



**Cronos LLM**

• INVESTOR DECK · APRIL 2026 · CONFIDENTIAL

# The AI that audits Web3 before hackers do.

Cronos LLM is an autonomous, multi-model security intelligence platform for EVM smart contracts — audit-grade analysis in minutes, at 1/1000th the cost.

**\$6B+**

LOST TO HACKS (2022–2024)

**<3%**

CONTRACTS EVER AUDITED

**\$2.50**

COST PER CRONOS AUDIT

**4–8 min**

TIME TO FULL REPORT

## THE PROBLEM

# The audit market is fundamentally broken.

47% of all DeFi hacks exploit vulnerability classes existing tools already know about — but coverage does not scale.



**\$15,000 – \$150,000**

Cost of a single manual audit. Prohibitive for 97% of all deployed contracts.



**3 – 6 weeks**

Turnaround time for a traditional engagement. DeFi protocols launch in days.



**~400 auditors globally**

Qualified smart contract security researchers. Demand is 10x supply.



**Upgradeable contracts**

One-time audits are obsolete. Every proxy upgrade re-exposes the full attack surface.

*“The question is not if you will be hacked. It’s whether you knew before it happened.”*

THE SOLUTION

# Cronos LLM

Agentic, multi-model security intelligence. Full pentest in 4–8 minutes for \$2.50.

Developer submits contract address or source code

- ↓ Cronos fetches from blockchain · Etherscan V2 · Sourcify · proxy resolution
- ↓ Slither static analysis · 80+ detectors · auto solc version switching
- ↓ Mythril symbolic execution · mathematical proof of exploit paths · GPU-accelerated
- ↓ RAG knowledge base · 22 SWC entries · 8 DeFi hack post-mortems · ERC patterns
- ↓ Foundry / Anvil PoC · live exploit on mainnet fork · confirmed or refuted
- ↓ Claude Opus 4.6 generates professional audit report — severity, remediation, PDF



### Claude Opus 4.6

Premium audit reports · PoC reasoning · exploit generation

Highest reasoning



### Claude Sonnet 4.6

Agent orchestration · tool selection · high-volume screening

10x throughput



### Gemini 2.0 Pro Ultra

Training data synthesis · knowledge base enrichment · model teaching

1M token context



### Local LLM · RTX 4090

Codestral 22B / Llama 3.1 70B · pre-screening · zero API cost

\$0 marginal

# Hybrid cloud + local GPU cluster

Cloud handles availability. Local GPUs handle compute intensity — slashing marginal cost to near zero at scale.



## GPU Node #1

Mini PC · RTX 4090 · 24GB VRAM · Windows + WSL2. Mythril symbolic execution — 3x faster than cloud CPU.



## GPU Node #2

Mini PC · RTX 4090 · 24GB VRAM · Windows + WSL2. Foundry PoC farm — 2 parallel Anvil mainnet forks.



## Dev Laptop

16-core · 64GB RAM · Windows. Development pipeline · n8n local fallback · testing.



## Cloud: Hetzner CCX53

16 vCPU · 64GB RAM · NVMe SSD · \$250/month. pens-api · n8n · MongoDB · ChromaDB · Redis



## MCP-Native

Full MCP server · SSE transport · connects Claude Desktop, Cursor, n8n tool nodes instantly.

MARKET OPPORTUNITY

# \$890M market. 3% penetration.

The smart contract security market is underpenetrated, price-inelastic, and growing as TVL expands.

<b>\$890M</b> Annual audit market (2025)	<b>57M+</b> Active EVM contracts on mainnet	<b>14k</b> New contracts deployed daily
---	--	--

## Revenue model — Month 3 target

TIER	PRICE	VOLUME	MRR
On-demand audit	\$49 / contract	200 audits	\$9,800
Developer plan (unlimited)	\$199 / mo	30 subscribers	\$5,970
Enterprise API	\$999 / mo	5 clients	\$4,995
White-label (audit firms)	\$2,500 / mo	2 firms	\$5,000
<b>Month 3 MRR target</b>			<b>\$25,765</b>

## EXECUTION

# 3 weeks to launch. 3 months to revenue.

Hard KPI gates at every phase. No fluff milestones.

### WEEK 1

#### Infrastructure

- Flash Windows machines — CUDA, Docker Desktop, WSL2
- Deploy Hetzner cloud server, all containers healthy
- Smoke test: audit Uniswap V2, detect known vulnerabilities

### WEEK 2

#### Intelligence Layer

- n8n agent workflow live — Claude Opus + Sonnet wired
- Gemini Ultra pipeline: 500 synthetic audit training examples
- 10 real audits on known-vulnerable CTF contracts — validated

### WEEK 3

#### Launch

- Fine-tuning run #1: LoRA on Codestral with audit data
- Web audit submission portal live
- 5 beta testers: 3 DeFi protocols, 2 audit firms — public launch

### MONTH 1

#### Validation — KPI: 95% detection accuracy

- 50 audits against known-vulnerable contracts
- Gate: detection >93%, false positives <15%, avg time <6 min

### MONTH 2

#### Revenue — KPI: \$5,000 MRR

- Paid tiers: \$49 on-demand, \$199/mo dev plan launched
- 3 audit firm white-label pitches · multi-chain expansion

### MONTH 3

#### Breakthrough — KPI: \$25,765 MRR

- CronosLM v1: proprietary fine-tuned model (500+ real audits)
- 15 EVM chains · 1 responsible disclosure · enterprise pricing live

USE OF FUNDS

# \$30,000 USDT — deployed with precision.

38% hardware — yours to keep as a tangible asset. 62% operating runway for 6 months.

Hardware · 2x RTX 4090 Mini PCs + Laptop	\$11,500 · 38%
Development · 3-week intensive sprint	\$7,064 · 24%
LLM APIs · Opus + Sonnet + Gemini Ultra (3 months)	\$5,500 · 18%
Business Development · legal, brand, marketing	\$3,500 · 12%
Cloud Infrastructure · Hetzner + APIs (6 months)	\$2,436 · 8%



### Break-even Month 2

Cloud + API costs ~\$3,000/mo covered by first enterprise clients.



### 10x ROI Target

\$25,765 MRR means \$308k ARR run-rate. 10x return within 12 months.



### Hardware Stays

RTX 4090 cluster is a tangible depreciable asset. Zero cloud lock-in.

THE ASK

# \$30,000

## USDT funding round

Equity or revenue share — negotiable.  
Weekly Telegram updates. Full source access under  
NDA.

• 3-week deployment

• \$25,765 MRR · Month 3

• Multi-LLM · MCP-native

• Local GPU · no lock-in

• Live demo on request

*"We are not building a tool. We are building the immune system for Web3."*

cronos.analyst.click · Confidential — April 2026