AI and the Future of On-Chain Trust and Safety

Building Security Detection at Scale for Web3

DSS

+

IDID.xyz

Rodrigo Navarro Lajous
Staff Engineer at Webacy

The Threat Landscape at Scale

The Challenge	The Opportunity
100+ blockchains, different runtimes 100M+ transactions per day - Hundreds of scams launched daily - Same attacker behaviors across chains	- Unify fragmented multi-chain data - Detect repeating behavioral patterns - Predict and block attacks before users are impacted

Takeaway #1

- **Attackers change code. They don't change behavior.**
- **That's our advantage.**

IDID.xyz

The Scale of the Problem

Base October 2025

- 500,000+ new contracts deployed
- 18–20k new addresses per day
- 31,000 contracts analyzed
- 174,236 exploit detections in 30 days

Risk Levels

- 33.95% average rug-pull rate
- 51.6% peak rug-pull day
- Contracts triggering 8+ exploit signals = 9× more likely to rug

Takeaway #2

- The volume is enormous.
- The behaviors repeat.
- Static detection cannot keep up.

Why This Matters

What We Can Predict

- **Hidden mint + top-5 > 90% → 93% rug probability**
- **High-risk deployer clusters → 87% rug rate**
- **Cross-chain fingerprints → 75–80% early detection**

What It Changes

- **Users get warned before they sign**
- **Exchanges avoid toxic listings**
- **Protocols stop exploits before liquidity drains**

Final Takeaway

- **Behavior is the signal. Code is not enough.**
- **If you only scan code, you miss 90%+ of real attacker behavior.**
- **Integrate behavioral + financial analytics into your stack.**

Thanks!

Rodrigo Lajous

Staff Engineer

𝕏 @arlequin_eth

in /rodrigo-lajous

.xyz