DWeb Server: The One-Click Censorship-Resistant Publishing Platform

"Publish anonymously. Index persistently. Distribute widely. Discover reliably."

The Problem: Truth Under Siege

The infrastructure of free speech is under coordinated attack:

- **40+ lawsuits** against Internet Archive by media companies
- **October 2024**: Internet Archive hacked 2 weeks before US election
- **Rising censorship**: UK mandates, Russian DNS blocking, China's Great Firewall expansions
- **Cloudflare's gatekeeper model**: Charging to access websites
- **Whistleblowers silenced**: No safe way to publish without revealing identity

The need is urgent. Freedom of the Press Foundation's response: *"We need this!"*

The Solution: Nine Years in the Making

DWeb Server is the first platform to unify all five pillars from the historic **2016 DWeb Summit** into a single product:

1. **OIP (Decentralized Library of Alexandria)** - Blockchain metadata + BitTorrent (Tim Berners-Lee called it "thrilling")
2. **IPFS** - Content-addressed permanent storage
3. **WebTorrent** - Browser-compatible peer-to-peer streaming
4. **GUN** - Encrypted real-time database synchronization
5. **DIDs (Decentralized Identifiers)** - W3C standard for self-sovereign identity

Plus modern additions: Tor anonymity, WordPress authoring, AI-powered search, decentralized DNS.

Result: Zero central points of failure. No single entity that can shut it down.

What Makes It Revolutionary

🎭 True Anonymity

- Tor onion routing hides publisher IP addresses
- No email, no personal information, just a 12-word recovery phrase
- Create-but-don't-send: Sign offline, submit from different network

🏠 One-Click Home Deployment

- Flash Raspberry Pi image → boot → publish in 10 minutes
- Docker Compose for power users
- $35-200 one-time cost, **$0/month** ongoing

📝 WordPress Authoring

- Familiar interface journalists already know
- Local cryptographic signing
- Export signed packages for courier delivery across borders

🔍 Gateway-Scoped Moderation

- Each operator decides what to index
- Content rejected by one gateway appears on others
- No global censorship authority

🧠 Local AI Assistant (Alfred)

- On-device question answering
- No cloud dependencies, complete privacy
- Voice interface for accessibility

🌐 Decentralized Name Resolution

- ENS for mainstream reach (fast)
- GNS for private lookups (no query leakage)

- Human-readable names without ICANN control

💎 Persistent & Discoverable

- Records survive even when publishers go offline
- Multiple gateways replicate the index
- Content distributed via peer-to-peer networks
- End-to-end cryptographic verification

How It Works (Simple Version)

```
1. AUTHOR: Write in WordPress (familiar tool)
   ↓
2. SIGN: Generate DID signature (anonymous identity)
   ↓
3. SUBMIT: Send via Tor onion (hides your IP)
   ↓
4. INDEX: Gateway adds to searchable database
   ↓
5. DISTRIBUTE: Content seeded on BitTorrent/IPFS
   ↓
6. PERSIST: Metadata stored on blockchain (permanent)
   ↓
7. DISCOVER: Anyone can search across gateways
   ↓
8. VERIFY: Readers confirm authenticity via signatures
```

Key Innovation: If the gateway goes down, if the publisher disappears, if a government tries to censor—the content persists. It's already on the blockchain, already seeded on peer networks, already replicated across multiple gateways.

Two Deployment Models: Choose Your Trade-Off

🏰 Model 1: Self-Hosted (Maximum Control)

For: Whistleblowers, high-stakes publishers, privacy advocates

Setup: Flash Pi image, generate DID, publish

Benefits:

- ✅ Zero registration
- ✅ Your keys never leave your device
- ✅ You control moderation

Cost: $35-200 hardware, technical setup

☁️ Model 2: Gateway Registration (Maximum Convenience)

For: Journalists, researchers, first-time users

Setup: Visit gateway, username + password (no email), publish

Benefits:

- ✅ No hardware needed
- ✅ Multi-device access
- ✅ Instant start

Cost: $0, trust gateway with encrypted keys

Critical: You can export your identity and migrate between models anytime. Not locked in.

Current Status: 80% Complete

✅ Already Built (OIP 0.8)

- Docker Compose deployment
- BitTorrent/WebTorrent/IPFS distribution
- Alfred AI with local LLM
- Advanced Elasticsearch search
- GUN encrypted synchronization
- Gateway moderation controls
- HD wallet authentication

🔄 Next 18 Weeks to 1.0

Phase	Timeline	Deliverables
Phase 1	3 weeks	DID identity system, create-but-don't-send
Phase 2	5 weeks	WordPress plugin, Tor integration
Phase 3	5 weeks	Name resolution (ENS + GNS)
Phase 4	5 weeks	Raspberry Pi image, Archive.org backups

Total: 4.5 months to production launch.

The Historical Moment

2016: The DWeb Summit

- Internet Archive convenes first Decentralized Web Summit
- Five foundational technologies discussed
- Vision: No single point of control

2016-2024: Evolution

- Technologies mature independently
- OIP proof-of-concepts by Caltech, Wyoming, Imogen Heap
- GUN enables encrypted peer-to-peer data
- IPFS and WebTorrent become production-ready
- DIDs evolve from concept (2016) → W3C Working Group (2019) → official W3C Recommendation standard (July 2022)

2025-2026: Convergence

DWeb Server is the first platform to integrate all five pillars into a unified product that Brewster Kahle envisioned:

> "Censorship resistant WebServer. Easy and fun, no monthly fee, open source, private, reliable. One-click downloadable software package to build your own webserver that protects writer privacy."

Technical Innovation: Location Agnostic

Key Principle: Adherence to W3C DID specification means index metadata can live anywhere.

Think of it like a library's card catalog: The cards tell you what books exist and how to find them, but the cards themselves can be stored in different places—wooden drawers, a digital database, or the cloud—while still pointing to the same books on the shelves.

The DID specification is like the Dewey Decimal Classification: Just as Dewey Decimal numbers tell you where to find a book on the shelf, DIDs tell you where to find content on the network. But because DIDs are built for decentralized networks, they're also **universal identifiers**—like having a Dewey Decimal number that works across every library in the world. A DID doesn't just locate content on one gateway; it uniquely identifies that exact record across *any* gateway, anywhere.

DWeb Server's index works the same way:

- Currently uses Arweave for persistent index storage (the "card catalog")
- DIDs (the "Dewey Decimal system") provide universal identifiers that work across all gateways
- Could switch to Bitcoin, Ethereum, or any other chain without changing what the index points to
- The actual content lives on peer networks (BitTorrent, IPFS)—the "books on the shelves"
- Same DID works on every gateway—universal identification across the entire network
- Application layer remains identical regardless of where the index is stored
- True portability and resilience

Not locked to blockchain hype—built on open standards.

Comparison: What Exists vs. What We Built

Feature	DWeb Server	Medium/Substack	SecureDrop	ZeroNet
Anonymity	Tor built-in	Email required	Tor (complex)	Tor optional
Authoring	WordPress	Web editor	N/A	HTML editing
Persistence	Blockchain + P2P	Centralized	Temporary	DHT only
Setup	10 minutes	Instant	Days (IT staff)	Complex
Cost	$0/month	$0-50/month	$500+ setup	$0/month
Moderation	Gateway-scoped	Platform-wide	N/A	None
Discovery	Full-text search	Platform	N/A	Hard
Status	Production	Active	Active	Inactive

The gap: Nothing combines WordPress ease + Tor anonymity + blockchain permanence + peer distribution.

Use Cases: Real People, Real Impact

📰 Independent Journalist

Investigative reporter covering corporate corruption

Problem: SLAPP lawsuits, platform takedowns, loss of hosting

Solution: Publish via WordPress + Tor → indexed permanently → content survives legal pressure

---

🔬 Academic Researcher

University scientist with findings threatening pharmaceutical industry

Problem: University pressure, funding threats, suppression of data

Solution: Publish datasets with cryptographic signatures → provenance verified → cannot be disappeared

---

🕵️ Whistleblower

Government analyst with evidence of wrongdoing

Problem: Network surveillance, retaliation, identification

Solution: Air-gapped signing → courier carries USB → submitted from coffee shop → complete anonymity

---

🏛️ Archivist/Historian

Researcher studying suppressed information

Problem: Content disappearing before it can be studied

Solution: Search across multiple gateways → verify authenticity → content persists even if original publishers offline

---

Why This Succeeds Where Others Failed

1. Familiar Tools

WordPress, not command-line interfaces. Writers use tools they already know.

2. True Anonymity

Tor built-in, not bolted-on. Publishers' IPs never exposed.

3. One-Click Deploy

Raspberry Pi image, not complex server configuration. Non-technical users can run nodes.

4. Economic Sustainability

$0/month, not subscription fees. Self-hosted on home networks.

5. Gateway-Scoped Moderation

Operators have control, not a free-for-all. Legal safe harbors maintained.

6. Proven Foundation

9 years of evolution, not vaporware. Tim Berners-Lee endorsement. Production deployments.

7. Standards-Based

W3C DID spec, not proprietary lock-in. True interoperability and portability.

The Market Opportunity

Immediate Adopters

- **Investigative journalism** organizations (FPF, EFF, ProPublica)
- **Whistleblower platforms** (beyond SecureDrop's submission model)
- **Academic researchers** in controversial fields
- **Human rights activists** in authoritarian regimes
- **Independent media** seeking censorship resistance

Broader Market

- **Privacy advocates** (existing community of 100K+)
- **Decentralized web enthusiasts** (DWeb Summit community)
- **WordPress users** (43% of all websites—465+ million sites)
- **Alternative media** (WeAreChange, TimCast already using OIP 0.8)

Network Effects

Each gateway operator increases resilience. Each publisher increases content value. Each reader increases discovery value.

Goal: 100 gateways, 1,000 publishers, 10,000 records by end of year 1.

Risk Management: We've Thought This Through

Risk	Mitigation
Timing attacks	Batched submission with randomized delays
Operator liability	Gateway-scoped moderation + legal safe harbors
Storage exhaustion	Size caps, rate limits, peer distribution
Spam/abuse	Hash denylists, tag policies, reputation systems
Key loss	12-word mnemonic backup, rotation support
Blockchain failure	DID spec abstraction = portable to any chain
Tor blocking	Create-but-don't-send, I2P alternative (future)
Low adoption	WordPress integration, one-click deploy, historical credibility

Philosophy: Build for resilience, not perfection. Multiple fallbacks at every layer.

The Team & Credibility

Historical Track Record

- **2016**: DLOA presented at first DWeb Summit
- **2016**: Tim Berners-Lee endorsement ("thrilling")
- **2016-2024**: Deployments for Caltech, Wyoming counties, Imogen Heap
- **2024**: Production use by WeAreChange.org and TimCast.com

Community Support

- **Internet Archive**: Brewster Kahle's direct involvement and vision
- **Freedom of the Press Foundation**: "We need this!"
- **DWeb Summit community**: 9 years of collaboration

Open Source

- Entire codebase open source
- Forks cannot be prevented
- Community-driven development

- No single point of organizational control

Call to Action: The Window Is Now

For Stakeholders

This is the moment. Censorship is accelerating. Attacks on Internet Archive demonstrate vulnerability. Journalists need this yesterday.

We're asking for:

- **Partnership** with Internet Archive, FPF, EFF
- **Testing** by friendly journalists and activists (Phase 2 beta)
- **Funding** for security audit and Raspberry Pi production
- **Community building** for gateway operator network

For Developers

- **Week 3**: OIP 0.9 DID system ready for review
- **Week 8**: WordPress plugin beta testing
- **Week 13**: Raspberry Pi image alpha
- **Week 18**: Production 1.0 launch

Join us: github.com/DevonJames/oip-arweave-indexer

For Gateway Operators

- **Be part of infrastructure** that makes censorship impossible
- **Run from home** on a $35 Raspberry Pi
- **Control your moderation** policies
- **Support free speech** without unlimited liability

The Vision: Unstoppable Publishing

Imagine a world where:

- **Whistleblowers** can expose wrongdoing without fear

- **Journalists** publish stories that survive legal pressure
- **Researchers** share findings that challenge power
- **Activists** organize without surveillance
- **Information** persists beyond any entity's control

This isn't future technology. 80% is already built. 4.5 months to production.

The five pillars from the 2016 DWeb Summit—OIP/DLOA, IPFS, WebTorrent, GUN, and DIDs—unified for the first time.

WordPress authoring. Tor anonymity. Blockchain permanence. Peer distribution. Decentralized DNS. Local AI. Gateway-scoped moderation.

Zero central points of failure. No monthly fees. One-click deploy.

Contact & Next Steps

Project Lead: amy@alexandria.io
Repository: github.com/DevonJames/oip-arweave-indexer
Version: 2.4 (November 6, 2025)
Status: 80% complete, 18 weeks to 1.0

Immediate Opportunities:

1. **Review full PRD** (comprehensive technical specification available)
2. **Join Phase 1 testing** (OIP 0.9 DID system - 3 weeks)
3. **Beta WordPress plugin** (journalists needed for Phase 2)
4. **Run test gateway** (Raspberry Pi image in Phase 4)
5. **Become stakeholder** (Internet Archive, FPF, EFF partnership)

The choice is simple:

- Continue with platforms that can be censored, shut down, pressured
- Or build infrastructure that makes censorship impossible

We choose the latter. Join us.

"The best way to predict the future is to build it."
— DWeb Summit, 2016

"Censorship resistant WebServer. Easy and fun, no monthly fee, open source, private, reliable."
— Brewster Kahle, 2024

DWeb Server: Where the vision becomes reality.