🌟 371 OS

Revolutionary Autonomous Agent Operating System

MIT License | Node.js 18+ | Built with Nx | Powered by ElizaOS | Deployed on Akash

Beyond MCP Limitations: The next evolution in AI agent coordination through blockchain-based Universal Tool Servers, achieving **97.6% cost reduction** and true agent autonomy.

📖 371 OS README v2.0

🌟 Core Innovations

- **Universal Tool Server Architecture:** Stateless, blockchain-based agent coordination beyond MCP limitations
- **Self-Aware Agents:** ElizaOS-powered agents that understand and manipulate their own workspace
- **97.6% Cost Reduction:** Through Akash Network decentralized infrastructure
- **Blockchain Registry:** Decentralized agent discovery with cryptographic trust (Ethereum + IPFS)
- **Enterprise Security:** Zero-trust integration with Secretless Broker and ACI.dev

🏗️ Agent Ecosystem

CEO Agent (Mimi) ──┬── Strategic Decision Making ├── Cost Optimization (97.6% reduction) └── Resource Allocation CTO Agent (Zara) ──┬── Technical Architecture ├── Plugin Development └── System Design CFO Agent (Maya) ──┬── Financial Analysis ├── Budget Optimization └── ROI Calculations CLO Agent (Alex) ──┬── Legal Compliance ├── Governance Frameworks └── Regulatory Oversight

🚀 Revolutionary Technology Stack

Nx Workspace
Monorepo with affected analysis for 40x efficiency gains

ElizaOS + Qoder
Self-aware agent capabilities with workspace manipulation

Ethereum Smart Contracts
Decentralized agent registry and coordination

IPFS Storage
Distributed metadata for agent capabilities

Akash Network
97.6% cost reduction through decentralized infrastructure

Enterprise Security
Secretless Broker + ACI.dev integration

🔗 Quick Links

Getting Started Guide | Milestone Report | Source Code

📋 Executive Brief: AI-Augmented System Architect

The Category We Own

AI-Augmented System Architect (AASA): An enterprise architect for the agentic era—designing cognition-augmented systems that are safe by design, governed end-to-end, zero-trust native, and production-grade from day one.

Tagline: Autonomy with guardrails. Outcomes with evidence.

🎯 Market Signals

- 78% of UK/I C-suite already using AI agents
- NIST AI RMF 1.0 + ISO/IEC 42001 codified governance
- Zero Trust + Secretless patterns mature
- Agentic patterns documented by AWS/IBM/Microsoft

💰 Revenue Targets

- Phase 1: Validate Pieces→Akash pipeline
- Phase 2: **$50k MRR target**
- KPI: 80% workflows agent-first
- Cost advantage: 97.6% via Akash

🏛️ Signature Frameworks

AZTA: Agentic Zero-Trust Architecture
Maps agent loops to ZTA components (PE/PA/PEP), app-layer identity, Secretless pattern

CAER: Cognition-Augmented Enterprise Reference
Bridges event-driven to agentic workflows with LLM planners, routers, tool callers

AIMS-Ops: ISO/IEC 42001 + NIST AI RMF
Operating model fusing AI management standards with lifecycle governance

CharacterOps: Persistent Agent Personas
Venice.ai Characters as durable business personas with privacy controls

🔒 Non-Negotiable Guardrails

Zero Trust
NIST 800-207/207A

Secretless
No creds in app code

Standards
ISO 42001 + AI RMF

📊 10-Slide Strategic Deck

The AI-Augmented System Architect

Cognition-Augmented Systems with Enterprise Guardrails

🧠 Local-First Cognition → 🔗 Universal Tool Servers → ⛓️ Decentralized Runtime

Beyond MCP: Universal Tool Server Architecture

Traditional MCP Limitations

- Tight coupling between agents and tools
- Local context assumptions
- No decentralized discovery
- Limited trust mechanisms

UTS Innovation

- Stateless, blockchain coordination
- Ethereum registry + IPFS metadata
- Cryptographic trust
- Tool reuse without coupling

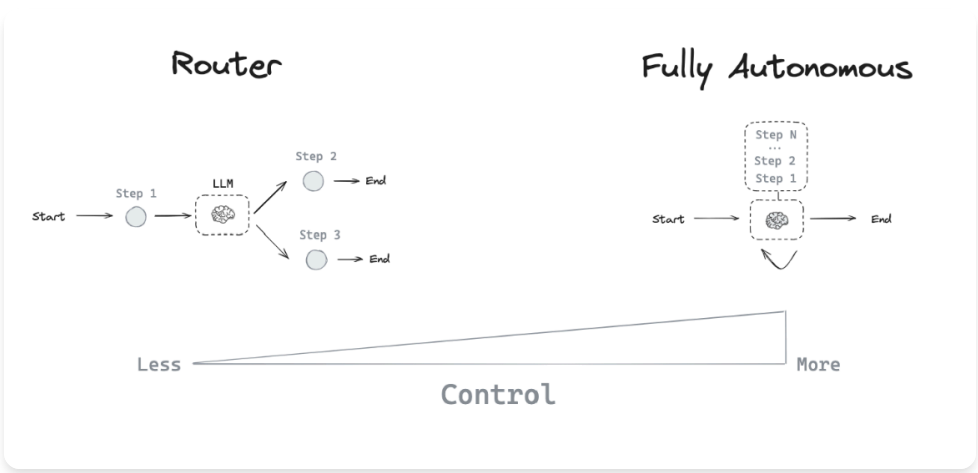


Figure: Agent Architecture Patterns (Source: LangGraph)

371 OS Core Architecture

Cognition Layer

Pieces as local-first memory cortex, capturing workflow patterns for hyper-personalized agents

Orchestration

Nx monorepo + Qoder "Agent Factory" + ElizaOS self-aware plugins + MCP coordination

Infrastructure

Akash Network exclusive deployment (97.6% cost reduction) + Status/DAO governance

Multi-Agent Orchestration Patterns

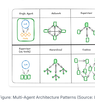


Figure: Multi-Agent Architecture Patterns (Source: LangGraph)

Collaboration
Shared scratchpad, router-based transitions

Supervisor
Central coordinator, independent agent scratchpads

Hierarchical
Supervisor of supervisors, nested teams

Zero Trust + Secretless Security

NIST 800-207 ZTA Tenets

- Per-session least-privilege access
- Dynamic policy (identity + asset state)
- Encrypted/authenticated comms everywhere
- Continuous telemetry collection
- Policy Engine/Administrator/Enforcement Points

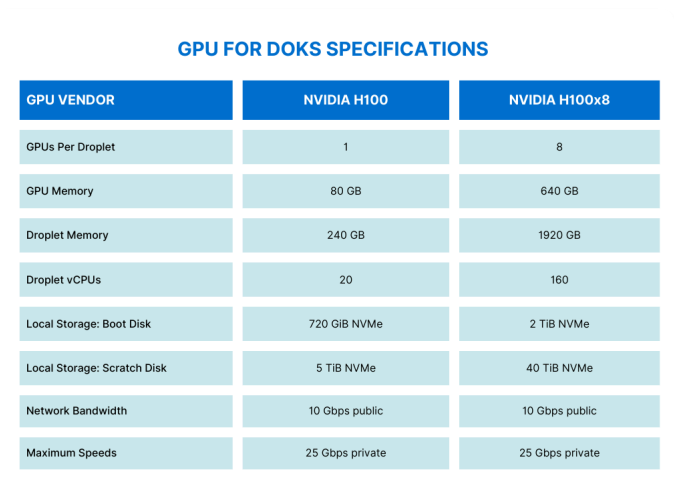
Secretless Pattern

- Agents never touch credentials
- Transparent rotations
- Sidecar/local proxy pattern
- K8s-friendly deployment

Architecture Flow

Agent Request → Policy Engine Decision ↓ Policy Admin Configures Path ↓ Secretless Broker Injects Creds ↓ Policy Enforcement Point Allows ↓ Tool Execution (with audit trail)

GPU Infrastructure: Bridge to Decentralization



GPU FOR DOKS SPECIFICATIONS

GPU VENDOR	NVIDIA H100	NVIDIA H100x8
GPUs Per Droplet	1	8
GPU Memory	80 GB	640 GB
Droplet Memory	240 GB	1920 GB
Droplet vCPUs	20	160
Local Storage: Boot Disk	720 GiB NVMe	2 TiB NVMe
Local Storage: Scratch Disk	5 TiB NVMe	40 TiB NVMe
Network Bandwidth	10 Gbps public	10 Gbps public
Maximum Speeds	25 Gbps private	25 Gbps private

Figure: DigitalOcean Kubernetes GPU Options (Source: DigitalOcean)

Current: DO K8s GPU Nodes

- AMD MI300X/325X + NVIDIA H100
- Single vs 8x configurations
- Training, inference, distributed workloads
- Familiar enterprise bridge

Target: Akash Exclusive

- Decentralized, censorship-resistant
- 97.6% cost reduction demonstrated
- Permissionless deployment
- Staged migration with identical guardrails

Governance: ISO/IEC 42001 + NIST AI RMF

ISO/IEC 42001 AIMS

World's first AI Management System standard

- Policies, objectives, PDCA cycle
- AI lifecycle governance
- Risk/opportunity management
- Continuous improvement

NIST AI RMF Functions

- **GOVERN**: Culture, policies, accountability
- **MAP**: Context, risks, system categorization
- **MEASURE**: Metrics, TEVV processes
- **MANAGE**: Response, resource allocation

12 GAI Risk Categories

Confabulation	Info Integrity
Data Privacy	Info Security
Harmful Bias	IP Violations
Human-AI Config	Value Chain
Environmental	CBRN Info
Violent Content	Abusive Content

Each risk mapped to concrete controls in agent patterns

The Augmented Architect Role

Figure: The Augmented Architect (Source: Forrester)

Curator
Architecture graph maintenance, pattern libraries, anti-pattern detection

Facilitator
Cross-team coordination, stakeholder alignment, decision acceleration

Critical Thinker
AI guides but doesn't dictate, guardrail design, feedback loop optimization

CharacterOps: Persistent Agent Personas

Figure: Ventus.ai Characters Interface

Private by Design

- Conversations stay in local browser
- Uncensored, consistent personalities
- Web-enable selectively
- Context files for deep knowledge

Business Applications

- C-Suite agents (CEO, CTO, CFO, CLO)
- Department heads with domain expertise
- Brand voice consistency
- Regulatory compliance personas

Roadmap & Success Metrics

🎯 Phase Targets

Phase 1 (Weeks 1-4)
Validate Pieces + Akash pipeline
Launch monetizable product

Phase 2 Target
$50k MRR

📊 *Key Metrics*

Autonomy KPI
≥80% workflows agent-first

Cost Advantage
97.6% Reduction
via Akash Network

🚀 Ready to Ship

Local-first cognition • Universal Tool Servers • Zero Trust • Autonomous economics

🌟 371 OS

Revolutionary Autonomous Agent Operating System

Beyond MCP • 97.6% Cost Reduction • True Agent Autonomy

🔗 Resources

- Source Code
- Getting Started
- Milestones

📚 Standards & Citations

- NIST AI RMF 1.0 & GAI Profile
- ISO/IEC 42001 (AIMS)
- NIST 800-207 (Zero Trust)
- CyberArk Secretless
- AWS Agentic Patterns
- LangGraph Multi-Agent