

# Insider Trading on Decentralised Exchanges: Detecting Market Abuse On-Chain

## Executive Summary

The decentralised exchange (DEX) landscape presents a unique paradox for market integrity: while the underlying blockchain technology offers unprecedented transparency, its pseudonymous nature facilitates sophisticated market abuse. Analysis indicates that more than half (56%) of certain token listings on centralised exchanges (CEXs) show signs of pre-announcement insider trading executed via DEXs. Traditional surveillance models are insufficient for this environment as they lack the ability to bridge the gap between on-chain trading activity and off-chain confidential information. To combat this, institutions must adopt crypto-native surveillance that integrates event-based analytics, wallet attribution, and cross-market monitoring. As global regulatory frameworks like MiCA in the EU and the UK's Market Abuse Regime for Cryptoassets take effect, the shift from voluntary risk management to mandatory regulatory capability is accelerating.

## The Landscape of Market Abuse in DeFi

Decentralised exchanges allow users to trade assets directly via smart contracts without a central operator or transfer of custody. While this architecture improves technical resilience and accessibility, it creates specific vulnerabilities for misconduct.

## Key Risks and Challenges

- **Competing Characteristics:** DEXs offer transparency through public ledgers, yet pseudonymity allows traders to operate multiple wallets without opening conventional accounts.
- **The Scale of the Problem:** A 2023 study by Solidus Labs analyzed 234 ERC-20 listing announcements and found:
  - **56%** of listings reviewed (131 events) contained indicators of insider trading.
  - **411** suspected trading events were identified.
  - **105** individual wallets or wallet clusters were involved.
- **Repetitive Behavior:** More than half of the suspected entities appeared in at least two listing events, with some clusters trading before more than ten announcements.

## Access to Information

Insider trading is not limited to exchange employees. Non-public, price-sensitive information regarding token listings can be accessed by:

- Token issuers and their advisers.
- Market makers and technology providers.
- Communications agencies.
- Listing committees.

## Mechanics of DEX-Based Insider Trading

The operating model for insider trading on DEXs follows a specific sequence of accumulation and disposal. | Stage | Action || ----- | ----- || **1. Information Access** | Acquisition of non-public listing details (asset name and announcement timing). || **2. Venue Selection** | Trading on DEX liquidity pools where the token is available prior to its CEX debut. || **3. Obfuscation** | Dividing purchases across multiple wallets and routing funds through bridges or intermediary addresses. || **4. Accumulation** | Exchanging stablecoins or Ether for the target token via automated market makers. || **5. Disposal** | Selling the token into the price surge following the public CEX announcement. |

## Surveillance Evolution: On-Chain vs. Off-Chain Data

Effective detection requires a hybrid approach that reconciles transaction data with organizational records.

## Limitations of Legacy Systems

Traditional trade-surveillance systems are built for centralized order books and identifiable accounts. They often fail because:

- **Blind Spots:** A CEX might see the post-announcement sale but cannot see the pre-announcement DEX purchase.
- **Lack of Attribution:** Blockchain monitors may see trades but lack access to the confidential listing calendars and employee records needed to establish intent.

## The Crypto-Native Model

Advanced analytics, such as the Solidus Labs HALO platform, correlate on-chain token swaps with off-chain events. Suspicion is established by combining multiple indicators:

- **Timing:** Purchasing a token shortly before an announcement with no prior trading history of that asset.
- **Profitability:** Realizing material gains immediately following the news.
- **Network Links:** Shared funding sources or common destination addresses for proceeds (wallet clustering).
- **Repetition:** Recurring patterns of successful "speculation" across multiple unrelated listings.

## Regulatory Frameworks and Expectations

Regulators are increasingly treating crypto-market surveillance as a required capability.

- **United States:** Authorities have successfully prosecuted insider trading cases involving confidential CEX listing information (e.g., the Coinbase case). These cases prove that pseudonymity does not prevent attribution when wallets can be linked to exchange accounts, devices, or communications.
- **European Union (MiCA):** The Markets in Crypto-Assets regulation explicitly prohibits insider dealing, unlawful disclosure, and market manipulation. It mandates that professional entities maintain systems to detect and report market abuse.

- **United Kingdom:** The UK has finalized a dedicated Market Abuse Regime for Cryptoassets, placing gatekeeper responsibilities on trading platforms to perform on-chain monitoring.

### Distinguishing Between Types of Market Abuse

A resilient control stack must distinguish between insider trading (misuse of non-public information) and other forms of on-chain manipulation:

1. **Maximal Extractable Value (MEV):** Strategies like "sandwiching" where validators or searchers profit from influencing transaction ordering.
2. **Front-Running:** Observing pending transactions in the mempool and paying higher fees to jump the queue.
3. **Wash Trading:** Creating false volume through transactions between accounts under common control.
4. **Pump-and-Dump Schemes:** Coordinated promotion and trading to artificially inflate prices.
5. **Liquidity Manipulation:** Artificially adding or withdrawing assets to influence market confidence.

### Strategic Recommendations for Financial Leaders

To protect market integrity, financial crime leaders should implement a multi-layered control stack:

- **Information Governance:** Restrict access to listing decisions and maintain rigorous logs of who viewed confidential data.
- **Personal Dealing Policies:** Extend employee surveillance to include self-hosted wallets and DEX trading activity.
- **Cross-Market Coverage:** Connect data from CEX orders, DEX swaps, bridges, and social media activity to eliminate blind spots.
- **Wallet Clustering:** Use entity-resolution techniques to identify coordinated activity hidden behind multiple addresses.
- **Data Integration:** Combine blockchain transparency (the transaction path) with verified identities, event calendars, and external intelligence.

### Conclusion

Decentralisation does not eliminate the risk of insider trading; it shifts the venue and the nature of the evidence. By leveraging the radical transparency of the blockchain and integrating it with off-chain organizational intelligence, institutions can transform public ledger data into a defensive advantage.