📖Introduction

Copy

Smart contract security faces a significant challenge. The rise of AI-generated smart contracts is outpacing human auditing capacity, fundamentally changing how code is deployed in Web3. While traditional security relies on manual audits commissioned by project teams, this model has scaling limitations - most contracts will deploy without comprehensive security review.

Wakehacker introduces a paradigm shift: a next-generation **utility AI agent** designed for the **vibe coding era**. Operating autonomously, it hunts for smart contract vulnerabilities 24/7, identifying them before hackers can exploit.

The agent operates through three core mechanisms:

- **Autonomous Scanning**: Proactively analyzes new and existing contracts
- **Community-Driven**: Responds to security analysis requests from any user
- **Token-Gated Access**: Detailed findings available through token deposits

This model transforms security from a project-centric service into a public utility. Wakehacker will not stop until it **scans every smart contract on Etherscan and DEX Screener**, collecting token deposits for discovered vulnerabilities.

Powered by Wake Framework's **three years of production auditing** experience with major protocols including Lido, Safe, and Axelar, Wakehacker brings **institutional-grade security tools** to scale.

Discover Wake Framework's proven track record ↗ in identifying critical vulnerabilities.

Next
Agentic Security Model

Archived copy · cryp2nova.com

Last updated 1 year ago

Archived copy · cryp2nova.com