The Impact of Spoofing on Bitcoin Market Microstructure

Kose John [1] Jingrui Li [2] Ruming Liu [2] Steve Yang [2]

[1]Leonard N. Stern School of Business, New York University [2]School of Business, Stevens Institute of Technology

Motivation

Market manipulation in cryptocurrency is one of the concern due to the lack of regulation. Some mainupation schemes include: Wash trading (Cong et al. 2023), stablecoin manipulation (Griffin & Shams 2020), and pump-and-dump schemes (Li et al. 2021). In traditional financial markets, **spoofing is a microstructure-based manipulation** that exploits the mechanics of market microstructure to distort prices or create a misleading appearance of supply and demand. This paper investigates spoofing in Bitcoin order books on the Coinbase.

Background: 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. Here are some key actions involved in spoofing:

1. **Placing large non-bona fide (fake) orders** with no intention of execution.
2. **Creating artifical order book imbalances**. Manipulate market perception to push prices in a desired direction.
3. **Executing genuine trades on the opposite side**. The real orders on the other side if executed.
4. **Cancellation of spoof orders**. Withdraw fake orders before they are filled.

Spoofing is explicitly prohibited in th U.S. In 2020, CFTC ordered JPMorgan Chase to pay a record $920 million for spoofing and manipulation in precious metals and Treasuries.

Detection of Spoofing Order

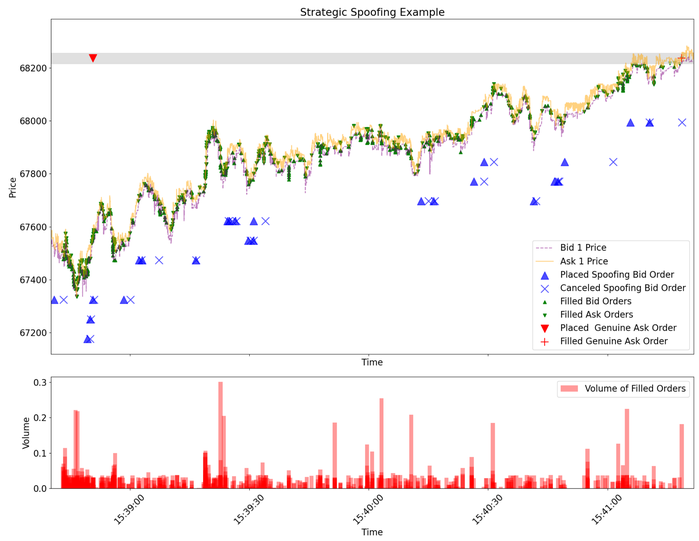
Regulatory authorities detect spoofing by analyzing trader-level order streams. However, this approach relies on access to private data. Our Bitcoin level 3 data is collcted from Coinbase which does not provide trader identification numbers in its trade or quote data, making it impossible to perfectly match trades and quotes to the same individual trader. We propose a novel algorithm for detecting "strategic spoofing" based on below facts:

- The order sizes accompanied with the data unambiguously link an individual limit order submission with its subsequent cancellation or re-submission.
  - On Coinbase, the minimum trade size is 1×10^{-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.
- 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.

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]

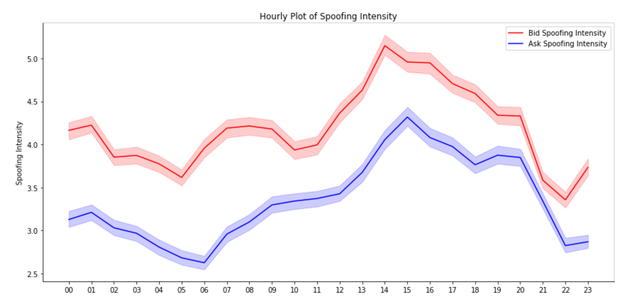
Visualization of a strategic spoofing scheme

1. Genuine ask order is submitted at T_0.
2. Beginning at timer T_1, a series of bid spoofing orders are submitted, cancelled, revised and resubmitted.
3. Genuine ask order is filled at T_{n-1}.
4. The final spoofing order is cancelled at T_n.



Spoofing Intensity

We convert the detected spoofing activity into a 1-minute level numeric measure of spoofing intensity amd spoofing volume. We define our measure of bid (ask) spoofing intensity as the time-weighted average number of strategic bid (ask) spoofing events occurring within one minute. 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. 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.



Spoofing Intensity and Bitcoin Returns

We find that **Bitcoin returns are significantly related to spoofing activities**, suggesting that manipulators are motivated to engage in spoofing for manipulation purposes. We also test that **spoofing volume is a critical determinant of spoofing profit**.

	R_t			Bid Spoofing Profit			Ask Spoofing Profit	
BSI_t	$7.33 \times 10^{-4***}$	$6.05 \times 10^{-4***}$	$\overline{BSV_t}$	0.0026^{***}	0.0027^{***}	$\overline{ASI_t}$	0.0095^{***}	0.0055^{***}
ASI_t	$-9.56 \times 10^{-4***}$	$-8.08 \times 10^{-4***}$						
Controls		Yes	Controls		Yes	Controls		Yes

Note: Controls include trading volume, bid-ask spread, volatility, order book imbalance, order imbalance, and lagged returns. BSI (BSV) represents the bid spoofing intensity (volume), and ASI (ASV) represents the ask spoofing intensity (volume).

Spoofing and Market Quality

The market quality measures we consider include volume-synchronized probability of informed trading (VPIN), the bid–ask spread, and the percentage quoted spread (PQS). We divide the data into two groups: minutes with spoofing activity and minutes without spoofing activity. The results indicate that **all three measures deteriorate during spoofing episodes compared with periods without spoofing**.

	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%

We further apply a difference-in-differences identification strategy, where the treatment group consists of minutes with spoofing activity, and the control group consists of minutes before and after such activity. The key explanatory variables include indicators for periods during and after spoofing events, as well as the size of spoofing orders.

	VPIN	Spread	PQS
During Spoofing × Spoofing Size	0.26^{***}	0.93^{*}	$2.4 \times 10^{-5***}$
After Spoofing × Spoofing Size	-0.08^{***}	-1.77^{***}	$-1.6 \times 10^{-5**}$
Controls	Yes	Yes	Yes

We demonstrate that spoofing exerts a significant, short-lived but economicallymeaningful 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**.

Other Findings

- Order book imbalances can significantly increase returns over both minute- and hourly-level.
- Strategic spoofing involves an abnormally high rate of order cancellations.
- Our spoofing metrics effectively capture the phenomenon of "trades opposing quotes."

Acknowledgements

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.

ronming1303.github.io

RUMING LIU

rumingliu1303@gmail.com