Market Abuse in Crypto Markets

A practical guide to countering market abuse in crypto.

Table of Contents

Introduction

What is crypto market abuse?

If you're already familiar with crypto market abuse and compliance, move onto Page 6 where we explore solutions, specific examples, and how to efficiently surveil crypto markets.

What is crypto market abuse?

Crypto market abuse is the act of manipulating crypto markets in order to influence the price of assets and the wider market with a view to financially profiting. It can take many forms, all of which are considered unfair and illegal.

Predominant market abuse typologies in crypto

Wash Trading

At its core, wash trading is a manipulative trading practice where an entity buys and sells the same asset repeatedly to create the illusion of market activity. In a market with thousands of crypto assets, wash trading can be a way for token issuers to differentiate and a way for exchanges to increase their ranking on platforms like Coin market cap.

Insider Trading

Insider trading takes place when an individual with privileged, non-public information about a crypto asset uses it to trade unfairly, making a profit before others have a chance to react. This often involves developers, exchange executives, or influencers who gain early knowledge of an upcoming token listing, partnership, or security exploit.

Spoofing

When traders place large, deceptive orders with no intention of executing them, this is known as spoofing, and is designed to mislead other market participants about supply and demand in the order book, influencing price movements in a way that benefits the manipulator.

Front-running

Front-runninginvolves an entity exploiting privileged information to place orders ahead of others for unfair advantage. In crypto, this often happens when insiders or bots detect pending transactions on the blockchain and strategically jump ahead to profit before those trades are executed. This practice is commonly and mostly observed in DeFi markets.

Key Numbers

How much abuse is there in crypto markets?

The scale of crypto market abuse.

As the number of cryptocurrencies, innovations, and investment vehicles grows rapidly, bad actors are increasingly taking advantage of small, low liquidity assets and new technologies to manipulate market conditions and illegally profit.

The evidence supporting this trend is quickly accruing. In fact, our own research showcases the full extent of illicit activity happening in pockets across the crypto space;

While exploring a Uniswap pool we found 30% of all wallets in the pool were engaged in wash trading. The accuracy of this analysis was later confirmed by the FBI.

This is just one example, but reflects the very real nature and size of the threat.

With such exponential growth in abuse, market participants need to take action sooner rather than later, and have the necessary solutions in place to spot warning signs at market-scale, across every asset on every exchange.

Compliance

What am I expected to do?

Market abuse undermines the market integrity of crypto and actively creates distrust amongst users while hampering potential industry growth. To tackle this challenge, regulatory bodies have taken action, imposing various requirements to ensure market participants understand their role in identifying and weeding out illicit activity.

In this section, we're going to take a top-level look at the compliance expectations on exchanges and regulators.

For Exchanges

In terms of market abuse, general regulatory expectations for exchanges focus on ensuring they have the systems and processes in place to effectively monitor, detect and prevent abuse activity on their platforms.

These expectations are typically explicitly outlined in regulations, as seen by the example taken from the EU's Markets in Crypto-assets Regulation (MiCA) below:

Market In Crypto-assets Regulation (MiCA) - Article 62 - Authorisation of CASPs (5)

"Crypto-asset service providers shall establish and maintain effective arrangements, systems, and procedures to ensure compliance with this Regulation, including measures to detect and prevent market abuse."

In the event an exchange fails to develop these capabilities and is then found enabling or allowing market abuse typologies, they're often hit with severe financial penalties...

As of May 2025, penalties amounting to more than €540 million have been handed out as a result of non-compliance in crypto (Coinlaw.io).

Compliance

What am I expected to do?

For Regulators and Competent Authorities

When it comes to regulators and authorities, priorities focus on upholding the compliance regime. To achieve this outcome for market abuse, it's essential regulators have high-quality and reliable data to effectively surveil the crypto markets within their jurisdiction, oversee the licenses given, and ensure the terms are upheld.

This requirement is often enshrined in regulation, as seen by the example taken from MiCA below:

> **Market in Crypto-assets Regulation (MiCA) - Article 60 (14)**
>
> **The competent authorities shall establish and maintain effective arrangements, systems, and procedures to detect and report suspicious orders and transactions that could constitute market abuse.**

Other regulations across different regions stipulate similar requirements for overseeing authorities, and this highlights the critical role trade surveillance platforms play in maintaining market integrity.

As regulatory scrutiny intensifies, data platforms will be integral in helping regulators and authorities gain deep visibility into market activity, detect large-scale anomalies, and identify the venues facilitating them.

Kaiko's Data

How our data supports crypto market surveillance

Designed to support market surveillance solutions to bring market abuse events to light and ensure organizations can meet their compliance obligations, Kaiko's Level 1 & Level is offer the most accurate data in the market.

Developed to meet the needs of exchanges, market makers and regulators, Kaiko provides data critical for market oversight and visibility, automatically highlighting unusual anomalies and ensuring the necessary data is available to meet and uphold market abuse regulations.

"Made for crypto, inspired by traditional finance practices"

Kaiko's data

Comprehensive trade and order book data
Cross-market data (150+ exchanges) gives regulators full market oversight and trading platforms comprehensive benchmarking, eliminating blindspots.

Granular data
Available at the granular tick level, as regular snapshots, or as aggregated metrics for overall sentiment.

Holistic market surveillance
Power automated, continuous cross-market surveillance across 100+ CeFi and DeFi venues.

Insights

How data tackles market abuse?

With market abuse taking on many forms, it can be difficult to visualize exactly what's required to root them out. In this section we're going to explore a few top-level examples of market abuse typologies and how data helps compliance teams direct their investigations to identify them.

Wash Trading

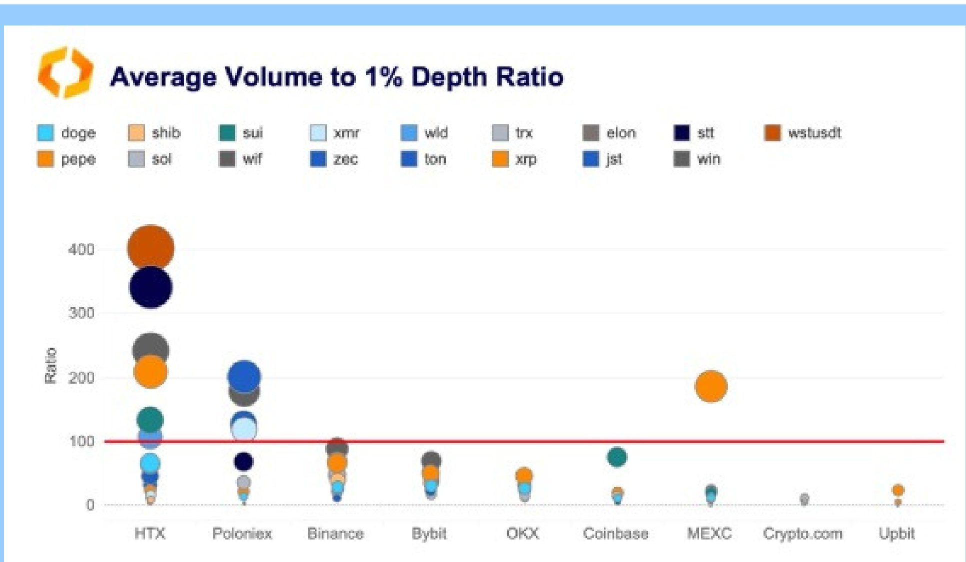
Kaiko's Level 1 & Level 2 Data plays a key role in detecting wash trading. Let's explore a few data points and how they spotlight these anomalies:

In 2019, Gotbit's CEO openly discussed his unethical business of helping crypto projects "fake it until they make it", using small exchanges incentivized to accept such practices on their platforms. Gotbit, its CEO, and two directors were also charged as part of this case, for similar schemes involving numerous cryptocurrencies.

However, despite its scale, spotting this kind of manipulation on centralized exchanges is hard. These exchanges only show order book and trade data at the market level, so it's difficult to pinpoint inorganic trading. Still, this data can be very helpful for flagging concerns by comparing trading patterns and market metrics across exchanges.

Volume-to-liquidity ratio

For instance, if trading volume significantly surpasses liquidity (1% market depth) across assets and exchanges, it might be a sign of wash trading.

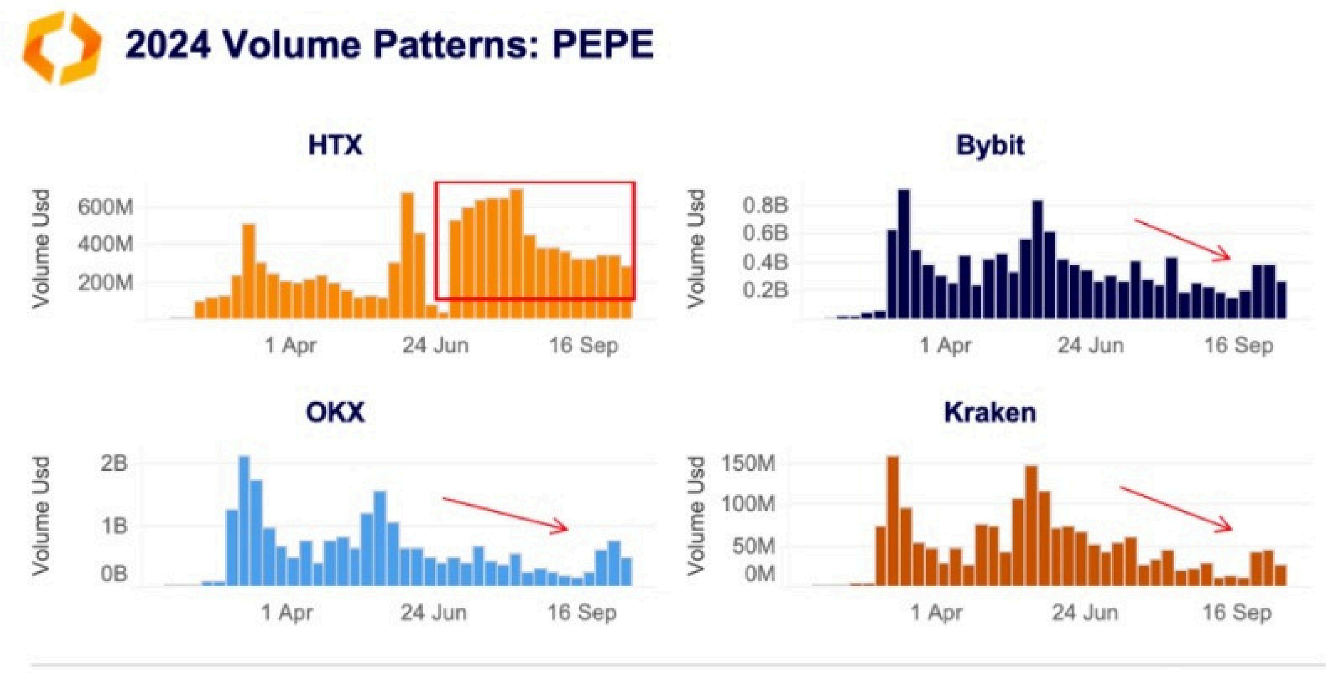


Insights

How data tackles market abuse?

The volume-to-liquidity ratio, sourced from Kaiko data, reveals that HTX and Poloniex have the highest number of assets with volume-to-liquidity ratios above 100x. We can also see that tokens such as meme coins, privacy tokens, and low-cap altcoins often show unusually high volume-to-depth ratios.

It's important to note that the volume-to-liquidity ratio is not a perfect indicator, as trade volumes can be heavily influenced by exchange programs aiming to increase volume on the exchange, like zero taker-fee campaigns. To gain confidence in artificial volume suspicions, we can use Kaiko data to examine cross-exchange correlation of volume. Volume trends tend to be correlated over long periods of time across exchanges, for an asset. Consistent, monotonic volume, periods of zero volume, or discrepancies between different exchanges can signal irregular trading activity.

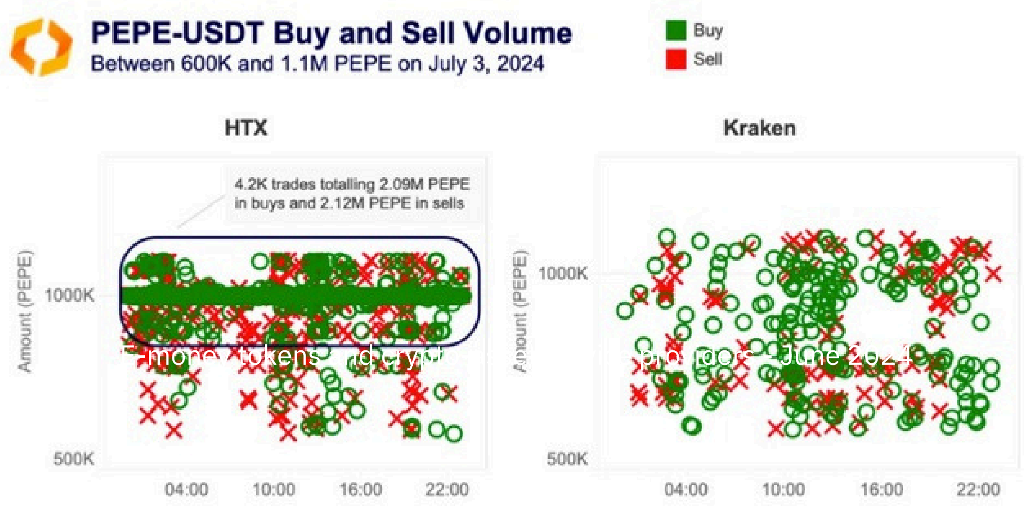


For example, in the chart above, when we look at PEPE, a token with a high trade volume-to-liquidity ratio on some exchanges, we can see big differences in volume trends between HTX and other platforms in 2024. PEPE volumes on HTX stayed high and even rose in July, while they dropped on most other exchanges.

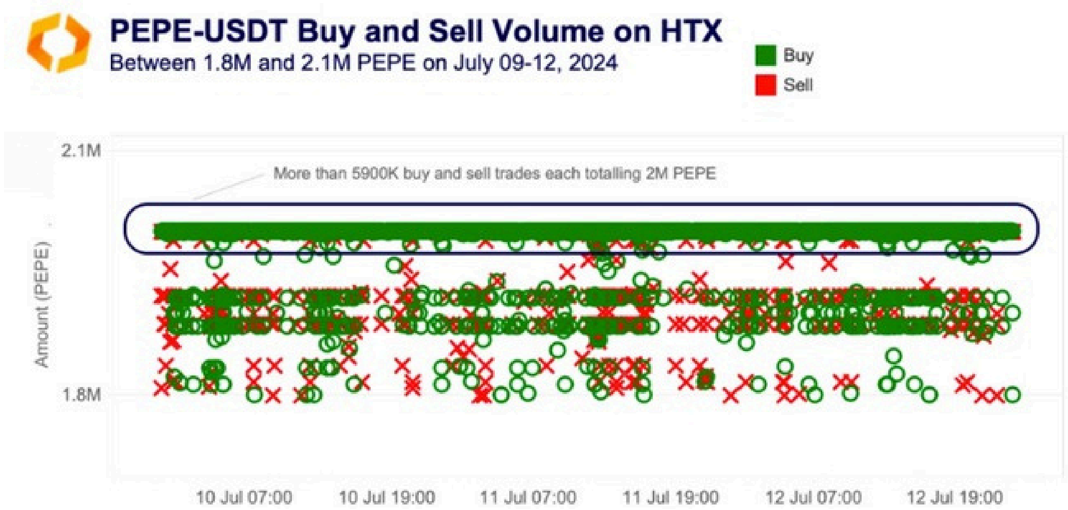
Insights

How data tackles market abuse?

Looking at more detailed trade data from Kaiko, we can see a distinct trading pattern for the PEPE-USDT market on HTX. On July 3rd, there were 4,200 buy and sell orders of 1M PEPE each within 24 hours, averaging 180 trades per hour. This pattern was unlike the trades on Kraken during the same time, which seemed more organic and retail-driven, with less uniform trade sizes and timing.



Similar patterns were seen on other days in July for the same trading pair, confirming automated trading activity. For example, between July 9-12, over 5900 buy and sell trades of 2M PEPE each were executed.



Insights

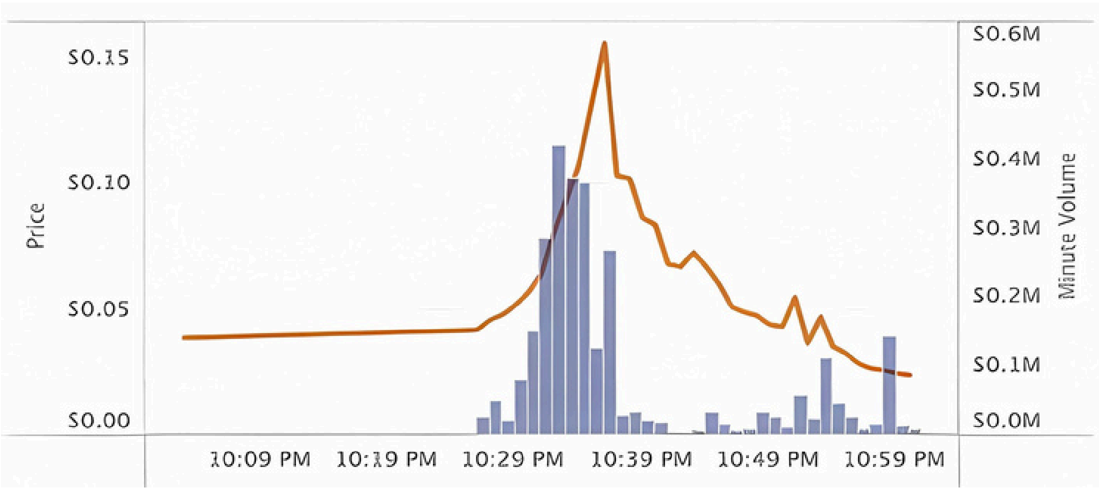
How data tackles market abuse?

Price Manipulation

Trade data available from Kaiko can be used to explore orders designed to manipulate illiquid assets and help identify cross-exchange price manipulation strategies related to oracle exploits.

Let's take a look at the Mango Markets incident to see how this works. In 2022, a manipulator opened $483 million worth of MNGO perpetual futures positions on Mango Markets, a DeFi perpetuals platform. Two minutes later, this same entity initiated large MNGO buy trades on highly illiquid spot markets, including FTX and Ascendex, driving up the price.

MNGO-USD Price & Volume on FTX
10:26 AM – 10:36 AM UTC, October 11, 2022



As a result of this activity, MNGO's price on perpetual markets on Mango Markets, determined by the oracle (calculated as an aggregate of spot market prices without outlier management), jumped over 350%. This resulted in the manipulator's long position yielding a $116 million profit, draining Mango Markets' platform. You can see exactly how this played out from our chart above, generated via Kaiko's data.

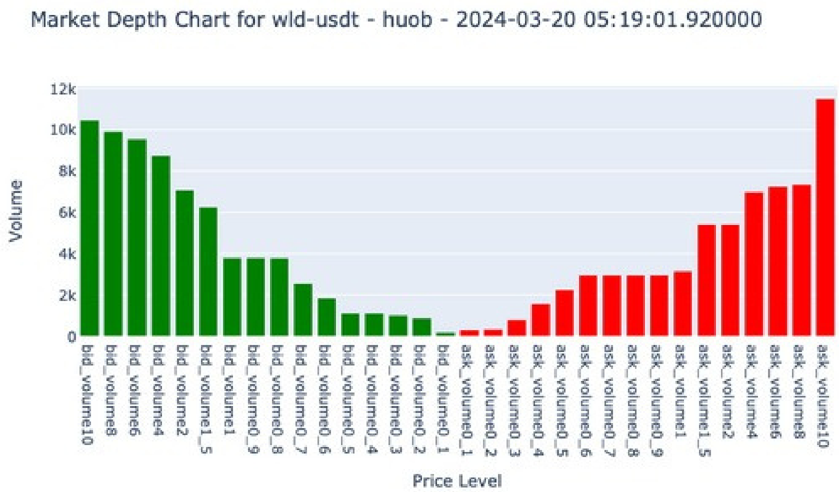
Insights

How data tackles market abuse?

Spoofing

Monitoring order books is critical to identifying the manipulative bids and asks that lie at the heart of spoofing. In many instances, this form of manipulation will display itself in the form of bid or ask walls. This is showcased in the chart generated from Kaiko data below:

As you can see this spoofing incident caused a highly unnatural bid wall to occur. Just 11 minutes later, the market returned to normal (chart below), however in that short time period, many interim trades were intiated, taking advantage of the manipulated sentiment.



Using Kaiko’s Data

Efficiently surveil crypto markets

With a clear view on the market abuse challenges facing crypto market participants and regulators, we built our data to help detect such activity and at scale. In this section, we take a closer look at how this is accomplished.

Use historical market data to systematically identify patterns, trends and anomalies: Leveraging extensive historical data, Kaiko offers your automated systems the critical baseline needed to systematically identify anomalies. This means when something unusual occurs, you have an automated system that internally justifies alerts before they go to the compliance team. This is fundamental to building an efficient crypto trade surveillance process in your organization, allowing for effective screening at scale without creating unmanageable yields of false positives.

Kaiko offers comprehensive customization options, giving you the ability to fully configure your trade surveillance system strategy and regularly adapt your screening parameters to effectively weed out false positives. This ongoing management is key to putting efficiency at the heart of your market abuse compliance strategy, and ensuring your team can focus on genuine threats.

Access continuous data for immediate market abuse detection and response: By leveraging continuous data, you can detect fraudulent activity in the moment, ensuring you can take action fast to limit any potential disruption or damage a bad actor may cause. This is particularly critical for preventing cascading effects from the original act and maintaining market integrity. This can also work as a deterrent to fraud, if market participants are aware that live market data is being screened systematically, they will likely think twice before attempting to perpetrate manipulation, particularly if they believe it will be flagged before they can get away with their gains.

Summary

Identifying market abuse in crypto markets is an ongoing battle, and as technologies and cryptocurrencies continue to evolve, the need for accurate data that can highlight suspicious market anomalies is critical. Combining data and evidence from past events will be key for exchanges and regulators to effectively identify potential market abuse behaviours, and this is where trade surveillance systems come into play.

With Kaiko's data, exchanges and market makers can not only showcase to regulators that they're meeting their compliance obligations, but also benchmark the activity on their platform to highlight alignment with the rest of the market. This plays a crucial role in alleviating regulator concerns and avoiding financial penalties that are quickly becoming commonplace for those who contravene compliance regulations.

For regulators, Kaiko provides the ability to see whats happening in the market at a top-level and investigate anomalies in the exchanges they license is key to maintaining a successful compliance regime. This visibility not only helps regulatory teams home in on venues enabling illicit activity, but also provides the critical market overview required to effectively oversee activity across their jurisdiction.

Kaiko

About Kaiko

Our data solutions serve 200+ clients worldwide, from financial institutions, to regulators, and crypto-native enterprises.

Data Feeds

Market data feeds for trading, risk management, and research.

Analytics Solutions

Proprietary data solutionsfor risk management, asset valuation, and compliance.

Monitoring Solutions

Market-level and blockchain solutions for surveillance and AML/CFT compliance.

Kaiko Indices

Crypto benchmarks built on enterprise-grade data. 24/7 infrastructure and support.

AICPA SOC

Learn more at www.kaiko.com

BMR