AgentLISA Whitepaper

Building the Security Infrastructure for the AI Agent Economy

---

Executive Summary

AgentLISA is the world's first AI-powered smart contract security platform purpose-built for the autonomous agent economy. As Web3 transitions from human-operated protocols to AI-driven agentic commerce, security infrastructure must evolve from reactive audits to continuous, programmable protection.

Our mission: Make institutional-grade security accessible, affordable, and autonomous.

Market Opportunity

The smart contract security market is projected to reach $15B+ by 2028, yet current solutions cannot scale:

- Manual audits cost $50K-$500K and take 4-8 weeks
- 97% of Web3 projects lack formal security audits
- $4B+ lost to smart contract exploits in 2023-2024
- Emerging AI agent economy requires **programmable, real-time security**

AgentLISA addresses this gap with AI-native infrastructure that delivers audit-grade analysis in minutes at <1% traditional cost.

Traction & Validation

Since our $12M Series A funding, we have achieved significant traction:

Platform Adoption

- **90,000+** registered developer teams
- **4,000+** premium subscribers
- **$1M+** ARR with 30%+ MoM growth
- **$10B+** in smart contract value secured
- **100%** accuracy on production audits (Arcadia Finance, Taiko, Virtuals Protocol)

AI Agent Economy Leadership

- **#4 ranking** on x402scan autonomous agent leaderboard

- **PaymentShield** securing autonomous payment transactions
- First security infrastructure integrated into x402 payment protocol

Research & Data Leadership

- **LISA-Bench:** 10,185 labeled and verified vulnerability samples across Solidity, Rust & Move
- **Industry's largest** curated dataset for Web3 security AI training
- **Open benchmark** adopted by leading AI labs for evaluating LLM security capabilities
- **Academic partnerships** with NTU, HKUST, Lingnan University, contributing to frontier security research

LISA-Bench Impact: Our proprietary dataset doesn't just power AgentLISA—it's becoming the industry standard for training and evaluating AI security models, establishing a sustainable data moat while accelerating ecosystem-wide security capabilities.

The Platform

1. Agentic Auditor — Multi-Chain Smart Contract Security

Industry-first AI-powered security platform with omnichain scanning across Solidity, Rust and Move. Powered by a multi-agent architecture that mirrors elite security research teams.

Specialized Agent Framework:

- **Reentrancy Agent** — Detects cross-function and cross-contract reentrancy
- **Access Control Agent** — Audits permissions and ownership structures
- **Price Manipulation Agent** — Identifies oracle and MEV vulnerabilities
- **State Consistency Agent** — Tracks execution paths across complex DeFi protocols
- **Business Logic Agent** — Verifies implementation vs. specification alignment
- **General Purpose Agent** — Comprehensive coverage for emerging attack vectors

TrustLLM Foundation: Purpose-built LLM trained on 10+ years of audit reports and vulnerability data in collaboration with NTU's Cyber Security Lab and other research labs worldwide.

CARL Self-Evolution: Continuous Auditing and Retraining Loop ensures the platform improves with every scan through validated real-world data feedback.

2. PaymentShield — Autonomous Payment Security

Application-layer security infrastructure for x402 and autonomous payment protocols. As AI agents transact autonomously, PaymentShield provides real-time transaction validation, anomaly detection, and exploit prevention.

Critical for the Agent Economy:

- Validates payment logic before execution
- Detects unusual transaction patterns in real-time
- Protects agent wallets from manipulation attacks
- Enables secure agent-to-agent commerce

3. Wallet Health Check — Real-Time Protection

Continuous monitoring for wallet security across all major chains:

- Private key exposure detection
- Suspicious approval monitoring
- Credential compromise alerts
- Integration with agent wallets for autonomous protection

4. LISA-Bench — The Security Intelligence Engine

Industry's first and largest security benchmark dataset for:

- Training specialized Web3 security models
- Evaluating frontier LLM capabilities in vulnerability detection
- Establishing industry standards for AI-powered security
- Open research collaboration with academic institutions

Dataset Composition:

- **10,000+** labeled and verified vulnerability samples
- Coverage across **Solidity, Rust & Move**
- **Real-world exploit patterns** from historical incidents
- **Continuously updated** through CARL feedback loop

Developer Integration

AgentLISA integrates seamlessly into modern development workflows:

- **IDE Plugins** — Real-time analysis in VSCode and Cursor
- **GitHub Actions** — Automated security gates on every commit
- **Direct Scanning** — Analyze deployed contracts across 20+ chains instantly
- **x402 Protocol** — Programmable API access for human developers and autonomous AI agents

---

The $LISA Token Economy

Why Web3 Security Needs a Native Asset

Traditional security markets operate on closed, expensive service models. The agent economy requires **open, programmable, continuous** security infrastructure. $LISA creates the economic foundation for this transition.

Token Utility

1. Payment for Services

- $LISA is the primary payment token across AgentLISA products, including security scans, subscriptions, premium feature access etc.

2. Bug Bounty Programs

- $LISA funds protocol-specific bug bounties. Researchers can optionally stake $LISA to increase submission priority and credibility, and rewards for valid findings are paid in $LISA.

3.Community Validation and Curation

- $LISA aligns incentives for threat intelligence review and severity labeling. Reputation-based multipliers reward consistent high-quality contributions, while slashing applies to stake-backed invalid or malicious submissions.

4. Ecosystem Development

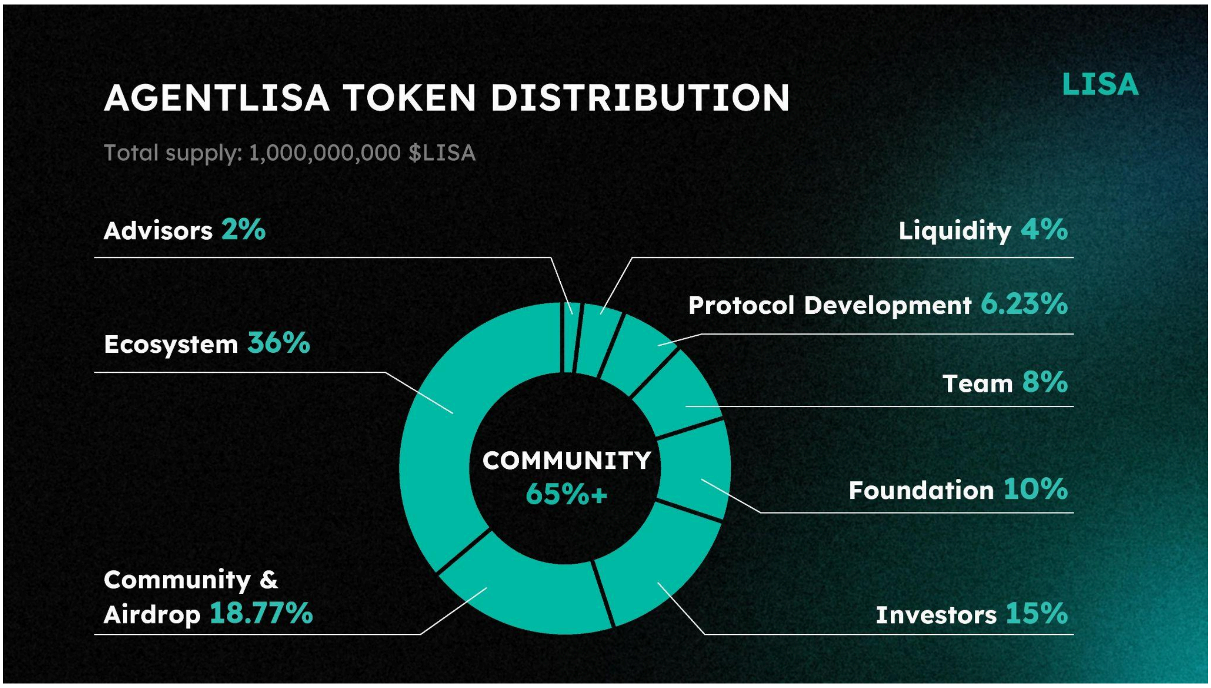
- $LISA supports the AI agent ecosystem through revenue sharing for agent developers, access to specialized security models, and rewards for contributing LISA-Bench training data or improvements.

5.Governance

- $LISA holders participate in protocol governance, including decisions on platform parameters, bounty rules, treasury allocation, and ecosystem priorities.

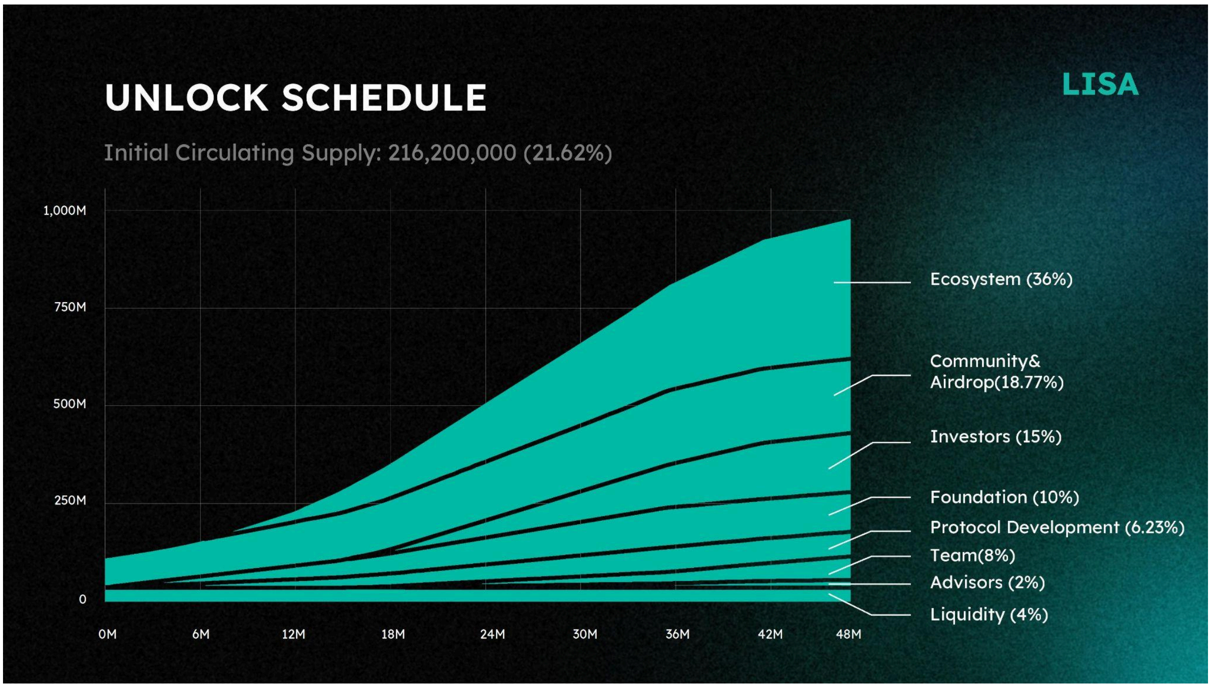
Token Distribution

Total Supply: 1,000,000,000 $LISA
TGE Date: December 18, 2025
Initial Circulating Supply: 216,200,000 (21.62%)



Category	Allocation	Vesting	Purpose
Ecosystem	36%	3mo cliff, 24mo linear	Grants, partnerships, developer incentives
Community & Airdrop	18.77%	Mixed (see below)	User rewards, CEX programs, community growth
Foundation	10%	12mo linear	Protocol R&D, academic partnerships
Protocol Development	6.23%	12mo linear	Core platform engineering
Investors	15%	12mo cliff, 18mo linear	Seed + Private round participants

Team	8%	12mo cliff, 36mo linear	Founding team and core contributors
Advisors	2%	12mo cliff, 24mo linear	Strategic advisors
Liquidity	4%	Unlocked at TGE	DEX pools and market support



Community & Airdrop Breakdown (18.77%)

- **7.77%** — Binance Alpha, Binance Spot Reserve, and other CEXs marketing
- **11%** — Community incentives distributed over 24 months

Roadmap to Market Leadership

Q4 2025 — Token Launch & Platform Expansion

✅ **$LISA TGE** — December 18, 2025
✅ **Exchange Listings** — Major CEX and DEX liquidity
✅ **Multi-Chain Launch** — Full Solidity, Rust, and Move support

✅ **Developer Tooling** — VSCode, Cursor, GitHub integrations
✅ **PaymentShield Beta** — x402 autonomous payment security

H1 2026 — From Detection to Delivery

Product Goal: Transform AgentLISA from a detection platform into a complete security delivery system that bridges AI analysis with institutional-grade assurance.

- **Hybrid Audit Platform** — Seamless AI-to-human handoff workflow combining autonomous analysis with expert review for institutional clients
- **Enterprise White-Label Solutions** — Customizable security workflows for Big 4 firms and specialist auditors to leverage AgentLISA's infrastructure under their own branding
- **CARL Evolution Upgrade** — Advanced self-improving capabilities including:
    - Automated retraining pipelines with validated vulnerability data
    - Cross-chain vulnerability pattern recognition
    - Community-driven model improvement with incentivized feedback loops
    - Real-time model performance monitoring and A/B testing
- **LISA-Bench Public Release** — Open-source benchmark dataset for research community, establishing AgentLISA as the academic standard for Web3 security AI evaluation

H2 2026 — Continuous Defense & Enhanced Compliance

- **Real-Time Monitoring** — Live on-chain exploit detection, AI agentic payment fraud detection and alerts
- **Economic Simulation** — Flash loan and oracle manipulation modeling
- **Regulatory Compliance** — MAS/SEC/MiCA-mapped reporting
- **Enterprise SLAs** — Institutional-grade dashboards and guarantees

2026+ — The Autonomous Security Layer

- **Formal Verification** — Mathematical proof integration
- **L1/L2 Expansion** — New chain and language support
- **Community Model Development** — Open-source agent contributions
- **Full Stack of Agentic Security Suite** — Expand beyond smart contract, blockchain to general agentic software security

---

Learn More

- **Website:** agentlisa.ai
- **Documentation:** agentlisa.ai/docs
- **Twitter:** @AgentLISA_ai
- **Telegram:** @AgentLISA_AI
- **GitHub:** github.com/agentlisa

AgentLISA is building the security layer for the next generation of Web3.

As the autonomous agent economy scales from billions to trillions in value, security infrastructure must be continuous, programmable, and accessible. AgentLISA makes this possible — today.

Token Generation Event: December 18, 2025

This document is for informational purposes only and does not constitute financial advice. Please conduct your own research before participating in any token sale.