

SENTINEL COIN

AI-POWERED SECURITY MIDDLEWARE FOR SOLANA

Technical Whitepaper | Version 1.4 | August 2026

Token: SENT | Network: Solana

CA: 5YyFARizABCqN7GPAPgS66LTsQ4D9o9TzWjamH5Wpump

sentinelcoin.net

Abstract

SENTINEL is an AI-powered transaction security middleware protocol built on the Solana blockchain. It provides real-time threat detection, wallet screening, and token security analysis at the application layer – sitting between users and the Solana network without modifying the core consensus or encryption protocol.

The SENT token is the utility and governance token that powers access to the SENTINEL protocol, incentivises security node operators, and aligns stakeholder interests toward building a safer on-chain environment for all Solana users.

Unlike traditional security tools that are centralised, expensive, and require KYC, SENTINEL is permissionless, community-governed and accessible to anyone. The live AI screener is available at sentinelcoin.net with no account or signup required.

1. The Problem

1.1 Solana Users Face Constant Threats

The Solana ecosystem processed trillions in DEX volume in 2025. This scale attracts sophisticated attackers. MEV bots, wallet drainers, phishing contracts and rug pulls cost Solana users hundreds of millions of dollars annually.

Key attack vectors include:

- MEV sandwich attacks – bots front-run and back-run user trades to extract value
- Wallet drainers – malicious contracts requesting unlimited token approvals
- Rug pulls – tokens with unrevoked mint authority or unlocked liquidity
- Phishing sites – fake dApps mimicking legitimate protocols
- Honeypot tokens – contracts that allow buying but block selling

1.2 Real Losses – Real Data

SENTINEL has tested 34 confirmed real-world MEV bot addresses. Combined stolen by tested bots: \$500M+. Notable cases:

- arsc DeFi wallet (Ai4zq...VXKKT) – \$287M stolen – SENTINEL score: 95/100 BLOCK
- arsc Cold Wallet (9973h...zywp6) – \$30M stolen – SENTINEL score: 92/100 BLOCK
- 2026 Validator MEV Bot – \$500M+ pool – SENTINEL score: 96/100 BLOCK
- B91 Bot – 82,000 attacks – SENTINEL score: 91/100 BLOCK

1.3 Existing Solutions Are Inadequate

Current approaches fall into two categories: centralised enterprise services (Chainalysis, TRM Labs) that are expensive and require KYC; and basic wallet warning systems that rely on static blocklists rather than dynamic AI analysis. Neither is permissionless, real-time or accessible to individual users.

2. The SENTINEL Solution

2.1 Three-Layer Architecture

Layer 1 – AI Transaction Screener (Live)

An AI inference model analyses wallet addresses and token contracts in real time. Every scan evaluates:

- Wallet age and behavioral history
- Transaction instruction signatures
- Token approval scope analysis
- MEV attack probability scoring
- Fund source risk assessment
- Rug pull risk indicators
- Honeypot pattern detection

Response time: under 80 milliseconds. Verdict: CLEAR (0-20) / CAUTION (21-50) / DANGER (51-100).

Layer 2 – AES-256-GCM Encryption (Phase 2)

Application-layer encryption hides transaction metadata before broadcast. MEV bots watching the mempool see an encrypted blob – they cannot determine the token, size or slippage tolerance of the trade. This prevents front-running and sandwich attacks at the source.

Layer 3 – Decentralised Oracle Network (Phase 3)

SENT stakers run security oracle nodes globally. Community-governed threat intelligence database. 40% of protocol fees distributed to node operators.

3. Live Product

3.1 Wallet Screener

Available free at sentinelcoin.net/screener.html. Users paste any Solana wallet address or contract and receive a full threat analysis in seconds. No account. No signup. No barriers.

Output includes: risk score 0-100, MEV probability, fund source risk, threat flags, verdict (CLEAR/CAUTION/BLOCK) and plain-language assessment.

3.2 Token Security Scanner

Available at sentinelcoin.net/token-scanner.html. Scans any token contract address for rug pull risk, honeypot patterns, mint authority status, LP lock verification and suspicious wallet flows. Generates a downloadable PDF security report.

Live market data pulled from DexScreener, Solana RPC and GoPlus simultaneously. Each report includes on-chain data, threat flags, suspicious wallet trace, terminal output and AI security assessment.

3.3 Proof of Concept – \$XST Token Case Study

The most powerful validation of the SENTINEL Token Scanner is a real-world documented case. Before the \$XST token collapsed from a \$70 million market cap to approximately \$4 million – a loss of over 94% – SENTINEL scanned it and returned the following result:

```
// — SENTINEL TOKEN SCAN —
> contract:      XTuo1fV7HHMhs4BYiwtrWSLsMCJNrooH2AsswTYZqP
> token:         Unknown (UNKNOWN)
> mint_authority: unknown ⚠
> freeze_auth:   unknown ⚠
> lp_locked:     unknown ⚠
> honeypot_risk: HIGH ⚠
> rug_score:     72/100
> verdict:       ■ DANGER ■
```

SENTINEL flagged \$XST with the following threat indicators:

- No verifiable on-chain metadata found for the contract address
- Mint authority unconfirmed – active mint allows unlimited supply inflation
- Freeze authority unknown – potential honeypot vector
- Liquidity pool lock status unverified – instant LP removal risk
- Token not listed on Jupiter, Birdeye or CoinGecko
- pump.fun launch pattern – historically high rug rate (85%+)
- No audited smart contract code publicly available
- Honeypot risk: HIGH

\$XST market cap: \$70,000,000 → \$4,000,000. Loss: -94.3%. SENTINEL called it.

This is not a simulated test or a backtested result. SENTINEL scanned \$XST live, returned a 72/100 DANGER verdict, and the token subsequently rugged. This is verifiable on-chain by anyone using public Solana block explorers.

Any user who scanned \$XST through SENTINEL before buying would have been warned not to invest. This is exactly the protection SENTINEL exists to provide.

3.4 Paid Security Services

Three paid services are available for projects:

- Formal Audit Request – Basic (500K SENT), Pro (2M SENT), Enterprise (10M SENT) – comprehensive PDF security report within 24-48 hours
 - Project Verification – 5,000 SENT – for projects requesting manual on-chain review and score update
-

4. Technical Architecture

4.1 AI Model

The SENTINEL AI model uses Claude (Anthropic) with custom threat scoring prompts trained on confirmed MEV bot addresses, known rug pull patterns and Solana exploit history. The model evaluates:

- Wallet behavioral patterns vs known MEV signatures
- Contract instruction analysis for malicious patterns
- Fund source tracing through transaction history
- Token security parameters from on-chain data
- Cross-reference against GoPlus security database

4.2 Data Sources

- DexScreener API – live price, volume, liquidity, pair data
- Solana RPC (mainnet-beta) – on-chain account and transaction data
- GoPlus Security API – mint authority, freeze authority, transfer fee
- Rugcheck – risk scoring cross-reference
- SENTINEL MEV Blackbook – 34 confirmed bot addresses

4.3 Stack

- Frontend: HTML/CSS/JavaScript – deployed on Netlify
- AI Layer: Anthropic Claude Sonnet via direct API
- PDF Generation: jsPDF – client-side branded reports
- Blockchain: Solana SPL Token Standard
- Token Lock: Streamflow Finance
- DEX: PumpSwap (graduated pump.fun bonding curve)

4.4 Smart Contract Infrastructure

SENTINEL currently utilises smart contracts for two core functions: developer token vesting and liquidity locking. Both are deployed on Solana mainnet and publicly verifiable.

Developer Token Vesting – Streamflow Finance

The founding developer token allocation is locked inside a Streamflow Finance vesting smart contract on Solana mainnet. Streamflow is an audited, battle-tested vesting protocol used by hundreds of Solana projects. The lock contract enforces the vesting schedule programmatically – no human action can release tokens ahead of schedule.

Contract address:

4hULt3fs6z11aw9VpKVHeRH1Xet7bUDGF1PBAToTUnVF

Verify at:

app.streamflow.finance/contract/solana/mainnet/
4hULt3fs6z11aw9VpKVHeRH1Xet7bUDGF1PBAToTUnVF

Liquidity Pool Lock – PumpSwap

100% of SENTINEL liquidity is permanently locked via LP token burn on PumpSwap. Burning LP tokens removes them from circulation permanently, making liquidity withdrawal mathematically impossible. This is the strongest possible form of LP locking – it requires no third-party lock contract and has no expiry date.

LP pair address:

84gz1EYQ2mfrYhGsUVECr5DxJzxL5vY63VvxXtQdudn

4.5 Smart Contract Audit Roadmap

SENTINEL holds itself to the same security standard it applies to others. A project that scans tokens for unaudited contracts must itself undergo a formal third-party smart contract audit before deploying protocol-level infrastructure.

The following audit milestones are planned as SENTINEL scales:

Phase 2 – Pre-SDK Audit

Before the SENTINEL TypeScript SDK is published to npm and integrated into third-party dApps, a formal security audit of all smart contract code will be conducted by a reputable third-party auditing firm. Target auditors include:

- OtterSec – Solana-native security firm with extensive SPL token and protocol audit experience
- Halborn – blockchain security firm with Solana expertise
- Sec3 – specialised Solana smart contract auditor

The audit will cover:

- SENTINEL vesting and payment contract logic
- API access control and payment verification contracts
- Any smart contracts deployed as part of the SDK integration layer
- Oracle node registration and staking contracts (if deployed before Phase 3 launch)

Phase 3 – Oracle Network Audit

Before the decentralised oracle node network goes live, a comprehensive audit of all staking, governance and revenue distribution contracts will be conducted. Given the financial value at stake in a staking system, this audit will be mandatory before any SENT holder can stake tokens.

Audit Transparency Commitment

All audit reports will be published in full on sentinelcoin.net and linked from the SENTINEL whitepaper. SENTINEL will not redact findings – both passed and flagged items will be publicly disclosed. Any critical findings will be resolved before the audited contracts go live.

This is consistent with SENTINEL's core principle: if we flag unaudited contracts as a risk factor for other tokens, we must hold ourselves to the same standard.

5. Token Economics

5.1 Token Details

- Name: Sentinel Coin
- Symbol: SENT
- Network: Solana
- Standard: SPL Token
- Total Supply: 958,469,734 SENT
- Tax: 0% buy and sell
- Mint Authority: Revoked
- Freeze Authority: None
- Ownership: Fully Renounced
- LP: Locked 100% Forever
- Developer Tokens: Locked on Streamflow

5.2 Distribution

- 80% – Public Sale (pump.fun bonding curve, no presale)
- 8% – Protocol Development (24 month linear vest)
- 6% – Ecosystem and Grants (12 month linear vest)
- 4% – Security Node Bootstrap (released Phase 3)
- 2% – Team (12 month cliff, 24 month vest – Streamflow locked)

5.3 Token Utility

- API Access Payments – dApps pay SENT per 1,000 transaction screens
- Token Scanner Access – full security report with PDF
- Formal Audit Requests – 500K to 10M SENT depending on tier
- Project Verification – 5,000 SENT per verification request

- Security Node Staking – operators stake SENT to run oracle nodes (Phase 3)
 - Governance – holders vote on AI model parameters and protocol upgrades
 - Revenue Share – 40% of protocol fees to SENT stakers (Phase 3)
-

6. Security and Verification

6.1 On-Chain Security

- GoPlus Security: 0 risky items, 0 attention items
- Rugcheck Score: 1 – GOOD – No risks found
- Mint Authority: Revoked
- Freeze Authority: None
- LP Locked: 100% permanently via LP token burn
- Ownership: Fully renounced
- Developer Lock: Streamflow contract
4hULt3fs6z11aw9VpKVHeRH1Xet7bUDGF1PBAToTUnVF

6.2 Verification Links

GoPlus:
gopluslabs.io/token-security/solana/5YyFARizABCqN7GPAPgS66LTsQ4D9o9TzWjamH5Wpump
Rugcheck: rugcheck.xyz/tokens/5YyFARizABCqN7GPAPgS66LTsQ4D9o9TzWjamH5Wpump
Solscan: solscan.io/token/5YyFARizABCqN7GPAPgS66LTsQ4D9o9TzWjamH5Wpump
Streamflow:
app.streamflow.finance/contract/solana/mainnet/4hULt3fs6z11aw9VpKVHeRH1Xet7bUDGF1PBAToTUnVF

7. Roadmap

Phase 1 – Foundation (In Progress)

- ✓ SENT launched on pump.fun – August 2026
- ✓ Graduated bonding curve to PumpSwap
- ✓ Liquidity locked forever
- ✓ Ownership renounced
- ✓ Mint authority revoked
- ✓ Developer tokens locked on Streamflow
- ✓ Live AI wallet screener at sentinelcoin.net
- ✓ Token security scanner with PDF reports
- ✓ 34 MEV bots confirmed – 100% detection rate
- ✓ \$XST flagged DANGER – confirmed rug – \$70M to \$4M
- ✓ Technical whitepaper v1.4 published
- ⌚ CoinGecko listing
- ⌚ Jupiter verification
- ⌚ TypeScript SDK v1

Phase 2 – SDK, Encryption and Audit (1-3 Months)

- SENTINEL TypeScript SDK published to npm
- AES-256-GCM application-layer encryption
- First 2-3 official dApp integrations
- Public threat intelligence dashboard
- Third-party smart contract security audit (OtterSec / Halborn / Sec3)
- Full audit report published publicly on sentinelcoin.net

Phase 3 – Oracle Network (3-9 Months)

- Decentralised security oracle node network
- Comprehensive oracle and staking contract audit before launch
- SENT staking with 40% revenue share
- On-chain governance
- CEX listings
- Cross-chain expansion

Phase 4 – DAO and Scale (9-24 Months)

- SENTINEL DAO
- Open-source AI model
- Enterprise studio licensing
- 50+ dApp integrations
- 1M+ transactions screened monthly

Phase 5 – Public Sector Engagement (24+ Months)

- Long-term goal: establish working relationships with regulatory and law enforcement agencies engaged in cryptocurrency oversight
- Intent to make SENTINEL's scam and rug-pull detection findings available as a resource agencies can reference during their own investigations
- Intent to help agencies navigate specific on-chain situations – flagged tokens, suspicious wallet activity, and scam patterns – as a subject-matter resource, not a replacement for an agency's own investigative process
- This phase depends on completing the audits and validation work described in Phases 2-4 first – no formal government engagement exists today, and none is claimed

8. Team

- Blackphntom – Director / Developer
- Mr. Frozen – Head of Marketing
- Ghost – Marketing
- Kieff – Administration

- Arw777 - Administration
- Showtime - Head of Networking
- JeanC5 - Administration

SENTINEL was founded by an independent developer with direct experience building and operating server infrastructure – giving the project ground-level understanding of how digital economies work, how they are exploited and what security tooling users actually need.

9. Community and Links

- Website: sentinelcoin.net
 - AI Screener: sentinelcoin.net/screener.html
 - Token Scanner: sentinelcoin.net/token-scanner.html
 - Whitepaper: sentinelcoin.net/sentinel-whitepaper.pdf
 - Twitter/X: @SentinelCoinAIx
 - Telegram: t.me/sentinelcoinai
 - Discord: discord.gg/PqftRm4vcv
 - Email: Sentinelnetworksrpgmod@gmail.com
-

Disclaimer

This whitepaper is for informational purposes only and does not constitute financial, investment or legal advice. Cryptocurrency investments involve significant risk. Past performance is not indicative of future results. Always do your own research (DYOR) before making any investment decision. The SENTINEL team makes no guarantees regarding token price, returns or future development milestones.