DCDN Cloud — Whitepaper v2.0

Decentralized Content Delivery, Security & Cloud Computing

March 2026

1. Abstract

DCDN Cloud is a decentralized cloud infrastructure platform that replaces centralized CDN, WAF, DNS, and computing providers with a network of independent node operators. Node operators contribute server resources and earn DCDN tokens for delivering content, processing requests, and blocking threats. The platform uses GeoIP-based smart routing, container sandboxing with gVisor, and a mathematically-proven anti-gaming mechanism to ensure fair reward distribution and network integrity.

2. Problem

Current cloud infrastructure suffers from:

- **Centralization risk** — a single provider controls availability, pricing, and data
- **Vendor lock-in** — migration between CDN providers is complex and risky
- **Opaque pricing** — bandwidth overages, hidden fees, enterprise-only features
- **No operator incentives** — server infrastructure is a cost center, not a revenue opportunity
- **Single point of censorship** — one entity can deplatform any customer

3. Solution

DCDN Cloud creates a decentralized alternative where:

- **Anyone can run a node** and earn tokens for contributing resources
- **No single entity controls** the network — nodes are independently operated
- **Smart routing** sends users to the nearest node via GeoIP DNS
- **Security is sandboxed** — customer workloads run in gVisor containers with seccomp profiles

- **Revenue is shared** — 70% to node operators, 25% to RSP token holders, 5% to treasury

---

4. Architecture

4.1 Network Topology

```
User Request → CoreDNS (GeoIP) → Nearest Edge Node → Cache Hit? → Serve
                                                    → Cache Miss → Origin Fetch → Cache + Serve
```

- **CoreDNS with GeoIP** — resolves domain to nearest node's IP based on client continent
- **Edge Nodes** — nginx with local static content, reverse proxy to coordinator for API calls
- **Coordinator** — central API server for configuration, billing, node management
- **WireGuard Mesh** — encrypted inter-node communication for cert sync, verifier, management

4.2 Node Architecture

Each node runs:

Component	Purpose
dcdn-node (Rust binary)	CDN proxy, caching, WAF, SSL termination
nginx	HTTPS edge with HTTP/3, Brotli, TLS 1.3
gVisor	Container sandbox runtime
seccomp	Syscall filtering for containers
WireGuard	Encrypted management tunnel
Agent	Heartbeat, task execution, graceful shutdown

4.3 Security Layers

1. **Network** — UFW firewall, only ports 80/443 exposed, management via WireGuard only
2. **Container** — gVisor runtime + seccomp profile, no host access, no Docker socket mount
3. **Network Policy** — iptables rules block container → host/metadata/other-networks
4. **Agent Auth** — HMAC challenge-response + Fernet encrypted transit + TLS cert pinning
5. **Remote Verifier** — coordinator independently audits node integrity via SSH
6. **Reputation System** — automatic scoring (0-100), auto-suspend below 20

---

5. DCDN Token

5.1 Token Details

Property	Value
Name	DCDN Token
Contract	`0x9547b7C5c4FDBfc375473037a6699b2Ec2e55729`
Standard	ERC-20
Chains	Ethereum, Polygon, BNB Chain, Base, Arbitrum, Cronos, Hyperliquid

5.2 Token Generation

DCDN tokens are **only minted when a customer pays for services**. There is no pre-mine, no inflation schedule, no arbitrary minting. The token supply directly equals the platform's real revenue.

```
Customer pays $100 for CDN service
  → $100 worth of DCDN tokens minted
  → 70% ($70) → Node operators (proportional to work done)
  → 25% ($25) → RSP Revenue Sharing Protocol (distributed to DCDN holders)
  → 5%  ($5)  → Treasury (development, operations)
```

5.3 Node Operator Rewards

Node operators earn fixed DCDN token amounts for work performed:

Activity	Reward
Bandwidth delivered	**1 DCDN per GB**
Requests served	**0.5 DCDN per 10,000 requests**
Threats blocked (WAF)	**1 DCDN per 10,000 inspections**

Rewards are in **fixed token amounts** — not pegged to USD. The USD value of rewards depends on the market price of DCDN on decentralized exchanges.

5.4 Price Floor Mechanism

A protocol-operated bot maintains a $0.02 buy floor on Uniswap V2: - Always places buy orders at $0.02 for DCDN/USDC - Funded from treasury's USDC reserves - Maximum $50 per trade, $500 daily limit - Ensures node operators can always sell at minimum break-even price

---

6. Node ID System

Every node receives a system-generated identifier:

```
Format: DCDN-{REGION}-{4hex}
Example: DCDN-EU-309a, DCDN-US-e901, DCDN-SA-a2db
```

- **Region** — auto-detected from server IP via GeoIP (EU/US/SA/AS/OC/AF)
- **ID** — random 4-character hex suffix, guaranteed unique
- **Operators cannot choose** their node ID — prevents impersonation
- **1 IP = 1 node** — prevents sybil attacks

---

7. Anti-Gaming Mechanism

7.1 The Attack Vector

A malicious node operator could generate fake WAF “threats” against their own node to earn extra DCDN tokens. The cost of generating fake traffic (botnet) vs. the reward must always be unfavorable.

7.2 Threat Reward Distribution

When a node’s WAF activity exceeds a dynamic threshold, the reward is automatically distributed across multiple nodes:

```
Normal:  1 node handles threats → 1 node gets reward
Spike:   threshold exceeded → other nodes join defense → reward splits equally
```

7.3 The Continuous Threshold Formula

```
threshold = 1 + (botnet_cost / (avg_threats / 10000 × token_price)) × 0.95
```

Where: - `botnet_cost` = estimated minimum botnet cost per day ($0.50) - `avg_threats` = network average threats per node (rolling) - `token_price` = current DCDN market price from DEX - `0.95` = 5% safety margin

Properties: - Attacker profit is **mathematically guaranteed negative** at any token price - At $0.01: threshold = 45x (permissive — no incentive to attack) - At $1.00: threshold = 1.44x (tight) - At $100: threshold = 1.004x (very tight) - At $1000: threshold = 1.0004x (near-zero margin) - **Scales automatically to infinity** — zero maintenance required

7.4 Helper Node Selection

When distribution activates: 1. Same-owner nodes are **excluded** (extra layer, not primary defense) 2. Nodes from **different regions** get priority (geographic diversity) 3. Higher **reputation** nodes selected first (trusted operators benefit)

7.5 Anomaly Detection

When a node's threats exceed 3× the distribution threshold, an admin alert fires via Telegram. This does not trigger automatic punishment — it flags for human review.

7.6 Why It Works

The defense is **mathematical, not identity-based**: - An attacker running 1 node or 100 nodes with different identities faces the same math - The formula ensures `total_reward × price < attack_cost` regardless of who receives the reward - No proof of identity needed, no punishment for false positives - The system simply makes attacks economically irrational

---

8. Reputation System

Score	Status	Effect
80-100	Healthy	Full rewards, priority for helper selection
50-79	Warning	Full rewards, monitored
20-49	Degraded	Admin alert, under review
0-19	Auto-suspended	No new workloads, manual review required

Positive events: Successful heartbeat, passed audit, uptime streak **Negative events:** Missed heartbeat, failed challenge, integrity mismatch, security violation

---

9. Graceful Shutdown Protocol

Node operators can stop their node without penalty:

```
Operator stops node → Agent sends SIGTERM → POST /agent/shutdown → status = "offline"
```

- **Planned shutdown** → no reputation impact, no alert
- **Unexpected crash** → 5 minutes without heartbeat → alert + reputation impact

10. Platform Services

Service	Description
CDN	Global content caching with configurable TTL, purge API
WAF	AI-powered SQLi/XSS detection, DDoS protection, bot management
DNS	Full DNS hosting with GeoIP smart routing
SSL/TLS	Free wildcard certificates, auto-renewal, HTTP/3 support
Edge Functions	Node.js/Python/Deno execution in sandboxed containers
Cloud Compute (VPS)	Docker-based instances with full lifecycle management
Image CDN	Auto WebP/AVIF conversion, resize, crop on-the-fly
Uptime Monitoring	Multi-region HTTP/HTTPS/TCP checks with alerting
Email Routing	Forwarding with custom aliases
AI Agents	Hosted AI assistants with persistent memory and skills

11. Revenue Model

Plan	Price	Target
Free	$0	Trial
Standard	$5/mo	Personal sites
Pro	$15/mo	Growing projects
Business	$59/mo	Teams & agencies
Enterprise	Custom	Large organizations

Additional revenue: VPS add-ons ($3-60/mo), bandwidth overage, premium AI tokens.

12. Smart Contracts

Contract	Address	Purpose
DCDNToken	`0x9547b7C5c4FDBfc375473037a6699b2Ec2e55729`	ERC-20 token

Contract	Address	Purpose
NodeRewardPool	`0x98d525395b856FDAbA5ef363a4CE47c75BEE256A`	Merkle-based reward claims
RevenueConnector	`0xdf8a37f8a590981695BdBf248A233623f9e7df76`	RSP revenue sharing (immutable)
BillingEngine	`0xb4C73De90cAC6b54413D0DD512f980D892614c21`	Auto-conversion on payment

---

13. Roadmap

Phase	Status
Core CDN + WAF + DNS	✅ Live
Node operator rewards	✅ Live
GeoIP smart routing	✅ Live
Anti-gaming mechanism	✅ Live
Container sandboxing (gVisor)	✅ Live
Node Admin panel	✅ Live
One-liner node installer	✅ Live
Etherscan contract verify	🔜 This week
Uniswap pool + floor bot	🔜 This week
CoinGecko / CMC listing	🔜 Q2 2026
Multi-chain node support	📋 Planned
Governance voting	📋 Planned

---

14. Conclusion

DCDN Cloud replaces centralized cloud infrastructure with a decentralized network where: - Node operators earn tokens proportional to their contribution - The anti-gaming formula makes attacks mathematically unprofitable at any scale - Security is enforced through sandboxing, not trust - Token supply is backed by real revenue, not speculation - The system scales and adapts automatically without manual intervention

DCDN Cloud — Decentralized infrastructure for the open internet.

Website: dcdncloud.com | Token: Etherscan | Revenue Sharing: rsp.cash