Proceedings of ICFTBA 2024 Workshop: Finance's Role in the Just Transition
DOI: 10.54254/2754-1169/143/2024.GA18969

Problems and Solutions in US Stock Market

Zihe Liu[1,a,*]

[1]*Herbert Business School, University of Miami, Miami, US*
a. zxl1186@miami.edu
**corresponding author*

Abstract: This research explores critical challenges facing the U.S. stock market, specifically focusing on the impacts of algorithmic trading-induced market volatility and cybersecurity threats. Algorithmic trading, which utilizes high-speed computer systems to make trades, has increased market efficiency but also introduced risks of extreme price fluctuations and "flash crashes". In parallel, the digitalization of financial markets has heightened exposure to cybersecurity threats, posing risks to trading integrity and data security. To address these issues, this study proposes two targeted solutions. For the issue of market volatility driven by algorithmic trading, the research recommends implementing circuit breakers and trading halts. These mechanisms can prevent severe market disruptions by temporarily pausing trading during extreme price movements, allowing the market to stabilize and preventing panic-driven selloffs. For the cybersecurity challenges, the study suggests enhancing information sharing and fostering collaborative defense strategies among financial institutions and regulatory bodies. By encouraging greater collaboration, the financial sector can more effectively identify and counteract cybersecurity threats, reducing vulnerabilities across the market.

Keywords: Market volatility, Cybersecurity threats, US.

1. Introduction

The stock market plays a crucial role in the economy by serving as a platform where companies can raise capital to fund operations, innovation, and expansion. For investors, it provides an opportunity to grow wealth by buying shares in companies they believe will perform well over time. The stock market also reflects the broader economy's health, with indices like the S&P 500 or Dow Jones often serving as barometers for economic trends. Moreover, the stock market helps facilitate liquidity, enabling the quick buying and selling of assets, which allows investors to realize gains or cut losses efficiently. By offering a space where public companies can be valued and traded, the stock market contributes to economic growth, encourages corporate transparency, and promotes efficient allocation of resources.

The U.S. stock market is a vital component of the American economy, impacting everything from corporate funding to individual wealth creation. As a primary source of capital for businesses, it enables companies to raise funds for expansion, innovation, and job creation, which in turn drives economic growth. The U.S. stock market also plays a significant role in the financial stability of households, as millions of Americans invest in stocks directly or indirectly through retirement accounts like 401(k)s and IRAs. Furthermore, it serves as a critical economic indicator, with

DOI: 10.54254/2754-1169/143/2024.GA18969

movements in major indices, such as the S&P 500 and the Dow Jones Industrial Average, offering insights into economic trends and investor confidence. In addition, the global influence of the U.S. stock market extends beyond its borders, affecting international markets and economies, as it sets trends and attracts foreign investment. This interconnectedness underscores its importance as a key driver of economic resilience and prosperity in the U.S.

The U.S. stock market is a cornerstone of the nation's economy, enabling companies to raise capital, promoting economic growth, and providing investment opportunities for individuals and institutions alike. However, it faces significant challenges, particularly with the rise of algorithmic trading and high market volatility, which relies on computer programs to execute trades at high speeds, can lead to extreme price swings and "flash crashes" that disrupt market stability. Another pressing concern is cybersecurity; as financial markets become increasingly digital, they are more vulnerable to cyberattacks. Cybersecurity threats pose risks not only to the integrity of trading systems but also to the vast amounts of sensitive data handled by financial institutions. Addressing these issues is critical to maintaining the resilience and reliability of the U.S. stock market, as they have far-reaching implications for both the economy and investors.

2. Problems

2.1. Algorithmic Trading and Market Volatility

Automated trading, especially HFT, has been widely adopted in the financial markets. It can help make markets more efficient and offer liquidity but also has problems, such as high market fluctuations and manipulation.

Automated trading systems rely on mathematical models and computer programs to make trading decisions quickly and make thousands of trades per second. Kirilenko and Lo also stated that algorithmic trading contributes more than 50% of trading volume in U.S. equities and futures markets [1]. Such a high turnover of these fast trades tends to create high volatility and drastic price swings, especially during periods of market stress.

The Flash Crash of May 6, 2010, is one of the most famous examples of the risks that algorithmic trading may present. In this event, the Dow Jones Industrial Average fell by about 9% within minutes before rising again. In their report on the Flash Crash, the U.S. Securities and Exchange Commission and the Commodity Futures Trading Commission noted that automated trading systems worsened the price drop [2].

Furthermore, certain types of algorithmic trading, such as some types of HFT, have been accused of practicing manipulative activities. These may include "spoofing," which is placing and subsequently canceling a large order in a bid to create an illusion of market depth, or "layering," which is placing multiple orders with successively higher or lower prices to manipulate the price. They can skew market prices and harm other market players, tiny investors.

2.2. Cybersecurity Threats in Financial Markets

This is especially the case as more financial markets go online. Intrusions into financial markets, their infrastructures, and exchanges are costly and can lead to loss of data, money, and market credibility.

The financial sector is one of the most attractive targets for cybercriminals because of the potential monetary reward and because it plays a significant part in the global economy. Boston Consulting Group's report reveals that financial services firms are three hundred times more likely to be attacked by cybercriminals than firms in other industries [3].

Cyberattacks can take various forms, including malicious activities such as Distributed Denial of Service (DDoS) attacks, which overload systems and interfere with trading. Hackers may target databases containing consumers' personal and financial data, leading to potential identity theft and

DOI: 10.54254/2754-1169/143/2024.GA18969

financial fraud. Additionally, viruses and Trojans can compromise trading systems, allowing attackers to embezzle funds or disrupt normal operations. Another common tactic involves exploiting human weaknesses through social engineering, which enables attackers to infiltrate systems by manipulating users into revealing sensitive information or performing actions that compromise security.

The vulnerability of financial markets to cyber threats was brought to the forefront in 2017 when Equifax, one of the biggest credit rating agencies in the United States of America, lost about 147 million people's information to hackers.

3. Solutions

3.1. Implement Circuit Breakers and Trading Halts

A number of proposals have been made to address the risks associated with algorithmic trading and decrease the level of market fluctuations. One of the most effective is the use of more complex circuit breakers and trading halts. Circuit breakers are trading halts implemented on an exchange or for individual securities when their prices reach specified levels.

The United States Securities and Exchange Commission established new circuit breaker rules after the 2010 Flash Crash. These rules include market-wide trading halts based on specific percentage drops in the S&P 500 Index across all exchanges. The SEC also implemented adjustments to the up-limit-down mechanisms that regulate the trading of individual stocks within certain price levels, introducing tighter circuit breakers that address price fluctuations over shorter durations. Additionally, the rules offer security-specific circuit breakers that consider the nature and average volatility of particular securities. The thresholds for these circuit breakers are adaptable, allowing them to depend on the general market situation and recent changes. The SEC has worked on developing more sophisticated circuit breakers and trading halts that activate when securities or indices reach predetermined levels across exchanges, aiming to reduce excessive volatility and maintain orderly markets.

In 2012, the U.S. Securities and Exchange Commission released amended circuit breaker rules in response to the 2010 Flash Crash. These rules include market-wide circuit breakers that suspend trading on all exchanges once the S&P 500 index has declined by specific percentages [4]. They also introduced restrictions that prevent trading in specific securities from occurring outside certain price levels. The updated rules include higher-tier circuit breakers designed to address abrupt price changes within shorter time intervals, as well as security-specific circuit breakers that take into account the normal fluctuations of each security stock. The SEC also proposed smart circuit breakers capable of adjusting their parameters based on general market conditions and recent fluctuations across exchanges. Moreover, they reduced the up-limit-down mechanisms that regulate trading for individual securities within specific price ranges. The amendments encourage tighter circuit breakers that address price fluctuations over shorter periods and security-specific circuit breakers tailored to the characteristics and average volatility of particular securities. These circuit breakers can adapt their thresholds according to recent market conditions. The SEC’s development of more sophisticated circuit breakers and trading halts aims to temporarily suspend trading on exchanges or for individual securities whenever prices hit predefined thresholds, ultimately promoting market stability and preventing excessive volatility.

The U.S. Securities and Exchange Commission introduced updated circuit breaker rules following the 2010 Flash Crash. These rules include market-wide circuit breakers that halt trading across all exchanges whenever the S&P 500 Index drops by specific percentages. Additionally, they implemented limit up-limit down mechanisms to prevent trades in individual securities from occurring outside a specified price band. To further enhance this system, regulators could consider

DOI: 10.54254/2754-1169/143/2024.GA18969

implementing more granular circuit breakers that respond to rapid price movements over shorter time frames. They could also introduce security-specific circuit breakers tailored to each stock's unique characteristics and typical volatility. Furthermore, developing adaptive circuit breakers that adjust their thresholds based on overall market conditions and recent volatility could help improve market stability and responsiveness.

Moreover, regulators could impose "speed bumps" or the average time orders need to stay at a specific price range. This would involve locking orders in the market for a certain period before they can be canceled, which may well help eradicate some manipulative practices like spoofing.

3.2. Enhance Information Sharing and Collaborative Defense

As financial markets are highly integrated, improving information exchange and developing collective protection measures against cyber threats is essential This solution involves several key components aimed at strengthening cybersecurity across the financial sector. First, Cybersecurity Information Sharing plays a critical role. Developing or enhancing current systems for the timely dissemination of cyber threat intelligence among financial institutions, regulators, and relevant security agencies is crucial. One example is the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States, though there is room to expand its scope and impact [5]. Strengthening Public-Private Partnerships is also necessary. Building stronger relationships between government organizations and private-sector financial institutions can enhance cybersecurity efforts, including conducting cyber warfare drills, developing cybersecurity policies and frameworks, and coordinating responses to major cyber threats. Cross-border Cooperation is another important element, as the integration of global financial markets necessitates increased cooperation on cybersecurity. This can involve harmonizing cybersecurity policies and regulations, regulating information exchange, and collaborating on combating cybercrime activities. Conducting Industry-wide Cyber Exercises regularly would also prove beneficial. High-frequency, high-volume exercises covering various threat types can identify potential gaps in market-wide systems and procedures, thereby increasing response coordination. Expanding the Cybersecurity Talent Pool is as well essential for addressing the shortage of qualified cybersecurity specialists in the financial sector. Promoting cybersecurity literacy and education through initiatives such as university sponsorship, corporate training programs, and outreach to people of all ages and backgrounds could help build a more skilled workforce [6]. Finally, increasing cooperation and information sharing across the financial industry would enable a more robust and coordinated defense against cyber threats. The World Economic Forum has emphasized that now is the time to take decisive action to address the threat posed by cybercriminals to the financial sector [7].

In light of emerging cybersecurity risks, financial institutions and market participants should incorporate a robust cybersecurity plan. This framework should be based on the best practices of international standards, such as the NIST Cybersecurity Framework or ISO/IEC 27001 [8]. A critical component of this framework is Risk Assessment, which involves systematic and thorough evaluations of cybersecurity threats and risks related to technology, procedures, and personnel. Another essential element is Multi-layered Defense; institutions should employ firewalls, intrusion detection systems, encryption, and access control measures to create multiple barriers against potential threats [9].

A well-designed Incident Response Plan is also important. Institutions should develop and rehearse an effective plan to facilitate a swift and organized response to cyber incidents. Employee Training is vital for reducing the risk of social engineering attacks, and continuous, inclusive cybersecurity education and training should be provided to all employees. Furthermore, in order to manage Third-party Risk, financial institutions must conduct regular and thorough security assessments of third-party vendors and service providers, ensuring they comply with best

DOI: 10.54254/2754-1169/143/2024.GA18969

cybersecurity practices. Finally, Continuous Monitoring and Improvement should be prioritized. By using continuous monitoring tools and conducting periodic security assessments, institutions can stay responsive to new threats and evolving risks.

Financial institutions should also incorporate other modern technologies, such as artificial intelligence and machine learning, to improve their Cybersecurity. These technologies can aid in threat detection and response in real-time and may be able to prevent threats before they become critical.

4. Conclusion

The challenges posed by algorithmic trading-induced volatility and cybersecurity threats to the U.S. stock market underscore the need for proactive measures. Implementing circuit breakers and trading halts offers a practical solution to mitigate extreme price fluctuations, allowing for market stability during times of unexpected volatility. This approach not only protects investors but also maintains overall confidence in the market's integrity. Additionally, enhancing information sharing and fostering collaboration between financial institutions and regulatory bodies are essential steps to safeguard against cybersecurity threats. By working together, these entities can establish stronger defense mechanisms, reducing vulnerabilities across the financial landscape. Addressing these issues through targeted strategies will ultimately contribute to a more resilient and secure stock market, fostering long-term stability and growth.

This research holds significant potential applications for bolstering market stability and security in an increasingly digitalized financial world. By establishing circuit breakers and trading halts as standard responses to algorithm-driven volatility, markets can be better equipped to handle sudden disruptions, paving the way for a more resilient trading environment, ensuring that future financial markets remain stable, secure, and responsive to new challenges.

References

[1] *Kirilenko, A. A., & Lo, A. W. (2013). Moore's law versus Murphy's law: Algorithmic trading and its discontents. Journal of Economic Perspectives, 27(2), 51-72.*

[2] *Act, E. U.S. Securities and Exchange Commission. development, 586(139,257), 1-163.*

[3] *Jacobides, M. G., Lang, N., & von Szczepanski, K. (2019). What does a successful digital ecosystem look Like? Boston Consulting Group.*

[4] *Lin, K., Gurrola-Perez, P., & Speth, B. (2022). Circuit breakers and market quality. In-Circuit Breakers and Market Quality, SSRN.*

[5] *Nish, A., & Naumaan, S. (2022). Cyber Threat Landscape: Confronting Challenges to the Financial System. Carnegie Endowment for International Peace.*

[6] *Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. Computer Science & I.T. Research Journal, 5(4), 903-925.*

[7] *Index, G. S. M. (2020). World Economic Forum.*

[8] *Securities, U. S. (2014). Exchange Commission (SEC). 2012. SEC charges Satyam Computer Services with financial fraud.*

[9] *Solansky, S. T., & Beck, T. (2021). Interorganizational information sharing: Collaboration during cybersecurity threats. Public Administration Quarterly, 45(1), 105-122.*