

EVM WATCHTOWER: REAL-TIME BLOCKCHAIN FORENSICS & RISK SCORING FOR WEB3 INVESTORS

Explainable, instantly actionable intelligence that lets investors spot deployer fraud, honeypots, and coordinated rugpulls before funds move.

THE PROBLEM: SPEED AND OPACITY IN ETHEREUM SECURITY

EXPLOSIVE VOLUME

Scam tokens and factory-generated fraud deploy every block, overwhelming manual investigation.

SLOW DETECTION

Traditional post-mortem analysis is too slow—money is stolen before teams can respond.

OPAQUE SIGNALS

Existing risk scores are black boxes with little transparency or breakdowns for investors.

NEED

Real-time, explainable intelligence that maps relationships and shows WHY a contract is risky.





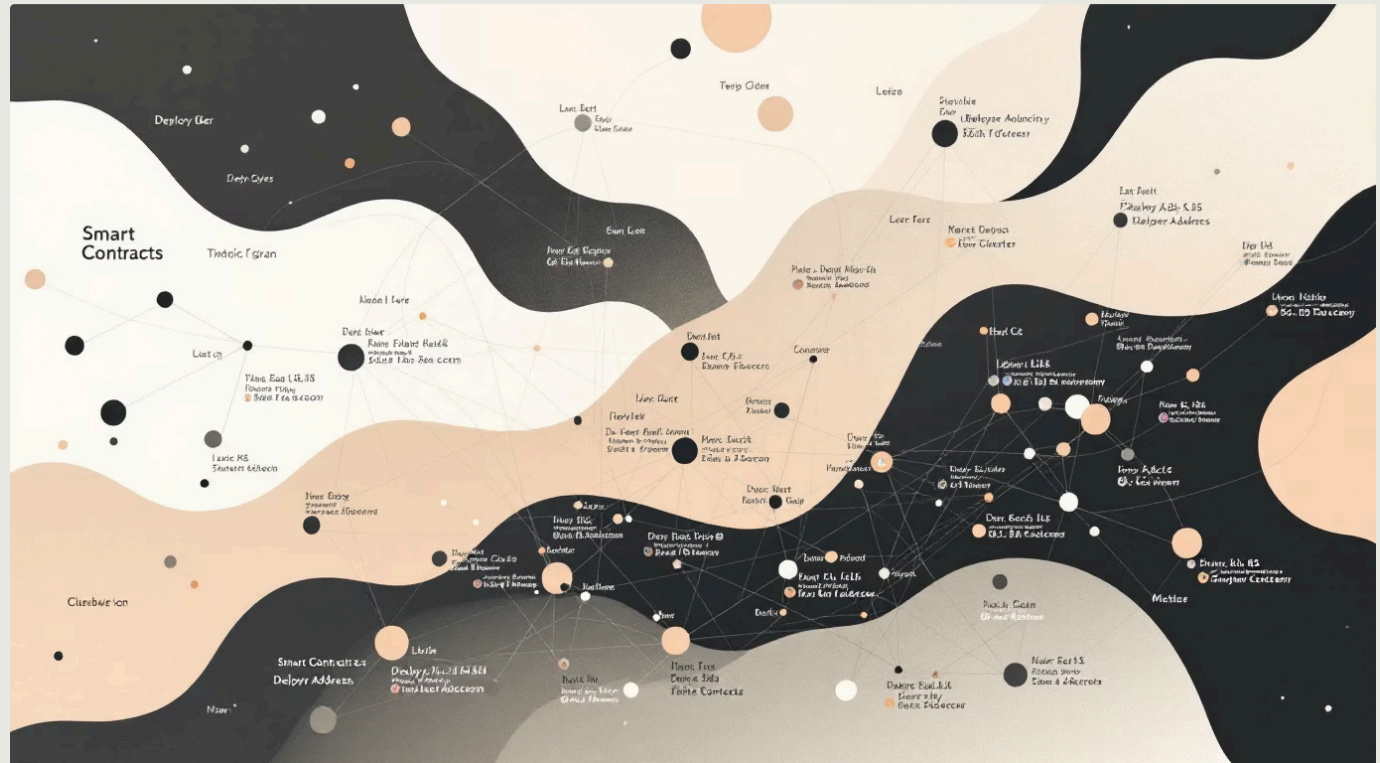
Streams and filters 100,000+ mempool events instantly, enabling immediate detection at block time.



Transparent heuristic-based scores (0–100) with clear component breakdowns for explainability.



Visualizes deployer relationships and clusters by bytecode hash to expose scam networks.



HOW WATCHTOWER DETECTS THREATS

- **VULNERABILITY SCANNING**

Detects reentrancy, unchecked delegatecalls, signature malleability, and other exploitable patterns.

- **HONEYPOT DETECTION**

Finds hidden minting, deceptive ownership renouncement, and transfer-trap logic before users add liquidity.

- **PROXY & METAMORPHIC RISKS**

Flags proxies, metamorphic redeployments, and gas-dependent logic that enable stealthy changes.

- **CONTROL-FLOW ANALYSIS**

Identifies infinite loops and factory-driven expansion patterns that indicate scalable fraud.



VISUAL INTELLIGENCE: MAPPING THE DARK FOREST

Bytecode pivot clusters contracts by code similarity; deployer webs reveal coordination; heatmaps surface risk hotspots humans often miss—so investors can see threats before liquidity flows.

BYTECODE PIVOTING

Groups contracts by bytecode hash to catch reused malicious templates.

DEPLOYER WEBS

Instantly exposes coordinated rugpull rings and funding sources.



CASE STUDY 1: THE HIDDEN TAX HONEYPOT

A token marketed as “0% Tax” actually set a 99% transfer fee via constructor arguments. Watchtower scored it CRITICAL (98/100) within 12 seconds of deployment, enabling alerts that prevented investor losses and exposed malicious intent.



Detection combined constructor parsing, token transfer simulation, and bytecode comparison to known honeypot templates.



CASE STUDY 2: THE “PEPE” COPYCAT RUGPULL RING

Fourteen tokens launched simultaneously. Graph Explorer linked them to one Tornado Cash–funded deployer and a shared bytecode cluster. Coordinated rugpull was identified before liquidity was added, protecting investors and enabling rapid takedown intelligence.

SIMULTANEOUS LAUNCHES

Pattern matched factory-driven deployments.

FUNDING LINK

On-chain funding traced to anonymizing service.



TECHNOLOGY: SPEED, PRIVACY & SCALABILITY

FRONTEND

React 19 + TypeScript + SQLite for a responsive, local-first UI that preserves investigator privacy.

BACKEND

High-throughput Go API for historical aggregation and cross-chain normalization.

Epoch-aware heuristics adjust detection around protocol upgrades (Merge, Shanghai). Local-first forensics means investigation data is stored client-side, protecting alpha and user privacy while enabling collaboration through shareable, explainable signals.

WHY ETH WATCHTOWER MATTERS TO WEB3 INVESTORS

TRANSPARENT SCORES

Risk ratings come with component explanations—so you know exactly why a contract is risky.

PROACTIVE DEFENSE

Detect fast-moving scams before liquidity is added and losses occur.

VISUAL FORENSICS

Graph-based tools make complex deployer ecosystems understandable for due diligence and capital allocation.



JOIN THE FUTURE OF ETHEREUM SECURITY

ETH Watchtower is the frontline defense for Web3 investors—real-time, transparent, and visual. Request a demo or read the whitepaper to see how explainable risk scoring and graph forensics can protect capital and improve decision-making.

REQUEST A DEMO

<https://rnts08.github.io/eth-watchtower>

READ THE WHITEPAPER

[Whitepaper & Technical Details](#)

<https://rnts08.github.io/eth-watchtower/whitepaper.md>



WATCHTOWER TUI: REAL-TIME INTELLIGENCE, YOUR WAY

Experience the full power of ETH Watchtower directly in your terminal. Our client-side, local-first TUI provides power users with a privacy-preserving interface for real-time threat detection, allowing for immediate analysis and decision-making on unfolding blockchain events.

LIVE EVENT FEED

Monitor mempool activity as it happens, filtering for high-risk contracts and suspicious transactions.

EXPLAINABLE RISK SCORES

Instantly view transparent risk scores for new deployments, with breakdowns of contributing factors.

PRIVACY-CENTRIC

Local-first processing ensures your investigative data and alpha remain on your machine.

FAST & EFFICIENT

Optimized for rapid navigation and data consumption, ideal for power users and analysts.

WATCHTOWER TUI: EVM WATCHTOWER IN ACTION

Dive into the direct interface of the Watchtower TUI, offering privacy-preserving, real-time intelligence directly in your terminal. See how power users interact with live data and granular risk insights.

