Countering Market Abuse

December 2022

CryptoCompare Research
research@cryptocompare.com

Market Manipulation Practices

Market integrity issues are rampant within the digital asset sector due to the relative immaturity of the industry and its decentralised and fragmented nature. Many studies have endeavoured to uncover abusive market practices that appear within cryptocurrency markets, with significant evidence found to support that these issues are prevalent. This includes:

- **Wash Trading**: A type of market manipulation in which an investor sells and buys the same financial assets simultaneously to artificially inflate activity in a market. There is evidence of wash trading in both centralised and decentralised exchanges.
- **Spoofing**: The technique by which a market participant attempts to impact the price of an asset by creating fictitious orders – a single order is quickly cancelled before it can be filled.
- **Layering** is a series of spoofs in which several orders are placed along a ladder of progressively higher (layering offers) or lower (layering bids) values.
- **Front-Running**: The act of executing a trade (either buy or sell) with knowledge that a trade or group of trades will shortly follow thereafter. In the traditional stock markets, front-running is strictly prohibited. However, in digital asset markets most data is publicly accessible. In some instances, retail users would be able to use bots to carry out front-running. Exchanges may also be able to front-run their own customers unless they maintain strong procedures to avoid such a conflict.

There are three main reasons why these issues are abundant in crypto:

- ***First***, the immaturity of the industry has meant that even centralised exchanges are not adequately regulated. Furthermore, lower-tier exchanges often take a more hands off approach at market monitoring, and so these venues are more heavily exploited.
- ***Second***, trading volumes and liquidity in crypto markets are fragmented across a plethora of centralised exchanges, resulting in smaller markets which are easier to abuse, while manipulation can be hidden within larger markets.
- ***Third***, the use of market surveillance solutions has historically not been a common practice. As per CryptoCompare's latest Exchange Benchmark, **62.4%** of assessed exchanges have a market surveillance system in place, of which only **18.1%** used an external surveillance solution. This is an area that will have to be improved if the industry is to successfully tackle market integrity issues.

Of course, there are other manipulative practices in crypto - such as phishing attacks and hacks. However, for the sake of this primer, we will focus on the four abusive practices mentioned. We now carry out a data driven analysis of these activities.

Wash Trading

There are 3 steps we take to identify wash trading on centralised exchanges:

1. Trading volumes typically spike when volatility in markets rise, i.e. a medium to high positive correlation between volume and volatility signals normal market behaviour. If there is low correlation between volume and volatility, it suggests unusual activity in trading volume. We use a threshold of < 0.1 correlation.

2. Following the above, we have to identify outliers in volume data. For example, a significant spike in monthly volumes on a given exchange.

3. Lastly, once we have identified anomalous market behaviour and a spike in volumes, we must look at patterns in trade data that deviate from the norm, such as an unusually large number of trades on one side of the book (buy or sell), or repetitive trades at the same trade size.

After deriving the volume-volatility correlation for over 100 exchanges, 23 exchanges have attained a correlation of under 0.1 over the last 100 days. A single exchange ('**Exchange A**') stands out, which reported artificial and/or erroneous volumes - $2.5tn in August 2022, up from $33.8bn the month prior.

1 hour trade data snapshots for the BTC-USDC pair on Exchange A shows non-standard behaviour on August 16th. First, 55.1% of all trades in the day take place at an extremely low trade size of 0.000001 BTC, creating the impression of a large amount of trading activity. Second, 91.1% of the transactions are sell-side trades, suggesting consistent trading against orders already in the book, a tell-tell sign of wash trading as it simplifies the process of false activity by trading against one's own orders. When comparing this snapshot to other exchanges, we see very different results, outlined in Figure 1.

Figure 1: BTC-USDC Trade Data Metrics, 16 August 2022

Exchange	% of trades at most common trade size	% of sell side trades
Exchange A	55.1%	91.1%
Bitstamp	0.59%	66.9%
Binance	0.26%	47.9%

Spoofing

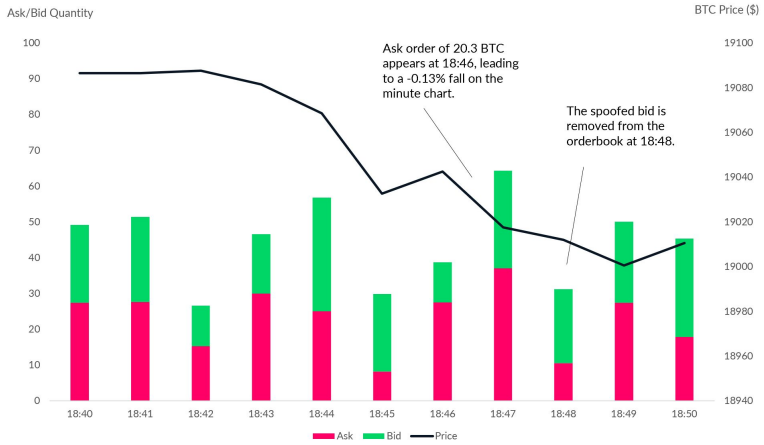
Spoofing can often be seen on larger exchanges because manipulative traders assume they can obscure their activity when more volume is present. We assume the following conditions need to be met to identify orders as spoofing:

1. The order must be unusually large to influence other market participants. Our threshold is that the order should be 10x the average trade size at that given snapshot.

2. The order should be close to the current price to influence the market. Our threshold is that the order should be placed within the 0.10% depth from the current price.

3. The order should not be filled so as to have the desired price impact on the trading pair. For instance, if the spoofed order is a bid, the price should move away from the price at which the order is placed without being filled.

Figure 2: BTC-USDT Orderbook, October 11th



In the following example, we explore the BTC-USDT order book of an exchange integrated into CryptoCompare's API. We consider any orders above 20 BTC within 0.10% depth as our threshold. On October 11, 18:00 - 19:00 GMT, the price of Bitcoin fluctuated within the $19,050 - $19,100 range.

At 18:46, a trader placed an ask order of 20.8 BTC at a price level of $19,036 while BTC was trading at $19,043. Within a minute, the price of BTC fell 0.13% to $19,018. Order book data at 18:48 shows that the ask order was removed by the trader without being filled, therefore suggesting this could be an instance of spoofing.

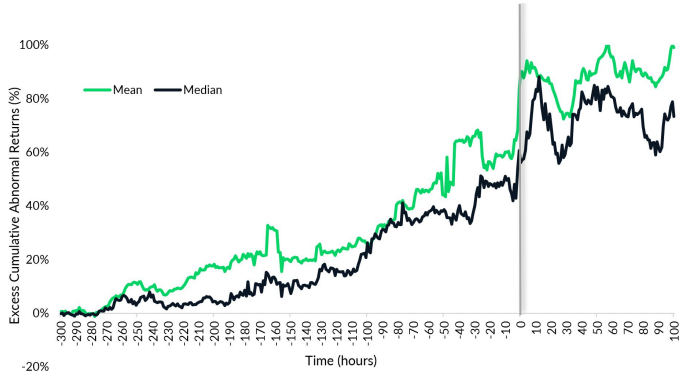
While a limitation of the above is that it is impossible to understand the motives behind such trades, if such activity occurs on a recurring basis from one trading account it is likely that it is spoofing.

Front-Running

Insider Trading has become one of the most common types of front-running in crypto, particularly within centralised exchanges. Exchange employees often have access to sensitive information that allows them to purchase a token ahead of its listing on an exchange, in anticipation of price appreciation following the listing announcement.

A study by CryptoCompare Data Analyst and PhD Candidate, Luke Johnson, identified digital wallets of individuals that traded in a manner suggesting access to significant, insider information on exchange listings. Token listings that are exploited as insider trading will typically see excess *cumulative abnormal returns (**CAR**)* in the runup to the exchange listing, which experiences a significant pump immediately following the announcement of the token listing. **CAR** measures the returns of a portfolio over and above the expected return of that asset, thus being a comparative metric against non-insider trading wallets. The analysis is illustrated in Figure 4 below.

Figure 3: Mean and Median Excess CAR for tokens traded in 4 wallets carrying out insider trading



While a Coinbase employee was charged for similar misconduct, it is important to note that these activities are widespread within the digital asset sector. The study above suggests that 10 - 25% of cryptocurrency listings will involve some type of insider trading activity. While relating to a different asset type, over the summer of 2022 an OpenSea employee was also charged for an NFT insider trading case.

On the other hand, the innate transparency of blockchains and cryptocurrency transactions means that front-running via insider information can to a large extent be identified. For example, Binance recently investigated internal transactions following allegations of potential front-running after OSMO's listing on the exchange on the 28th of October, concluding that the investigated transactions were legitimate transactions rather than insider trading.

Other types of front-running are more challenging to identify and to assess, such as the use of bots who pre-program trades based on the results of a given event. These bots may also pay larger blockchain gas fees in order to have their transaction be processed first by miners or validators.

Industry Next Steps

Market manipulation practices such as Wash Trading, Spoofing and Front-Running are detrimental to the industry's progress towards an open and fair market. By allowing these malpractices on their platforms, users may be affected by a lack of real liquidity, suffer financial losses due to spoofing, and be under a trading disadvantage due to front-running. This would only lead to increased distrust in the asset class, which should be avoided at all costs.

Due to the infancy of the industry and lack of clarity from authorities, regulations are still yet to prove their effectiveness in stopping these market manipulation techniques. For instance, spoofing and wash trading have long been deemed illegal, but such practices continue to be prevalent in crypto markets today.

However, exchanges and third-party technology companies have developed tools to address these issues and protect users. Some solutions that should be considered by the industry include:

1. **Data Availability & Quality**: Increased data transparency from exchanges makes it possible to identify market manipulation. As such, the industry should prioritise market data availability to identify and minimize malpractices like washtrading. Digital asset data providers should also ensure to carry out diligent quality assurance checks to raise data accuracy and market integrity.

2. **Use of Market Surveillance**: Trade surveillance and monitoring software are effective in identifying and alerting exchanges about suspicious transactions that could be market abuse. Exchanges may use both internally developed software as well as external providers to detect and deter market manipulation.

3. **Engage with Regulatory Bodies**: In 2022 the regulatory scrutiny on the digital asset industry has undoubtedly increased, with regulatory bodies such as the SEC investigating multiple cases of market manipulation. Others are committing to industry-specific regulatory frameworks, with the EU Council recently approving the Markets in Crypto Assets (MiCA) legislation. Exchanges should engage with regulatory bodies on a continuous basis to reach fair and appropriate legislation that does not dampen innovation in the industry.

59% *of exchanges graded in CryptoCompare's Exchange Benchmark offer the ability to query full historical trade data*

62% *of exchanges graded in CryptoCompare's Exchange Benchmark have a market surveillance system in place*

32% *of exchanges graded in CryptoCompare's Exchange Benchmark are part of an industry group that promotes best practices relating to Market Integrity, Compliance, Transparency, and more.*

Disclosures

The content found in this Report is for informational purposes only, you should not construe any such information or other material as legal, tax, investment, financial, or other advice.

This Report contains the proprietary information of CryptoCompare and its partners. It is intended to be used internally within your organization and by receiving this information, you agree that except with the prior written permission of CryptoCompare and its partners, such information shall not be used for any unauthorized purpose and shall not be published or disclosed by you to third parties, in whole or part.

The information contained in this Report, including all forecasts and projections, are provided to you on an "AS IS" basis for use at your own risk. CryptoCompare and its partners will not be responsible for any action you take as a result of this Report or any inaccuracies, inconsistencies, formatting errors, or omissions in this Report. CryptoCompare and its partners make no representations or warranties, express or implied, as to the accuracy or completeness of the information contained herein, and will not have any liability to you or any other person resulting from the use of such information by you or any of your representatives.