MCP SERVER | NO CODE | CLOUD HOSTED

Blockdaemon Blockchain Infrastructure MCP for AI Agents

Cross-chain blockchain data retrieval for auditing and development

Blockdaemon Blockchain Infrastructure MCP gives your AI agents unified access to institutional-grade data across major blockchain protocols, including Bitcoin, Ethereum, and Solana. Track transaction histories, get Unspent Transaction Outputs, list block metadata, or generate detailed financial reports—all from one place.

A+ Quality Score 100/100

web3 | bitcoin | ethereum | blockchain-data | crypto-api

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/blockdaemon-blockchain-infrastructure

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Blockdaemon (Blockchain Infrastructure) MCP

4 tools available
Cloud-hosted on Vinkius

Manually checking multiple blockchains for the same piece of information is a nightmare. You jump between developer consoles, run different API calls, and spend hours trying to correlate data points across Bitcoin, Ethereum, and Algorand just to get a full picture of an address's activity. This MCP changes that. It connects your AI agent directly to Blockdaemon's Ubiquity API, giving you one unified pane for all multi-chain data.

Whether you need to verify the latest block details or track complex transaction flows across different protocols, this connector handles it. You can use it to list recent blocks, query a full history of transactions, calculate UTXO sets specific to certain chains, and even run comprehensive financial reports on addresses from varied ecosystems like Algorand or Stellar.

By connecting your agent through Vinkius, you get access to all this specialized crypto data without writing custom wrappers for every single chain. Just ask your AI client what you need, and it handles the complexity of retrieving accurate, structured blockchain records.

Core Capabilities

01 — Retrieve Block Metadata

You can get a list of block identifiers and associated metadata for major protocols like Bitcoin, Ethereum, Solana, and Polkadot.

02 — Track Full Transaction Histories

Query the complete transaction history for any specified account address across all supported networks.

03 — Manage UTXO Sets

Fetch Unspent Transaction Outputs (UTXOs), which is crucial data for managing assets on specific chains like Bitcoin and Litecoin.

04 — Generate Financial Reports

Produce detailed financial reports, including total balance and earned rewards, for addresses on protocols such as Algorand, Stellar, or Tezos.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/blockdaemon-blockchain-infrastructure** — connect your AI agent in three steps.

01 Subscribe to this MCP and provide your specific Blockdaemon API Key.

02 Your AI client connects using the key, establishing a direct link to the multi-chain data streams.

03 You instruct your agent on what data you need (e.g., 'Show me all transactions for this address'), and it executes the necessary queries.

The bottom line is, you tell your AI client what blockchain data you want, and it handles the connection and retrieval of accurate information from multiple protocols.

Built For

This MCP is built for professionals who deal with multi-chain assets or require high-detail financial auditing. It helps developers debug complex smart contracts and allows data analysts to correlate records across disparate blockchain ecosystems without switching tools.

Web3 Developer

Debugging transaction flow, verifying block headers, and writing code that interacts with multiple live mainnet environments.

Crypto Data Analyst

Aggregating financial reports and historical transaction data across different chains for cross-platform auditing or research papers.

Treasury Operations Manager

Monitoring wallet activity, checking UTXO sets, and confirming asset movements before large capital transfers.

What Changes When You Connect

01 Analyze transaction history quickly. Instead of running separate queries, your agent handles fetching the full list of transactions using `list_transactions` across multiple chains.

02 Confirm asset status instantly. Quickly check Unspent Transaction Outputs (UTXOs) for assets on UTXO-based chains with `get_utxos`, saving time on manual wallet checks.

03 Audit financials easily. Generate comprehensive reports, including rewards and total balance, using `get_financial_report` for cross-chain comparisons.

04 Debug block data without leaving your IDE. Use the MCP to retrieve specific block identifiers and metadata with `list_blocks`, keeping your workflow in one place.

05 Maintain separation of environments. The MCP lets you switch between mainnet and testnet settings effortlessly, which is critical for safe development.

Real-World Applications

Investigating a suspected theft

A user needs to follow the money trail after an address is compromised. They ask their agent to fetch all transactions and then correlate those findings with block metadata using `list_transactions` and `list_blocks`. The agent returns a clear, chronological map of transfers across three different chains.

Pre-merger asset reconciliation

A data analyst needs to combine balance sheets from multiple protocols (Stellar, Algorand). They use the MCP's capability to run financial reports (`get_financial_report`) for every major address, getting a unified total value report without manual spreadsheet work.

Auditing dormant crypto wallets

A treasury manager needs to know if any old UTXOs still exist in a large corporate wallet. They use the MCP's function for fetching Unspent Transaction Outputs (`get_utxos`), immediately identifying assets that need to be re-monitored or swept.

Verifying smart contract deployment

A developer needs proof that a specific contract was deployed and recorded correctly. They ask the agent to list recent blocks using `list_blocks` for Ethereum, confirming the exact block height where the transaction occurred.

Patterns to Avoid

Mixing up UTXO data with account balances

✗ AVOID

Assuming that just because an address has a balance means it has unspent outputs. This leads to failed transactions and incorrect asset accounting.

✓ INSTEAD

Always confirm the available funds by running `get_utxos`. Don't rely only on general account balances when managing assets for specific chains.

Forgetting cross-chain data correlation

✗ AVOID

Running a financial report for an address on Algorand, then forgetting to check the same activity history on Tezos. You miss half the picture.

✓ INSTEAD

Use this MCP's ability to connect multiple protocols in one query. Ask your agent to generate reports or track transactions across specific chains simultaneously.

Ignoring mainnet vs testnet differences

✗ AVOID

Running a development script against the main network when you only meant to simulate on a test environment, wasting resources and getting live data.

✓ INSTEAD

Always verify the intended environment. The MCP lets you switch between mainnet and testnet seamlessly within your query.

The Right Fit

Use this MCP if your work involves analyzing assets or transactions across multiple distinct blockchain protocols, or if you need highly granular data like Unspent Transaction Outputs (UTXOs). This is essential for serious crypto auditing and development. Don't use it if you only need basic API calls against a single, isolated network endpoint; other general-purpose APIs might suffice. If your goal is simply to write code in the blockchain language itself without reading external data, then this MCP isn't what you need—you'd want an execution environment tool instead.

Blockdaemon Blockchain Infrastructure for Cross-Chain Transaction History Analysis

Today, checking a single wallet's history is tedious. You have to log into one service for Bitcoin data, another for Ethereum, and maybe a third for Algorand just to piece together what happened last week. This means copying addresses, running separate API calls, and spending hours cross-referencing spreadsheets.

With this MCP, you simply ask your agent for the full transaction history of an address across all relevant protocols. The output is unified: one coherent timeline showing every asset movement regardless of which chain it hit. You get immediate, consolidated clarity.

Blockdaemon Blockchain Infrastructure for Financial Reporting and UTXO Management

The manual process for treasury management involves running multiple checks: first, finding the current total balance; second, checking if there are any leftover Unspent Transaction Outputs (UTXOs); and finally, generating a report of earned rewards. These steps require complex scripting.

Now, you ask your agent to generate an account's financial report. It runs all those checks—total balance, UTXO status, and reward calculation—and hands you one clean document. The data is ready for action.

Blockdaemon Blockchain Infrastructure: 4 Tools for Crypto Data Auditing

These four tools allow your agent to retrieve specific blockchain data, including block lists, UTXOs, financial reports, and full transaction records.

#	TOOL	DESCRIPTION
01	`list_blocks`	Retrieves a list of identifiers for blocks on various blockchain networks.
02	`get_financial_report`	Generates a detailed financial report summarizing an address's total holdings and activity over a period.
03	`list_transactions`	Fetches a complete list of transaction records associated with a specific account address.
04	`get_utxos`	Determines the Unspent Transaction Outputs for an asset on UTXO-based blockchains.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U What were the last five transactions involving this Bitcoin address?

Bitcoin Transaction History

DATE	AMOUNT	TO ADDRESS	STATUS
2023-10-25	0.5 BTC	1A1zP1e...	Confirmed
2023-10-24	1.2 BTC	Change Address	Confirmed
2023-10-23	0.05 BTC	Exchange A	Confirmed

Note: The full transaction details are available upon request.

U Give me a financial snapshot for this Algorand address.

Financial Report (Algorand)

Period: Last 30 Days
Total Balance: 1,245.8 ADA
Rewards Earned: 35.1 ADA
Transaction Volume: 789.2 ETH-Equivalent Units

The report indicates steady activity with a significant reward spike in the last week.

U List the most recent block details for Ethereum mainnet.

Ethereum Block Details

- **Block Height:** 19283746
- **Timestamp:** 2026-06-12T14:30:00Z
- **Miner/Validator:** Node Operator X
- **Transaction Count:** 350
- **Gas Used:** 12,345,678

Frequently Asked Questions

01 **How can I check assets across Bitcoin and Ethereum using the Blockdaemon MCP for AI Agents?**

You can ask your agent to pull data from both chains simultaneously. The MCP handles the multi-protocol connection, allowing you to compare transaction histories or generate combined financial reports in one go.

02 **Does the Blockdaemon Blockchain Infrastructure MCP support testnet environments?**

Yes, it does. You can easily switch between mainnet and testnet protocols through the MCP's interface. This is crucial for development when you need to simulate transactions without risking real funds.

03 **Is this MCP better than just using a standard API key for my agent?**

Yes, because it unifies everything. Instead of needing separate code and keys for Bitcoin's UTXOs, Ethereum's blocks, and Algorand's reports, the MCP gives your AI agent one simple interface to access all that data.

04 **Can I track a wallet's full history using the Blockdaemon Blockchain Infrastructure MCP?**

Absolutely. You can query the complete list of transactions for any address across supported networks. The agent will provide a detailed, chronological record of every movement.

05 **What kind of data does the Blockdaemon Blockchain Infrastructure MCP use to generate reports?**

It gathers institutional-grade metadata directly from major blockchain protocols. This includes total balances, calculated rewards earned, and transaction volume figures for accurate auditing.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"blockdaemon-blockchain-infrastructure": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Blockdaemon (Blockchain Infrastructure) is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Blockdaemon (Blockchain Infrastructure). All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Blockdaemon (Blockchain Infrastructure) MCP
Server ID	`019e386d-f73a-70a7-af23-5a41394ae4df`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/blockdaemon-blockchain-infrastructure.