

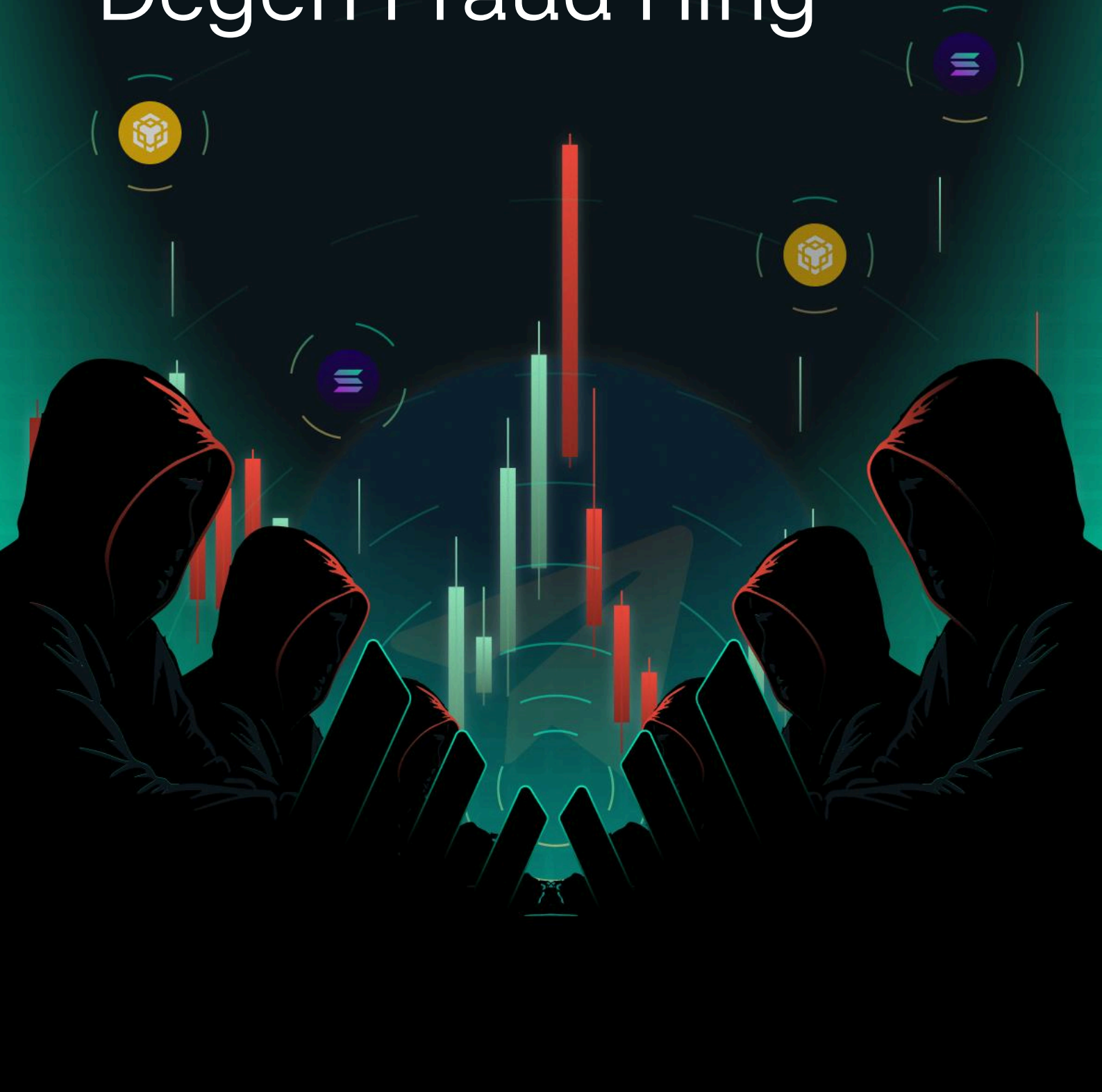
SOLIDUS
LABS



A SOLIDUS LABS REPORT
DECEMBER 2025

Crypto Pump-and-Dump

Inside a Multi-Chain Degen Fraud Ring



Introduction

Crypto pump-and-dump schemes have evolved into highly coordinated, multi-chain manipulation networks capable of generating six-figure profits within hours. Their speed, automation, and structure fundamentally diverge from manipulation patterns seen in traditional finance.

This report presents a forensic investigation into “PumpCell,” an invite-only Telegram ring of experienced crypto “degens” – risk-tolerant traders active in early-stage tokens, experimental markets, and high-volatility onchain environments. While the broader degen ecosystem often centers around speculative experimentation, the coordinated behaviors uncovered in PumpCell represent an illicit, highly structured subset of activity within that landscape.

Drawing on comprehensive, real-time analysis of smart contract deployments, onchain transaction patterns, and wallet clustering – alongside token lifecycle reconstruction and confidential chat logs, this Solidus Labs investigation provides a rare, unfiltered view of crypto-native market manipulation and highlights major supervisory blind spots for exchanges, regulators, and compliance teams.

Using the PumpCell case, this report illustrates how the permissionless nature of digital assets enables manipulation mechanics that differ fundamentally from pump-and-dump schemes in traditional finance. The differences span the manipulation life cycle, from asset creation, liquidity formation, and bot-synchronized coordination, to social-narrative propagation, and exit strategies.

Taken together, these domains form a manipulation environment that is structurally, behaviorally, and technologically distinct from TradFi markets. The report analyzes how these dynamics operate in practice, why legacy surveillance tools struggle to surface them, and how modern, crypto-native supervision must evolve. We conclude by highlighting how the most critical blind spots these schemes expose – collusion around token deployments, AMM-driven wash patterns, multi-chain money laundering, and CEX off-ramp behavior—require the type of investigative capabilities Solidus Labs routinely provides to regulators, law enforcement, and virtual asset service provider (VASP) supervision teams.

Pump-and-dump fraud rings are now multi-chain and real-time. If your surveillance stack isn't built for the digital era, maybe it's time to dump it.

PART I

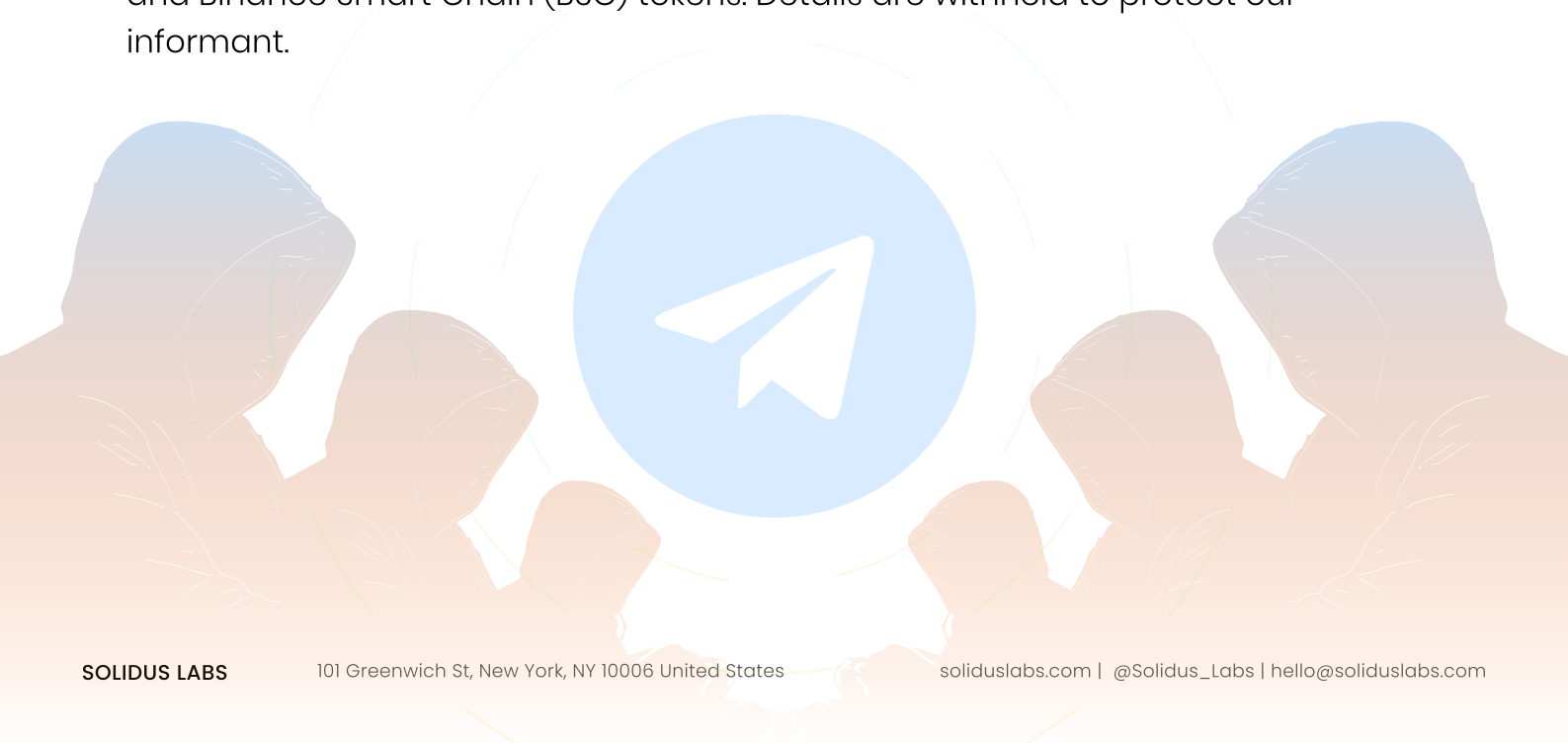
PumpCell: Inside a Multi-Chain Pump-and-Dump Ring

Pump-and-dump schemes and rug pulls have long existed in crypto, with Telegram groups playing a central role. More recently, memecoin rug pulls and scams found product market fit, with platforms like pump.fun enabling “rug pulls as a service.” Solidus Labs’ 2025 research found that 98% of tokens launched on the platform were explicit rug pulls, resulting in hundreds of millions of dollars in annual investor losses.

But what is it like to be on the “winning” side of these scams?

The premise is simple. You get together with a couple friends. If your combined wealth surpasses \$100k, you probably have enough capital to bring most newly created pump.fun tokens to levels that will trigger bot alerts and get other people to invest. As long as you can attract new buyers, you will profit. You make between \$1-3k per day on a dozen clicks. This is the life of a “trencher”. Trading meme coins is rarely profitable when you do it alone. But like so many other things, strength is in numbers. It's not a game of luck or skill, it's about manipulating other investors to buy after you.

This investigation describes how an invite-only Telegram group (codename “PumpCell”) has been orchestrating rapid pump-and-dump schemes on Solana and Binance Smart Chain (BSC) tokens. Details are withheld to protect our informant.



PumpCell: Inside The Degen Fraud Ring

Active since at least October 2024, chat logs from October 2025 reveal a coordinated operation aimed at inflating prices of micro-cap tokens, in order to later dump them for a profit. Members of the group, all seasoned in the crypto degen culture, share new tokens and deploy their own. The group's purpose is to pump token prices through coordinated buys and hype, attract unsuspecting investors, then profit by selling at the peak. In practice, their chat is filled with real-time price updates, forwardings from trading bots, and smug post-mortems of successful pumps. For example, one recent Solana token, \$ZERO, reached a fully diluted valuation (FDV) of nearly \$2 million within an hour of launch under the group's watch. Such dramatic rises, often measured in thousands of percent gains, are the hallmark of the group's activities.



Figure 1: Price chart for the ZERO token, selected by the "PumpCell" Telegram group for Pump & Dump. Source: TradingView.

Methodology Note:

This investigation draws on blockchain telemetry across Solana, BSC, and Ethereum; token lifecycle reconstruction; wallet behavioral clustering; DEX liquidity analysis; and a curated dataset of confidential Telegram chat logs. Data reflects activity from September 2024 through October 2025. Visuals included herein are produced via Solidus Labs' internal analytics tools.

Pump Playbook Overview

The playbook for deploying a token, coordinating the pump mechanics, and profiting, is well established:

- 1** **Token Launch:** Members either deploy new tokens themselves (e.g., contracts ending in "4444" for Four.meme tokens) or monitor known deployers. Relaunches after failed attempts are common, with liquidity seeded for quick takeoff. Liquidity seeding refers to the initial deposit of both the new token and a base currency like BSC or SOL into a trading pool, which enables others to buy and sell the token. The seeded liquidity determines the initial price and trading volume capacity.
- 2** **Bot-Driven Entry:** They use sniper bots (e.g., Maestro, Banana Gun) to buy the newly deployed token within seconds of liquidity opening. These bots monitor the blockchain for new token launches and automatically execute buy orders the moment trading becomes available, often faster than any human could react. This creates instant spikes – one member bragged about being "up 2x" in minutes. They also use Telegram groups like Scanners to get "tips" on the next memecoins to buy (with widely variable degrees of success).
- 3** **Fake Hype:** They spin fake narratives for their tokens using memes, cultural references, and parody accounts to bait retail. One token was hyped as "the Italian brainrot of China" to exploit the combination of viral phrases alongside absurd cultural mashups.
- 4** **Coordinated Dump:** As prices peak, insiders exit quietly while mocking those who track wallets or sell at a loss ("getting farmed"). Profits are celebrated in slang ("60 racks"). Dump timing is sensitive – distrust surfaces during exits. No one wants to be left behind or be the last to sell.

The group exploits copy traders who follow high-PnL wallets. Buying random tokens with their high PnL wallets, specifically to attract copy traders, then dumping them for guaranteed profit while copy traders are left holding worthless bags. Because copy traders always buy after someone, they are naturally at a disadvantage. It's unclear to what extent plays are coordinated with other Telegram groups, but there seem to be levels to insider information, a hierarchy among the thousands of Telegram groups operating this way. In the "trenches", the more followers you have, the more you profit.

Larping Projects and Faking Legitimacy

A signature tactic in the group is "larping" – creating or promoting tokens that impersonate legitimate projects and trending themes to lure buyers.

The members openly refer to such coins as "larps" (i.e., role-playing as something they are not). Far from being discouraged, a fake narrative is seen as a marketing tool. "I think even if it's larp it will pump," one member said optimistically while already sitting on a 4x gain. The chat history documents several parody tokens:

Mimicking Major Trends

The group launched or jumped on tokens named after popular concepts like Maneki (the lucky cat), 熊猫 (Chinese for "panda"), or even the Shanghai Composite Index. These coins have no real business behind them, but by adopting buzzy names, they attract retail traders. In mid-October, a pump of the token "上证综合指数6900" (literally "Shanghai Composite Index 6900") was deployed on BSC and immediately branded as if it were a financial derivative. The group's logs show the token skyrocketed to a \$64K market cap on FourMeme within minutes. This absurd parody of a stock index was entirely contrived – a textbook larp – yet the coordinated effort made it briefly appear "legit" to outsiders watching the volume and price spike.

Fake Profiles & Communities

Members create Telegram channels or X personas to fabricate a backstory for tokens. In chats, bot outputs link to token X searches and community pages, seeding social media with a narrative (e.g., an "intern leak" or new Binance launchpad). They role-play a genuine project, though internally they are cynical, referring to it as a "larp." They proceed because the perception of legitimacy is sufficient to draw the liquidity needed for profit. They also flaunt their wins on a dedicated X account.

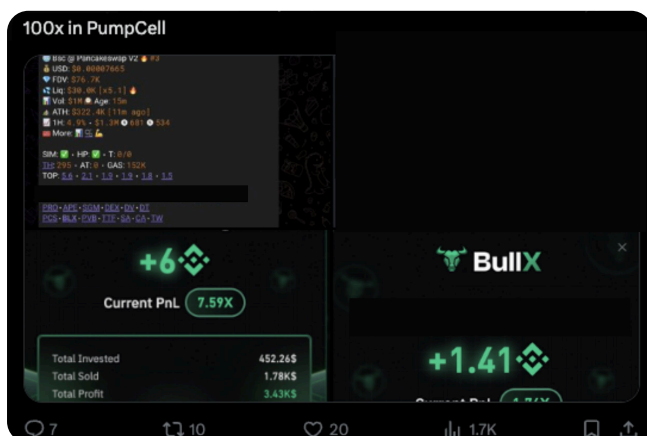


Figure 2a: Tweet boasting pump & dump wins on X.

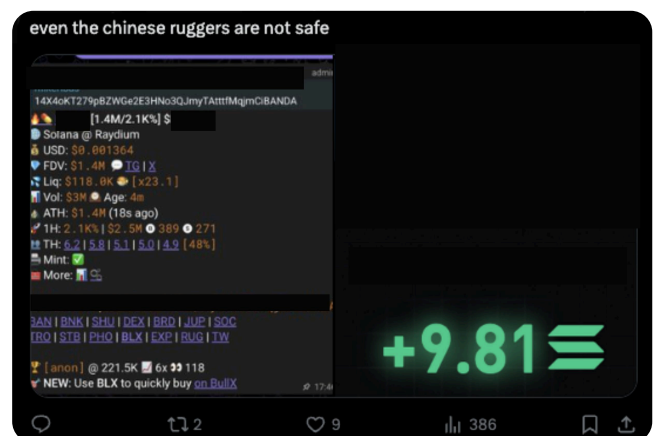


Figure 2b: Tweet boasting pump & dump wins on X.

Selected Pump Events (October 2025)

\$ZERO

Solana, Early October 2025

Token posted on Oct 3 with immediate group action. FDV surged from near-zero to \$1.9M within an hour on ~\$92K liquidity. Bots flagged \$3M volume in 44 minutes. A wallet link marked "🟡" signaled exit liquidity. The token crashed shortly after.

灵感菇 /

“Inspiration Mushroom”

BSC, Oct 9, 2025

Shilled as a viral Chinese meme. Member claimed it was "huge over there." FDV hit \$508K (+368%) rapidly. Described internally as "the Italian brainrot of China." Price dumped hours later after insiders offloaded.

SCI6900

BSC, Oct 10, 2025

Fake stock-index-themed token, relaunched by a group member after the first version was "nuked." Liquidity was bundled to push cap to \$100K within 30 minutes; ~\$60K profit claimed. The whole operation was completed in less than an hour.

According to self-reported profit and loss statements shared within the group chat, members collectively generated approximately \$800,000 in profits during October 2025 alone.

Notably, all three tokens utilized [DEX Screener's](#) paid advertising system. The paid promotions create an appearance of legitimacy that helps lure unsuspecting retail investors into what are essentially coordinated pump-and-dump operations.



Figure 3a: 灵感菇 / “Inspiration Mushroom” price chart (BSC, Oct 9, 2025). Source: TradingView.



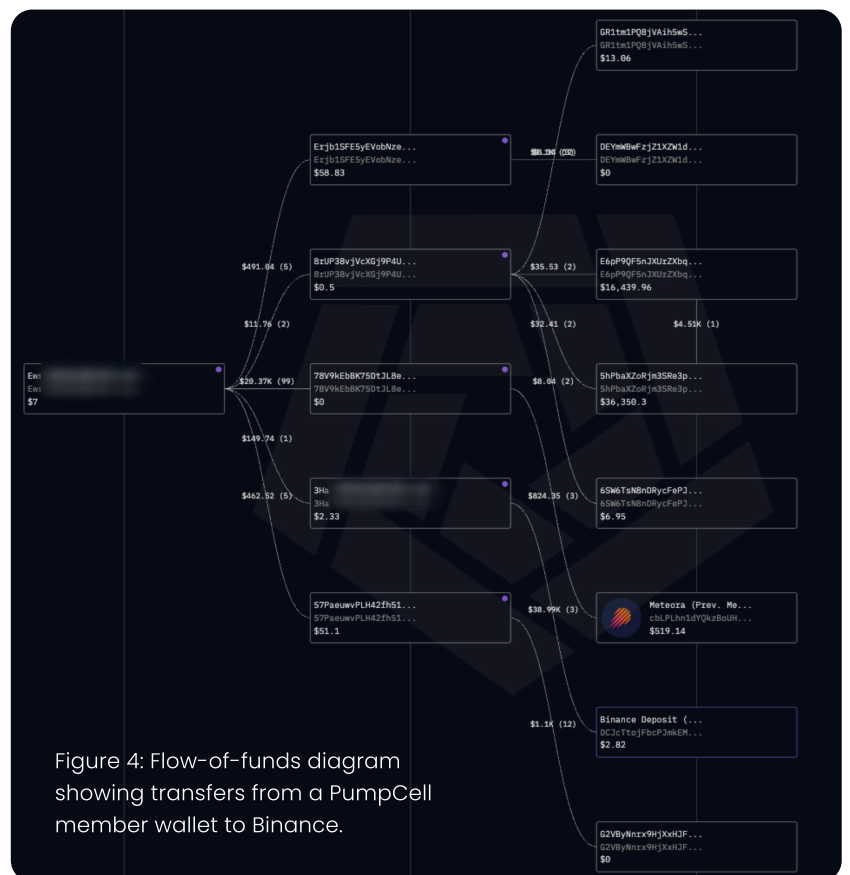
Figure 3b: SCI6900 price chart (BSC, Oct 10, 2025). Source: TradingView.

Laundering the Profits and Cashing Out on CEXs

The scammers, of course, must offboard their funds from the crypto ecosystem to realize their profits. Solidus Labs found the scammers offloaded their profits to both regulated and non-regulated (no- or light-KYC) exchanges. In fact, of the wallets analyzed by Solidus Labs, over 25% were connected to a Centralized Exchange deposit or hot wallet. Figure 3 shows an example of an address belonging to one of the PumpCell members, which offloads \$39k to a Binance deposit address.

These coordinated pump-and-dump schemes are currently major blind spots for the Trade Surveillance and AML programs of Centralized Exchanges.

This sophisticated operation extends beyond onchain manipulation and money movement to offchain money laundering. Two sources familiar with the real-world identities of these members confirmed that members regularly cash out their crypto profits through an Eastern European contact who operates an in-person OTC service, delivering physical cash in exchange for crypto transfers.



The arrangement allows the group to convert their illicit proceeds into untraceable currency while avoiding taxation and regulatory oversight. Chat logs reference meetings and cash deliveries, indicating this cash-out method is a regular part of their operational structure, further demonstrating the organized and professional nature of their illicit activities.

Group Dynamics: Overconfidence, Slang, and Suspicion

The group chat is laced with bravado, slang, and toxic humor. Members flex wins with "let's gooo" while mocking each other with slurs. They switch between English and regional European dialects, blending memes with degen lingo. Behind the jokes is clear mistrust—wallet-tracking sparks open hostility, with one insulted for "being the king of wusses" for monitoring others' trades. It's a fragile alliance of opportunists—greedy, cynical, and ready to turn on each other at dump time.

Psychologically, the chat reveals a blend of overconfidence and jaded realism. Members seem to assume that "normies" (outsiders) exist to be exploited, and they show little remorse about misleading buyers with fabricated narratives. Their confidence stems from past wins and the technical edge their tools provide. They frequently use operational slang like "larp," "deployer," "bundles," "nuke," and "rug," indicating a shared understanding of their pump-and-dump playbook. This cynicism acts as a bonding mechanism – by joking about their own scams, they normalize them within the group.

In summary, the Telegram logs paint a vivid picture of an organized pump-and-dump ring. This group leverages quick coordination, bot automation, and social media marketing to manipulate token markets on Solana and BSC. Their chats highlight patterns of behavior with clear red flags: insider trading, market manipulation, use of false information to induce trading, touting, and collusion to defraud external investors. And the involvement of off-chain, unregulated services demonstrates how digital fraud operations increasingly rely on traditional criminal networks for money laundering services.

For investigators and compliance professionals, these logs provide an unfiltered look at how illicit crypto pump-and-dump operations are run: highly coordinated, psychologically manipulative, and fueled by a mix of arrogance and opportunism. The challenge in curbing such schemes lies in penetrating this closed loop of actors who, as the evidence shows, are both highly adaptive and deeply cynical about the very markets they exploit.

PART II

The Unique Mechanics of Pump-and-Dump Schemes in Crypto vs. TradFi

1. How Crypto Market Architecture Reshapes Manipulation

PumpCell illustrates how the permissionless nature of digital asset markets fundamentally reshapes the mechanics of pump-and-dump manipulation.

In traditional markets, issuance is regulated, liquidity is intermediated, and execution is tied to account-level identity. In crypto, assets can be deployed in seconds with transferable or revokable contract ownership and permissions, deployer-controlled liquidity, and instantly reproducible contract templates. Automated market makers can replace order books, creating environments where shallow pools and bonding-curve dynamics – particularly on chains like Solana – can allow a handful of coordinated buys to generate dramatic price increases.

Sub-second sniper bots detect new token issuances and execute at speeds unattainable for human traders – a capability that, when coordinated within a pump group, helps manufacture the sharp early price spikes that create an illusion of organic momentum. By synchronizing entries in the first blocks of liquidity and acting on pre-arranged information, these bots concentrate volume, trigger automated trading alerts, and draw in copy traders and retail buyers who misread the activity as genuine demand. In traditional markets, such ultra-low-latency execution is typically confined to institutional firms operating under strict regulatory controls; in crypto, it is widely accessible to retail participants and routinely used to accelerate these manipulation cycles.

And because narratives spread through viral channels such as Telegram amplification networks, meme cycles, X bot accounts, and paid placements, social attention directly fuels price formation, liquidity depth, and volatility.

Taken together, these factors illustrate how crypto's market structure fundamentally reshapes the mechanics, speed, and visibility of manipulation compared to traditional markets.

2. Why Legacy Surveillance Tools Cannot Detect These Patterns

These structural dynamics fall far outside the assumptions embedded in legacy surveillance systems. Tools designed primarily for equities markets rely on centralized venues, account-based identity, order-book signals, and scheduled data ingestion. They are not built to interpret AMM liquidity behavior, bonding-curve dynamics, deployer-controlled liquidity, bot-synchronized trading, or multi-chain mobility. Nor can they correlate the dozens of pseudonymous wallets an actor may use across Solana, BSC, and Ethereum, or connect onchain activity to off-ramp flows through centralized exchanges, multi-hop transfers, burner wallets, and even offline cash brokers.

To legacy systems, these patterns register as isolated micro-events; in practice, they form a single coordinated lifecycle: token creation > AMM manipulation > bot-accelerated execution > social-narrative amplification > cross-chain movement > fiat extraction.

This disconnect between how manipulation operates and how legacy systems perceive it is precisely why crypto-native abuse often remains structurally invisible to traditional surveillance frameworks.

3. What Modern Supervision Must Deliver

Detecting schemes like PumpCell therefore requires a supervisory model and investigation capabilities designed for crypto's full topology and velocity. This means real-time analytics capable of interpreting AMM mechanics and bonding-curve behavior; behavioral clustering across wallets, pools, chains, and contracts; detection of bot-driven execution patterns; and unified visibility across on- and off-chain fund flows, including CEX interfaces and nontraditional cash-out channels. Without this multi-layered view, the core mechanics of crypto-native manipulation remain structurally obfuscated.

PumpCell is not an outlier - it is the operating model of modern digital-asset abuse, and it reveals the limits of legacy surveillance tools built for a different market altogether.

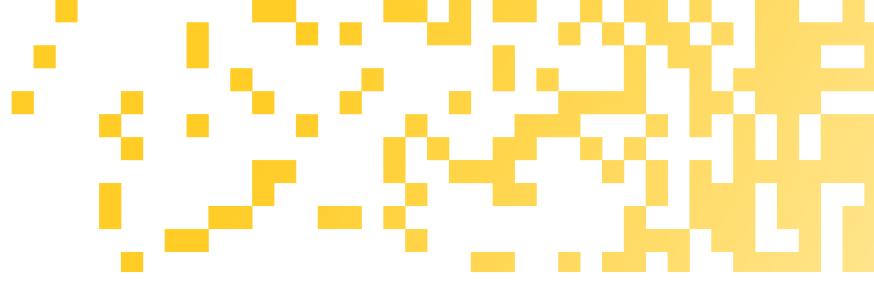
Solidus Labs' Professional Services

Solidus Labs' Professional Services team provides expert-level investigative support to global regulators, VASP supervision teams, and law enforcement agencies in uncovering complex crypto-native market abuse.

Our work focuses on reconstructing full manipulation lifecycles across chains and liquidity pools; identifying serial scam rings and recurring behavioral fingerprints; performing code-level analysis of smart contract ownership, permissions, and upgrade mechanisms; clustering pseudonymous wallets through execution patterns and interaction graphs; and tracing illicit fund flows from AMMs to centralized exchanges, no-KYC venues, OTC brokers, and offline cash networks.

By converting fragmented onchain activity into coherent, evidentiary narratives, Solidus enables supervisory authorities to establish control, intent, and monetization pathways with clarity - supporting proactive supervision in regulated and permissionless markets defined by pseudonymity, fragmented market structure, and high-velocity multi-chain activity.

SOLIDUS
LABS



Born in Crypto. Built for Efficiency Across All Asset Classes

Founded in 2018 by Goldman Sachs veterans, Solidus Labs was built with a bold vision: to merge Wall Street’s rigor, crypto-native innovation, and cybersecurity dynamics—reinventing modern compliance and unlocking exponential efficiency at scale.

At the core of this transformation is HALO, Solidus’ Agentic-Based Compliance platform, powered by Solidus’ unmatched signal depth to deliver surveillance across any venue, product, or asset class.

Battle-tested in the most volatile and fast-moving markets, HALO leverages advanced anomaly detection, agentic automated workflows, and intelligent case management to reduce alert fatigue, streamline operations, and accelerate decision-making.

Breaking free from outdated models, HALO’s detection architecture focuses on trading behavior and intent, not just static rules—leveraging diverse, cost-efficient risk signals to surface deeper, more actionable insights.

The result is surveillance that’s future-proof by design, paired with exponential efficiency—empowering scaling firms to move faster with less overhead.

Trusted by compliance teams around the world

BYBIT

CIRCLE

BitMEX

etoro

PAXOS

FALCONX

ZODIA
MARKETS

Bullish

OSL

Laser Digital
NOMURA Group

Gate.io

crypto.com

HASHKEY
GLOBAL

ARKHAM

KAIRON
LABS

KUCOIN

anchorage
digital

Learn More

Schedule a call with a Solidus expert

GET IN TOUCH

