ISSN 0002-306X. Proc. of the RA NAS and NPUA Ser. of tech. sc. 2025. V. LXXVIII, N1

UDC 004.8

COMPUTER SCIENCE AND INFORMATICS

DOI: 10.53297/0002306X-2025.v78.1-87

A.SH. HARUTYUNYAN

CENSORSHIP RESISTANCE IN WEB3 ACCESS LAYERS: AN ENGINEERING PERSPECTIVE ON INDEPENDENT RENDERING GATEWAYS

Censorship resistance is a core value of Web3, yet practical access to decentralized websites remains dependent on centralized gateways such as ***ipfs.io, .link***, and ***.limo***, which are susceptible to regulatory takedowns and availability limitations. This paper investigates the technical barriers to truly censorship-resistant access in decentralized web architectures and presents an engineering-driven analysis of ***dweb3.wtf***, a dedicated rendering gateway developed within the Web3Compass infrastructure. The system directly interfaces with decentralized name systems such as ENS and Unstoppable Domains, autonomously resolves content hashes via on-chain resolvers, and renders the associated IPFS-hosted sites via self-hosted infrastructure. By eliminating reliance on third-party APIs and centralized frontends, the gateway offers a robust alternative to Web2-style intermediaries. This paper presents the architecture, implementation, and performance characteristics of ***dweb3.wtf***, evaluating its effectiveness in ensuring access continuity, domain coverage, and reduced external dependency.

Keywords:Web3, Decentralised web, Censorship Resistance, IPFS, ENS, Proxy Gateway, Autonomous Infrastructure.

Introduction. The decentralized web aims to distribute control across protocols rather than institutions. Core components-such as IPFS for storage and ENS for naming-offer verifiable and permissionless alternatives to traditional hosting and DNS. However, the decentralized vision encounters a critical bottleneck in practice: access tooling. While decentralized websites can exist independently of central servers, users still rely on Web2-compatible gateways to retrieve and render this content in mainstream environments.

Today, most users attempting to open a decentralized site-such as one resolved through an ENS domain-must pass through a gateway like ***ipfs.io***, which aggregates content from IPFS nodes and displays it in a browser-readable form. These gateways, although technically functional, are subject to centralized policies, regional restrictions, and legal compliance demands. Their failure or censorship renders the decentralized site effectively inaccessible, undermining the very premise of decentralization.

This access-layer fragility necessitated an engineering response. Within the development of Web3Compass-a real-time, protocol-aware search system for decentralized domains-a dedicated rendering layer was introduced under the hostname ***dweb3.wtf.*** Its role is to serve as a censorship-resistant, low-latency, self-hosted gateway capable of resolving and rendering IPFS-linked content from multiple domain registries without introducing centralized chokepoints. This paper describes the challenges, design considerations, and technical implementation of this gateway, contributing to the broader discourse on usable, censorship-resistant infrastructure in Web3.

Analysis of the existing works. Censorship resistance in the decentralized web is often cited as one of its primary advantages over traditional Internet infrastructure. The foundational theory behind censorship resistance lies in the removal of single points of control-namely centralized servers and domain name registrars-which are vulnerable to legal or regulatory pressures. Systems such as the InterPlanetary File System (IPFS) and blockchain-based domain registries like Ethereum Name Service (ENS) and Unstoppable Domains (UD) exemplify this design by enabling content and naming records to be stored in peer-to-peer or on-chain networks rather than in state-governed databases.

Despite this theoretical robustness, practical access to decentralized content is frequently routed through centralized gateways. Studies have identified that services such as ***ipfs.io, cloudflare-ipfs.com***, and ***.limo*** often act as chokepoints in the architecture, rendering them susceptible to takedowns, surveillance, or content filtering under legal obligation or voluntary moderation frameworks [1]. Research by Mooney [2] on IPFS gateways highlights that many of these nodes cache and serve limited subsets of content, often prioritizing popular or whitelisted CIDs, thereby undermining claims of neutrality and censorship-resistance.

Decentralized domain resolution faces parallel issues. While ENS and UD provide cryptographically verifiable mappings between names and content hashes, resolution tools such as browser extensions or embedded resolvers are required to translate these names into retrievable IPFS paths. The existing browser integrations (e.g., Brave) support ENS resolution, but rely on fallback APIs and do not cover all protocols or domain extensions. Moreover, even with resolution tools, content hosting remains dependent on node availability or pinning services-often provided by centralized actors such as Pinata or Infura-reintroducing dependence on third parties [3].

Approaches to bypass centralized choke points have included user-side tooling (e.g., self-hosted IPFS nodes), local resolvers, and gateway diversification. However, these solutions require advanced technical knowledge, limiting adoption. The introduction of censorship-resistant rendering gateways, like ***dweb3.wtf***, aligns with prior academic recommendations emphasizing the need for decentralized

delivery infrastructure. As identified by Raviv & Kim [1], the redundancy of access paths and the independence from centralized DNS resolution or gateway policy are key indicators of effective censorship resistance.

In parallel, broader Web3 studies emphasize the trade-off between accessibility and decentralization. Systems that provide smoother user experience often reintroduce central points of control in the name of performance, reliability, or legal compliance [4]. Consequently, truly censorship-resistant gateways must strike a balance: enabling universal access while maintaining technical and legal autonomy. The engineering approach described in the Web3Compass system—operating dedicated IPFS nodes, independently resolving domain records, and hosting a custom rendering gateway-directly responds to this gap by providing reliable, regulation-independent access to decentralized content.

Architecture and Implementation. The dweb3.wtf gateway was engineered as an autonomous access layer within the Web3Compass ecosystem to ensure uninterrupted availability of decentralized web content, independent of centralized resolution or rendering services. Its architecture addresses two key constraints in decentralized access: 1) resolution of domain names across heterogeneous blockchain-based registries, and 2) retrieval and rendering of content hosted on decentralized storage networks, primarily IPFS.

Domain resolution layer

The first stage of the gateway's operation is protocol-aware domain resolution. Web3Compass continuously monitors the decentralized domain name systems such as ENS (Ethereum Name Service), Unstoppable Domains (hosted on Polygon), and BNB NS (via SpaceID). Each registry is queried using dedicated resolvers. In the case of ENS, a smart contract stores the resolver address for each domain. The resolver is subsequently queried via standard interfaces such as *contenthash()* to extract the content identifier (CID). Similar methods are applied to other registries, using specific resolution logic per contract specification.

To ensure modularity and fault-tolerance, the resolution layer uses asynchronous event monitoring from blockchain networks through APIs such as Alchemy and subgraphs (e.g., ENS subgraph). Upon detection of a new or updated domain, the system extracts metadata including the CID and caches the mapping internally for lookup by the gateway.

IPFS integration and content retrieval

The CID obtained from the resolver is used to access the content stored on the InterPlanetary File System (IPFS). To avoid dependency on public gateways such as ipfs.io, dweb3.wtf is backed by a cluster of self-hosted IPFS nodes maintained by Web3Compass. This infrastructure allows direct retrieval of content without routing through centralized services, ensuring resilience against both downtime and takedown requests.

To guarantee persistence, Web3Compass selectively pins content on its own IPFS nodes. Content under 100MB and identified as HTML-based is prioritized for pinning, while non-relevant formats (e.g., videos, ZIP files, PDFs) are excluded from indexing and delivery. If content is not pinned, the gateway gracefully falls back to public gateways, but only as a last resort, preserving the censorship-resistant priority of self-hosted infrastructure.

Rendering and dynamic content handling

Once retrieved, content is rendered and served through dweb3.wtf. A critical challenge addressed here is support for Single Page Applications (SPAs) and client-side rendered content, which require execution of JavaScript to fully build the Document Object Model (DOM). To solve this, the gateway integrates a headless browser stack (e.g., Puppeteer) that programmatically loads the page, waits for the DOM to stabilize, and scrapes the final HTML before serving it to users.

This ensures that decentralized websites relying on in-browser rendering are fully accessible through dweb3.wtf, a capability often absent in alternative gateways that serve static content only. The system detects whether a site requires headless rendering based on the response structure and automatically initiates dynamic rendering if necessary.

Domain coverage and unified routing

Unlike other gateways limited to specific TLDs, dweb3.wtf is designed to support a wide variety of decentralized domain extensions indexed by Web3Compass. This includes *.eth, .crypto, .polygon, .dao, .wallet, .nft, .zil, .x*, and emerging namespaces such as *.tomi* and *.bnb*. The routing engine recognizes the domain extension, matches it to its corresponding resolution logic, and fetches the CID accordingly.

Once resolved, URLs are mapped to a unified access structure. For instance:

https://dweb3.wtf/ipfs/<CID>/

https://dweb3.wtf/<domain.extension>/

This enables seamless integration of human-readable names with underlying content identifiers, maintaining user-friendly navigation without compromising backend decentralization.

API and rate limiting

To support programmatic access, dweb3.wtf exposes an API with a simple authentication mechanism using API keys. The current rate limiting policy allows 60 requests per minute per key, sufficient for moderate third-party use cases while preventing abuse. This complements the frontend interface and allows for integration into other applications or browser extensions.

Evaluation. The evaluation of dweb3.wtf as a censorship-resistant rendering gateway focuses on its functional alignment with the Web3Compass objectives: independence from centralized chokepoints, broad decentralized domain coverage, reliable content delivery, and compatibility with dynamic web architectures.

Availability and uptime strategy

Unlike traditional IPFS gateways such as *ipfs.io* or *cloudflare-ipfs.com*, which are subject to regional takedown orders and infrastructural downtime, dweb3.wtf operates via a self-hosted IPFS cluster maintained by Web3Compass. This ensures content is not reliant on public access nodes, which may become unresponsive or filtered. While public fallback is implemented, it activates only when internal nodes fail, preserving autonomy as the default mode of operation.

The infrastructure is intentionally redundant: multiple IPFS nodes ensure content availability through selective pinning and fallback tolerance. For instance, content under 100MB deemed HTML-relevant is proactively pinned across nodes, guaranteeing persistent access even in the absence of active external replication.

Domain diversity and protocol compatibility

A key performance indicator for dweb3.wtf is the breadth of supported decentralized domains. As indexed by Web3Compass, the gateway successfully renders websites associated with domain extensions such as *.eth, .crypto, .wallet, .polygon, .zil, .nft, .x, .dao, .bnb, .tomi,* and others. Each domain family is mapped to its respective on-chain registry (ENS, CNS/UD, BNB NS via SpaceID), and dweb3.wtf applies custom resolution logic per protocol.

This registry-agnostic design ensures broader compatibility than most Web3 redirectors, which typically support only a subset (e.g., ENS domains). The unified routing format-resolving both CID and human-readable names-enables consistent access across heterogeneous naming systems.

Rendering depth: static vs. dynamic sites

To accommodate Single Page Applications (SPAs) and client-rendered content, dweb3.wtf integrates a headless browser rendering pipeline. This feature is essential for Web3 content that relies heavily on JavaScript and in-browser DOM construction, which cannot be parsed by static crawlers.

The gateway automatically detects whether dynamic rendering is required based on the initial response and triggers headless rendering accordingly. This design ensures that both static and dynamic decentralized websites are served in their fully built form, avoiding incomplete or empty page loads-a known limitation of competing IPFS gateways.

User access and API integration

Programmatic interaction is supported via an authenticated API, with a rate limit of 60 requests per minute per key. While this is not designed for high-throughput scraping, it enables controlled integration into third-party applications or browser extensions. By exposing gateway logic through an API, dweb3.wtf supports both end-user access and developer tooling, enhancing its role as a practical censorship-resistant access layer.

Conclusion and future work. This paper presents an engineering analysis of dweb3.wtf, a censorship-resistant rendering gateway developed as part of the Web3Compass infrastructure. The system addresses the key technical limitation of decentralized web access: the dependency on centralized gateway services for resolution and content rendering. By integrating self-hosted IPFS nodes, dynamic rendering support, and protocol-aware domain resolution for a wide range of registries-including ENS, Unstoppable Domains, and BNB NS-dweb3.wtf demonstrates a practical architecture for preserving access continuity and autonomy in Web3 environments. Unlike generalized gateway services such as ipfs.io or .limo, the implementation of dweb3.wtf deliberately avoids reliance on centralized intermediaries wherever feasible. The system resolves domain records using verified on-chain data, fetches content via its own IPFS infrastructure, and renders both static and dynamic websites with in-browser JavaScript dependencies via a headless rendering layer. This ensures that even client-rendered decentralized sites remain accessible through a Web2-compatible interface, without compromising on censorship resistance.

Future work on the platform will focus on expanding domain registry support and improving routing efficiency. While the current system integrates a diverse range of domain extensions and resolution schemes, additional protocols and emerging name services may require custom integration logic. Another area for improvement is the robustness of content pinning and node reliability under varying network conditions. While the fallback to public gateways is retained for availability assurance, efforts will continue to prioritize access via self-hosted infrastructure as the default pathway.

Finally, opportunities exist to integrate decentralized frontend verification methods, enabling users to view cryptographic proofs of content origin and immutability directly within the rendering layer. This could further strengthen the trust guarantees of the access system without introducing behavioral tracking or identity linkage.

Through dweb3.wtf, Web3Compass provides a concrete, deployable solution to one of the decentralized web's core bottlenecks: practical, reliable, and censorship-resistant access. The architecture serves as a model for similar gateway efforts and contributes to a more resilient decentralized internet infrastructure.

REFERENCES

1. **Raviv, O., & Kim, M**. Decentralized Web: A Review of IPFS, Gateways, and Censorship Resistance // IEEE Internet Computing, -2022.- Vol. 26, no. 3.- P. 45–52.
2. **Mooney, J., Kumar, S., & Zhang, Y.** Measuring the Reliability and Bias of IPFS Public Gateways // In Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS). -2023.

3. **Wang, T., Gupta R., & Ren, K.** Understanding and Securing Content Resolution in Decentralized Name Services..// NDSS Symposium. -2023.
4. **Zhao, L., & Li, H.** Balancing Usability and Censorship Resistance in Decentralized Web Systems// Journal of Web Engineering. -2021-. Vol. 20, no. 5.- P. 1013–1031.

National Polytechnic University of Armenia. The material is received on 01.12.2025

Ա.Շ. ՀԱՐՈՒԹՅՈՒՆՅԱՆ

ԳՐԱՔՆՆՈՒԹՅԱՆԸ ԴԻՄԱԿԱՅՈՒՄ WEB3 ՄՈՒՏՔԻ ՇԵՐՏԵՐՈՒՄ. ԱՆԿԱԽ ՄԱՏՈՒՑՄԱՆ ԴԱՐՊԱՍՆԵՐ. ՀԱՅԱՅՔ ՃԱՐՏԱՐԱԳԵՏԻ ՏԵՍԱՆԿՅՈՒՆԻՑ

Web3-ի գրաքննությանը դիմակայելու հիմնական արժեքը հակասում է կենտրոնացված դարպասների (ipfs.io, .link, .limo) կախվածությանը: Ուսումնասիրվում են ապակենտրոնացված կայքերի մատչելիության տեխնիկական խոչընդոտները, և ներկայացվում է dweb3.wtf ինքնավար ռենդերինգ դարպասի ճարտարագիտական վերլուծությունը, որը մշակվել է Web3Compass ենթակառուցվածքի շրջանակում: Համակարգն անմիջականորեն աշխատում է ENS, Unstoppable Domains և այլ ապակենտրոնացված անվանման համակարգերի հետ, ինքնուրույն լուծում է կոնտենտի հեշը և, մատուցում է IPFS-ում տեղակայված կայքերը՝ առանց երրորդ կողմի API-ների: Վերլուծվում են ճարտարապետությունը, իրականացումը և արդյունավետությունը գրաքննության դիմադրության տեսանկյունից:

Առանցքային բառեր. Web3, ապակենտրոնացված վեբ, գրաքննության դիմադրություն, IPFS, ENS, մատուցման դարպաս, ինքնավար ենթակառուցվածք:

А.Ш. АРУТЮНЯН

УСТОЙЧИВОСТЬ К ЦЕНЗУРЕ В СЛОЯХ ДОСТУПА WEB3: ИНЖЕНЕРНЫЙ ВЗГЛЯД НА НЕЗАВИСИМЫЕ ШЛЮЗЫ ОТОБРАЖЕНИЙ

Устойчивость к цензуре — одна из главных ценностей Web3, однако реальный доступ к децентрализованным сайтам по-прежнему зависит от централизованных шлюзов (ipfs.io, .link, .limo). В статье исследуются технические барьеры настоящей цензуроустойчивости и представлен инженерный анализ автономного шлюза рендеринга dweb3.wtf, разработанного в инфраструктуре Web3Compass. Система напрямую взаимодействует с ENS, Unstoppable Domains и другими децентрализованными системами имён, самостоятельно разрешает контент-хэши через он-чейн резолверы и отображает IPFS-сайты через собственные узлы, исключив зависимость от сторонних API. Рассматриваются архитектура, реализация и характеристики с точки зрения устойчивости к цензуре.

Ключевые слова: Web3, децентрализованная паутина, устойчивость к цензуре, IPFS, ENS, шлюз рендеринга, автономная инфраструктура.