FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Market Abuse In Crypto Markets

Aug 2025

Contents

About

FINMA is Switzerland's independent financial-markets regulator. Its mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes, and their asset managers and fund management companies. It also regulates insurance intermediaries. It is charged with protecting creditors, investors and policyholders. FINMA is responsible for ensuring that Switzerland's financial markets function effectively.

For more information, visit https://www.finma.ch

The Global Finance & Technology Network (GFTN) is a Singapore-headquartered organisation that leverages technology and innovation to create more efficient, resilient, and inclusive financial systems through global collaboration. GFTN hosts a worldwide network of forums (including its flagship event, the Singapore FinTech Festival); advises governments and companies on policies and the development of digital ecosystems and innovation within the financial sector; offers digital infrastructure solutions; and plans to invest in financial technology startups through its upcoming venture fund, with a focus on inclusion and sustainability.

For more information, visit www.gftn.co

The Point Zero Forum is an annual gathering of 2,000 leading central bankers, regulators, policymakers, industry leaders, technologists, and investors from around the world. Over three days of dialogue and collaboration, we work to align policy, finance, and technological roadmaps to advance sustainability, inclusivity, innovation, and efficiency in the global financial ecosystems.

For more information, visit https://www.pointzeroforum.com/

GFTN Insights is a year-round series that connects senior officials and industry leaders across continents to address key financial and tech challenges. Held under Chatham House rules, these dialogues foster partnership, culminating in the two-day Insights Forum in Singapore.

For more information, visit https://gftn.co/programmes/gftn-insights

Executive Summary

This roundtable discussion focused on the issues of market abuse risks in crypto markets and the appropriate regulatory response. Crypto markets continuously demonstrate risks of market abuse, including challenges due to new technological vulnerabilities like smart contract exploits. Traditional patterns such as pump-and-dump schemes persist, but crypto markets provide criminals with more powerful tools for market abuse and also present unique risks due to their decentralized nature. Key issues include wash trading, flash loans, pump-and-dump schemes, and maximum extractable value (MEV), all of which undermine market integrity.

The need for a market abuse regime for crypto assets was emphasized by participants of the roundtable, focusing on insider trading, liquidity and price manipulation, disclosure requirements, surveillance, and data sharing. It was concluded that existing regulatory frameworks for securities trading can provide a regulatory baseline that needs to be complemented with specific elements. Those components take the unique market structure with off-chain and on-chain transactions as well as regulated and unregulated marketplaces spread across various jurisdictions and therefore the need for global cooperation into account.

1 Market Abuse Patterns in Crypto Markets

Wash Trading: Wash trading involves executing trades between linked accounts to artificially inflate trading volume. This misleads investors into believing that a token is more popular or liquid than it is. It boosts platform rankings and token exposure, especially on decentralized exchanges (DEXs) and unregulated or lightly supervised centralized exchanges (CEXs). The practice undermines price discovery and market integrity, leading to distorted market conditions and a loss of trust in crypto markets.

Flash Loans: Flash loans are uncollateralized loans that are repaid within a single transaction. These loans enable complex attacks with almost zero cost and zero risk to the issuer, making them highly attractive for manipulation. They are used to manipulate prices across DEXs and for oracle exploits, feeding false price data into smart contracts. Flash loans are also employed in governance attacks on Decentralized Autonomous Organizations (DAOs), where borrowed tokens are used to buy votes. These attacks are difficult to detect, especially when bundled into automated smart contracts.

Maximal Extractable Value (MEV): MEV refers to the profit that can be made from reordering transactions on the blockchain, allowing certain actors to manipulate transaction sequences for profit. Validators, miners, and bots on DEXs use MEV strategies such as front-running by inserting a trade before a user's transaction, back-running by following a large trade to profit from subsequent price movements, or sandwich attacks where front- and back-running are combined in a single transaction to extract value. These practices are most relevant in decentralized markets (not CEX) and they undermine trust in DeFi protocols and DEXs by creating distorted incentives that favor profit over user interests. Independent of the question if MEV extraction is legal, it can have systemic implications and comes with ethical and structural risks.

Pump-and-Dump Schemes: These schemes involve creating coordinated hypes around low-value or meme tokens, often driven by social media platforms and influencers. The price of the token spikes, followed by a rapid sell-off by the insiders who initiated the pump, leaving mostly retail investors holding near-worthless tokens. Pump-and-dump schemes are difficult to track due to the pseudonymity of the actors involved and the cross-border, cross-chain nature of the activity.

Other Emerging Abuse Patterns: Cross-chain manipulation involves exploiting so called bridges between blockchains or wrapped assets to manipulate prices or take advantage of vulnerabilities across different blockchains. Similarly, the artificial inflation of total value locked (TVL) inflates TVL figures to increase the perceived value of a DeFi platform, misleading investors about its true liquidity and security. Finally, centralized exchange staff could benefit from inside information about token listings by buying tokens just before their prices multiply.

2 New Technologies and Market Structures Elevate Risks

New technological developments also elevate risks. While certain market abuse practices and patterns in traditional finance transfer over to crypto assets, crypto markets also present unique challenges. The pseudonymity of users, fragmentation of markets, lack of reference markets, and the limited history of issuers contribute to an enhanced risk landscape. Crypto markets allow for new forms of manipulation specific to the technology, such as smart contract exploits and decentralized finance (DeFi) vulnerabilities. New risks also result from the direct participation of retail customers in crypto markets. Some actors even offer Market Manipulation-as-a-Service, artificially inflating trading volumes to meet exchange listing requirements, using wash trading on both centralized exchanges and decentralized platforms to manipulate the token's value. Even if blockchain-analysis tools have advanced, such forms of manipulative behavior are still hard to detect. Questions arise as to whether the unique characteristics of crypto markets require a tailored regulatory approach to achieve the same regulatory outcome as in traditional markets. A key question is also who the primary addressee of these rules should be.

3 Regulatory Challenges and How To Overcome Them

Many manipulative practices are already covered by existing regulatory frameworks, but these only apply to securities or sometimes other traditional financial instruments like derivatives. Hence, targeted regulatory frameworks such as MiCA (Markets in Crypto-Assets Regulation) include similar provisions against market manipulation for crypto markets. Yet, **enforcement of such rules remains a challenge**, given the decentralized nature of crypto markets.

For an **effective regime protecting against market abuse**, it is essential to address the challenges and define core areas of oversight, including disclosure obligations on insider information, insider information dissemination, and cross-platform information sharing. However, the crypto world presents unique challenges to the application of traditional regulatory concepts, and it requires a high degree of cooperation. The enforcement of rules against market abuse, in particular, requires cross-border cooperation and technical expertise to address the challenges posed by the global and decentralized nature of the crypto market, and to avoid regulatory arbitrage.

In addition to the traditional requirements and duties for intermediaries, **on-chain monitoring capabilities** might be required. Such tools can be critical to detecting market manipulation in the crypto space, where trades can be executed quickly and anonymously. However, blockchain monitoring tools are still evolving, making it difficult to base requirements on established standards.

Due to the fragmented market structure, crypto asset trading platforms should be required to **share information about incidents** of market abuse across platforms, with the understanding that platforms may apply technological solutions to detect and respond to potential market manipulation practices. As such, disclosure requirements for crypto assets should follow similar rules to those applicable to traditional financial instruments, including relevant exemptions.

In the traditional financial market, a sound regulation of securities issuers is key to ensure transparency and avoid market abuse. However, in the world of crypto assets, the concept of issuer is not always clear, or the issuer is unknown. It may be necessary to set more specific duties for the crypto asset trading platforms themselves and to applicants seeking admission of a crypto asset to a trading platform. This approach would for example ensure that those with privileged information about the listing or status of a crypto asset are subject to insider trading rules.

The combination of on- and off-chain data is critical for identifying systemic networks in which manipulators and fraudsters operate. This data can reveal where these bad actors may be nested within services or platforms. Real-time data analysis of thousands of potential instances of market manipulation – such as wash trading, spoofing and pump-and-dump schemes – can help track suspicious activity across numerous assets. One of the key challenges is to locate the unique structure of transactional activities so that patterns of market abuse can be identified even in decentralized, pseudonymous environments. The crypto market is characterized by its **data-rich environment**, where vast amounts of transaction data can be collected from public blockchain ledgers and exchanges. While this data is accessible, it often **lacks context**, which is typically available in traditional markets. As a result, regulatory approaches may need to generate the necessary context by requiring relevant disclosures from issuers or other involved parties.

The use of specific **reg-tech tools** might contribute to reducing compliance costs. Collaboration between platforms (e.g. sharing of reg-tech solutions and findings) could significantly reduce the burden for platforms and improve the quality of detection of market manipulation at the same time, even if the responsibility remains with each individual platform.

The concept of **embedded supervision** within the platform infrastructure itself is also a potential extension of the reg-tech approach mentioned before. By embedding regulatory oversight tools directly into the trading platform infrastructure, **real-time monitoring** could be enabled and many of the challenges of detecting market abuse could be solved. On-chain analytics providers gain relevance in this situation, as they generate additional context for transactions, something that traditional markets often provide by default.

Finally, the issue of **cross-border information sharing** between regulators remains critical to addressing market abuse on crypto trading platforms. Additional Memoranda of Understanding (MoUs) between regulators may be necessary to facilitate cooperation, share intelligence, and respond to market manipulation across jurisdictions. Given the borderless nature of crypto assets, it is essential that regulators take a holistic approach to combating market abuse and ensuring a level playing field for all market participants. This integrated regulatory framework ensures that regulators and market participants can address the evolving landscape of market abuse in crypto assets while maintaining the integrity of the financial system. Challenges, however, arise from differing regulatory maturity levels. Therefore, the development of shared technical standards or interoperable audit frameworks could pave the way forward in this regard.

4 Conclusion

The crypto market abuse landscape is constantly evolving, with new risks emerging as technology advances. Regulatory frameworks provide a baseline for the regulation of crypto markets and are still relevant. However, the blockchain technology creates additional challenges, highlighting the need for an effective regulatory response. Close collaboration between regulators, technology providers and crypto asset trading platforms will be essential to effectively address market abuse. The development of a specific crypto market abuse regime is an important first step in addressing these risks. Continued innovation, oversight, and international cooperation are critical to staying ahead of emerging threats.

Global Finance &
Technology Network (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com