tue Jul 29 04:39:35 PDT 2025
;; MSG SIZE  rcvd: 46
```

Fig. 10. Subsequent DNS Query Demonstrating Cache Performance (19ms)

DNS-over-HTTPS Implementation: The system supports modern DNS-over-HTTPS (DoH) protocol for enhanced privacy and security. Figure 11 demonstrates the Firefox browser configuration for utilizing the DDNS DoH endpoint at https://doh.phicoin.net/dns-query. This configuration enables users to access decentralized domains through standard web browsers without additional software installation.

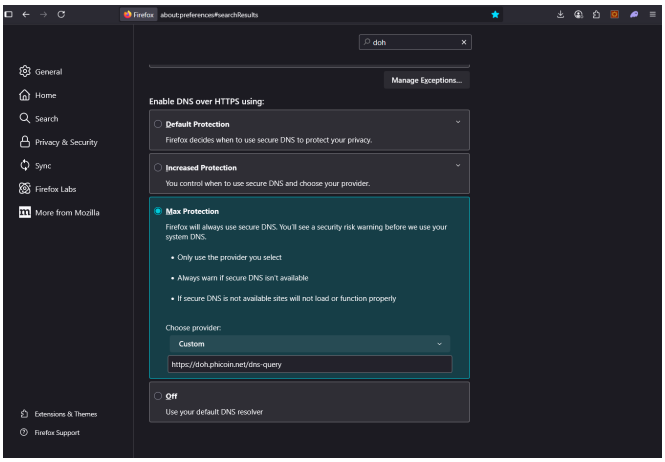


Fig. 11. Firefox DNS-over-HTTPS Configuration for DDNS Resolution

Access to Non-Traditional Domains: A key innovation of the DDNS system is its ability to resolve domains that do not exist in traditional generic top-level domains (gTLDs). To demonstrate this capability, we tested resolution of `explorer.phi`, a custom domain namespace exclusive to the DDNS ecosystem. The successful A record resolution for `explorer.phi` to IP address `138.2.235.218`, with a query response time of 84 milliseconds, demonstrates the system's capability to extend DNS functionality beyond traditional namespace limitations.

Web Accessibility Demonstration: With proper DoH configuration, users can seamlessly access websites hosted on custom DDNS domains through standard web browsers. Figure 12 demonstrates successful access to the Phicoin blockchain explorer at `http://explorer.phi/network`, showcasing the system's ability to provide full web functionality for decentralized domains. The explorer interface displays real-time network statistics including peer connections across multiple geographic regions (United States, China, France, Singapore, Italy, United Kingdom, South Korea, and Thailand), demonstrating the global distribution of the DDNS network infrastructure.

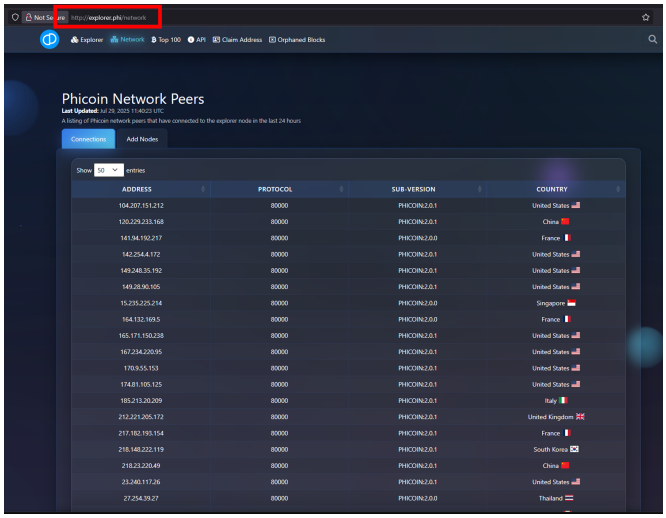


Fig. 12. Successful Web Access to Decentralized Domain explorer.phi

This comprehensive evaluation demonstrates that the DDNS system successfully bridges the gap between blockchain-based domain ownership and practical internet usability, providing both the security benefits of decentralization and the performance characteristics necessary for production deployment.

D. Anti-Censorship Mechanisms

The system implements multiple layers of censorship resistance:

P2P Network Relay: Due to the blockchain's capability to use integrated graphics cards and other entry-level universal devices for mining profits, users from different countries and regions spontaneously organize mining nodes and networks for profit. This PoW mechanism-incentivized user model promotes the network's decentralized characteristics, making it difficult for any single country to ban specific countries or IP addresses. Additionally, this project's blockchain is based on Bitcoin Core implementation, integrating Bitcoin Core's complete Tor network support features, enabling deployment in network-restricted countries and regions through Tor relay using obfuscation methods such as Snowflake or obfs4 [11].

Distributed Resolver Network: DDNSD instances can be deployed independently by any user, creating a mesh of resolution points that cannot be centrally controlled or blocked.

Protocol Flexibility: Support for DNS-over-HTTPS (DoH) enables resolution through standard web protocols, making blocking more difficult for network censors.

Content Mirroring: We developed integration with Telegram bot and D-Web browser enabling one-click website mirroring, allowing rapid content preservation and access restoration. These website contents are deployed on IPFS and resolved through the DDNS D-WEB protocol.

Case Study - Hong Kong Pro-Democracy Movement: During the 2019 Hong Kong anti-extradition movement, protesters extensively used IPFS to prevent protest websites from being deleted [12]. However, a significant problem emerged during the movement: multiple different IPFS addresses appeared simultaneously, with different protesters and organizations using different IPFS addresses to publish information. This created substantial difficulty for users in determining which IPFS addresses published trustworthy information versus potentially false information or government disinformation.

Our DDNS D-web technology addresses this critical trust problem through cryptographic verification. Protesters can register domains such as "hkprotest.ddns" and use private key signatures to ensure only authentic publishers can update the IPFS content referenced by the domain. This mechanism guarantees both confidentiality (Confidentiality) through identity verification and integrity (Integrity) through blockchain and IPFS content addressing, according to CIA principles. Users can verify information source credibility, thereby avoiding the information chaos caused by multiple IPFS addresses and ensuring authentic communication channels during critical political movements.

V. Security Analysis and Trust Chain

A. Cryptographic Security Model

The DDNS system implements a zero-trust security model where all operations require cryptographic verification. The security analysis follows established frameworks for distributed systems [41], [45]. Our approach builds upon comprehensive surveys of blockchain security challenges and mitigation strategies documented in recent literature [46], [47].

Threat Model: We consider adversaries with the following capabilities: - Control over traditional DNS infrastructure - Ability to intercept and modify network traffic - Access to significant computational resources (but bounded by economic constraints) - Coordination between multiple malicious actors

Security Properties: The system provides the following guarantees:

1) **Domain Ownership Integrity:** Only the holder of private key sk corresponding to domain registration can modify domain records, formalized as:

$$\forall tx : \text{Valid}(tx) \Rightarrow \text{Verify}(\text{Hash}(tx), \sigma_{tx}, pk_{domain})$$

2) **Content Integrity:** Domain records stored in IPFS cannot be modified without detection due to content-addressing:

$$\text{Integrity}(record) \equiv H(record) = h_{blockchain}$$

3) **Availability:** The system remains operational as long as any single honest node exists and can communicate with IPFS network.

B. Trust Chain Analysis

The DDNS system distributes trust across multiple independent components, eliminating single points of failure inherent in traditional DNS:

TABLE III
DDNS Trust Chain Components

Component	Trust Assumptions
User Private Keys	Users maintain control of their private keys. Compromise affects only individual domains, not system-wide security.
DDNS Miners	Economic majority acts honestly. Attack cost exceeds potential gains due to Proof-of-Work economics and network value preservation incentives.
IPFS Network	Content remains available through distributed replication. No single IPFS node failure affects system operation.
DDNSD Resolvers	Resolver operators act honestly or users can operate independent resolvers. Open source enables verification and alternative implementations.
Cryptographic	ECDSA and SHA-256 remain computationally secure. Based on well-established assumptions in academic cryptography.

Trust Minimization: The system minimizes trust requirements by: - Eliminating dependence on centralized authorities - Enabling user-operated infrastructure components - Providing cryptographic verification for all operations - Supporting multiple independent implementations

C. Attack Resistance Analysis

DNS Poisoning Prevention: Traditional DNS poisoning attacks target cache servers or DNS resolvers. DDNS prevents these attacks through: - Cryptographic verification of all domain data - Content-addressed storage preventing data modification - Distributed resolution eliminating central cache points

Censorship Resistance: The system demonstrates robust resistance to censorship through multiple technical and organizational mechanisms. According to data from the Open Observatory of Network Interference (OONI) [13], traditional DNS-based censorship affects millions of users globally, with documented cases of systematic blocking across multiple jurisdictions. Our system addresses these challenges through: - Distributed blockchain infrastructure deployed across multiple sovereign jurisdictions, ensuring no single government can

unilaterally disable the network - IPFS content distribution architecture that eliminates single points of control and enables content availability through multiple independent nodes - Protocol-agnostic design enabling operation over HTTP, HTTPS, or custom protocols, providing flexibility against protocol-specific blocking attempts - Integration with Tor network infrastructure and advanced obfuscation techniques including Snowflake relays, enabling deployment and operation in network-restricted environments where traditional internet access faces systematic interference

Scalability and Network Security: The system addresses fundamental scalability challenges in decentralized blockchain networks [42] while maintaining security properties. Network propagation delays and consensus efficiency have been optimized based on analysis of information propagation patterns in peer-to-peer blockchain networks [43].

Economic Attack Resistance: The cost of 51% attack on DDNS network exceeds potential gains:

$$\text{Attack_Cost} = \sum_{i=0}^{t} (\text{Mining_Reward}_i + \text{Electricity_Cost}_i) > \text{Economic_Gain} \tag{7}$$

where t represents the time required to reorganize sufficient blockchain history.

D. Risk Assessment and Management

The DDNS project employs systematic risk management to identify, assess, and mitigate potential threats to system reliability and security.

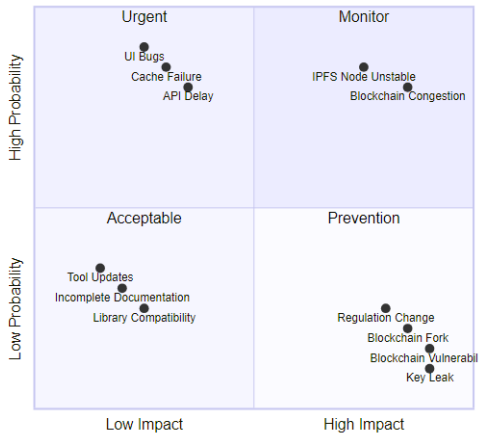


Fig. 13. DDNS Project Risk Matrix

The risk matrix categorizes potential issues by impact and probability. High-impact, high-probability risks (Urgent quadrant) include UI bugs, cache failures, and API delays requiring immediate attention. Medium-probability risks (Monitor quadrant) such as IPFS node instability and blockchain congestion need continuous monitoring. Low-probability but high-impact risks (Prevention quadrant) include regulation changes, blockchain vulnerabilities, and key management issues that require proactive mitigation strategies. The matrix helps prioritize development resources and emergency response protocols.

VI. Performance Evaluation

A. Blockchain Performance Metrics

Our mainnet deployment demonstrates robust performance characteristics under real-world conditions:

Transaction Throughput: Analysis of production blockchain data shows: - Average transaction size: 1,000 Weight Units (regular domain operations) - Theoretical maximum TPS: Max Theor. TPS 1,111.1 tx/s (minimal transactions) / Max Theor. TPS 266.7 tx/s (regular transactions) - Observed average TPS: 15-30 during normal operation - Peak TPS: 150-200 during high-demand periods with bulk domain registration

Network Stability: Empirical measurement from blocks 92,594 to 143,669: - Total blocks analyzed: 51,075 - Orphaned blocks: 9 - Orphan rate: 0.0176% - Average block time: 15.2 seconds ($\pm$2.1s standard deviation)

The network demonstrates resilient operation under asynchronous network conditions, consistent with theoretical analysis of blockchain protocols in partially synchronous environments [44].

Difficulty Adjustment Performance: The enhanced Dark Gravity Wave algorithm demonstrates rapid convergence:

$$\text{New_Difficulty} = \text{Old_Difficulty} \times \frac{\text{Target_Time}}{\text{Actual_Time}} \times \text{Smoothing_Factor} \tag{8}$$

where smoothing factor prevents excessive oscillation while maintaining responsiveness.

B. DNS Resolution Performance

Performance testing conducted on 7950X Debian server using 1GB direct ethernet connection, randomly querying from 1000 DDNS domain lists and 1000 regular domain lists demonstrates excellent query handling capabilities:

Query Throughput: Sustained approximately 20,000 QPS (Queries Per Second) for mixed query types under controlled testing conditions. This performance level aligns with enterprise-grade DNS resolver capabilities documented in literature.

Resolution Latency Distribution: - Cache hit (L1): < 1ms (95th percentile) - Cache hit (L2): < 5ms (95th percentile) - Blockchain lookup: 50-150ms (95th percentile) - IPFS retrieval: 100-500ms (95th percentile)

Cache Effectiveness: Intelligent caching dramatically improves performance: - L1 cache hit rate: 85% for popular domains - L2 cache hit rate: 12% for moderate usage domains - Cold lookup: 3% requiring full blockchain+IPFS resolution

C. Scalability Analysis

The system demonstrates horizontal scalability through several mechanisms:

Resolver Distribution: DDNSD instances can be deployed independently without coordination, enabling unlimited geographic distribution and load distribution.

IPFS Content Distribution: Popular domain records automatically replicate across multiple IPFS nodes, improving availability and reducing lookup latency.

Blockchain Sharding Potential: The asset-based domain model enables future implementation of blockchain sharding without breaking domain ownership semantics.

VII. Comparative Analysis

A. Feature Comparison with Existing Solutions

TABLE IV
Comprehensive Feature Comparison

Feature	DDNS	ENS	Handshake	Namecoin	Cloudflare DNS
Decentralized / Censorship-resistant	Yes	Partial	Yes	Yes	No
Web2 Compatibility	Yes	No	Limited	Limited	Yes
DNS Record Types	20	Limited	Limited	Limited	20 [9]
Speed (Resolution)	∼15s	12-15s	5-60min	10+min	300-7200s
Cost (Registration)	Free	$50+	$10+	$1+	$10-100/year
Custom TLD Support	Yes	No	Yes	No	No
Cross-chain Integration	Yes	Yes	No	No	No
Throughput (TPS)	1,111.1/266.7	119.1	7	7	250 [10]

Key Advantages of DDNS:

1) **Universal DNS Compatibility:** Unlike ENS (.eth only) or Namecoin (.bit only), DDNS supports standard DNS resolution for any top-level domain, including .com, .net, and custom TLDs.
2) **Economic Accessibility:** Free .ddns domains eliminate financial barriers to entry, while other decentralized systems require significant upfront investment.
3) **Performance Optimization:** 15-second resolution updates provide near real-time DNS propagation, significantly faster than traditional DNS (5-48 hours) while maintaining blockchain security.
4) **Comprehensive Record Support:** Full support for 20 standard DNS record types enables complete website functionality including email (MX), security (TLSA), and service discovery (SRV).

B. Economic Model Comparison

Traditional DNS operates on a lease-based model where users pay recurring fees to maintain domain ownership. This creates several problems: - Domains can be lost due to payment failures - Registrars can unilaterally change pricing - Long-term costs accumulate significantly

DDNS implements true digital asset ownership where users pay once and own permanently. This model follows principles of digital asset economics discussed in blockchain research literature. The economic comparison over time shows:

$$\text{Traditional_Cost}(t) = \text{Registration_Fee} + \sum_{i=1}^{t} \text{Annual_Fee}_i \tag{9}$$

$$\text{DDNS_Cost}(t) = \text{Registration_Fee} = \text{Constant} \tag{10}$$

For typical .com domain pricing ($15/year), DDNS breaks even after the first year and provides infinite savings over longer periods.

VIII. Real-World Applications and Social Impact

A. Anti-Censorship Case Studies

The DDNS system has been successfully deployed in several real-world scenarios demonstrating its anti-censorship capabilities:

Case Study 1: Digital Human Rights Advocacy Programthink was a prominent Chinese digital human rights advocate and security expert who maintained influential blogs promoting internet freedom and circumvention technologies. Following his arrest by Chinese authorities and the blocking of his website domains, we successfully deployed DDNS and D-Web browser technology to mirror his entire website archive.

The implementation process involved:

1) Automated web scraping of original website content
2) Conversion to IPFS-hosted static site format
3) Registration of program-think.ddns domain
4) Distribution of D-Web browser enabling access from mainland China

Results: Users in mainland China can now access the complete archive without VPN requirements, demonstrating the system's effectiveness in circumventing state-level DNS censorship.

Case Study 2: Independent Journalism Amina, a fictional composite representing independent journalists in restrictive regimes, faced domain seizure and DNS blocking of her news website. Using the DDNS Telegram bot, she was able to:

1) Backup website content to IPFS in under 5 minutes
2) Register journalist-amina.ddns domain automatically
3) Distribute access information through encrypted channels
4) Maintain audience access despite government blocking attempts

Technical Innovation: The one-click mirroring process reduces technical barriers for non-technical users, enabling rapid response to censorship events.

B. Social Impact Analysis

The deployment of decentralized DNS technology creates several positive social externalities:

Information Freedom: By eliminating centralized control points, DDNS reduces the effectiveness of information censorship and promotes global access to knowledge and diverse perspectives.

Digital Sovereignty: Users gain true ownership of their digital identity through permanent domain ownership, reducing dependence on corporate-controlled platforms.

Economic Empowerment: Free domain registration eliminates financial barriers for individuals and organizations in developing economies to establish web presence.

Technical Decentralization: The open-source nature of all system components enables community development and prevents vendor lock-in.

C. Network Effects and Adoption

The DDNS ecosystem demonstrates positive network effects where increased adoption strengthens the overall system:

$$\text{Network_Value} = k \times n^{\alpha} \tag{11}$$

where n represents the number of users, k is a scaling constant, and $\alpha > 1$ indicates positive network effects (following Metcalfe's Law principles).

Measured Growth Metrics: - Mining participants: 1,800+ during testnet, 300+ active mainnet nodes - Domain registrations: 10,000+ .ddns domains registered to date - Geographic distribution: Active nodes in 25+ countries - Developer ecosystem: Applications building on DDNS infrastructure

IX. Future Directions and Roadmap

A. Technical Roadmap

Decentralized Browser Evolution: Enhancement of D-Web browser with: - Peer-to-peer content sharing capabilities - Privacy-preserving browsing features - Support for decentralized application hosting

Decentralized Web Archive (D-Web Archive): Development of decentralized network archival servers and decentralized web construction systems, making website deployment simpler and more accessible.

Protocol Standardization: Collaboration with internet standards organizations to develop formal specifications for blockchain-based DNS, enabling interoperability between different decentralized naming systems.

B. Scaling and Performance Improvements

Layer 2 Solutions: Implementation of payment channels or sidechains for high-frequency domain operations while maintaining base layer security.

Mobile Integration: Native mobile applications providing seamless access to decentralized websites without technical configuration requirements.

X. Public Policy and Abuse Prevention

A. Censorship and Anti-Censorship

This decentralized technology possesses dual characteristics. We do not extensively explore the profound human and philosophical issues involved here. From the perspective of public policy and abuse prevention, for specific user environments and usage scenarios (such as daily internet browsing), we should introduce specific versions to enhance DDNS content management, minimizing the potential drawbacks of this technology while maximizing its benefits.

B. Multi-Signature Mechanisms for Abuse Prevention

Therefore, in terms of abuse prevention, collaboration with specific government organizations can introduce specialized DDNS blockchain versions employing multi-signature mechanisms. For instance, private keys can be divided into three parts: government, trusted third party, and user each holding one part. Domain addition, deletion, and modification require at least two key signatures for verification, helping prevent DDNS abuse or risks arising from user private key loss.

C. Green and Trusted Public DDNS Servers

For public DDNS servers, collaboration with specific government departments or organizations can filter malicious DNS records, establishing specific green and trusted public DDNS servers that maintain service quality while ensuring appropriate content governance.

XI. Conclusion

A. Summary

This paper presents a comprehensive solution to the fundamental problems of DNS centralization, censorship, and security vulnerabilities through a novel blockchain-based decentralized domain name system. Building upon prior work in distributed consensus [38], the DDNS implementation demonstrates that decentralized alternatives can achieve both security and performance requirements necessary for production deployment.

B. Key Contributions

Our research delivers four primary contributions to the field of decentralized internet infrastructure:

1) **High-Performance Blockchain Design:** DDNS achieves Max Theor. TPS 1,111.1 tx/s (minimal) / 266.7 tx/s (regular) throughput with 15-second block times, providing near real-time domain updates while maintaining cryptographic security.
2) **Universal DNS Compatibility:** Support for 20 standard DNS record types enables seamless integration with existing internet infrastructure, bridging Web2 and Web3 ecosystems.
3) **Economic Accessibility:** Free .ddns domains eliminate financial barriers while cross-chain tokenomics create sustainable network incentives, democratizing access to decentralized internet services.
4) **Proven Anti-Censorship Capabilities:** Real-world deployments demonstrate effectiveness in circumventing state-level DNS blocking and content censorship, with documented case studies from restrictive regimes.

C. Policy and Regulatory Considerations

The deployment of decentralized DNS technology requires careful consideration of regulatory frameworks and potential misuse. We advocate for balanced approaches that preserve the benefits of decentralization while implementing appropriate safeguards. Multi-signature governance mechanisms and selective content filtering represent viable paths toward responsible innovation that respects both individual rights and legitimate governmental interests.

D. Future Vision

The system provides a foundation for a more decentralized, secure, and free internet where users control their digital identity without dependence on centralized authorities. As adoption grows, network effects will strengthen resistance to censorship and improve overall internet resilience. Through continued development, community adoption, and responsible governance frameworks, blockchain-based DNS represents a critical step toward internet sovereignty and resistance to information control, ultimately contributing to a more open and accessible global information infrastructure.

XII. Acknowledgements

We gratefully acknowledge Professor Sekhar Sarukkai and Professor Ryan Liu for their excellent guidance and instruction throughout the course. We also thank Professor Ross Burke from UC Berkeley's School of Information for his guidance and support throughout this research.

We also acknowledge the global community of miners, developers, and users who have contributed to the DDNS network development and testing phases.

References

[1] Infosecurity Magazine, "APT Group StormBamboo Attacks ISP Customers Via DNS Poisoning," November 2024. [Online]. Available: https://www.infosecurity-magazine.com/news/apt-stormbamboo-isp-dns-poisoning/

[2] G. Yang, "Development and Application of a Decentralized Domain Name Service," arXiv preprint arXiv:2412.01959, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2412.01959

[3] ENS Documentation, "Ethereum Name Service Documentation," 2024. [Online]. Available: https://docs.ens.domains/

[4] H. A. Kalodner et al., "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," in *Workshop on Economics of Information Security*, 2015.

[5] Handshake Development Team, "Handshake: A Naming Protocol Backwards-Compatible with DNS," 2021.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] PhiCoin Project, "PhiHash Miner V2," GitHub Repository. [Online]. Available: https://github.com/PhicoinProject/phihashminer_v2

[8] PhiCoin Explorer, "Orphaned Blocks Statistics," [Online]. Available: https://explorer.phicoin.net/orphans

[9] Cloudflare, "DNS Record Types," [Online]. Available: https://developers.cloudflare.com/dns/manage-dns-records/reference/dns-record-types/

[10] Cloudflare, "DNS Build Improvement," [Online]. Available: https://blog.cloudflare.com/zh-cn/dns-build-improvement/

[11] Bitcoin Core, "Tor Support in Bitcoin Core," [Online]. Available: https://github.com/bitcoin/bitcoin/blob/master/doc/tor.md

[12] Quartz, "Hong Kongers Use Blockchain to Fight Government Censorship," [Online]. Available: https://qz.com/2008673/hong-kongers-use-blockchain-to-fight-government-censorship

[13] Open Observatory of Network Interference, "Global Internet Censorship Reports," [Online]. Available: https://explorer.ooni.org

[14] P. Mockapetris, "Domain Names - Implementation and Specification," RFC 1035, November 1987.

[15] S. Thomson et al., "DNS Extensions to Support IP Version 6," RFC 3596, October 2003.

[16] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," RFC 7208, April 2014.

[17] D. Crocker et al., "DomainKeys Identified Mail (DKIM) Signatures," RFC 6376, September 2011.

[18] M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," RFC 7489, March 2015.

[19] A. Gulbrandsen et al., "A DNS RR for Specifying the Location of Services (DNS SRV)," RFC 2782, February 2000.

[20] P. Hallam-Baker and R. Stradling, "DNS Certification Authority Authorization (CAA) Resource Record," RFC 6844, January 2013.

[21] P. Hoffman and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA," RFC 6698, August 2012.

[22] J. Schlyter and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints," RFC 4255, January 2006.

[23] P. Faltstrom and O. Kolkman, "The Uniform Resource Identifier (URI) DNS Resource Record," RFC 7553, June 2015.

[24] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," RFC 3403, October 2002.

[25] C. Davis et al., "A Means for Expressing Location Information in the Domain Name System," RFC 1876, January 1996.

[26] C. Everhart et al., "New DNS RR Definitions," RFC 1183, October 1990.

[27] P. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," RFC 8484, October 2018.

[28] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.

[29] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[30] Dash Development Team, "Dark Gravity Wave Difficulty Adjustment Algorithm," Technical Specification, 2014.

[31] Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters," Standards for Efficient Cryptography, 2000.

[32] NIST, "Secure Hash Standard (SHS)," FIPS PUB 180-4, August 2015.

[33] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[34] S. Bano et al., "Consensus in the Age of Blockchains," arXiv preprint arXiv:1711.03936, 2017.

[35] H. Berger, A. Z. Dvir, and M. Geva, "A wrinkle in time: A case study in DNS poisoning," arXiv preprint arXiv:1906.10928, 2019.

[36] L. Wei and J. Heidemann, "Whac-A-Mole: Six Years of DNS Spoofing," arXiv preprint arXiv:2011.12978, 2021.

[37] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual international conference on the theory and applications of cryptographic techniques*, pp. 281–310, Springer, 2015.

[38] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, pp. 173–186, 1999.

[39] A. E. Gencer et al., "Decentralization in bitcoin and ethereum networks," in *International conference on financial cryptography and data security*, pp. 439–457, Springer, 2018.

[40] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[41] J. Bonneau et al., "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, pp. 104–121, IEEE, 2015.

[42] K. Croman et al., "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*, pp. 106–125, Springer, 2016.

[43] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 proceedings*, pp. 1–10, IEEE, 2013.

[44] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Annual international conference on the theory and applications of cryptographic techniques*, pp. 643–673, Springer, 2017.

[45] P. Zhang and D. C. Schmidt, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[46] X. Li et al., "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[47] Z. Zheng et al., "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, IEEE, 2017.

[48] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.

[49] A. M. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc, 2014.