Patterns in Chaos: Cross-Chain Forensics at Scale

Rodrigo Navarro Lajous
Staff Engineer at Webacy

DuneCon25

Coming Up

01 The Multi-Chain Forensics Challenge

02 5 Forensics Patterns

03 Wrap up

The Multichain Forensics Challenge

“Chaos is predictable when you know the patterns”

The Multichain Forensics Challenge

The Challenge

- 100+ blockchains to be monitored
- Different execution models: EVM vs Solana vs Move vs TON vs Sui vs Stellar
- +100 Millions of transactions to be analyzed daily
- Same scam patterns, different implementations

The Opportunity

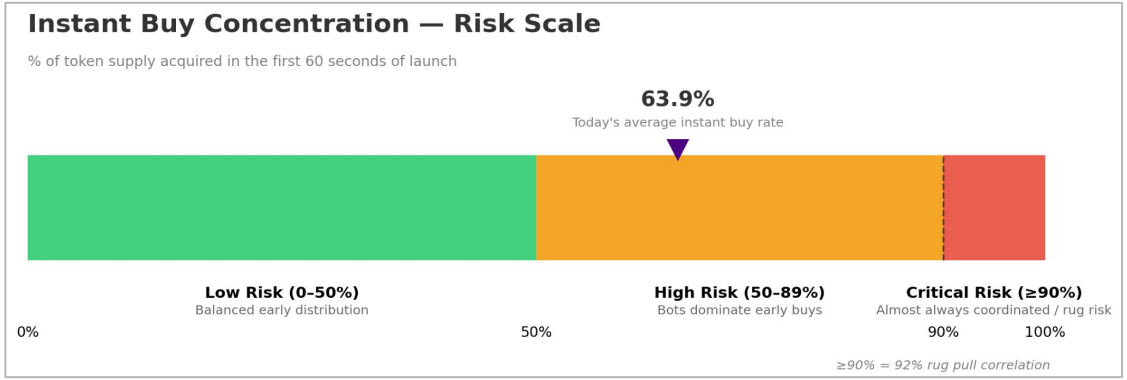
- Unify cross-chain intelligence by connecting fragmented data into one view
- Identify recurring patterns that reveal scam behaviors across every execution type
- Prevent scams before they happen by predicting and blocking fraudulent activity

Pattern #1 - Sniper Detection

The Pattern: *Sophisticated bots buy a large majority of supply within seconds of launch. Real users get excluded and launches become rigged.*

How it works:

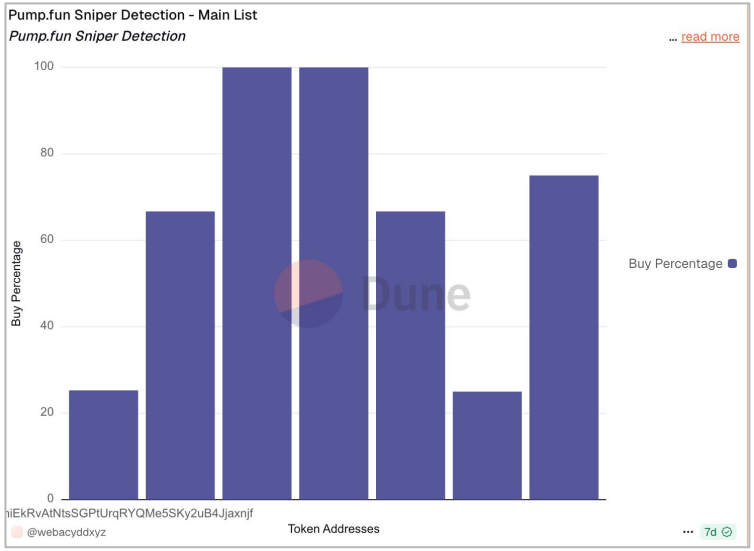
1. Launch → Bots instantly acquire >50% of supply
2. Supply concentrates in a few wallets → price control
3. Early holders dump or rug → exit profit
4. Repeat across new tokens and chains



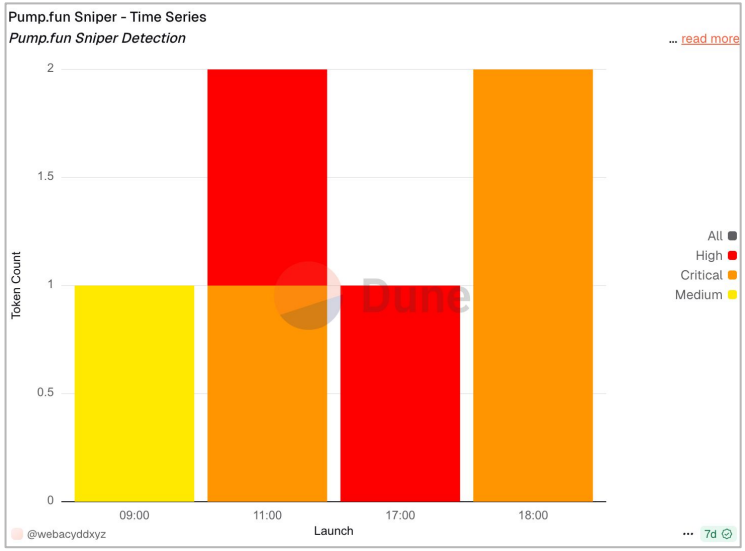
What we found

- 64% of your competition isn't human
- You're not competing against other traders → You're competing against sub-second bots
- Human reaction time = 200-300ms. Bot reaction time = <10ms
- Human reaction is no longer an edge → **it's a disadvantage.**

Token ranking



No safe windows

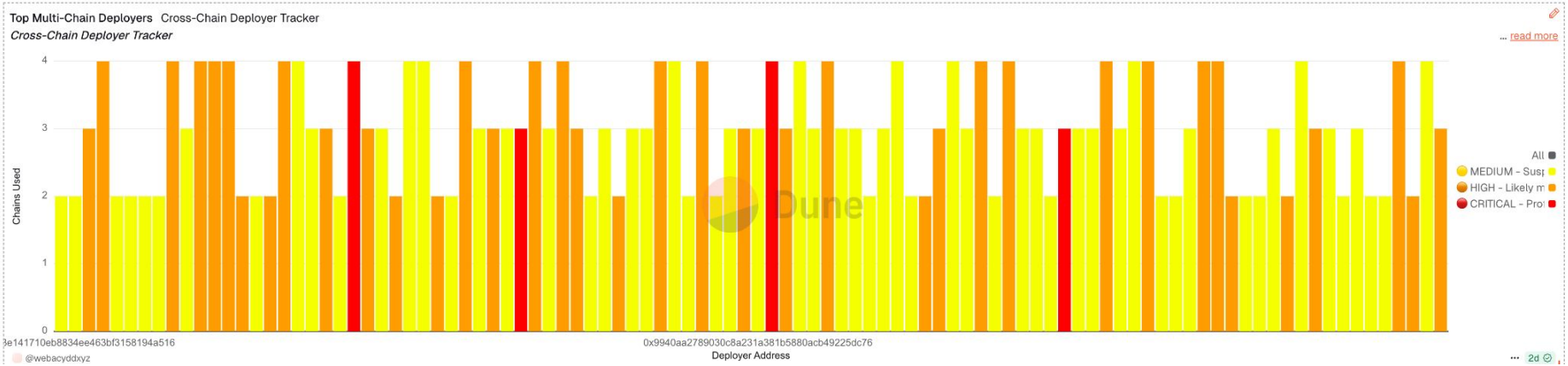


Pattern #2 - Cross-Chain Attribution

The Pattern: *Scammers migrate chains thinking new chain = new identity.*
They're wrong. Behavioral patterns persist.

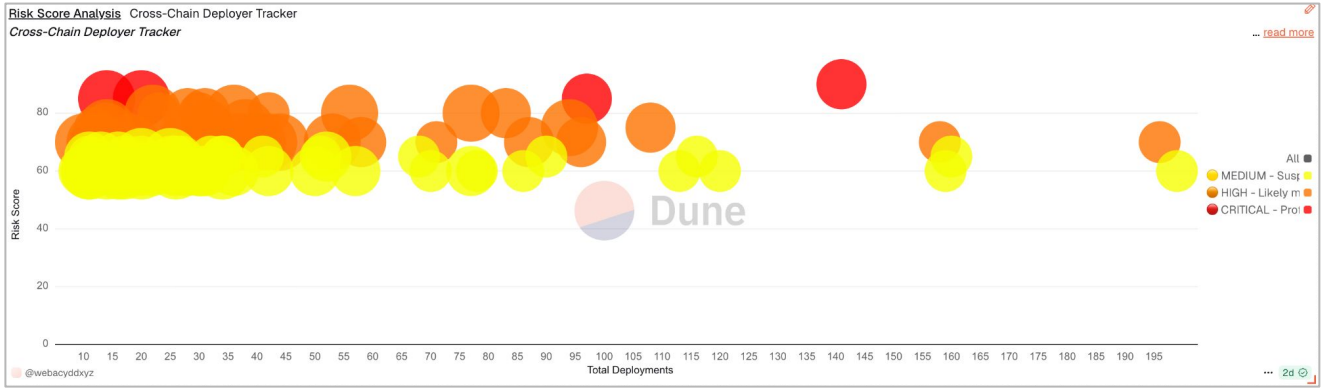
How it works:

1. Deploy on Chain A → Rugpull → Profit
2. Bridge funds to Chain B (don’t tell them but we find their fingerprints)
3. Deploy similar contract → Rugpull → Profit
4. Repeat on Chains C, D, E...

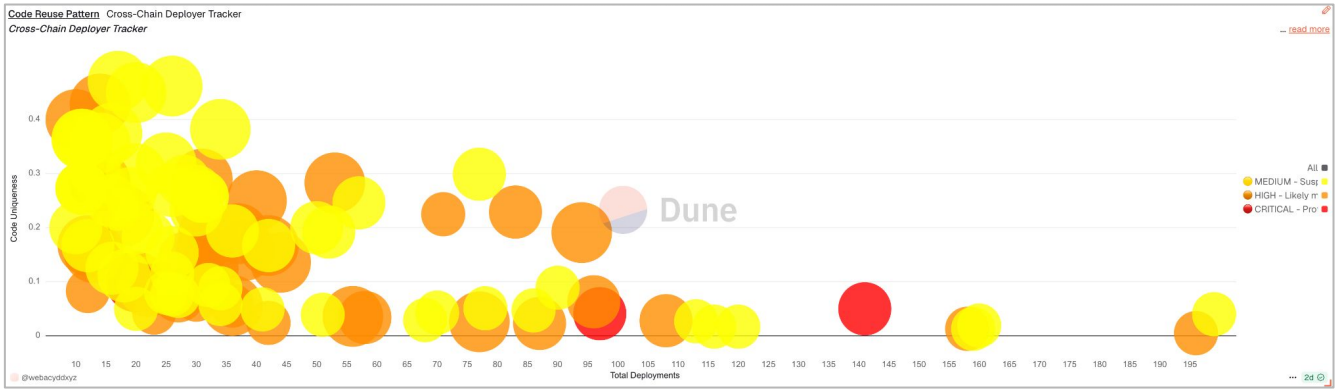


What We Caught

75–80 % success rate → most flagged deployers were later confirmed in real scams



Same deploy patterns repeat across chains → new chain ≠ new identity



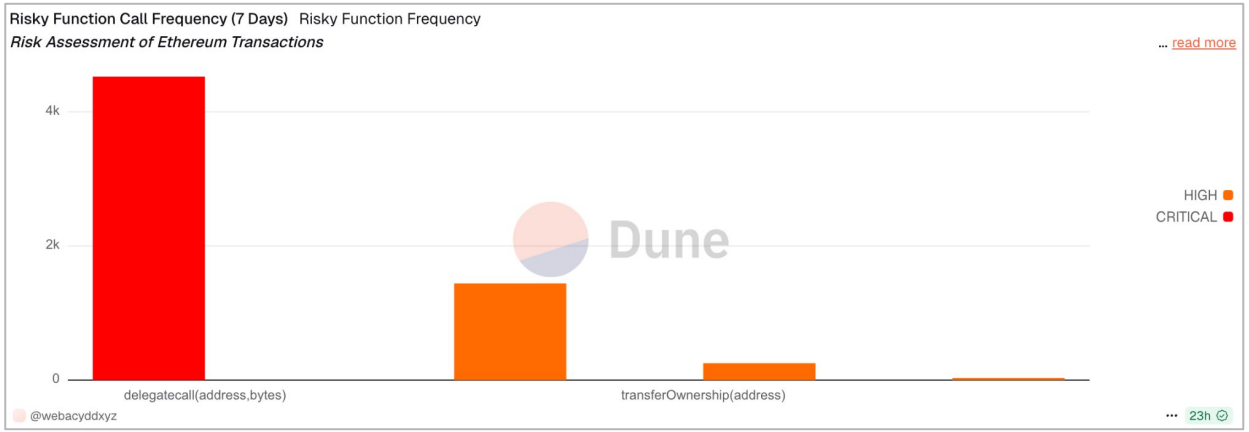
Pattern #3 - Function Signature Risks

The Pattern: *Hidden danger in smart contract calls*

Context matters:

- transferOwnership() → Medium Risk
- DELEGATECALL + transferOwnership() → CRITICAL RISK 🚨
- *Same function, different context — very different outcome.*

So What?
Over 4 000 DELEGATECALLs in 7 days
→ ~700 triggered transferOwnership()
≈ 1 in 3 of these led to confirmed exploits or rug pulls

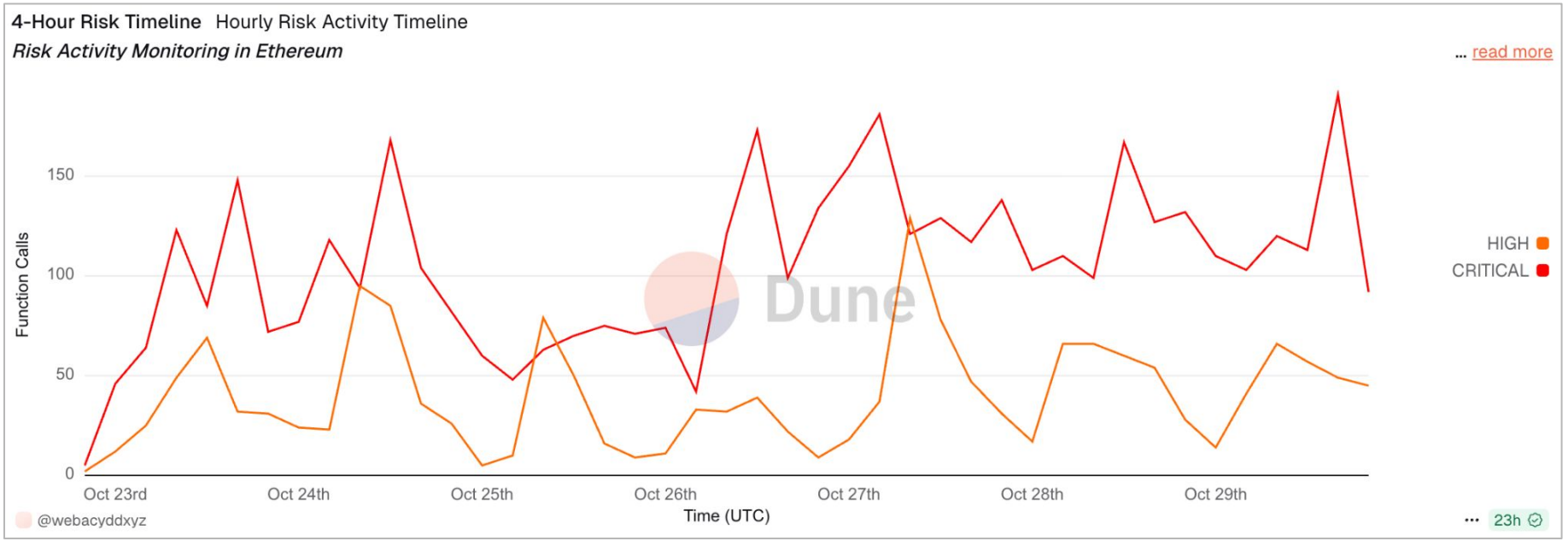


What We Caught

The Scenario: *Ledger user about to sign transaction*

👤 User sees:
"Approve token swap"
✅ Looks legitimate

🔍 Analysis detected:
DELEGATECALL → transferOwnership()
🔴 CRITICAL THREAT



Pattern #4 - Behavioral Attacks

The Pattern

Two-pronged attack using dust transactions

Reputation Poisoning

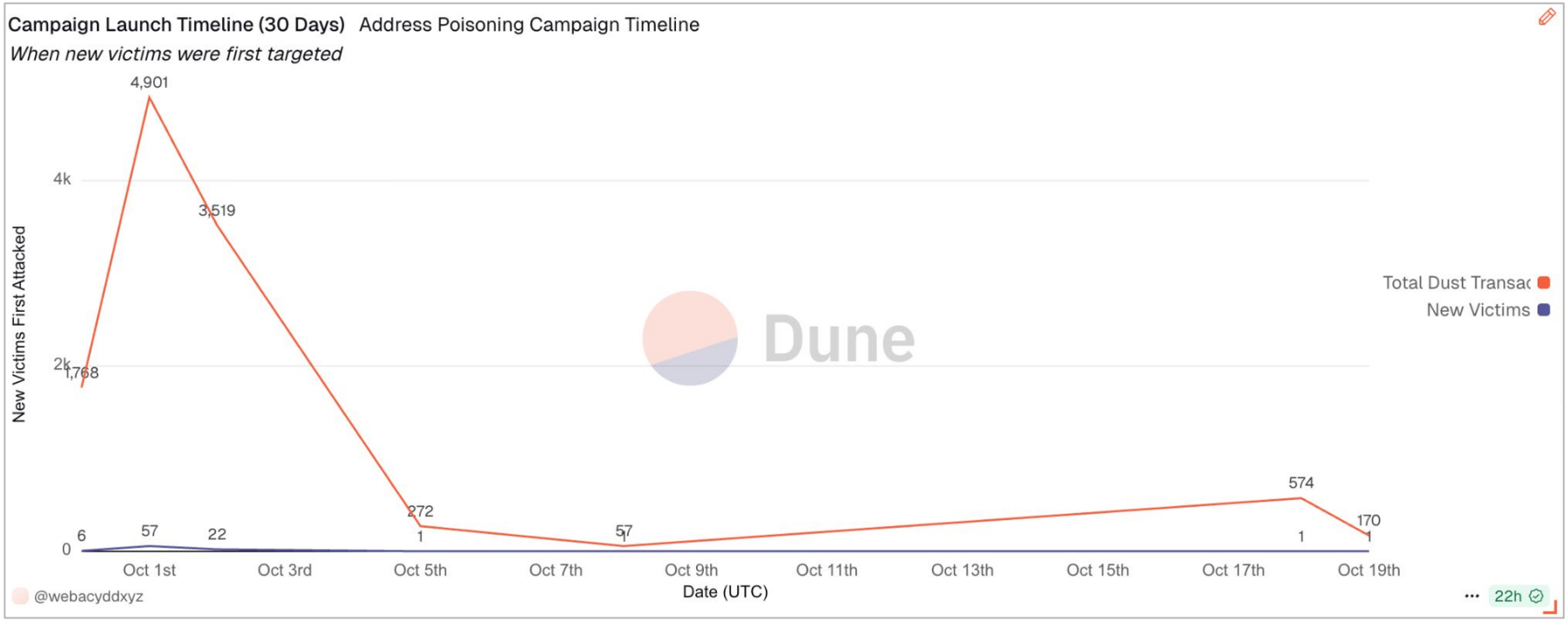
1. 200–500 malicious micro txs
2. Contaminates wallet history
3. Exchanges flag wallet → frozen

Address Poisoning

4. Lookalike “from” addresses (same first 4 + last 4)
5. User copies fake address
6. → ***Funds go to attacker***

Impact: Cheap (~$3K) • 7K victims • Permanent damage

What We Caught



Pattern #5 – Bonding Curve Concentration

The Pattern

Pump.fun's market design concentrates power — bots and scammers win, retail loses.

The mechanism

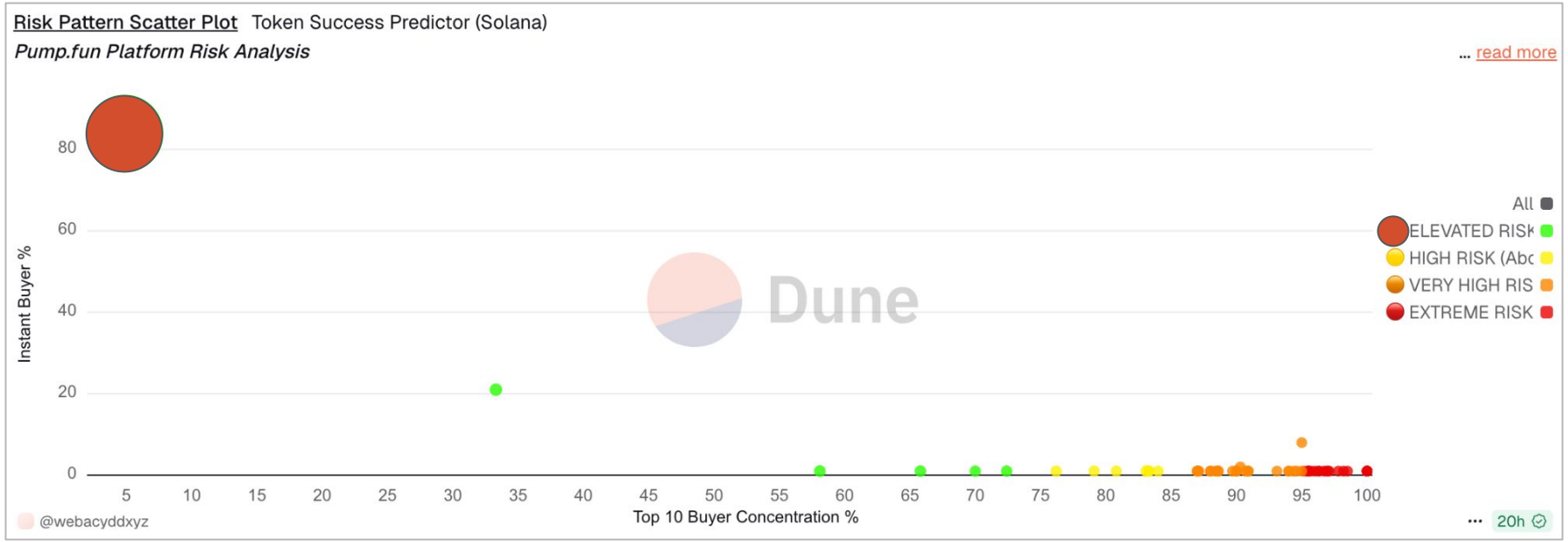
- Bonding curve favors early, large buyers
- 24/7 bot activity = no fair launch windows
- Retail participants systematically disadvantaged
- Top 10 wallets dominate liquidity & control supply

Results

- 60% of launches → >95% top-10 holder concentration
- 25% more between 85–95% concentration
- Only 5% of launches show <75% (rare on Pump.fun)
- 78% of those high-concentration tokens → rug-pulls

What We Caught

Across 300+ Pump.fun launches, risk increases sharply once top-10 buyers exceed 90% control.



Thanks!

Rodrigo Lajous

Staff Engineer

@arlequin_eth

info@webacy.com