Development and Application of a Decentralized Domain Name Service

Guang Yang
University of California, Berkeley
guangyang19@berkeley.edu

2024

Abstract

The current Domain Name System (DNS), as a core infrastructure of the internet, exhibits several shortcomings: its centralized architecture leads to censorship risks and single points of failure, making domain name resolution vulnerable to attacks. The lack of encryption in the resolution process exposes it to DNS hijacking and cache poisoning attacks [1]. Additionally, the high operational costs limit participation and innovation among small to medium-sized users [2]. To address these issues, this paper proposes a Decentralized Domain Name Service (DDNS) based on blockchain (Phicoin [25]) and distributed storage (IPFS). By leveraging the immutability of blockchain and the content verification of IPFS [3], the system achieves decentralized storage and distribution of domain name records, eliminating the centralized dependencies of traditional DNS. With a block time of 15 seconds, the system supports rapid broadcasting of domain name updates, significantly improving resolution efficiency. The DDNS aims to serve as a complement or backup to the existing DNS system, providing a pollution-resistant, censorship-resistant, high-performance, and low-cost domain name resolution solution, offering a new technical path for the security and stability of the internet.

Keywords

Blockchain, Decentralized Domain Name Service, Phicoin, IPFS, Security, Anti-DNS Spoofing, Anti-Censorship.

1 Introduction

1.1 Background

The Domain Name System (DNS) is a critical infrastructure of the internet, responsible for translating user-friendly domain names into machine-readable IP addresses [4]. It serves as the backbone of internet communication, enabling users to access websites and online services seamlessly. However, the traditional DNS system, due to its centralized architecture, has gradually exposed several limitations [5]:

- **Single Point of Failure:** Centralized authoritative and caching servers can lead to widespread service interruptions if they fail [6].
- **Susceptibility to Censorship:** The centralized architecture makes DNS services prone to control or interference, allowing manipulation of resolution records to restrict user access [7].
- **High Operational Costs:** The substantial deployment and maintenance costs of authoritative and caching servers limit participation by small and medium-sized enterprises and individual users [2].

Common threats to the DNS system include:

- **DNS Hijacking:** Attackers tamper with resolution records to redirect legitimate domain names to malicious IP addresses, luring users to phishing sites or ad pages [8].
- **DNS Cache Poisoning:** Injection of forged resolution results into DNS server caches, causing users to be redirected to incorrect addresses [9].
- **Censorship and Blocking:** Modification or blocking of resolution requests to restrict access to specific domain names or content [10].

1.2 Motivation

With the continuous growth of the internet, the centralized architecture of the traditional DNS system faces increasing challenges in security, reliability, and scalability [11]. Centralized authoritative servers not only become prime targets for network attacks and censorship but also affect the availability of domain name resolution services due to single points of failure [6]. Furthermore, attacks like DNS hijacking and cache poisoning exploit the lack of data integrity verification in traditional DNS systems, leading to tampered resolution records and severely threatening user security and privacy [12]. These issues highlight the urgent need for a technical solution that can compensate for the shortcomings of the traditional DNS system.

Decentralized technologies offer a new approach to domain name resolution systems [12]. By utilizing the distributed ledger and immutability of blockchain [13], domain name records can be managed in a decentralized manner, avoiding single points of failure and data tampering. Combining this with IPFS's distributed storage capabilities [14], the storage and distribution of resolution records become more flexible and efficient, capable of meeting future complex DNS protocol extension needs. This paper aims to develop a Decentralized Domain Name Service (DDNS) that, through a decentralized architecture and cryptographic verification mechanisms, achieves pollution resistance, censorship resistance, high performance, and low cost in domain name resolution services, providing a reliable complement or alternative to the existing DNS system.

1.3 Related Work

Existing decentralized DNS solutions like Ethereum Name Service (ENS) [15] and Namecoin [7] have made significant strides in enhancing privacy and censorship resistance.

- **ENS:** Utilizes the Ethereum blockchain to manage domain names ending with `.eth`, allowing users to associate metadata and cryptocurrency addresses with human-readable names [16].
- **Namecoin:** A fork of Bitcoin that enables the registration of `.bit` domains on its blockchain [7].

Advantages of Existing Solutions:

- Enhanced privacy.
- Resistance to censorship.
- Elimination of central authority control.

Limitations of Existing Solutions:

- Performance issues due to blockchain scalability constraints [17].
- Potential centralization risks in the management of top-level domains [10].
- Higher costs associated with blockchain transactions [18].

Our Contribution:

The DDNS system proposed in this paper introduces the Phicoin blockchain [25], designed specifically for domain name services with a 15-second block time to enhance performance. The system focuses on fair participation, asset compatibility, and ultra-low costs, addressing the limitations of existing solutions by improving scalability and reducing operational expenses.

Table 1: Comparison of Decentralized DNS Solutions

Feature	Traditional DNS	ENS	Namecoin	Handshake	Phicoin (This Work)
Decentralization	No	Yes	Yes	Yes	Yes
Performance	High	Medium	Medium	Medium	High
Censorship Resistant	Low	High	High	High	High
Cost (per domain)	High	High	Medium	Medium	Super Low ($0.00025)
Blockchain Speed	N/A	15 sec	10 min	10 min	15 sec
Extensibility	Limited	Flexible	Limited	Limited	Flexible

2 System Design

2.1 Architecture Overview

The DDNS system leverages blockchain and distributed storage technologies to decentralize domain name resolution. The key components include:

- **Phicoin Blockchain:** Used for domain asset binding and verification. It records domain name ownership and updates, ensuring immutability and transparency [25].
- **IPFS (InterPlanetary File System):** Used for distributed storage of resolution data. It stores domain resolution data (e.g., IP addresses), enabling decentralized retrieval of this information [14].

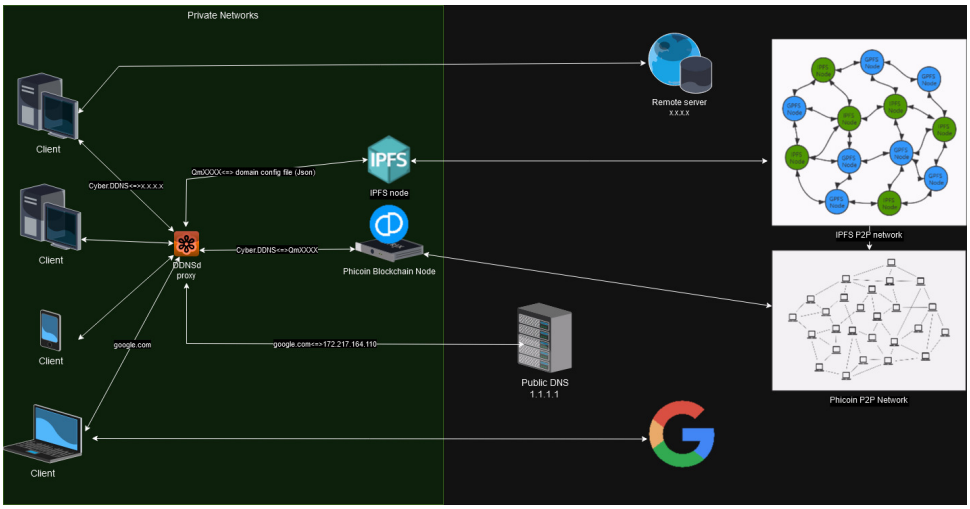

Figure 1: DDNS System Architecture

2.2 Key Components

2.2.1 Phicoin Blockchain

Design Goals:

1. **Economic Efficiency:** Achieve ultra-low costs to encourage widespread adoption [25].
2. **Fair Participation:** Ensure equal opportunities for all participants without central nodes or masternodes [25].
3. **Asset Compatibility:** Support domain name assets and other digital assets [25].

Current Participation:

- **Test Mining Phase:** Over 1,800 participants.
- **Post-Mainnet Launch:** Over 300 global nodes running.

Phicoin utilizes the ASIC-resistant **Phihash** algorithm, mined using GPUs [25]. The value is determined by the user's work contribution and recognition, promoting true decentralization through self-incentivization.

2.2.2 Decentralized Domain Name Service Protocol

Domain Types:

Category	Description
Phicoin Top-Level Domains	Used to create Phicoin top-level domains (pTLDs), such as `.ddns`. Anyone with a GPU can mine Phicoin and create a TLD [25].
Sub Domains	Used to create second-level domains with specific rules:
Asset Structure	Maximum of 32 characters.
Data Structure	`!` denotes root asset, `/` denotes separator.
Properties	• Non-reissuable. • Quantity of 1. • Unit of 1.
Initial Binding Hash	`000...000` (64 zeros).
Deactivation Hash	`Qm000...000` (46-character IPFS hash).
Management Rights	Transferred to a specified address upon creation.
Fees	• Creation Fee: 0.1 phi. • Modification Fee: 0.1 phi.
No Annual Fees	Domains never expire.
Subdomains	Supports creation of subdomains up to a total length of 30 characters.

Table 2: Phicoin Domain Rules and Properties

2.2.3 Domain Templates

Domain records are defined using JSON files, enabling flexibility and extensibility [15].

Basic Record Types:

- **Type A (IPv4 Address):**

```
{
  "Type": "A",
  "Address": "192.168.1.1"
}
```

- **Type AAAA (IPv6 Address):**

```
{
  "Type": "AAAA",
  "Address": "2001:db8::1"
}
```

- **Type CNAME (Canonical Name):**

```
{
  "Type": "CNAME",
  "Target": "example.com"
}
```

- **Type MX (Mail Exchange Record):**

```
{
  "Type": "MX",
  "MailServer": "mail.example.com",
  "TTL": 3600,
  "Priority": 10
}
```

Extensibility:

Users can extend these templates to include additional record types as needed, such as TLSA for DANE (DNS-based Authentication of Named Entities) records [19].

2.2.4 IPFS Integration

Binding IPFS Hashes with Domain Assets:

- Users create and host the domain configuration JSON files using an IPFS client [14].
- The data is distributed across the IPFS network.
- In this study, Pinata's free API is utilized, allowing management of up to 500 files—sufficient for typical domain resolution needs.

2.2.5 Domain Resolution

Design Goals:

1. **Compatibility with Existing DNS:** Ensure that traditional DNS queries are handled appropriately.
2. **DDNS Protocol Domain Resolution:** Enable resolution of DDNS domains.

Implementation:

- **Local DNS Proxy Service Deployment:**
  - **Traditional Domain Queries:** Forwarded to public DNS servers like 1.1.1.1.
  - **DDNS Domain Queries:**
    1. Retrieve the IPFS hash from the Phicoin blockchain based on the domain name [25].
    2. Fetch the domain configuration JSON file from IPFS using the hash.
    3. Parse the JSON file to extract the domain records.
    4. Return the resolution result to the user.

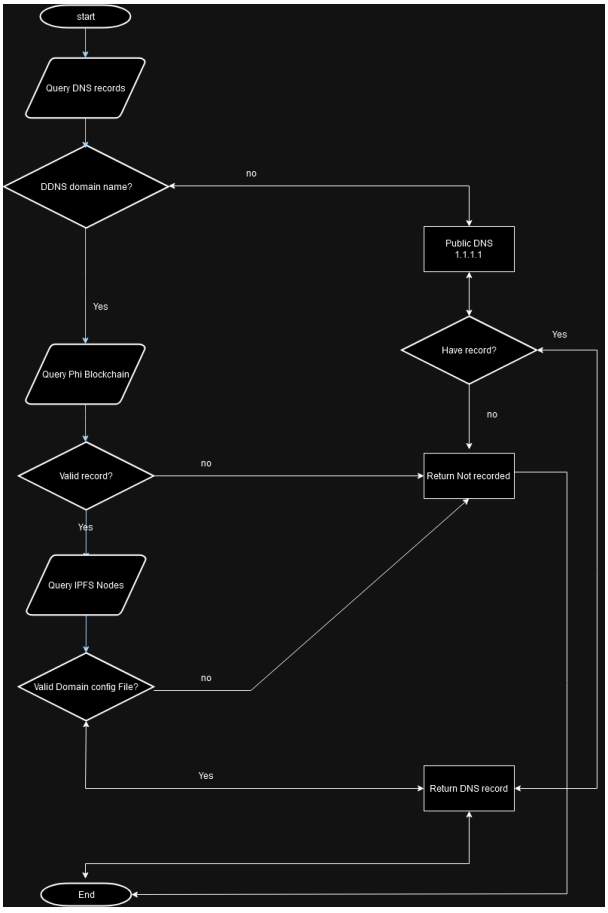

Figure 2: DDNS Domain Resolution Process

3 Implementation

3.1 Core Functions

- **Registering pTLDs:** Creation of new top-level domains on the Phicoin blockchain [25].
- **Adding Subdomains:** Generation of second-level and subdomains under a pTLD.
- **Disabling Subdomains:** Deactivation of subdomains by updating the associated IPFS hash.
- **Setting Domain Records:** Updating the domain's IPFS hash to point to the correct JSON configuration file.
- **DNS Domain Resolution Forwarding Service:** Handling traditional DNS queries by forwarding them to standard DNS servers.
- **DDNS Domain Resolution Service:** Resolving DDNS domains using the Phicoin blockchain and IPFS.

3.2 Codebase and Modules

Main Modules:

- `ddnsd.py`: The primary daemon responsible for handling DNS queries. It interfaces with the Phicoin blockchain and IPFS to resolve domain names and return the results to clients.
- `ddns_domain_registration.ipynb`: A Jupyter Notebook that demonstrates how to register domains, manage subdomains, and update domain records on the blockchain.

Module Functionalities:

- **Blockchain Interaction:** Functions to interact with the Phicoin blockchain for querying domain assets and associated IPFS hashes [25].
- **IPFS Interaction:** Methods to retrieve and pin JSON configuration files on IPFS.
- **DNS Server Integration:** Implements a DNS server that can handle both traditional DNS and DDNS queries.
- **Configuration Management:** Tools for domain owners to create and update domain records.

4 Evaluation

4.1 Security Analysis

Identity and Trust Management

- **User Roles:**
  - **pTLD Operators:** Control top-level domains (e.g., `.ddns`) through ownership of the corresponding blockchain assets [25].

  - **Subdomain Owners:** Manage second-level domains under a pTLD, with rights transferred via blockchain transactions.
  - **Visitors:** Users who perform domain name resolutions without needing Phicoin.

- **Security Mechanisms:**
  - **Private Keys:** Domain creation, modification, and deactivation require transactions signed with the owner's private key [25].
  - **Immutable Records:** Domain records are bound to unique IPFS hashes, ensuring data integrity [14].

Confidentiality, Integrity, and Availability (CIA)

- **Confidentiality:** While the blockchain is transparent, sensitive data (like private keys) remain confidential [13]. Domain ownership changes require private key signatures, ensuring only authorized modifications.
- **Integrity:** The immutability of blockchain records and IPFS's content-addressable storage ensure that domain records cannot be tampered with without detection [8].
- **Availability:** Decentralization eliminates single points of failure. Even if some nodes fail or are attacked, the system remains operational [21].

Resistance to Attacks

- **DNS Hijacking Prevention:**
  - Local resolution using the blockchain and IPFS reduces reliance on external servers, mitigating hijacking risks [8].
  - Cryptographic verification of data authenticity prevents attackers from injecting false records [20].
- **DNS Cache Poisoning Prevention:**
  - End-to-end data integrity verification ensures that only valid records are accepted [9].
  - The decentralized nature of the system reduces the effectiveness of poisoning attacks [8].
- **Censorship Resistance:**
  - No central authority controls the domain records, making it difficult for adversaries to censor or block domains [10].
  - Users can run local nodes, accessing and sharing data without centralized intermediaries [18].

4.2 Trust Chain Analysis

Component	Description
Root Trust Element	Blockchain: Immutable ownership of domains and records. Ownership tracked as assets; private keys authorize all actions.
Validation and Integrity	IPFS: Stores domain data securely and decentrally. Content-addressed storage ensures authenticity; hashes bound to blockchain prevent tampering.
Participants	- pTLD Operators: Manage top-level domains like .ddns. Trust based on ownership of blockchain assets. - Subdomain Owners: Control second-level domains; rights transferred through blockchain. - Visitors: Perform domain name resolutions via verified blockchain-IPFS data.
Security Layers	- Private Key Cryptography: Ensures authorized actions. - Immutability: Prevents retroactive alterations. - Decentralization: Enhances availability and censorship resistance.
Anti-Attack Mechanisms	- DNS Hijacking: Local resolution via blockchain and IPFS mitigates risks. - Cache Poisoning: Cryptographic verification ensures only valid data is used. - Censorship Resistance: No central authority to enable censorship.
Operational Support	- Fees: Low-cost creation and modification. - Compatibility: Supports traditional and DDNS queries.
Future Enhancements	- Adding DNSSEC-like features for stronger identity verification. - Expanding record types for broader functionality.

Figure 3: Trust Chain for Decentralized Domain Name Service (DDNS)

4.3 Performance Analysis

System Performance

- **Fast Record Broadcasting:**
  - The 15-second block time allows rapid propagation of domain updates across the network [25].
- **Efficient Query Handling:**
  - Optimized storage and indexing enhance query speed, supporting high query rates on standard hardware [12].
- **Scalability:**
  - The use of IPFS allows the system to handle large amounts of data efficiently [14].
  - JSON-based records facilitate easy addition of new record types, ensuring future extensibility.

5 Future Work

5.1 Feature Enhancements

- **Support for Additional DNS Protocols:** Extend domain templates to include records like TLSA for DANE, enabling secure certificate verification without traditional Certificate Authorities (CAs) [19].
- **User Interface Improvements:** Develop intuitive tools and graphical interfaces for domain registration and management to lower the entry barrier for non-technical users [22].
- **Public DDNS Resolution Nodes:** Deploy public nodes compatible with traditional DNS to facilitate adoption and ease of use for end-users [8].

6 Conclusion

This paper presents a secure, efficient, and low-cost decentralized DNS system that addresses several shortcomings of the traditional DNS. By leveraging blockchain and IPFS technologies, the DDNS system provides a censorship-resistant and tamper-proof domain name resolution service. It enhances the robustness of the internet infrastructure and offers a viable complementary solution to existing DNS systems.

Future Applications and Potential:

The DDNS system paves the way for more decentralized internet services, promoting security, privacy, and equal participation. Its scalable and flexible design makes it a strong solution for future internet infrastructure developments.

References

[1] ICANN, "DNSSEC – What Is It and Why Is It Important?" [Online]. Available: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

[2] A. Vakali and G. Pallis, "Content Delivery Networks: Status and Trends," *IEEE Internet Computing*, vol. 7, no. 6, pp. 68–74, 2003.

[3] IPFS Documentation. [Online]. Available: https://docs.ipfs.io/

[4] P. Mockapetris, "Domain Names - Concepts and Facilities," RFC 1034, 1987.

[5] H. Gao *et al.*, "An Empirical Reexamination of Global DNS Behavior," in *Proceedings of the ACM SIGCOMM 2013 Conference*, 2013, pp. 267–278.

[6] G. C. Moura *et al.*, "Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event," in *Proceedings of the 2016 Internet Measurement Conference*, 2016, pp. 255–270.

[7] H. A. Kalodner *et al.*, "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," in *WEIS*, vol. 1, 2015, pp. 1–23.

[8] Z. Li *et al.*, "B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1674–1686, 2021.

[9] S. Son and V. Shmatikov, "The Hitchhiker's Guide to DNS Cache Poisoning," in *International Conference on Security and Privacy in Communication Systems*, Springer, 2010, pp. 466–483.

[10] C. Patsakis *et al.*, "Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS," *IEEE Access*, vol. 8, pp. 118559–118571, 2020.

[11] A. Herzberg and H. Shulman, "DNSSEC: Security and Availability Challenges," in *2013 IEEE Conference on Communications and Network Security (CNS)*, IEEE, 2013, pp. 365–366.

[12] H. Liu *et al.*, "A High Performance, Scalable DNS Service for Very Large Scale Container Cloud Platforms," in *Proceedings of the 19th International Middleware Conference Industry*, 2018, pp. 39–45.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

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

[15] ENS Documentation. [Online]. Available: https://docs.ens.domains/web/records

[16] P. Xia *et al.*, "Ethereum Name Service: The Good, the Bad, and the Ugly," *arXiv preprint arXiv:2104.05185*, 2021.

[17] M. Carlsten *et al.*, "On the Instability of Bitcoin Without the Block Reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 154–167.

[18] M. Ali *et al.*, "Blockstack: A Global Naming and Storage System Secured by Blockchains," in *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, 2016, pp. 181–194.

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

[20] A. Yakubov *et al.*, "A Blockchain-Based PKI Management Framework," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2018, pp. 1–6.

[21] X. Duan *et al.*, "DNSLedger: Decentralized and Distributed Name Resolution for Ubiquitous IoT," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, 2018, pp. 1–3.

[22] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2018, pp. 9–15.

[23] V. (vinced), "Namecoin - A Distributed Naming System Based on Bitcoin," [Online]. Available: `https://bitcointalk.org/index.php?topic=6017`, April 18, 2011.

[24] A. (Appamatto), "BitDNS and Generalizing Bitcoin," [Online]. Available: `https://bitcointalk.org/index.php?topic=1790.0`, November 15, 2010.

[25] Phicoin Dev Team, "PHICOIN (PHI): The PoW High-Performance Infrastructure," version v0.3, 2024.

Appendix

Scoring Directions

The following scoring criteria from the assignment are addressed in this paper:

1. **What establishes identity and trust?**
    - The use of blockchain for domain ownership and private keys for authorization establishes identity and trust within the system.
2. **What are known vulnerabilities or attacks?**
    - Discussed DNS hijacking, cache poisoning, and how the DDNS system mitigates these attacks.
3. **Discuss Confidentiality / Availability / Integrity**
    - Explored how the system ensures CIA through design choices like decentralization and cryptographic verification.
4. **What are relevant tools and techniques for defense or detection?**
    - Described the use of blockchain and IPFS as tools to defend against common DNS attacks.
5. **A working demonstration of the system**
    - Provided code links and described the implementation of the DDNS system.

Acknowledgements

I sincerely thank Professor Ross Burke from UC Berkeley's I School for his invaluable guidance and support throughout the course, which greatly helped shape this project.

Special thanks to Peter Trinh provided me a solar farm that I can use free electricity to run Phicoin's seeder nodes, mining pools, and test mining algorithm.

Code Links

The codebase for this project is available at:

- GitHub Repository: `https://github.com/GY19A/ddns`