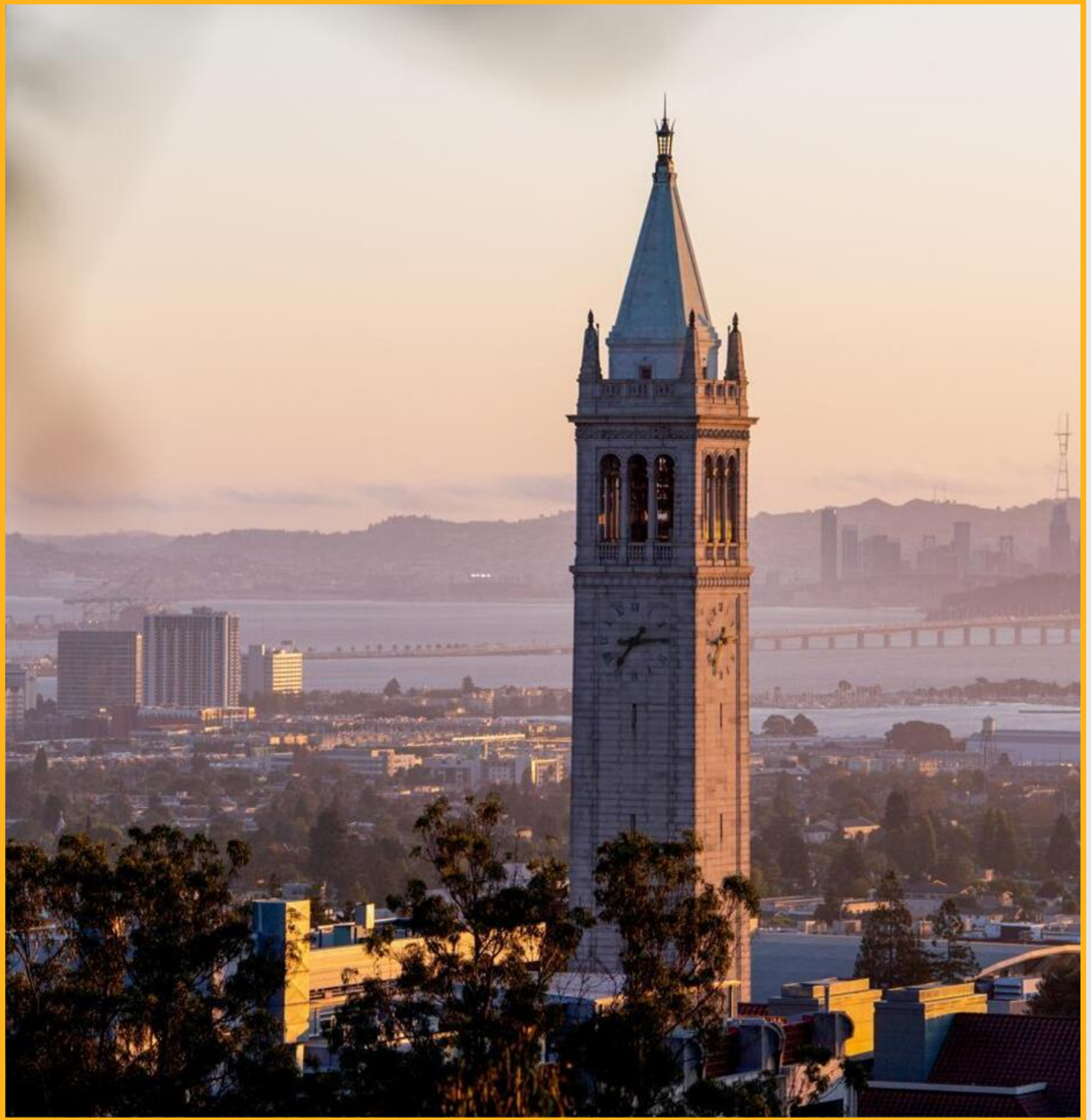
UC Berkeley

Blockchain-based Decentralized Domain Name System

MICS Summer 2025 Capstone

Alma Nkemla • Amuru Serikyaku
Edward Tatchim • Guang Yang
Osman Sharaf • Peter Trinh



DECENTRALIZED DOMAIN NAME DDNS

Team Member Roles & Responsibilities

Thomas

Engineering & Product Manager

Amu

Engineering

Edward

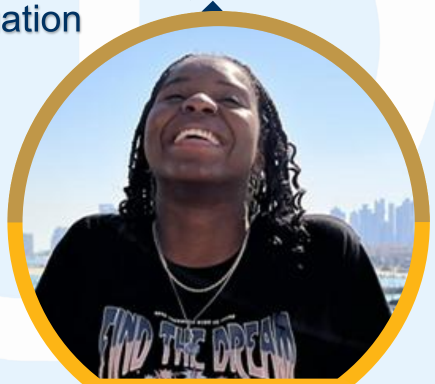
Security & Evaluation

Peter

Engineering & Product Manager

Osman

Engineering



Alma

Communications & Outreach

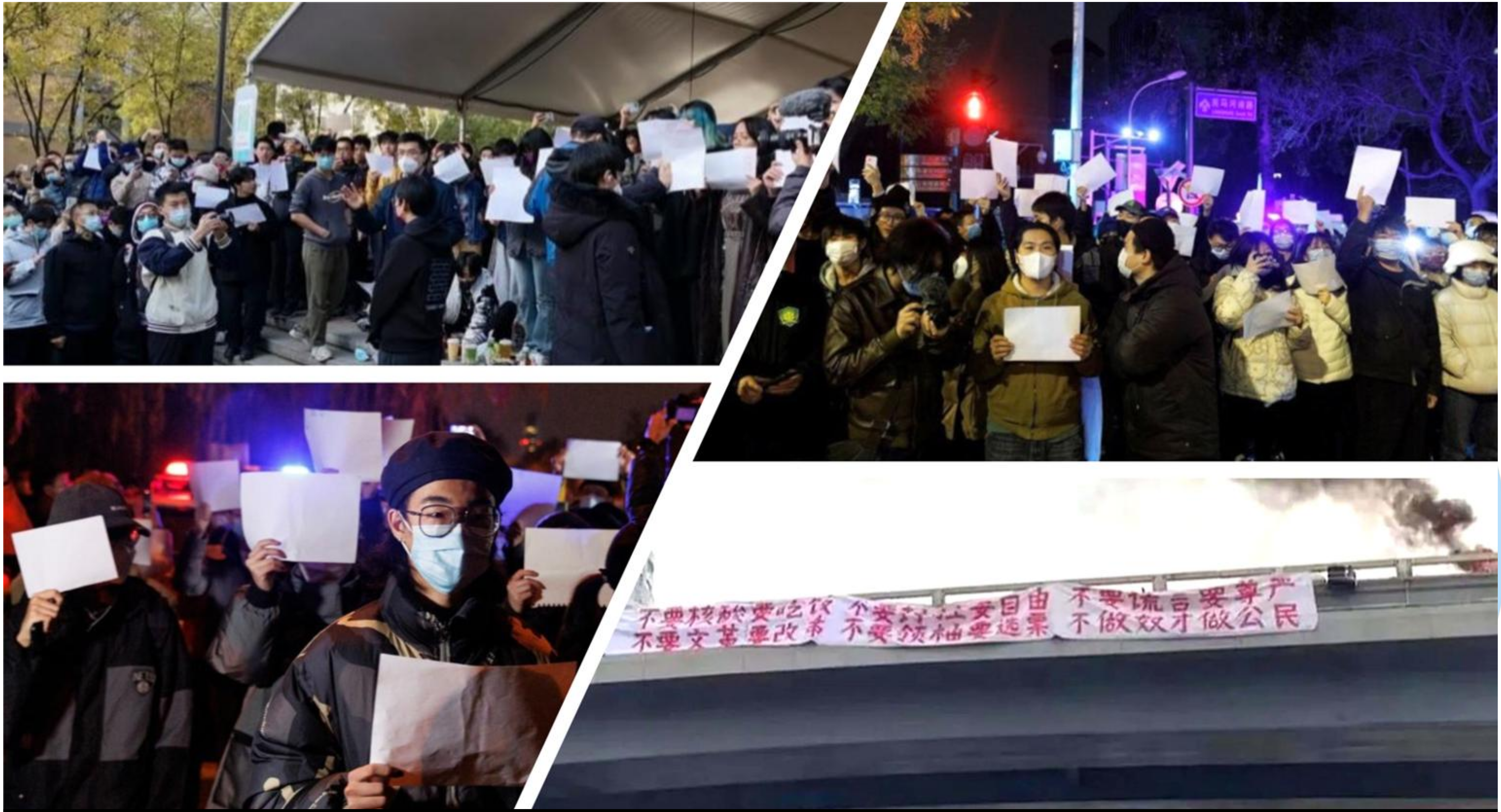
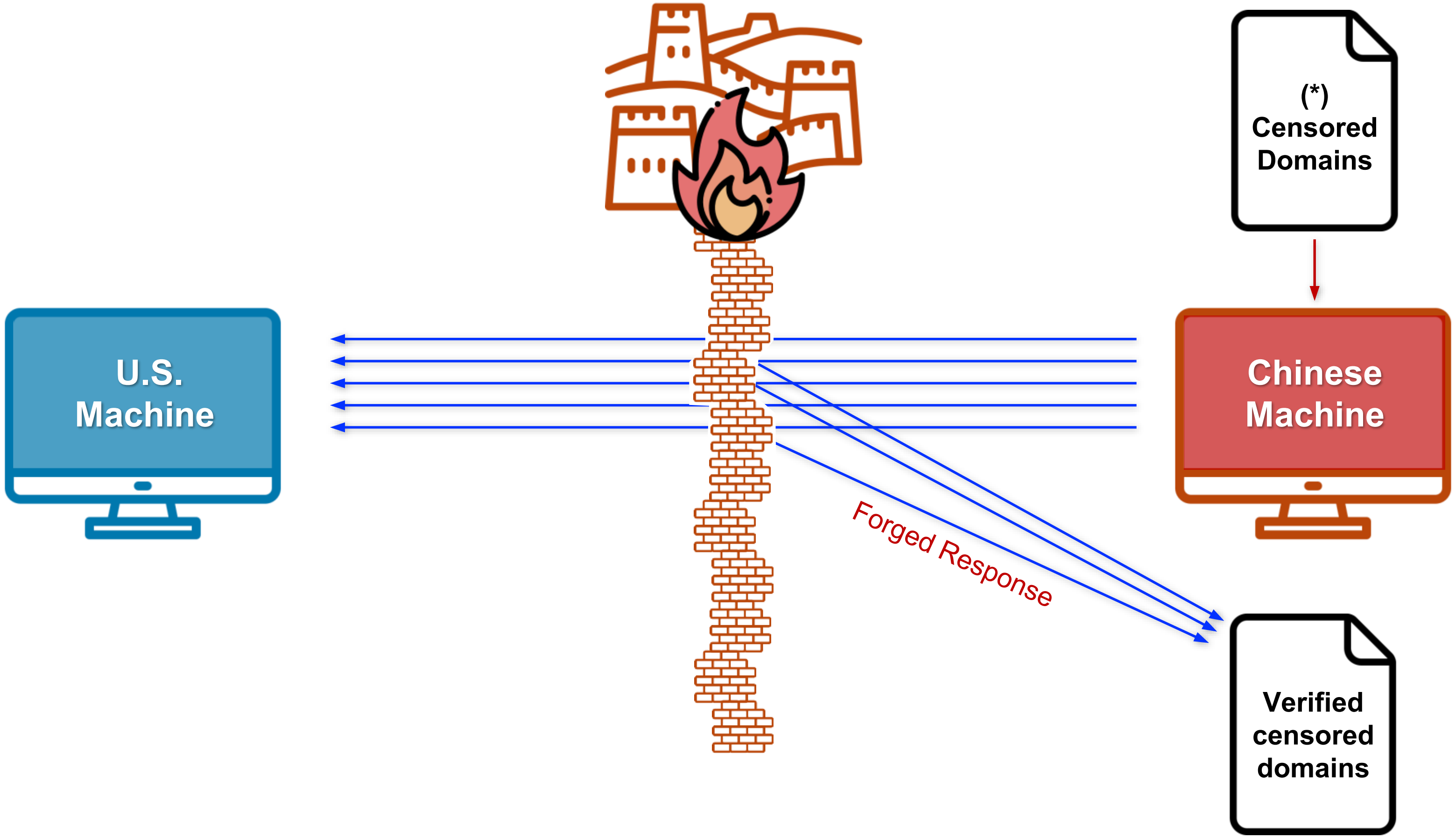

不要核酸要吃饭 不要封控要自由 不要谎言要尊严
不要文革要改革 不要领袖要选票 不做奴才做公民

Photo: Students in China protest at the Sitong Bridge Protest during the White Paper Revolution, October 13, 2022 – December 7, 2022

Chinese Censorship Tactics

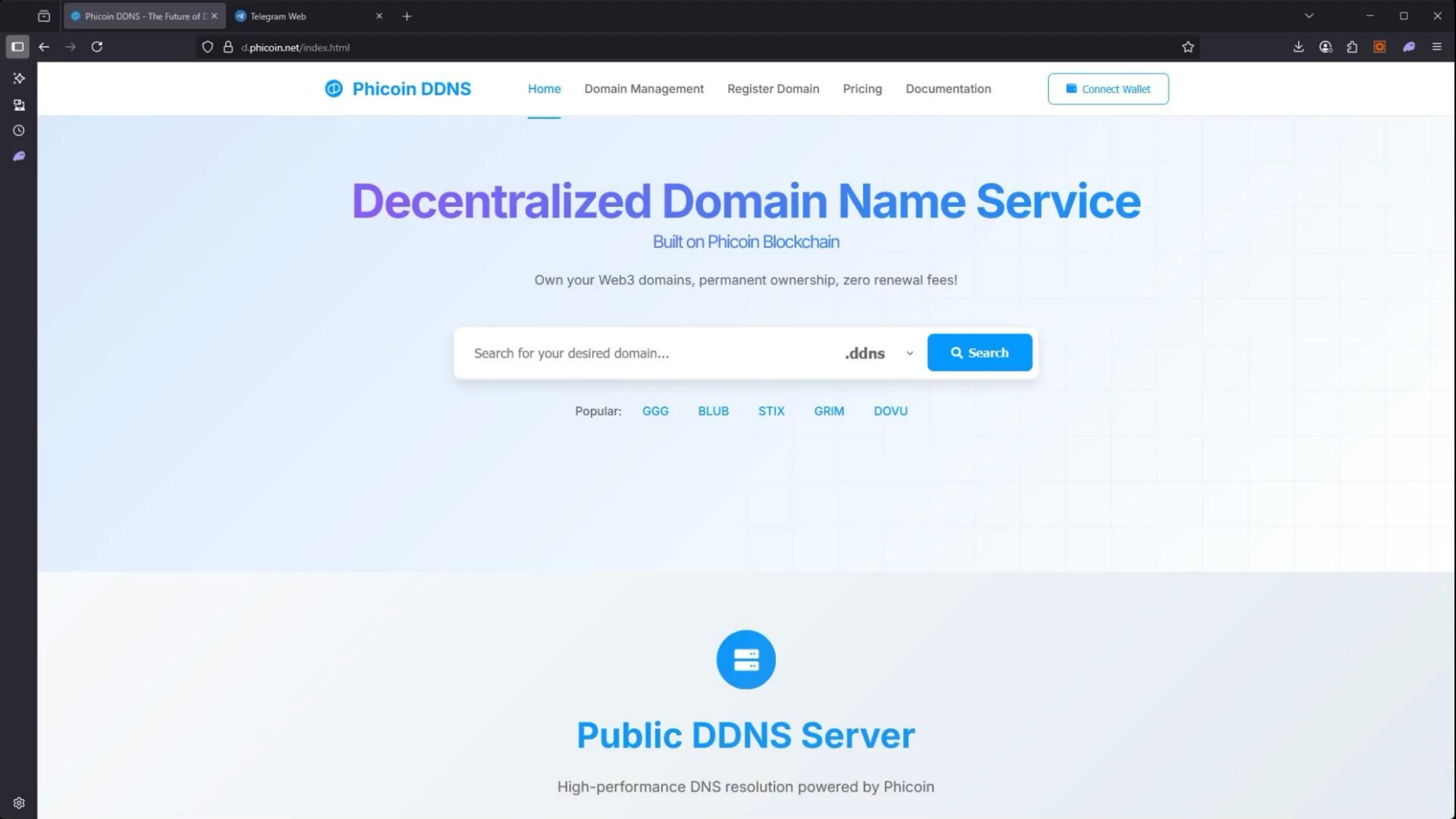


DDNS Value Proposition

- Circumvent censorship regimes
- Rapid deployment of information, at the time of need
- Freedom in a sovereign digital frontier

Our Guiding Principles

1. Enable censorship-resistant domain resolution
2. Provide cryptographic verification for DNS operations
3. Maintain compatibility with existing internet infrastructure
4. Eliminate single-points-of-failure



Phicoin DDNS

Home | Domain Management | Register Domain | Pricing | Documentation

Connect Wallet

Decentralized Domain Name Service

Built on Phicoin Blockchain

Own your Web3 domains, permanent ownership, zero renewal fees!

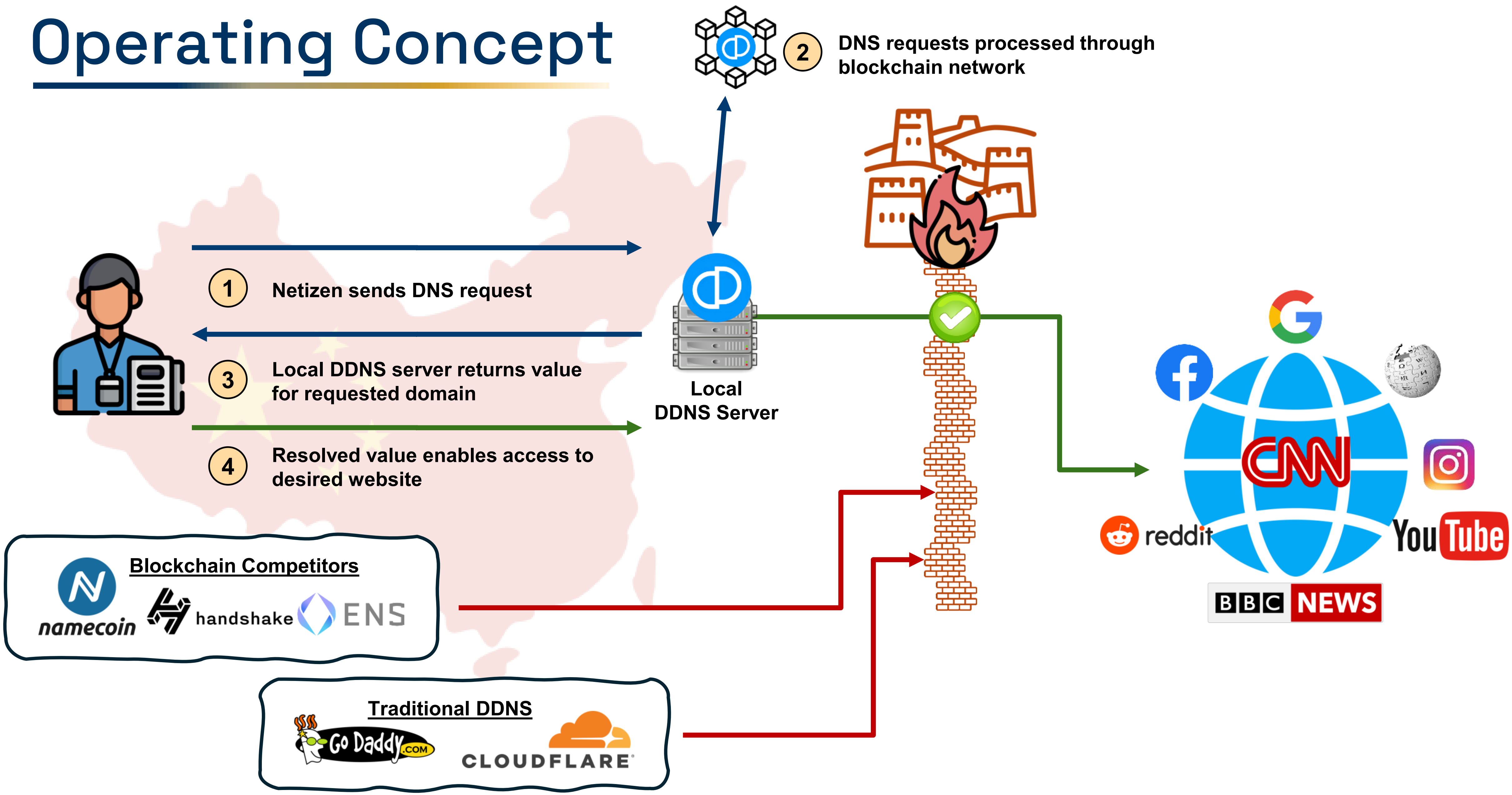
Search for your desired domain... .ddns Search

Popular: GGG BLUB STIX GRIM DOVU

Public DDNS Server

High-performance DNS resolution powered by Phicoin

Operating Concept



2 DNS requests processed through blockchain network

1 Netizen sends DNS request

3 Local DDNS server returns value for requested domain

4 Resolved value enables access to desired website

Local DDNS Server

Blockchain Competitors

Traditional DDNS

STRIDE Matrix

Spoofing

Preventing fake identities and forged registrations through cryptographic verification

Tampering

Ensuring data integrity by leveraging blockchain and IPFS immutability

Repudiation

Establishing accountability through auditable and traceable records

Information Disclosure

Protecting sensitive data with encryption and access controls

Denial of Service

Maintaining system availability through redundancy and rate limiting

Elevation of Privilege

Securing user keys and node privileges with secure management practices

51% of the global internet population

. . .

2 billion

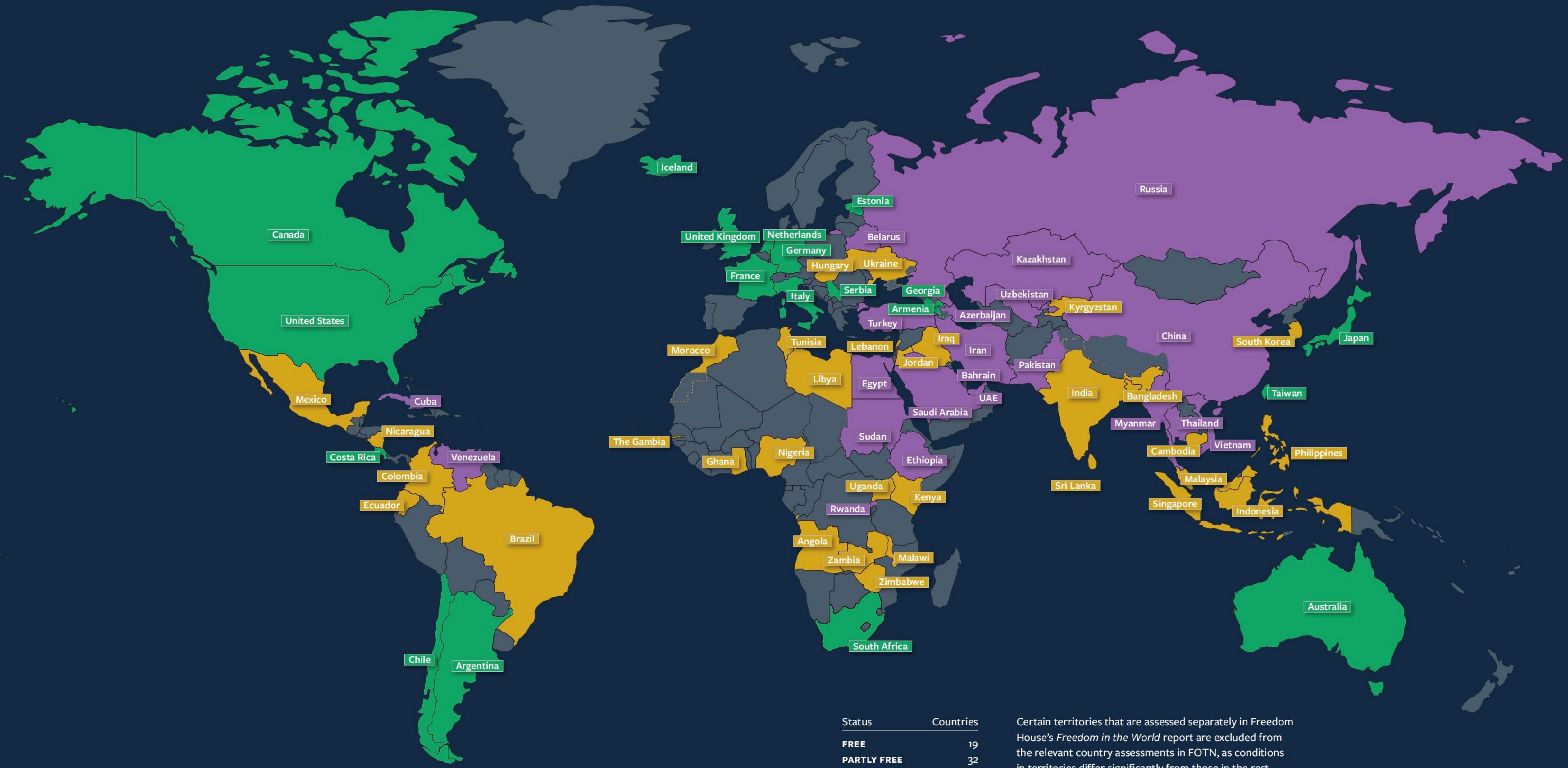
612,384,329 people

lived under “partly free” or “not free” internet governance regimes.

Source: Freedom House - Freedom of the Net 2024

FREEDOM ON THE NET 2024

Source: Freedom House (2024)

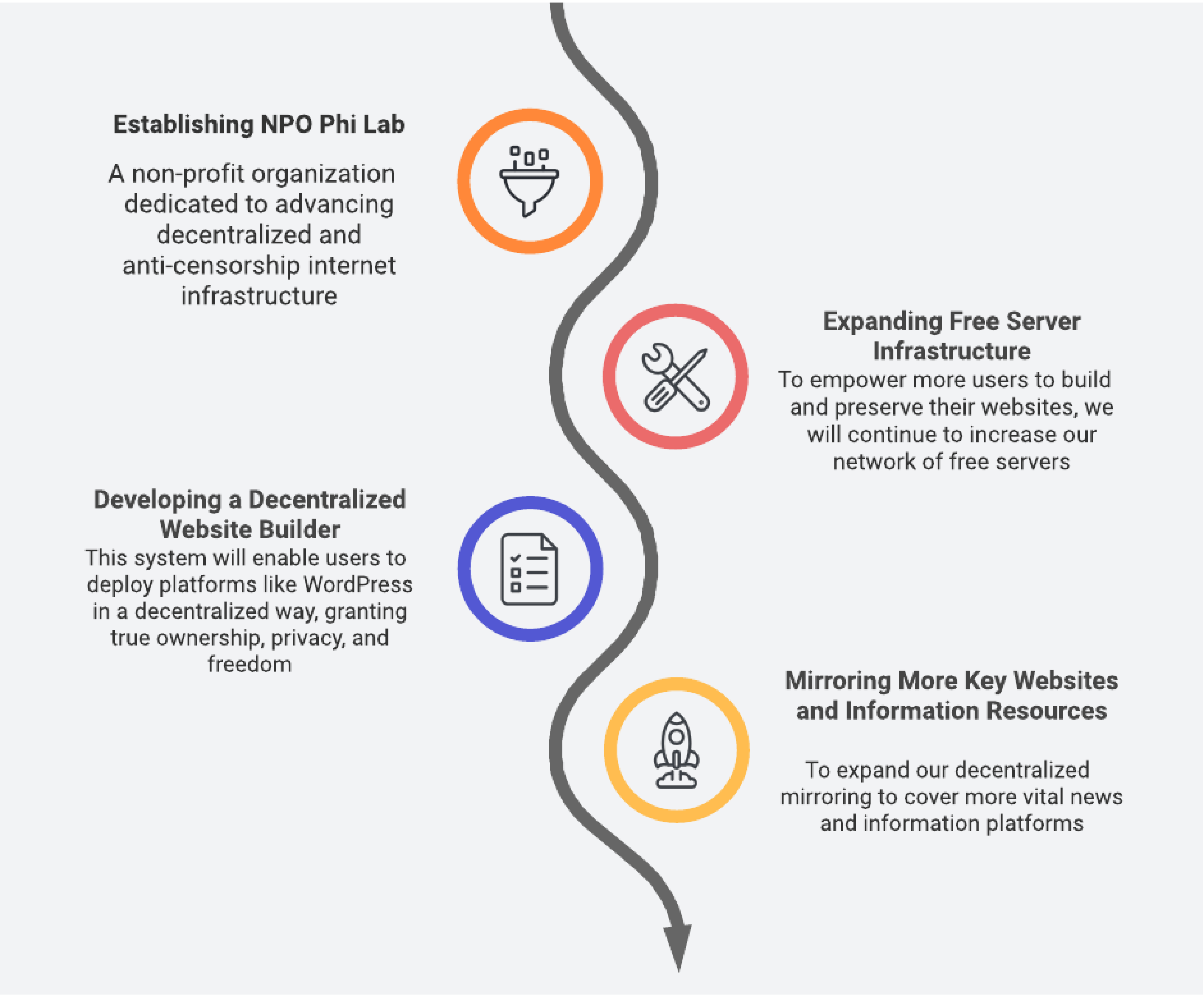


🟩 FREE 🟨 PARTLY FREE 🟪 NOT FREE ⬛ NOT ASSESSED

Status	Countries
FREE	19
PARTLY FREE	32
NOT FREE	21
Total	**72**

Certain territories that are assessed separately in Freedom House's *Freedom in the World* report are excluded from the relevant country assessments in FOTN, as conditions in territories differ significantly from those in the rest of the country. For more information about the report's geographical coverage, visit freedomonthenet.org.

Roadmap



Establishing NPO Phi Lab

A non-profit organization dedicated to advancing decentralized and anti-censorship internet infrastructure

Expanding Free Server Infrastructure

To empower more users to build and preserve their websites, we will continue to increase our network of free servers

Developing a Decentralized Website Builder

This system will enable users to deploy platforms like WordPress in a decentralized way, granting true ownership, privacy, and freedom

Mirroring More Key Websites and Information Resources

To expand our decentralized mirroring to cover more vital news and information platforms

To those who risk everything for a free and open internet.

Start using DDNS now:

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

For more technical details: https://eprint.iacr.org/2025/1381.pdf