# The Impact of Spoofing on Bitcoin Market Microstructure

Kose John* Jingrui Li† Ruming Liu‡ Steve Yang§

March 13, 2026

**Abstract**

This paper investigates spoofing in Bitcoin order books on the Coinbase platform. Using high-frequency data, we show that order-book imbalances predict Bitcoin returns at both minute- and hourly-level horizons. We introduce a novel metric to quantify spoofing intensity and document its pronounced effect on Bitcoin prices: higher bid spoofing intensity is associated with positive returns, whereas greater ask spoofing intensity is associated with negative returns. Spoofing activity intensifies during periods of elevated trading volume, enabling spoofers to extract larger profits. Our estimates indicate that, after controlling for other factors, a one-unit increase in spoofing volume corresponds to a 27-basis-point increase in bid spoofing profit and a 55-basis-point increase in ask spoofing profit. Finally, we demonstrate that spoofing widens bid-ask spreads and deteriorates overall market quality. These findings underscore the pervasive impact of spoofing on cryptocurrency market microstructure.

***Keywords:*** *Spoofing, Bitcoin, Market Microstructure, Market Manipulation, Market Quality.*

*Leonard N. Stern School of Business, New York University. Email: kj1@stern.nyu.edu.

†Corresponding Author. School of Business, Stevens Institute of Technology. Email: jli264@stevens.edu.

‡School of Business, Stevens Institute of Technology. Email: rliu38@stevens.edu.

§School of Business, Stevens Institute of Technology. Email: syang14@stevens.edu.

Acknowledgment: We would like to thank Joel Hasbrouck for his many comments and suggestions, which have significantly improved the quality of this paper. We also thank the seminar participants at the 2025 CIE-USA/GNYC Annual Convention for their helpful feedback and insights.

# 1 Introduction

The rise of cryptocurrency markets has profoundly transformed the financial sector, introducing decentralized, borderless, and technologically sophisticated trading platforms that challenge conventional financial systems. These markets open new opportunities for investment and wealth generation, globally accessible with minimal entry barriers. However, the innovative nature of cryptocurrencies introduces significant vulnerabilities. Concerns about potential market manipulation, including practices like spoofing — where traders place large, non-genuine orders to influence perceptions of market supply or demand — are increasingly under scrutiny. This study examines the existence and impact of such activities in Bitcoin order books, aiming to explore their implications for market efficiency and price discovery processes.

Market manipulation broadly refers to trading activities undertaken with the intent to create artificial prices or a misleading appearance of market activity. The law-and-economics literature highlights intent and artificiality as defining elements of manipulation, viewing such conduct as illegal when it undermines price accuracy and market liquidity (Fischel and Ross, 1991; Kyle and Viswanathan, 2008). From a market microstructure perspective, manipulation can take trade-based, information-based, or action-based forms, each interfering with the process of price discovery (Putniņš, 2012). Common examples include wash sales, matched orders, corners, squeezes, and pump-and-dump schemes, all of which can affect the process of price discovery. Although these practices are well documented in equities and derivatives markets, comparable patterns have also emerged in cryptocurrency trading.

Cryptocurrencies like Bitcoin, known for their inherent volatility and market sensitivity, may be particularly vulnerable to disruptive practices such as spoofing in environments that are not heavily regulated.[1] This involves strategic trades that could potentially cause

[1]For an in-depth analysis of the determinants of Bitcoin volatility, including the role of retail trading, anonymity preferences, and sentiment, see John and Li (2025). They decompose Bitcoin's realized volatility into continuous and jump components, showing that innovations in Robinhood retail trading predict future continuous volatility, while innovations in Monero trading volume predict the jump component.

significant price fluctuations and be exploited for undue advantage. This paper studies the presence and impacts of such activities within the Bitcoin market, striving to comprehend their influence on market dynamics and pricing structures.

Addressing manipulative practices like spoofing in cryptocurrency markets is particularly challenging due to the platforms' unique characteristics. Unlike traditional financial markets, which benefit from well-established regulatory frameworks and transparent operational practices, cryptocurrency exchanges often suffer from inconsistent oversight and a lack of transparency. Moreover, the pseudonymous nature of transactions further complicates efforts to monitor and curb manipulative behaviors. Previous studies, such as Cong et al. (2023) on wash trading and Li et al. (2021) on pump-and-dump schemes, have underscored the vulnerability of these markets to various forms of manipulation. These findings raise concerns about how such practices might distort market prices and erode confidence in cryptocurrencies as viable investment vehicles.

Despite extensive research on market manipulation, the mechanisms and effects of spoofing in cryptocurrency markets remain largely unexplored. Spoofing – marked by the rapid submission and cancellation of orders designed to mislead other traders – can amplify price volatility, drain liquidity, and undermine market stability. This paper provides the first systematic examination of spoofing behavior in cryptocurrency markets, focusing on Bitcoin order books from the Coinbase exchange. By documenting its prevalence and market impact, we shed light on how spoofing distorts price discovery and deteriorates key market quality metrics, including bid-ask spreads and depth.

This paper makes several important contributions to the literature. First, it is the first paper to examine limit-order-book based market manipulation in cryptocurrency markets, providing a detailed analysis of spoofing on Bitcoin price dynamics and demonstrating how order-book imbalances can significantly increase returns over both minute- and hourly-level

intervals.[2] [3] Our study also examines the differential effects of bid and ask spoofing on price movements, thereby enhancing our understanding of the direct consequences of manipulative trading behaviors in cryptocurrency markets. Our findings reveal a statistically significant postive relationship between heightened spoofing activities and Bitcoin returns, underscoring the susceptibility of these markets to manipulation through strategically timed trading that challenge market integrity.

Second, we introduce an innovative methodology for detecting and quantifying spoofing intensity. Building on Hasbrouck and Saar (2013), Dimpfl and Peter (2021), and Do and Putniņš (2023), we identify spoofing episodes – ordered sequences of submissions, cancellations, and opposite-side executions that likely originate from the same trader. In the absence of trader identifiers, orders are matched by side, size proximity, and timing, with spoofing defined as large, short-lived orders canceled immediately after the execution of an opposite-side genuine trade. Spoofing intensity is measured as the time-weighted number of episodes per minute, and spoofing volume as their aggregate size. This algorithm detects high-frequency manipulation patterns in real time and, when applied to Bitcoin order books on Coinbase, effectively captures the detailed structure of spoofing behavior with broad applicability to other digital asset markets.

Third, an important contribution of this paper is the quantitative assessment of the relationship between spoofing volume and spoofing profits. In our analysis, bid spoofing profit is calculated as the return from Bitcoin's price at the end of the spoofing event relative to its price at the beginning, thereby capturing the immediate impact of spoofing on price dynamics. We find that a one-unit increase in bid spoofing volume is associated with a

[2]This paper differs from pump-and-dump manipulation studies (Li et al. (2021); see also Allen and Gale (1992); Aggarwal and Wu (2006), which document trade-based schemes that cause rapid price spikes and reversals. In contrast, spoofing relies on the submission and cancellation of limit orders to distort order-book depth and influence prices.

[3]We also build on the order flow imbalance (OFI) concept introduced by Cont, Kukanov, and Stoikov (2014) , who first documented a positive relationship between order-book imbalance and short-term price changes. OFI is defined as the net change in volume at the best bid and ask (i.e., additions minus cancellations) over a short interval, making it a one-level version of what we call "order-book imbalance." Consequently, our imbalance measure (as originally defined in Chordia et al. (2002)) is closely related to – and can be viewed as a generalization of – the OFI concept.

27-basis-point increase in bid spoofing profit, while a comparable increase in ask spoofing volume corresponds to a 55-basis-point increase in ask spoofing profit, even after controlling for various market factors. Because spoofers can lock in these gains before genuine market forces can reverse prices, spoofing yields unusually high risk-adjusted returns compared to non-manipulative strategies, which must bear full exposure to price volatility. This evidence not only illuminates the economic incentives driving spoofing behavior but also underscores its significant implications for market quality, as such low-risk, high-return opportunities can skew competition and undermine price integrity.

Last but not least, by examining the broader implications of spoofing for market quality, this study provides novel evidence on its impact on liquidity and information asymmetry. Using a difference-in-differences identification strategy, we show that spoofing activity significantly worsens market conditions by widening bid-ask spreads and elevating measures of adverse selection. These findings highlight that spoofing imposes a clear deterioration in market quality, undermining liquidity provision and impairing informational efficiency in cryptocurrency markets.

We now provide an overview of our empirical results. Our study examines the impact of spoofing on Bitcoin order books, revealing that order book imbalances significantly influence Bitcoin returns at both minute and hourly intervals. This correlation underscores the sensitivity of Bitcoin prices to manipulative trading activities, which can distort market perceptions and trigger substantial price fluctuations. We find that bid spoofing intensity exerts a positive and statistically significant effect on returns, leading to price increases, whereas ask spoofing intensity exerts a negative and statistically significant effect, causing price decreases. These findings illustrate the dual nature of spoofing, with its capacity to either inflate or depress prices depending on the direction of the spoofing activity.

Furthermore, our analysis shows that spoofing tends to intensify during normal U.S. trading hours. This pattern suggests that spoofers strategically concentrate their activities during peak periods, likely leveraging increased trading volume to obscure their manipu-

lative actions and maximize their market impact. Additionally, our results indicate that spoofers achieve higher profits during periods of elevated trading volume and price volatility, highlighting the economic incentives that drive such behavior.

Moreover, we quantitatively assess the relationship between spoofing volume and spoofing profits, providing the first systematic evidence on the short-term profitability of manipulative order-book strategies in cryptocurrency markets. Our analysis reveals that spoofers are able to extract economically meaningful profits from strategically timed spoofing episodes. Specifically, we find that a one-unit increase in bid spoofing volume is associated with a 27 basis-point increase in bid-side spoofing profit, while a comparable one-unit increase in ask spoofing volume corresponds to a 55 basis-point increase in ask-side spoofing profit – even after controlling for order imbalance, volatility, and liquidity conditions. These results indicate that spoofing creates favorable, low-risk profit opportunities by temporarily skewing market perceptions and inducing price movements in the direction of the manipulator's genuine trades. Such asymmetric returns highlight the incentive structure behind spoofing, distinguishing it from conventional trading strategies that must bear full exposure to market volatility.[4]

Lastly, our findings reveal that spoofing activities exert detrimental effects on market quality, consistent with Fox et al. (2021). The difference-in-differences estimates in Table 8 show that during spoofing episodes, larger spoofing orders significantly widen bid–ask spreads, increase $VPIN$, and raise percentage quoted spreads. These effects highlight that spoofing heightens adverse-selection risk and discourages liquidity provision, as market participants respond to manipulative order flow by demanding greater compensation for trading. Overall, spoofing produces pronounced distortions in market quality, marked by wider spreads and elevated $VPIN$, underscoring its disruptive role in cryptocurrency markets.

The rest of the paper is organized as follows: Section 2 reviews the relevant literature,

[4]In this sense, spoofing profits resemble quasi-arbitrage gains: traders exploit transient mispricing that they themselves create through artificial order-book pressure, earning short-term returns with limited downside risk. These self-generated arbitrage conditions arise not from market inefficiency per se, but from deliberate microstructure distortions that temporarily dislocate prices from fundamental value.

offering a foundation of theoretical and empirical insights; Section 3 details the data used in the analysis; Section 4 examines the impact of order imbalance and order book imbalance on Bitcoin returns, establishing the market microstructure framework that underpins our analysis; Section 5 details our novel methodology for detecting spoofing in Bitcoin order books, including the algorithm for identifying strategic spoofing in the absence of explicit trader identifiers; Section 6 investigates the effects of spoofing on market outcomes, highlighting its influence on Bitcoin returns and overall market quality; Section 7 explores the economic incentives of spoofing by quantifying the relationship between spoofing volume and spoofing profit; Section 8 presents robustness tests of our measures, including analyses of abnormal order cancellations and trades opposing quotes; and Section 9 concludes.

## 2 Literature Review

This section provides an overview of the existing literature on market behaviors in cryptocurrencies, highlighting practices that are potentially indicative of manipulation across various cryptocurrency exchanges, often in environments with limited regulatory oversight. For instance, Cong et al. (2023) analyze wash trading activities, noting that a significant portion of reported volumes on some unregulated exchanges may not be genuine. This could potentially distort market rankings and affect prices, posing risks to investors and market stability. Li et al. (2021) examine instances of pump-and-dump schemes, finding that coordinated actions, possibly on platforms like Telegram, can lead to short-term price spikes followed by sharp declines, potentially resulting in wealth shifts from uninformed to more informed market participants. Further studies, such as those by Li et al. (2022), explore vulnerabilities within decentralized finance (DeFi) platforms, discussing incidents in the meme token markets that resemble "rug pull" schemes, where liquidity is suddenly withdrawn, possibly leaving investors with worthless assets. These contribute to an understanding of the complex dynamics at play in both centralized and decentralized cryptocurrency markets.

Spoofing, a practice well-studied in traditional financial markets, has significant implications for cryptocurrency markets. Do and Putniņš (2023) have developed empirical techniques to detect spoofing by analyzing patterns such as high quoting activity, abnormal order cancellations, and cyclical fluctuations in market depth. These indicators, validated by cross-market data, provide high detection accuracy and are fundamental for identifying spoofing behaviors in Bitcoin order books. Additionally, Dimpfl and Peter (2021) note that cryptocurrency exchanges exhibit higher market microstructure noise than traditional markets, complicating the detection of price manipulation. Furthermore, Khomyn and Putniņš (2021) discuss how automated market-making strategies can lead to high order cancellation rates, which may sometimes indicate manipulative behaviors like spoofing.

The literature provides extensive documentation on the behavioral aspects of spoofing and other manipulative strategies across different markets. Lee et al. (2013) examine how traders on the South Korea Exchange exploited order disclosure rules to profit from creating artificial order book imbalances. Although specific market structures and regulations differ, their findings on the profitability and impact of spoofing are relevant to cryptocurrency markets, where similar behaviors may arise in the absence of stringent disclosure requirements. Stenfors et al. (2023) provide insights into cross-market spoofing, demonstrating how manipulators exploit relationships between closely related markets to execute spoofing strategies. While their focus is on foreign exchange markets, the methods and findings have implications for cryptocurrencies, particularly given the interdependencies among various crypto assets.

The broader implications of market manipulation extend beyond individual trading strategies. Griffin and Shams (2020) reveal how the issuance of unbacked Tether tokens inflated Bitcoin prices during the 2017 cryptocurrency boom. Similarly, Foley et al. (2019) document the substantial involvement of cryptocurrencies in illegal activities, emphasizing the need for robust regulation to curb abuses. These studies underscore the interconnectedness of manipulation, market dynamics, and regulatory challenges in cryptocurrency markets. Several studies examine the intricacies of order book dynamics and their relationship to

market quality. Chordia et al. (2002) and Chakravarty (2001) investigate order imbalances and stealth trading in traditional markets, respectively, providing insights into how trading behaviors influence liquidity and price discovery.

Khomyn and Putniņš (2021) and Fox et al. (2021) further explore the order cancellations and their implications for market quality. While legitimate high cancellation rates may result from market-making activities, spikes in these rates can indicate manipulative intent, such as spoofing. These findings provide critical context for examining order cancellation patterns in Bitcoin order books. Together, this body of literature underscores the importance of understanding and mitigating spoofing behaviors to preserve the integrity and efficiency of cryptocurrency markets. This paper builds on these insights to investigate the prevalence and impact of spoofing in Bitcoin order books, contributing to the broader discourse on market manipulation in the rapidly evolving landscape of cryptocurrency trading.

The literature on spoofing and market manipulation has evolved significantly, especially on the ethical dimensions. Heinz (2017) argues that ineffective regulation not only exacerbates market inefficiencies but also raises serious ethical concerns regarding fairness and transparency. Aitken, Aspris, Foley, and de B. Harris (2018) explore the interplay between market fairness and efficiency in the context of algorithmic trading, highlighting that while increased automation can enhance transactional efficiency, it also elevates the risk of manipulative practices that undermine ethical standards in financial markets. MacKenzie (2022) critically examines spoofing within futures trading, focusing on the moral implications of delineating between legitimate trading strategies and deceptive manipulative tactics. Hersch (2020) contends that spoofing – placing orders without intent to execute to create a false impression of demand – is morally impermissible, as it fundamentally differs from acceptable forms of bluffing in poker by undermining the critical economic role of speculative trading. This ethical debate is further advanced by Khorasanee (2024), who controversially defends spoofing as a form of market bluffing, although this view is countered by arguments that such practices violate fundamental ethical norms of market conduct. Complementing these

discussions, Cartea, Jaimungal, and Wang (2020) and Tao, Day, Ling, and Drapeau (2022) provide quantitative models that not only analyze the impact of spoofing on price manipulation and market microstructure but also draw attention to the ethical costs associated with market deception. Wang and Wellman (2017) use an agent-based approach to demonstrate how spoofing distorts prices and diminishes market surplus, challenging the ethical integrity of financial markets

Extensive research has examined high-frequency trading (HFT) strategies, known for their rapid response to market events, and their potential implications for cryptocurrency markets, drawing insights from their established role in traditional financial settings. According to Hasbrouck and Saar (2013), low-latency trading improves traditional market quality measures by decreasing spreads and reducing short-term volatility – factors that may also influence the dynamics of cryptocurrency markets. Further, Brogaard et al. (2014) show that HFTs facilitate price efficiency in traditional financial markets by trading in the direction of permanent price changes and countering transitory pricing errors. This behavior, observed both under average conditions and on highly volatile days, is primarily driven by liquidity-demanding orders. Additionally, their paper reveals that the direction of HFT trading correlates with public information, such as macroeconomic announcements and market-wide movements, and predicts short-term price changes. Beyond these seminal works, a large body of research explores various HFT pairs and strategy classes – such as cross-asset arbitrage between equities and futures, latency-driven market-making in options and FX, and statistical arbitrage among correlated securities – each illustrating how high-frequency interactions transmit information and liquidity shocks across venues. These interlinked HFT activities underscore the complex, multi-asset ecosystem of modern electronic trading, offering a useful benchmark for understanding emerging forms of algorithmic and manipulative behavior in cryptocurrency markets.

# 3 Data

Our Bitcoin data is level 3 data, including all trades, fills, adds, cancels, and modifications of trades and quotes for transactions on Coinbase. We obtained the data from Kaiko. In addition to the level 3 data, we also obtained order book snapshot, which provides snapshots taken every 25 seconds. The snapshot data comprises the best five bid and ask prices along with their respective sizes. This comprehensive dataset spans 24 hours a day, 7 days a week, covering the period from January 1, 2024, to March 31, 2024.

Certain market imbalance measures can be calculated according to established conventions. Order imbalance is defined as the difference between the number of buyer-initiated trades and seller-initiated trades. Similarly, order book imbalance is calculated as the cumulative size of the top five bid orders minus the cumulative size of the top five ask orders. Market quality is evaluated using metrics such as the Roll measure, the volume-synchronized probability of informed trading, and the percentage quoted spread. Volatility is assessed based on the executed trade prices of Bitcoin. We also introduce spoofing intensity and spoofing volume as measures of spoofing activities in the market. These metrics rely on an algorithm to match orders submitted by the same trader, which will be discussed in detail in a later section.

# 4 Bitcoin Order Imbalance and Order Book Imbalance

Traditionally, trading volume serves as a critical link between trading activity and returns. Chordia et al. (2002) define order imbalance as the difference between the number of buyer-initiated trades and seller-initiated trades, demonstrating that daily order imbalances significantly influence returns on the New York Stock Exchange.[5] Similarly, in the Bitcoin market, we observe that the impact of order imbalances remains pronounced across various

[5]See Cont, Kukanov, and Stoikov (2014), who define order flow imbalance (OFI) as the net change in volume at the best bid and ask (additions minus cancellations) over a short interval. Order-book imbalance, as used in this paper (and as originally defined in Chordia et al. (2002)), generalizes OFI by aggregating depth and executed volume across multiple price levels and/or longer horizons.

time intervals.

*[Insert Table 1 Here]*

Table 1 presents the effect of order imbalances on Bitcoin returns. To examine their relationship, a signed measure of order imbalance is used to capture the distinction between excess buying pressure and excess selling pressure. Accordingly, order imbalance is divided into positive and negative components, which are included as separate regressors in the analysis.

We report results across five different time intervals, ranging from 1 minute to daily. Our primary focus is on the 1-minute interval, where the findings reveal that contemporaneous order imbalance (OIB) has a highly significant impact on market returns in the expected direction: excess buy (sell) orders push prices up (down). Additionally, lagged order imbalance exhibits a significant negative effect on contemporaneous returns, consistent with the inventory stabilization hypothesis proposed by Chordia et al. (2002). This suggests that previous imbalances tend to reverse, thereby exerting a negative influence on current returns. The results are similar for other scenarios with longer time intervals.

In addition to the impact of order imbalance—reflecting the buy and sell imbalance of executed trades—the imbalance of unexecuted quotes on the limit order book may also influence traders' decisions and, consequently, affect Bitcoin returns. Do and Putniņš (2023) highlight that order book imbalances can be strategically used by manipulator to create a false impression of buying or selling interest, thereby influencing other traders' actions and market prices. To quantify the imbalance of unexecuted quotes on the limit order book, we define order book imbalance (OBIB) as the cumulative size of the top five bid orders minus the cumulative size of the top five ask orders. We estimate a regression that examines the relationship between Bitcoin returns[6] and order book imbalance.

*[Insert Table 2 Here]*

[6]Bitcoin returns are calculated as the percentage change between the opening and closing prices over the specified period.

In Table 2, Column 1, the results indicate that 1-minute level unbalanced buying quotes positively impact contemporaneous Bitcoin returns, while unbalanced selling quotes drive returns downward. Furthermore, lagged unbalanced quotes exhibit a reverse effect on contemporaneous returns, suggesting a corrective mechanism in response to prior imbalances. In Column 2, we include order imbalance and lagged returns as control variables. The results remain consistent and significant, with one exception: the coefficient for lagged unbalanced selling quotes is not statistically significant, although it retains the expected sign. The impact of hourly order book imbalance follows similar patterns, as shown in Columns 3 and 4. These results indicate that the imbalance of unexecuted quotes can influence Bitcoin prices, highlighting a potential strategy for manipulators to affect market prices without executing orders.

# 5 Detection of Spoofing

Spoofing is a prominent form of market manipulation in which traders submit non-genuine orders with the intent to create a false impression of market depth or directional pressure and mislead other participants about true supply and demand conditions. In this section, we introduce the algorithm used to detect spoofing activity and measure its intensity. Lee et al. (2013) utilized trader identifiers from the South Korea Exchange to match the sequential behaviors of individual traders. Their study examined how traders exploited order disclosure rules to profit by creating artificial imbalances in the order book. However, Coinbase does not provide trader identification numbers in its trade or quote data, making it impossible to perfectly match trades and quotes to the same individual trader. To address this limitation, we adopt the methodology of Hasbrouck and Saar (2013), which identifies "strategic runs" as patterns of sequential trading activity likely originating from a single trader, and develop an algorithm for detecting "strategic spoofing." To construct a measure of spoofing activity, we start by identifying "strategic spoofing," defined as linked patterns of spoof order submissions,

cancellations, and the execution of opposite-side genuine orders that are likely initiated by the same trader.

In particular, our "strategic spoofing" is constructed as follows. The order sizes accompanied with the data unambiguously link an individual limit order submission with its subsequent cancellation or re-submission. Since our data lack trader identification numbers, our algorithm inevitably introduces some noise in the detection of spoofing activity. However, on Coinbase, the minimum trade size is $1 \times 10^{-8}$ Bitcoin, allowing traders to submit nearly any trade size, unlike stock traders with more rigid size constraints. This flexibility in trade size enables us to confidently link order messages from same trader, even in the absence of explicit trader identification numbers. The simplest form of strategic bid spoofing involves four messages: the submission of an ask limit order that the manipulator intends to execute, the submission of a spoofing bid limit order designed to influence the market price but not executed, the execution of the ask limit order, and the cancellation of the spoofing bid limit order. In practice, the size of the spoofing order is not necessarily equal to the size of the executed order. Spoofing orders are typically larger in size as their purpose is to create an imbalance in the order book and influence the market price. Our algorithm matches spoof order submissions, cancellations, and re-submissions based on order size. To link these spoof orders to an executed, opposite-side genuine order, we verify that the closest executed order before the final cancellation of the spoof order is on the opposite side of the order book and was submitted within one minute prior to the onset of spoofing activity.

*[Insert Table 3 Here]*

Table 3 illustrates an example of bid spoofing, showing a spoofing series with a spoofing size of 0.038 Bitcoin. The manipulator places the genuine ask order at time $T_0$. Beginning at time $T_1$, the manipulator initiates spoofing, submitting, canceling, and re-submitting orders repeatedly until the genuine ask order is executed just before the final cancellation of the

spoof order at time $T_n$.[7]

*[Insert Figure 1 Here]*

In Figure 1, we plot an example of a bid-spoofing manipulation that occurred on March 8, 2024, from 15:39 to 15:42. The blue dots represent the placement and cancellation of spoofed bid orders. The red dot indicates the execution of the opposite order. The green dots represent the execution of all bid and ask orders during this period. The solid and dotted lines show the level-1 bid and ask prices, respectively. The red bars indicate the sizes of executed orders during this period. In this example, we observe that the manipulator pumps the price from \$67,500 to \$68,200, during which the genuine order is filled.

*[Insert Table 4 Here]*

We report summary statistics of spoofing activities in Table 4. Each spoofing event is categorized by its length, measured by the number of revision orders. "Spoofing time" denotes the duration from the submission of the initial spoofing order to the cancellation of the final spoofing order, while "cancellation time gap" refers to the interval between consecutive revision orders. "Spoofing size" indicates the volume of spoofing orders, and "genuine order size" denotes the volume of the corresponding genuine orders. Table 4 shows a positive correlation between spoofing time and spoofing length: operations with multiple revisions tend to last longer. The distribution of cancellation time gaps is highly skewed: although the average gap ranges from 6 to 26 seconds, the median is below one second, indicating that most spoofing orders are cancelled almost immediately. Finally, spoofing orders are approximately three times larger than genuine orders, consistent with the notion that spoofers submit large orders to create order-book imbalances and influence market prices.

In conclusion, spoofing runs are generally short and characterized by rapid cancellations, as evidenced by the highly skewed cancellation-time distribution with a median gap under

[7] In our analysis, we focus on spoofing episodes whose duration ($T_n - T_1$) is below the 80th percentile (55 minutes) to eliminate extreme-value considerations.

one second. These patterns underscore the high-frequency nature of spoofing manipulations. Moreover, spoofing orders are, on average, three times larger than genuine orders, highlighting that manipulators submit unusually large volumes to distort order-book depth and influence price formation.

# 6 Spoofing and Its Impact

## 6.1 Spoofing Intensity and Bitcoin Returns

In the previous section, we introduced the algorithm for detecting spoofing activity. In this section, we now convert the detected spoofing activity into a 1-minute level numeric measure of spoofing intensity.

In order to construct a robust measure of spoofing intensity that is less susceptible to measurement error, we enhance the raw strategic spoofing data by applying two additional transformations. The first transformation involves considering only longer spoofing length—those consisting of 10 or more messages—when constructing the measure. While our methodology for linking cancellations and resubmissions of orders can lead to misclassifications, for a run with many resubmissions to be misidentified purely due to such errors, there would need to be an unbroken chain of spurious linkages. This suggests that longer spoofing activities are more likely to accurately represent genuine spoofing behavior, making them more reliable for measurement.

Following the methodology of Hasbrouck and Saar (2013), the second transformation we use to reduce measurement error is the time-weighting of the number of spoofing activities, rather than simply aggregating the spoofing activities. We define our measure bid(ask) spoofing intensity, as the time-weighted average of the number of strategic bid(ask) spoofing

that occur within 1 minute.[8] We also define the bid(ask) spoofing volume as the time-weighted average of the spoofing size of strategic bid(ask) spoofing that occurs within 1 minute. This measure captures the aggression of spoofing activities.

*[Insert Figure 2 Here]*

We present time-series plots of spoofing intensity, spoofing volume, and Bitcoin price in figure 2. The first plot shows daily bid and ask spoofing intensity at the one-minute level, while the second plot depicts daily bid and ask spoofing volume at the same resolution. The green lines represent Bitcoin prices from January 2024 to March 2024. From these plots, we observe a potential correlation between spoofing intensity, spoofing volume, and Bitcoin price movements.

*[Insert Figure 3 Here]*

Figure 3 presents the daily and hourly level spoofing intensity and spoofing volume for the first three months of 2024. The first two plots illustrate the daily trend of spoofing intensity and spoofing volume. The last two plots illustrate the hourly trend of spoofing intensity and spoofing volume. All solid lines represent the mean of spoofing intensity(volume) of date(hour), the shaded area denotes the range of 25th to 75th percentile. The time is reported as GMT, which is 5 hours ahead of EST in our sample. We note that spoofing orders are more prevalent during U.S. stock trading hours. Both spikes of bid and ask spoofing orders are observed shortly after the opening of the market, which aligns with the findings in the stock market by Lee et al. (2013).

The goal of bid (ask) spoofing activity is to drive up (down) the Bitcoin price, leading us to expect that bid (ask) spoofing intensity will be positively (negatively) related to Bit-

[8]The time-weighting of this measure works as follows. Suppose we construct bid spoofing intensity for the interval 9:00:00 am– 9:01:00 am. If a spoofing started at 8:59:30 am and ended at 09:01:00 am, it was active for the entire interval and hence it adds 1 to the intensity measure. A run that started at 8:59:30 am and ended at 9:00:30 am was active for 30 seconds (out of 60) in this minute, and hence adds 0.5 to the measure. Similarly, a spoofing that was active for 6 seconds within this interval adds 0.1.

coin returns. To test this assumption, we regress Bitcoin returns on spoofing intensity and spoofing volume, with the results presented in Table 5.

*[Insert Table 5 Here]*

In Table 5, column 1 shows that the coefficient for bid spoofing intensity is significantly positive at the 1% level. A 100-unit increase in bid spoofing intensity results in a 7.33% additional Bitcoin return within the same minute. Conversely, the coefficient for ask spoofing intensity is significantly negative at the 1% level, with a 100-unit increase in ask spoofing intensity leading to a 9.56% reduction in return within the same minute. The effect is slightly asymmetric, with ask spoofing having a stronger impact. In column 2, where we include order imbalance, order book imbalance, and lagged returns as control variables, the results remain significant at the 1% level. The last two columns present the results when spoofing intensity is replaced with spoofing volume. The findings remain significant and align with our expectations, though the effects are more symmetric under this metric. Column 4 shows that after controlling for order imbalance, order book imbalance, and lagged Bitcoin returns, a 100-unit increase in bid spoofing volume results in a 5.28% additional Bitcoin return within the same minute. Conversely, a 100-unit increase in ask spoofing volume leads to a 25.0% reduction in Bitcoin return. In summary, Table 5 demonstrates that Bitcoin returns are significantly related to spoofing activities, suggesting that manipulators are motivated to engage in spoofing for manipulation purposes.

*[Insert Table 6 Here]*

Previous literature has focused on the relationship between price impact, trading volume, and informed trading. In Table 6, we include three additional control variables – trading volume, bid-ask spread – and regress the absolute value of contemporaneous Bitcoin returns on spoofing intensity and spoofing volume. Table 6 indicates that both bid and ask spoofing intensity (volume) have a significant contemporaneous price impact on Bitcoin. In Table 6,

the same variables are used to predict Bitcoin returns for the following minute. The results show that both bid and ask spoofing intensity (volume) also have a substantial price impact on Bitcoin in the subsequent minute. This finding is not surprising, as spoofing activities may persist for more than one minute, with prior bid (ask) spoofing intensity ultimately influencing Bitcoin prices in the future. In summary, Tables 6 demonstrates that spoofing activities have a significant price impact.

## 6.2 Spoofing and Market Quality

Separating spoofing orders from bona fide orders is inherently challenging, both technically and legally, as demonstrating "intent" to generate artificial prices requires evidence of manipulative behavior. Spoofing orders – placed and canceled rapidly – create false impressions of supply or demand, distorting price signals and undermining liquidity despite appearing similar to legitimate limit orders. Fox et al. (2021) argue that spoofing orders are often intertwined with informed trading, making them especially difficult for liquidity providers to detect. From a regulatory standpoint, proving intent has significant implications for market quality: manipulative actions can widen spreads, increase adverse-selection risk, and degrade price discovery. Consequently, understanding how spoofing affects market quality is critical for evaluating the integrity and efficiency of cryptocurrency trading venues. In this section, we assess the extent to which spoofing compromises key market-quality indicators – namely the volume-synchronized probability of informed trading (VPIN), the bid–ask spread, and the percentage quoted spread – by contrasting periods with and without spoofing activity. This approach allows us to isolate the direct impact of manipulative order-book practices on liquidity and adverse-selection dynamics.

The market-quality measures we consider include VPIN, the bid–ask spread, and the

percentage quoted spread.[9] We divide the data into two groups: minutes with spoofing activity and minutes without spoofing activity.

*[Insert Table 7 Here]*

Table 7 presents descriptive statistics on market quality across these two groups. The results indicate that all three measures deteriorate during spoofing episodes compared with periods without spoofing. Specifically, when spoofing activity is present, the market exhibits wider bid–ask spreads, higher percentage quoted spreads, and elevated $VPIN$. These patterns suggest that spoofing increases adverse-selection risk, prompting market makers to widen spreads in order to protect against potential informed trading. The wider spread raises transaction costs and reduces available liquidity, while elevated $VPIN$ reflects higher order-flow toxicity, implying less efficient price discovery and a marked decline in overall market quality.

*[Insert Table 8 Here]*

Table 8 presents regression estimates of the impact of spoofing on market quality. The key explanatory variables include indicators for periods during and after spoofing events, the size of spoofing orders, and the size of genuine orders, defined as the final executed order at the end of a spoofing sequence. Panel A shows that a one-unit increase in spoofing size during the spoofing period raises $VPIN$ by 0.26 and significantly widens both the bid–ask spread and the percentage quoted spread relative to the pre-spoofing period. These adverse effects, however, are transitory: once spoofing ceases, $VPIN$ quickly reverts, and the execution of a genuine one-unit order after spoofing reduces $VPIN$ by 0.45 relative to the spoofing period. Columns 2 and 3 reveal consistent patterns of deterioration in spread measures,

[9]VPIN quantifies order-flow toxicity by measuring the imbalance between buy-initiated and sell-initiated volume over synchronized volume buckets (Easley, López de Prado, and O'Hara (2012)). The bid-ask spread is the difference between the best ask and best bid prices, reflecting immediate execution costs. The percentage quoted spread is the bid-ask spread divided by the mid-price, expressed as a percentage, standardizing spread costs relative to price levels.

underscoring that spoofing activity significantly reduces market quality by widening spreads and increasing trading costs.

Panel B replaces the post-spoofing × genuine order size with post-spoofing × spoofing size in the interaction terms. The coefficients remain statistically significant but indicate a different dynamic: during spoofing, bid–ask and quoted spreads remain wide and $VPIN$ stays elevated, signaling a sustained deterioration in market quality. Taken together, the results from Panels A and B consistently show that spoofing deteriorates market quality by widening spreads and increasing adverse-selection risk.

The evidence from Table 8 demonstrates that spoofing exerts a significant, short-lived but economically meaningful impact on key market-quality metrics. Spoofing widens bid–ask spreads and elevates $VPIN$, reflecting heightened adverse-selection risk and reduced price-discovery efficiency. These results underscore that spoofing orders materially undermine market quality, even if their effects dissipate quickly, highlighting the disruptive nature of manipulative trading in cryptocurrency markets.

# 7 Spoofing Profit

Understanding the risk-adjusted profitability of spoofing is critical, as it highlights the economic incentives that distinguish spoofing from ordinary trading strategies. By creating artificial price signals, spoofers can extract rents while shouldering far less risk than regular traders. For example, Navinder Sarao's well-known "flash crash" manipulation of E-MINI futures on May 6, 2010 – where he spoofed orders of over 2,000 contracts—yielded approximately $2 million in profit, largely because his spoofing orders exposed him to minimal adverse price-movement risk.[10] This parallels findings in high-frequency trading (HFT), where firms earn superior risk-adjusted returns by exploiting speed advantages and ephemeral

[10]See U.S. Department of Justice, "Futures Trader Pleads Guilty to Illegally Manipulating Futures Market in Connection with 2010 Flash Crash," available at https://www.justice.gov/archives/opa/pr/futures-trader-pleads-guilty-illegally-manipulating-futures-market-connection-2010-flash.

information (Baron et al., 2019).[11]

In this section, we examine the effect of spoofing volume on the profit generated from spoofing activities. In our regression analysis, the dependent variables are bid spoofing profit ($BSP$) and ask spoofing profit ($ASP$). Based on the findings of Lee et al. (2013) and Do and Putniņš (2023), most spoofing activities last less than one hour; therefore, we primarily focus on spoofing activities that start and end within the same hour.

For bid spoofing activity, we assume that the spoofer buys Bitcoin at the beginning of the first spoofing order and sells it at the end. The profit proxy, $BSP$, represents the hourly average profit from bid spoofing trades, calculated as the return of Bitcoin's price at the end of the spoofing event relative to its price at the beginning. For ask spoofing activity, we assume that the spoofer sells Bitcoin at the beginning of the first spoofing order and buys it back at the end. The corresponding profit proxy, $ASP$, represents the hourly average profit from ask spoofing trades, computed as the return of Bitcoin's price at the beginning of the spoofing event relative to its price at the end.

The explanatory variables include bid spoofing volume ($\overline{BSV}$) and ask spoofing volume ($\overline{ASV}$). Here, $\overline{BSV}$ is measured as the mean of $BSV$ within the same hour as the bid spoofing profit, and $\overline{ASV}$ is measured similarly for ask spoofing profit. Spoofing length ($SL$) is the number of revision orders in the spoofing activity. The $\overline{SL}$ is calculated as the average spoofing length of bid (or ask) spoofing orders within the hour. Additional control variables include order book imbalance, order imbalance, volatility, bid-ask spread, spoofing length, strong spoofing indicator, and spoofing time. Specifically, $\overline{OBIB}$, $\overline{OIB}$, and $\overline{SPREAD}$ represent the mean values of order book imbalance, order imbalance, and bid-ask spread, respectively, measured within the same hour as $BSV$ or $ASV$, and $\sigma_t$ measures the Bitcoin volatility during that hour.

*[Insert Table 9 Here]*

[11] Likewise, Brogaard, Hendershott, and Riordan (2014) document that algorithmic traders achieve outsized risk-adjusted performance through strategies that limit downside exposure. Quantifying spoofing's risk-adjusted returns thus reveals how manipulators leverage artificial liquidity to outperform traditional market participants and underscores the broader threat spoofing poses to market integrity.

Our analysis in Table 9 shows that, in one-hour spoofing events—where bid spoofing profit is measured as the return of the executed genuine ask order price relative to the Bitcoin market price at the beginning of the spoofing episode – a one-unit increase in bid spoofing volume is associated with a 26 basis-point increase in profit, while a one-unit increase in ask spoofing volume is linked to a 95 basis-point increase in profit, even after controlling for various market factors.

The regression specifications in Table 9 incorporate several key control variables that capture market conditions, such as order book imbalance, order imbalance, volatility, and bid-ask spread. This robust framework allows us to isolate the impact of spoofing volume on profitability. The statistically significant coefficients indicate that spoofing volume is a critical determinant of spoofing profit, providing strong evidence that spoofers are able to exploit short-term market inefficiencies for economic gain. Moreover, the differential magnitude of the effects on bid versus ask spoofing profits suggests an asymmetry in how spoofing influences market prices, which may reflect differences in the strategies employed by spoofers on the bid and ask sides.

# 8 Robustness Test

This section conducts a series of robustness tests to validate the consistency and reliability of our main empirical findings on spoofing behavior and its market impact. We examine whether the relationships identified between spoofing intensity, Bitcoin returns, and market quality remain stable under alternative specifications and complementary measures. First, we test whether our spoofing metrics capture abnormal cancellation activity, a hallmark of manipulative trading, by analyzing the frequency of canceled orders that would otherwise have been executed. Second, we investigate whether spoofing intensity coincides with trades executed on the opposite side of the order book, consistent with strategic intent to mislead market participants. These robustness analyses confirm that our spoofing detection algo-

rithm accurately identifies manipulative trading patterns and that the estimated effects on prices and liquidity are not artifacts of measurement error or model specification.

## 8.1 Spoofing Intensity and Abnormal Cancellation

Strategic spoofing involves an abnormally high rate of order cancellations. This occurs because spoofing orders are not intended to execute and ultimately result in cancellations. Additionally, spoofing orders may need to be canceled and resubmitted as market conditions evolve to maintain a low probability of execution and sustain the false market perception. To capture these abnormal cancellations, we define abnormal cancelled bid orders ($ACB$) as the number of bid orders that, if not canceled, would have been executed within the same minute of their cancellation. Similarly, abnormal cancelled ask orders ($ACA$) represent the number of ask orders that, if not canceled, would have been executed within the same minute of their cancellation. These abnormal orders are not intended for execution, and we believe they are closely associated with spoofing activities.

*[Insert Table 10 Here]*

Table 10 investigates whether our metrics for spoofing activities capture the abnormal cancellation phenomenon. The coefficients of interest are all significantly positive at the 1% level. The first two columns show that when bid spoofing activity is high, more bid orders that would have been executed are instead abnormally canceled. Specifically, an increase of one unit in bid spoofing intensity leads to 15.12 additional abnormal canceled bid orders within the same minute. Similarly, 1-unit increase in bid spoofing volume leads to 16.27 more abnormal canceled bid orders in the same minute. The third and fourth columns reveal similar results, indicating that when ask spoofing activity is high, more abnormal canceled ask orders exist in the same minute.

In conclusion, our metrics for spoofing activities effectively reveal some abnormal cancellation which are highly likely related to strategic spoofing.

## 8.2 Spoofing Intensity and Trades Oppose Quotes

The manipulator creates a false perception of market trends by placing spoofing orders, with the true intention of triggering the execution of their hidden orders on the opposite side. We classify executed orders into two categories: seller-initiated and buyer-initiated trades. Seller-initiated trades ($SIT$) are measured as the number of executed ask trades, while buyer-initiated trades ($BIT$) are measured as the number of executed bid trades. We expect that strong bid (ask) spoofing intensity is typically accompanied by an increase in the execution of ask (bid) orders.

*[Insert Table 11 Here]*

Table 11 presents the regression results of trades opposing quotes. The coefficients of interest are all significantly positive at the 1% level. Both the first and second columns indicate that when there is a high level of bid spoofing activity, seller-initiated ask orders are more likely to be executed. An increase of one unit in bid spoofing intensity results in 0.56 additional seller-initiated trades within the same minute. Similarly, 1-unit increase in bid spoofing volume leads to 0.47 more seller-initiated trades in the same minute. The third and fourth columns reveal similar findings, indicating that when ask spoofing activity is high, buyer-initiated bid orders are more likely to be executed.

In conclusion, our metrics for spoofing activities effectively capture the phenomenon of "trades opposing quotes."

# 9 Conclusion

In this paper, we investigate the prevalence and market impact of spoofing in Bitcoin order books on the Coinbase platform. Our analysis aims to uncover how manipulative trading practices – specifically spoofing – shape short-term Bitcoin returns, liquidity provision, and overall market quality. Leveraging high-frequency order book data and a novel algorithm

designed to detect strategic spoofing sequences, we provide a detailed characterization of how such deceptive trading behavior distorts price formation and microstructure dynamics. By integrating empirical evidence on spoofing intensity, profitability, and its effects on liquidity and spreads, this study offers a comprehensive assessment of the mechanisms through which manipulation operates within digital currency markets.

Our empirical results demonstrate that order-book imbalances exert a significant influence on Bitcoin returns at both minute- and hourly-level intervals. Higher bid-side spoofing intensity leads to positive price movements, whereas greater ask-side spoofing intensity drives prices downward, confirming that spoofing can both inflate and depress market prices depending on its directional intent. When examining profitability over one-hour spoofing episodes, we find that a one-unit increase in bid spoofing volume raises bid-side profits by 27 basis points, while a comparable increase in ask spoofing volume raises ask-side profits by 55 basis points. These abnormal returns are achieved with minimal exposure to adverse price movements, as spoofers exploit short-lived liquidity distortions to capture near risk-free gains. In contrast, legitimate trading strategies must bear full market volatility, resulting in substantially lower risk-adjusted returns. The exceptionally high profitability of spoofing highlights the strong incentives for manipulators to engage in such behavior and underscores the importance of effective monitoring and enforcement mechanisms to safeguard market integrity and fair competition in digital asset markets.

In addition to these return and profitability effects, our analysis demonstrates that spoofing significantly deteriorates market quality. The regression analysis shows that spoofing episodes are accompanied by wider bid-ask spreads, elevated VPIN, and higher percentage quoted spreads, all indicative of reduced liquidity and heightened adverse-selection risk. These distortions highlight how spoofing disrupts the normal process of order submission and price formation, reducing the depth and reliability of the order book. The magnitude of these distortions is economically meaningful, as they erode confidence in the fairness and integrity of the market. These findings reveal that spoofing not only yields abnormally high

profits for manipulators but also imposes substantial costs on liquidity providers and other market participants, thereby degrading overall market quality in cryptocurrency exchanges.

A key methodological contribution is our robust detection framework, which adapts "strategic run" methodology of Hasbrouck and Saar (2013) to identify linked sequences of spoof order submissions, cancellations, and opposite-side executions without relying on trader identifiers. This approach can be readily extended to other digital asset markets and similar manipulative behaviors, providing a replicable tool for both academic research and regulatory monitoring.

In conclusion, this paper advances the literature on market microstructure and manipulation by documenting the price dynamics of spoofing, quantifying its abnormal profitability, and demonstrating its adverse impact on market quality. Beyond its academic contribution, the analysis provides practical implications for the design of surveillance and monitoring systems aimed at preserving transparency and integrity in emerging digital asset markets.

# Reference


Aitken, M. J., Aspris, A., Foley, S., and de B. Harris, F. H. (2018). Market fairness: The poor country cousin of market efficiency. Journal of Business Ethics, 147, 5-23.

Aggarwal, R.K. and Wu, G., 2006. Stock market manipulations. The Journal of Business, 79(4), pp.1915-1953.

Allen, F. and Gale, D., 1992. Stock-price manipulation. The Review of Financial Studies, 5(3), pp.503-529.

Barclay, M.J. and Warner, J.B., 1993. Stealth trading and volatility: Which trades move prices?. Journal of financial Economics, 34(3), pp.281-305.

Baron, M., Brogaard, J., Hagströmer, B. and Kirilenko, A., 2019. Risk and return in high-frequency trading. Journal of Financial and Quantitative Analysis, 54(3), pp.993-1024.

Brogaard, J., Hendershott, T. and Riordan, R., 2014. High-frequency trading and price discovery. The Review of Financial Studies, 27(8), pp.2267-2306.

Cartea, Á., Jaimungal, S., and Wang, Y. (2020). Spoofing and price manipulation in order-driven markets. Applied Mathematical Finance, 27(1-2), 67–98. Taylor and Francis.

Chakravarty, S., 2001. Stealth-trading: Which traders' trades move stock prices?. Journal of Financial Economics, 61(2), pp.289-307.

Chordia, T., Roll, R. and Subrahmanyam, A., 2002. Order imbalance, liquidity, and market returns. Journal of Financial economics, 65(1), pp.111-130.

Cong, L.W., Li, X., Tang, K. and Yang, Y., 2023. Crypto wash trading. Management Science, 69(11), pp.6427-6454.

Cont, R., Kukanov, A. and Stoikov, S., 2014. The price impact of order book events. Journal of financial econometrics, 12(1), pp.47-88.

Dimpfl, T. and Peter, F.J., 2021. Nothing but noise? Price discovery across cryptocurrency exchanges. Journal of Financial Markets, 54, p.100584.

Do, B.L. and Putniņš, T.J., 2023. Detecting Layering and Spoofing in Markets. Available at SSRN 4525036.

Easley, D., López de Prado, M.M. and O'Hara, M., 2012. Flow toxicity and liquidity in a high-frequency world. The Review of Financial Studies, 25(5), pp.1457-1493.

Eigelshoven, F., Ullrich, A. and Parry, D., 2021, December. Cryptocurrency Market Manipulation-A Systematic Literature Review. In ICIS.

Félez-Viñas, E., Johnson, L. and Putniņš, T.J., 2022. Insider Trading in Cryptocurrency Markets. Available at SSRN 4184367.

Fischel, D.R. and Ross, D.J., 1991. Should the law prohibit manipulation in financial markets. Harv. L. Rev., 105, p.503.

Foley, S., Karlsen, J.R. and Putniņš, T.J., 2019. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. The Review of Financial Studies, 32(5), pp.1798-1853.

Fox, M.B., Glosten, L.R. and Guan, S.S., 2021. Spoofing and its Regulation. Colum. Bus. L. Rev., p.1244.

Griffin, J.M. and Shams, A., 2020. Is Bitcoin really untethered?. The Journal of Finance, 75(4), pp.1913-1964.

Hasbrouck, J. and Saar, G., 2013. Low-latency trading. Journal of Financial Markets, 16(4), pp.646-679.

Heinz, J. D. (2017). Spoofing: Ineffective Regulation Increases Market Inefficiency. DePaul L. Rev., 67, 77.

Hersch, G. (2020). You can bluff but you should not spoof. Business and Professional Ethics Journal, 39(2), 207–224. JSTOR.

Howell, S.T., Niessner, M. and Yermack, D., 2020. Initial coin offerings: Financing growth with cryptocurrency token sales. The Review of Financial Studies, 33(9), pp.3925-3974.

John, K. and Li, J., 2025. Bitcoin price volatility: Effects of retail traders, illegal users, and sentiment. Journal of Corporate Finance, p.102837.

Khomyn, M. and Putniņš, T.J., 2021. Algos gone wild: What drives the extreme order cancellation rates in modern markets?. Journal of Banking & Finance, 129, p.106170.

Khorasanee, K. (2024). Spoof, Bluff, Go For It: A Defence of Spoofing. Journal of Business Ethics, 189(1), 201–215. Springer.

Kyle, A.S. and Viswanathan, S., 2008. How to define illegal price manipulation. American Economic Review, 98(2), pp.274-279.

Lee, E.J., Eom, K.S. and Park, K.S., 2013. Microstructure-based manipulation: Strategic behavior and performance of spoofing traders. Journal of Financial Markets, 16(2), pp.227-252.

Li, T., Shin, D., Sun, C. and Wang, B., 2022. The dark side of decentralized finance: Evidence from meme tokens. Available at SSRN.

Li, T., Shin, D. and Wang, B., 2021. Cryptocurrency pump-and-dump schemes. Available at SSRN 3267041.

Liu, J., Makarov, I. and Schoar, A., 2023. Anatomy of a run: The terra luna crash (No. w31160). National Bureau of Economic Research.

MacKenzie, D. (2022). Spoofing: Law, materiality and boundary work in futures trading. Economy and Society, 51(1), 1–22. Taylor and Francis.

O'Leary, D.E., 2018. Open information enterprise transactions: Business intelligence and wash and spoof transactions in blockchain and social commerce. Intelligent Systems in Accounting, Finance and Management, 25(3), pp.148-158.

Putniņš, T.J., 2012. Market manipulation: A survey. Journal of economic surveys, 26(5), pp.952-967.

Roll, R., 1984. A simple implicit measure of the effective bid-ask spread in an efficient market. The Journal of finance, 39(4), pp.1127-1139.

Ruan, Q. and Streltsov, A., Perpetual Contracts and Market Quality: Evidence from Cryptocurrencies.

Stenfors, A., Doraghi, M., Soviany, C., Susai, M. and Vakili, K., 2023. Cross-market spoofing. Journal of International Financial Markets, Institutions and Money, 83, p.101735.

Tao, X., Day, A., Ling, L., and Drapeau, S. (2022). On detecting spoofing strategies in high-frequency trading. Quantitative Finance, 22(8), 1405–1425. Taylor and Francis.

Wang, X., and Wellman, M. P. (2017). Spoofing the limit order book: An agent-based model. In Workshops at the Thirty-First AAAI Conference on Artificial Intelligence.

**Table 1: Returns on Bitcoin, contemporaneous and lagged order imbalances and lagged returns**

The dependent variables are the daily, hourly, 30-minute, 5-minute, and 1-minute returns on the Bitcoin, denoted as $R_t$. Explanatory variables include contemporaneous and lagged positive and negative daily, hourly, 30-minute, 5-minute, or 1-minute scaled order imbalances ($OIB \times 10^{-2}$) measured in amount of trades. The control variables include lagged positive and negative Bitcoin returns. The standard errors of parameters for column [Hourly], [30-min], [5-min], and [1-min] are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $R_t$ | | | | |
|---|---|---|---|---|---|
| | [Daily] | [Hourly] | [30-min] | [5-min] | [1-min] |
| Excess buy orders, | 0.0133 | 0.0138 | 0.0148 | 0.0164 | 0.0200 |
| $Max[0, OIB_t \times 10^{-2}]$ | (6.25)*** | (7.75)*** | (9.64)*** | (12.81)*** | (15.38)*** |
| Excess sell orders, | 0.0122 | 0.0149 | 0.0150 | 0.0183 | 0.0210 |
| $-\lvert Min[0, OIB_t \times 10^{-2}]\rvert$ | (5.85)*** | (10.31)*** | (11.79)*** | (15.36)*** | (24.75)*** |
| Lagged excess buy orders, | -0.0028 | -0.0019 | -0.0019 | -0.0009 | -0.0010 |
| $Max[0, OIB_{t-1} \times 10^{-2}]$ | (-1.26) | (-1.91)* | (-2.55)*** | (-0.90) | (-2.96)*** |
| Lagged excess sell orders, | -0.0041 | -0.0023 | -0.0031 | -0.0028 | -0.0060 |
| $-\lvert Min[0, OIB_{t-1} \times 10^{-2}]\rvert$ | (-1.93)* | (-3.00)*** | (-4.07)*** | (-4.30)*** | (-1.77)* |
| Lagged positive return, | -0.0179 | 0.0133 | -0.0231 | -0.0237 | 0.0148 |
| $Max[0, R_{t-1}]$ | (-0.37) | (0.76) | (-1.67)* | (-2.99)*** | (2.59)*** |
| Lagged negative return, | -0.085 | -0.0197 | -0.0163 | -0.0553 | -0.005 |
| $-\lvert Min[0, R_{t-1}]\rvert$ | (-1.77)* | (-1.19) | (-1.20) | (-3.34)*** | (-0.09) |
| Intercept | $-6 \times 10^{-4}$ | $-2.01 \times 10^{-5}$ | $8.81 \times 10^{-6}$ | $-1.71 \times 10^{-5}$ | $-1.33 \times 10^{-6}$ |
| | (-0.42) | (-0.28) | (0.23) | (-1.43) | (-0.45) |
| $R^2$ | 0.081 | 0.049 | 0.044 | 0.038 | 0.041 |
| # of Observations | 1214 | 29100 | 51911 | 301060 | 1488674 |

**Table 2: Returns on Bitcoin, contemporaneous and lagged order book imbalances, order imbalance, and lagged return**

The dependent variables are the hourly, and 1-minute returns on the Bitcoin, denoted as $R_t$. Explanatory variables include contemporaneous and lagged positive and negative hourly, or 1-minute scaled order book imbalances ($OBIB \times 10^{-2}$) measured in average of aggregate order quantity on the top 5 bid levels minus aggregate order quantity on the top 5 ask levels. The control variables include order imbalance and lagged Bitcoin return.The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $R_t$ | | | |
|---|---|---|---|---|
| | [1-min] | | [Hourly] | |
| Order book Bid-Ask imbalance, | 0.0173 | 0.0209 | 0.2963 | 0.4079 |
| $Max[0, OBIB_t \times 10^{-2}]$ | $(9.53) * **$ | $(11.45) * **$ | $(1.99) * *$ | $(2.76) * **$ |
| Order book Ask-Bid imbalance, | 0.0127 | 0.0143 | 0.5987 | 0.5420 |
| $-\lvert Min[0, OBIB_t \times 10^{-2}]\rvert$ | $(4.92) * **$ | $(5.76) * **$ | $(2.42) * *$ | $(2.39) * *$ |
| Lagged order book Ask-Bid imbalance, | $-0.0081$ | $-0.0056$ | $-0.1188$ | $-0.2031$ |
| $Max[0, OBIB_{t-1} \times 10^{-2}]$ | $(-5.37) * **$ | $(-3.82) * **$ | $(-0.72)$ | $(-1.37)$ |
| Lagged order book Bid-Ask imbalance, | $-0.0038$ | $-0.0023$ | $-0.5082$ | $-0.5252$ |
| $-\lvert Min[0, OBIB_t \times 10^{-2}]\rvert$ | $(-1.70)*$ | $(-1.07)$ | $(-2.28) * *$ | $(-2.20) * *$ |
| Order imbalance, | | 0.0270 | | 0.0118 |
| $OIB_t \times 10^{-2}$ | | $(13.85) * **$ | | $(6.35) * **$ |
| Lagged return, | | $-0.0255$ | | $-0.0163$ |
| $R_{t-1}$ | | $(-2.57) * **$ | | $(-0.689)$ |
| Intercept | $2.97 \times 10^{-7}$ | $-6.54 \times 10^{-6}$ | $1 \times 10^{-4}$ | $7.01 \times 10^{-5}$ |
| | (0.05) | $(-1.31)$ | (0.46) | (0.266) |
| $R^2$ | 0.003 | 0.063 | 0.008 | 0.079 |
| # of Observations | 113937 | 113937 | 2173 | 2173 |

**Table 3: Detection of spoofing, example of a bid spoofing**

A spoofing is a series of submissions, cancellation that are linked by direction, size, and timing, and which are likely to arise from a same trader. The series is ended at $T_n$ by a cancellation after another order on order book is filled. This table shows an example of spoofing series with spoofing size 0.038. At time $T_0$, the trader places the genuine ask order. The trader begins spoofing at time $T_1$. After several rounds of order submissions and cancellations, the trader places the final order at $T_{n-1}$. Following the execution of the genuine order, the trader cancels the order at $T_n$, marking the end of the spoofing activity.

| | |
|---|---|
| $T_0$ | Genuine Ask Order Submitted |
| $T_1$ | Submission [Side: Bid, Price: \$40000, Size: 0.038] |
| $T_2$ | Cancellation [Side: Bid, Price: \$40000, Size: 0.038] |
| $T_3$ | Submission [Side: Bid, Price: \$40020, Size: 0.038] |
| $T_4$ | Cancellation [Side: Bid, Price: \$40020, Size: 0.038] |
| $T_5$ | Submission [Side: Bid, Price: \$40015, Size: 0.038] |
| $T_6$ | Cancellation [Side: Bid, Price: \$40015, Size: 0.038] |
| ... | ... |
| $T_{n-1}$ | Submission [Side: Bid, Price: \$40010, Size: 0.038] |
| | Genuine Ask order filled |
| $T_n$ | Cancellation [Side: Bid, Price: \$40010, Size: 0.038] |

**Table 4: Spoofing Activity Statistics**
This table reports the statistics of spoofing activities. Each activity of bid and ask spoofing is categorized based on its spoofing length, quantified by the number of revision orders. Spoofing time measures the duration from the submission of the initial spoofing order to the cancellation of the final spoofing order. Cancellation time gap refers to the time interval between consecutive revision orders. Spoofing size denotes the volume of spoofing orders. Genuine order size denotes the volume of genuine orders. Spoofing distance quantifies the difference between the price of the spoofing order and the best bid or ask price. Spoofing proportion quantifies the relative size of a spoofing order by dividing it to the aggregated volume of the best five bid or ask quotes in the limit order book.

| Bid Spoofing Length | | [10,20) | [20,30) | [30,40) | [40,50) | >=50 |
|---|---|---|---|---|---|---|
| Count | | 2154 | 598 | 241 | 71 | 156 |
| Spoofing Time (s) | Mean | 63.14 | 81.39 | 77.01 | 239.62 | 397.42 |
| | Std | 253.87 | 263.35 | 264.76 | 595.88 | 669.4 |
| | 25% | 6.91 | 11.65 | 14.21 | 21.71 | 31.87 |
| | 50% | 12.5 | 20.51 | 25.3 | 38.19 | 84.8 |
| | 75% | 27.18 | 43.14 | 48.95 | 91.44 | 375.8 |
| Cancellation Time Gap (s) | Mean | 7.52 | 5.88 | 3.19 | 8.48 | 18.31 |
| | Std | 48.13 | 43.15 | 18.19 | 27.59 | 151.41 |
| | 25% | 0.43 | 0.32 | 0.24 | 0.36 | 0.35 |
| | 50% | 0.95 | 0.81 | 0.7 | 0.87 | 0.9 |
| | 75% | 1.94 | 1.7 | 1.42 | 1.91 | 3.57 |
| Spoofing Size (Bitcoin) | Mean | 0.14 | 0.14 | 0.17 | 0.13 | 0.12 |
| | Std | 0.24 | 0.24 | 0.33 | 0.17 | 0.26 |
| | 25% | 0.06 | 0.06 | 0.06 | 0.05 | 0 |
| | 50% | 0.08 | 0.08 | 0.08 | 0.08 | 0.05 |
| | 75% | 0.11 | 0.11 | 0.11 | 0.11 | 0.09 |
| Genuine Order Size (Bitcoin) | Mean | 0.04 | 0.04 | 0.04 | 0.03 | 0.03 |
| | Std | 0.07 | 0.08 | 0.13 | 0.04 | 0.05 |
| | 25% | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 |
| | 50% | 0.02 | 0.02 | 0.01 | 0.01 | 0.01 |
| | 75% | 0.04 | 0.05 | 0.04 | 0.04 | 0.04 |
| Spoofing Distance ($) | Mean | 28.29 | 45.71 | 35.93 | 65.89 | 118.7 |
| | Std | 75.08 | 224.32 | 103.22 | 184.59 | 719.19 |
| | 25% | 3.71 | 6.87 | 7.52 | 6 | 4.04 |
| | 50% | 20.83 | 23.36 | 21.36 | 27.64 | 13.2 |
| | 75% | 37.12 | 35.52 | 32.43 | 38.3 | 29.77 |
| Spoofing Proportion (%) | Mean | 31% | 32% | 31% | 33% | 24% |
| | Std | 68% | 84% | 72% | 64% | 72% |
| | 25% | 8% | 8% | 7% | 7% | 1% |
| | 50% | 16% | 15% | 14% | 15% | 7% |
| | 75% | 33% | 29% | 30% | 25% | 20% |

| Ask Spoofing Length | | [10,20) | [20,30) | [30,40) | [40,50) | >=50 |
|---|---|---|---|---|---|---|
| Count | | 1294 | 357 | 137 | 52 | 101 |
| Spoofing Time (s) | Mean | 63.1 | 113.71 | 129.88 | 197.95 | 522.35 |
| | Std | 272.39 | 392.22 | 414.74 | 453.1 | 759.51 |
| | 25% | 6.1 | 9.71 | 11.27 | 17.44 | 23.28 |
| | 50% | 11.93 | 18.9 | 22.26 | 29.12 | 101.68 |
| | 75% | 23.73 | 37.95 | 50.33 | 65.34 | 811.27 |
| Cancellation Time Gap (s) | Mean | 13.23 | 11.82 | 12.47 | 49.76 | 5.33 |
| | Std | 99.35 | 77.89 | 98.18 | 274.48 | 9.71 |
| | 25% | 0.29 | 0.27 | 0.17 | 0.12 | 0.16 |
| | 50% | 0.7 | 0.65 | 0.48 | 0.43 | 1.13 |
| | 75% | 1.61 | 1.63 | 1.33 | 1.04 | 6.02 |
| Spoofing Size (Bitcoin) | Mean | 0.11 | 0.1 | 0.11 | 0.08 | 0.07 |
| | Std | 0.2 | 0.13 | 0.16 | 0.14 | 0.14 |
| | 25% | 0.05 | 0.05 | 0.05 | 0.03 | 0.01 |
| | 50% | 0.07 | 0.08 | 0.07 | 0.06 | 0.03 |
| | 75% | 0.1 | 0.1 | 0.1 | 0.08 | 0.07 |
| Genuine Order Size (Bitcoin) | Mean | 0.05 | 0.05 | 0.06 | 0.05 | 0.07 |
| | Std | 0.1 | 0.13 | 0.15 | 0.09 | 0.19 |
| | 25% | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 |
| | 50% | 0.02 | 0.02 | 0.03 | 0.02 | 0.02 |
| | 75% | 0.05 | 0.04 | 0.04 | 0.04 | 0.04 |
| Spoofing Distance ($) | Mean | 41.16 | 39.14 | 66.24 | 192.83 | 30.98 |
| | Std | 187.42 | 86.3 | 305.72 | 1212.91 | 108.68 |
| | 25% | 13.48 | 13.77 | 10.77 | 13.99 | 6.89 |
| | 50% | 27.21 | 25.88 | 24.1 | 23.03 | 12.46 |
| | 75% | 43.42 | 39.13 | 39.76 | 36.89 | 28.96 |
| Spoofing Proportion (%) | Mean | 32% | 27% | 32% | 16% | 13% |
| | Std | 73% | 44% | 68% | 20% | 24% |
| | 25% | 9% | 8% | 8% | 5% | 1% |
| | 50% | 19% | 16% | 16% | 11% | 6% |
| | 75% | 34% | 28% | 27% | 21% | 14% |

**Table 5: Returns on Bitcoin, spoofing intensity, and spoofing volume**
The dependent variables are the 1-minute returns on the Bitcoin, denoted as $R_t$. Explanatory variables include contemporaneous 1-minute bid spoofing intensity ($BSI$), bid spoofing volume ($BSV$), ask spoofing intensity($ASI$), and ask spoofing volume ($ASV$). $BSI$ is measured by the time-weighted average of the number of bid spoofing orders in an interval. $BSV$ is measured by the time-weighted average of the order size of bid spoofing orders in an interval. $ASI$ is measured by the time-weighted average of the number of ask spoofing orders in an interval. $ASV$ is measured by the time-weighted average of the order size of ask spoofing orders in an interval. The control variables include order book imbalance, order imbalance, and lagged Bitcoin return. The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $R_t$ | | | |
|---|---|---|---|---|
| Bid spoofing intensity, | $7.33 \times 10^{-4}$ | $6.05 \times 10^{-4}$ | | |
| $BSI_t$ | (13.71)*** | (12.29)*** | | |
| Ask spoofing intensity, | $-9.56 \times 10^{-4}$ | $-8.08 \times 10^{-4}$ | | |
| $ASI_t$ | (-7.46)*** | (-6.27)*** | | |
| Bid spoofing volume, | | | $6.53 \times 10^{-4}$ | $5.28 \times 10^{-4}$ |
| $BSV_t$ | | | (3.32)*** | (2.97)*** |
| Ask spoofing volume, | | | $-2.69 \times 10^{-3}$ | $-2.50 \times 10^{-3}$ |
| $ASV_t$ | | | (-5.29)*** | (-4.69)*** |
| Order book imbalance, | | $1.40 \times 10^{-2}$ | | $1.42 \times 10^{-2}$ |
| $OBIB_t \times 10^{-2}$ | | (10.41)*** | | (10.53)*** |
| Order imbalance, | | $2.63 \times 10^{-2}$ | | $2.68 \times 10^{-2}$ |
| $OIB_t \times 10^{-2}$ | | (13.88)*** | | (14.01)*** |
| Lagged return, | | $-2.35 \times 10^{-2}$ | | $-2.19 \times 10^{-2}$ |
| $R_{t-1}$ | | (-2.89)*** | | (-2.72)*** |
| Constant | $2.25 \times 10^{-6}$ | $-4.15 \times 10^{-6}$ | $5.58 \times 10^{-6}$ | $-1.39 \times 10^{-6}$ |
| | (0.91) | (-1.60) | (2.15)** | (-0.52) |

**Table 6: Absolute returns on Bitcoin, spoofing intensity, and spoofing volume**
The dependent variable is the 1-minute absolute returns on the Bitcoin. Explanatory variables include contemporaneous 1-minute bid spoofing intensity ($BSI$), bid spoofing volume ($BSV$), ask spoofing intensity($ASI$), and ask spoofing volume ($ASV$). $BSI$ is measured by the time-weighted average of the number of bid spoofing orders in an interval. $BSV$ is measured by the time-weighted average of the order size of bid spoofing orders in an interval. $ASI$ is measured by the time-weighted average of the number of ask spoofing orders in an interval. $ASV$ is measured by the time-weighted average of the order size of ask spoofing orders in an interval. The control variables include trading volume, bid-ask spread, absolute order book imbalance, absolute order imbalance, and absolute lagged Bitcoin return. The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $\lvert R_t \rvert$ | | | $\lvert R_{t+1} \rvert$ | |
|---|---|---|---|---|---|
| Bid spoofing intensity, | 0.0001 | | | 0.0001 | |
| $BSI_t$ | $(4.06)^{***}$ | | $BSI_t$ | $(4.73)^{***}$ | |
| Ask spoofing intensity, | 0.0002 | | | 0.0004 | |
| $ASI_t$ | $(2.83)^{***}$ | | $ASI_t$ | $(3.75)^{***}$ | |
| Bid spoofing volume, | | $2.58 \times 10^{-5}$ | | | 0.0002 |
| $BSV_t$ | | (0.44) | $BSV_t$ | | $(1.83)^{**}$ |
| Ask spoofing volume, | | 0.0012 | | | 0.0015 |
| $ASV_t$ | | $(2.72)^{***}$ | $ASV_t$ | | $(5.60)^{***}$ |
| Trading volume, | 0.0002 | 0.0002 | | $9.98 \times 10^{-5}$ | $9.93 \times 10^{-5}$ |
| $VOL_t$ | $(16.77)^{***}$ | $(17.23)^{***}$ | $VOL_t$ | $(11.04)^{***}$ | $(11.13)^{***}$ |
| Bid-ask spread, | $2.89 \times 10^{-5}$ | $2.88 \times 10^{-5}$ | | $2.78 \times 10^{-5}$ | $2.78 \times 10^{-5}$ |
| $SPREAD_t$ | $(15.80)^{***}$ | $(16.08)^{***}$ | $SPREAD_t$ | $(14.48)^{***}$ | $(14.66)^{***}$ |
| Order book imbalance, | 0.0012 | 0.0013 | | 0.0009 | 0.001 |
| $\lvert OBIB_t \rvert \times 10^{-2}$ | (1.11) | (1.14) | $\lvert OBIB_t \rvert \times 10^{-2}$ | (0.74) | (0.77) |
| Order imbalance, | $-0.0091$ | $-0.0089$ | | -0.0071 | $-0.0069$ |
| $\lvert OIB_t \rvert \times 10^{-2}$ | $(-4.68)^{***}$ | $(-4.65)^{***}$ | $\lvert OIB_t \rvert \times 10^{-2}$ | $(-5.59)^{***}$ | $(-5.52)^{***}$ |
| Lagged return, | 0.095 | 0.094 | | 0.17 | 0.16 |
| $\lvert R_{t-1} \rvert$ | $(11.45)^{***}$ | $(10.89)^{***}$ | $\lvert R_t \rvert$ | $(24.22)^{***}$ | $(21.97)^{***}$ |
| Constant | $8.05 \times 10^{-5}$ | $8.31 \times 10^{-5}$ | Constant | 0.0001 | 0.0001 |
| | $(4.92)^{***}$ | $(5.28)^{**}$ | | $(7.09)^{***}$ | $(7.49)^{***}$ |
| $R^2$ | 0.336 | 0.337 | | 0.196 | 0.197 |

**Table 7: Statistics of market quality when spoofing activity exists**
This table reports the mean of market quality at the 1-minute level when spoofing intensity is non-zero, when spoofing intensity is zero, and the difference between them. The market quality measures include Volume-synchronized probability of informed trading ($VPIN$), bid-ask spread ($SPREAD$), and percentage quoted spread ($PQS$).

| | Without spoofing activity | With spoofing activity | Difference |
|---|---|---|---|
| $VPIN$ | 0.55 | 0.78 | 0.23 |
| $SPREAD$ | 12.01 | 12.22 | 0.21 |
| $PQS$ | 0.021% | 0.022% | 0.001% |

**Table 8: Impact of spoofing to market quality**
The dependent variables are measures of market quality, namely the bid–ask spread ($SREAD$), the percentage quoted spread ($PQS$), and the volume-synchronized probability of informed trading ($VPIN$), observed one minute before, during, and one minute after spoofing events. The explanatory variables include time indicators specifying whether the period is during or after spoofing events, the spoofing size, defined as the volume of spoofing orders, and the genuine size, defined as the volume of genuine orders. The control variables include trading volume, absolute order book imbalance, absolute order imbalance, and absolute Bitcoin return. The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| **Panel A:** | | | |
|---|---|---|---|
| | **VPIN** | **Spread** | **PQS** |
| Const | 0.58 | 9.72 | $1.79 \times 10^{-4}$ |
| | (92.72)*** | (72.92)*** | (83.06)*** |
| During Spoofing × Spoofing Size | 0.26 | 0.98 | $2.4 \times 10^{-5}$ |
| | (10.54)*** | (1.88)* | (2.88)*** |
| After Spoofing × Genuine Size | -0.45 | -2.79 | $-2.9 \times 10^{-5}$ |
| | (-9.48)*** | (-2.73)*** | (-1.77)* |
| Order imbalance | 0.16 | -0.88 | $-5 \times 10^{-6}$ |
| $\lvert OIB_t \rvert$ | (40.26)*** | (-10.4)*** | (-3.54)*** |
| Order book imbalance | 0.05 | 0.72 | $8 \times 10^{-6}$ |
| $\lvert OBIB_t \rvert$ | (3.02)*** | (2.2)** | (1.52) |
| Trading Volume | $-1 \times 10^{-6}$ | $1.4 \times 10^{-5}$ | $1 \times 10^{-6}$ |
| $VOL_t$ | (-36.0)*** | (20.39)*** | (15.6)*** |
| Return | -35.53 | 2147.35 | 0.037372 |
| $\lvert R_t \rvert$ | (-9.0)*** | (25.46)*** | (27.44)*** |

| **Panel B:** | | | |
|---|---|---|---|
| | **VPIN** | **Spread** | **PQS** |
| Const | 0.57 | 9.73 | $1.79 \times 10^{-4}$ |
| | (91.74)*** | (73.29)*** | (83.38)*** |
| During Spoofing × Spoofing Size | 0.26 | 0.93 | $2.4 \times 10^{-5}$ |
| | (10.76)*** | (1.79)* | (2.84)*** |
| After Spoofing × Spoofing Size | -0.08 | -1.77 | $-1.6 \times 10^{-5}$ |
| | (-3.91)*** | (-3.87)*** | (-2.11)** |
| Order imbalance | 0.16 | -0.89 | $-5 \times 10^{-6}$ |
| $\lvert OIB_t \rvert$ | (39.85)*** | (-10.51)*** | (-3.6)*** |
| Order book imbalance | 0.05 | 0.75 | $8 \times 10^{-6}$ |
| $\lvert OBIB_t \rvert$ | (3.29)*** | (2.29)** | (1.58) |
| Trading volume | $-1 \times 10^{-6}$ | $1.5 \times 10^{-5}$ | $1 \times 10^{-6}$ |
| $VOL_t$ | (-35.92)*** | (20.54)*** | (15.65)*** |
| Return | -34.07 | 2164.26 | 0.04 |
| $\lvert R_t \rvert$ | (-8.59)*** | (25.66)*** | (27.55)*** |

**Table 9: Spoofing Profit**

The dependent variables are bid spoofing profit ($BSP$) and ask spoofing profit ($ASP$). $BSP$ represents the hourly average profit from bid spoofing trades occurring within a given hour. Each bid spoofing profit is calculated based on the return of executed genuine order price relative to Bitcoin market price at the beginning of spoofing. $ASP$ represents the hourly average profit from ask spoofing trades occurring within a given hour. Each ask spoofing profit is calculated based on the return of Bitcoin's market price at the beginning of ask spoofing relative to executed genuine order price. Explanatory variables include bid spoofing volume ($\overline{BSV}$) and ask spoofing volume ($\overline{ASV}$). $\overline{BSV}$ is measured as the mean of $BSV$ within the same hour of $BSP$. $\overline{ASV}$ is measured as the mean of $ASV$ within the same hour of $ASP$. Spoofing length ($SL$) is the number of revision orders of the spoofing activity. $\overline{SL}$ is measured as the average of $SL$ of bid(ask) spoofing orders within the hour. Other control variables include order book imbalance, order imbalance, volatility, bid-ask spread, spoofing length, strong spoofing indicator, and spoofing time. $\overline{OBIB}$, $\overline{OIB}$, and $\overline{SPREAD}$ are calculated as the mean values of $OBIB$, $OIB$, and $SPREAD$, respectively, within the same hour of $BSP$ or $ASP$. $\sigma_t$ measures the Bitcoin volatility within the same hour of $BSP$ or $ASP$. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | Bid spoofing profit, $BSP$ | | Ask spoofing profit, $ASP$ | |
|---|---|---|---|---|
| Bid spoofing volume, $\overline{BSV_t}$ | 0.0026<br>(2.16)** | 0.0027<br>(2.43)** | | |
| Ask spoofing volume, $\overline{ASV_t}$ | | | 0.0095<br>(4.73)*** | 0.0055<br>(2.89)*** |
| Order book imbalance, $\overline{OBIB_t} \times 10^{-2}$ | | -0.026<br>(-2.62)*** | | -0.02<br>(-1.28) |
| Order imbalance, $\overline{OIB_t} \times 10^{-2}$ | | 0.0048<br>(0.93) | | -0.0083<br>(-1.23) |
| Volatility, $\sigma_t$ | | $5.70 \times 10^{-6}$<br>(2.60)*** | | $1.21 \times 10^{-5}$<br>(3.84)*** |
| Bid-ask spread, $\overline{SPREAD_t}$ | | $2.60 \times 10^{-5}$<br>(4.69)*** | | $1.01 \times 10^{-5}$<br>(1.26) |
| Spoofing length, $\overline{SL_i}$ | | $7.07 \times 10^{-6}$<br>(6.98)*** | | $1.61 \times 10^{-5}$<br>(9.86)*** |
| Constant | 0.0005<br>(37.28)*** | $5.47 \times 10^{-5}$<br>(1.19) | 0.0007<br>(32.25)*** | $5.28 \times 10^{-5}$<br>(0.74) |
| $R^2$ | 0.004 | 0.178 | 0.024 | 0.181 |

**Table 10: Abnormal cancellations**

The dependent variables are the abnormal cancelled bid order ($ACB$), and abnormal cancelled ask order ($ACA$). $ACA$ represents the number of cancelled ask orders that, if not cancelled, would have been executed within the same minute of cancellation. $ACB$ represents the number of cancelled bid orders that, if not cancelled, would have been executed within the same minute of cancellation. Explanatory variables include contemporaneous 1-minute bid spoofing intensity ($BSI$), bid spoofing volume ($BSV$), ask spoofing intensity($ASI$), and ask spoofing volume ($ASV$). $BSI$ is measured by the time-weighted average of the number of bid spoofing orders in an interval. $BSV$ is measured by the time-weighted average of the order size of bid spoofing orders in an interval. $ASI$ is measured by the time-weighted average of the number of ask spoofing orders in an interval. $ASV$ is measured by the time-weighted average of the order size of ask spoofing orders in an interval. The control variables include order book imbalance, order imbalance, Bitcoin volatility, and Bitcoin return. The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $ACB_t$ | | $ACA_t$ | |
|---|---|---|---|---|
| Bid spoofing intensity, | 15.12 | | | |
| $BSI_t$ | (6.57)*** | | | |
| Bid spoofing volume, | | 16.27 | | |
| $BSV_t$ | | (3.44)*** | | |
| Ask spoofing intensity, | | | 15.91 | |
| $ASI_t$ | | | (5.54)*** | |
| Ask spoofing volume | | | | 14.47 |
| $ASV_t$ | | | | (1.93)* |
| Order book imbalance, | 799.01 | 804.75 | -895.24 | -896.64 |
| $OBIB_t \times 10^{-2}$ | (8.83)*** | (8.83)*** | (-9.27)*** | (-9.24)*** |
| Order imbalance, | -470.94 | -464.64 | 345.23 | 339.66 |
| $OIB_t \times 10^{-2}$ | (-7.07)*** | (-6.98)*** | (7.28)*** | (7.16)*** |
| Volatility, | 2.99 | 2.99 | 2.90 | 2.90 |
| $\sigma_t$ | (28.98)*** | (28.96)*** | (43.05)*** | (43.03)*** |
| Return, | -8596.81 | -8492.51 | 8559.35 | 8497.57 |
| | (-18.85)*** | (-18.76)*** | (20.60)*** | (20.53)*** |
| Constant | 5.47 | 5.59 | 4.74 | 4.79 |
| | (4.71)*** | (4.81)*** | (4.68)*** | (4.72)*** |
| $R^2$ | 0.412 | 0.411 | 0.430 | 0.429 |

**Table 11: Trades oppose quotes**

The dependent variables are the 1-minute level seller-initiated trades ($SIT$) and buyer-initiated trades ($BIT$). $SIT$ is the number of executed ask trades. $BIT$ is the number of executed bid trades. Explanatory variables include contemporaneous 1-minute bid spoofing intensity ($BSI$), bid spoofing volume ($BSV$), ask spoofing intensity($ASI$), and ask spoofing volume ($ASV$). $BSI$ is measured by the time-weighted average of the number of bid spoofing orders in an interval. $BSV$ is measured by the time-weighted average of the order size of bid spoofing orders in an interval. $ASI$ is measured by the time-weighted average of the number of ask spoofing orders in an interval. $ASV$ is measured by the time-weighted average of the order size of ask spoofing orders in an interval. The control variables include order book imbalance, order imbalance, and lagged Bitcoin return. The standard errors of parameters are clustered by date. *, **, *** denote statistical significance at the 10%, 5%, and 1% levels, respectively.

| | $SIT_t$ (Seller-initiated trades) | | $BIT_t$ (Buyer-initiated trades) | |
|---|---|---|---|---|
| Bid spoofing intensity, | 0.56 | | | |
| $BSI_t$ | (10.10)*** | | | |
| Bid spoofing volume, | | 0.47 | | |
| $BSV_t$ | | (2.98)*** | | |
| Ask spoofing intensity, | | | 1.01 | |
| $ASI_t$ | | | (7.00)*** | |
| Ask spoofing volume | | | | 2.81 |
| $ASV_t$ | | | | (4.30)*** |
| Order book imbalance, | 0.54 | 0.82 | 1.13 | 1.14 |
| $OBIB_t \times 10^{-2}$ | (0.37) | (0.54) | (0.75) | (0.74) |
| Order imbalance, | -55.9 | -55.6 | 44.9 | 44.6 |
| $OIB_t \times 10^{-2}$ | (-19.04)*** | (-18.95)*** | (15.28)*** | (15.20)*** |
| Lagged return, | -51.0 | -49.6 | -48.1 | -48.3 |
| $R_{t-1}$ | (-2.70)*** | (-2.62)*** | (-2.55)** | (-2.57)** |
| Constant | 0.36 | 0.37 | 0.36 | 0.37 |
| | (16.97)*** | (17.16)*** | (17.19)*** | (17.20)*** |
| $R^2$ | 0.255 | 0.253 | 0.185 | 0.185 |

**Figure 1: Strategic Spoofing Example**

In Figure 1, we plot a example of strategic bid spoofing happened on March 8th from 15:39 to 15:42. The blue dots represent the placement and cancellation of spoofing bid orders. The red dot represents the execution of opposite order. The green dots represent the execution of all bid and ask orders happened during the period. The solid and dotted lines represent the level 1 bid and ask prices respectively. The red bars represent the size of executed orders during this period.

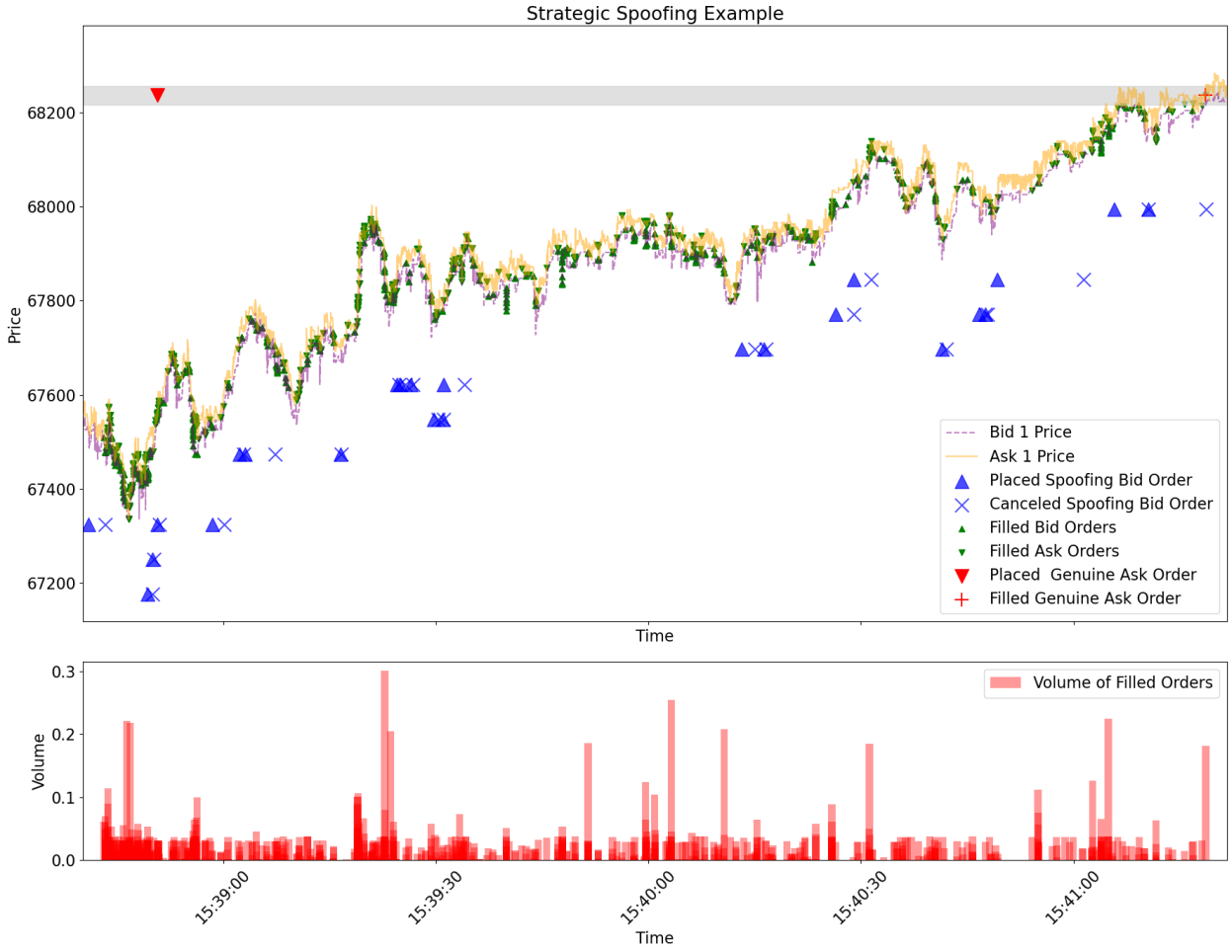
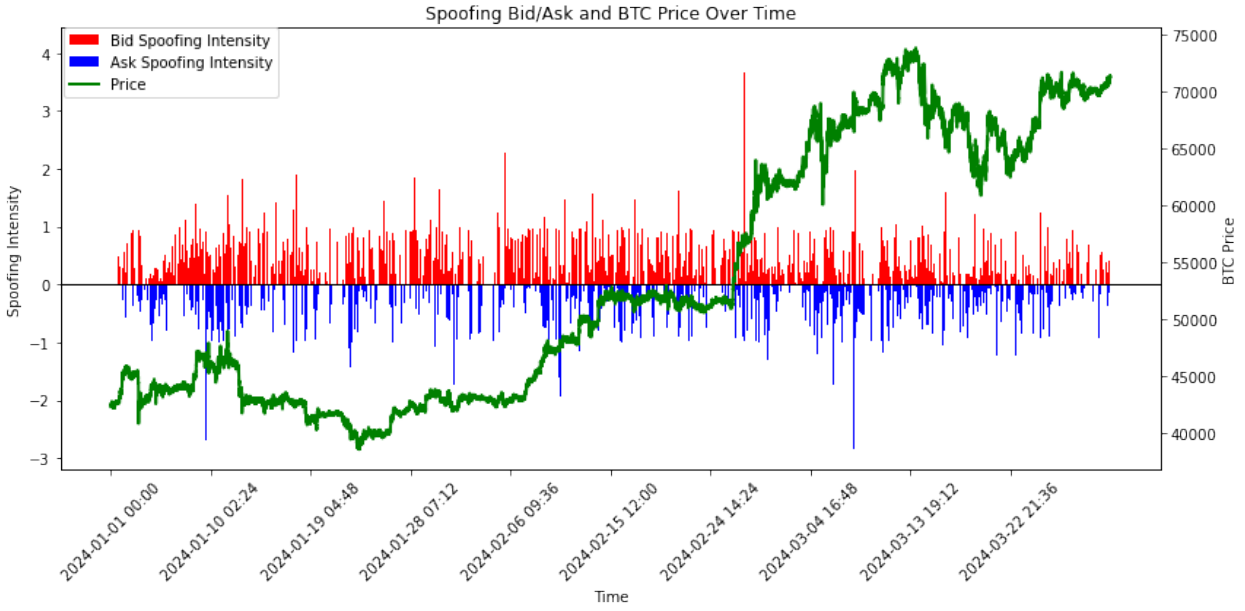


**Figure 2: Spoofing Intensity and Spoofing Volume**
The first plot illustrates the daily bid and ask spoofing intensity at the 1-minute level. The second plot illustrates the daily bid and ask spoofing volume at the 1-minute level. The green lines plot the Bitcoin price during January 2024 to March 2024.



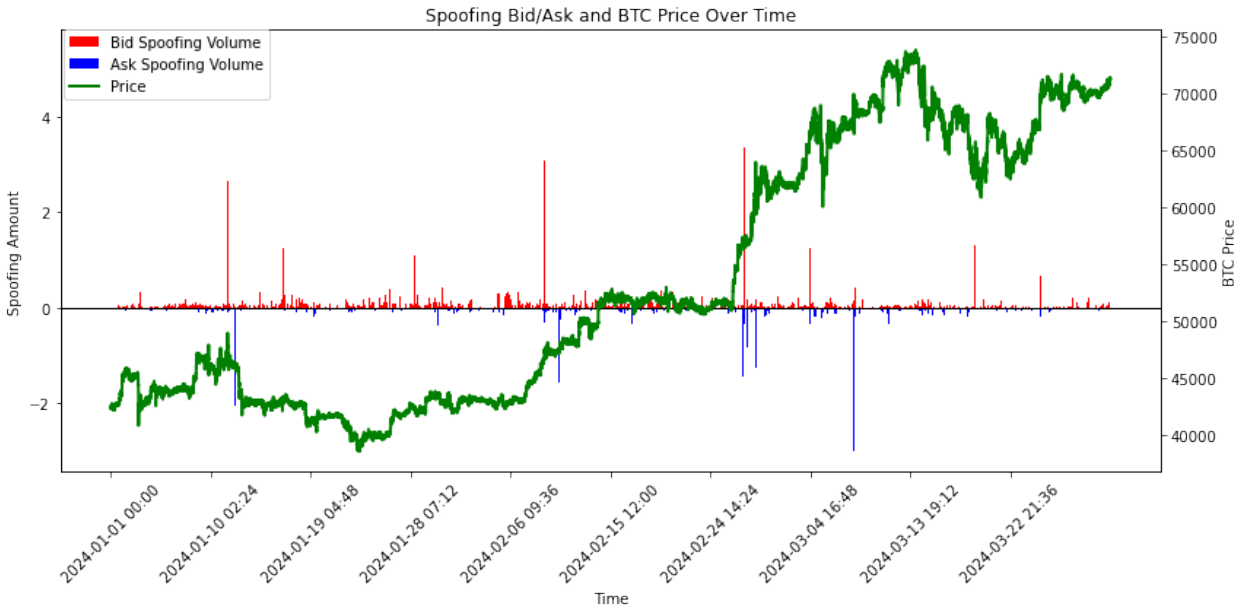



**Figure 3: Time Series of Spoofing Intensity and Spoofing Volume**
The first plot illustrates the daily bid and ask spoofing intensity at the 1-minute level. The second plot illustrates the daily bid and ask spoofing volume at the 1-minute level. The third plot illustrates the hourly bid and ask spoofing intensity at the 1-minute level. The fourth plot illustrates the hourly bid and ask spoofing volume at the 1-minute level. All solid lines represent the mean, the shaded area denotes the range of 25th to 75th percentile.

