Development and Application of a Decentralized Domain Name Service

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

2024 Cyber 201 Final Project

Public Waste Photography
© 2008 Bernard Delmundo

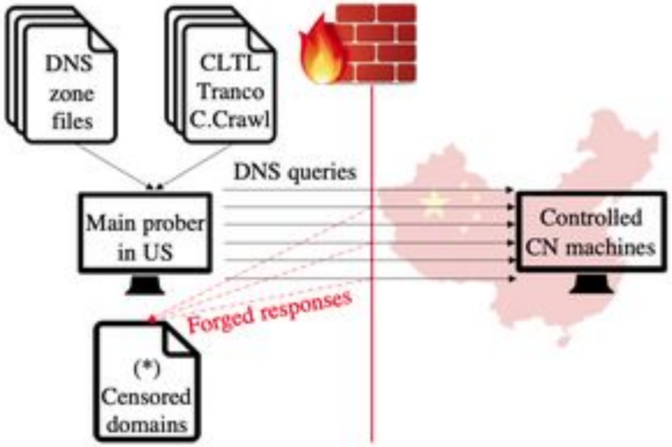


Figure 1: Probing the GFW's DNS poisoning from outside.

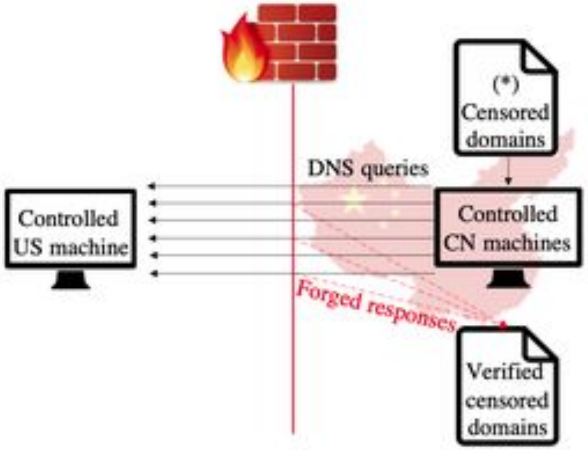
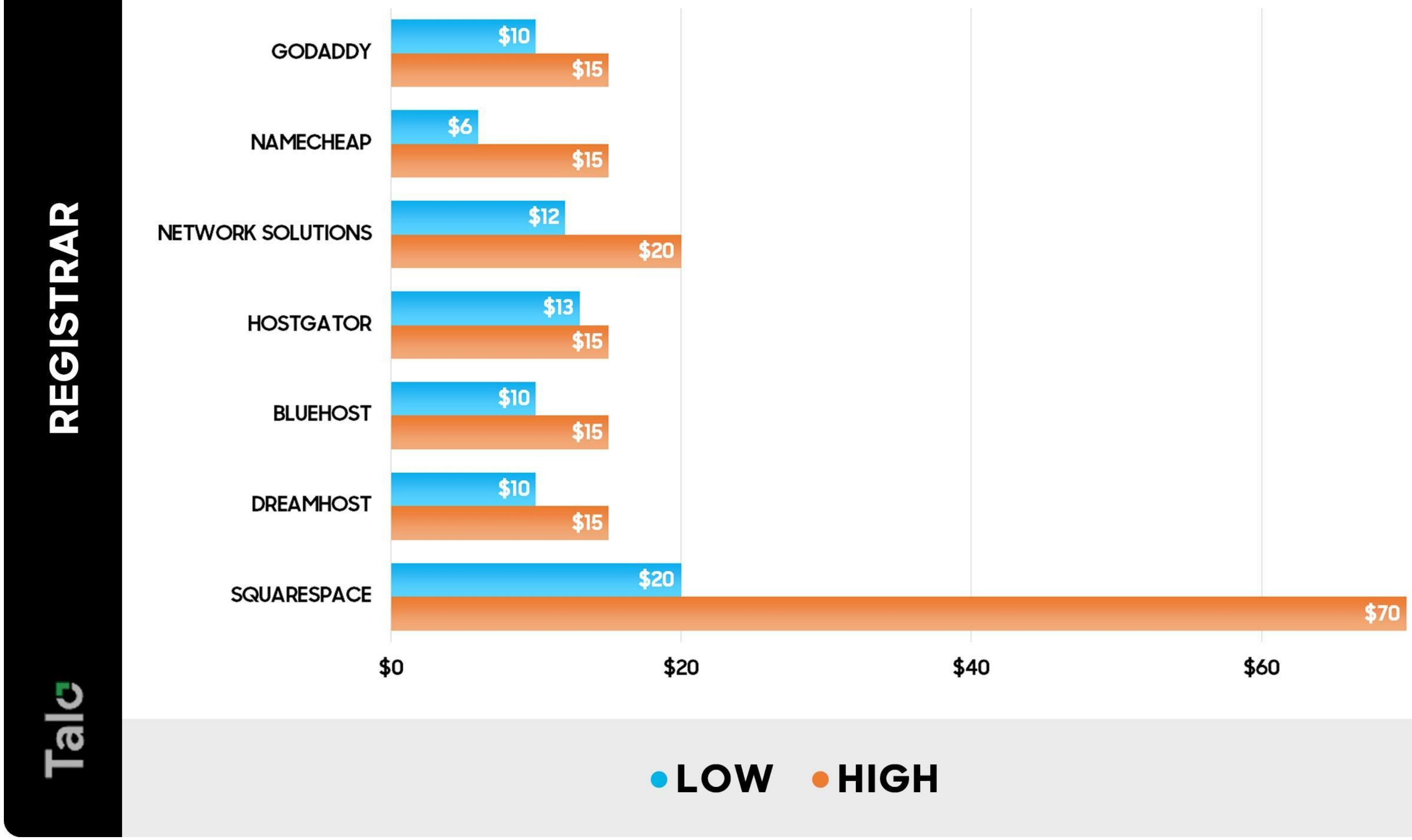


Figure 2: Verifying poisoned domains from inside the GFW.

External Probing and Internal Verification of the China's Great Firewall

DOMAIN NAME PRICE BY COMPANY
.COM DOMAIN INTRODUCTORY (FIRST YEAR) RATES



Berkeley
UNIVERSITY OF CALIFORNIA

ETHEREUM NAME SERVICE

UNSTOPPABLE DOMAINS

handshake

namecoin

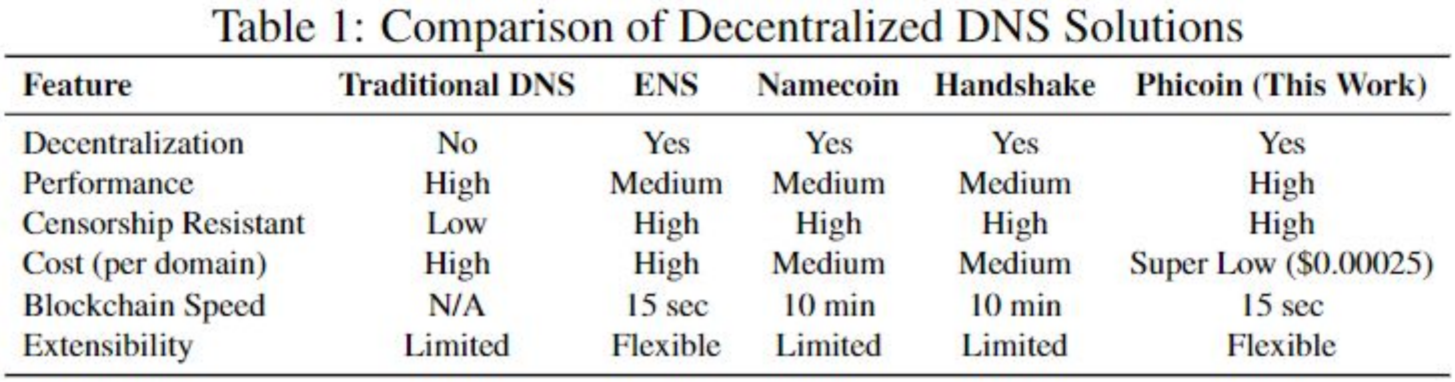


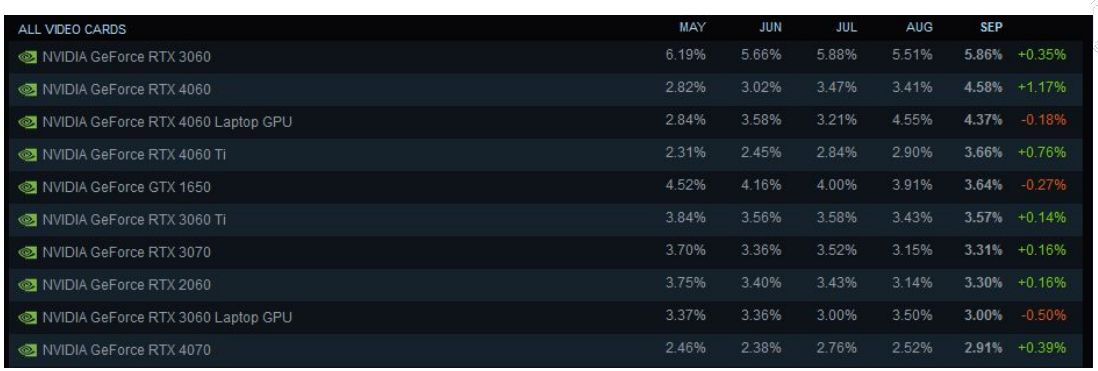
Table 1: Comparison of Decentralized DNS Solutions

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

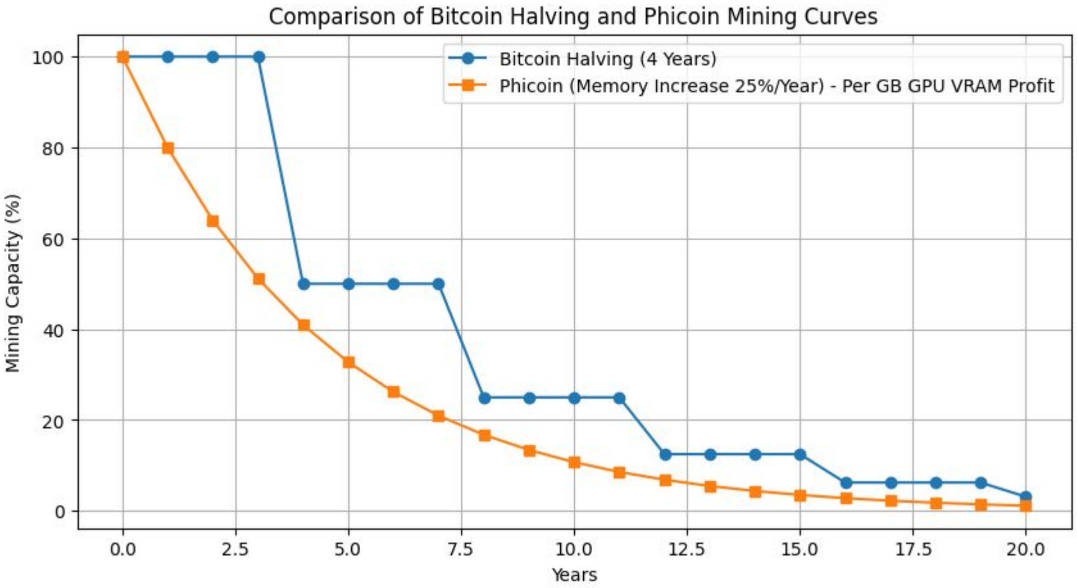
- Name: Phicoin
  The PoW High-Performance Infrastructure
- Symbol: Φ .
- Block Time: 15 seconds.
- Block Size: 4 MB

- TPS: 1,092 TPS
- DAG Size: > 4 GB
- DAG Increasing: 25% / year
- Total Supply: unlimited
- Halving Times: 1

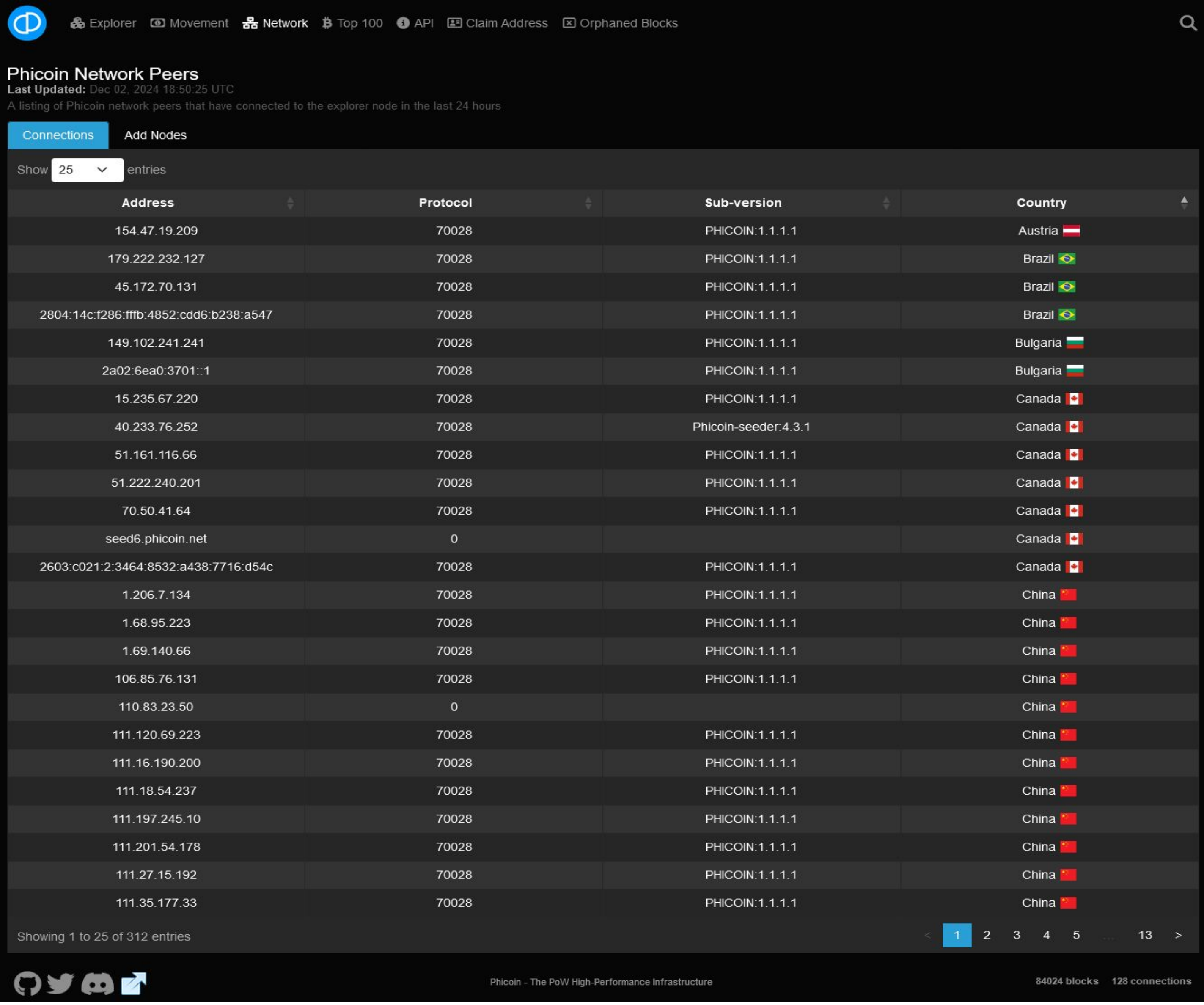
Steam Hardware Survey: September 2024



ALL VIDEO CARDS	MAY	JUN	JUL	AUG	SEP	
NVIDIA GeForce RTX 3060	6.19%	5.66%	5.88%	5.51%	5.86%	+0.35%
NVIDIA GeForce RTX 4060	2.82%	3.02%	3.47%	3.41%	4.58%	+1.17%
NVIDIA GeForce RTX 4060 Laptop GPU	2.84%	3.58%	3.21%	4.55%	4.37%	-0.18%
NVIDIA GeForce RTX 4060 Ti	2.31%	2.45%	2.84%	2.90%	3.66%	+0.76%
NVIDIA GeForce GTX 1650	4.52%	4.16%	4.00%	3.91%	3.64%	-0.27%
NVIDIA GeForce RTX 3060 Ti	3.84%	3.56%	3.58%	3.43%	3.57%	+0.14%
NVIDIA GeForce RTX 3070	3.70%	3.36%	3.52%	3.15%	3.31%	+0.16%
NVIDIA GeForce RTX 2060	3.75%	3.40%	3.43%	3.14%	3.30%	+0.16%
NVIDIA GeForce RTX 3060 Laptop GPU	3.37%	3.36%	3.00%	3.50%	3.00%	-0.50%
NVIDIA GeForce RTX 4070	2.46%	2.38%	2.76%	2.52%	2.91%	+0.39%



Phihash mining curves



Phicoin Network Peers

Last Updated: Dec 02, 2024 18:50:25 UTC

A listing of Phicoin network peers that have connected to the explorer node in the last 24 hours

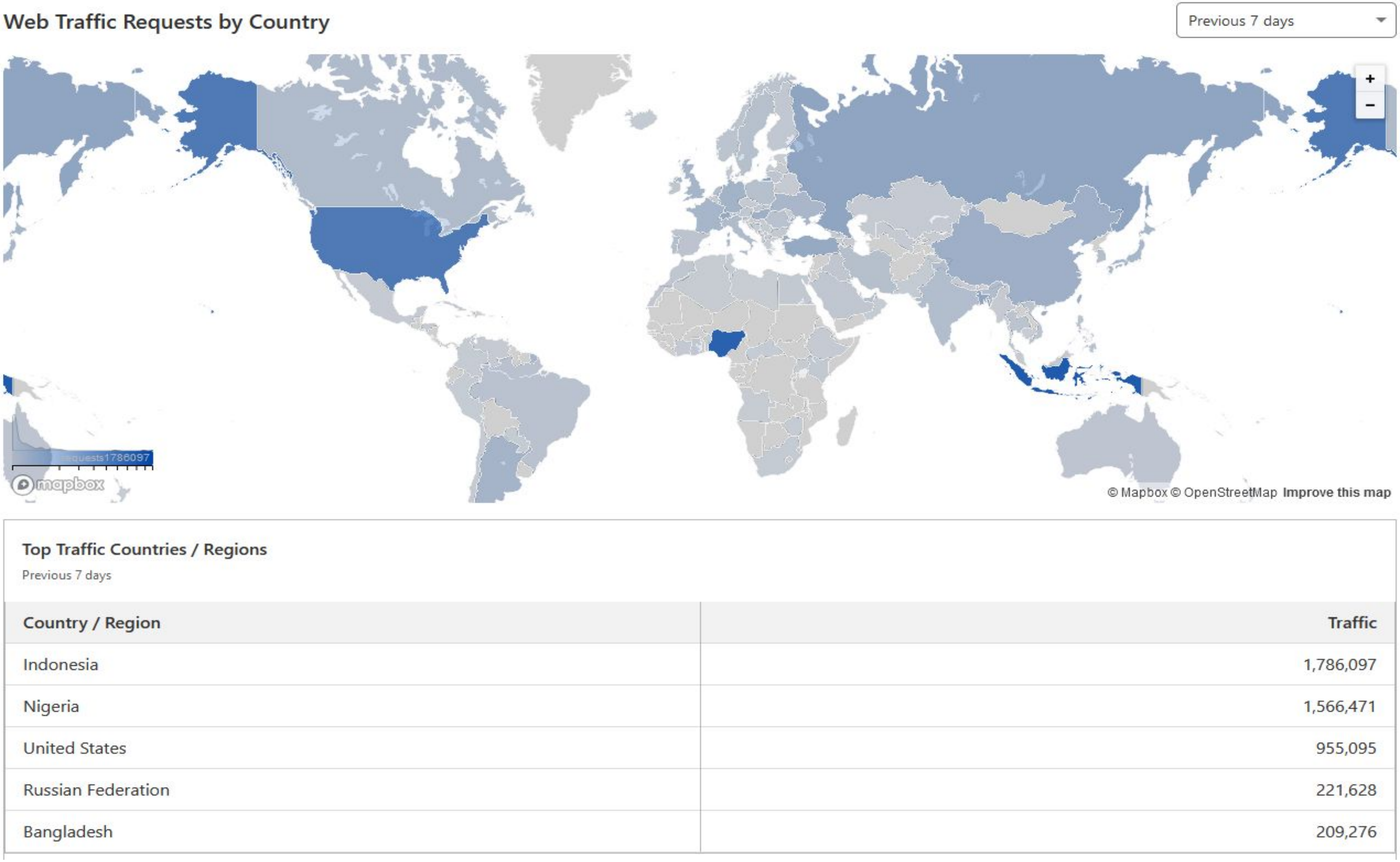
Show 25 entries

Address	Protocol	Sub-version	Country
154.47.19.209	70028	PHICOIN:1.1.1.1	Austria
179.222.232.127	70028	PHICOIN:1.1.1.1	Brazil
45.172.70.131	70028	PHICOIN:1.1.1.1	Brazil
2804:14c:f286:fffb:4852:cdd6:b238:a547	70028	PHICOIN:1.1.1.1	Brazil
149.102.241.241	70028	PHICOIN:1.1.1.1	Bulgaria
2a02:6ea0:3701::1	70028	PHICOIN:1.1.1.1	Bulgaria
15.235.67.220	70028	PHICOIN:1.1.1.1	Canada
40.233.76.252	70028	Phicoin-seeder:4.3.1	Canada
51.161.116.66	70028	PHICOIN:1.1.1.1	Canada
51.222.240.201	70028	PHICOIN:1.1.1.1	Canada
70.50.41.64	70028	PHICOIN:1.1.1.1	Canada
seed6.phicoin.net	0		Canada
2603:c021:2:3464:8532:a438:7716:d54c	70028	PHICOIN:1.1.1.1	Canada
1.206.7.134	70028	PHICOIN:1.1.1.1	China
1.68.95.223	70028	PHICOIN:1.1.1.1	China
1.69.140.66	70028	PHICOIN:1.1.1.1	China
106.85.76.131	70028	PHICOIN:1.1.1.1	China
110.83.23.50	0		China
111.120.69.223	70028	PHICOIN:1.1.1.1	China
111.16.190.200	70028	PHICOIN:1.1.1.1	China
111.18.54.237	70028	PHICOIN:1.1.1.1	China
111.197.245.10	70028	PHICOIN:1.1.1.1	China
111.201.54.178	70028	PHICOIN:1.1.1.1	China
111.27.15.192	70028	PHICOIN:1.1.1.1	China
111.35.177.33	70028	PHICOIN:1.1.1.1	China

Showing 1 to 25 of 312 entries

Phicoin - The PoW High-Performance Infrastructure

84024 blocks 128 connections



Web Traffic Requests by Country

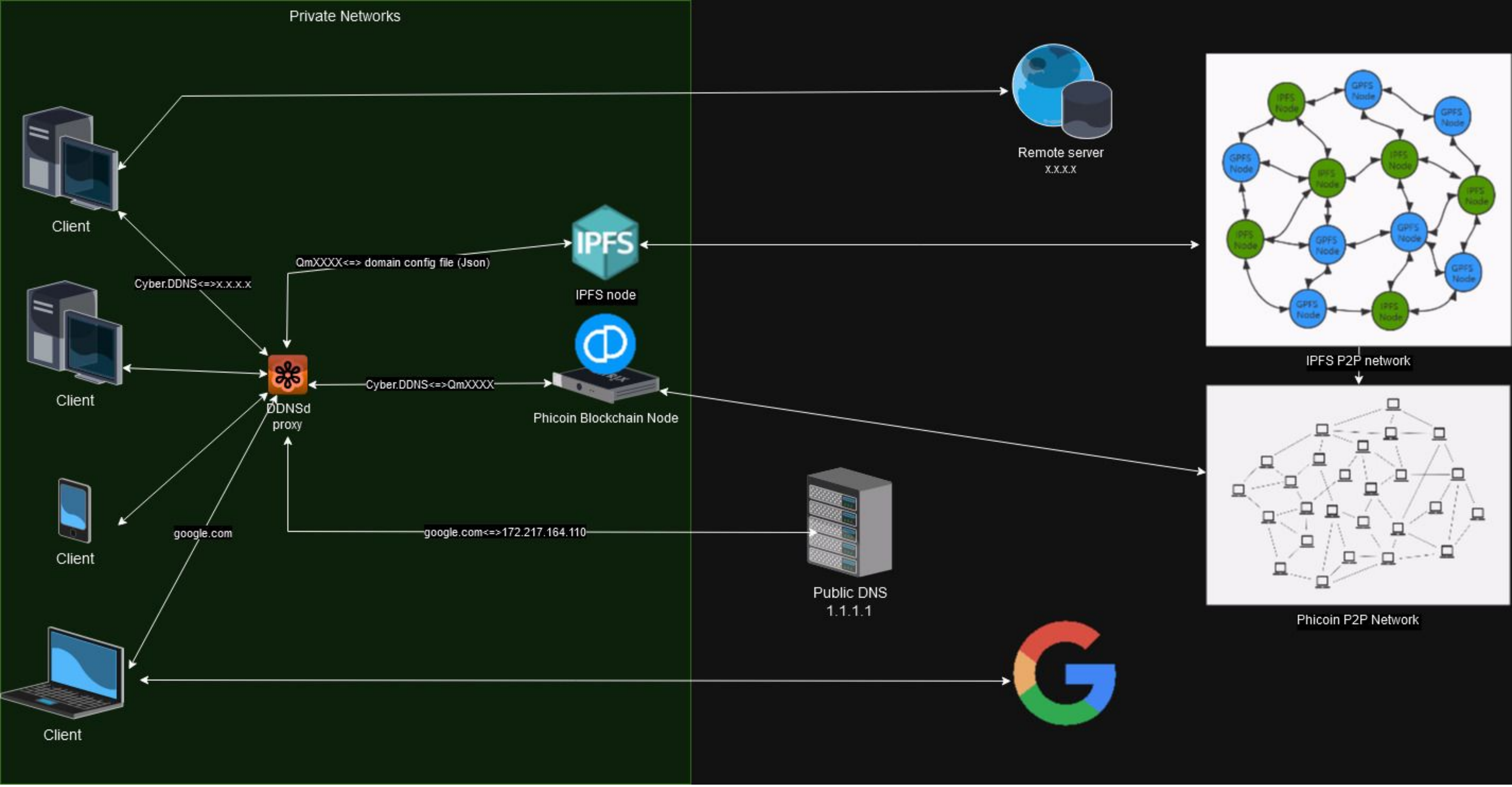
Previous 7 days

Top Traffic Countries / Regions

Previous 7 days

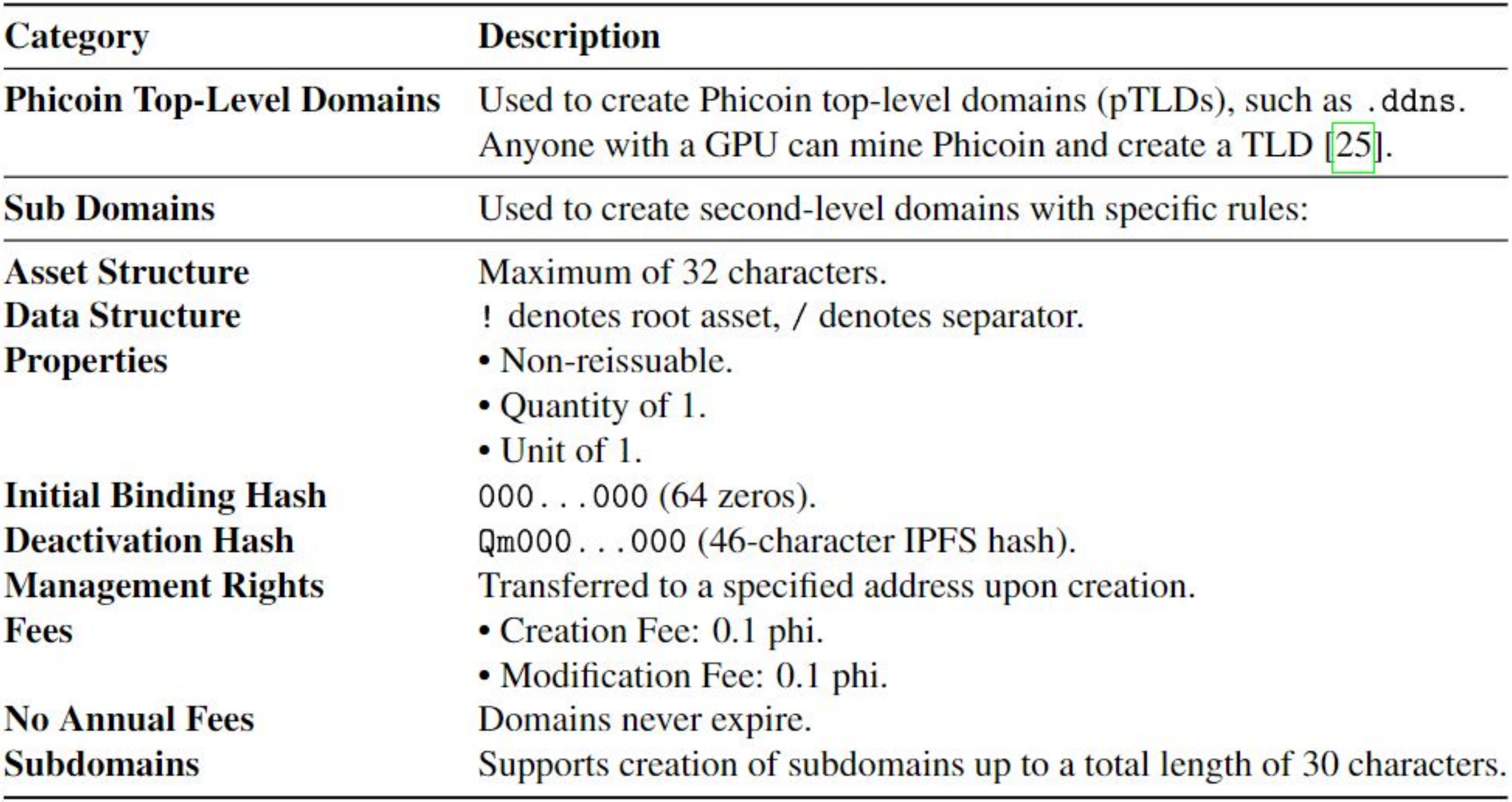
Country / Region	Traffic
Indonesia	1,786,097
Nigeria	1,566,471
United States	955,095
Russian Federation	221,628
Bangladesh	209,276

Berkeley
UNIVERSITY OF CALIFORNIA



DDNS System Architecture

Domain Types:

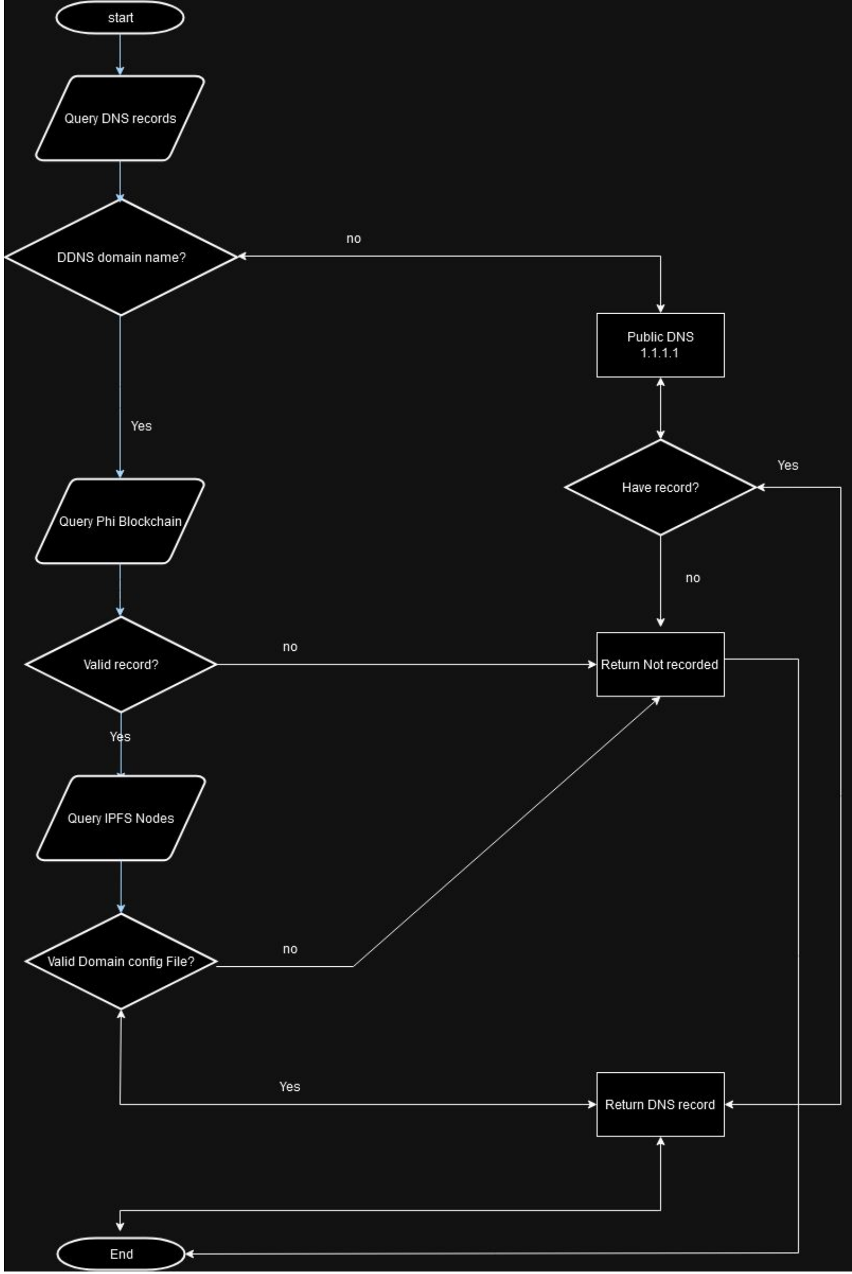


Category	Description
Phicoin Top-Level Domains	Used to create Phicoin top-level domains (pTLDs), such as `.ddns`. Anyone with a GPU can mine Phicoin and create a TLD [25].
Sub Domains	Used to create second-level domains with specific rules:
Asset Structure	Maximum of 32 characters.
Data Structure	`!` 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.

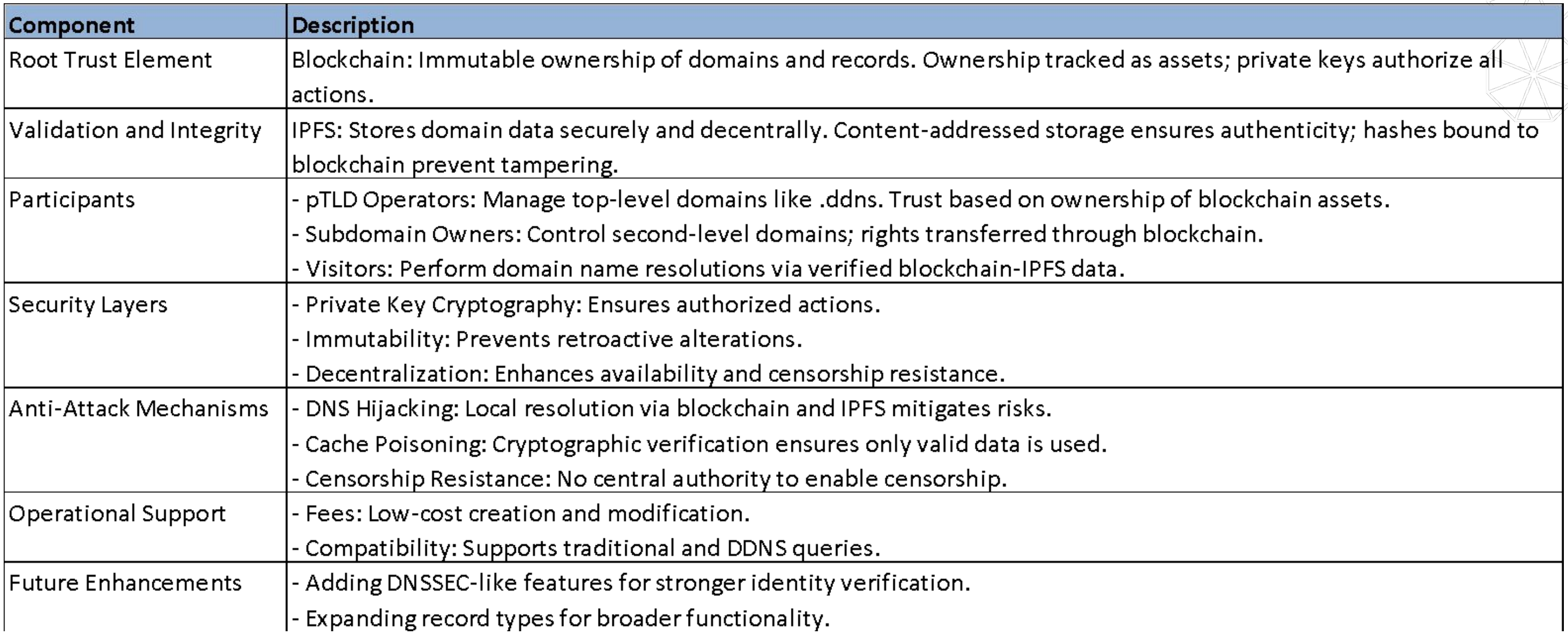
Table 2: Phicoin Domain Rules and Properties

DDNS Domain Queries:

1. Retrieve the IPFS hash from the Phicoin blockchain based on the domainname .
2. 2. Fetch the domain configuration JSON file from IPFS using the hash.
3. 3. Parse the JSON file to extract the domain records.
4. 4. Return the resolution result to the user



DDNSD Flow Chart

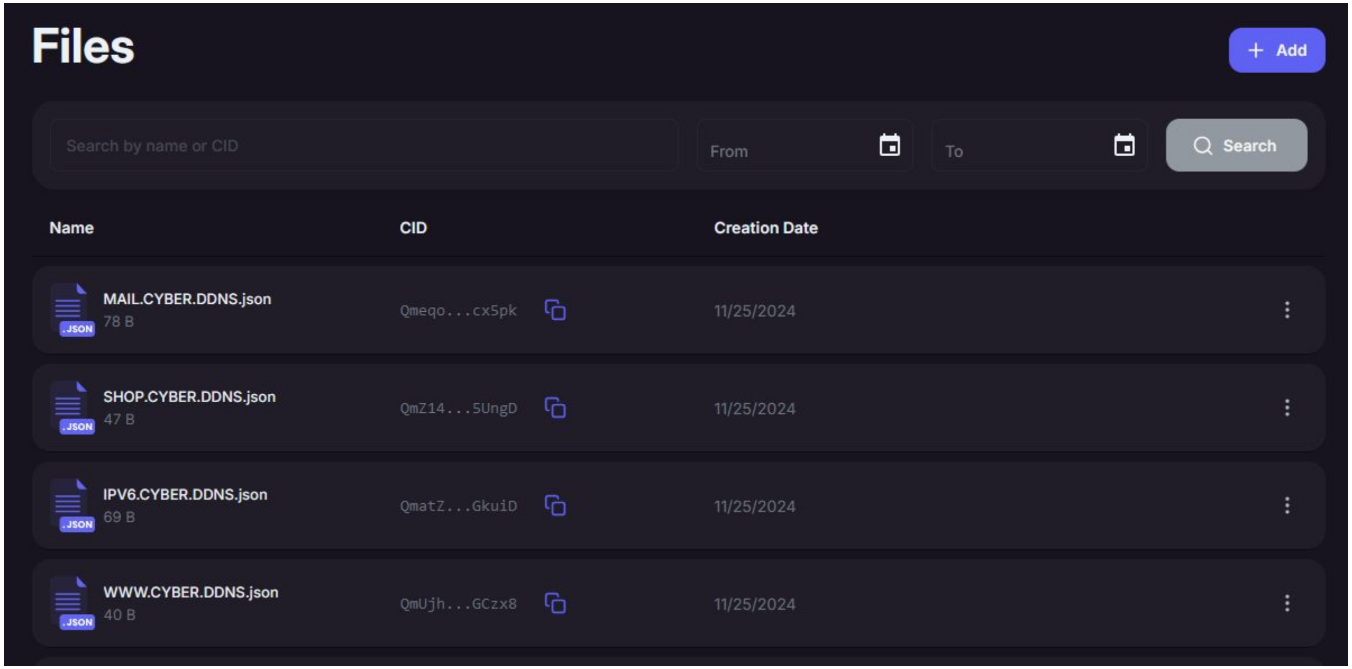


Component	Description
Root Trust Element	Blockchain: Immutable ownership of domains and records. Ownership tracked as assets; private keys authorize all actions.
Validation and Integrity	IPFS: Stores domain data securely and decentrally. Content-addressed storage ensures authenticity; hashes bound to 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.

Trust Chain Analysis for Decentralized Domain Name Service (DDNS)

Berkeley
UNIVERSITY OF CALIFORNIA

Demo:

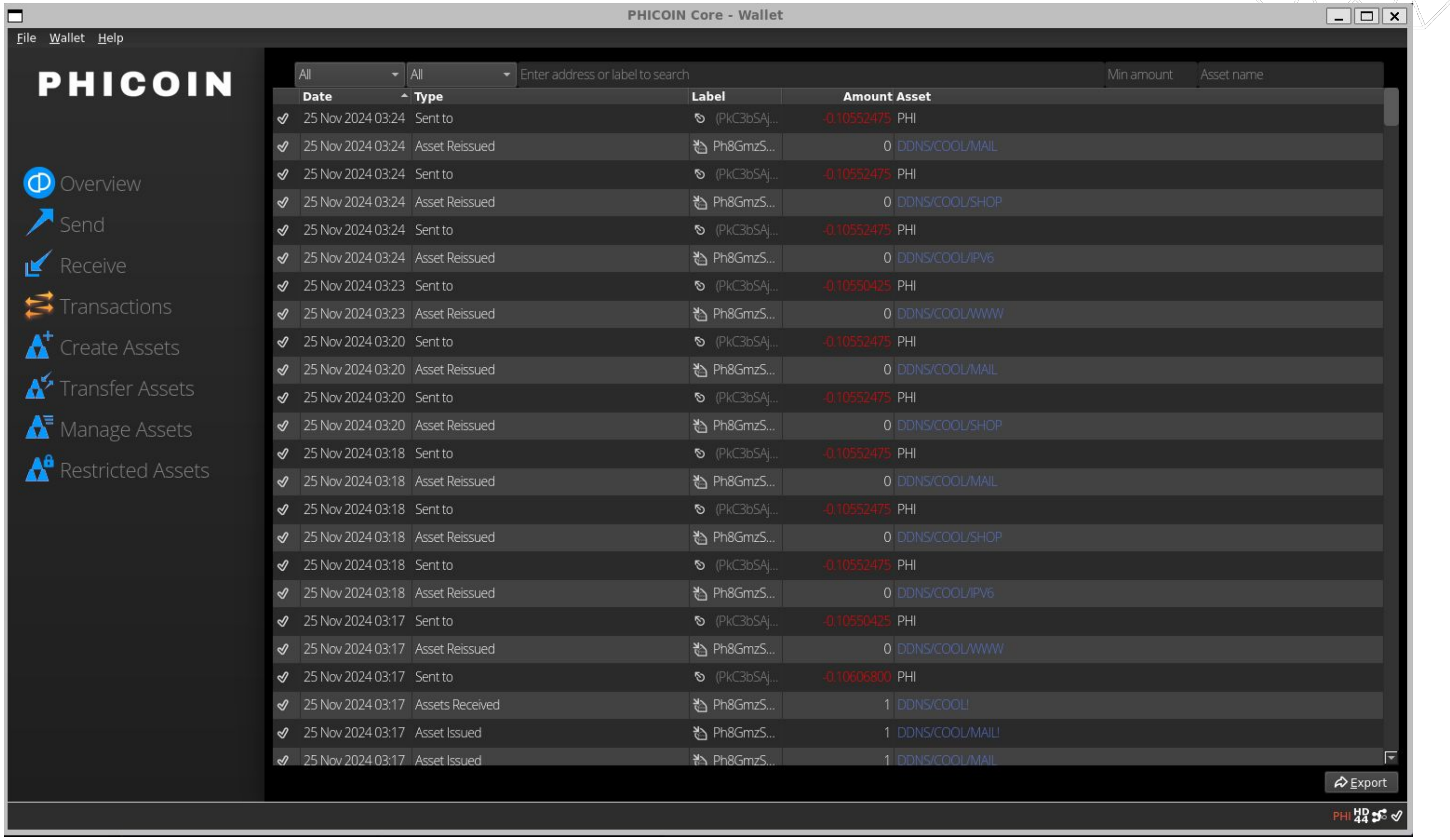


Files

Name	CID	Creation Date
MAIL.CYBER.DDNS.json 78 B	Qmeqo...cx5pk	11/25/2024
SHOP.CYBER.DDNS.json 47 B	QmZ14...5UngD	11/25/2024
IPV6.CYBER.DDNS.json 69 B	QmatZ...GkuiD	11/25/2024
WWW.CYBER.DDNS.json 40 B	QmUjh...GCzx8	11/25/2024

Successfully uploaded to IPFS

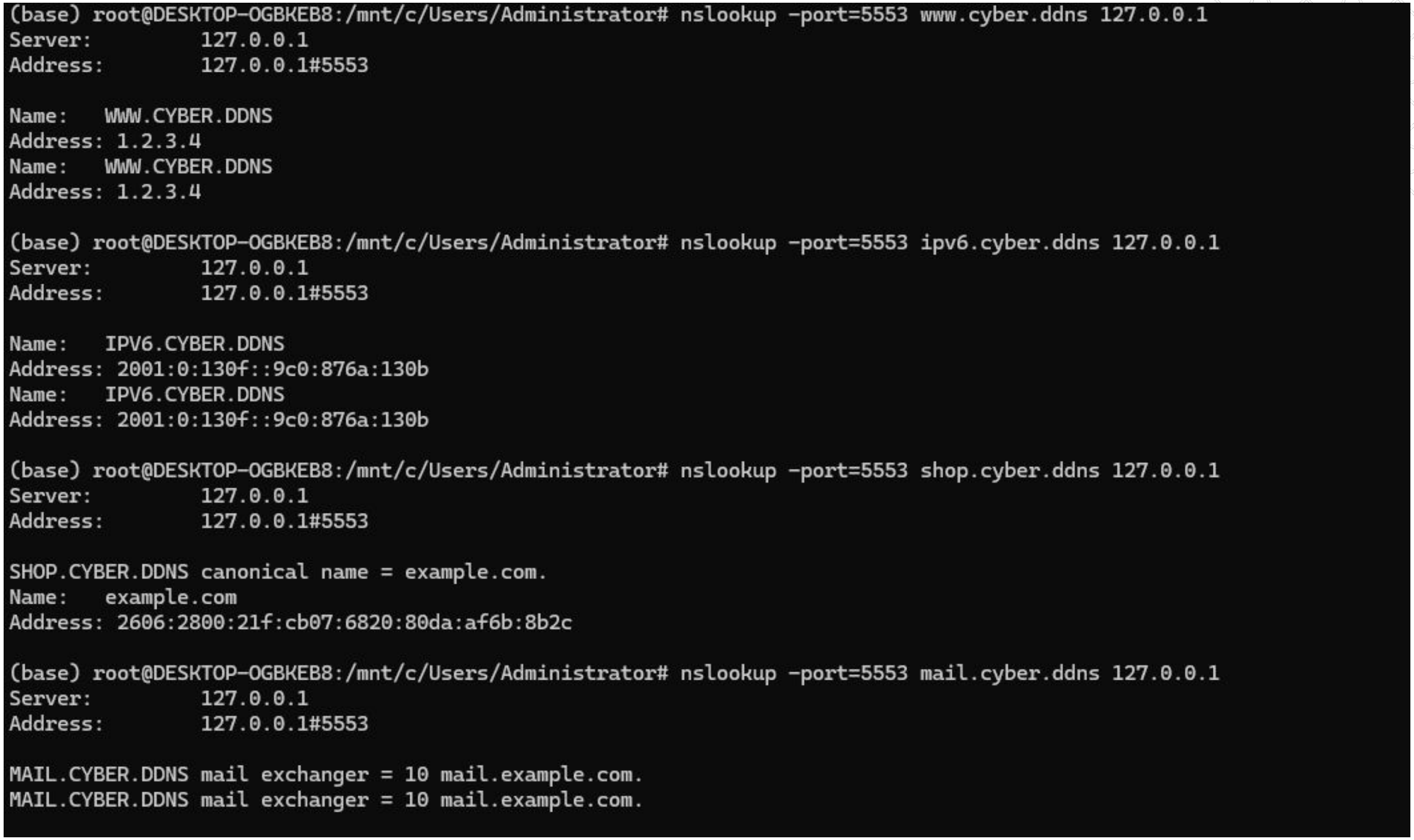
Demo:



	Date	Type	Label	Amount	Asset
✓	25 Nov 2024 03:24	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:24	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/MAIL
✓	25 Nov 2024 03:24	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:24	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/SHOP
✓	25 Nov 2024 03:24	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:24	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/IPV6
✓	25 Nov 2024 03:23	Sent to	(PkC3bSAj...	-0.10550425	PHI
✓	25 Nov 2024 03:23	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/WWW
✓	25 Nov 2024 03:20	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:20	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/MAIL
✓	25 Nov 2024 03:20	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:20	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/SHOP
✓	25 Nov 2024 03:18	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:18	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/MAIL
✓	25 Nov 2024 03:18	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:18	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/SHOP
✓	25 Nov 2024 03:18	Sent to	(PkC3bSAj...	-0.10552475	PHI
✓	25 Nov 2024 03:18	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/IPV6
✓	25 Nov 2024 03:17	Sent to	(PkC3bSAj...	-0.10550425	PHI
✓	25 Nov 2024 03:17	Asset Reissued	Ph8GmzS...	0	DDNS/COOL/WWW
✓	25 Nov 2024 03:17	Sent to	(PkC3bSAj...	-0.10606800	PHI
✓	25 Nov 2024 03:17	Assets Received	Ph8GmzS...	1	DDNS/COOL!
✓	25 Nov 2024 03:17	Asset Issued	Ph8GmzS...	1	DDNS/COOL/MAIL!
✓	25 Nov 2024 03:17	Asset Issued	Ph8GmzS...	1	DDNS/COOL/MAIL

Deployment on blockchain

Demo:



```
(base) root@DESKTOP-OGBKEB8:/mnt/c/Users/Administrator# nslookup -port=5553 www.cyber.ddns 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#5553

Name:   WWW.CYBER.DDNS
Address: 1.2.3.4
Name:   WWW.CYBER.DDNS
Address: 1.2.3.4

(base) root@DESKTOP-OGBKEB8:/mnt/c/Users/Administrator# nslookup -port=5553 ipv6.cyber.ddns 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#5553

Name:   IPV6.CYBER.DDNS
Address: 2001:0:130f::9c0:876a:130b
Name:   IPV6.CYBER.DDNS
Address: 2001:0:130f::9c0:876a:130b

(base) root@DESKTOP-OGBKEB8:/mnt/c/Users/Administrator# nslookup -port=5553 shop.cyber.ddns 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#5553

SHOP.CYBER.DDNS canonical name = example.com.
Name:   example.com
Address: 2606:2800:21f:cb07:6820:80da:af6b:8b2c

(base) root@DESKTOP-OGBKEB8:/mnt/c/Users/Administrator# nslookup -port=5553 mail.cyber.ddns 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#5553

MAIL.CYBER.DDNS mail exchanger = 10 mail.example.com.
MAIL.CYBER.DDNS mail exchanger = 10 mail.example.com.
```

Verify using nslookup

Future Work:

- **Support for Additional DNS Protocols:** Extend domain templates to include recordslike TLSA for DANE, enabling secure certificate verification without traditional Certifi-cate Authorities (CAs)

- **User Interface Improvements:** Develop intuitive tools and graphical interfaces for do-main registration and management to lower the entry barrier for non-technical users.

- **Public DDNS Resolution Nodes:** Deploy public nodes compatible with traditional DNSto facilitate adoption and ease of use for end-users.

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.

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 who provided me with a solar farm so that I can use free electricity to run Phicoin's seeder nodes, mining pools, and mining machines.

Thank You!

Berkeley
UNIVERSITY OF CALIFORNIA