PUBLIC WHITEPAPER

Inspector Whitepaper

Solana on-chain risk intelligence and trust infrastructure

Version 2.0 · July 2026

Website: https://www.chain-inspector.com

Table of Contents

1. Executive Summary

Inspector is a Solana-focused on-chain analytics and risk intelligence platform designed to help users evaluate token risk, liquidity conditions, holder concentration, authority exposure, and other trust signals before making decisions.

The goal of Inspector is not to promise that a token is safe. The goal is to organize fragmented on-chain data into structured, reviewable, evidence-backed risk surfaces.

Solana token markets move quickly. New tokens appear, liquidity changes, holder structures shift, and project risk can evolve after the first scan. Inspector is built to support this environment through scanning, monitoring, verification workflows, automation, and future launch-assessment tools.

Core ecosystem direction:

- Inspector Scan - structured token risk review.
- Monitoring - ongoing attention to changing token conditions.
- Verification - evidence-based trust criteria and review workflows.
- Sol Auto Scan - planned automated discovery and alerting direction.
- SafeLaunch - future launch-risk module.
- Telegram Alerts - notification layer for selected signals.

Inspector's mission is to become a practical trust layer for Solana token evaluation: transparent, security-conscious, and useful without pretending to remove all risk.

2. Problem Statement

Solana token markets are fast, fragmented, and difficult to evaluate manually.

Common risks include:

- concentrated holders;
- suspicious authority settings;
- unstable or removable liquidity;
- misleading social signals;
- short-lived hype cycles;

- rapidly changing token ownership;
- incomplete or inconsistent public data;
- scam patterns that only become visible after launch;
- user overconfidence caused by shallow scanner results.

Many tools provide quick checks, but quick checks can create false confidence when the underlying context is incomplete. A token may pass simple filters while still having structural, liquidity, authority, or behavioral risk.

Users need risk intelligence that is evidence-backed, transparent about uncertainty, structured enough to compare, updated when conditions change, resistant to manipulation, and clear about limitations.

---

3. Inspector Ecosystem

3.1 Inspector Scan

Inspector Scan is the core token review workflow. It evaluates available on-chain and market data and presents structured findings such as token identity, mint data, authority exposure, liquidity context, holder concentration, top-holder distribution, available confidence levels, community or usage signals where applicable, and review notes when data is incomplete.

A scan is not a guarantee of safety, price performance, liquidity stability, or future behavior. It is a decision-support surface for clearer review.

3.2 Monitoring

A token's risk profile can change after the first scan. Monitoring is the direction of Inspector that focuses on ongoing changes, such as liquidity movement, holder concentration shifts, authority changes, new risk flags, scan-count trends, safety-score movement, and unusual activity patterns.

The objective is to reduce reliance on a single initial snapshot. Inspector's long-term direction is to keep attention on change, not only first-state review.

3.3 Verification

Verification is intended to be a stricter evidence-based review layer. A token should only be eligible for an Inspector verification status if it meets published criteria at the time of review. These criteria may include liquidity, authority, holder concentration, data confidence, and other risk factors.

Inspector Verified indicates that a token met Inspector's published verification criteria at the time of review. It is not a guarantee of future safety, price performance, liquidity permanence, team behavior, or absence of risk.

3.4 Sol Auto Scan

Sol Auto Scan is a planned automation direction based on an earlier working Inspector module. The purpose is to discover new Solana tokens, process them through Inspector's risk framework, classify them into signal bands, and send alerts when a token matches selected conditions.

Sol Auto Scan is intended for discovery and monitoring assistance. It must not be presented as a guaranteed profit engine or automated investment recommendation.

3.5 Telegram Alerts

Telegram alerts are intended to provide fast notifications when selected Inspector conditions are met. Potential alert types include high-score token discovery, monitored token risk changes, liquidity condition changes, holder concentration changes, verification state changes, and selected band matches from planned automation.

Telegram alerts are notification infrastructure. They are not financial advice.

3.6 SafeLaunch

SafeLaunch is a future module direction. Its purpose is to evaluate launch readiness and launch-related risk conditions before or during token deployment. This may include structural checks, liquidity planning, authority posture, and other launch-risk factors.

SafeLaunch is not currently described as a public guarantee system. It is a future Inspector ecosystem direction.

---

4. Risk Scoring Philosophy

Inspector's scoring philosophy is based on structured evidence, not hype.

A useful risk system should show what was checked, show what could not be checked, separate evidence from assumptions, reduce false confidence, track changes over time, and avoid pretending that one score explains everything.

Inspector scoring should be treated as a decision-support layer, not a decision-maker. A high score does not mean safe forever. A low score does not always mean scam. A missing-data warning is itself important risk context.

Inspector should clearly surface uncertainty when data is incomplete, unavailable, unstable, or inconsistent.

---

5. Data and Signal Categories

Inspector may evaluate signals across several categories:

- Token structure: mint information, supply context, authority settings, metadata

consistency, and known token-program behavior.

- Liquidity context: available liquidity data, pool structure, lock or unlock context

where supported, liquidity concentration, and changes over time.

- Holder distribution: top-holder concentration, single-wallet exposure, top-10 supply,

abnormal distribution patterns, and potential sybil-like structures where detectable.

- Market and usage signals: scan activity, most-scanned trends, community signals,

token discovery patterns, and safety-score movement.

- Monitoring signals: changes after first scan, new warnings, risk movement, liquidity

movement, and holder concentration changes.

---

6. Security and Abuse Resistance

Inspector must be built with security and abuse resistance as a core requirement.

Public security principles include:

- server-side payment verification and entitlement enforcement;
- strict request validation at public boundaries;
- secure session handling;
- replay-resistance principles for sensitive actions;
- rate limiting and abuse monitoring;
- protection against spoofed payment or entitlement states;
- protection against manipulated scan or leaderboard activity;

- careful handling of public and private API keys;
- privacy-minimal logging that avoids exposing sensitive data.

The security goal is practical resilience. Inspector should be difficult to manipulate, hard to abuse at scale, and transparent about limitations. Detailed endpoint paths, database schema, callback verification internals, signing algorithms, provider secrets, anti-abuse thresholds, and unpublished controls are intentionally excluded from this public document.

---

7. Payment and Access Model

Inspector is a digital SaaS service. Where paid access is offered and enabled, customer payments are collected in EUR through the displayed third-party payment provider. Inspector does not store card details. Access is activated only after server-side payment confirmation and remains linked to the authenticated Inspector account identity.

Where Paysera payment options are displayed and enabled, EUR payments are processed through Paysera's hosted payment environment. Inspector does not conduct cryptocurrency buying, selling, exchange, custody, or transfer services through Paysera.

Phantom wallet authentication remains the private Inspector account identity. The wallet is used for Inspector account/session identity and entitlement ownership; it is not proof that a fiat payment succeeded. A browser return or redirect alone does not activate access.

Inspector may maintain accounting-ready records such as local order references, payment status, amount, currency, entitlement linkage, and support/review state where required for service operation, accounting, security, dispute resolution, or legal compliance.

---

8. Monetization Direction

Inspector may offer one-time access periods, pay-as-you-go products, premium analysis, monitoring, alerts, or other clearly described digital-service products. Current products, prices, access durations, and payment availability are those displayed in the live service.

Potential future products must remain clearly identified as planned or potential until they are actually available in the service. Inspector should not present recurring billing as active unless it is implemented and displayed to customers.

Any monetization model should be designed around transparency, clear entitlements, and server-verified payment status.

9. Verification and Advertising Boundaries

Inspector may support verification workflows and visibility placements, but these must be clearly separated.

Verification should be based on published criteria. Advertising or spotlight placement should not imply safety, endorsement, or verification unless the token independently qualifies under the verification rules.

Recommended principle: paid visibility must not be confused with earned trust status.

This protects users, the platform, and the credibility of Inspector.

10. Limitations and Disclaimers

Inspector is a risk intelligence and analytics platform.

Inspector does not provide financial advice. Inspector does not provide investment, legal, tax, brokerage, exchange, custody, or trading advice. Inspector does not guarantee that a token is safe. Inspector does not guarantee price performance, profitability, sellability, liquidity permanence, holder behavior, authority behavior, or project conduct. Inspector does not remove the need for user judgment.

Inspector outputs depend on available data, supported sources, system availability, and the state of the Solana ecosystem at the time of review.

Users should treat Inspector as a decision-support tool, not as a substitute for independent research.

11. Roadmap

Inspector's roadmap is expected to evolve in phases:

- Core scanner: token scanning, structured risk output, basic usage flow, access control,

and public-facing product interface.

- Trust surfaces: improved risk scoring, discovery surfaces, clearer evidence

presentation, public content, and legal/company presentation.

- Monitoring: token change tracking, risk movement detection, alert conditions, and

monitoring-oriented UX.

- Verification: published verification criteria, review workflows, public limitations,

and separation between verification and advertising.

- Sol Auto Scan: automated token discovery, risk-band classification, Telegram alerting,

and scalable data-source handling.

- SafeLaunch: launch-readiness review, launch-risk framework, and pre-launch or

early-launch signal analysis.

- Ecosystem expansion: integrations with wallets, bots, trading tools, or Solana

infrastructure where appropriate.

Roadmap items are directional and may change based on technical, legal, accounting, market, and security requirements.

---

12. Partnerships and Integrations

Inspector may pursue integrations with relevant Solana ecosystem participants, such as wallets, DEX interfaces, token discovery platforms, Telegram bots, analytics tools, trading interfaces, and developer tools.

Unless a partnership is formally announced, such references should be understood as potential integration directions, not confirmed partnerships.

---

13. Legal Operator

Inspector is operated by:

Mažoji bendrija Deimienlabs

Company code: 308039346

Registered office: Bistryčios g. 40-21, LT-10321 Vilnius, Lithuania

Contact: hello@chain-inspector.com

Website: https://www.chain-inspector.com

Inspector is developed as a software / SaaS analytics platform focused on Solana on-chain risk intelligence.

---

14. Vision Statement

Inspector is being built to become a trust infrastructure layer for Solana token evaluation.

The long-term vision is to help users move from fragmented signals and emotional decisions toward structured, evidence-backed review.

Inspector should not create false certainty. Inspector should make uncertainty visible. Inspector should not sell hype. Inspector should organize risk. Inspector should help users see what matters before they act.

The ecosystem direction is clear: scan, monitor, verify, alert, and support safer decision-making in fast-moving Solana markets.

---

15. Version History

Version 1.1 - September 2025

Early founder vision and authorship record focused on Inspector as an advanced Solana anti-rug scanner.

Version 2.0 - July 2026

Updated ecosystem whitepaper reflecting Inspector's broader direction: scanning, monitoring, verification, Sol Auto Scan, SafeLaunch, Telegram alerts, SaaS payment wording, and official operation by Mažoji bendrija Deimienlabs.