The Blockchain Challenge: The Impact of Cryptocurrency Heists on Market Trends and Investor Behaviour

MINGNAN LI

PhD

University of York

School for Business and Society

May 2025

Abstract

Cryptocurrency heists have become an increasingly frequent and disruptive phenomenon, raising concerns about their broader impact on the cryptocurrency market. This thesis uses an event study approach, using various cryptocurrency heists as case studies to systematically examine the impact of cryptocurrency heists on the cryptocurrency market. The first study investigates the impact of cryptocurrency heists on Bitcoin's market efficiency within the Adaptive Market Hypothesis (AMH) framework. Using permutation entropy and the Complexity–entropy causality plane, the study finds that Bitcoin's efficiency declines significantly on and immediately after most major cryptocurrency heists, highlighting the impact of security breaches on Bitcoin market stability and further supporting the notion that Bitcoin market efficiency evolves in response to changes in the external environment. The second study examines the bidirectional predictive relationship between Bitcoin price and investor sentiment using the Cryptocurrency Fear & Greed Index (CFGI). A time-varying Granger causality analysis around the KuCoin exchange heist reveals that while no significant feedback loop exists before this heist, a strong sentiment-price interaction emerges afterwards. This intensified sentiment-price predictive relationship suggests that heightened uncertainty following a heist amplifies investor reactions, creating price declines and market panic. The third study extends the analysis to decentralised finance (DeFi), assessing liquidity shocks and spillover effects by low-frequency price impact measures and the Quantile VAR model from six major DeFi heists. Findings indicate that while affected platforms' native DeFi tokens experience severe liquidity declines, spillover effects on mainstream DeFi tokens remain limited, suggesting some degree of DeFi market stability. This thesis contributes to the literature by demonstrating that cryptocurrency heists significantly impact market stability and investor behaviour. The findings emphasise the importance of robust security measures, crisis management, and governance improvements to mitigate risks in the cryptocurrency market.

Acknowledgement

First of all, I would like to express my deepest gratitude to my supervisors, Dr Viktor Manahov and Prof John Ashton, for their invaluable guidance, continuous support, and insightful feedback throughout my research journey. Their patience, encouragement, and expertise have been instrumental in shaping this thesis.

I would also like to extend my sincere thanks to my TAP member, Dr Lewis Ramsden, whose thoughtful discussions and constructive suggestions have greatly contributed to the development of my work. I am equally grateful to the members of my examination committee, Dr Maryam Alhalboni and Prof Alistair Milne, for their insightful comments and challenging questions during my viva. Their feedback has significantly enhanced the quality and clarity of this thesis.

I am deeply thankful to my family and friends for their unwavering encouragement and understanding, which have been a constant source of motivation throughout this challenging yet rewarding academic journey.

Finally, I wish to express my heartfelt gratitude to my partner, Dr Kexin Liu, whose support and patience have been invaluable in enabling the smooth completion of this research. I would also like to thank my cat, Maotai, for his quiet companionship during the long days and nights of writing. His presence has been a source of calm and comfort throughout this journey.

I sincerely appreciate everyone who has been part of my research and life. Their guidance, kindness, and encouragement have made this four-year journey not only intellectually fulfilling but also genuinely enjoyable.

Author's Declaration

I hereby declare that this thesis is the result of my own original work and has not been submitted, either wholly or in part, for any other degree or qualification at this or any other University. All sources used have been properly acknowledged.

This thesis incorporates material that has been published in peer-reviewed journals. These publications are based on research that I conducted independently. The input of my supervisors to the published papers was limited to academic guidance consistent with standard doctoral supervision, including high-level feedback on structure, theoretical positioning, and responses to peer review. All data collection, data analysis, interpretation of results, and the writing of the manuscripts were undertaken solely by me.

I confirm that my supervisors did not participate in the substantive content development of the published work beyond the normal expectations of doctoral supervisory support. The published outputs included in this thesis therefore satisfy the requirements of independent authorship, and the thesis as a whole represents my own intellectual contribution.

Contents

Chapter 1 Thesis Introduction

1.1 Thesis Background

Cryptocurrency is a digital asset designed to function as a medium of exchange, using cryptographic technology to secure transactions, control the creation of new units, and verify asset transfers (Corbet et al., 2019a). Unlike traditional financial systems that rely on centralised institutions such as banks and governments, cryptocurrency operates on decentralised networks, primarily using blockchain technology (Dorofeyev et al., 2018; Ghosh et al., 2020; Härdle et al., 2020). This decentralisation offers several advantages, including lower transaction costs, enhanced privacy, global accessibility, and financial inclusion for individuals without access to traditional banking services (Chen & Bellavitis, 2020; Ozili, 2022; Hayes, 2024). For example, in countries with an underdeveloped banking infrastructure, individuals can use cryptocurrencies to send and receive payments without relying on traditional banks. In Venezuela, where hyperinflation has severely devalued the national currency, many citizens have turned to Bitcoin and other cryptocurrencies to preserve wealth and conduct transactions beyond the reach of government-imposed capital controls (Mills, 2024).

Since Bitcoin was first introduced by Satoshi Nakamoto (2008), more than 9,000 cryptocurrencies have emerged, including Ethereum, Ripple, Binance Coin, and Solana. As of 2024, the total market capitalisation of cryptocurrencies has reached approximately $3.18 trillion (CoinMarketCap, 2024). Over the past decade, academic research on cryptocurrency has expanded rapidly, exploring various aspects of this emerging financial ecosystem. Corbet et al. (2019a) conducted a comprehensive review of cryptocurrency studies published between 2014 and 2018 and found that market efficiency had received the greatest attention, accounting for 26 of the 104 papers reviewed. This was followed by research on the cryptocurrency structure (18 papers), as well as studies on price dynamics and diversification, which comprised 12 and 11 papers, respectively. More recently, Almeida and Gonçalves (2024) classified the body of research on the microstructure of the cryptocurrency market up to 2021, showing that topics such as market efficiency, liquidity, volatility, uncertainty, price behaviour, connectedness, and investment attributes have continued to attract significant academic interest. This sustained attention is largely driven by the inconsistent and often contradictory findings across studies regarding the microstructural characteristics of the cryptocurrency market.

The analysis of cryptocurrency's market efficiency is predominantly anchored in the framework of the Efficient Market Hypothesis (EMH). The EMH posits that asset prices fully and immediately reflect all available information (Fama, 1970). EMH is commonly classified into three forms according to the type of information incorporated into prices: the weak form, which states that prices reflect all historical price and return information; the semi-strong form, which holds that prices adjust rapidly to all publicly available information; and the strong form, which asserts that prices fully incorporate both public and private (insider) information. Early evidence generally supports a high level of efficiency in most developed markets, where returns are generally found to be largely unpredictable based on past price information (Lim, 2007; Hull & McGroarty, 2014; Rizvi et al., 2014; Ali et al., 2018). By contrast, studies focusing on emerging markets report a weak form of efficiency, suggesting greater return predictability and slower information incorporation (Huang, 1995; Lee et al., 2001; Cajueiro & Tabak, 2004; Jin, 2006; Hoque et al., 2007).

In the cryptocurrency market, Urquhart (2016) applied a series of randomness tests and demonstrated that the Bitcoin market was inefficient between August 1, 2010, and July 31, 2016, although such inefficiencies tended to diminish over time. Similarly, Kang et al. (2022) found that speculative trading contributed significantly to Bitcoin's inefficiency. A range of studies employing multifractality analysis of time series (Bariviera, 2017; Alvarez-Ramirez et al., 2018; Al-Yahyaee et al., 2018; Jiang et al., 2018; Takaishi, 2018; Yi et al., 2022; Kakinaka & Umeno, 2022) also suggest that the Bitcoin market is inefficient. However, some evidence indicates weak-form efficiency. Nadarajah and Chu (2017) and Tiwari et al. (2018) reported that Bitcoin may exhibit weak-form efficiency, while Zargar and Kumar (2019) found that low-frequency Bitcoin returns followed a memory-less random process during 2013–2018. Nevertheless, they cautioned that traders could still obtain abnormal returns through high-frequency speculative strategies. Overall, these conflicting findings indicate that Bitcoin's market efficiency is not static but evolves in response to changes in market conditions. Differences in methodological approaches, sample periods, and market environments contribute to varying empirical results across studies.

This has prompted scholars to study market efficiency from a dynamic perspective. Khuntia and Pattanayak (2018), Stosic et al. (2019), and Khursheed et al. (2020) showed that the efficiency of Bitcoin and other major cryptocurrencies fluctuates between efficient and inefficient states over time, with efficiency tending to deteriorate during periods of market turbulence and to improve under more stable conditions. In addition, Mensi et al. (2019a,

2019b, 2019c) demonstrated that inefficiency is more pronounced when the cryptocurrency market is declining, while it appears to subside during bullish phases. Mokni et al. (2024) employed the adjusted market inefficiency magnitude (AMIM) metric and a quantile regression model to further confirm the time-varying behaviour of Bitcoin's market efficiency. Existing studies have also identified several key factors that influence the evolution of market efficiency. For example, improvements in liquidity (Brauneis & Mestel, 2018; Wei, 2018; Al-Yahyaee et al., 2020; Takaishi & Adachi, 2020; Mokni et al., 2024), the development of derivatives markets (Köchling et al., 2019; Ruan et al., 2021), and strengthened regulatory oversight (Alexander & Heck, 2020) have all been shown to enhance the efficiency of the Bitcoin market. Therefore, market efficiency should be understood from a dynamic rather than a static perspective.

Similarly, the liquidity of the cryptocurrency market has continued to receive sustained attention from scholars. Liquidity represents one of the fundamental attributes of financial markets, reflecting the ease with which assets can be traded without generating significant price movements. A liquid market supports efficient price discovery, reduces trading frictions, enables effective risk sharing, and strengthens investor confidence (Amihud & Mendelson, 1986; Pástor & Stambaugh, 2003). In contrast, illiquidity tends to amplify pricing deviations, heighten trading frictions, and, in extreme cases, contribute to systemic vulnerabilities (Brunnermeier & Pedersen, 2009). Consequently, liquidity has become a central dimension for understanding market quality, return dynamics, and investor behaviour (Chordia et al., 2000). A substantial body of studies has examined liquidity through the lens of information asymmetry, which is regarded as a key determinant of trading conditions.

Akerlof (1978) proposed that when one party possesses superior information, adverse selection problems arise, discouraging uninformed participants from trading, thereby reducing market activity and depth. Extending this insight to financial markets, Grossman and Stiglitz (1980) argued that information can never be fully reflected in prices, as the cost of acquiring information ensures a persistent imbalance between informed and uninformed traders. This informational disparity generates uncertainty for less-informed traders, causing them to trade more cautiously and withdraw liquidity from the market. Kyle (1985) further formalised the strategic interaction between informed and uninformed traders, showing that informed traders exploit their informational advantage gradually to avoid revealing it, while uninformed traders face higher valuation uncertainty and reduce their trading aggressiveness. This behaviour slows the incorporation of information into prices and diminishes the

willingness of uninformed traders to supply liquidity. Glosten and Milgrom (1985) directly linked information asymmetry to liquidity provision by demonstrating that market makers widen spreads to protect themselves against losses when trading with better-informed investors. As information asymmetry increases, market makers require greater compensation for adverse selection risk, raising trading costs and reducing liquidity.

Collectively, these findings show that information asymmetry reduces the willingness of uninformed participants to trade, increases the cost of supplying liquidity, and ultimately weakens market liquidity. Empirical evidence from traditional markets demonstrates that information disparities between informed and uninformed traders are closely linked to liquidity fluctuations, market participation, and asset price dynamics (Stoll, 1989; Hasbrouck, 1991; Brennan & Subrahmanyam, 1996; Huang & Stoll, 1997; Chordia et al., 2000; Easley et al., 2002; Pástor & Stambaugh, 2003). These studies collectively underline that liquidity conditions are strongly shaped by the information environment and that information asymmetry plays an integral role in explaining variations in market functioning.

Information asymmetry is particularly pronounced in the cryptocurrency market owing to decentralisation, limited disclosure requirements, and the anonymity of market participants (Othman et al., 2019; Park & Chai, 2020; Alfieri et al., 2025). The fragmented nature of trading across numerous exchanges further contributes to information frictions, which can lead to pricing discrepancies and arbitrage opportunities (Makarov & Schoar, 2020). Evidence also suggests that informed trading plays a measurable role in cryptocurrency pricing, as information-based trading components have been found to correlate positively with return volatility and negatively with several liquidity metrics (Tiniç et al., 2023). Moreover, information asymmetry has been shown to weaken liquidity in token issuance markets, particularly during periods of security shocks such as cyberattacks, with tokens issued on the same blockchain as the attacked asset being disproportionately affected (Manahov & Li, 2025c). The majority of empirical findings further suggest that cryptocurrencies exhibit lower liquidity and more fragile trading conditions relative to traditional financial assets (Loi, 2018; Corbet et al., 2019a; Smales, 2019; Trimborn et al., 2020). Taken together, this literature establishes information asymmetry as a crucial theoretical foundation for understanding the liquidity characteristics of the cryptocurrency market.

As the cryptocurrency has emerged as a new asset class with a rapidly expanding range of cryptocurrencies, scholars have increasingly examined the level of interconnectedness between cryptocurrencies and traditional financial assets, as well as across cryptocurrencies themselves, to understand patterns of risk transmission and spillover effects. The interconnectedness among assets is not only a reflection of co-movements but also reveals how information and shocks propagate across markets. Hasbrouck (1995) introduced a framework to quantify the contribution of different markets to price discovery, demonstrating that some markets lead in incorporating information while others follow. This highlights that price discovery is not confined to individual markets; rather, it is a collective process shaped by the interaction and relative informational dominance of different trading venues. As a result, the degree of connectedness between markets reflects the efficiency of cross-market information transmission and the level of market integration (Baele, 2005). While price discovery models explain how information diffuses across markets, they do not fully capture the transmission of shocks and volatility. Diebold and Yilmaz (2012) later formalised this notion by proposing a connectedness framework to measure the extent and direction of return and volatility spillovers across markets, offering a broader perspective on cross-market interdependence. These approaches have since been widely used to assess the degree of interdependence between financial markets (Samarakoon, 2011; Dhanaraj et al., 2013; Zhang et al., 2017; Raddant & Kenett, 2021; Hoque et al., 2024), offering a useful lens through which to examine cryptocurrency market linkages.

Research examining interconnectedness within cryptocurrency markets generally provides evidence of return and volatility spillovers across major cryptocurrencies. Before 2017, Bitcoin's price dynamics appeared relatively isolated, with limited interaction with other cryptocurrencies (Zięba et al., 2019). However, Kumar and Anandarao (2019) found that spillover effects strengthened substantially after 2017 and were further amplified following major market events such as Chinese regulatory interventions and the creation of Bitcoin Cash in 2018 (Zeng et al., 2020; Karimi et al., 2023). The later studies suggest a high level of co-movement and contagion within the market, indicating that shocks in one cryptocurrency can rapidly transmit to others (Corbet et al., 2018b; Tiwari et al., 2020; Shahzad et al., 2021). More recent findings indicate that Ethereum has increasingly assumed a leading role as a transmitter of volatility within the cryptocurrency network, frequently driving spillover effects across the market (Kumar et al., 2022). Interestingly, smaller-capitalisation cryptocurrencies have also been shown to exert influence on major cryptocurrencies (Huynh

et al., 2020), suggesting a non-hierarchical and evolving dependency structure within the cryptocurrency network. However, the degree of interconnectedness among cryptocurrencies is not consistent across studies. Some evidence indicates that major cryptocurrencies exhibit weak correlations and lack a common long-run trend (Gil-Alana et al., 2020; Kostika & Laopodis, 2020), and no clear lead–lag relationship between Bitcoin and Ethereum has been identified during certain periods (Sifat et al., 2019). Consequently, an increasing number of scholars recognise that cryptocurrency connectedness is time-varying, strengthening during periods of market stress and weakening in calmer market conditions (Antonakakis et al., 2019; Aslanidis et al., 2019).

Studies exploring the linkages between cryptocurrencies and traditional financial assets present mixed evidence (Adelopo & Luo, 2025). Kalyvas et al. (2021) identified positive return co-movements between cryptocurrencies and technology or clean energy indices, especially when market sentiment strengthens. Spillover effects from cryptocurrencies to commodities and equity markets have also been documented, with Bitcoin influencing precious metals, equities, and certain currency markets (Kurka, 2019; Rehman, 2020; Elsayed et al., 2022). Evidence further shows that cryptocurrencies can both transmit and receive information flows from global markets. For example, the US oil index acts primarily as a spillover recipient, whereas the European oil index serves as a source of information to the cryptocurrency market (Huynh et al., 2022). However, other studies characterise cryptocurrencies as relatively segmented from traditional financial markets. For example, Aslanidis et al. (2019) reported weak or insignificant correlations between cryptocurrencies and conventional assets, including bonds, equities, gold, and broad financial indices. No cointegration relationship has been identified in many cases (Corbet et al., 2018b; Gil-Alana et al., 2020), supporting the view that the cryptocurrency may serve as a potential diversification instrument, particularly for commodity risk (Milunovich, 2018; Giudici & Abu-Hashish, 2019; Huynh et al., 2024).

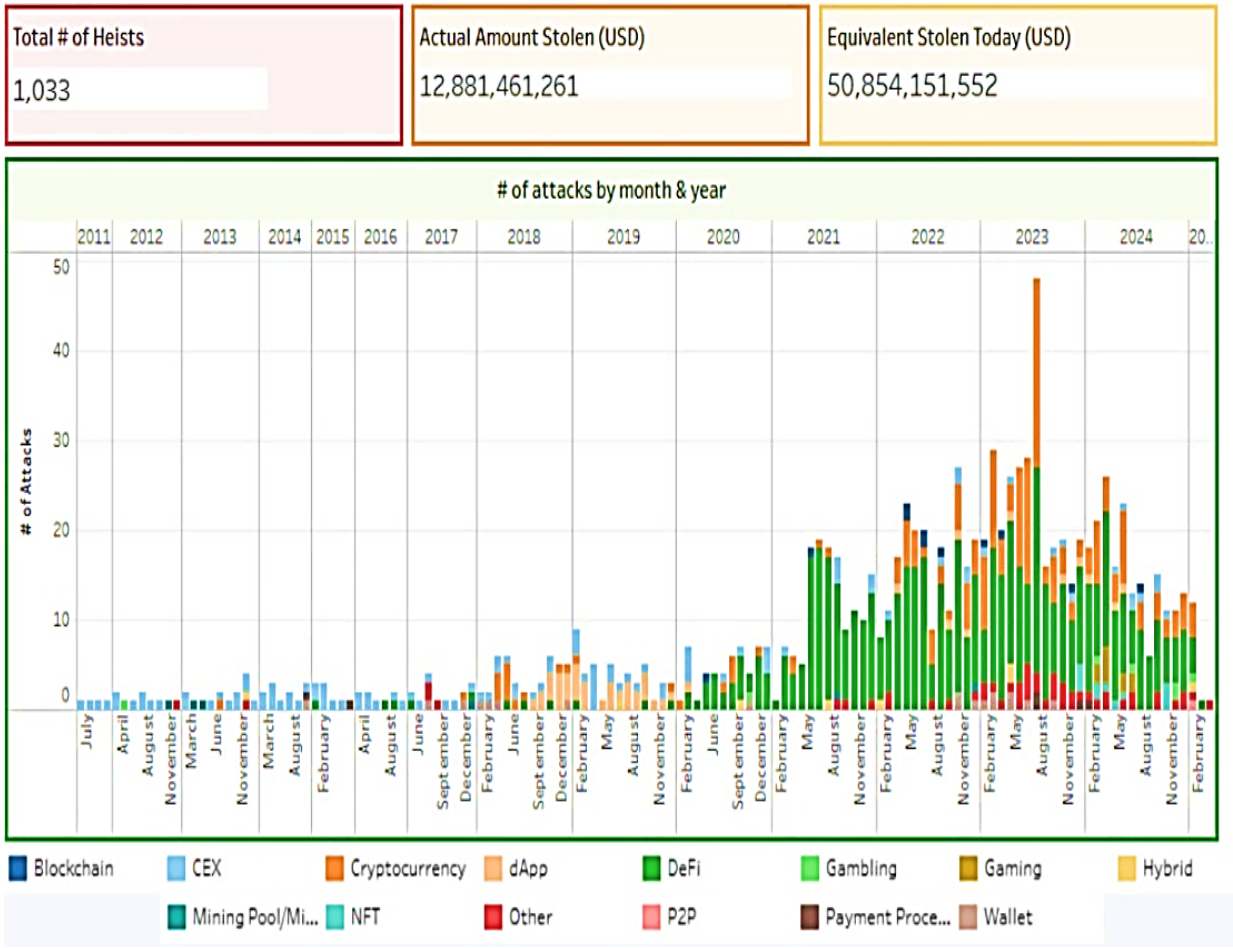
Beyond market efficiency, liquidity, and interconnectedness, several other research directions have contributed to a broader understanding of the cryptocurrency market. A widely established finding is that cryptocurrencies exhibit pronounced volatility (Cheung et al., 2015; Wu et al., 2022), with substantial heterogeneity across cryptocurrencies in terms of return behaviour, regime dynamics, and sensitivity to external shocks (Bejaoui et al., 2020), particularly during periods of geopolitical tension or major news events (Aysan et al., 2019; Katsiampa, 2019b; Cheng & Yen, 2020). Building on this, scholars have sought to explain

and predict return patterns in the cryptocurrency market. Evidence shows that various measures of market uncertainty and risk, such as economic policy uncertainty (Demir et al., 2018; Cheng & Yen, 2020), volatility indices (Panagiotidis et al., 2019), and size and reversal factors (Shen et al., 2020), offer greater explanatory and predictive power than traditional asset-pricing models. There is also evidence that simple price-based indicators, including previous closing prices and recent high prices, possess predictive power for future returns (Yang & Zhao, 2021). These return dynamics have been linked to speculative behaviour, with several studies documenting the presence of price bubbles in the cryptocurrency market, reinforcing the view that price formation is often driven by speculation rather than fundamentals (Phillips et al., 2011, 2015b; Baek & Elbeck, 2015; Corbet et al., 2018a; Fry, 2018; Hafner, 2020). What is more, some studies have examined the investment properties of cryptocurrencies. Findings suggest that they may provide diversification benefits relative to traditional financial assets (Corbet et al., 2018b; Giudici & Abu-Hashish, 2019; Kurka, 2019; Gil-Alana et al., 2020), particularly for cryptocurrencies with higher market capitalisation and liquidity (Wang et al., 2019). In certain cases, Bitcoin has also demonstrated hedging capabilities against geopolitical risk (Aysan et al., 2019; Kurka, 2019) and inflation expectations (Blau et al., 2021).

Despite significant progress in understanding the financial characteristics of the cryptocurrency market, one critical dimension remains notably underexplored: the impact of hacking events on market functioning. Unlike traditional financial systems, cryptocurrency trading operates under a decentralised and irreversible structure with weak regulatory oversight and limited investor protection, rendering the market highly vulnerable to security breaches and cyberattacks (Corbet et al., 2019a). Once a security breach or theft occurs, the stolen assets are typically irretrievable, which can rapidly erode investor confidence and trigger spillover effects across tokens and trading platforms (Manahov & Li, 2025a, 2025b). As the cryptocurrency market has expanded rapidly, security risks have intensified, particularly with the growing frequency of cryptocurrency heists (Barnes, 2018; Gandal et al., 2018; Corbet et al., 2020a; Corbet, 2021; Chen et al., 2023). These incidents involve hackers exploiting vulnerabilities in cryptocurrency exchanges, wallets, and decentralised finance (DeFi) platforms to steal large amounts of digital assets. One of the most well-known cases is the Mt. Gox exchange theft in 2014. This was the first large-scale hacking attack on a cryptocurrency exchange and remains the largest Bitcoin theft suffered by an exchange to date. The platform had been losing funds since 2011, but the theft was only discovered in

February 2014. Over the years, hackers stole 100,000 Bitcoins from the exchange itself and 750,000 Bitcoins from its customers. At that time, these Bitcoins were valued at $470 million, but today, their value would be approximately $81.3 billion. Shortly after the hack, Mt. Gox exchange entered liquidation proceedings (Hunter, 2024). Figure 1.1 shows that since 2021, the frequency of cryptocurrency heists has significantly increased, with a particular focus on attacks targeting DeFi platforms. For instance, before 2021, the average number of cryptocurrency heists per month did not exceed 10. However, since 2021, this figure has doubled, reaching an average of 20 cryptocurrency heists per month, with attacks on DeFi platforms accounting for more than half of them. In July 2023 alone, the number of cryptocurrency heists surged to nearly 50, with almost 30 specifically targeting DeFi platforms. To date, hackers have stolen over $12 billion in funds. If hackers were to retain all the cryptocurrency they had stolen and cash it out, their wealth would amount to approximately $50 billion (Tsihitas, 2025).

Figure 1.1: Number of cryptocurrency heists between 2011 and 2024



Source: https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/

During the early stage of my doctoral research, I co-authored a study with one of my supervisors that examined how cryptocurrency heists affected the performance of tourism tokens (Manahov & Li, 2024). This preliminary work provided the empirical evidence that hacking incidents significantly influence investor behaviour within a specific segment of the cryptocurrency market. However, as I expanded this study and reviewed the wider literature, it became apparent that academic attention to cryptocurrency heists remained limited, fragmented, and insufficiently integrated into mainstream discussions of cryptocurrency market microstructure. Existing studies predominantly examine market behaviour under normal market conditions or during macroeconomic or geopolitical shocks, yet offer limited insights into how extreme, endogenous events such as cryptocurrency heists disrupt market functioning. These cryptocurrency heists are fundamentally different from external shocks because they directly undermine trust in the decentralised financial system and challenge the security of the decentralisation system. Existing studies have primarily focused on short-term price responses to hacking incidents (Corbet et al., 2020a; Hu et al., 2020; Grobys, 2021; Chen et al., 2023; Umar, 2021, 2025), with limited attention to their broader implications for market efficiency, liquidity, and the transmission of shocks across cryptocurrencies and platforms. A deeper examination of these mechanisms is therefore essential to understand how security breaches reshape market functioning and to identify vulnerabilities within the cryptocurrency ecosystem. This research gap forms the starting point of this thesis and motivates the development of the research agenda explored in the subsequent chapters.

1.2 Thesis Motivation

The growing prevalence of cryptocurrency heists has raised questions about how security vulnerabilities within decentralised financial ecosystems impact market behaviour. Given that cyberattacks have become a frequent occurrence in the cryptocurrency market, understanding their effects extends beyond the realm of security concerns, becoming an important issue that influences market dynamics, asset pricing, liquidity, and cross-platform spillover effects. These incidents provide a unique lens through which we can examine how the cryptocurrency market responds to endogenous shocks originating from within the system. However, despite the increasing frequency and scale of cryptocurrency heists, there is still limited empirical evidence in the academic literature regarding the extent and scope of their impact. This research gap highlights the need for a more comprehensive investigation into the financial consequences of security breaches in the cryptocurrency market.

This thesis focuses on Bitcoin due to its dominant position in the cryptocurrency market, high liquidity, and role as a benchmark asset that can better reflect overall cryptocurrency market dynamics compared to smaller, less liquid tokens (Antonakakis et al., 2019). Most scholars classify Bitcoin as a financial asset rather than a currency. For example, Luther and White (2014) argued that Bitcoin's price instability makes it unsuitable as a payment method. Similarly, Yermack (2024) found that Bitcoin fails to fulfil the fundamental functions of a currency, namely serving as a medium of exchange, a store of value, and a unit of account. Bitcoin's high volatility introduces significant short-term risks compared to traditional fiat currencies. Baek and Elbeck (2015) further contended that Bitcoin is better understood as a financial asset, given its speculative nature and price being largely driven by market participants rather than intrinsic value.

Given Bitcoin's classification as a financial asset, understanding its market efficiency becomes particularly important. Market efficiency determines whether asset prices accurately reflect all available information, which is essential for price discovery, risk management, and investment decision-making (Fama, 1970; Malkiel, 2003). As Corbet et al. (2019a) have stated, Bitcoin's market efficiency has been one of the most widely studied topics in the field of cryptocurrency research. Most empirical studies indicate that Bitcoin's market exhibits inefficiencies (Urquhart, 2016; Bariviera, 2017; Alvarez-Ramirez et al., 2018; Al-Yahyaee et al., 2018). However, as the market matures through improvements in liquidity, the adoption of derivatives, and increased regulatory oversight, the Bitcoin market has the potential to become more efficient over time (Brauneis & Mestel, 2018; Wei, 2018; Shanaev et al., 2020; Takaishi & Adachi, 2020; Shynkevich, 2021). Therefore, based on the current empirical findings, we can infer that Bitcoin's market efficiency is not fixed but rather evolves in response to changes in the external environment. While Bitcoin market efficiency has been widely studied, the impact of cryptocurrency heists on its efficiency remains underexplored. Analysing Bitcoin's market efficiency following such incidents can help us better understand their effects on market dynamics, providing investors with clearer investment insights while offering valuable guidance for regulators in formulating more effective policies to maintain market stability.

Existing literature on Bitcoin's market efficiency has primarily examined it through the lens of the EMH. However, a key limitation of this approach is that it views market efficiency as a static concept, assuming that markets are either fully efficient or entirely inefficient, which is inconsistent with the constantly evolving market environment and investor behaviour. As

previous empirical studies have shown, Bitcoin's market efficiency varies under different market conditions. Therefore, market efficiency should be regarded as a dynamic concept that adapts to changing conditions (Lo, 2004). Based on this assumption, it is essential to analyse how Bitcoin's market efficiency evolves before and after cryptocurrency heists from a dynamic perspective to provide a more comprehensive assessment of their impact on market efficiency.

If Bitcoin's market efficiency is affected by cryptocurrency heists, then it is essential to further explore the potential driving factors behind these efficiency changes in the context of such incidents. Behavioural finance theory (Shleifer, 2000; Barberis & Thaler, 2003) suggests that during extreme market incidents, investors may engage in panic-driven trading, exacerbating market inefficiencies. Previous studies have shown that investor sentiment plays a crucial role during black swan events in financial markets (Fisher & Statman, 2000; Zouaoui et al., 2011; Chundakkadan & Nedumparambil, 2022; Hsu & Tang, 2022). It is reasonable to hypothesise that sentiment is also a key factor influencing Bitcoin's market efficiency following cryptocurrency heists. Fear-driven or panic-induced emotional reactions can exacerbate inefficiencies and prolong market instability. For instance, panic selling may lead to excessive volatility and cause prices to deviate from their fundamental values (Baker & Ricciardi, 2014; Lal et al., 2024). Additionally, sentiment-driven trading reduces liquidity (Chiu et al., 2018; Dunham & Garcia, 2021) as investors hesitate to participate in the market during heightened uncertainty, further impairing efficiency. In such an environment, misinformation and herd behaviour can spread rapidly, distorting price discovery and delaying market stabilisation. Given the significant influence of sentiment on trading behaviour, investigating the interaction between price movements and investor sentiment during cryptocurrency heists is essential.

Finally, considering that DeFi has become a crucial component of the cryptocurrency market[1], it is important to acknowledge that while decentralisation may improve financial efficiency, it also introduces significant vulnerabilities to security breaches. In recent years, hacking attacks have increasingly targeted DeFi platforms, yet the existing literature has paid limited attention to how the DeFi ecosystem responds to such incidents. Therefore, broadening the analytical scope beyond Bitcoin is necessary to investigate the potential repercussions of cryptocurrency heists on the DeFi ecosystem. The spillover effects posit that when a shock

[1] According to data provided by Statista (2025), as of February 2025, DeFi accounts for 3.6% of the total cryptocurrency market cap.

occurs in one market or asset, it may transmit through channels such as price linkages, capital flows, and investor sentiment to other related markets or assets, thereby generating broader systemic impacts (Diebold & Yilmaz, 2012). In the DeFi context, although individual platforms are technically independent, they are tightly interconnected through shared investor bases, similar smart contract protocols, and cross-platform liquidity pools. This structural interdependence creates a high potential for contagion effects. When a DeFi platform experiences a critical security breach or a large-scale cryptocurrency heist, the resulting turmoil may not only cause severe fluctuations in the price of its native DeFi token but also undermine investor confidence in the broader DeFi ecosystem. Such fear-driven reactions may trigger panic selling and liquidity withdrawals across other DeFi platforms, potentially transforming a platform-specific incident into a risk affecting the entire DeFi market.

Therefore, by analysing how major DeFi heists (i.e. cryptocurrency heists targeting DeFi platforms) affect both platform-specific token (DeFi token) performance and the broader DeFi market, it could assess whether these incidents generate systemic risks beyond the directly affected platforms. Since DeFi operates without traditional financial intermediaries, understanding its resilience to security breaches is essential for evaluating its long-term sustainability and regulatory needs.

1.3 Aims and Objectives

This thesis aims to systematically investigate the impact of cryptocurrency heists on the cryptocurrency market, including market efficiency, investor sentiment, and risk contagion among different crypto assets. Based on the findings, this thesis will also explore potential regulatory measures to mitigate the adverse effects of cryptocurrency heists, thereby enhancing market stability and investor confidence, and providing policy guidance for building a more secure and sustainable cryptocurrency ecosystem.

The first study (in Chapter 2) of this thesis examines how cryptocurrency heists influence Bitcoin's market efficiency. Within the Adaptive Market Hypothesis (AMH) framework, this chapter analyses the twelve largest cryptocurrency heists (Mt. Gox, Coincheck, KuCoin, PancakeBunny, Poly Network, Bitmart, Wormhole, Ronin Network, Beanstalk, Nomad, Binance and FTX) and their effects on Bitcoin's market efficiency. In contrast to the EMH, which treats market efficiency as a static concept, the AMH views market efficiency as dynamic and evolving in response to external shocks and changes in investor behaviour. Therefore, it is more suitable for examining the impact of unexpected incidents such as

cryptocurrency heists on Bitcoin's market efficiency. This chapter uses the permutation entropy and the Complexity–entropy causality plane to assess changes in Bitcoin's market efficiency the day before, the day of, and the day after the cryptocurrency heist. The findings indicate that Bitcoin's market efficiency declines significantly on the day of and immediately following these cryptocurrency heists, characterised by reduced permutation entropy and increased complexity. Furthermore, the chapter reveals that tokens directly targeted by theft experience even greater efficiency losses compared to Bitcoin. This suggests that investor attention is disproportionately drawn to affected tokens, amplifying their volatility while causing a relatively smaller impact on Bitcoin's efficiency. These results underscore the importance of market stability measures and enhanced security protocols to mitigate the disruptive effects of cryptocurrency heists.

The second study (in Chapter 3) of this thesis investigates the bidirectional predictive relationship between Bitcoin price and market sentiment in the context of cryptocurrency heists from a behavioural finance perspective. Using the Cryptocurrency Fear & Greed Index (CFGI) as a proxy for investor sentiment, this study applies a time-varying Granger causality test to analyse the predictive relationship between Bitcoin price and sentiment before and after the KuCoin exchange heist (large amounts of Bitcoin stolen). The results show that there is no statistically significant bidirectional predictive relationship between Bitcoin price and CFGI 90 days before the KuCoin exchange heist. However, within 90 days of the KuCoin exchange heist, a strong feedback loop emerges, where CFGI fluctuations statistically significantly influence Bitcoin price movements and vice versa. This intensified predictive relationship suggests that heightened uncertainty amplifies investor reactions, potentially creating a cycle of price declines and market panic. Additionally, this chapter finds that the bidirectional predictive relationship between Bitcoin price and CFGI does not always hold after cryptocurrency heists. Only cryptocurrency heists that directly impact Bitcoin exhibit a strong sentiment-price feedback mechanism, whereas those targeting other crypto assets display a weaker predictive relationship. This may be attributed to CFGI primarily measuring sentiment within the Bitcoin market, making it less reflective of fluctuations in other cryptocurrencies. These findings underscore the importance of understanding market sentiment dynamics during periods of heightened uncertainty, as they play a crucial role in shaping price movements and investor behaviour. Finally, this chapter also employs a TVP-VAR-based connectedness approach to examine the impact of CFGI volatility during the KuCoin exchange heist. The results indicate that CFGI fluctuations have a weaker influence

on other cryptocurrencies, such as Ethereum and Binance Coin, than on Bitcoin. This suggests that the effects of CFGI volatility remain primarily confined to the Bitcoin market, with minimal impact on other cryptocurrency markets during the KuCoin exchange heist. As a result, while investors can use CFGI to make short-term trading decisions for Bitcoin during Bitcoin-specific heists, its applicability to other cryptocurrencies may be limited. Relying solely on CFGI may lead investors with diversified cryptocurrency portfolios to draw misleading conclusions, potentially affecting the effectiveness of their investment strategies.

The third study (in Chapter 4) of this thesis expands the analysis beyond Bitcoin to examine the impact of cryptocurrency heists on the DeFi ecosystem. This chapter investigates six major DeFi heists in 2022 (Qubit Finance, Ronin Network, Beanstalk, Maiar Exchange, Binance and Mango Markets) and their effects on the liquidity of the stolen platforms' native DeFi tokens and overall DeFi market stability. Using low-frequency price impact measures (the Amihud illiquidity ratio, the Amivest liquidity ratio, and the Kyle and Obizhaeva estimator) and the Quantile VAR model (QVAR model), the analysis reveals that the liquidity of stolen platforms' native DeFi tokens declines sharply after a DeFi heist. At the same time, the level of interconnectedness among mainstream DeFi tokens is significantly higher than that between the stolen platform's native DeFi token and mainstream DeFi tokens. This indicates that the volatility spillover effect from the stolen platform's native DeFi token to mainstream DeFi tokens is relatively limited. Despite the severe disruption experienced by the affected platform, the overall DeFi market has remained relatively stable. However, if investor confidence in DeFi security deteriorates, for example in the event of attacks targeting DeFi governance mechanisms, market-wide volatility may increase, posing risks to the entire DeFi ecosystem. These findings emphasise the importance of robust security measures, transparency in crisis management, and continuous improvements in DeFi governance to sustain market stability.

1.4 Contributions and Limitations

This thesis makes several significant contributions to the literature on cryptocurrency markets, particularly in the context of cryptocurrency heists and their broader implications. First, it provides a systematic examination of how cryptocurrency heists impact Bitcoin's market efficiency, an area that has remained largely underexplored. While prior studies have primarily assessed Bitcoin's efficiency through the lens of the EMH, this thesis adopts a dynamic framework based on the AMH to capture the evolving nature of market efficiency

before and after cryptocurrency heists. By employing permutation entropy and Complexity–entropy causality plane, this thesis empirically demonstrates that Bitcoin's efficiency deteriorates significantly during most cryptocurrency heists. This finding further indicates that Bitcoin market efficiency is dynamically changing based on the market conditions, and highlights the disruptive impact of security breaches on market stability.

Changes in investor sentiment can influence investor behaviour, potentially leading to fluctuations in market efficiency. Therefore, this thesis further extends its analysis to investor sentiment, representing a critical yet underexplored factor in understanding the bidirectional predictive relationship between price and sentiment during extreme market incidents. By using CFGI to examine the bidirectional predictive relationship between Bitcoin price and investor sentiment, this thesis finds that heists targeting Bitcoin amplify the predictive relationship between sentiment and Bitcoin price dynamics. The heightened uncertainty following such heists strengthens the feedback loop between CFGI fluctuations and Bitcoin price movements, creating a cycle of falling prices and rising panic sentiment. However, this sentiment-price feedback loop appears to be primarily confined to Bitcoin, with limited impact on other major cryptocurrencies. This finding suggests that although the CFGI provides useful insights into Bitcoin price movements during crisis incidents, its applicability to other cryptocurrencies may be limited. This highlights the importance for investors of not relying solely on a single sentiment indicator. Instead, they should take into account the differences in construction methodologies and emphasis across various sentiment measures, and adopt a more comprehensive approach by combining multiple indicators to capture shifts in market sentiment better.

Another key contribution of this thesis is its expansion of the analysis beyond Bitcoin to the DeFi ecosystem, a rapidly growing sector that has increasingly become a target for hacking attacks. While existing literature has largely focused on DeFi's potential, regulation, and risk-return characteristics, little attention has been given to how security breaches affect its liquidity and stability. This thesis fills this gap by investigating major DeFi heists in 2022 and their effects on both the liquidity of stolen platforms' native DeFi tokens and the broader DeFi market. The results show that although DeFi platforms are vulnerable to hacking attacks, such security risks are often localised in nature. In particular, attacks targeting smaller DeFi projects tend to have a limited impact on the broader DeFi ecosystem. However, the results also show a high level of connectivity between mainstream DeFi platforms. When mainstream DeFi platforms are compromised, the consequences can trigger widespread

market contagion. Therefore, to prevent such systemic risks, it is essential to strengthen security mechanisms, improve governance structures, and enhance the transparency of crisis management. These measures are crucial for reducing the likelihood of DeFi-related attacks and maintaining investor confidence in the market.

In addition to its empirical contributions, this thesis advances academic knowledge in three key dimensions. First, it systematically reviews and synthesises major cryptocurrency heists and conceptualises such security breaches as internally rooted shocks with externally disruptive characteristics. This introduces a novel analytical perspective that differs from traditional studies focusing on macroeconomic or policy shocks. By integrating market microstructure theory with behavioural finance, the thesis provides a comprehensive explanation of how security incidents influence market efficiency, investor sentiment, liquidity, and risk transmission mechanisms. Second, this thesis integrates a variety of analytical tools in terms of methodology. It not only adopts commonly used event study methods, Granger causality tests, and liquidity indicators, but also introduces models and methods that are less commonly used in security event analysis. For example, it introduces methods such as permutation entropy and the Complexity–entropy causality plane in market efficiency analysis to more sensitively capture the dynamic changes in efficiency under the impact of security events, thus providing a methodological supplement to the study of market reactions under extreme events. Third, this thesis offers new insights into risk transmission by uncovering the mechanisms through which security breaches propagate within the DeFi ecosystem. By distinguishing between the strong internal interconnectedness of mainstream DeFi tokens and the comparatively weaker spillover effects from peripheral DeFi tokens to the mainstream, the findings show that project heterogeneity and the presence of mainstream DeFi tokens help to localise the impact of hacking incidents and mitigate disruption. However, the results also reveal that contagion can intensify when compromised DeFi platforms share similar governance mechanisms with other platforms, amplifying market reactions. These findings underscore the importance of robust governance frameworks and security design for preserving stability in the rapidly evolving DeFi landscape, and they deepen our understanding of risk diffusion mechanisms in the DeFi market.

Despite these contributions, this thesis has several limitations. First, the study focuses on selected cryptocurrency heists, meaning that its findings may not be fully generalisable to all security breaches within the cryptocurrency market. The selected cases primarily involve well-known heists with large-scale thefts, while smaller-scale hacking incidents or internal

fraud remain underexplored. Different types, scales, and degrees of cryptocurrency heists may also influence market reactions differently, yet they are not comprehensively examined in this study. Second, the CFGI presents several methodological constraints. While Alternative.me discloses the index's six components' weighting scheme, it does not provide their underlying numerical values, thereby preventing detailed component-level analysis. As a result, it is challenging to determine which factors predominantly drive sentiment fluctuations during critical events such as cryptocurrency heists. A valuable direction for future studies would be to disentangle the relative contributions of market-based components (e.g., volatility and trading volume) and behavioural components (e.g., social media activity and search intensity). Doing so would enhance understanding of whether sentiment shifts are primarily driven by objective market dynamics or by behavioural responses. Future studies could address this limitation by employing sentiment indices that allow component-level decomposition or by constructing new sentiment measures capable of isolating heterogeneous drivers of market sentiment.

Thirdly, the study's analysis of market efficiency is primarily focused on short-term effects, examining efficiency changes before, during, and immediately after cryptocurrency heists. While this approach captures immediate market disruptions, it does not account for the long-term recovery process or potential structural changes in market efficiency over time. Future studies could extend this analysis by investigating whether efficiency gradually returns to pre-heist levels or whether certain inefficiencies persist due to lingering market uncertainty. Fourthly, the liquidity analysis of DeFi tokens relies on low-frequency price impact measures, which, while useful, may not fully capture real-time liquidity dynamics in decentralised markets. Given that DeFi operates through automated market makers (AMMs) rather than traditional order books (Mohan, 2022), incorporating high-frequency liquidity indicators could offer deeper insights into how liquidity providers respond to security breaches.

Finally, this thesis does not explicitly consider the role of regulatory responses or institutional actions following cryptocurrency heists. Government interventions, such as asset freezes, trading suspensions, or legal actions against perpetrators, may significantly influence market sentiment and efficiency, but these factors fall outside the scope of this thesis. Moreover, cryptocurrency regulation is currently in a state of high complexity and ongoing evolution. For example, the European Union has adopted the Markets in Crypto-Assets (MiCA) framework to establish a unified regulatory environment. In contrast, the United States continues to lack a coherent regulatory system, with different agencies offering conflicting

guidance on how to classify and regulate digital assets. China, by comparison, has taken a prohibition-based approach. These divergent regulatory paths raise an important question for future research: which regulatory model—proactive and harmonised (EU), fragmented yet enforcement-driven (US), or prohibitive (China)—is most effective in maintaining market stability and protecting investors in the aftermath of major security incidents? As regulatory frameworks continue to develop globally, future studies could explore how different regulatory responses to security incidents affect market stability and investor confidence.

Overall, this thesis offers a comprehensive and novel contribution to the understanding of how cryptocurrency heists affect market efficiency, investor sentiment, and DeFi market stability. By integrating multiple methodological approaches and extending the analysis beyond Bitcoin to DeFi, this thesis provides valuable insights for investors, market participants, and policymakers seeking to navigate the risks associated with security breaches in the cryptocurrency ecosystem. The remainder of this thesis is structured as follows. Chapter 2 empirically investigates the impact of cryptocurrency heists on Bitcoin's market efficiency. Using permutation entropy and the Complexity–entropy causality plane within the framework of the AMH, it examines how efficiency dynamically evolves before and after major hacking incidents. Chapter 2 extends the analysis to investor sentiment, exploring the bidirectional predictive relationship between Bitcoin price movements and sentiment during security breaches. Employing the time-varying Granger causality test, it provides new insights into the sentiment-price feedback loop under extreme market stress. Chapter 4 shifts the focus to the DeFi ecosystem, analysing how major DeFi heists affect token liquidity and cross-platform contagion using the low-frequency price impact measures and the QVAR model. Finally, Chapter 5 concludes the thesis by summarising the main findings, discussing their theoretical and practical implications, highlighting limitations, and proposing a clear agenda for future studies.

Chapter 2 The Impact of Cryptocurrency Heists on Bitcoin's Market Efficiency

Parts of this chapter have been published in the International Journal of Finance and Economics

2.1 Introduction

Do cryptocurrency heists affect the market efficiency of the Bitcoin market? This chapter examines this substantial risk posed to the Bitcoin market (Krückeberg & Scholz, 2020; Lyócsa et al., 2020; Corbet et al., 2020a) by the presence of cryptocurrency hacking incidents on the platforms where cryptocurrencies are traded. Cryptocurrency heists have led to more than $12 billion in stolen funds. When we account for rising cryptocurrency prices, if hackers were to liquidate all stolen cryptocurrencies today, their total wealth would surpass $50 billion (Tsihitas, 2025). These cryptocurrency heists, which have been increasing in both frequency and magnitude, have significantly impacted the cryptocurrency community, directly affecting investor trust, shaking market confidence and may cause investors to exit the market.

Bitcoin is the most popular cryptocurrency, but its price has experienced extreme volatility since its inception, soaring from one cent to approximately $66,000 in 2021 before dropping to $16,000 in early 2023 and substantially increasing to around $100,000 in 2024 (CoinGecko, 2024). This extreme volatility has altered how people view the function and role of Bitcoin, from being a cryptocurrency to being increasingly perceived as a financial asset (Yermack, 2024; Baek & Elbeck, 2015; Baur et al., 2018). While Bitcoin and other cryptocurrencies have emerged as a new investment sector, their high volatility challenges monetary authorities and impacts the financial system. The unique market environment of cryptocurrency results in market efficiency dynamics that differ from traditional financial assets. For example, the relative immaturity of the cryptocurrency market, with a large proportion of retail investors, often leads to decisions driven more by sentiment and speculation than by rational analysis (Rudkin et al., 2023; Brini & Lenz, 2024). This market immaturity often leads to heightened price volatility. Additionally, because the regulatory environment for cryptocurrencies is still developing, the market is particularly vulnerable to manipulation and fraud (Eigelshoven et al., 2021). Manipulative practices (e.g. pump-and-dump schemes) are common in the cryptocurrency market. These activities disrupt normal

market operations, preventing prices from accurately reflecting true information. Lastly, the rapid development of blockchain technology, while enhancing transparency and information dissemination, also introduces instability due to smart contract vulnerabilities and scalability challenges (Ghosh et al., 2020; Singh et al., 2021). Therefore, scholars believe that examining cryptocurrency's market efficiency across different contexts is crucial for understanding its pricing mechanisms and stability (Naeem et al., 2021a; Aslam et al., 2023). As the frequency of cryptocurrency heists increases, understanding their impact on market efficiency is essential for investors to adjust strategies and for policymakers to implement effective regulations.

This chapter employs the Adaptive Market Hypothesis (AMH) framework to examine Bitcoin's market efficiency changes during the twelve largest cryptocurrency heists (Mt Gox, Coincheck, KuCoin, PancakeBunny, Poly Network, Bitmart, Wormhole, Ronin Network, Beanstalk, Nomad, Binance and FTX). As cryptocurrency heists mainly involve multiple tokens, this chapter also considers if the token(s) predominantly stolen within cryptocurrency heists are explanatory. Adopting an Econophysics approach, this chapter uses permutation entropy and Complexity–entropy causality plane to measure Bitcoin's dynamic market efficiency during multiple cryptocurrency heists. The results show that Bitcoin's market efficiency fluctuates over time, with significant drops in permutation entropy during many cryptocurrency heists, indicating a decline in efficiency. Furthermore, it also finds that different tokens react differently to cryptocurrency heists, with variable market efficiency and volatility. Specifically, investors tend to focus more on the token(s) most affected by cryptocurrency heists, resulting in greater volatility and more pronounced declines in those tokens' market efficiency. According to AMH, external changes lead to dynamic fluctuations in market efficiency. If investors fail to adapt, efficiency declines due to maladaptive behaviour. The uncertainty and chaos from a cryptocurrency heist make it hard for investors to quickly process and analyse new information, delaying rational decision-making and triggering emotional reactions like panic selling or buying. This causes prices to deviate from their true price, reducing market efficiency. However, market efficiency may recover as new information is gradually absorbed and investors adjust.

This study is essential for many reasons, including the safety and stability of the Bitcoin market, the protection of investors, and perhaps most of all, the scale, growing frequency, and increasing magnitude of these hacking incidents. The Bitcoin market relies on trust and transparency among participants, and cryptocurrency heists could trigger investor concerns

about the security of cryptocurrency platforms, prompting investors to sell off their holdings to avoid losses. This fear may lead to a herd effect in the market, amplifying volatility and generating further market inefficiency (Bouri et al., 2019; Gurdgiev & O'Loughlin, 2020; Raimundo Júnior et al., 2022). Further, some cryptocurrency platforms lack adequate security measures to protect customer assets, and the anonymity and irreversibility of cryptocurrency transactions make these thefts challenging to trace. This allows cryptocurrency thieves to exploit vulnerabilities and steal assets. After a platform suffers an attack, investors often struggle to obtain comprehensive details or accurately assess future risks. This uncertainty exacerbates information asymmetry, further affecting market efficiency (Barron & Qu, 2014; Hu & Prigent, 2019).

The findings offer important insights for both investors and policymakers. Investors should adapt strategies in response to changing external conditions. When the market is disrupted, efficiency may temporarily decline, so investors should avoid rigid strategies and instead continuously assess market signals and adapt to new environments. During cryptocurrency heists, investors could use high-frequency data and automated tools to respond swiftly, minimising losses caused by delayed market reactions. Additionally, diversifying holdings could reduce individual token volatility, mitigating risks in periods of inefficiency. For policymakers, these fluctuations highlight the need for stronger regulatory frameworks. Enhancing oversight of cryptocurrency exchanges through higher security standards and regular audits could help reduce the risk of cryptocurrency heists. Requiring timely disclosure of security breaches will also enable the market to react more quickly, minimising the impact of information asymmetry on market efficiency.

The contribution to the literature is examining cryptocurrency heists and their influence on market efficiency. While numerous scholars have explored multiple financial issues within the Bitcoin market (Corbet et al. 2019a) and have repeatedly examined Bitcoin and its market efficiency, the impact of cryptocurrency heists remains an overlooked area. Recent literature on Bitcoin's market efficiency has focused on specific timeframes (Urquhart, 2016; Bariviera, 2017; Jiang et al., 2018; Yi et al., 2022) or global crises like the COVID-19 pandemic (El Montasser et al., 2022; Kakinaka & Umeno, 2022; Wu et al., 2022). Similarly, the impact of launching Bitcoin derivatives (Köchling et al., 2019; Ruan et al., 2021; Shynkevich, 2021; Strych, 2022) and altering regulatory frameworks (Alexander & Heck, 2020; Shanaev et al., 2020) have also been examined. This study contributes to this contemporary literature on the

market conditions influencing Bitcoin's market efficiency by examining the impact of cryptocurrency heists.

This chapter is structured as follows. The second section reviews the literature review, and the third discusses the data and methodology. The fourth section reports empirical results, and the fifth section provides conclusions and implications for investors and policymakers and explores future study directions.

2.2 Literature Review

A voluminous literature has examined Bitcoin's market efficiency. This work can be divided into efficiency testing and identifying factors affecting market efficiency. Most efficiency tests indicate that Bitcoin's market is inefficient. However, as the market matures and improves in areas like liquidity, derivatives adoption, and government regulation, the Bitcoin market may become efficient.

2.2.1 Bitcoin Market Efficiency Test

A starting point for testing market efficiency is randomness tests. Urquhart (2016) used daily Bitcoin returns as samples and conducted the Ljung–Box, Runs, Bartels, AVR, BDS, and R/S Hurst tests. The findings indicated that the Bitcoin market was inefficient between August 1, 2010, and July 31, 2016. Nadarajah and Chu (2017) conducted the same tests on the odd integer powers of Bitcoin returns, providing conflicting results. Tiwari et al. (2018) used seven robust long-term dependency estimators to evaluate market efficiency, reporting that the Bitcoin market was generally efficient between 2010 and 2017, with some exceptions occurring from April to August 2013 and August to November 2016.

These methods have also examined the causes of Bitcoin market inefficiency. Kang et al. (2022) assessed Bitcoin's market efficiency using the Runs, Durbin–Watson, and variance ratio tests after the 2017 price surge and concluded that speculative investment led to market inefficiency. Zargar and Kumar (2019) used a series of variance ratio tests and found that low-frequency Bitcoin returns followed a memoryless stochastic process from 2013 to 2018, indicating market efficiency. However, this result may have been misleading, as high-frequency traders could gain additional returns over time through speculation.

The second way to test market efficiency is to examine the multifractal properties of time series. For example, Bariviera (2017), Alvarez-Ramirez et al. (2018), and Al-Yahyaee et al. (2018) used the Hurst exponent, reporting that between 2011 and 2014, the Hurst exponent

was generally above 0.5, indicating a long-term dependence on daily returns and inefficiency in the Bitcoin market. Jiang et al. (2018), Takaishi (2018) and Yi et al. (2022) used the generalised Hurst exponent and found that from 2010 to 2018, the Bitcoin market exhibited long-term dependence, indicating inefficiency. Kakinaka and Umeno (2022) applied the asymmetric multifractal detrended fluctuation analysis (A-MFDFA) method and the generalised Hurst exponent, and their results showed that following the COVID-19 pandemic, market efficiency was strong in the long-term but weak in the short term. This suggests that a herd effect operates in the cryptocurrency market during black swan events like pandemics, leading to market inefficiency.

2.2.2 Factors Affecting Bitcoin Market Efficiency

The above multifractal methods have also been employed to identify factors affecting Bitcoin's market efficiency. Commonly discussed factors include (i) liquidity, referring to how easily Bitcoin can be bought and sold; (ii) the impact of derivatives, which could improve market efficiency by enhancing liquidity, providing hedging opportunities, and improving price discovery; and (iii) regulatory policies, which could offer a stable, transparent environment for investors and potentially improve market efficiency.

Brauneis and Mestel (2018) used the Corwin–Schultz spread estimator, log-market capitalisation, turnover ratio, and Amihud illiquidity ratio to examine liquidity. They found that as liquidity increased, Bitcoin's market efficiency improved. Wei (2018) and Takaishi and Adachi (2020) also used the Amihud illiquidity ratio and found that Bitcoin's market efficiency improved after 2017. These authors proposed that lower liquidity resulted in fewer active traders and slower responses to new information, reducing market efficiency. Conversely, more liquid markets attract active traders who can act on new information, improving efficiency. Al-Yahyaee et al. (2020) examined the relationships between the market transaction value and Bitcoin market value to quantify liquidity, discovering that improved liquidity enhanced market efficiency while greater volatility reduced market efficiency.

Multiple studies have also examined the introduction of cryptocurrency derivatives, producing some conflicting findings. Köchling et al. (2019) argued that the introduction of Bitcoin futures reduced barriers for institutional investors and provided a way to short Bitcoin. Their study applied Urquhart's (2016) methodology to discover that Bitcoin's market efficiency improved after the futures launch. This is important as previous studies have

displayed that the participation of institutional investors and short-selling can improve market efficiency (Boehmer & Kelley, 2009; Saffi & Sigurdsson, 2011). Shynkevich (2021) employed technical analysis and revealed that before the introduction of Bitcoin futures, returns were significantly predictable, but technical trading rules became less effective after these derivatives were introduced. Distinctly, Ruan et al. (2021) used multifractal detrending moving-average cross-correlation analysis and non-linear Granger causality tests, demonstrating a strong positive correlation between Bitcoin spot and futures returns, indicating that futures improved the spot market's efficiency. Lastly, Strych (2022) examined the effects of margin trading and short selling on Bitcoin's market efficiency, finding that efficiency declined when both were introduced. High levels of market efficiency were also recorded when only short selling was allowed, suggesting margin trading was the main reason for the decline in efficiency.

While some cryptocurrency trading platforms, such as Coinbase, actively comply with regulatory requirements, many others—including BitMEX and Huobi Global—enable trading in largely unregulated environments, particularly in derivatives markets where extreme leverage (e.g., 100 × leveraged contracts) is common. Using minute-level data, Alexander and Heck (2020) compared price discovery across spot exchanges, perpetual contracts, and both regulated and unregulated futures markets to assess the influence of regulatory oversight. Their findings indicated that Bitcoin prices on unregulated derivatives exchanges were vulnerable to manipulation via high-frequency trading strategies, demonstrating inefficiencies in the Bitcoin market. Moreover, their results underscored the need for stronger regulatory involvement and harmonised legislative frameworks in cryptocurrency derivatives markets to enhance overall market efficiency and stability. Shanaev et al. (2020) used data from 120 regulatory interventions to examine how cryptocurrency markets responded to changes in regulatory oversight. However, they found that announcements concerning anti-money-laundering measures or foreign exchange controls did not significantly alter market efficiency, while notable price reactions occurred only on the announcement day. This suggests that the cryptocurrency market exhibits characteristics of weak-form efficiency, where prices adjust rapidly to publicly available information but do not fully incorporate all relevant information. They also argued that excessive regulatory intervention could hinder the development of the cryptocurrency industry. Allowing the market to operate within a more accessible and innovation-friendly regulatory environment could, therefore, reduce volatility and enhance price stability.

2.2.3 Adaptive Market Hypothesis

Empirical evidence in the literature suggests that market efficiency may vary over time, and external changes can drive shifts in efficiency. This implies that market efficiency is not static but dynamically evolves in response to environmental conditions. Therefore, the traditional Efficient Market Hypothesis (EMH), which categorises markets as simply efficient or inefficient, may not adequately explain the observed fluctuations in market efficiency.

One of the core assumptions of EMH is that investors are fully rational. According to Fama (1965), the influence of irrational behaviour is negligible, as it is offset by more rational market participants. However, an increasing number of behavioural finance studies have shown that irrational behaviour is both persistent and widespread. Phenomena such as the Ellsberg Paradox, loss aversion, and probability matching demonstrate that cognitive biases are common. Moreover, major financial events such as the dot-com bubble and the subprime mortgage crisis further reflect the prominent role of irrationality in financial markets. Therefore, rational expectations constitute only one aspect of investor behaviour and cannot fully capture all market dynamics.

In contrast to the assumption of full rationality under the EMH, Simon (1990) proposed the theory of bounded rationality. He argued that investors face decision-making costs and stop processing information when the marginal benefit equals the marginal cost. As a result, investors seek satisfactory rather than optimal decisions. However, critics argue that this theory assumes investors already know what the optimal decision is, otherwise, they would be unable to assess the value of further optimisation.

To address this criticism, Lo (2004) contended that investors do not need prior knowledge of optimal decisions. Instead, they form heuristics through trial and error. Their decisions generate feedback, which in turn influences future behaviour. Sentiment plays a crucial role in this feedback process. When investors receive positive feedback, they are likely to retain the heuristic; when feedback is negative, they adjust. As market conditions change, previously effective heuristics may become obsolete, leading to suboptimal behaviour. Lo (2004) referred to such behaviour not as irrationality, but as maladaptation—actions based on outdated heuristics in a new environment.

Building on this perspective, Lo (2004) integrated insights from sociobiology, evolutionary psychology, and evolutionary dynamics to propose the Adaptive Market Hypothesis (AMH). When market participants fail to adapt to market changes and exhibit maladaptive behaviour,

the market becomes inefficient. However, when market participants adjust to new market conditions through feedback, their behaviour aligns with the current market environment and efficiency returns (Lo, 2004). The adaptive behaviour of market participants does not occur independently of market forces but is driven by competition. The current market environment is the result of interactions among different participants. Self-interested individuals, competition, adaptation, natural selection, and environmental conditions form efficient markets (Lo, 2005).

The AMH not only explains the phenomena addressed by EMH but also accounts for behavioural anomalies that EMH cannot. These anomalies are interpreted as maladaptive behaviours rather than pure irrationality. As such, the AMH serves as an evolutionary alternative to the EMH. It asserts that market efficiency may appear and disappear over time as market conditions change. When investors fail to adapt, the market becomes inefficient; when they adjust, efficiency is restored. Thus, the predictability of returns emerges and fades in a cyclical, environment-driven manner.

AMH has been examined in multiple studies. Khuntia and Pattanayak (2018) used the Dominguez–Lobato conformance and the generalised spectral test in a rolling window to account for linear and non-linear correlations in Bitcoin returns from 2010 to 2017. Their results showed that market efficiency varied over time, with inefficient markets recorded from 2010–2012 and 2013–2014 and efficient markets observed between 2012–2013 and 2015–2017. These inconsistencies were associated with changes in the external financial environment, supporting the AMH. Similarly, Stosic et al. (2019) used the Complexity–entropy causality plane to find that Bitcoin and other major cryptocurrency markets moved between efficient and inefficient states over time. Khursheed et al. (2020) reached similar conclusions, adding an automatic portmanteau test to assess Bitcoin's AMH. These findings showed that price movements with linear and non-linear dependencies change over time, resulting in market efficiency falling during unstable conditions and market efficiency improving when conditions stabilise. Mokni et al. (2024) used the adjusted market inefficiency magnitude (AMIM) metric and a quantile regression model to show that Bitcoin's market efficiency fluctuates over time. They also identified how various factors influence market efficiency. Specifically, rising global financial stress tends to decrease market efficiency, while increased liquidity enhances it. Among the factors considered, liquidity appears to be the primary driver of changes in market efficiency.

In summary, previous studies have primarily tested for weak efficiency within the Bitcoin market. These studies have produced divergent findings, indicating that Bitcoin's market efficiency varies over time (Khursheed et al., 2020). Subsequently, the AMH has been applied to explain the dynamic nature of market efficiency, whereby environmental factors influence market efficiency. AMH is not a replacement for the EMH but helps to explain its empirical variations, offering a better understanding of time-varying efficiency (Patil & Rastogi, 2019; Khursheed et al., 2020), with current studies supporting the detection of Bitcoin's market efficiency using this AMH framework (Khuntia & Pattanayak, 2018; Chu et al., 2019; Khursheed et al., 2020; Noda, 2021; López-Martín, 2023).

However, most studies have focused on changes in Bitcoin's market efficiency within a specific timeframe or in the context of global events like the COVID-19 pandemic, while neglecting specific events within the cryptocurrency market, such as cryptocurrency heists. This oversight may hinder a full understanding of the impact of internal market events on Bitcoin's market efficiency and the vulnerabilities of the cryptocurrency ecosystem. Chawki (2022) discussed how cryptocurrencies have become targets for hacking, phishing, malware, extortion, and ransomware. The study highlighted the need for market participants to consider cryptocurrency security and the importance of developing appropriate regulatory measures. Current studies on the effects of cryptocurrency heists primarily centre on cryptocurrency market stability (Caporale et al., 2020; Corbet et al., 2020a), with less attention given to market efficiency, and the results are mixed. For instance, Krückeberg and Scholz (2020), using high-frequency Bitcoin data, identified significant arbitrage opportunities following cryptocurrency heists, indicating market inefficiency. In contrast, using daily data, Yousaf et al. (2021) found no evidence of herding behaviour during cyberattacks, suggesting high market efficiency. These differences may stem from variations in data scope and frequency, with high-frequency data potentially offering better insights into the short-term impacts of hacker attacks on the market. Moreover, the existing studies have focused only on post-heist market efficiency, neglecting to compare efficiency before and after the incident. This gap may lead to an incomplete understanding of cryptocurrency heists. By comparing market efficiency before and after a cryptocurrency heist, we can better assess the incident's impact and the speed of market recovery. Therefore, this chapter aims to address this gap by examining the issue within the AMH framework, contributing to the literature on the impact of cryptocurrency heists on market efficiency.

2.2.4 Application of the Permutation Entropy Model in Market Efficiency

Given that the existing literature has systematically examined different methods of testing market efficiency in the context of Bitcoin, a further question arises as to how to choose an appropriate approach to capture the dynamic evolution of market efficiency under extreme shocks. Among the various complexity-based measures, the permutation entropy model (Bandt & Pompe, 2002) is particularly suitable, as it effectively distinguishes random noise from deterministic structures and has been validated in studies of efficiency in stock, bond, and commodity markets.

The permutation entropy can capture the disorder and complexity within a time series, thereby revealing the dynamic changes in the market when it experiences external shocks. The underlying idea is that if asset prices follow a random walk hypothesis, converting them into a numerical sequence according to specific rules will result in disorder, with entropy reaching its maximum value. Conversely, if a relationship exists between past and future prices, the numerical sequence will display specific patterns, and entropy will not reach its maximum. Thus, calculating the price change entropy relative to the maximum entropy can reflect the predictability of the asset and quantify the current market efficiency (Zunino et al., 2010).

Zanin et al. (2012) highlighted the potential applications of permutation entropy in economics and finance. They argued that assessing market efficiency and development is a central issue in economics, and since market indicators' time series are often the only available objective information, they naturally serve as the basis for testing the EMH. In this context, permutation entropy can distinguish between deterministic chaos and random noise, and through the "forbidden patterns" method (i.e., ordinal patterns that are theoretically possible but never observed in the actual series) proposed by Bandt and Pompe (2002), it can uncover deterministic structures in financial time series. Empirical evidence shows that the number of forbidden patterns in different financial indicators, such as the Dow Jones Index, Nasdaq Index, IBM and Boeing stock prices, and the U.S. ten-year Treasury yield, is far greater than expected under randomness, and their temporal evolution reveals when markets shift from deterministic behaviour to being dominated by noise (Zanin, 2008).

A growing body of literature further confirms the usefulness of permutation entropy in detecting market efficiency. Zunino et al. (2009) compared 32 stock markets and found that developed markets exhibit fewer forbidden patterns and higher efficiency, while emerging

markets display greater predictability. Building on this idea, Zunino et al. (2010, 2011, 2012) introduced the Complexity–entropy causality plane to characterise efficiency in stock, commodity, and sovereign bond markets, effectively distinguishing between developed and emerging economies. Hou et al. (2017) examined the temporal evolution of permutation entropy in the Chinese stock market and found that permutation entropy declined significantly during two critical periods, each characterised by a rapid market boom followed by several severe crashes. Siokis (2018) employed permutation entropy and the Complexity–entropy causality plane to investigate the dynamics of informational efficiency in selected instruments from the U.S. money, bond, and stock markets around the Great Recession. The results revealed that, following the credit crunch and the collapse of Lehman Brothers, the efficiency of certain money market instruments decreased markedly, while the efficiency of stock market indices and bond market instruments remained relatively high.

Nevertheless, studies applying permutation entropy to Bitcoin remain limited. Lahmiri et al. (2018) found that Bitcoin returns from 2010 to 2017 were not random, indicating low efficiency. Sensoy (2019), using high-frequency data from 2013 to 2018, showed that the BTC/USD market was more efficient than the BTC/EUR market and that efficiency improved after 2016. Fernandes et al. (2022) employed permutation entropy and Fisher information to construct the Shannon–Fisher causality plane and analysed five cryptocurrencies before and after COVID-19. Their findings revealed high informational efficiency across these markets, with prices largely unpredictable.

In sum, permutation entropy has been widely applied to the study of efficiency across different markets and assets. It effectively distinguishes random noise from deterministic structure and captures the dynamic evolution of efficiency. Therefore, when examining Bitcoin's market efficiency under cryptocurrency heists, permutation entropy provides a suitable and reliable tool to capture the shift in market efficiency.

2.3 Data and Methodology

2.3.1 Data Selection and Variable Description

Alexander and Dakos (2020) reviewed 152 published papers and Social Science Research Network (SSRN) discussion papers on cryptocurrency data. Their analysis revealed that over 80 of these studies had issues related to data selection, including unreliable data sources, the use of non-concurrent time series data in multivariate analysis, and reliance on prices that did

not reflect actual transaction values. Consequently, they emphasised that discrepancies in data sources can lead to inconsistent findings, highlighting the need for scholars to exercise caution when selecting cryptocurrency data. Scholars face two challenges when selecting Bitcoin data: (i) determining daily prices and (ii) the data source. Vidal-Tomás (2021) found differences in the scaling features of Bitcoin returns calculated using closing prices (last price on each day), following a Brownian motion, versus weighted prices (the average of the prices across the 24-h period), which deviate from this random process. This study noted that scholars using closing prices perceive the market as exhibiting weak efficiency, whereas those using weighted prices report inefficient market conditions. Therefore, using differently calculated daily prices can lead to varying outcomes.

Additionally, Vidal-Tomás (2022) used the generalised Hurst exponent to analyse main cryptocurrency databases' scaling properties and underlying processes, including USD trading platforms (e.g. Coinbase), USD databases, which limit cryptocurrency price calculations to USD (e.g. Cryptocompare), and USD (cross-rate) databases, which are calculated by converting any non-US dollar cross rate into US dollars using the foreign exchange rate (e.g. CoinMarketCap, CoinGecko). All sources reported time series with the same underlying characteristics, suggesting that using different sources to calculate a unified Bitcoin price does not distort its underlying process. Therefore, the data source had minimal impact on Bitcoin's market efficiency studies.

In summary, the method used to calculate daily prices significantly impacts the results, while the choice of data source has relatively less influence. This chapter chooses Cryptocompare as the data source, which uses the closing price as the price proxy. Unlike weighted methods, the closing price more accurately reflects actual trading prices. Since cryptocurrency heists often happen quickly, typically within minutes or hours, low-frequency data might miss these fluctuations. Therefore, this chapter uses Bitcoin's 1-minute closing price in USD as the variable.

Tsihitas (2025) recorded the twelve largest cryptocurrency heists based on the stolen dollar amount. To investigate the impact of these cryptocurrency heists on Bitcoin's market efficiency, this chapter examines the changes in market efficiency on the day before, the day of, and the day after each cryptocurrency heist. From a theoretical perspective, in the cryptocurrency market, the most pronounced changes in price liquidity typically occur within 48 to 72 hours following a negative shock (Corbet et al., 2019b; Chu et al., 2019). Moreover,

news of cryptocurrency heists spreads rapidly across social media platforms such as Twitter, Reddit, and Telegram, enabling investors to react almost immediately after the incident (Guégan and Renault, 2021; Naeem et al., 2021b, 2021c). From a practical standpoint, this study aims to investigate the short-term direct effects of cryptocurrency heists on the Bitcoin market while minimising the influence of longer market fluctuations. A three-day event window is well-suited to capturing the impact of the shock while avoiding the introduction of noise from unrelated market dynamics, thereby improving the causal interpretation of the results. Table 2.1 presents the twelve largest cryptocurrency heists, spanning from 2014 to 2022, and displays the data range associated with each incident.

Table 2.2 reports the descriptive statistics of Bitcoin prices during the twelve cryptocurrency heists. The results indicate that price fluctuations across these incidents were substantial. For example, in the cases of the Bitmart exchange and PancakeBunny platform, the price ranges reached $13,757.79 and $10,964.63, respectively, suggesting considerable market turbulence. Moreover, the Jarque–Bera (JB) test indicates that Bitcoin prices deviate from normality in most cases, characterised by negative skewness and platykurtic kurtosis. This pattern implies a higher probability of extreme values in the left tail of the distribution, reflecting an increased likelihood of price declines during such incidents.

Table 2.1: Twelve cryptocurrency heists data range

Platform	Data range
Mt Gox	February 23, 2014, to February 25, 2014
Coincheck	January 25, 2018, to January 27, 2018
KuCoin	September 24, 2020, to September 26, 2020
PancakeBunny	May 19, 2021, to May 21, 2021
Poly Network	August 9, 2021, to August 11, 2021
Bitmart	December 3, 2021, to December 5, 2021
Wormhole	February 2, 2022, to February 4, 2022
Ronin Network	March 28, 2022, to March 30, 2022
Beanstalk	April 15, 2022, to April 17, 2022
Nomad	August 1, 2022, to August 3, 2022
Binance	October 6, 2022, to October 8, 2022
FTX	November 10, 2022, to November 12, 2022

Source: https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/

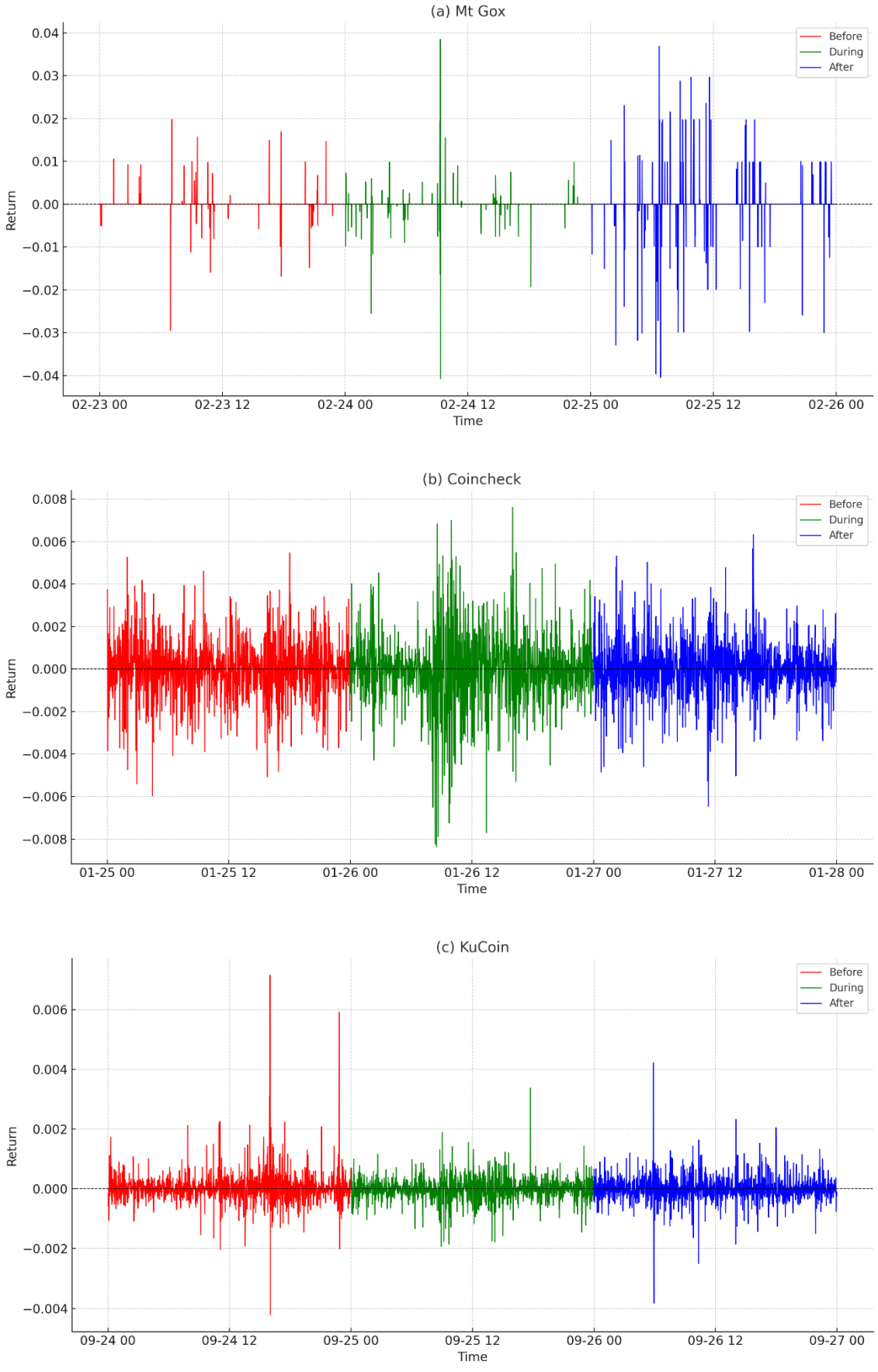
Table 2.2: Descriptive statistics of Bitcoin prices in twelve cryptocurrency heists

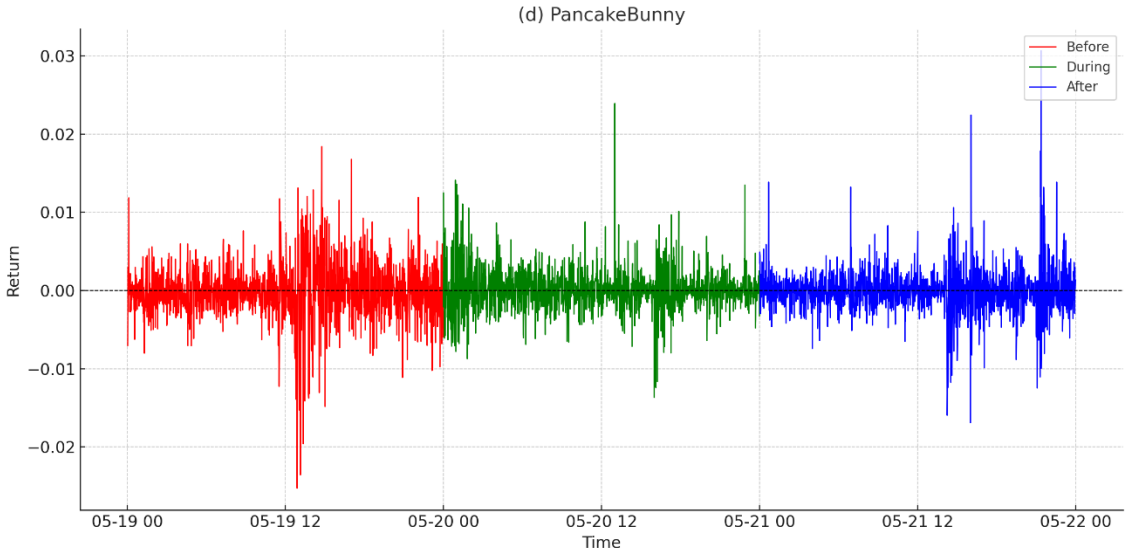
Platform	Obs	Mean	S.Dev.	Min	Max	Skew	Kurt	JB	ADF
Mt Gox	4320	573.76	45.12	450.00	645.64	-0.45	-0.86	280.90***	-2.65
Coincheck	4320	11186.00	274.12	10334.25	11723.02	-0.73	0.22	394.57***	-2.07
KuCoin	4320	10617.59	151.40	10223.14	10802.32	-1.22	-0.14	1072.30***	-1.85
PancakeBunny	4320	39379.49	1786.70	32600.00	43564.63	-0.77	0.49	467.58***	-2.98
Poly Network	4320	45524.68	878.73	42844.25	46746.73	-1.50	1.32	1923.50***	-2.02
Bitmart	4320	51350.70	3502.54	43781.92	57539.71	0.52	-1.35	521.40***	-0.94
Wormhole	4320	37852.60	1163.26	36277.29	41702.14	1.15	0.59	1019.70***	0.093
Ronin Network	4320	47372.66	288.08	46674.65	48184.74	0.15	-0.45	52.91***	-3.49**
Beanstalk	4320	40314.85	171.33	39580.56	40704.14	-0.83	0.72	593.05***	-2.26
Nomad	4320	23124.10	227.39	22673.61	23605.82	-0.04	-1.35	327.02***	-2.40
Binance	4320	19803.66	312.85	19276.37	20437.75	0.21	-1.43	399.50***	-3.21*
FTX	4320	16941.34	399.65	15678.51	18105.93	0.18	0.09	25.99***	-2.96

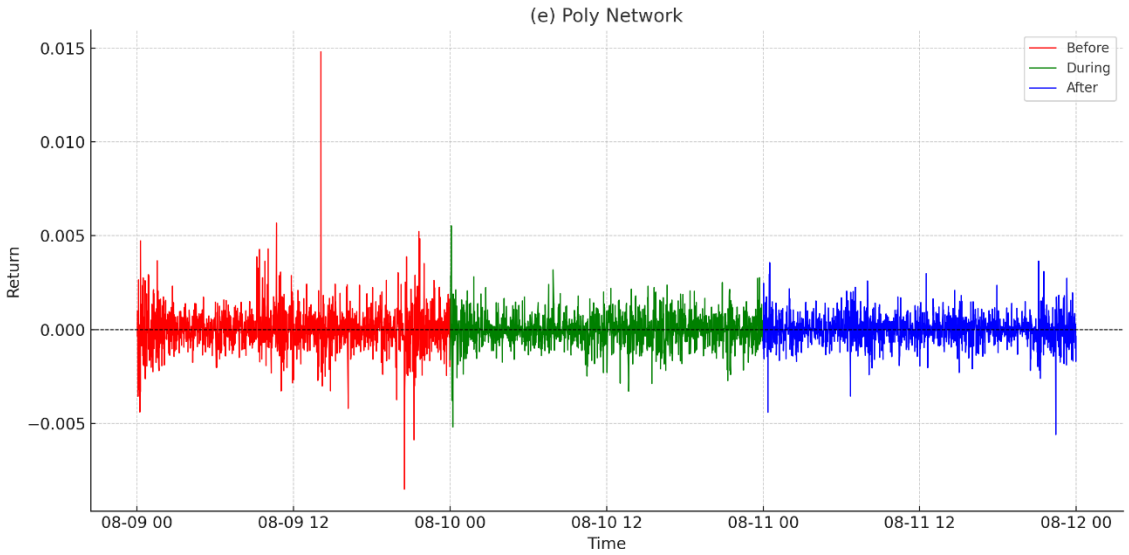
The data source is from Cryptocompare; **Skew:** Skewness, it is a measure of symmetry; **Kurt:** Kurtosis, it is a measure of whether the data are heavy-tailed or light-tailed relative to a normal distribution; **JB:** Jarque–Bera test; **ADF:** Augmented Dickey–Fuller test; *** At the 1% significance level; ** At the 5% significance level; * At the 10% significance level

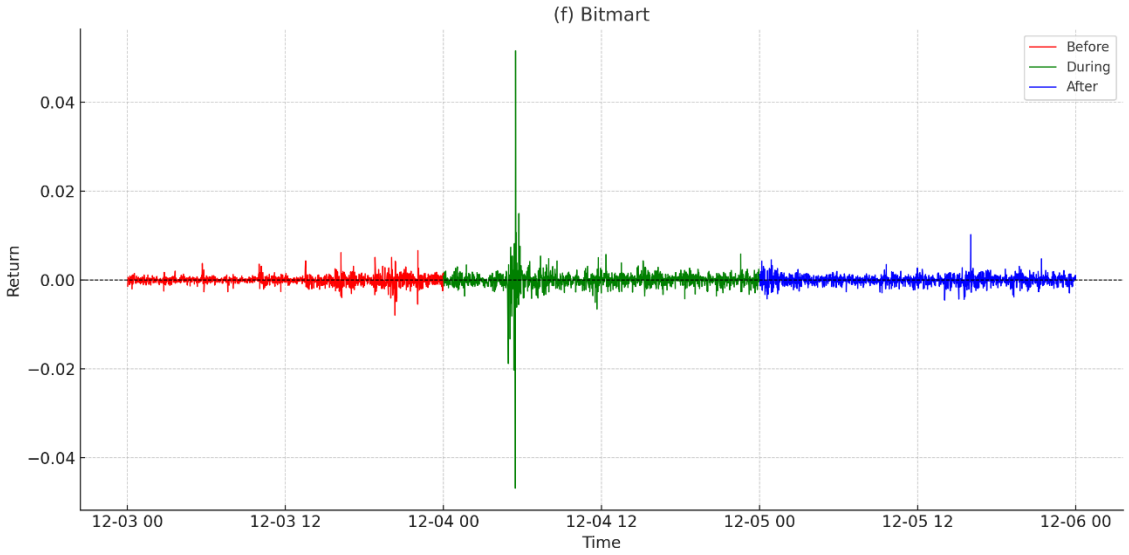
The descriptive statistics reveal abnormal distributional characteristics of Bitcoin prices around cryptocurrency heists, but do not capture the dynamic process of price changes. To address this limitation, Figure 2.1 presents Bitcoin returns before, during, and after each cryptocurrency heist, providing a direct view of the market's price response to these incidents. The results show that most cryptocurrency heists were accompanied by sharp fluctuations in Bitcoin returns, with the incident day typically marked by pronounced negative returns, indicating a broadly adverse market reaction to such extreme shocks. In contrast, the day before the incidents generally remained relatively stable, suggesting that cryptocurrency heists were largely unexpected rather than anticipated by the market. Post-event dynamics, however, reveal heterogeneous patterns: while major incidents such as Mt. Gox exchange, Coincheck exchange, and FTX exchange were followed by persistent negative effects and slower recovery, other incidents such as PancakeBunny platform or Ronin Network were quickly absorbed, with the market stabilising shortly afterwards. These findings highlight both the commonality of short-term panic-driven declines and the heterogeneity in impact severity.

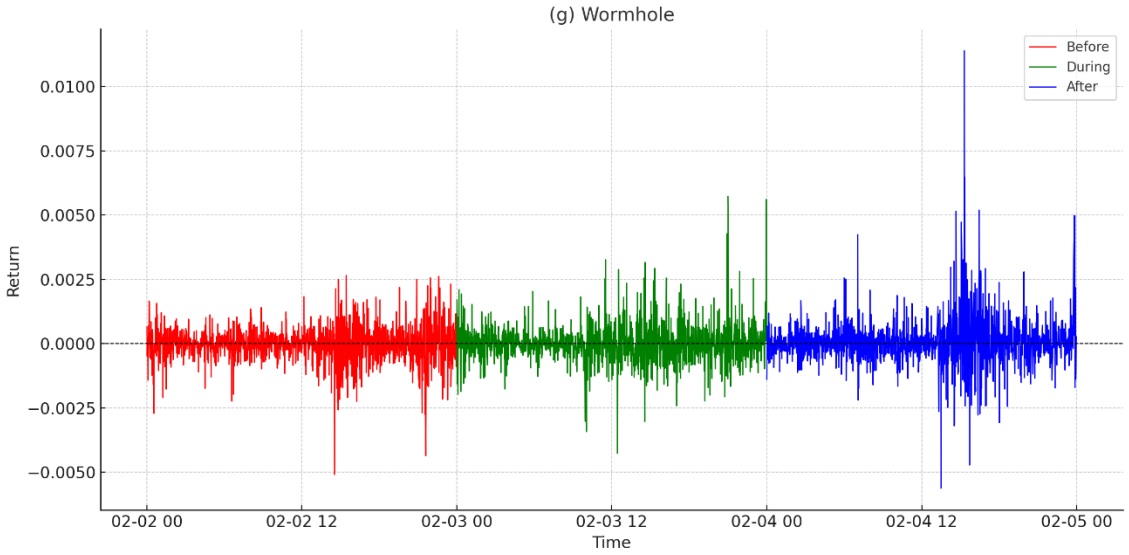
Figure 2.1: Bitcoin returns before, during, and after each cryptocurrency heist

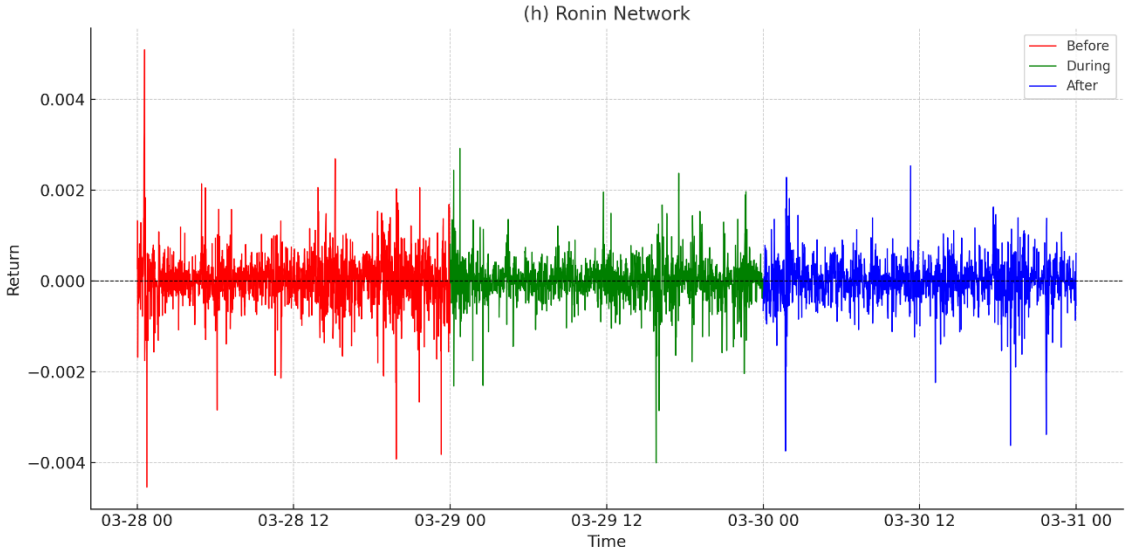


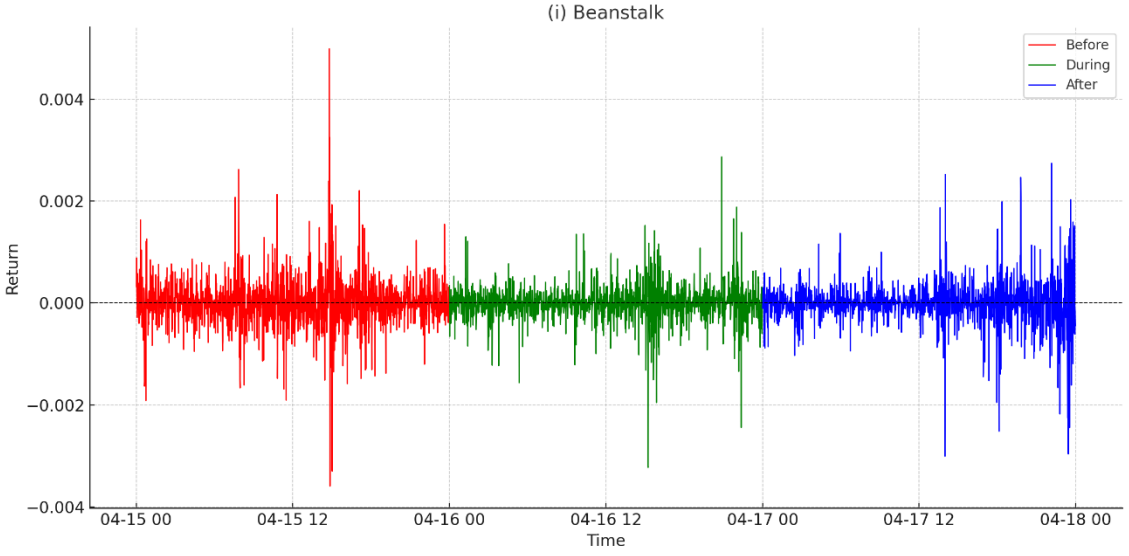

(d) PancakeBunny
Before
During
After
Return
0.03
0.02
0.01
0.00
−0.01
−0.02
05-19 00
05-19 12
05-20 00
05-20 12
05-21 00
05-21 12
05-22 00
Time

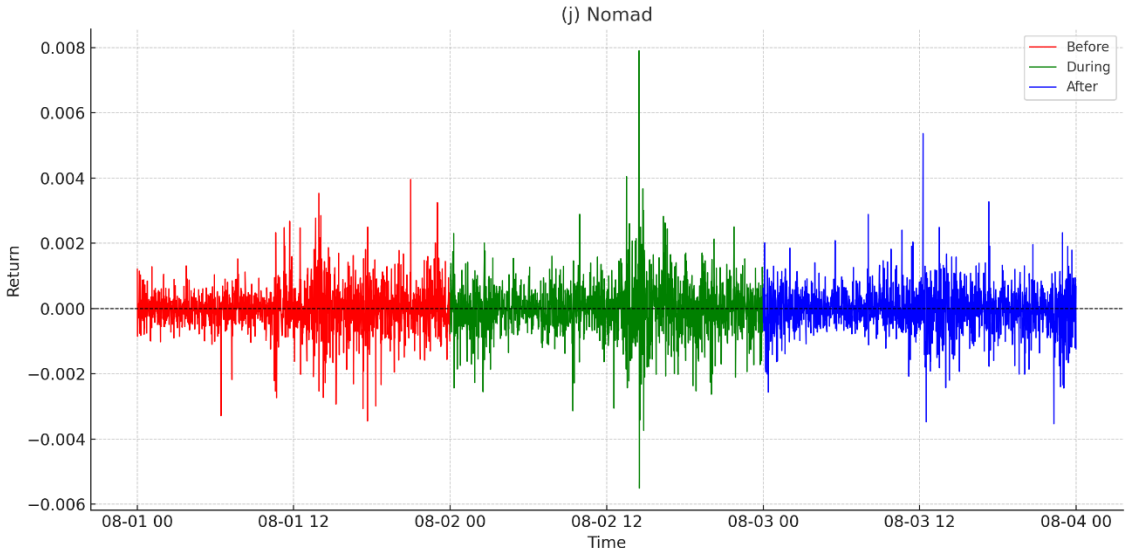

(e) Poly Network
Before
During
After
Return
0.015
0.010
0.005
0.000
−0.005
08-09 00
08-09 12
08-10 00
08-10 12
08-11 00
08-11 12
08-12 00
Time

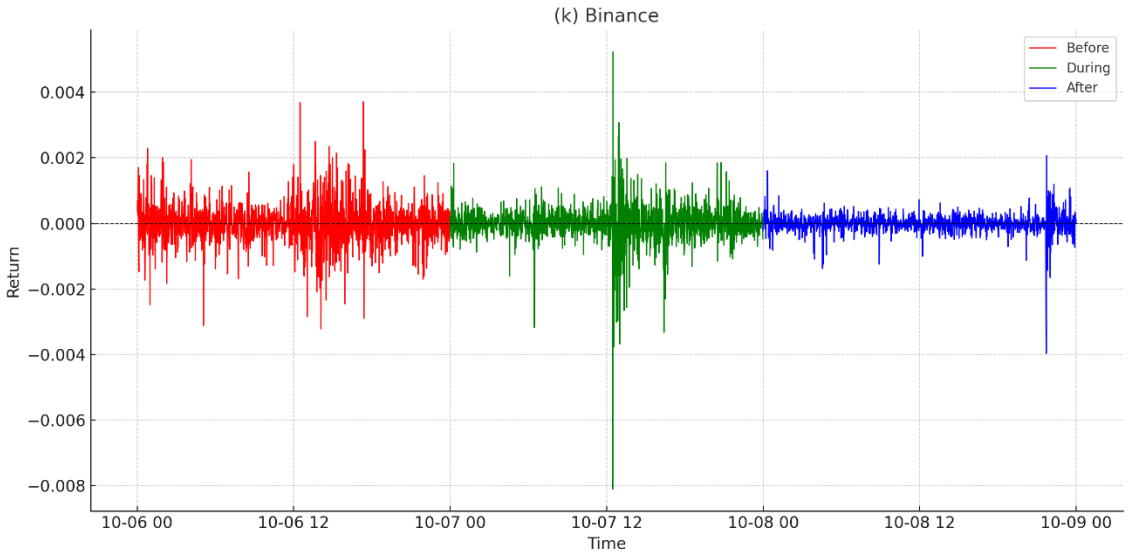

(f) Bitmart
Before
During
After
Return
0.04
0.02
0.00
−0.02
−0.04
12-03 00
12-03 12
12-04 00
12-04 12
12-05 00
12-05 12
12-06 00
Time

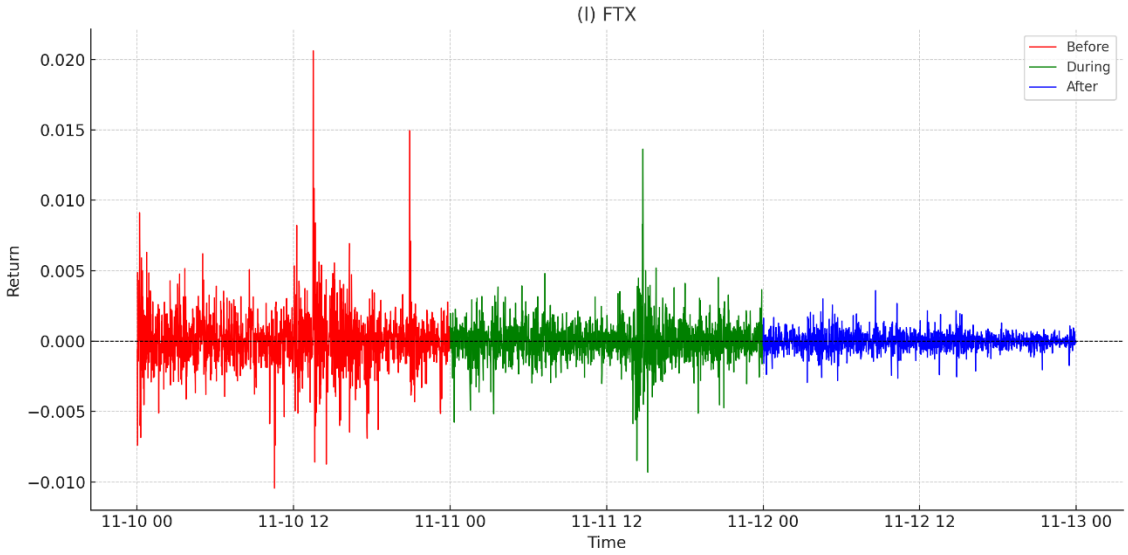

(g) Wormhole
Before
During
After
0.0100
0.0075
0.0050
0.0025
0.0000
−0.0025
−0.0050
Return
02-02 00
02-02 12
02-03 00
02-03 12
02-04 00
02-04 12
02-05 00
Time


(h) Ronin Network
Before
During
After
0.004
0.002
0.000
−0.002
−0.004
Return
03-28 00
03-28 12
03-29 00
03-29 12
03-30 00
03-30 12
03-31 00
Time


(i) Beanstalk
Before
During
After
0.004
0.002
0.000
−0.002
−0.004
Return
04-15 00
04-15 12
04-16 00
04-16 12
04-17 00
04-17 12
04-18 00
Time


(j) Nomad
Before
During
After
Return
0.008
0.006
0.004
0.002
0.000
−0.002
−0.004
−0.006
08-01 00
08-01 12
08-02 00
08-02 12
08-03 00
08-03 12
08-04 00
Time


(k) Binance
Before
During
After
Return
0.004
0.002
0.000
−0.002
−0.004
−0.006
−0.008
10-06 00
10-06 12
10-07 00
10-07 12
10-08 00
10-08 12
10-09 00
Time


(l) FTX
Before
During
After
Return
0.020
0.015
0.010
0.005
0.000
−0.005
−0.010
11-10 00
11-10 12
11-11 00
11-11 12
11-12 00
11-12 12
11-13 00
Time

While the return figures illustrate the pronounced volatility in Bitcoin prices during cryptocurrency heists, such graphical analysis only captures the magnitude of price fluctuations and does not address the core question of how market efficiency evolves. The essence of market efficiency lies in whether information is rapidly and fully incorporated into prices. Hence, it is essential to apply methods that characterise the complexity and correlation structures of time series to systematically examine market efficiency and uncover the dynamic impact of cryptocurrency heists on Bitcoin's market efficiency.

2.3.2 Permutation Entropy Model

The permutation entropy model is well-suited for analysing the impact of cryptocurrency heists on Bitcoin's market efficiency. Its advantage is its high sensitivity to small changes within a time series (Zanin et al., 2012). Cryptocurrency market often exhibits rapid price fluctuations and behavioural changes when subjected to external shocks, such as cryptocurrency heists (Corbet et al., 2019b; Bhatnagar et al., 2023). Permutation entropy can capture these short-term fluctuations and disorders, reflecting the immediate market efficiency changes. If the Bitcoin market quickly absorbs the information and stabilises after a cryptocurrency heist, permutation entropy should be high, indicating that the market remains efficient. Conversely, if permutation entropy remains low for an extended period, indicating that market price changes are highly predictable, it suggests that market efficiency has been negatively impacted. Therefore, the permutation entropy model directly quantifies the changes in market efficiency before and after such events.

Furthermore, the permutation entropy model does not rely on any specific probability distribution of the time series (Darbellay & Wuertz, 2000). The cryptocurrency market often exhibits complex and nonlinear behaviours, where price movements may not follow standard statistical distributions. The permutation entropy model provides the flexibility to measure market disorder and efficiency changes without assuming any particular distribution.

Finally, since this chapter uses Bitcoin's 1-minute price data as the variable, and the permutation entropy model is more effective at distinguishing time series when using prices rather than returns, it can be applied to non-stationary processes without the need to assess time series stationarity (Stosic et al., 2019). This means that when analysing the cryptocurrency market, there is no need for stationarity preprocessing (e.g. differencing or detrending), and we can directly apply permutation entropy to evaluate market disorder. This is particularly important for the rapidly changing cryptocurrency market, as it allows us to

capture the true dynamics of the market without being constrained by data preprocessing steps.

Following Bandt and Pompe (2002), the permutation entropy under the embedding dimension n ($n \geq 2$) is as follows:

$$H(n) = -\sum p(\pi) log p(\pi) \tag{1}$$

where $H(n)$ is the permutation entropy under the embedding dimension n, the factorial of n should be less than the number of samples. The value of the embedded dimension n does not affect the trend of the permutation entropy. $p(\pi)$ represents the probability of occurrence of each permutation. As usual, the log is base 2.

Bandt and Pompe (2002) gave an example to explain how the model works. There is a 1-dimensional time series dataset $S(t)$:

$$S(t) = \{4, 7, 9, 10, 6, 11, 3\} \tag{2}$$

Because the factorial of n should be less than the data point (there are 7 data points in the dataset $S(t)$), n can be 2 or 3. Using $n = 3$, $S(t)$ will be divided into overlapping column vector matrix as follows:

$$\begin{bmatrix} 4 & 7 & 9 & 10 & 6 \\ 7 & 9 & 10 & 6 & 11 \\ 9 & 10 & 6 & 11 & 3 \end{bmatrix} \tag{3}$$

To show the ordinal rankings of the data, an n-dimensional vector can be mapped into unique permutations π:

$$\pi = \{0, 1, 2, \cdots \mathrm{n} - 1\} \tag{4}$$

There are a total of six different possible permutations π of a 3-dimensional vector: $\pi_1 = \{0, 1, 2\}$, $\pi_2 = \{0, 2, 1\}$, $\pi_3 = \{1, 0, 2\}$, $\pi_4 = \{1\ 2, 0\}$, $\pi_5 = \{2, 1, 0\}$, and $\pi_6 = \{2, 0, 1\}$. For the column vector $\begin{bmatrix} 4 \\ 7 \\ 9 \end{bmatrix}$, we have $x_0 = 4, x_1 = 7, \text{and } x_2 = 9$. Since $x_0 < x_1 < x_2$, this column can be represented by the permutation $\pi_1 = \{0, 1, 2\}$. For the column vector $\begin{bmatrix} 9 \\ 10 \\ 6 \end{bmatrix}$, with $x_0 = 9, x_1 = 10, \text{and } x_2 = 6$, the order $x_2 < x_0 < x_1$ corresponds to the permutation $\pi_6 = \{2, 0, 1\}$. Thus, the matrix (3) can be represented as follows:

$$\begin{bmatrix} 0 & 0 & 2 & 1 & 2 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 2 & 1 & 2 & 1 \end{bmatrix} \quad (5)$$

The probabilities of occurrence of each permutation π are as follows: $p(\pi_1) = 2/5$, $p(\pi_2) = 0$, $p(\pi_3) = 1/5$, $p(\pi_4) = 0$, $p(\pi_5) = 0$, and $p(\pi_6) = 2/5$. Therefore, the permutation entropy under the embedding dimension (n) 3 is:

$$H(3) = -\left(\frac{2}{5}\right)\log_2\left(\frac{2}{5}\right) - \left(\frac{1}{5}\right)\log_2\left(\frac{1}{5}\right) - \left(\frac{2}{5}\right)\log_2\left(\frac{2}{5}\right) \approx 1.522 \quad (6)$$

If the following number can be accurately predicted from the previous one, $p(\pi)$ will be 1, resulting in $H(n)$ being 0, indicating an inefficient market. Conversely, if there is no relationship between the numbers, permutation entropy will be higher. Hence, the greater the permutation entropy, the more efficient the market. This chapter normalises the permutation entropy model to confine its results within the 0 to 1 range. The normalised permutation entropy model can be written as:

$$H_s[n] = H[n]/logn! \quad (7)$$

where $H_s[n]$ represents the normalised permutation entropy under the embedding dimension n. If $H_s[n]$ equals 1, it signifies an efficient market. Conversely, if $H_s[n]$ equals 0, it indicates an inefficient market. $H_s[n]$ equals the permutation entropy $H[n]$ divided by the maximum value of permutation entropy $logn!$, and the log is base 2.

2.3.3 Complexity–Entropy Causality Plane

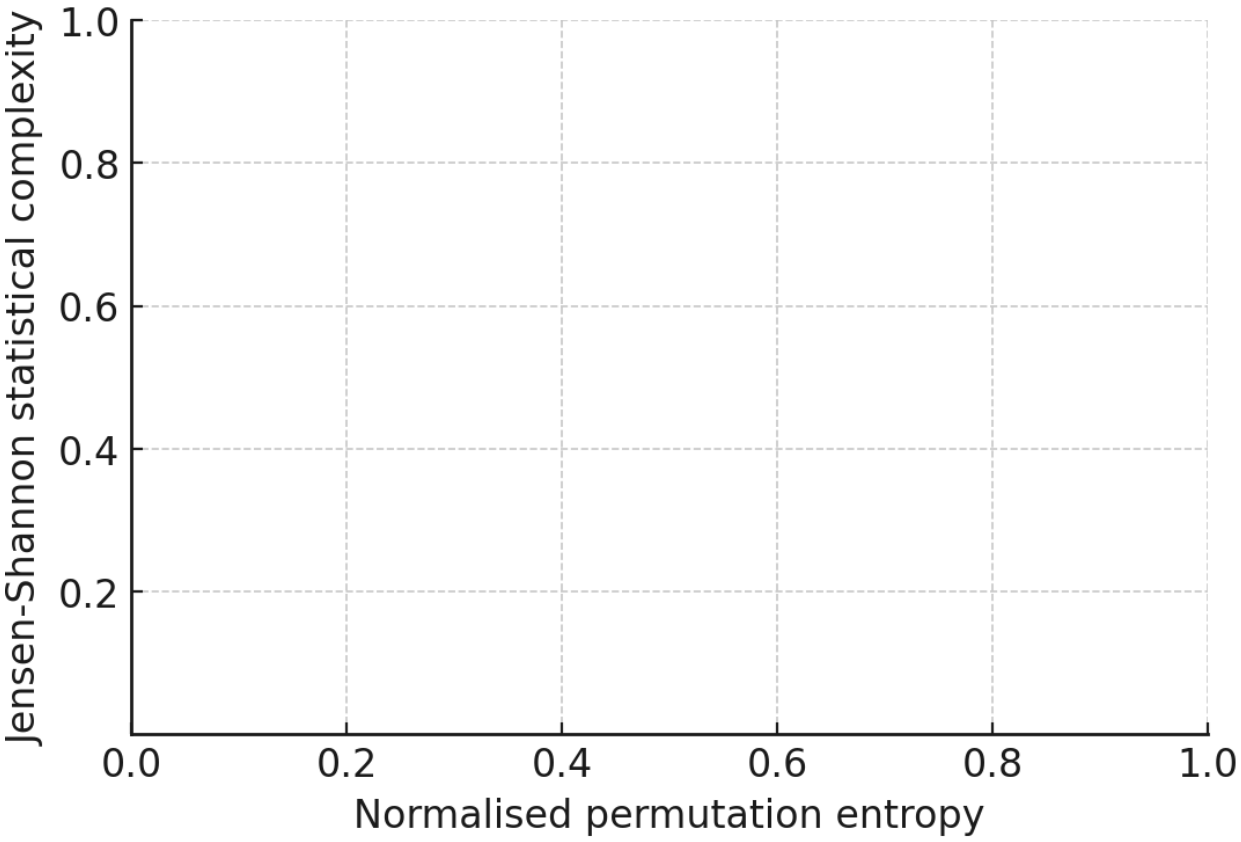
Although permutation entropy can assess the complexity of time series data, it does not account for its correlation structure. Additionally, the permutation entropy model cannot distinguish between varying degrees of periodicity and chaos or reveal information about probability distributions. The Complexity–entropy causality plane (Lamberti et al., 2004) addresses these issues with two parameters that reveal complementary information about a time series: (i) normalised permutation entropy measures a process's unpredictability, while (ii) Jensen–Shannon statistical complexity assesses the extent of privileged fluctuations for a given entropy level. Calculating these two quantities provides insights into the distribution of fluctuation patterns and the degree of correlation between these fluctuations (Zunino et al., 2010). The Jensen–Shannon statistical complexity $C_{JS}[n]$ can be shown as:

$$C_{JS}[n] = Q_j[n, n_e]H_s[n]$$
$$Q_j[n, n_e] = Q_0\left\{H\left[\frac{(n+n_e)}{2}\right] - \frac{H[n]}{2} - \frac{H[n_e]}{2}\right\} \quad (8)$$

where $Q_j[n, n_e]$ is a measure of disequilibrium and $Q_j[n, n_e] \in [0,1]$. Q_0 is a normalisation constant, which equals the inverse of the maximum possible value of $\{H[(n+n_e)/2] - H[n]/2 - H[n_e]/2\}$. $n_e = \{1/n!, \cdots, 1/n!\}$ is the uniform distribution. $C_{JS}[n]$ captures the fundamental dynamics and differentiates between varying degrees of periodicity and chaos. It offers valuable insights into the characteristics of the underlying probability distribution, with $C_{JS}[n]$ ranging from 0 to 1. Based on the range constraints of $H_s[n]$ and $C_{JS}[n]$, we can plot the Complexity–entropy causality plane (Figure 2.2).

Based on the work of Zunino et al. (2010), the Complexity–entropy causality plane provides a model-independent diagnostic tool that overcomes the limitations of traditional approaches. Jensen–Shannon statistical complexity is not a simple function of entropy; rather, it is derived from the divergence between the system's actual distribution and the uniform distribution, thereby capturing non-randomness and revealing the presence of "privileged states" or "ordered structures" within the series. In contrast, variance-based or GARCH-type models can capture changes in volatility and correlation structures but cannot reflect the degree of organisation in the underlying probability distribution. Therefore, Jensen–Shannon statistical complexity can distinguish randomness, correlations, and structural patterns within a unified framework, which information that conventional indicators such as GARCH or the Hurst exponent are unable to provide.

Figure 2.2: The Complexity–entropy causality plane



The market efficiency at a certain time can be plotted on this plane by the coordinates of normalised permutation entropy (X-axis) and Jensen-Shannon statistical complexity (Y-axis). The X-axis measures unpredictability in the market, while the Y-axis measures complexity. If the coordinates are closer to the lower right, it indicates higher entropy, lower complexity, and high market efficiency. Conversely, if the coordinates are closer to the upper left, it suggests lower entropy, higher complexity, and lower market efficiency.

According to the EMH, efficient markets should correspond to higher entropy and lower complexity (Zanin et al., 2012). When specific temporal patterns exist in a series, its position will deviate from the ideal point associated with a completely random process. Thus, the extent of deviation from this ideal point can be used to measure market inefficiency. The empirical findings of Zunino et al. (2010) demonstrated that the Complexity–entropy causality plane can robustly differentiate between developed and emerging markets. Developed markets cluster near the ideal random position (high entropy, low complexity), whereas emerging markets exhibit lower entropy and higher complexity, reflecting stronger long-range correlations and fat-tailed distributions. This suggests that the level of market development is closely aligned with its position on the plane, forming a downward trajectory from the upper left to the lower right. Such a trajectory not only reveals the evolutionary path from inefficient to efficient markets but also indicates that inefficiency primarily stems from correlations rather than distributional features alone.

Overall, the Complexity–entropy causality plane offers a visual representation of market conditions, enabling an intuitive assessment of the market's current state and its response to external shocks based on positioning points on the plane. Positions in the lower right denote an efficient market characterised by high entropy and low complexity, indicating high market efficiency. Conversely, positions in the upper left signify an inefficient market with low entropy and high complexity, suggesting the presence of predictable patterns and reduced efficiency. By observing how points on the plane shift over time, especially before and after cryptocurrency heists, we can visually track changes in market efficiency.

2.4 Empirical Results

2.4.1 Detection of Bitcoin's Market Efficiency

Since the calculation of permutation entropy and complexity does not require differencing or detrending, the raw 1-minute Bitcoin price data are used directly. The dataset is divided into consecutive non-overlapping hourly windows (e.g., 00:00–00:59, 01:00–01:59). For each window, all 1-minute observations within the hour are retained, and permutation entropy and complexity of that hour are calculated based on the resulting sequence. This approach allows us to capture the information dynamics at the hourly level.

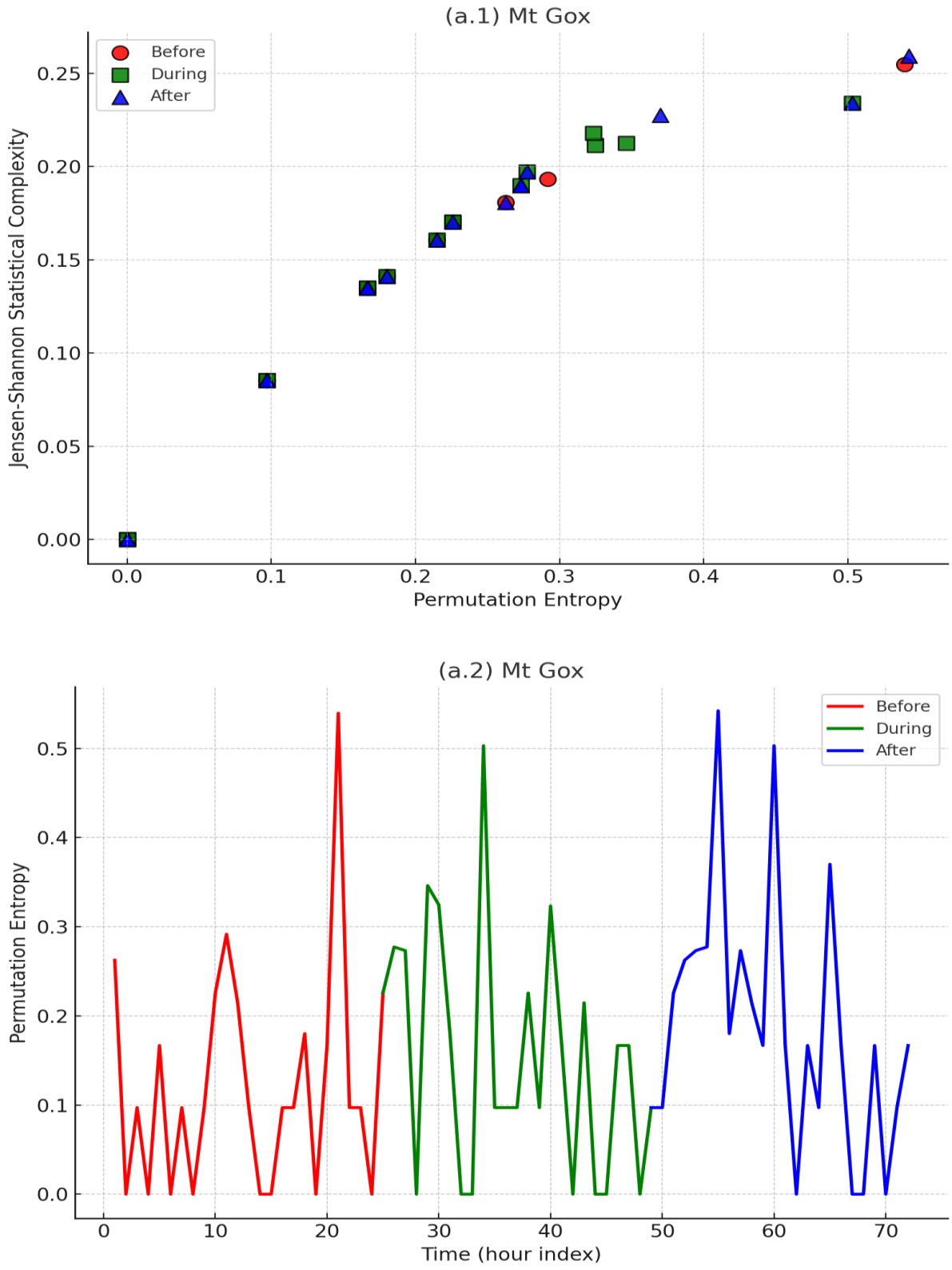
Figure 2.3 presents the Complexity–entropy causality plane (sub-figures a.1, b.1, c.1, …) and permutation entropy changes (sub-figures a.2, b.2, c.2, …) for twelve cryptocurrency heists. Permutation entropy is calculated with an embedding dimension of 3. In the Complexity–entropy causality plane, the red dots represent the hourly distribution of Bitcoin's market efficiency the day before the cryptocurrency heist, green squares represent the day of the cryptocurrency heist, and blue triangles represent the day after. Points closer to the upper left corner indicate lower market efficiency, while those near the lower right corner indicate higher efficiency. The permutation entropy figure illustrates the level of disorder in the Bitcoin market on the day before (red), the day of (green), and the day after the cryptocurrency heist (blue). A higher permutation entropy signifies greater disorder, while a lower value indicates less disorder. The results show that Bitcoin's market efficiency fluctuated before, during, and after these cryptocurrency heists, aligning with the AMH, which suggests market efficiency changes in response to external events.

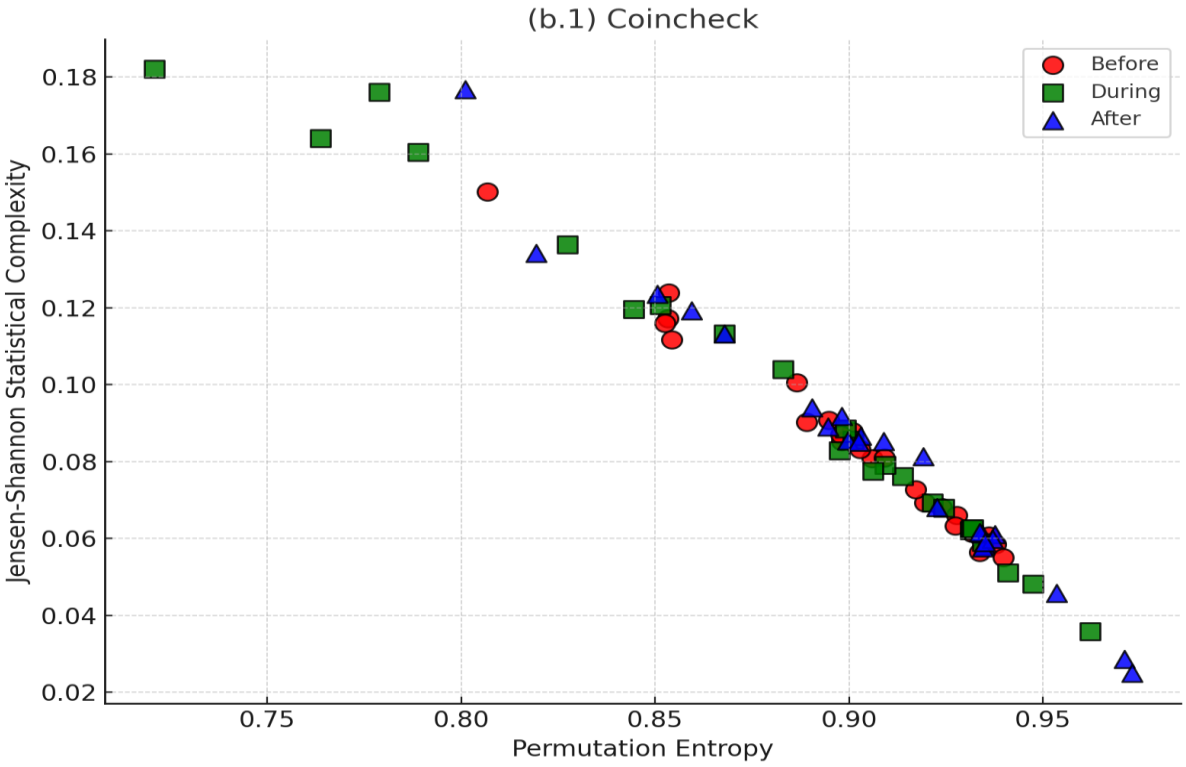
In most cases during and after cryptocurrency heists, the complexity–entropy points are located in the upper left corner, indicating high complexity and low permutation entropy,

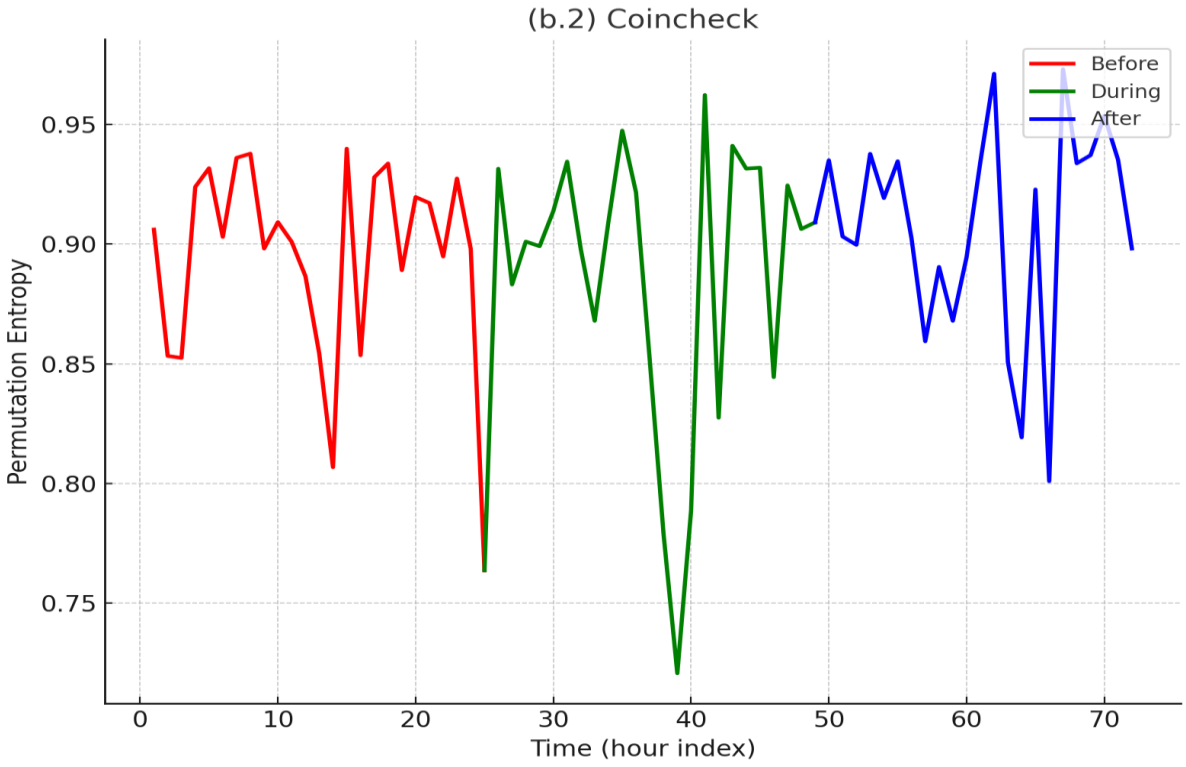
signalling low market efficiency. This supports AMH: investor sentiment and behavioural inadaptability could temporarily weaken price discovery and lower market efficiency during shocks like cryptocurrency heists. In the nine cryptocurrency heists, including Coincheck (Figure 2.3 b.2), KuCoin (Figure 2.3 c.2), Poly Network (Figure 2.3 e.2), Bitmart (Figure 2.3 f.2), Wormhole (Figure 2.3 g.2), Beanstalk (Figure 2.3 i.2), Nomad (Figure 2.3 j.2), Binance (Figure 2.3 k.2), and FTX (Figure 2.3 l.2), Bitcoin's permutation entropy dropped significantly during or after the cryptocurrency heists, showing a sharp decline in efficiency. In the six cryptocurrency heists (Coincheck, Poly Network, Bitmart, Wormhole, Nomad, and Binance), this drop was particularly evident during the cryptocurrency heists, reflecting the maladaptive behaviours of investors when faced with significant uncertainties and the asymmetry of market information.

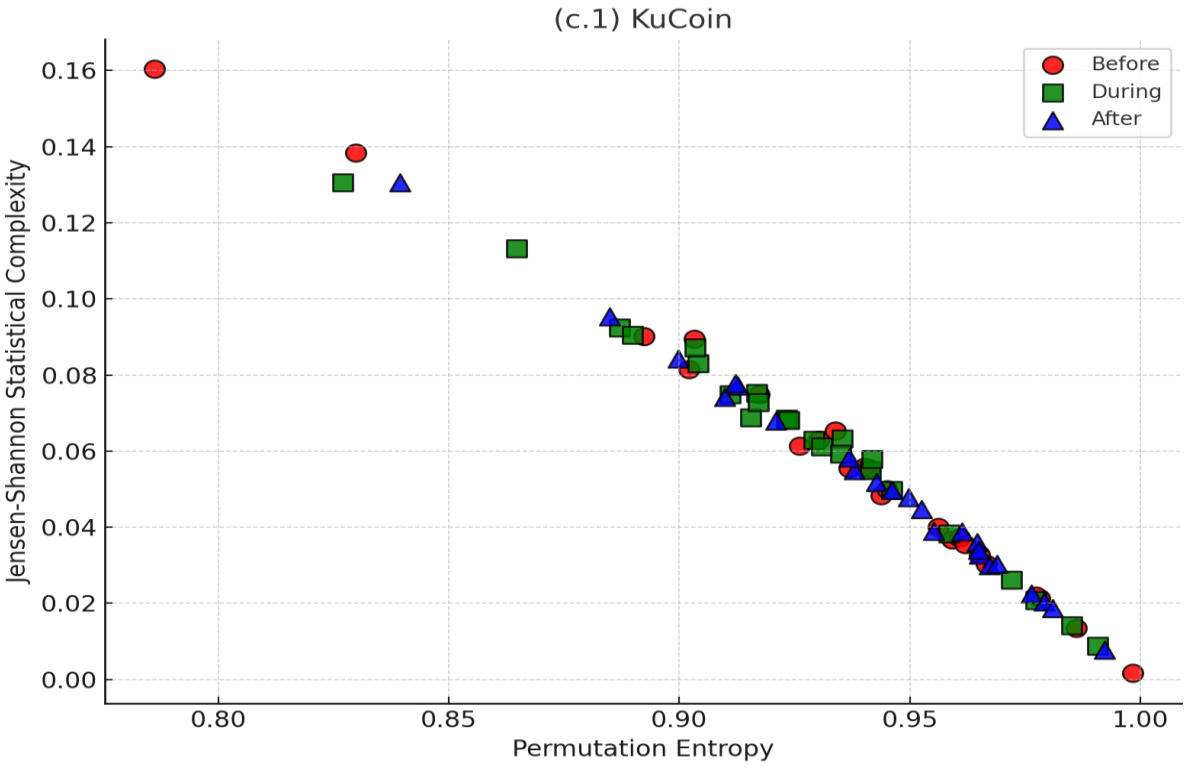
According to AMH, market efficiency fluctuates in response to shocks as investors fail to adapt to changing environments. When a cryptocurrency heist occurs, the sudden uncertainty and chaos make it difficult for investors to quickly process, understand, and analyse the new information related to the incident. This delay in information processing hinders investors from making rational decisions, often leading to emotional reactions like panic selling or buying, causing prices to deviate from their true price and further declining market efficiency. As the market gradually absorbs the information and investors adapt to the new environment, efficiency may recover. The findings highlight the dynamic nature of market adaptation and the significant impact that cryptocurrency heists have on investor behaviour and market mechanisms.

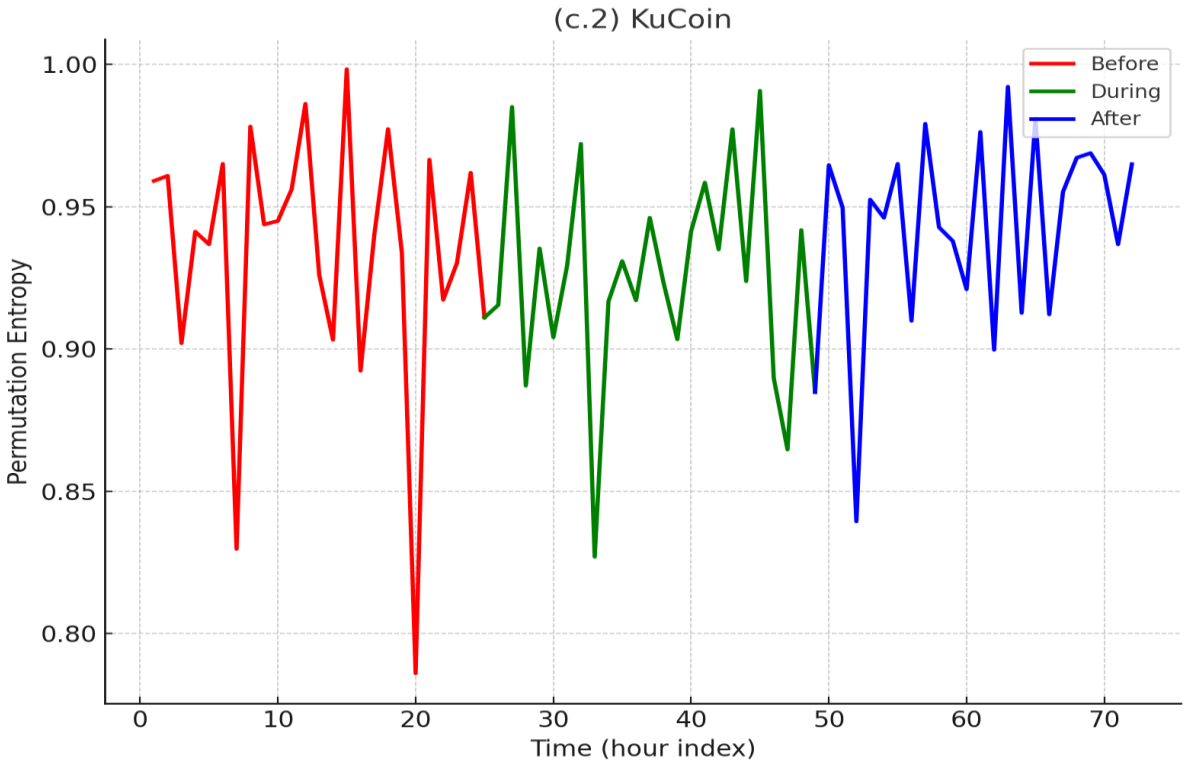
Figure 2.3: The Complexity–entropy causality plane and permutation entropy for the twelve cryptocurrency heists

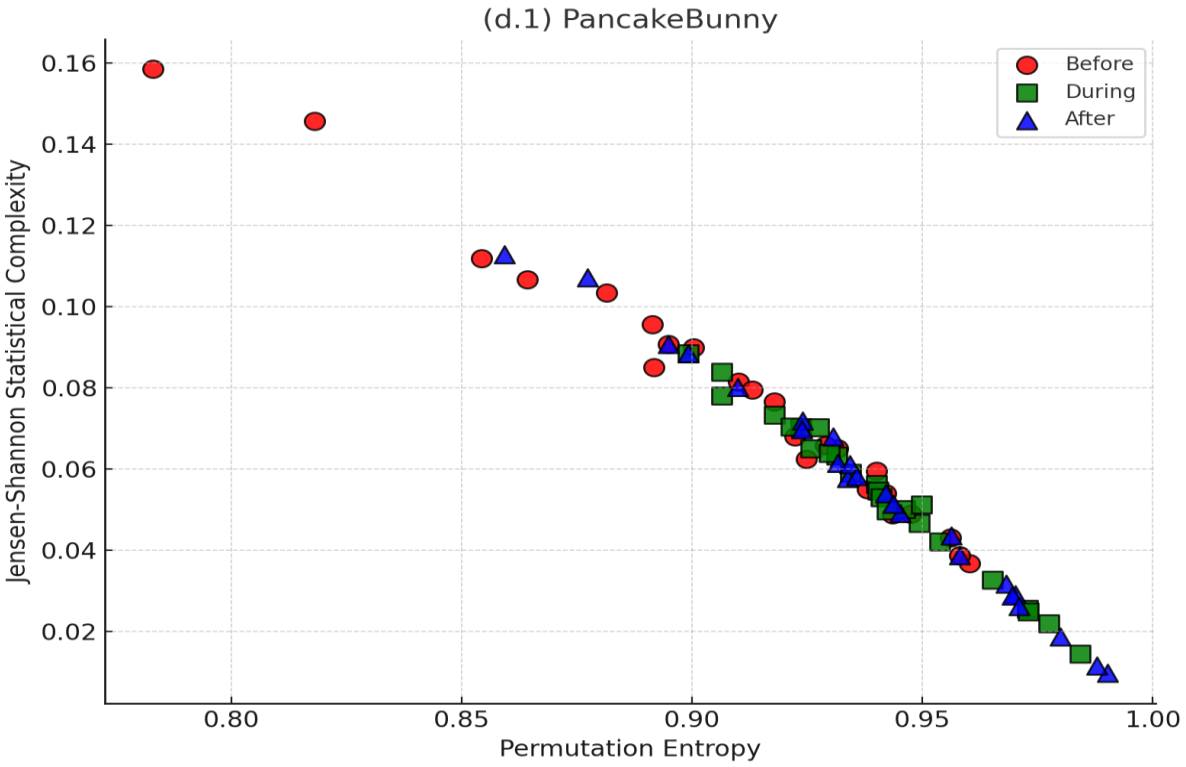


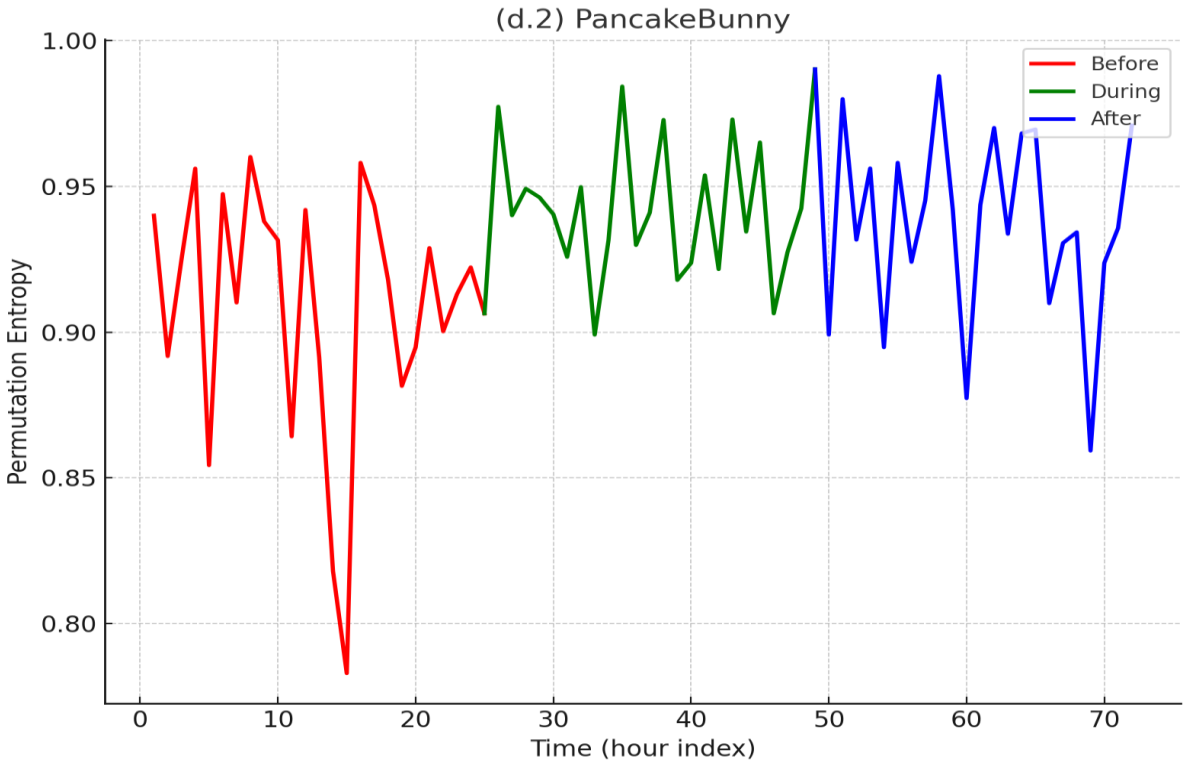

(b.1) Coincheck
Before
During
After
Jensen-Shannon Statistical Complexity
0.18
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.75
0.80
0.85
0.90
0.95
Permutation Entropy

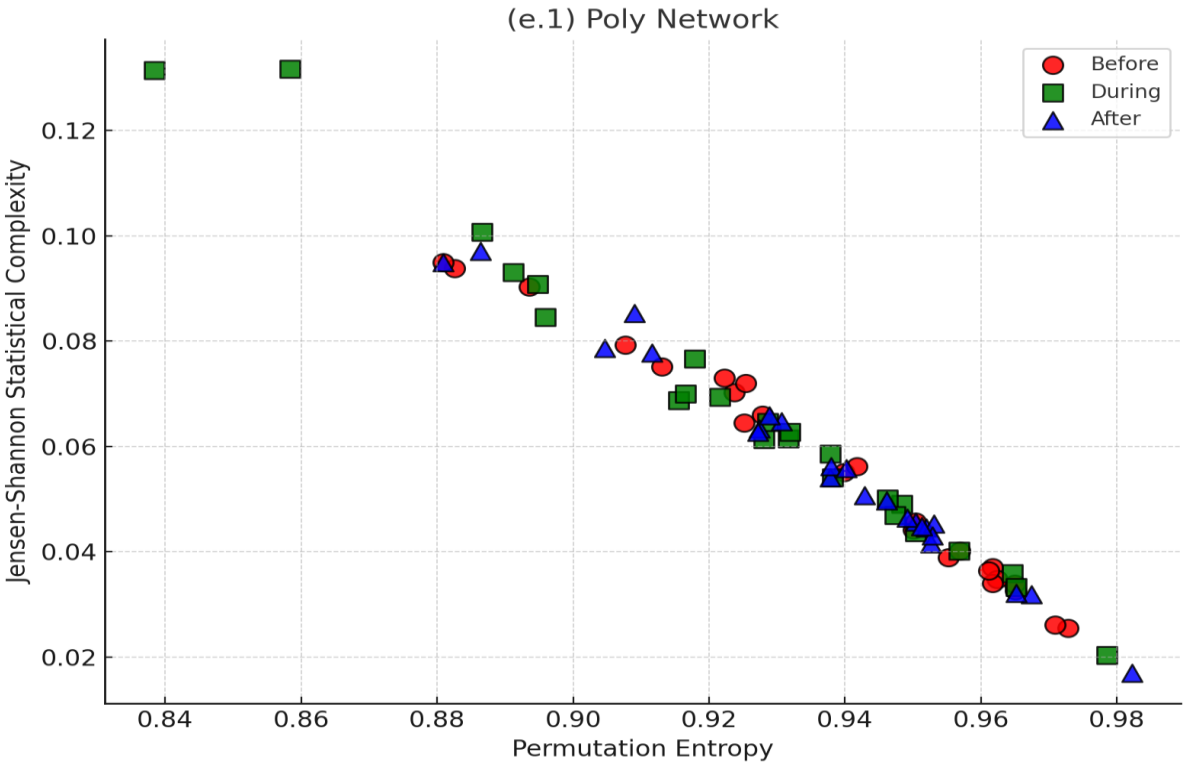

(b.2) Coincheck
Before
During
After
Permutation Entropy
0.95
0.90
0.85
0.80
0.75
0
10
20
30
40
50
60
70
Time (hour index)

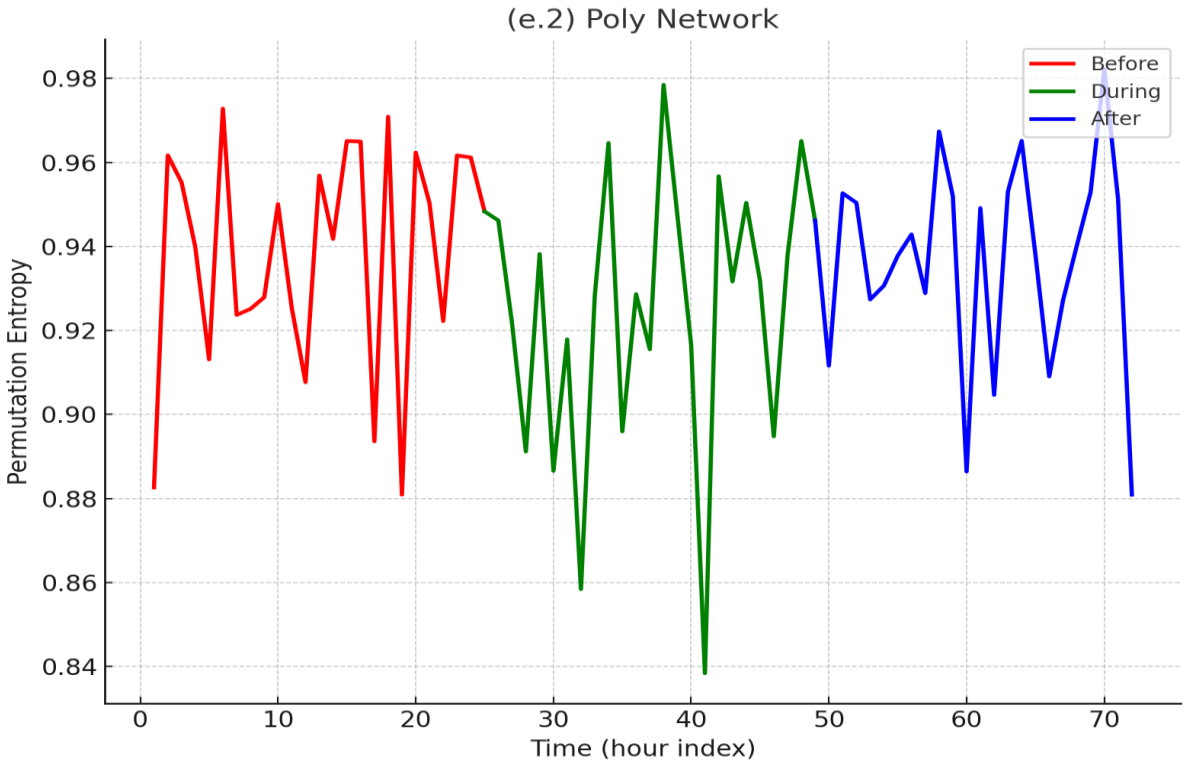

(c.1) KuCoin
Before
During
After
Jensen-Shannon Statistical Complexity
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.00
0.80
0.85
0.90
0.95
1.00
Permutation Entropy

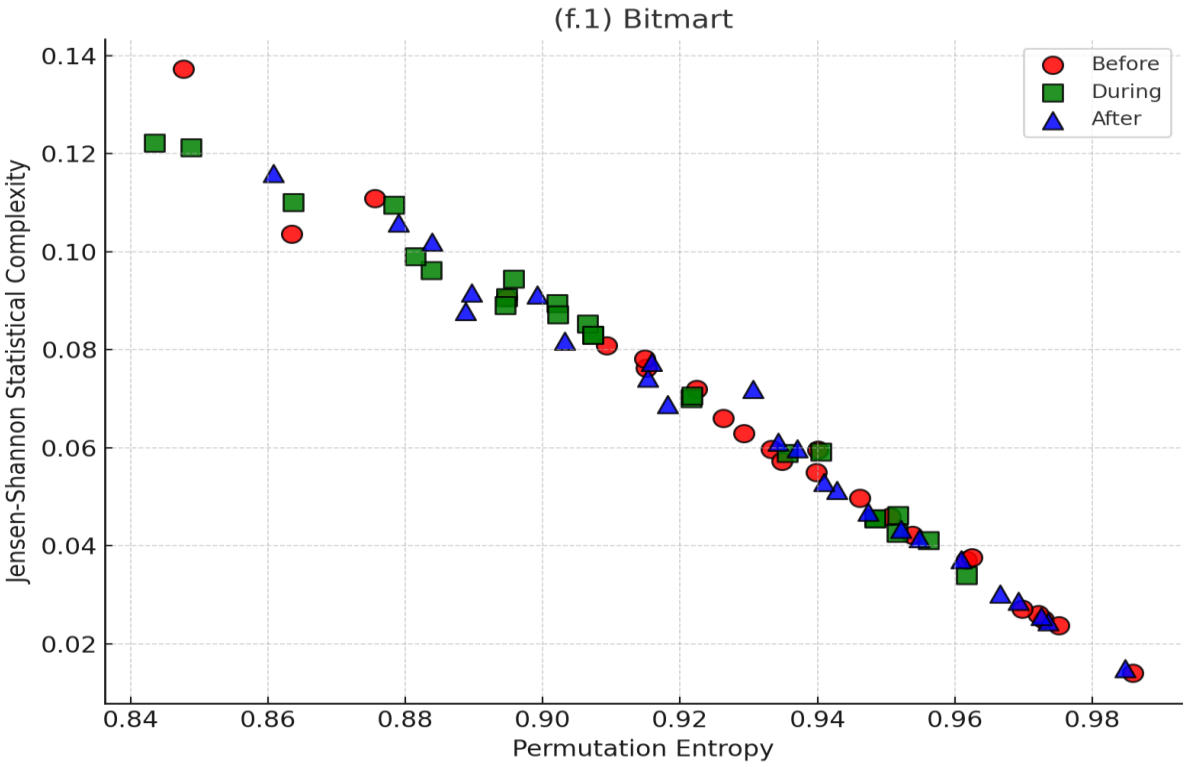

(c.2) KuCoin
Before
During
After
Permutation Entropy
1.00
0.95
0.90
0.85
0.80
0
10
20
30
40
50
60
70
Time (hour index)

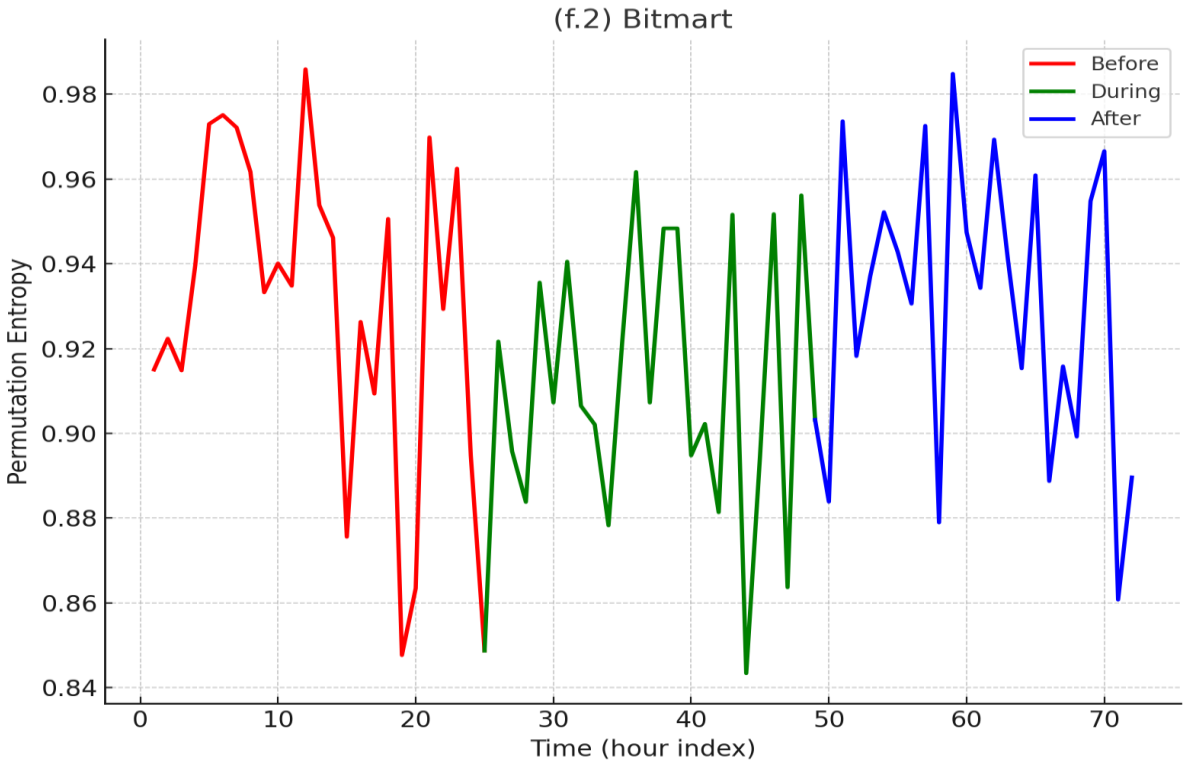

(d.1) PancakeBunny
Before
During
After
Jensen-Shannon Statistical Complexity
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.80
0.85
0.90
0.95
1.00
Permutation Entropy

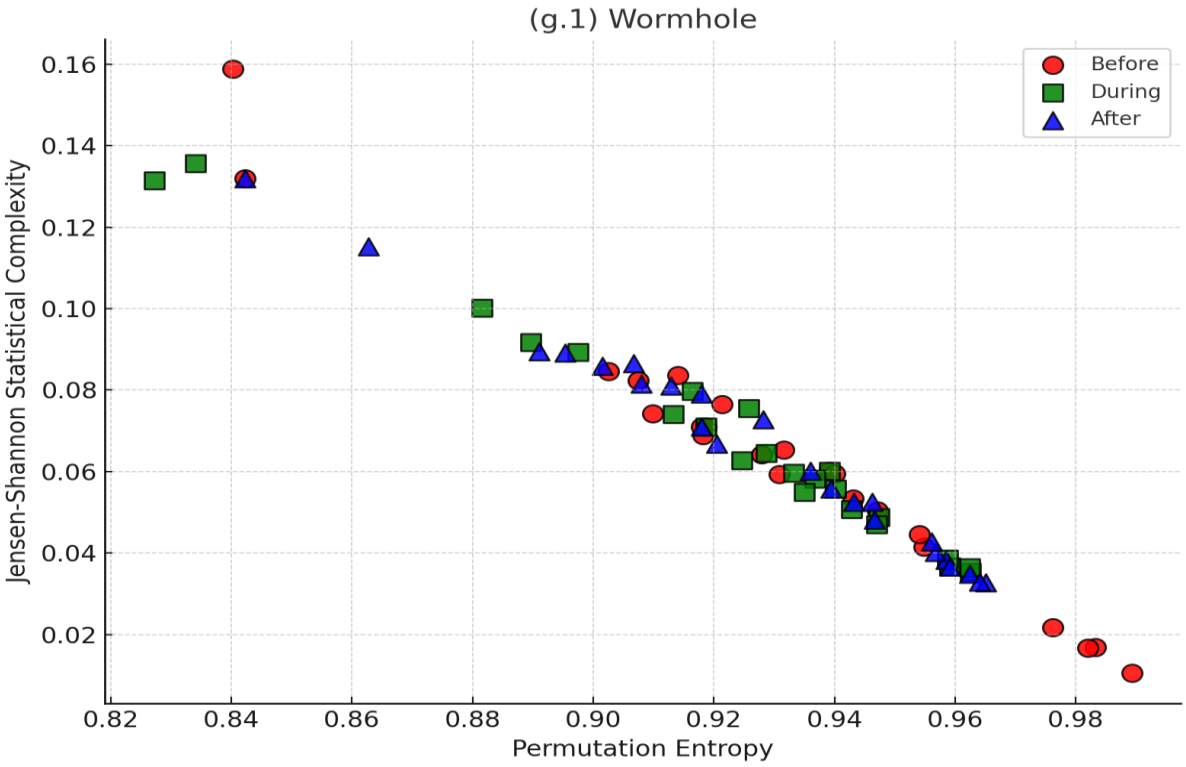

(d.2) PancakeBunny
Before
During
After
Permutation Entropy
1.00
0.95
0.90
0.85
0.80
0
10
20
30
40
50
60
70
Time (hour index)

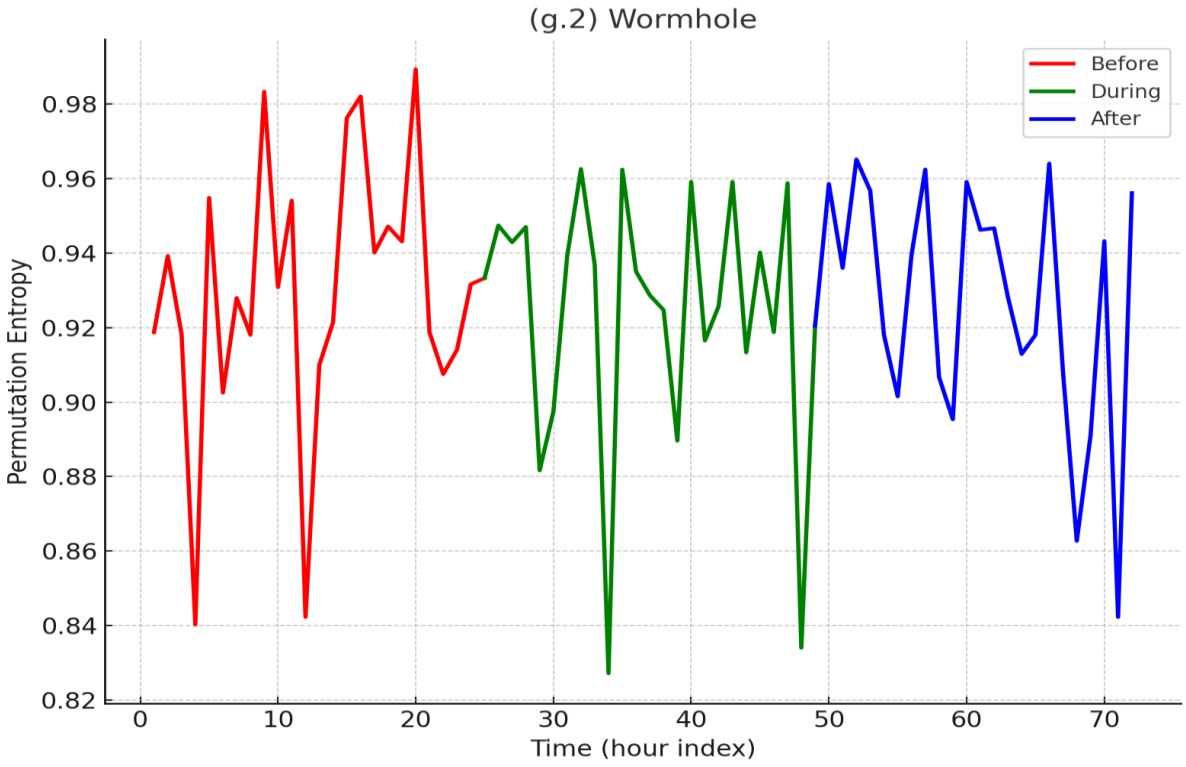

(e.1) Poly Network
Before
During
After
Jensen-Shannon Statistical Complexity
0.12
0.10
0.08
0.06
0.04
0.02
0.84
0.86
0.88
0.90
0.92
0.94
0.96
0.98
Permutation Entropy

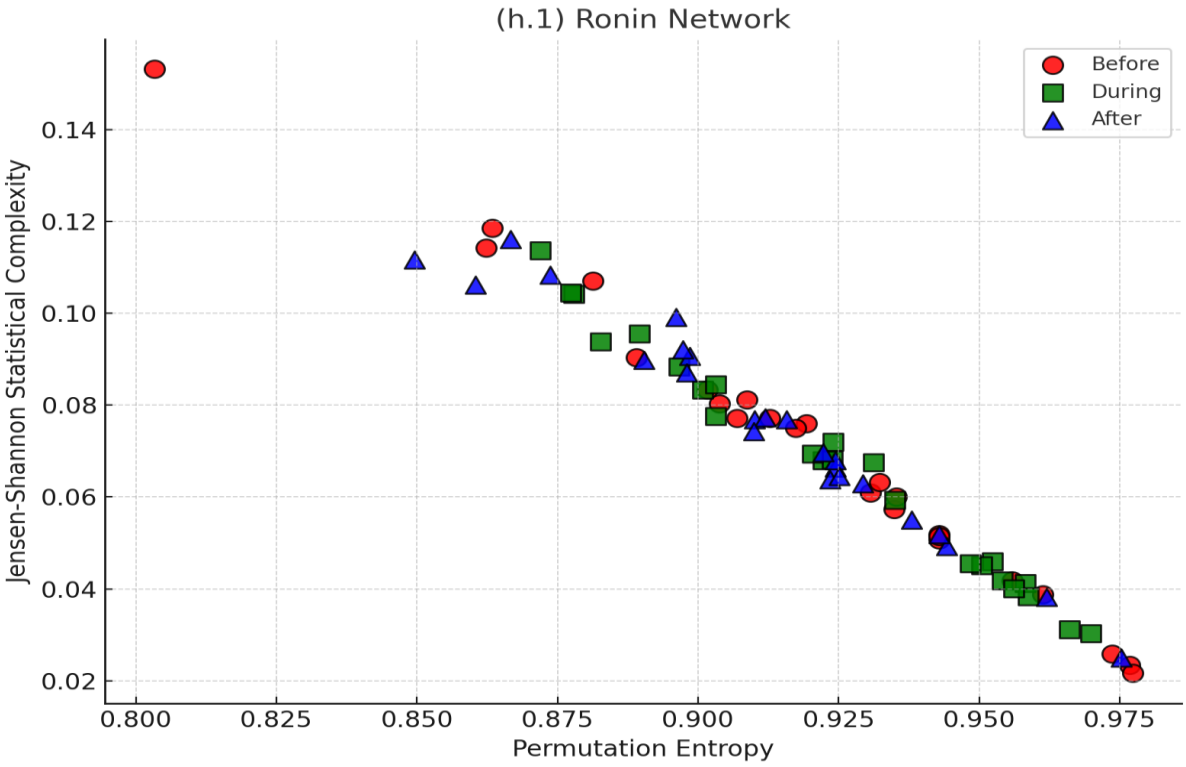

(e.2) Poly Network
Before
During
After
Permutation Entropy
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.84
0
10
20
30
40
50
60
70
Time (hour index)

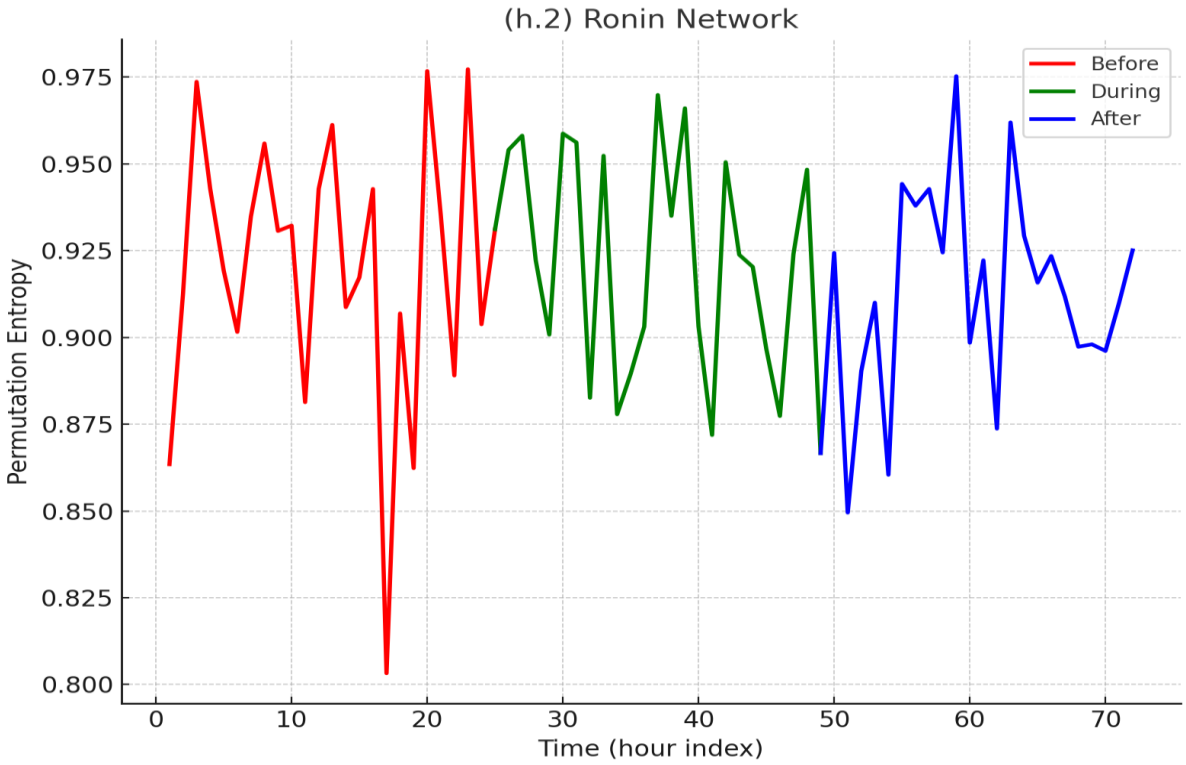

(f.1) Bitmart
Before
During
After
Jensen-Shannon Statistical Complexity
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.84
0.86
0.88
0.90
0.92
0.94
0.96
0.98
Permutation Entropy

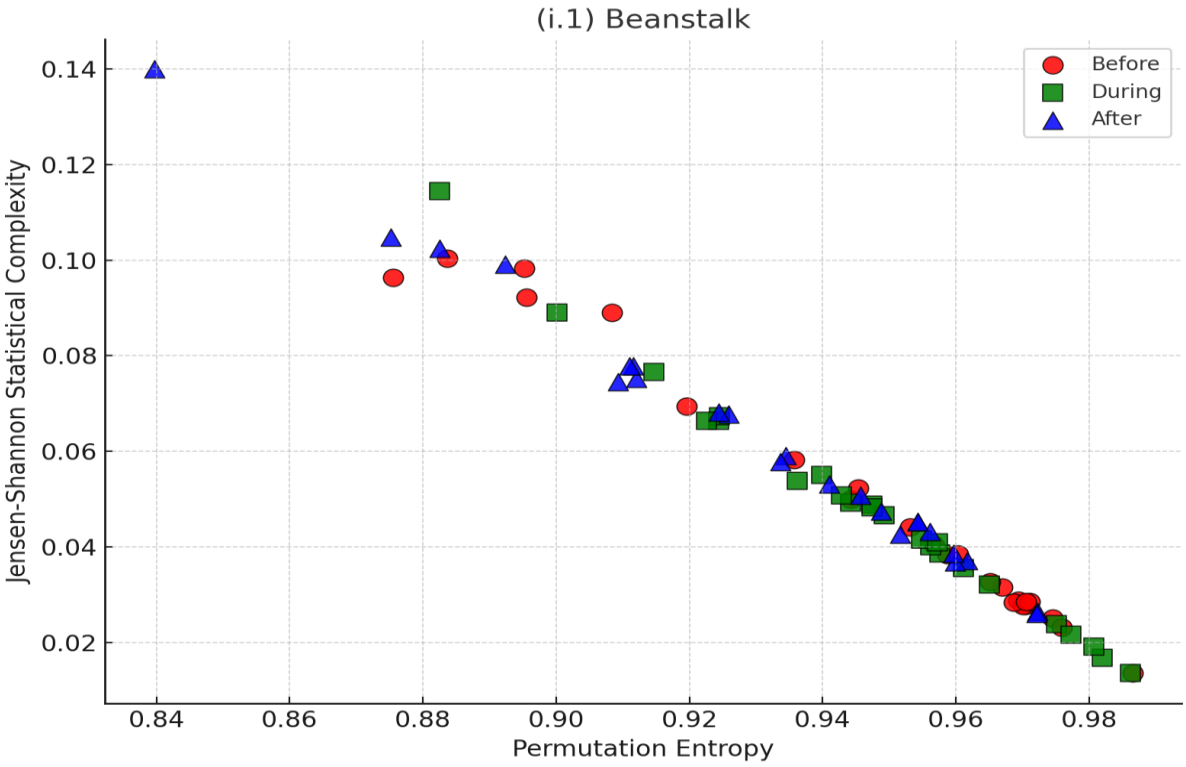

(f.2) Bitmart
Before
During
After
Permutation Entropy
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.84
0
10
20
30
40
50
60
70
Time (hour index)

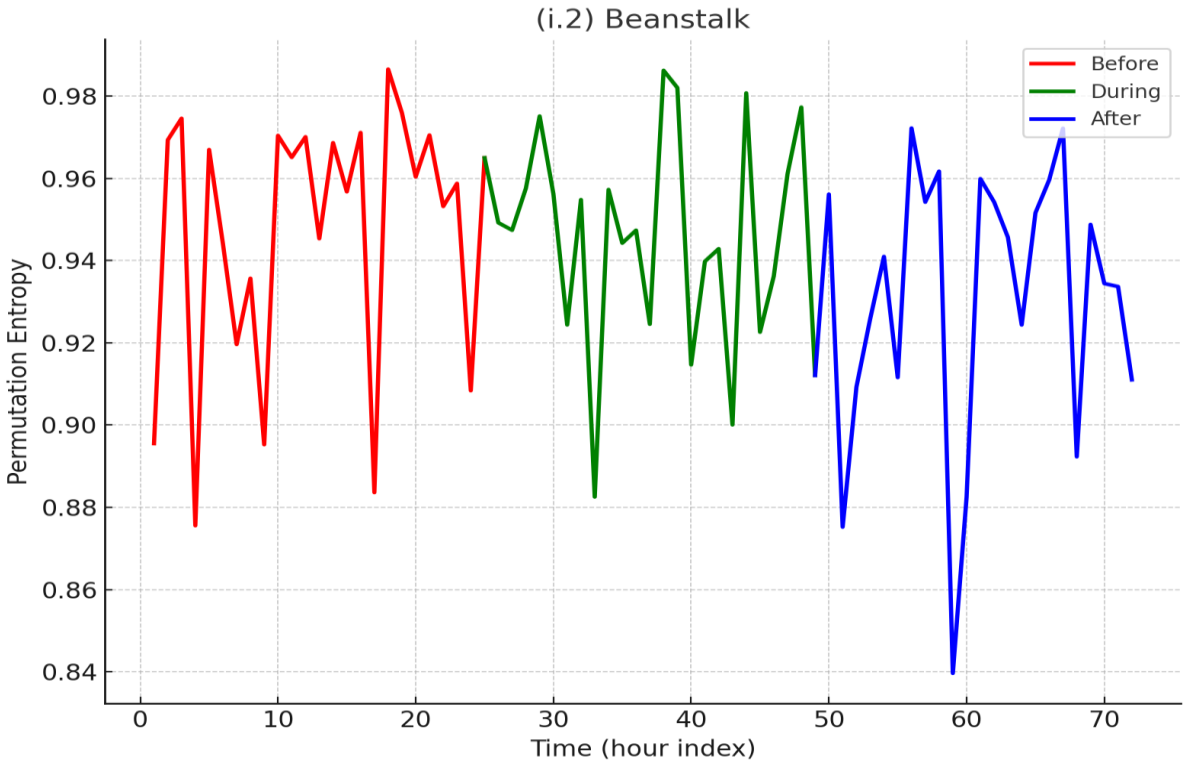

(g.1) Wormhole
Before
During
After
Jensen-Shannon Statistical Complexity
0.16
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.82
0.84
0.86
0.88
0.90
0.92
0.94
0.96
0.98
Permutation Entropy

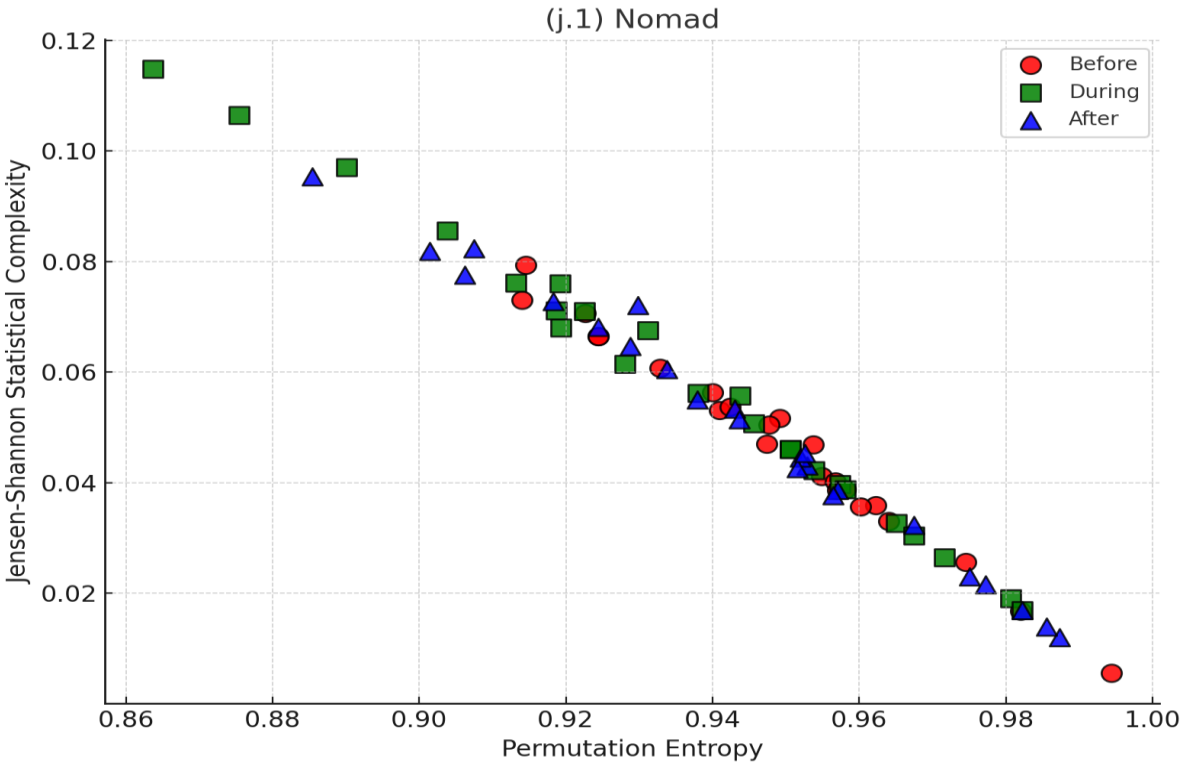

(g.2) Wormhole
Before
During
After
Permutation Entropy
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.84
0.82
0
10
20
30
40
50
60
70
Time (hour index)

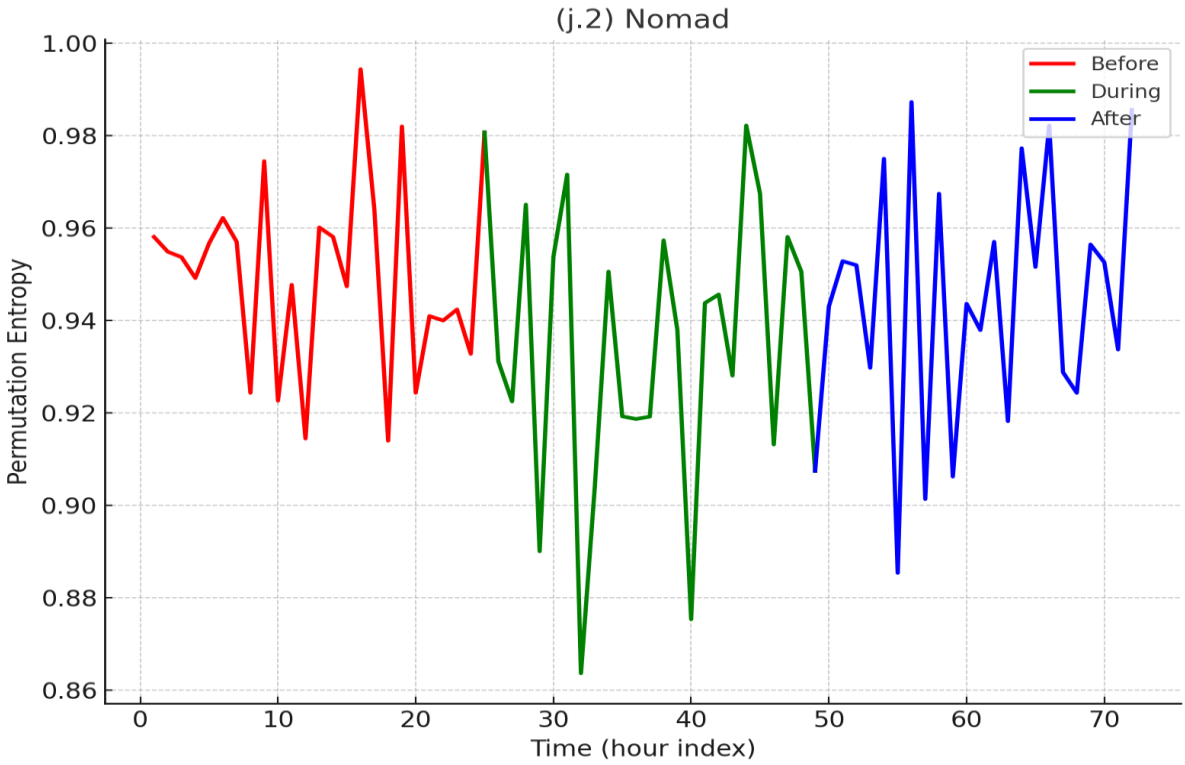

(h.1) Ronin Network
Before
During
After
Jensen-Shannon Statistical Complexity
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.800
0.825
0.850
0.875
0.900
0.925
0.950
0.975
Permutation Entropy

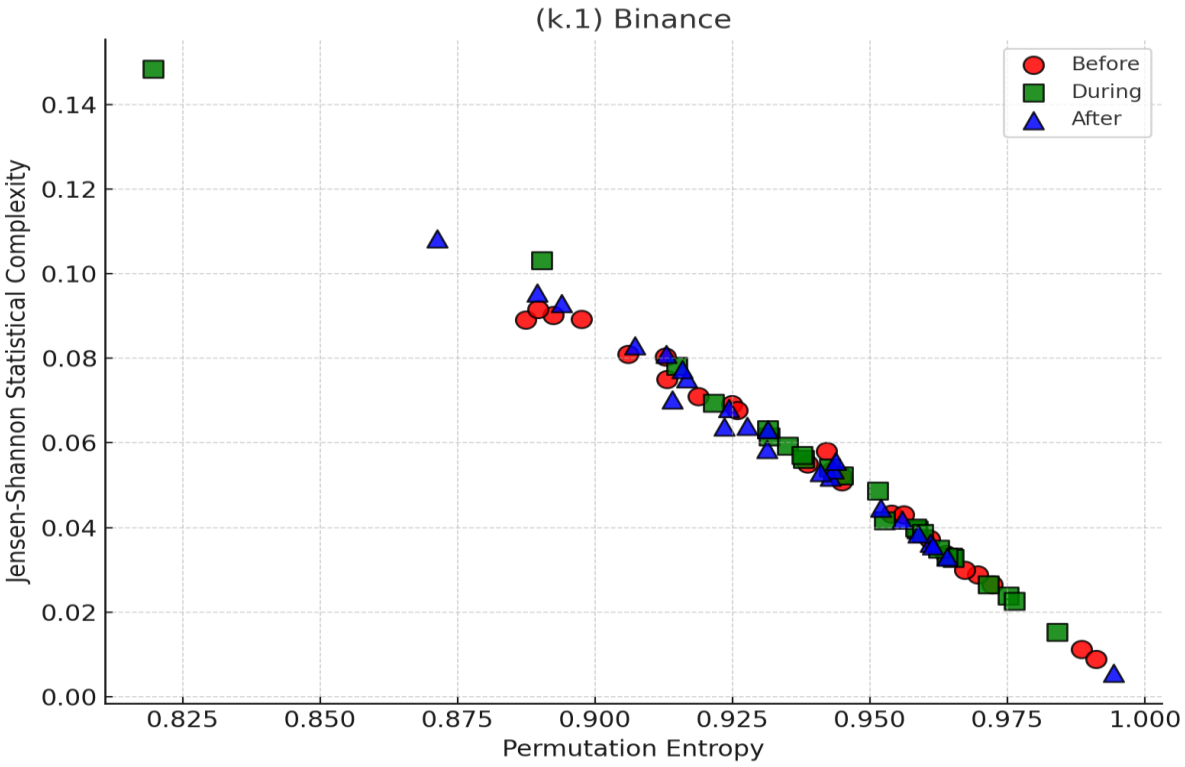

(h.2) Ronin Network
Before
During
After
Permutation Entropy
0.975
0.950
0.925
0.900
0.875
0.850
0.825
0.800
0
10
20
30
40
50
60
70
Time (hour index)

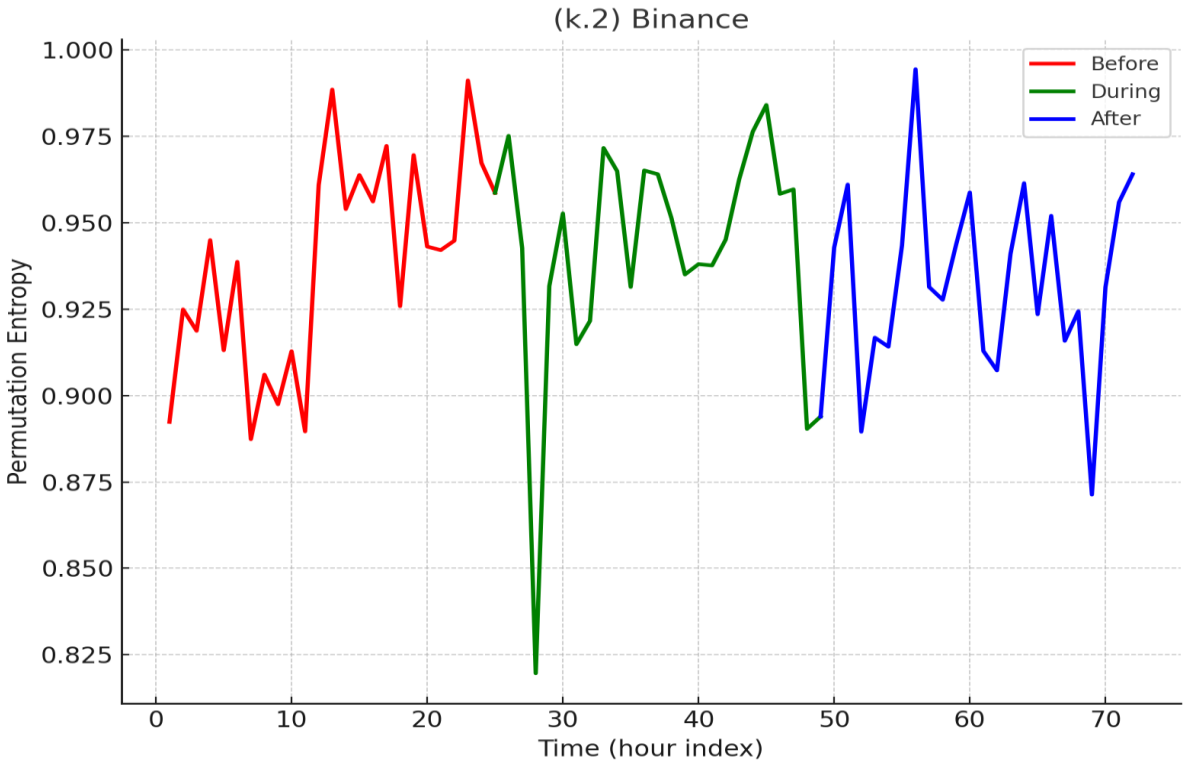

(i.1) Beanstalk
Before
During
After
Jensen-Shannon Statistical Complexity
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.84
0.86
0.88
0.90
0.92
0.94
0.96
0.98
Permutation Entropy

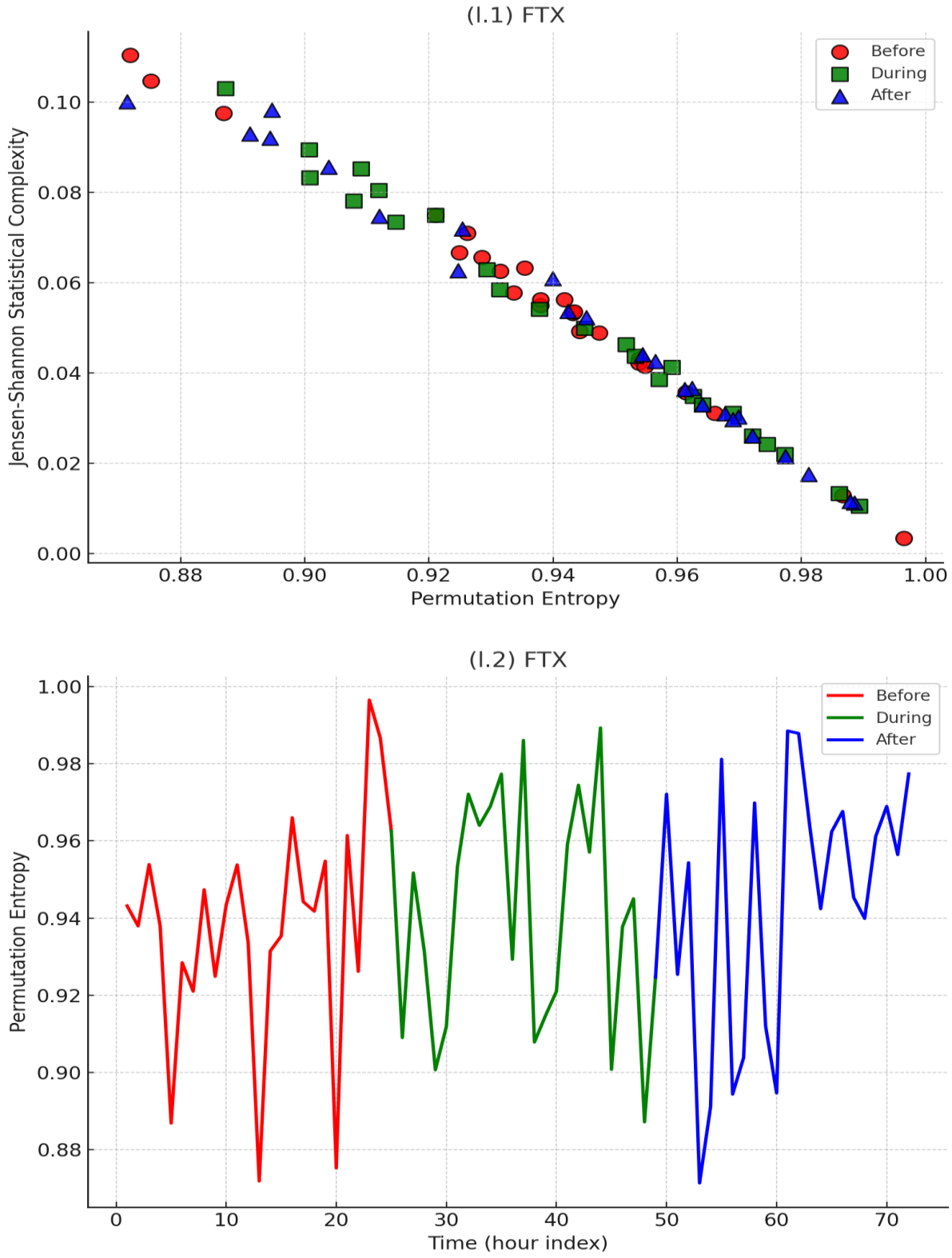

(i.2) Beanstalk
Before
During
After
Permutation Entropy
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.84
0
10
20
30
40
50
60
70
Time (hour index)


(j.1) Nomad
Before
During
After
Jensen-Shannon Statistical Complexity
Permutation Entropy
0.12
0.10
0.08
0.06
0.04
0.02
0.86
0.88
0.90
0.92
0.94
0.96
0.98
1.00


(j.2) Nomad
Before
During
After
Permutation Entropy
Time (hour index)
1.00
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0
10
20
30
40
50
60
70


(k.1) Binance
Before
During
After
Jensen-Shannon Statistical Complexity
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.00
0.825
0.850
0.875
0.900
0.925
0.950
0.975
1.000
Permutation Entropy


(k.2) Binance
Before
During
After
Permutation Entropy
1.000
0.975
0.950
0.925
0.900
0.875
0.850
0.825
0
10
20
30
40
50
60
70
Time (hour index)



In sub-figures a.1, b.1, c.1, …, coordinates located closer to the lower right corner indicate higher entropy, lower complexity, and thus higher market efficiency, whereas those positioned closer to the upper left corner reflect lower entropy, higher complexity, and lower market efficiency. In sub-figures a.2, b.2, c.2, …, higher permutation entropy corresponds to higher levels of market efficiency.

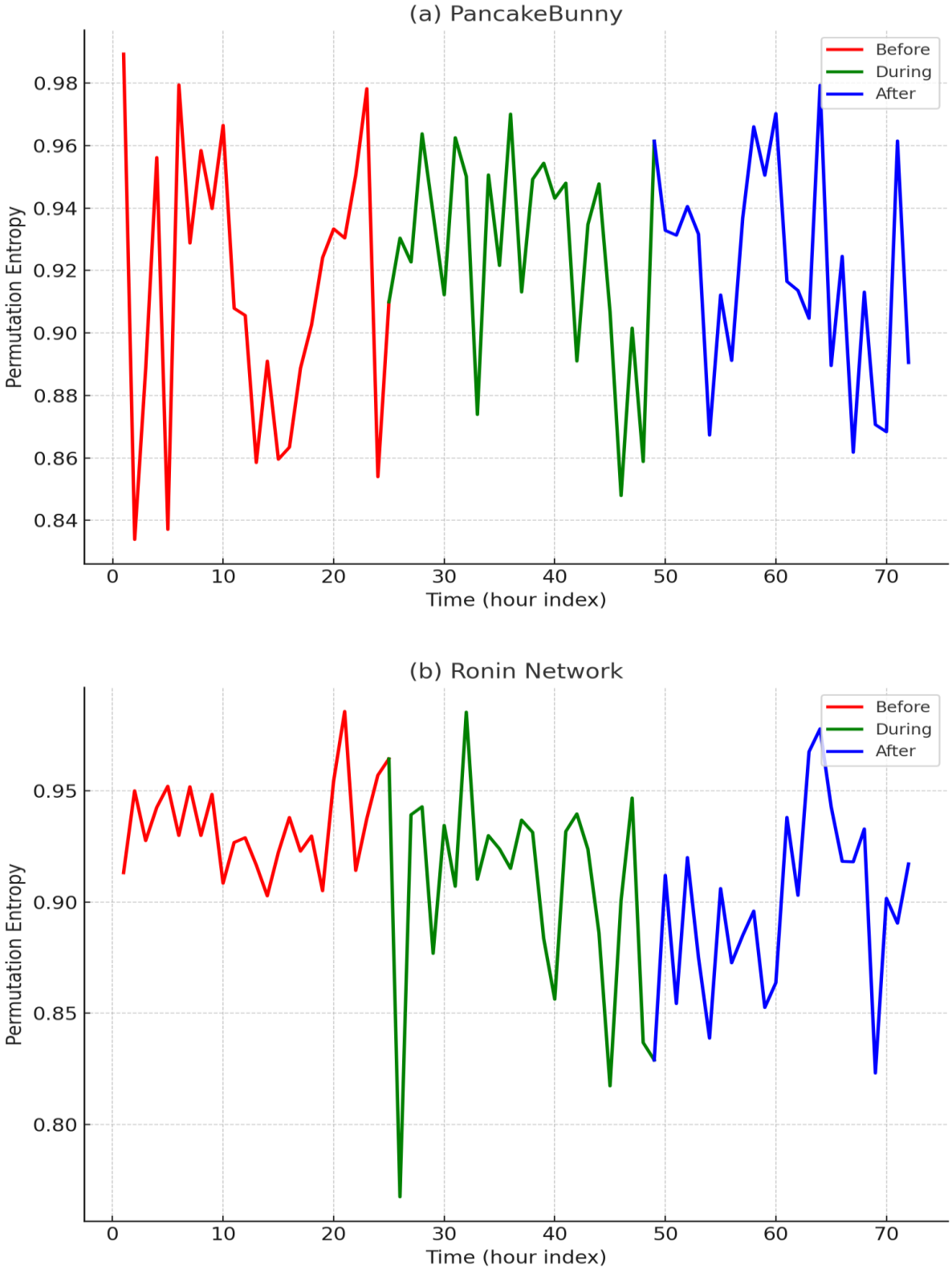
Notably, the Complexity–entropy causality plane for the Mt. Gox exchange heist (Figure 2.3 a.1) differs from other incidents. After the Mt. Gox exchange heist, most complexity–entropy

points shifted to the lower left corner, and permutation entropy (Figure 2.3 a.2) dropped to zero for 19 hours over three days, indicating a severe decline in market efficiency. As the world's largest Bitcoin exchange at the time, the Mt. Gox exchange heist resulted in the loss of approximately $450 million in Bitcoin, around 7% of the global Bitcoin supply. This incident triggered market panic, leading to mass sell-offs and significant price volatility. AMH highlights that market efficiency fluctuates as participants adapt to shocks. The Mt. Gox exchange heist, being the first large-scale hacking incident, disrupted the usual information-processing mechanisms. Investor panic and emotional reactions caused information transmission and price discovery to fail, leading to a sharp decline in market efficiency. Over time, the market may readjust and recover, but the initial drop in efficiency aligns with the dynamic efficiency characteristics outlined in AMH.

Moreover, Bitcoin's market efficiency did not significantly decrease during or after the PancakeBunny platform and Ronin Network heists. This may be because investors focused more on the tokens directly affected during these heists. In the PancakeBunny platform heist, hackers manipulated Binance Coin to steal approximately $200 million, while in the Ronin Network heist, they stole 173,600 Ethereum, totalling $620 million (Tsihitas, 2025). Subsequently, this chapter examines whether investors will pay more attention to Binance Coin and Ethereum than Bitcoin during these two cryptocurrency heists. This chapter collects 1-minute price data for Binance Coin and Ethereum from Cryptocompare and calculates their hourly permutation entropy. Figure 2.4 shows that the permutation entropy of Binance Coin and Ethereum fluctuated and dropped significantly during and after these two cryptocurrency heists.

While such cryptocurrency heists can affect the market efficiency of cryptocurrency markets, this impact varies across different tokens. For example, Ethereum was the most affected token in the Ronin Network heist; hence, its market efficiency changed significantly as investors focused more on the directly impacted tokens and adjusted their holdings accordingly. In contrast, although Bitcoin's market efficiency also fluctuated during this heist, its volatility was much lower than that observed in the Ethereum market.

Figure 2.4: The permutation entropy of Binance Coin in PancakeBunny platform heist and Ethereum in Ronin Network heist



Permutation entropy is calculated with an embedding dimension of 3. The sub-figures (a) and (b) illustrates the level of disorder in the Binance Coin and Ethereum market on the day before (red), the day of (green), and the day after the heist (blue). The higher the permutation entropy, the higher the market efficiency.

In summary, Bitcoin's market efficiency in the context of cryptocurrency heists is not static but fluctuates over time, consistent with previous findings (Lahmiri et al., 2018; Sensoy, 2019; Stosic et al., 2019; Fernandes et al., 2022). During or after most cryptocurrency heists, permutation entropy significantly declines, signalling a drop in market efficiency. However, in some cases, Bitcoin is less impacted as investors focus on the most affected tokens rather than Bitcoin, leading to a smaller decline in efficiency. Investors should adapt their strategies flexibly, avoid rigid approaches, and respond swiftly to external shocks based on market signals. Using high-frequency data makes it possible to promptly detect sudden shifts in investor sentiment and abnormal price fluctuations, providing early warning signals during periods of severe market turbulence and enabling investors to adjust their trading strategies swiftly, thereby managing losses or seizing opportunities more effectively under extreme shocks. At the same time, automated trading tools could execute buy and sell orders within milliseconds, quickly stopping losses or taking profits. Such strategies could also be automatically triggered to prevent investors from making suboptimal decisions during periods of panic, thereby helping to mitigate losses in times of large market fluctuations. Diversifying token holdings could also reduce the risks associated with the volatility of individual tokens, and by closely monitoring the most affected tokens, investors could better navigate fluctuations in market efficiency.

For policymakers, these fluctuations in market efficiency underscore the need for targeted regulatory frameworks. Increasing oversight of cryptocurrency exchanges, enforcing stricter security standards, and conducting regular audits could help reduce the risk of cryptocurrency heists. Additionally, requiring exchanges to promptly disclose security breaches and heist incidents would allow the market to respond more quickly, minimising the impact of information asymmetry on market efficiency. Maintaining efficient market conditions is essential for preserving investor confidence, liquidity, and stable price discovery in the cryptocurrency market. Several jurisdictions have already taken steps in this direction. For instance, the European Union's Markets in Crypto–Assets (MiCA) regulation mandates crypto service providers to meet security, transparency, and reporting standards, thereby reducing the risk of theft and improving market response to such events (Donnelly et al., 2024; Wronka, 2024). Similarly, following the Coincheck exchange heist, Japan's Financial Services Agency (2022) implemented stricter regulations requiring asset segregation and routine third-party audits for crypto exchanges, ensuring higher operational integrity.

Incorporating such practices globally could help build a more secure cryptocurrency ecosystem.

2.4.2 Robustness Checks

To ensure the robustness of the results, this chapter uses six classical randomness tests to assess Bitcoin's market efficiency during cryptocurrency heists. These include the Hurst exponent (Hurst, 1951), the Ljung–Box test (Ljung & Box, 1978), the Runs test (Wald & Wolfowitz, 1940), the Bartels test (Bartels, 1982), the Variance Ratio (VR) test (Lo & MacKinlay, 1988), and the BDS test (Broock et al., 1996). Although these tests are typically used within the framework of the EMH, they are applied here as methodological tools to detect deviations from randomness. The AMH does not reject the concept of market efficiency but instead conceptualises it as an evolving condition. Therefore, while grounded in EMH, the results of these tests can still provide complementary insights into the time-varying nature of market efficiency as proposed under the AMH framework.

The Hurst exponent measures the long-term memory of a time series, ranging from 0 to 1. A value above 0.5 suggests a positive long-term memory, below 0.5 indicates a negative long-term memory, and precisely 0.5 implies a random walk. The Ljung–Box test checks for serial correlation in the data, with the null hypothesis being no autocorrelation. The Runs test is a non-parametric test method for detecting the independence or randomness of a time series, and its null hypothesis is that the samples in the data set are random. The Bartels and VR tests detect whether the time series is a random walk. Their null hypothesis is that the time series is a random walk. The BDS test is a non-parametric statistical method that evaluates whether a time series exhibits autocorrelation or nonlinear correlation, assuming the null hypothesis that the series is independently and identically distributed.

Table 2.3 presents the p-value results of six randomness tests. Except for the VR test, which shows that the Bitcoin market is efficient during some cryptocurrency heists, the other five tests all indicate that it is inefficient during these cryptocurrency heists. These robustness test results align with the previous findings from the permutation entropy model and the Complexity–entropy causality plane.

Table 2.3: p-value results of six randomness tests in twelve cryptocurrency heists

Platform	Hurst exponent	Ljung–Box test	Runs test	Bartels test	VR test	BDS test
Mt Gox	0.54	0.00	0.00	0.00	0.00	0.00
Coincheck	0.59	0.00	0.00	0.00	0.00	0.00
KuCoin	0.49	0.00	0.00	0.00	0.00	0.00
PancakeBunny	0.59	0.00	0.00	0.00	0.19	0.00
Poly Network	0.52	0.00	0.00	0.00	0.00	0.00
Bitmart	0.61	0.00	0.00	0.00	0.82	0.00
Wormhole	0.44	0.00	0.00	0.00	0.05	0.00
Ronin Network	0.47	0.00	0.00	0.00	0.00	0.00
Beanstalk	0.60	0.00	0.00	0.00	0.22	0.00
Nomad	0.49	0.00	0.00	0.00	0.39	0.00
Binance	0.56	0.00	0.00	0.00	0.20	0.00
FTX	0.53	0.00	0.00	0.00	0.01	0.00

Before conducting the robustness tests, the data are subjected to necessary preprocessing procedures. Specifically, Bitcoin returns are calculated as $R_t = \mathrm{Ln}[(P_t)/(P_t - 1)] \times 100$, and the first differences are tested for stationarity using the Augmented Dickey–Fuller (ADF) test.

2.5 Conclusion

This chapter delves into the impact of cryptocurrency heists on the efficiency of the Bitcoin market. The analysis of permutation entropy and the Complexity–entropy causality plane reveals a significant reduction in market efficiency during most cryptocurrency heists. According to AMH, market efficiency fluctuates in response to shocks, as investors struggle to adapt to changing environments. The sudden uncertainty and chaos following a cryptocurrency heist make it challenging for investors to process, understand, and analyse the new information related to the incident. This delay in information processing impedes investors from making suitable decisions, often leading to sentiment reactions like panic selling or buying, causing prices to deviate from their true price and further declining market efficiency. This chapter also reports instances of cryptocurrency heists where Bitcoin's market efficiency does not decrease significantly. This suggests that investors may concentrate on the most impacted tokens when analysing specific incidents. Different tokens may respond differently to cryptocurrency heists, so investors should recognise that market efficiency and volatility vary among tokens.

The findings provide valuable insights for investors to refine their investment and risk management strategies. For instance, they should adapt their strategies flexibly and respond quickly to external shocks based on market signals. By using high-frequency data and

automated tools, investors could mitigate losses during periods of significant market volatility. The results also underscore the importance of distinguishing between different tokens, as they may react differently to cryptocurrency heists. Investors need to recognise that the volatility and efficiency of each token vary, and their investment strategies should be adjusted accordingly. Diversifying token holdings could help reduce the risks associated with the fluctuations of individual tokens, and by closely monitoring the most affected tokens, investors could better navigate changes in market efficiency.

Because Bitcoin's market efficiency declines during cryptocurrency heists, policymakers should work to enhance exchange and platform security standards and transparency to respond quickly to such incidents, reduce uncertainty, and maintain market stability. Policymakers also need to devise more effective regulatory measures that embrace a dynamic approach to mitigate market risks and minimise the influence of malicious activities. It is essential to maintain Bitcoin's market efficiency by implementing stricter security protocols on the platform and establishing transaction limits to prevent hackers' exploitation of vulnerabilities. For example, the European Union has taken the lead in implementing a unified framework through the Markets in Crypto–Assets (MiCA) regulation, which introduces comprehensive requirements for crypto service providers, including licensing, capital requirements, cybersecurity standards, and mandatory disclosure of security breaches. Japan, learning from high-profile incidents like the Coincheck exchange heist, now imposes strict oversight on cryptocurrency exchanges through the Financial Services Agency (FSA), requiring asset segregation, third-party audits, and robust security protocols. Such measures could be productively replicated internationally.

An important avenue for future studies is to extend the event window to longer horizons to capture the delayed effects of cryptocurrency heists. While this study adopts a three-day window to focus on immediate market reactions, some consequences may unfold over longer periods, particularly in cases where stolen cryptocurrencies or funds are eventually resituated. Asset restitution may not only accelerate market recovery but also strengthen investor confidence and liquidity, thereby reshaping the dynamics of market efficiency. Designing longer event windows would thus enable us to distinguish between short-term volatility shocks and medium- to long-term recovery processes. In addition, future studies should seek to develop statistical methods capable of testing whether changes in permutation entropy measures are significant, so as to provide a more rigorous assessment of the evolution of

market efficiency. While such tools are not yet fully developed, their advancement would offer valuable support for related studies.

Furthermore, the present study documents associations between cryptocurrency heists and shifts in Bitcoin's market efficiency, but it does not formally establish causality. This is a common limitation of entropy-based approaches, which are effective in detecting structural changes but not designed for causal identification. Future studies can integrate permutation entropy with econometric techniques such as Granger causality tests or structural break models to assess whether hacking incidents are genuine drivers of efficiency losses rather than coincidental correlates. Finally, the findings should be interpreted in the context of broader market conditions. The use of a three-day event window helps mitigate the influence of concurrent macroeconomic or regulatory events, but given Bitcoin's high volatility and its sensitivity to external shocks, it is difficult to rule out residual confounding entirely. Future studies can incorporate controls such as macroeconomic news shocks or global risk sentiment to more clearly isolate the marginal effect of cryptocurrency heists on market efficiency dynamics.

Overall, this chapter provides investors with important insights by enhancing their understanding of how extreme events affect the Bitcoin market and by improving their risk management practices. Investors should recognise that the Bitcoin market is vulnerable to cryptocurrency heists, particularly major events that have far-reaching consequences for the entire crypto community. Therefore, investors are advised to remain vigilant regarding market volatility and uncertainty and to formulate investment strategies accordingly to manage risk.

Chapter 3 The Relationship between Bitcoin Price and Market Sentiment: New Evidence from a Cryptocurrency Heist

Parts of this chapter have been published in the North American Journal of Economics and Finance

3.1 Introduction

With a 56.8% market share and the highest market value, Bitcoin dominates the cryptocurrency market. However, its price is highly volatile. For instance, the price of Bitcoin dropped from about $66,000 at the end of 2021 to just over $16,000 in early 2023, then surged back to $100,000 by December 2024 (CoinGecko, 2024). Traditional financial theories based on rational pricing models struggle to provide predictive or valuable insights into the pricing of highly volatile assets such as Bitcoin, as argued by Kristoufek (2013). Instead, Bitcoin's price is primarily driven by investors' perceptions of its growth potential (Cachanosky, 2019; Eom et al., 2019). Current studies have highlighted the crucial role of investor sentiment in Bitcoin price formation. Positive beliefs about Bitcoin's future may lead investors to buy more, driving up prices, while pessimistic beliefs could prompt selling and price declines. Therefore, understanding and analysing investor sentiment is key to understanding Bitcoin's price dynamics.

Previous studies have focused on the role of different sentiment indicators in predicting Bitcoin price, such as surveys, social media, indices, and Google search volume (Kaminski, 2014; Kapar & Olmo, 2021; Ullah et al., 2022; Kim et al., 2021; Meyer et al., 2023). However, these studies usually focus only on the impact of sentiment on price while ignoring the effect of prices on sentiment. Sentiment movements can influence price, and price can, in turn, affect sentiment movements. For instance, sentiment changes can drive price movements. Negative news or pessimistic sentiment on social media platforms can induce fear, prompting selling and price drops. Conversely, positive news or sentiment attracts buyers, driving prices up. On the other hand, a surge in Bitcoin price typically sparks excitement and optimism among investors, driving further investment and increasing the price. Conversely, price declines can trigger anxiety and panic, leading to selloffs and additional downward pressure on price. Moreover, many studies focused on global events, such as the COVID-19 pandemic and geopolitical conflicts, while neglecting the specific context of the Bitcoin market. This oversight may hinder our ability to discern whether

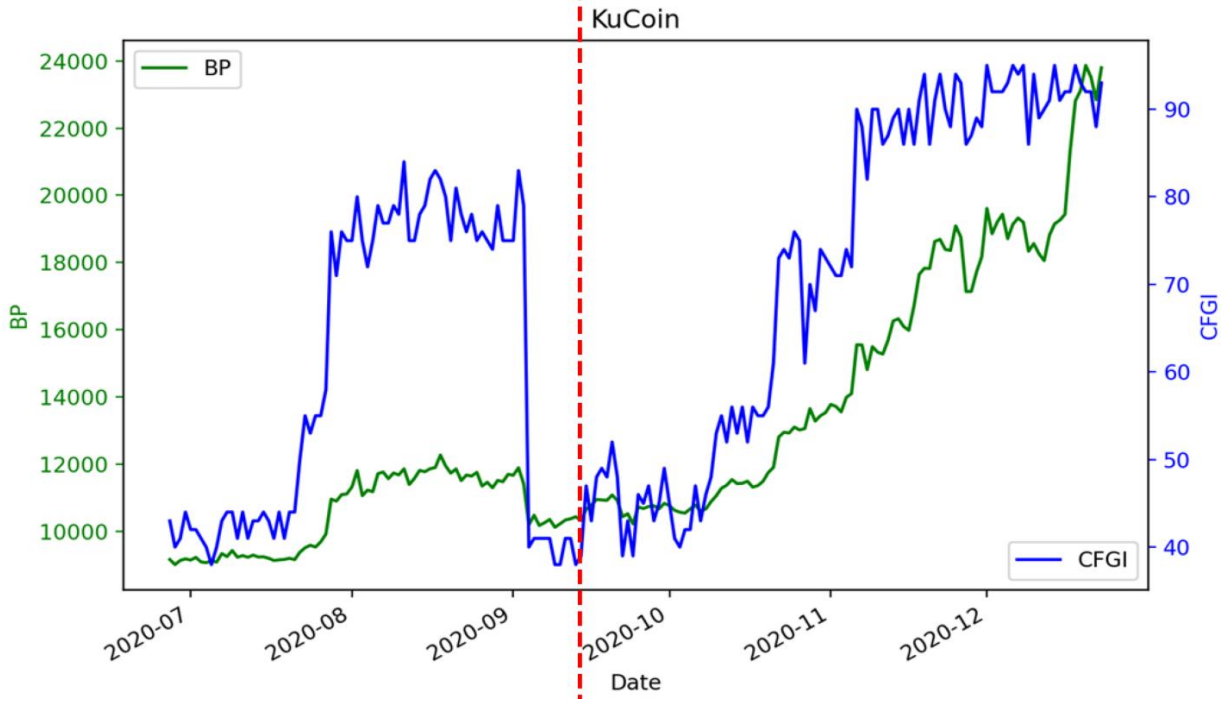
Bitcoin price fluctuations are primarily driven by Bitcoin market sentiment or broader sentiment in global financial markets, potentially leading to biased research results (Gaies et al., 2023).

Cryptocurrency heists offer a significant opportunity to examine the predictive relationship between price and sentiment. Many individuals store their cryptocurrencies in exchanges' hot wallets, linking the security of these assets to the exchanges. Over the years, hackers have targeted these exchanges, exploiting vulnerabilities to steal cryptocurrencies and make profits. The Mt. Gox exchange hack in 2014 and the Ronin Network platform attack in 2022 led to the theft of billions of dollars in Bitcoin and $595 million in Ethereum, respectively, underscoring this vulnerability. As the cryptocurrency with the highest price, Bitcoin garners significant attention from attackers. From 2011 to 2021, around 1.7 million Bitcoins, worth over $700 million, were stolen, representing about 10% of the total Bitcoin supply (Grobys et al., 2022). These attackers employ 51% attacks (i.e. control over 50% of the network) and exploit exchange and wallet vulnerabilities to steal Bitcoin and generate substantial profits (Wen et al., 2021). These heists amplify concerns about cryptocurrency ecosystem security, potentially sparking panic, anxiety, and selling pressure among investors (Marella et al., 2021). When the price drops significantly, the value of investors' assets shrinks rapidly, potentially intensifying market panic and anxiety. Additionally, the market may perceive a price decline as further confirmation of the incident's risks, reinforcing negative sentiment and leading to further market environment deterioration (Kapar & Olmo, 2021; Dias et al., 2022), such as a decline in market efficiency (Li et al., 2024).

This chapter uses the Crypto Fear & Greed Index (CFGI) as a proxy for investor sentiment in the Bitcoin market. Since CFGI primarily captures sentiment related to Bitcoin, the analysis focuses on cryptocurrency heists that directly target Bitcoin or involve the theft of a large amount of Bitcoin, thereby avoiding distortion of the relationship between Bitcoin price and sentiment. The most recent major incident of this kind was the KuCoin exchange heist. KuCoin, a Singapore-based cryptocurrency exchange, offers trading in over 200 different assets, with a daily trading volume of approximately $100 million. On September 25, 2020, KuCoin exchange suffered a cyberattack in which hackers infiltrated the exchange's system, obtained the private keys to its hot wallets, and transferred approximately $281 million worth of Bitcoin. This cryptocurrency heist is also one of the largest to date (Tsihitas, 2025). Although this incident does not compromise the Bitcoin blockchain itself, which is widely regarded as virtually hack-proof, it exposes security vulnerabilities in centralised trading

platforms and seriously damages investor confidence. This is because Bitcoin is the largest and most symbolic asset stolen, and it functions as the benchmark currency for the entire cryptocurrency market. Ordinary investors often fail to distinguish between "an exchange being hacked" and "Bitcoin itself being hacked," and thus may interpret such incidents as evidence of Bitcoin's insecurity. Moreover, as exchanges are the primary gateways to Bitcoin liquidity, their security is directly linked to trust in the Bitcoin market (Fang et al., 2025). For these reasons, the KuCoin exchange heist is not merely perceived as a case of asset loss but as a shock to the stability and safety of the Bitcoin ecosystem, likely exerting a deeper influence on Bitcoin price and sentiment than cryptocurrency heists involving other cryptocurrencies. Figure 3.1 illustrates the dynamics of Bitcoin price (BP) and CFGI over the three months before and after the KuCoin exchange heist. The figure shows that Bitcoin price and investor sentiment move somewhat together both before and after the incident. However, correlation does not necessarily imply a predictive relationship, highlighting the need for further investigation.

Figure 3.1: Bitcoin price (BP) and CFGI dynamics in the three months before and after the KuCoin exchange heist



The red dashed line marks the date of the KuCoin exchange heist on 25 September 2020. The Bitcoin price data is sourced from CoinGecko, while the CFGI data is obtained from Alternative.me.

Existing studies suggest that external shocks often amplify market reactions by altering investor sentiment (Polat et al., 2022; Anamika et al., 2023; Gaies et al., 2023). In the cryptocurrency market, sudden events such as hacks or exchange thefts not only cause direct asset losses but also intensify uncertainty and fear among participants. When sentiment deteriorates, panic selling may drive prices down, while falling prices in turn reinforce negative sentiment, creating a self-reinforcing feedback loop. Hence, it can be expected that after a cryptocurrency heist, the relationship between Bitcoin price and sentiment is more likely to exhibit a bidirectional predictive relationship. Based on this context, this chapter proposes the first hypothesis:

H1: KuCoin exchange heist may enhance the bidirectional predictability between Bitcoin price and CFGI.

However, since the CFGI is specifically designed to capture sentiment within the Bitcoin market, its effectiveness as a sentiment proxy may be limited in cryptocurrency heists that do not directly involve Bitcoin. In such cases, the sentiment and trading responses of investors may be concentrated on the affected token, with Bitcoin playing a less central role in the incident. As a result, the interaction between the Bitcoin price and CFGI may be weaker. Based on this reasoning, this chapter proposes the second hypothesis:

H2: In cryptocurrency heists not targeting Bitcoin, the influence of CFGI on Bitcoin price is weaker, and the impact of Bitcoin price on CFGI is also limited.

Additionally, as the benchmark asset in the cryptocurrency market, Bitcoin often profoundly influences the broader ecosystem (Katsiampa et al., 2019a; Kuma & Anandarao, 2019; Özdemir, 2022). While market panic triggered by the KuCoin exchange heist may ripple through other cryptocurrency markets, CFGI primarily reflects sentiment within the Bitcoin market. As such, relying on CFGI to predict other cryptocurrencies' performance in the KuCoin exchange heist may not be reliable. Therefore, this chapter proposes the third hypothesis:

H3: The volatility in CFGI caused by Bitcoin heist has a limited impact on other cryptocurrency markets.

There are three key findings in this chapter. First, time-varying Granger causality tests reveal that the predictive relationship between Bitcoin price and CFGI changes significantly before and after the KuCoin exchange heist. During the 90 days prior to the KuCoin exchange heist,

there is no statistically significant bidirectional predictive relationship between Bitcoin price and CFGI, with CFGI showing limited predictive power for Bitcoin price and vice versa. However, in the 90 days following the KuCoin exchange heist, a statistically significant bidirectional predictive relationship emerges, with CFGI's influence on Bitcoin price strengthening and Bitcoin price also influencing CFGI. This suggests that, although CFGI serves as a key indicator of Bitcoin market sentiment, its predictive relationship with Bitcoin price is dynamic. Under stable market conditions without major unexpected events, CFGI has limited predictive value for Bitcoin price, and minor price fluctuations exert little impact on CFGI. However, during major shocks, swings in market sentiment and increased price volatility amplify this relationship. For investors, it is important to approach panic-driven trading behaviour with caution during cryptocurrency heists, as sentiment responses may exacerbate price declines and lead to suboptimal decisions. At the same time, the dynamic interaction between Bitcoin price and sentiment during such periods highlights the potential of event-driven trading strategies, where sentiment indicators can serve as early warning signals for heightened market instability.

Second, no statistically significant bidirectional predictive relationship is found between Bitcoin price and CFGI in cryptocurrency heists that do not involve Bitcoin theft. In such cases, relying on CFGI to predict Bitcoin price, or using Bitcoin price to forecast changes in CFGI, is not an effective approach. However, if the cryptocurrency heist indirectly affects the Bitcoin market, a statistically significant bidirectional predictive relationship between Bitcoin price and CFGI can still be observed. This suggests that the predictive power of CFGI for Bitcoin price, as well as the influence of Bitcoin price on CFGI, is closely tied to whether the cryptocurrency heist impacts the Bitcoin market. Finally, using the TVP-VAR-based connectedness approach, this chapter finds that the CFGI volatility triggered by the KuCoin exchange heist does not exhibit statistically significant spillovers into other cryptocurrency markets. This indicates that the impact of CFGI fluctuations remains primarily confined to the Bitcoin market, with minimal influence on other cryptocurrency markets. However, while investors can use CFGI to make short-term trading decisions for Bitcoin during Bitcoin-specific heists, its applicability to other cryptocurrencies may be limited. Solely relying on CFGI could lead investors with diversified cryptocurrency portfolios to draw misleading conclusions.

These findings offer valuable insights for policymakers focused on the Bitcoin market. First, the intensified bidirectional predictive relationship between Bitcoin price and CFGI following

cryptocurrency heists that directly involve Bitcoin suggests that the market is highly sensitive to such security breaches. This underscores the importance of timely and transparent incident disclosure by affected exchanges to reduce uncertainty and prevent sentiment overreaction within the Bitcoin market. Second, the heightened volatility in CFGI during these incidents demonstrates its potential as a real-time sentiment indicator for Bitcoin-specific market risk. Regulators may consider incorporating CFGI into early warning systems for detecting risks in the Bitcoin market.

To sum up, this study is highly significant for two reasons. First, cryptocurrency heists substantially impact asset prices, market sentiment, and the overall stability of the ecosystem, warranting detailed analysis. Second, as cryptocurrencies emerge as a new frontier in financial markets, understanding the factors that influence market stability is critical for investors to adjust their strategies and for policymakers to implement effective regulation. This chapter is structured as follows. The second section presents the literature review, the third outlines the data and methodology, the fourth discusses the empirical results, and the fifth concludes the chapter. The sixth section contains the appendix, which includes robustness checks and supplementary analyses.

3.2 Literature Review

3.2.1 From Traditional Finance to Behavioural Finance

Modern financial theory is strongly influenced by two cornerstone concepts: the Capital Asset Pricing Model (CAPM) and the Efficient Market Hypothesis (EMH) (Sharpe, 1964; Fama, 1970). Both assume that investors are rational and able to respond efficiently to market information, thereby overlooking the complexities of actual investor behaviour and treating the stock market as inherently unpredictable. However, since the emergence of behavioural finance, many studies have shown that under incomplete information, investors' actions, attitudes, and preferences often deviate from the assumption of full rationality. Asset prices are not purely random and can, to some extent, be predictable (Zhang et al., 2017). Behavioural finance integrates insights from the broader social sciences into financial economics. Since the pioneering work of scholars such as Shiller (1981), De Bondt and Thaler (1985), Shefrin and Statman (1985), and Roll (1986), a substantial body of literature has emerged, positioning behavioural finance as an important complement to traditional financial theory.

Sentiment is a core concept in behavioural finance, which posits that sentiment influences individual decision-makers, institutions, and markets. For example, Kamstra et al. (2000) found that stock returns tended to be negative around the weekend when daylight saving time transitioned to standard time. They suggested investors suffering from seasonal affective disorder might experience negative sentiment due to the time change. Such sentiment can impair investors' ability to process information efficiently and concentrate on trading, leading to lower stock returns. Similarly, Hirshleifer and Shumway (2003) found that weather conditions could influence investor sentiment, positive on sunny days and negative on cloudy days. They observed that stock returns were significantly higher on sunny days and lower on cloudy days. This may be because positive sentiment enhances investors' capacity to process information and make rational decisions, whereas negative sentiment may induce doubt and pessimistic interpretations of subsequent information, resulting in suboptimal investment choices.

Ashton et al. (2003) suggested that there may be a relationship between national sports performance and stock market returns. Their findings indicated that when the England football team performed well in qualifying or final matches, subsequent stock market performance tended to improve; conversely, poor performance was associated with market declines. This may be attributed to the psychological boost from sporting success, which increases investors' confidence in the future. While the positive effect of victory has gradually diminished, the anomaly has persisted (Ashton et al., 2011). Similarly, Scholtens and Peenstra (2009) examined the relationship between football match results and stock price changes using data from eight national teams across 1,274 matches between 2000 and 2004. The results showed that stock markets generally reacted positively to victories and negatively to defeats, with losses triggering stronger price reactions than wins. Bernile and Lyandres (2011) further argued that such effects might be the result of systematic expectation bias. Investors may become overly optimistic before matches, only to be disappointed after unfavourable outcomes, which in turn drives pessimism and negative returns in the following trading days.

These studies indicate that investor sentiment plays an important role in the process of price formation, yet the relationship between sentiment and price is not unidirectional. Price fluctuations can, in turn, influence investor sentiment, creating a self-reinforcing feedback mechanism (Marczak & Beissinger, 2016; He et al., 2019; Kapar & Olmo, 2021). For example, when asset prices suddenly experience a sharp decline, investors often react with

panic and intensify selling pressure, which further drives prices down. Conversely, when prices rise rapidly, optimism and greed may attract more investors to enter the market, leading to momentum-driven buying that pushes prices even higher. This process, in which price changes trigger shifts in sentiment that subsequently amplify price movements, exemplifies the bidirectional interaction between price and sentiment.

Behavioural finance provides a theoretical framework to understand this mechanism, such as limited attention theory (Barber & Odean, 2008), overreaction theory (De Bondt & Thaler, 1985), and herding behaviour (Banerjee, 1992; Bikhchandani et al., 1992). Limited attention theory posits that individuals have limited cognitive resources and cannot process all information simultaneously, forcing them to allocate attention selectively. This limited attention makes investors more susceptible to salient information (e.g., media coverage, market sentiment), which may cause asset prices to become temporarily overvalued or undervalued. When asset returns are negative, investors tend to focus excessively on downward trends, increasing the likelihood of undervaluation; when returns are positive, they tend to overemphasise upward trends, increasing the likelihood of overvaluation. Overreaction theory highlights that, under uncertainty, investors often respond excessively to market information due to cognitive biases, leading to short-term deviations of asset prices from their intrinsic value. This is most visible in the form of excessive optimism in bull markets that drives prices higher and excessive pessimism in bear markets that accelerates declines, generating mutually reinforcing effects. Herding behaviour further emphasises that investors often do not act independently but instead follow the actions of others. In downturns, panic sentiment may trigger widespread selling, whereas in upswings, greed may fuel momentum-driven buying. Sentiment contagion and price dynamics reinforce one another, thereby amplifying volatility.

Taken together, these behavioural finance frameworks reveal that price fluctuations themselves stimulate psychological responses, while investor sentiment rapidly spreads through mechanisms such as herding, ultimately creating a bidirectional feedback loop between price and sentiment. This dynamic interaction provides a theoretical foundation for understanding the relationship between Bitcoin price and sentiment in the context of cryptocurrency heists. However, while these theories establish the foundations for the sentiment-price feedback mechanism, empirical validation remains a central challenge. Sentiment is inherently vague and subjective, and individuals may interpret and respond to the same situation differently. Consequently, scholars typically rely on proxy indicators to

measure sentiment, but different proxies may significantly affect the findings. In examining the relationship between Bitcoin price and sentiment, the choice of sentiment proxies can thus shape the results. The following section reviews the literature on various sentiment indicators to identify suitable measures for empirical analysis.

3.2.2 Sentiment Measures and Their Application in the Bitcoin Market

According to the survey, sentiment measures can be broadly categorised into direct and indirect (Bouteska et al., 2022). The first group measures investor sentiment through direct measurement, including two sentiment indicators: survey-based and sentiment analysis-based. Survey-based indicators, such as Sentix survey data, measure investor sentiment monthly by assessing investors' willingness to purchase Bitcoin. Scholars found that when investors are more willing to buy (optimism towards Bitcoin), Bitcoin price shows an upward trend. Moreover, negative sentiment from investors has a more pronounced impact on Bitcoin price than positive sentiment (AlNemer et al., 2021; Anamika et al., 2023). In studies using sentiment analysis-based indicators, Scholars often gather sentiment data from platforms like Twitter, BitcoinTalk, or Reddit to capture current investor sentiment. Kaminski (2014) examined three months of tweets related to Bitcoin, constructing a sentiment indicator from words indicating positive and negative sentiment. They found that sentiment mirrors market conditions rather than predicts Bitcoin price trends. However, Garcia and Schweitzer (2015) and Perry-Carrera (2018) used sentiment analysis methods on tweets with cryptocurrency-specific lexicons, discovering that sentiment can predict Bitcoin price trends using vector autoregression models. Kraaijeveld and De Smedt (2020) demonstrated Twitter sentiment's predictive ability on returns for Bitcoin, Bitcoin Cash, and Litecoin. Sattarov et al. (2020) analysed Bitcoin-related tweets and financial data, finding the predictive power of Twitter sentiment on Bitcoin price, achieving 62.48% accuracy in out-of-sample price predictions. Saleem et al. (2024) collected over 3 million tweets from 2013 to 2022 using 'bitcoin' and 'BTC' keywords. They employed the Valence Aware Dictionary and Sentiment Reasoner (VADER) and logistic regression model for sentiment analysis, showing that negative sentiment significantly impacts Bitcoin price declines. In contrast, positive sentiment has a minor role in driving price increases.

Twitter provides the Twitter Happiness Index, a direct sentiment indicator derived from about 10,000 sentiment-related words in randomly selected Twitter posts. Naeem et al. (2021b) assessed its predictive ability on returns of six major cryptocurrencies, revealing a significant

nonlinear Granger causality relationship with returns. Subsequently, Naeem et al. (2021c) employed bivariate cross-change plots and found their ability to predict Bitcoin returns under extreme market conditions, suggesting sentiment-based portfolio adjustments. However, Perry-Carrera (2018) noted that because Twitter is a platform for general users, many posts may be misclassified, leading to the collection of irrelevant information and an inefficient data-gathering process. Specialised cryptocurrency discussion platforms like BitcoinTalk, StockTwits, or Reddit are preferable to enhance sentiment data quality. These platforms have a high level of specialisation, reducing the likelihood of collecting unrelated information about Bitcoin. Mai et al. (2018) examined the dynamic interaction between investor sentiment on social media and Bitcoin price using text analysis and a vector error correction model. They found that investor sentiment is a significant predictor of Bitcoin price, but not all social media sentiments have an equal impact. Compared to sentiment gathered from Twitter, investor sentiment collected from professional discussion platforms or websites has a more significant influence on the future price of Bitcoin.

Therefore, recent studies focused on gathering investor sentiment from professional discussion platforms or websites. Chen et al. (2019) created a cryptocurrency-specific lexicon from StockTwits and Reddit messages. They used a local-momentum autoregression model and found sentiment effects during cryptocurrency bubbles that persist but reverse after the bubble bursts. Bouteska et al. (2022) developed a sentiment indicator using computational text analysis from StockTwits and Reddit, employing vector autoregression analysis to predict short-term returns in the Bitcoin market. Guégan and Renault (2021) analysed approximately one million StockTwits messages, finding a significant relationship between investor sentiment and Bitcoin returns only in high-frequency data at 15-minute intervals, disappearing as data frequency decreases.

The second group of measuring investor sentiment involves indirect measurement, which includes using cryptocurrency indices or Google search volume. One commonly used cryptocurrency index is the Cryptocurrency Volatility Index (CVI), developed by the research team at COTI (Currency of the Internet). This innovative tool aims to capture the overall volatility of the cryptocurrency market. Based on the Black–Scholes–Merton model, the CVI is calculated using the 30-day implied volatility of the two largest cryptocurrencies by market capitalisation, Bitcoin and Ethereum. It reflects not only idiosyncratic risk within the cryptocurrency market but also systemic risk. Gaies et al. (2024) used the CVI to reveal a strong dependence between instability in the U.S. financial system and volatility in the global

cryptocurrency market, a relationship that becomes even more pronounced during periods of financial turbulence. Their findings suggested a transmission mechanism of financial risk between the stock market and the cryptocurrency market, implying that during turbulent times, volatility in the cryptocurrency market could spill over into broader financial markets. Another commonly used cryptocurrency index is the Volatility Index of Cryptocurrency (VCRIX), proposed by Kim et al. (2021). Studies by Kim et al. (2021) and Bouteska et al. (2022) indicated that VCRIX can effectively predict market trends and has good predictive ability for Bitcoin returns.

Google search volume serves as another sentiment proxy. Using the vector autoregression model, Kristoufek (2013, 2015) found a close relationship between Bitcoin price, Google search volume, and Wikipedia search volume. Building on this, Abraham et al. (2018) predicted cryptocurrency prices using sentiment from both tweets and Google search volume, finding superior predictions from Google search volume. Goczek and Skliarov (2019) employed a factor-augmented vector error correction model, identifying Bitcoin's popularity, reflected in Google search volume, as the primary driver of its price. Eom et al. (2019) used autoregressive models to study sentiment's impact on Bitcoin returns and volatility changes, finding Google search volume informative in predicting Bitcoin volatility. Kapar and Olmo (2021) constructed vector error correction models for 2010–2017 and 2010–2019, considering factors like the S&P 500 Index, gold prices, Bitcoin Google search volume, and the FED Financial Stress Index. They found that from 2010 to 2018, all factors influenced Bitcoin price, with Google search volume positively impacting prices. However, Google search volume becomes the sole variable explaining Bitcoin price dynamics in subsequent periods. Sabalionis et al. (2021) utilised the VAR–GARCH–BEKK model to analyse how Google search volume, tweet counts, and blockchain active addresses impact Bitcoin and Ethereum prices over time. Results showed that while Google search volume and tweet counts have some influence on prices, they are much weaker compared to active addresses. Bouteska et al. (2022) similarly used Google search volume to study sentiment's predictive power on Bitcoin price during COVID-19. The results are consistent with their StockTwits and Reddit sentiment data findings, indicating that investor sentiment significantly impacts Bitcoin returns during the COVID-19 pandemic.

However, some studies have suggested that Google search volume has a limited impact on Bitcoin price. Aalborg et al. (2019) incorporated this variable into a factor model explaining Bitcoin price, finding minimal influence across different data frequencies. Cheah et al. (2022)

treated search volume as a sentiment proxy but discovered no significant relationship with Bitcoin returns in various samples and asset allocation tests. Discrepancies in findings may arise from differing research periods, data frequencies, or market conditions. Moreover, sentiment complexity and noisy trading in the Bitcoin market may lead to short-term inconsistencies between sentiment and prices, affecting research outcomes. Panagiotidis et al. (2019) observed Google search volume's greater predictiveness in cryptocurrency's early stages, yet with diminishing effectiveness over time. This may reflect the rise of professional discussion platforms, where investors rely less on internet searches to gauge sentiment, reducing Google search volume's representativeness in today's cryptocurrency market.

Most findings suggest sentiment could predict Bitcoin price, but limitations exist. Firstly, direct or indirect sentiment measures may not capture sentiment comprehensively, potentially biasing indicators (Gaies et al., 2023). For instance, sentiment classification indirect measures may be subjective, and data from platforms like Twitter or Reddit may have limited samples, not fully representing the Bitcoin market or sentiment (Kim et al., 2018). Also, manipulation, fake accounts, and bots can influence social media platforms, introducing biases to sentiment analysis (Chen et al., 2022; Weng & Lin, 2022). Social media data may also lack robustness and be influenced by cycles, intervals, and measurement methods (Ahmed, 2022; Cheah et al., 2022). In indirect measures, the popularity of professional social media forums has gradually diminished the capacity of such indicators to reflect sentiment, rendering them unsuitable as reliable proxies for sentiment (Panagiotidis et al., 2019; Gaies et al., 2023). Hence, adopting new sentiment measurement methods is crucial. One potential approach is a comprehensive method combining direct and indirect components to form a holistic sentiment measure rather than considering these elements separately.

3.2.3 Crypto Fear & Greed Index

This chapter recommends using the Crypto Fear & Greed Index (CFGI) as a proxy for Bitcoin market sentiment. This indicator integrates social signals and market trends to capture overall sentiment in the Bitcoin market. It is calculated by Alternative.me and released daily at midnight. The CFGI is specifically designed for Bitcoin and consists of six components: social media interest (15%), volatility (25%), market volume (25%), cryptocurrency surveys (15%), market dominance (10%), and Google search trends (10%).

Social media interest is measured using a Twitter sentiment analysis tool, which collects posts under Bitcoin-related hashtags and evaluates their interaction speed and frequency within a

given time frame. An abnormally high engagement rate indicates rising public interest in Bitcoin and reflects greedy market behaviour. Volatility is assessed by comparing current Bitcoin volatility and maximum drawdowns against the 30-day and 90-day averages, where unusually high volatility signals market fear. Market volume captures current trading activity and momentum relative to the 30-day and 90-day averages, with abnormally high buying volume in a bullish market reflecting excessive greed and optimism. Cryptocurrency surveys are conducted weekly in collaboration with the large public polling platform Strawpoll.com, typically collecting 2,000 to 3,000 responses, thereby providing a general measure of investor sentiment. Market dominance refers to Bitcoin's share of the total cryptocurrency market capitalisation. An increase in dominance indicates a flight to safety toward Bitcoin due to concerns about speculative alt-coin investments, which is interpreted as a signal of fear. Conversely, a decrease in dominance suggests a shift toward more speculative alt-coins, signalling greed. Finally, Google search trends, obtained from Google Trends, measure the number of searches for Bitcoin-related keywords. Rising searches for terms such as "Bitcoin price manipulation" are interpreted as signs of fear, while increased searches for "Bitcoin price prediction" reflect optimism in the market.

The CFGI identifies both positive and negative sentiment by combining the above data sources into a single value, ranging from 0 (extreme fear) to 100 (extreme greed). An increase in the CFGI indicates a rise in positive sentiment, whereas a decrease reflects a rise in negative sentiment. Gaies et al. (2023) highlighted CFGI's advantage in considering multiple factors in Bitcoin price formation. CFGI signals 'fear' amid Bitcoin volatility and low purchasing volume, while increased social media activity, like Google search trends and market dominance, shifts it towards 'greed'. Furthermore, by integrating direct investor survey responses, CFGI captures diverse behavioural factors ('fear' and 'greed') that might otherwise be analysed separately. Therefore, utilising CFGI provides a holistic view of sentiment trends among Bitcoin market participants, offering valuable insights for investors and policymakers to understand the psychological state of the Bitcoin market and anticipate potential trends.

The CFGI has increasingly become a widely accepted sentiment indicator in academic research. For instance, Gaies et al. (2023) employed a bootstrap rolling-window Granger causality test to examine the relationship between Bitcoin price and CFGI during the COVID-19 pandemic. Their findings suggested that the causal relationship between Bitcoin price and CFGI is not constant over time. Specifically, the interaction between panic

sentiment and Bitcoin price can be either negative or positive, with such bidirectional effects observed across several subperiods. More importantly, the nature of this relationship differs significantly before and during the pandemic, indicating that external shocks can alter the dynamic interplay between investor sentiment and price. Wang et al. (2024) reported a U-shaped relationship between CFGI and cryptocurrency price synchronicity. In particular, synchronicity decreases as CFGI rises, but when investors are in a state of extreme fear or greed, the herding behaviour driven by CFGI amplifies market co-movement, thereby increasing systemic risk and undermining portfolio diversification. Another study by Huang et al. (2024), using monthly data from 2016 to 2021 and employing both autoregressive distributed lag (ARDL) and error correction models (ECM), investigated the impact of CFGI on Bitcoin returns. The ARDL results revealed a significant long-term positive association, whereby heightened optimism and greed attract capital inflows that push Bitcoin's value upward, while heightened pessimism and fear trigger capital outflows that adversely affect market performance. The ECM analysis further confirmed that changes in sentiment exert direct and significant short-term effects on Bitcoin returns, underscoring the market's sensitivity to fluctuations in sentiment. Overall, these studies demonstrate that CFGI not only captures the multidimensional features of investor sentiment in cryptocurrency markets but also provides significant explanatory power for price volatility, market co-movement, and return dynamics.

3.2.4 Volatility and Structural Breaks in the Bitcoin Market

Although previous studies have proposed various sentiment measures and confirmed, to some extent, their predictive power for Bitcoin price, they often overlook the specific characteristics of the Bitcoin market. Compared with traditional financial assets, Bitcoin exhibits extreme volatility and frequent structural breaks following major shocks (Baur et al., 2018; Panagiotidis et al., 2022). These features not only influence the stability of the sentiment-price relationship but also provide a new perspective for understanding investor behaviour. Therefore, it is essential to review the literature on volatility and structural breaks to better understand Bitcoin's dynamics under extreme market conditions.

Previous studies have examined the time-varying behaviour of Bitcoin volatility within the GARCH framework. Gronwald (2014) employed an autoregressive jump intensity GARCH model and found that the Bitcoin price is particularly sensitive to extreme fluctuations, highlighting the market's vulnerability to sudden shocks. Bouoiyour and Selmi (2015)

evaluated the goodness-of-fit of different GARCH specifications over two sub-periods between 2010 and 2015. Their results indicated that in the earlier period, threshold GARCH models revealed high volatility persistence, whereas in the latter period, EGARCH suggested a reduction in persistence, implying that the evolution of market structure influences volatility dynamics. Bouri et al. (2017) compared the return-volatility relationship before and after the 2013 price crash. They found that before the crash, past shocks and volatility were negatively correlated, while the relationship disappeared afterwards. This suggests that before December 2013, positive shocks increased conditional volatility more than negative shocks, a reversed asymmetry compared with the stock market. They attributed this to Bitcoin's "safe-haven effect," whereby investors regarded Bitcoin as a hedge, causing volatility to rise alongside price increases. Similarly, Klein et al. (2018) adopted the asymmetric power ARCH (APARCH) and the fractionally integrated APARCH (FIGARCH) models, confirming the presence of asymmetric volatility in Bitcoin. Given that speculative activity intensifies during extreme price increases, volatility tends to rise during sharp upswings. They also identified strong persistence in variance shocks, indicating that once volatility rises, it declines only gradually over time. This persistence was especially evident during the boom of 2017 and the subsequent correction, when sharp price increases left volatility elevated for an extended period. Stavroyiannis (2018) employed a GJR–GARCH model to examine Bitcoin's Value-at-Risk (VaR) and related indicators, concluding that Bitcoin is highly volatile and more prone to breaching VaR thresholds than assets such as gold. Collectively, these findings demonstrate that Bitcoin's volatility is not only far higher than that of traditional assets but also characterised by persistence, asymmetry, and shifts, suggesting that its price dynamics are deeply shaped by external shocks and market state transitions.

Importantly, Bitcoin's high volatility does not occur in isolation but often coincides with structural breaks triggered by external shocks. Such breaks not only reshape the dynamics of price and volatility but also significantly affect investor sentiment, thereby amplifying market instability. Notably, the relationship between sentiment and volatility appears heterogeneous across studies. Cheung et al. (2015) documented the existence of bubbles in Bitcoin between 2011 and 2013, with their collapse coinciding with the failure of the Mt. Gox exchange. This structural break induced both drastic adjustments in price and volatility and a sharp deterioration in investor sentiment, which further destabilised the market. Wang et al. (2020) provided complementary evidence by showing that spikes in the Economic Policy Uncertainty (EPU) index exacerbate investor uncertainty, significantly increasing Bitcoin

volatility and trading volume while generating cross-country spillover effects. López-Cabarcos et al. (2021) further showed that investor sentiment exerts a significant influence on Bitcoin volatility, with negative sentiment and panic often associated with heightened volatility. Thus, Bitcoin's volatility may be amplified in both speculative environments and fear-driven markets, reflecting a dual sensitivity. This feature highlights how Bitcoin price dynamics are shaped by the interaction of market conditions and investor sentiment, in contrast to traditional financial markets, where volatility expansions are typically driven by negative shocks (Black, 1976; Christie, 1982; Campbell & Hentschel, 1992; Calvo & Mendoza, 2000).

Additionally, previous studies also found that different structural changes in the market have varying impacts on Bitcoin's volatility. Corbet et al. (2020b) revealed that cryptocurrencies react heterogeneously to U.S. Federal Reserve interest rate adjustments and quantitative easing (QE) announcements, with currency-based digital assets being particularly sensitive to policy shocks. These policy-driven structural breaks often trigger shifts in investor sentiment. Corbet et al. (2020c) further found that macroeconomic news related to unemployment and durable goods significantly influences Bitcoin returns, whereas announcements concerning GDP and CPI have a limited impact. This suggests that different types of external shocks elicit differentiated investor sentiment responses. Overall, these studies reveal that structural breaks often affect volatility by altering investor sentiment, underscoring its mediating role in cryptocurrency price dynamics. However, existing studies have primarily focused on shocks arising from structural breaks at the macroeconomic, policy, or financial market level. In contrast, there remains a lack of systematic investigation into how sudden events such as cryptocurrency heists shape investor sentiment and, through a bidirectional feedback mechanism, interact with Bitcoin's price dynamics. Addressing this gap, this chapter centres on the bidirectional interaction between Bitcoin price and sentiment in the context of cryptocurrency heists.

3.3 Data and Methodology

3.3.1 Variable and Descriptive Statistics

This chapter analyses the interaction between price and sentiment during the KuCoin exchange heist using the Bitcoin daily price (BP) in US dollars and the daily CFGI[2]. The

[2] CFGI only provides daily data.

Bitcoin price data is sourced from CoinGecko[3], while the CFGI data is obtained from Alternative.me. Since the dataset is daily data, it needs to ensure that the sample period is sufficiently long to guarantee the robustness of the model results. If the sample period is too short (less than one month), it may fail to capture the complete causal relationship. Conversely, a sample period that is too long (e.g. six months or one year) might dilute the heist's direct impact on investor sentiment and price dynamics due to the increasing influence of unrelated external factors over time. Manahov and Li (2024) found that, using daily data, a 120-day window could effectively capture the negative impact of cryptocurrency heists on the market. Building on this precedent, this chapter also employs a relatively long event window to trace the dynamics of price and sentiment surrounding the KuCoin exchange heist. However, a 120-day horizon risks incorporating unrelated macroeconomic, policy, or market events that could obscure the effect of the heist itself. To strike a balance between model robustness and noise minimisation, a 90-day window is therefore considered more appropriate. A 90-day period is sufficiently long to ensure an adequate sample size and capture short- to medium-term adjustments in price and sentiment, yet short enough to minimise external noise and ensure that the identified effects can be primarily attributed to the heist. Specifically, the pre-heist period spans from June 27, 2020, to September 24, 2020, while the post-heist period covers September 25, 2020, to December 23, 2020.

Table 3.1 (Panel A) presents the descriptive statistics of Bitcoin prices over the 90-day period before and after the KuCoin exchange heist. The results show that following the incident, the standard deviation increased from 1,040.61 to 3,827.55, indicating a significant rise in price volatility and heightened market uncertainty. The results of the Jarque–Bera (JB) and Augmented Dickey–Fuller (ADF) tests further confirm that Bitcoin prices exhibit non-normality and non-stationarity. Similarly, Table 3.1 (Panel B) provides the descriptive statistics for the CFGI over the same time frame. Its standard deviation increased from 17.17 to 18.73, suggesting greater fluctuations in investor sentiment following the KuCoin exchange heist. The JB and ADF tests also indicate that the CFGI is non-normally distributed and non-stationary.

Overall, the descriptive statistics for Bitcoin prices and CFGI reveal a similar pattern: a notable increase in volatility following the KuCoin exchange heist. This preliminary evidence

[3] Bitcoin price refers to the current global volume-weighted average price of Bitcoin traded on an active crypto asset exchange as tracked by CoinGecko. This closing price should be representative of the entire Bitcoin market.

suggests that extreme incidents may simultaneously intensify market uncertainty and investor sentiment fluctuations, laying the groundwork for further analysis of the dynamic relationship between Bitcoin price and market sentiment.

Table 3.1: Descriptive statistics of BP (Panel A) and CFGI (Panel B)

Data Range	Obs	Mean	S.Dev.	Skew	Kurt	JB	ADF
27/06/2020–24/09/2020	90	10532.16	1040.61	-0.13	-1.55	8.85**	-0.93
25/09/2020–23/12/2020	90	15423.10	3827.55	0.35	-0.96	5.00*	-2.41
Data Range	**Obs**	**Mean**	**S.Dev.**	**Skew**	**Kurt**	**JB**	**ADF**
27/06/2020–24/09/2020	90	57.92	17.17	0.23	-1.78	12.57***	-0.93
25/09/2020–23/12/2020	90	75.01	18.73	-0.57	-1.29	10.84***	-1.32

The Bitcoin price (BP) data is sourced from CoinGecko, while the CFGI data is obtained from Alternative.me; **Skew:** Skewness, it is a measure of symmetry; **Kurt:** Kurtosis, it is a measure of whether the data are heavy-tailed or light-tailed relative to a normal distribution; **JB:** Jarque–Bera test; **ADF:** Augmented Dickey–Fuller test; *** At the 1% significance level; ** At the 5% significance level; * At the 10% significance level

3.3.2 Bootstrap Full-Sample Granger Causality Test

This chapter first uses the Granger causality test to explore the bidirectional predictive relationship between Bitcoin price and CFGI (Granger, 1969). This test, grounded in the Vector Autoregression (VAR) model, assesses the causal relationship between two time series. Unlike conventional models based on economic principles, the VAR model is empirical, comprising multiple equations. Each equation links the endogenous variable to its lagged terms and those of other endogenous variables, enabling the estimation of dynamic relationships among them. Unlike single-variable autoregressive models, the VAR model captures interactions between multiple variables, improving analysis and prediction accuracy. It avoids a priori assumptions and specific functional forms, estimating parameters directly from data. This flexibility makes it adaptable to various situations (Sims, 1980).

Compared to the simple correlation analyses, which only capture the degree of association between variables, the Granger causality framework allows for testing whether one time series has predictive power over another in a temporal context. This is especially important when studying the interaction between sentiment and price, where feedback effects may exist and unfold over time. Since Bitcoin price and CFGI are time-dependent variables, the VAR-based Granger causality test captures the dynamic lagged interactions between them without requiring strict theoretical assumptions about their structural relationship. Moreover, it enables the analysis of whether the causal direction between price and sentiment changes under different market conditions, such as before and after a heist. These characteristics make

Granger causality testing a robust and flexible method for capturing the evolving nature of sentiment-price interactions in the cryptocurrency market.

The Granger causality test assumes that all the predictive information about the variable, Y_{1t} and variable Y_{2t} is contained within their respective time series. The bivariate VAR(p) can be represented as follows:

$$\begin{aligned} Y_{1t} &= C_{1,0} + \sum_{p=1}^{p} A_{1,1}(p) Y_{1,t-p} + \sum_{p=1}^{p} A_{1,2}(p) Y_{2,t-p} + \varepsilon_{1t} \\ Y_{2t} &= C_{2,0} + \sum_{p=1}^{p} A_{2,1}(p) Y_{1,t-p} + \sum_{p=1}^{p} A_{2,2}(p) Y_{2,t-p} + \varepsilon_{2t} \end{aligned} \tag{9}$$

where $Y_{1,t-p}$ and $Y_{2,t-p}$ are lagged time series, determined by information criteria. ε_{1t} and ε_{2t} are two uncorrelated white-noise series. If $A_{1,2}(p)$ is not statistically equal to 0, Y_{2t} is causing Y_{1t}. Similarly, if $A_{2,1}(p)$ is not statistically equal to 0, Y_{1t} is causing Y_{2t}. If both $A_{1,2}(p)$ and $A_{2,1}(p)$ are statistically nonzero, it indicates a feedback relationship between Y_{1t} and Y_{2t}, which can be referred to as bidirectional causality. In this chapter, Y_{1t} and Y_{2t} represent Bitcoin price (BP) and CFGI, respectively. Therefore, Equation (9) can be rewritten in the following form:

$$\begin{aligned} BP &= C_{1,0} + \sum_{p=1}^{p} A_{1,1}(p) BP_{t-p} + \sum_{p=1}^{p} A_{1,2}(p) CFGI_{t-p} + \varepsilon_{1t} \\ CFGI &= C_{2,0} + \sum_{p=1}^{p} A_{2,1}(p) BP_{t-p} + \sum_{p=1}^{p} A_{2,2}(p) CFGI_{t-p} + \varepsilon_{2t} \end{aligned} \tag{10}$$

Given the limited sample size in this study, relying solely on the traditional Granger causality test may result in biased estimates, particularly under small-sample conditions. To improve the accuracy and robustness of the results, this chapter adopts the Bootstrap full-sample Granger causality test as an extension of the traditional Granger framework. This method enhances inference by repeatedly resampling from the original dataset to construct the empirical distribution of the test statistics, thereby allowing for more precise significance testing without relying on strict distributional assumptions. Even with relatively small samples, the Bootstrap approach can extract more information from the data and mitigate the limitations of traditional Granger causality tests (Balcilar et al., 2010). Therefore, it serves as

a more reliable method for capturing shifts in the causal relationship between price and sentiment around extreme incidents.

3.3.3 Parameter Stability Test

In the full-sample Granger causality test, it is typically assumed that the parameters of the VAR model remain constant over time. However, this assumption may be violated if the underlying full-sample time series undergoes structural changes, rendering the results of the full-sample Granger causality test invalid. Therefore, this chapter examines the stability of short-term and long-term parameters. This chapter employs the *Sup-F*, *Ave-F*, and *Exp-F* tests developed by Andrews (1993) and Andrews and Ploberger (1994) to assess the short-term stability of the VAR model parameters and identify potential structural changes. Additionally, it also applies the *Lc* test proposed by Nyblom (1989) and Hansen (1992) to evaluate the long-term stability of all parameters within the VAR system.

The *Sup-F* statistic for testing the null hypothesis of no structural change in k coefficients is given by

$$\text{Supremum } S_T = \sup_{b_1 \le b \le b_2} S_T(b) \tag{11}$$

where b is the potential break date in the range $[b_1, b_2]$ for a sample size T. $S_T(b)$ is the Wald or Likelihood Ratio test (LR test) statistic evaluated at a potential break date b. The *Ave-F* and *Exp-F* tests statistic are

$$\text{Average } S_T = \frac{1}{b_2 - b_1 + 1} \sum_{b=b_1}^{b_2} S_T(b) \tag{12}$$

$$\text{Exponential } S_T = \ln\left[\frac{1}{b_2 - b_1 + 1} \sum_{b=b_1}^{b_2} \exp\left\{\frac{1}{2} S_T(b)\right\}\right] \tag{13}$$

The limiting distributions of the test statistics are given by

$$\begin{aligned} &\text{Supremum } S_T \to_d \sup_{\lambda \in [\varepsilon_1, \varepsilon_2]} S(\lambda) \\ &\text{Average } S_T \to_d \frac{1}{\varepsilon_2 - \varepsilon_1} \int_{\varepsilon_1}^{\varepsilon_2} S(\lambda) d\lambda \\ &\text{Exponential } S_T \to_d \ln\left[\frac{1}{\varepsilon_2 - \varepsilon_1} \int_{\varepsilon_1}^{\varepsilon_2} \exp\left\{\frac{1}{2} S(\lambda) d\lambda\right\}\right] \end{aligned} \tag{14}$$

where

$$S(\lambda) = \frac{\{B_k(\lambda) - \lambda B_k(1)\}'\{B_k(\lambda) - \lambda B_k(1)\}}{\lambda(1-\lambda)} \tag{15}$$

$B_k(\lambda)$ is a vector of k-dimensional independent Brownian motions, $\varepsilon_1 = b_1/T$, $\varepsilon_2 = b_2/T$, and $\lambda = \varepsilon_2(1-\varepsilon_1)/\{\varepsilon_1(1-\varepsilon_2)\}$.

Following Andrews (1993), this chapter trims 15% from both sides of the sample when conducting structural break tests, restricting the evaluation interval to (0.15, 0.85) fraction of the data. The full interval (0, 1) is not desirable because the *Sup-F* statistic diverges when the change point is near the sample boundaries. As Andrews (1993) notes, using the unrestricted interval results in a loss of power due to the divergence of the test statistics near zero or one. By restricting the interval, the *Sup-F* statistic converges in distribution and maintains higher power for detecting change points occurring within the central portion of the sample. Therefore, trimming improves the test's robustness and statistical reliability when the location of the change point is unknown. The p-values are generated using the bootstrap method with 1000 repetitions.

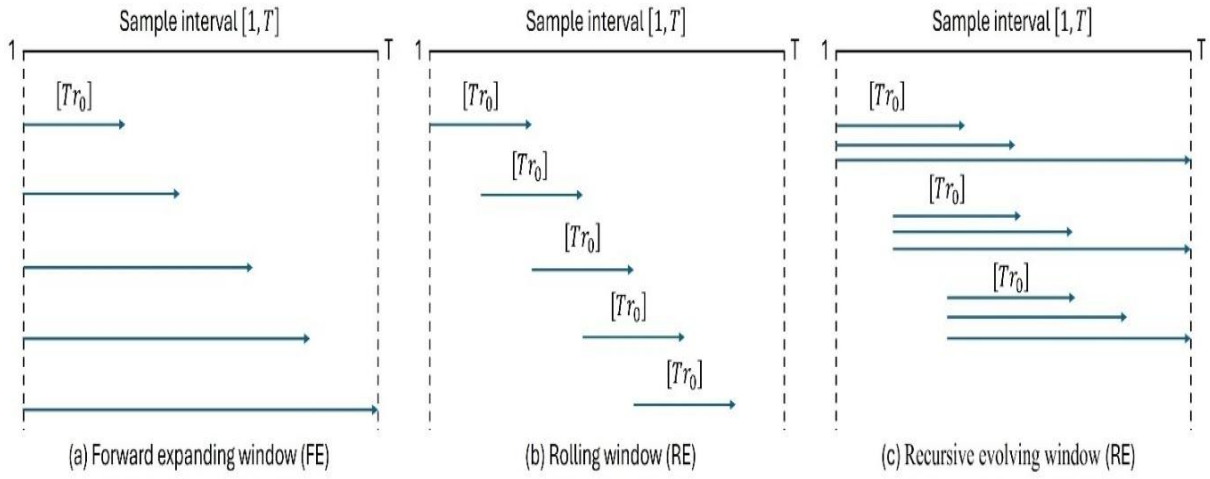
3.3.4 Time-Varying Granger Causality Test

If the parameters of the VAR model are unstable, this suggests that Granger causality may vary over time. To address this, recursive estimation methods are required to detect the potential time-varying nature of Granger causality (Thoma, 1994; Swanson, 1998; Baum et al., 2021). Baum et al. (2021) summarised three algorithms to generate sequences of Granger causality test statistics across different periods: forward expanding window (*FE*), rolling window (*RO*), and recursive evolving window (*RE*) algorithms. Figure 3.2 illustrates the workflows of these algorithms, where each arrow represents a possible subsample for calculating the relevant test statistics.

Suppose $\{y_0, y_1, y_2, \cdots, y_T\}$ is a sample with $T+1$ observations, and a number r which satisfies $0 < r < 1$. $[T_r]$ represents the integer part of the product. $\mathcal{T}_{r_1,r}$ will be used to represent the Wald test statistic computed on the subsample starting at $y_{[Tr_1]}$ and ending at $y_{[Tr]}$. The *FE* algorithm (Thoma, 1994) is a standard forward recursive approach. After determining the minimum window length Tr_0, the sample size is gradually expanded. In this recursive process, each subsample always starts from the first data point and progressively extends until the entire sample is used to calculate the final test statistic. This method can

capture the cumulative changes of long-term trends and causal relationships, but because the window continues to expand and the amount of data included gradually increases, the *FE* method is not sensitive to short-term fluctuations, and the results are usually smoother. The *RO* algorithm (Swanson, 1998; Arora & Shi, 2016) generates new windows by rolling forward one observation at a time and calculates the Wald test statistic for each window. Since only fixed-length data is used, the *RO* method is very sensitive to short-term changes and fluctuations, but its results are easily affected by the window size, and it is difficult to capture long-term trends or cumulative effects. In the *RE* algorithm, each observation is used as an endpoint for calculating a test statistic for all possible subsamples of size r_0 or larger. This process is repeated for every data point in the sample, except for the first one, while adhering to the minimum window size requirement. Consequently, a collection of Wald test statistics is generated for each observation beyond the initial data point (Phillips et al.,2015b). The *RE* algorithm combines the features of the *FE* and *RO* algorithms, taking into account both short-term dynamics and long-term trends and has a greater capacity to detect temporal instabilities (Baum et al., 2021).

Figure 3.2: Three different algorithms to generate Granger causality test statistic series for different periods



Source: Phillips et al. (2015a); Baum et al. (2021)

3.3.5 TVP-VAR-Based Connectedness Approach

This chapter also uses the extended TVP-VAR method proposed by Diebold and Yilmaz (2009, 2012) to investigate whether the volatility of CFGI spilt over into other cryptocurrency markets during the KuCoin exchange heist. This method not only addresses the potential

issue of results being dependent on lag selection caused by Cholesky factor orthogonalization (Diebold and Yilmaz, 2009), but also allows for the characterisation of both the direction and the dynamic evolution of volatility spillovers. These features could help us identify shock transmission channels and risk contagion mechanisms during extreme events. Furthermore, due to its ease of implementation and strong adaptability, this method has been widely adopted in the study of volatility spillovers across financial markets (Yarovaya et al., 2016; Yi et al., 2018; Mensi et al., 2021; Elsayed et al., 2022).

An N-variable TVP-VAR process with stationary covariance, as shown in Equation (16):

$$y_t = \Phi_{0,t} + \Phi_{1,t} y_{t-1} + \Phi_{2,t} y_{t-2} + \cdots + \Phi_{p,t} y_{t-p} + \varepsilon_t \tag{16}$$

where y_t is an N-dimensional column vector representing the volatility of N financial time series, each of which follows a covariance stationary process. ε_t is an N-dimensional disturbance vector with no serial correlation, where each component of ε_t is independent and identically distributed, following $\varepsilon_t \sim N(0, \Sigma_t)$, where Σ_t represents the covariance matrix. $\Phi_{0,t}$ is a $N \times 1$-dimensional intercept vector, and $\Phi_{1,t}$, $\Phi_{2,t}$, ⋯, $\Phi_{p,t}$ are $N \times N$-dimensional time-varying lag coefficient matrices.

If we define $\beta_t = \text{vecr}\left(\Phi'_{0,t}, \Phi'_{1,t}, \Phi'_{2,t}, \cdots, \Phi'_{p,t}\right)$, where $vecr(\cdot)$ denotes the column stacking operator, then assuming the coefficient vector β_t follows a random walk process of AR(1):

$$\beta_t = \beta_{t-1} + v_t \tag{17}$$

The disturbance term v_t is a time-invariant, independently and identically distributed (*i.i.d.*) Gaussian white noise process. Solving the above TVP-VAR model to get the posterior estimated coefficient $\hat{\beta}_t$, and rearranging to get the coefficient matrix $\widehat{\Phi}_{1,t}, \widehat{\Phi}_{2,t}, \cdots, \widehat{\Phi}_{p,t}$, we can use the following recurrence relation:

$$A_{h,t} = \widehat{\Phi}_{1,t} A_{h-1,t} + \widehat{\Phi}_{2,t} A_{h-2,t} + \cdots + \widehat{\Phi}_{p,t} A_{h-p,t} \tag{18}$$

The coefficient matrix $A_{h,t}$ associated with the TVP-VMA(∞) model can be calculated. Next, the H-step ahead Generalised Forecast Error Variance Decomposition (GFEVD) given by Koop et al. (1996) and Pesaran and Shin (1998) is defined as follows:

$$d_{ij,t}(H) = \frac{\sigma_{jj,t}^{-1} \sum_{h=0}^{H-1} \left(e_i' A_{h,t} \sum_t e_j\right)^2}{\sum_{h=0}^{H-1} \left(e_i' A_{h,t} \sum_t A_{h,t}' e_i\right)}, i, j = 1,2,\cdots,N \tag{19}$$

where $d_{ij,t}(H)$ represents the contribution of the j-th variable to the forecast error variance of the i-th variable at horizon H. $\sum_t$ represents the variance matrix of the vector of errors. σ_{jj} is denotes the j-th diagonal element of the $\sum$ matrix, and e_i is a vector with a value of one in the i-th position and zero otherwise.

To maintain consistency with the economic interpretation of traditional variance decomposition, the variance decomposition results are typically row-standardised.

$$\tilde{d}_{ij,t}(H) = \frac{d_{ij,t}}{\sum_{j=1}^{N} d_{ij,t}} \tag{20}$$

The total directional spillover index (*SI*) from variable i to variables j is:

$$TO = SI_{i \to j} = \frac{\sum_{j=1, i \neq j}^{N} \tilde{d}_{ji,t}}{\sum_{j=1}^{N} \tilde{d}_{ji,t}} \times 100 \tag{21}$$

The total directional spillover index (*SI*) from variables j to variable i is:

$$FROM = SI_{i \leftarrow j} = \frac{\sum_{j=1, i \neq j}^{N} \tilde{d}_{ij,t}}{\sum_{j=1}^{N} \tilde{d}_{ij,t}} \times 100 \tag{22}$$

The net total directional spillover (*NSI*) index is:

$$NET = NSI = SI_{i \to j} - SI_{i \leftarrow j} = TO - FROM \tag{23}$$

A positive value indicates that the variable is a net transmitter of volatility, whereas a negative value indicates that the variable is a net receiver of volatility.

The total connectivity index (*TCI*) among the variables is:

$$TCI = \frac{\sum_{i=1}^{N} \sum_{j=1, i \neq j}^{N} \tilde{d}_{ij,t}}{\sum_{i=1}^{N} \sum_{j=1,}^{N} \tilde{d}_{ij,t}} \times 100 \tag{24}$$

3.4 Empirical Results

3.4.1 Stationarity, Cointegration, and Stability Tests

Since Bitcoin price and CFGI are non-stationary series, differencing is required to make them stationary. Table 3.2 presents the statistical results from three linear unit root tests, namely the Augmented Dickey–Fuller (ADF) test, the Phillips–Perron (PP) test, and the Kwiatkowski–Phillips–Schmidt–Shin (KPSS) test, as well as one nonlinear unit root test, the Kapetanios–

Shin–Shell (KSS) test. After first-order differencing, the ADF, PP, and KSS tests reject the null hypothesis of a unit root and indicate that the series are stationary. At the same time, the KPSS test could not reject the null hypothesis of stationarity. Therefore, after the first-order difference, the Bitcoin price and CFGI become stationary series.

Table 3.2: Unit root tests (ADF, PP and KPSS) for BP and CFGI

	Before the heist (27/06/2020–24/09/2020)		**After the heist (25/09/2020–23/12/2020)**	
Unit root test	**BP**	**CFGI**	**BP**	**CFGI**
ADF	-10.577***	-10.045***	-8.482***	-13.254***
PP	-10.567***	-10.047***	-8.482***	-13.892***
KPSS	0.270	0.256	0.175	0.137
KSS	-4.744***	-4.192***	-3.670***	-3.507***

ADF: Augmented Dickey–Fuller test; **PP:** Phillips–Perron test; **KPSS:** Kwiatkowski–Phillips–Schmidt–Shin test; **KSS:** Kapetanios–Shin–Shell test; *** At the 1% significance level

Next, since the original series are non-stationary I(1) processes (each series itself is non-stationary, but its first-order difference is stationary), it is necessary to conduct cointegration tests to determine whether a long-term equilibrium relationship exists between them. If no cointegration is found, the series are differenced, and a VAR model is then constructed on the stationary series. In line with Johansen's (1988, 1991) methodology, the optimal lag length is first determined using the original (non-differenced) data. Table 3.3 shows that, based on the results of the Akaike Information Criterion (AIC), the Hannan–Quinn Criterion (HQ), the Schwarz Bayesian Information Criterion (SIC), and the Final Prediction Error (FPE), the optimal lag length between Bitcoin price and CFGI is 2, both before and after the KuCoin exchange heist.

Table 3.3: Lag order selection criteria

Panel A: Before the heist (27/06/2020–24/09/2020)								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
AIC	19.578	19.473*	19.482	19.555	19.611	19.576	19.561	19.653
HQ	19.649	19.591*	19.647	19.767	19.870	19.882	19.914	20.054
SIC	19.754*	19.766	19.893	20.083	20.256	20.339	20.441	20.651
FPE	1091096	982064.500*	991314.500	1067430	1130338	1094064	1081044	1189943
Panel B: After the heist (25/09/2020–23/12/2020)								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
AIC	20.918	20.839*	20.869	20.950	21.002	21.059	21.078	21.134
HQ	20.989	20.956*	21.034	21.162	21.261	21.365	21.431	21.534
SIC	21.094*	21.132	21.280	21.479	21.647	21.821	21.958	22.132
FPE	4166238	3848284*	3968362	4309626	4543618	4819291	4927004	5231672

AIC: Akaike Information Criterion; **HQ:** Hannan-Quinn Criterion; **SIC:** Schwarz Bayesian Information Criterion; **FPE:** Final Prediction Error; * Indicates lag order selected by the criterion

Table 3.4 reports the results of the Johansen cointegration trace test before and after the KuCoin exchange heist. Panel A shows that, for the pre-heist period, the null hypothesis of no cointegration (rank = 0) cannot be rejected, as the trace statistic (6.443) is below the 5% critical value (15.410). Similarly, for the post-heist period reported in Panel B, the null hypothesis of no cointegration is also not rejected, with a trace statistic of 4.775 compared with the 5% critical value of 15.410. These results suggest that Bitcoin price and CFGI do not share a long-term equilibrium relationship, either before or after the KuCoin exchange heist. Consequently, the analysis proceeds with a VAR model based on the first-differenced stationary series to capture short-run dynamics.

Table 3.4: Johansen cointegration test results for BP and CFGI before and after the KuCoin exchange heist

Panel A: Before the heist (27/06/2020–24/09/2020)					
Maximum rank	**Params**	**Log likelihood**	**Eigenvalue**	**Trace statistic**	**Critical value at 5%**
0	6	-843.997		6.443*	15.410
1	9	-842.053	0.043	2.555	3.760
2	10	-840.776	0.029		
Panel B: After the heist (25/09/2020–23/12/2020)					
Maximum rank	**Params**	**Log likelihood**	**Eigenvalue**	**Trace statistic**	**Critical value at 5%**
0	6	-906.614		4.775*	15.410
1	9	-904.261	0.052	0.069	3.760
2	10	-904.226	0.001		

* Selected rank

Building on the previous tests, this chapter employs the Bootstrap full-sample Granger causality test to examine the relationship between Bitcoin price and CFGI. Table 3.5 shows that, based on the first-order differenced series, the optimal lag length between Bitcoin price and CFGI is 1, both before and after the KuCoin exchange heist. This result provides the basis for constructing the VAR model. Before the KuCoin exchange heist, the results in Table 3.6 (Panel A) indicate no statistically significant bidirectional predictive relationship between Bitcoin price and CFGI. This implies that the Bitcoin price did not influence CFGI, and CFGI did not affect the Bitcoin price. However, after the KuCoin exchange heist, the results in Table 3.6 (Panel B) reveal a statistically significant bidirectional predictive relationship between Bitcoin price and CFGI. During this period, not only did the Bitcoin price influence CFGI, but CFGI also affected the Bitcoin price.

Table 3.5: VAR lag order selection criteria

Panel A: Before the heist (27/06/2020–24/09/2020)								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
AIC	13.837*	13.840	13.910	13.975	13.934	13.904	14.003	14.058
HQ	13.909*	13.960	14.078	14.191	14.198	14.217	14.363	14.466
SIC	14.017*	14.140	14.330	14.515	14.594	14.684	14.903	15.077
FPE	1021473*	1025266	1099814	1174877	1129681	1099571	1217433	1291394
Panel B: After the heist (25/09/2020–23/12/2020)								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
AIC	15.213*	15.229	15.310	15.366	15.421	15.457	15.512	15.531
HQ	15.285*	15.349	15.478	15.582	15.685	15.770	15.872	15.940
SIC	15.393*	15.529	15.730	15.906	16.081	16.237	16.412	16.551
FPE	4043913*	4110612	4461538	4723152	4997791	5196069	5505580	5636148

AIC: Akaike Information Criterion; **HQ:** Hannan–Quinn Criterion; **SIC:** Schwarz Bayesian Information Criterion; **FPE:** Final Prediction Error; ***** Indicates lag order selected by the criterion

Table 3.6: The results of Bootstrap full-sample Granger causality test

Panel A: Before the heist: (27/06/2020–24/09/2020)		
Null hypothesis	**F-Statistics**	**p-value**
BP does not Granger cause CFGI	4.060	0.222
CFGI does not Granger cause BP	0.122	0.713
Panel B: After the heist: (25/09/2020–23/12/2020)		
Null hypothesis	**F-Statistics**	**p-value**
BP does not Granger cause CFGI	2.182	0.037
CFGI does not Granger cause BP	6.555	0.016

p-value is calculated using 1000 bootstrap repetitions

Khalik and Shukur (2004) highlighted that the stability of VAR model parameters significantly impacts Granger causality tests conducted on the full sample. The presence of structural breaks may cause the parameters of the VAR model to be non-constant during full-sample estimation. The parameter stability results in Table 3.7 indicate that the parameters of the Bitcoin price (BP) equation, the CFGI equation, and the overall VAR system are not stable. For instance, before the KuCoin exchange heist (Panel A), the *Sup-F* test results show that the null hypothesis of short-term parameter stability is rejected at the 1% level for the BP equation, the CFGI equation, and the VAR system. The *Exp-F* test results further reveal that the null hypothesis of short-term parameter stability is rejected at the 5% level for the BP equation. After the KuCoin exchange heist (Panel B), the *Sup-F* test results again show that the null hypothesis of short-term parameter stability is rejected at the 1% level for all three equations. Additionally, the *Lc* test results indicate that the null hypothesis of long-term parameter stability for the VAR system is rejected at the 10% level.

Table 3.7: Parameter stability test

Panel A: Before the heist: (27/06/2020–24/09/2020)						
	BP equation		**CFGI equation**		**VAR system**	
	Statistics	**p-value**	**Statistics**	**p-value**	**Statistics**	**p-value**
Sup-F	21.703***	0.000	69.198***	0.001	33.739***	0.001
Ave-F	1.323	0.347	1.535	0.221	2.073	0.329
Exp-F	4.014**	0.049	27.691***	0.006	9.963**	0.021
Lc					0.351	0.915
Panel B: After the heist: (25/09/2020–23/12/2020)						
	BP equation		**CFGI equation**		**VAR system**	
	Statistics	**p-value**	**Statistics**	**p-value**	**Statistics**	**p-value**
Sup-F	9.250***	0.001	9.493***	0.001	14.370***	0.001
Ave-F	1.398	0.363	1.395	0.370	2.172	0.363
Exp-F	1.050	0.502	0.995	0.542	2.281	0.341
Lc					2.627*	0.072

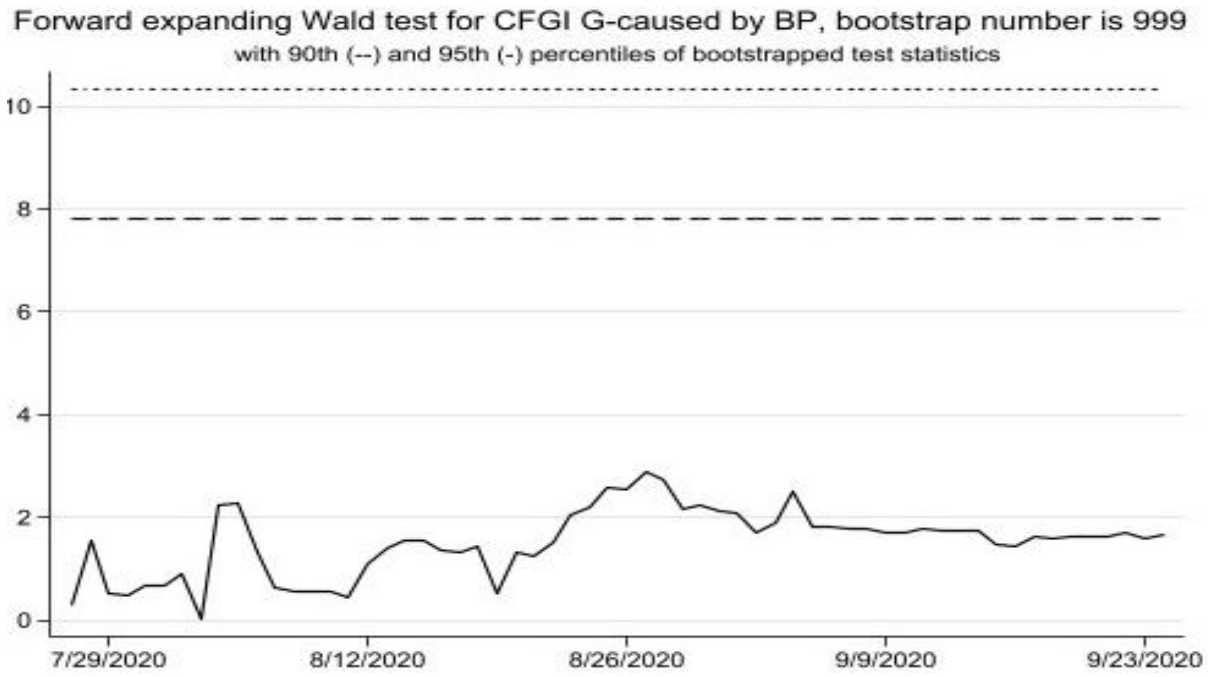
∗∗∗ At the 1% significance level; ∗∗ At the 5% significance level; ∗ At the 10% significance level; p-value is calculated using 1000 bootstrap repetitions

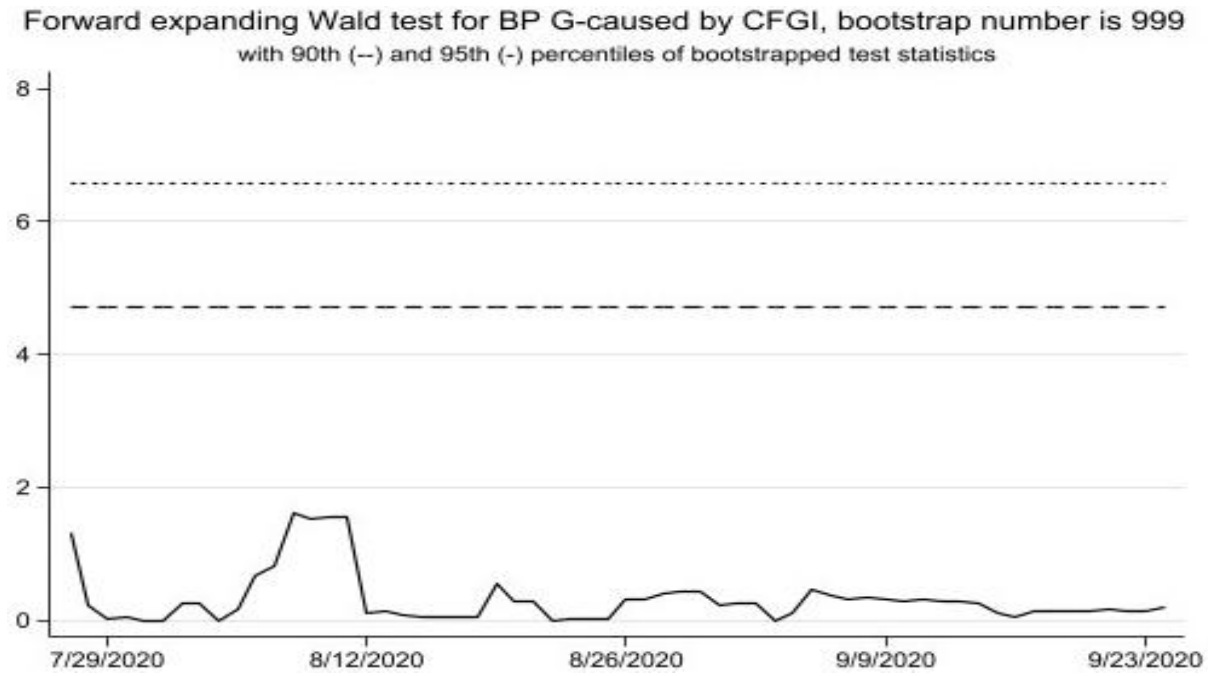
Given the potential presence of structural changes, traditional Granger causality tests may not be suitable. Therefore, this chapter employs time-varying Granger causality tests to examine the dynamic predictive relationship between Bitcoin price and CFGI. The main analysis adopts a rolling window size of 30 and 999 bootstrap repetitions.

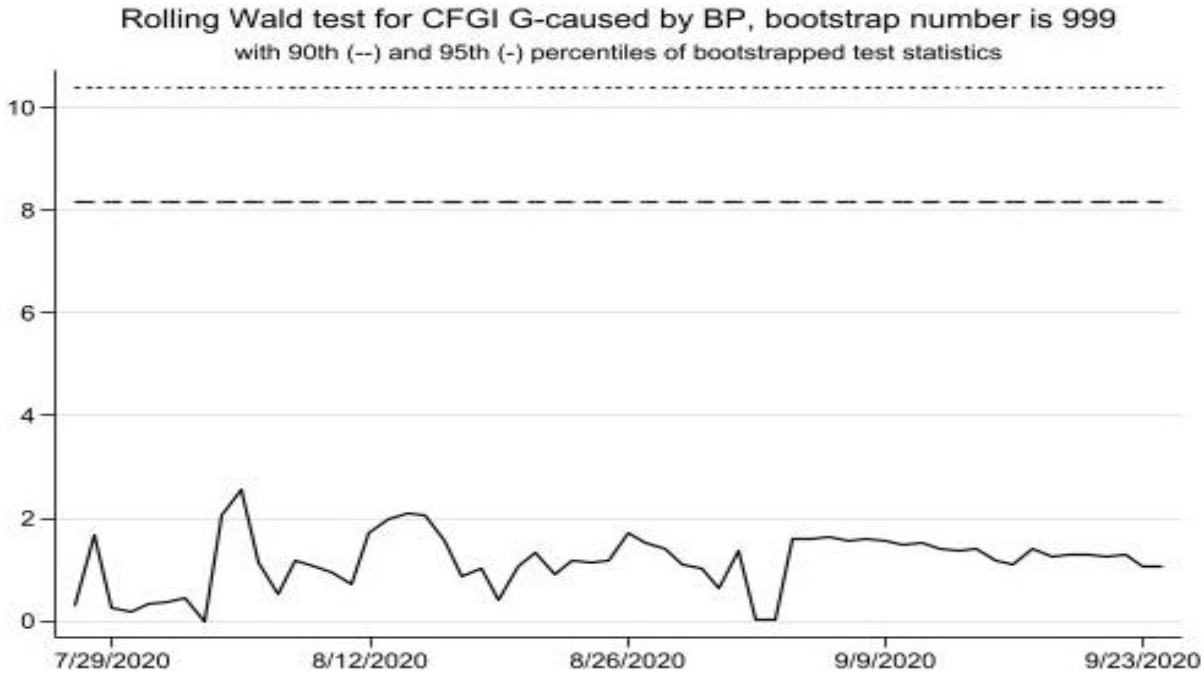
3.4.2 Time-Varying Granger Causality Test Results

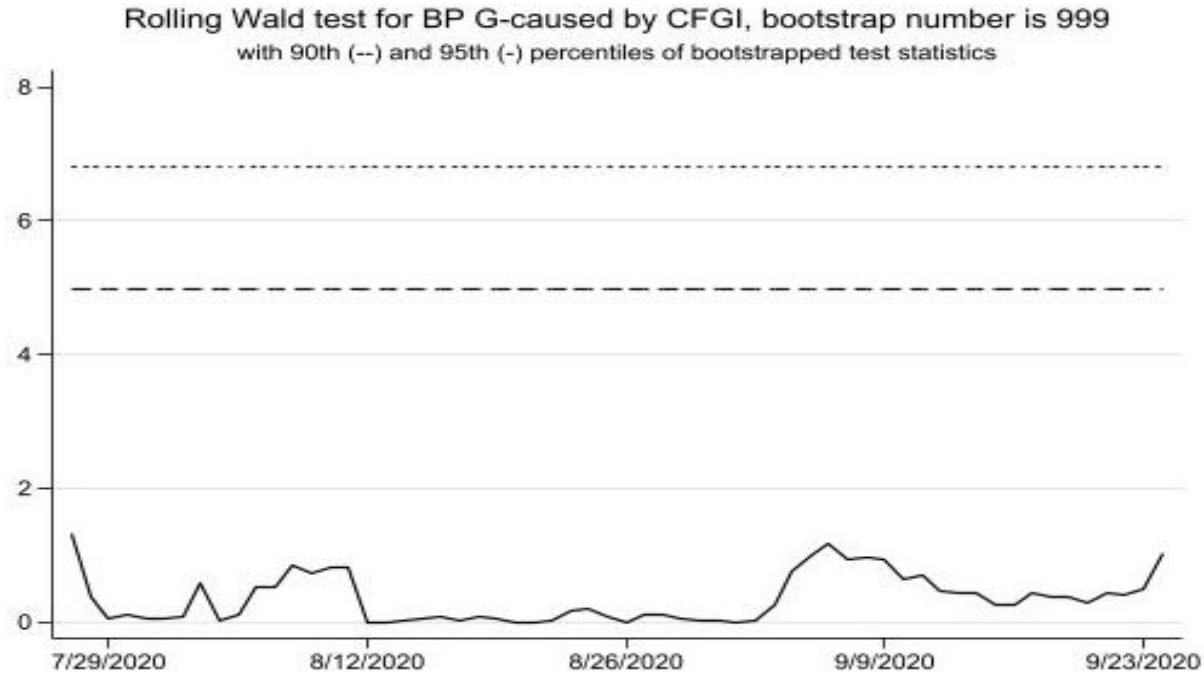
Figure 3.3 illustrates the time-varying Granger causality between Bitcoin price and CFGI before the KuCoin exchange heist. The null hypotheses are that Bitcoin price does not Granger cause CFGI and that CFGI does not Granger cause Bitcoin price, respectively. The Wald statistics used in all algorithms are robust to heteroskedasticity. The results from all three algorithms consistently indicate that no statistically significant bidirectional predictive relationship exists between Bitcoin price and CFGI, whether in short-term dynamics or long-term trends. This absence of causality suggests that, before the KuCoin exchange heist, there is no meaningful feedback loop between investor sentiment, as measured by CFGI, and Bitcoin price movements. In other words, shifts in CFGI do not significantly anticipate or drive changes in Bitcoin price, and likewise, fluctuations in Bitcoin price do not exert a substantial influence on the sentiment captured by CFGI. These findings imply that during relatively stable market conditions, the predictive relationship between sentiment and price remains weak, reflecting the limited informational role of CFGI in predicting Bitcoin price dynamics in the absence of extreme external shocks.

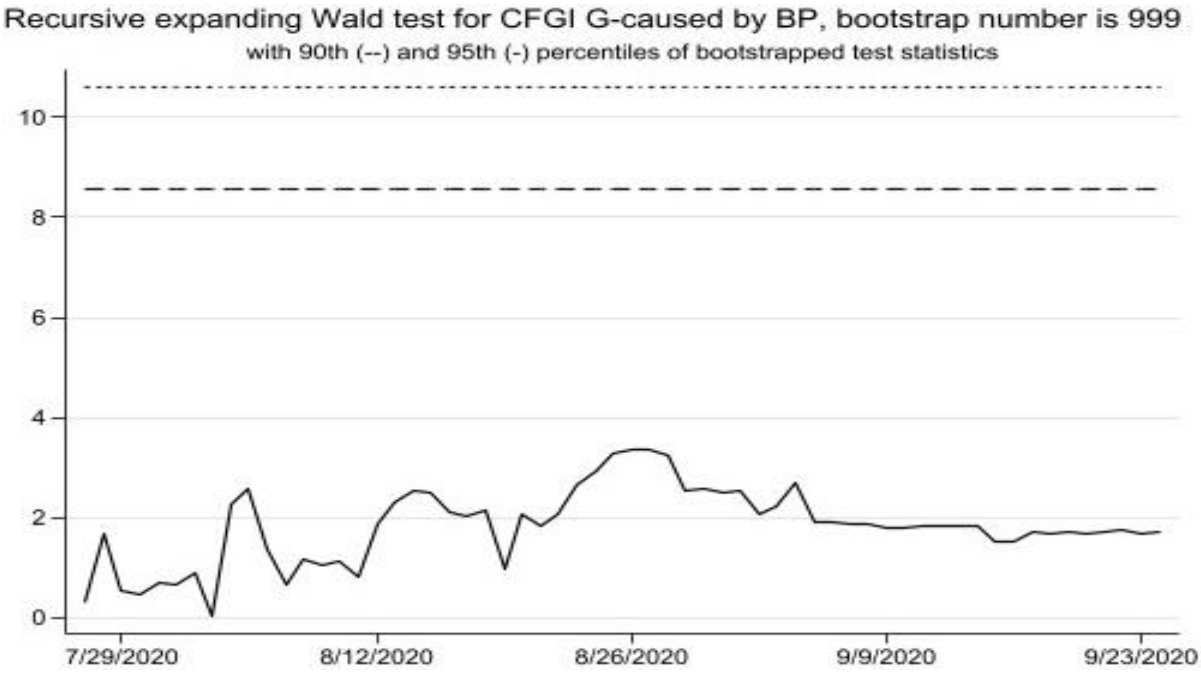
Figure 3.3: Time-varying Granger causality test results before the KuCoin exchange heist (window size = 30, using 30% of the sample, with 999 bootstrap repetitions)

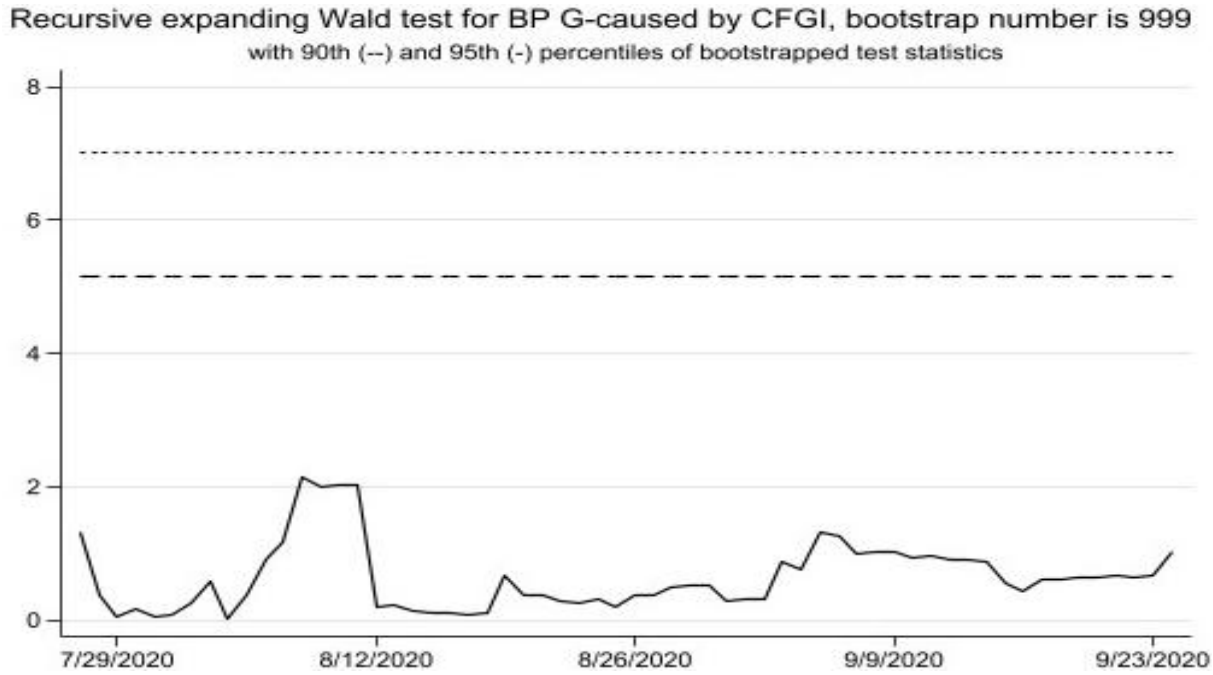





Rolling Wald test for CFGI G-caused by BP, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
0
7/29/2020
8/12/2020
8/26/2020
9/9/2020
9/23/2020


Rolling Wald test for BP G-caused by CFGI, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
7/29/2020
8/12/2020
8/26/2020
9/9/2020
9/23/2020



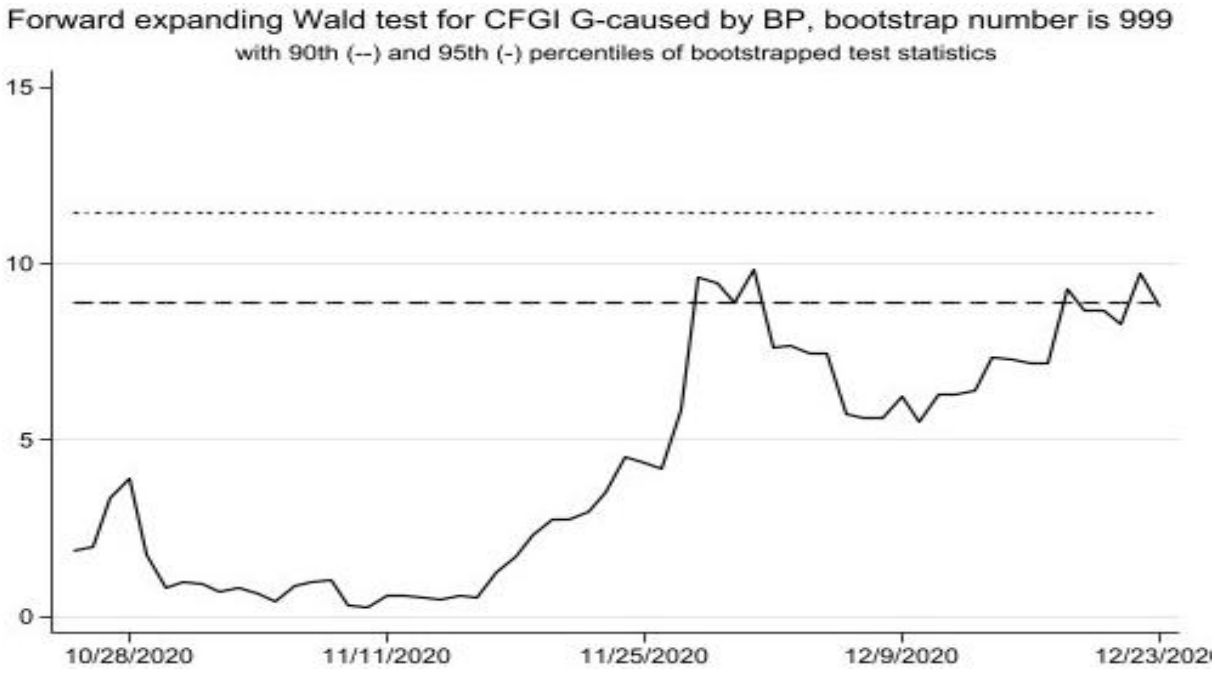


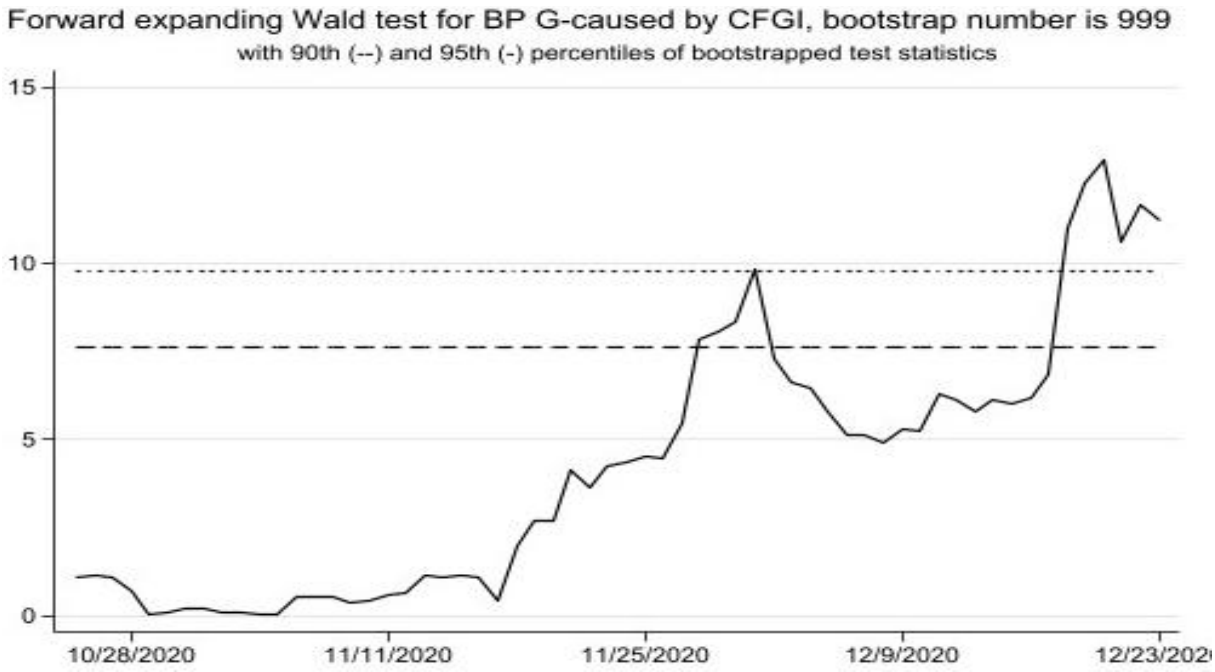
The rolling window size is 30, and the bootstrap repetition is 999. The dashed line represents the 95th percentile of the bootstrapped test statistics, while the dotted line corresponds to the 90th percentile. When the test statistic exceeds these critical values, the null hypothesis is rejected at the corresponding significance level, indicating that Bitcoin price Granger causes CFGI (or CFGI Granger causes Bitcoin price) during those periods.

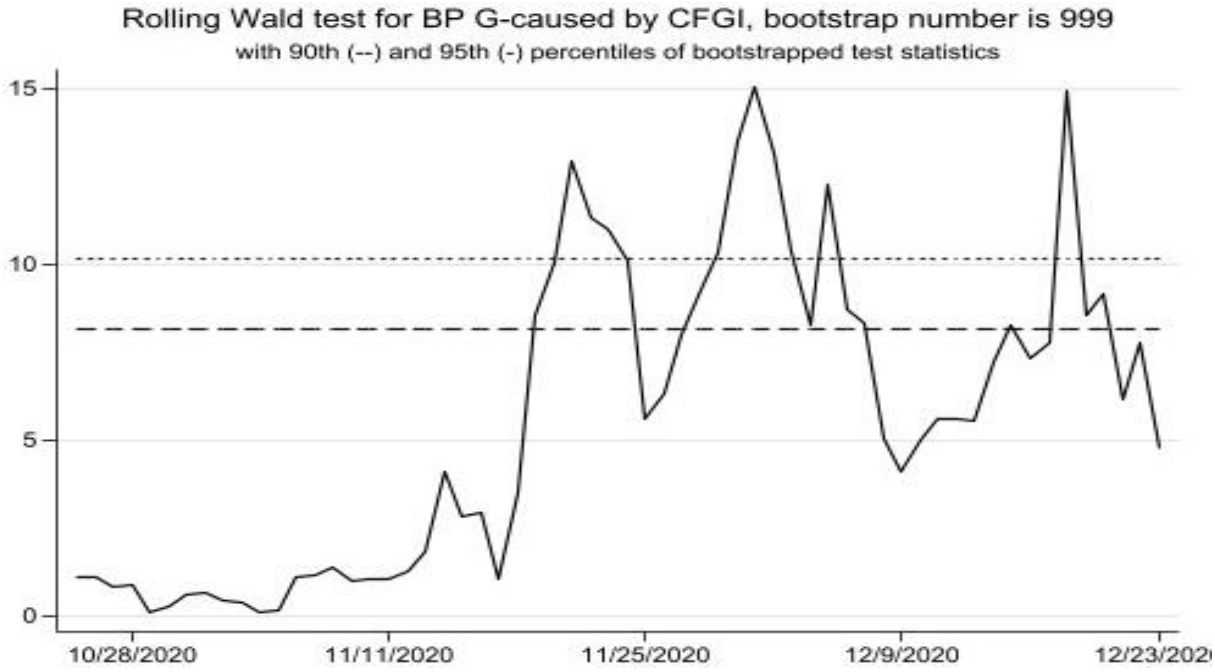
Figure 3.4 illustrates the time-varying Granger causality between Bitcoin price and CFGI after the KuCoin exchange heist. The *FE* algorithm reveals that while Bitcoin price and CFGI do not consistently influence each other in the long term, the Wald statistics exhibit a smooth and gradually increasing trend. This indicates that the influence of Bitcoin price on CFGI and vice versa has been slowly strengthening over the entire time horizon. Meanwhile, the *RO*

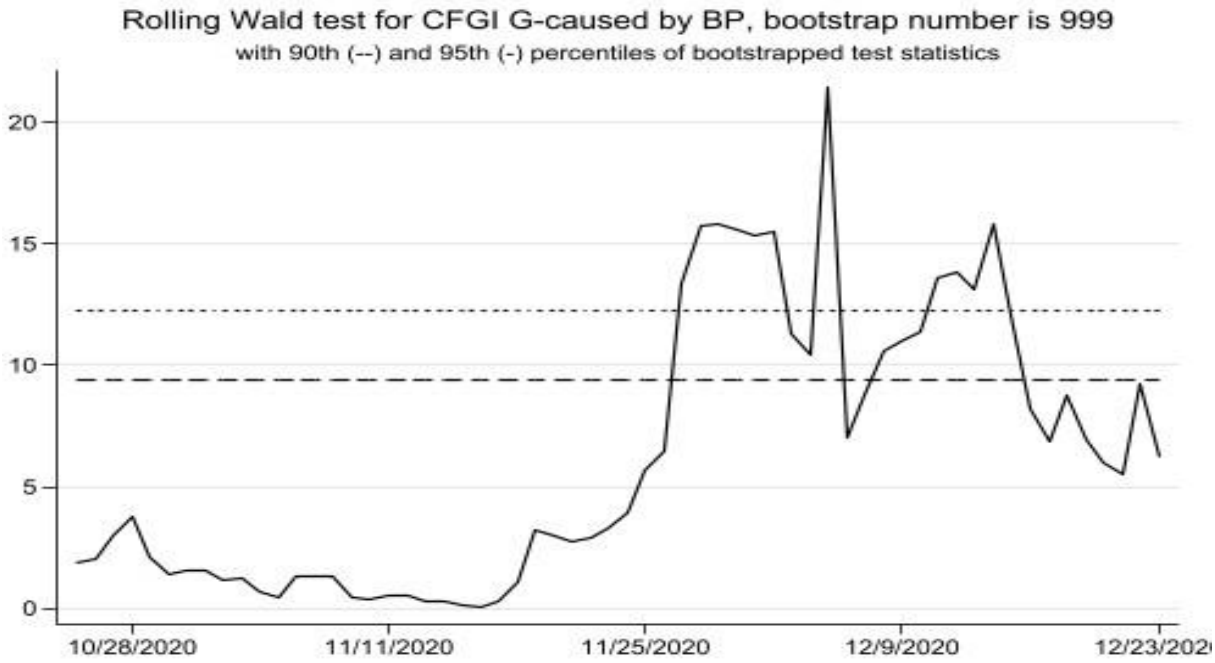
and *RE* algorithms reveal statistically significant bidirectional predictive relationship between Bitcoin price and CFGI across most of the sample period. In summary, the *RO* and *RE* algorithm results support the existence of statistically significant bidirectional predictive relationship between Bitcoin price and CFGI after the KuCoin exchange heist.

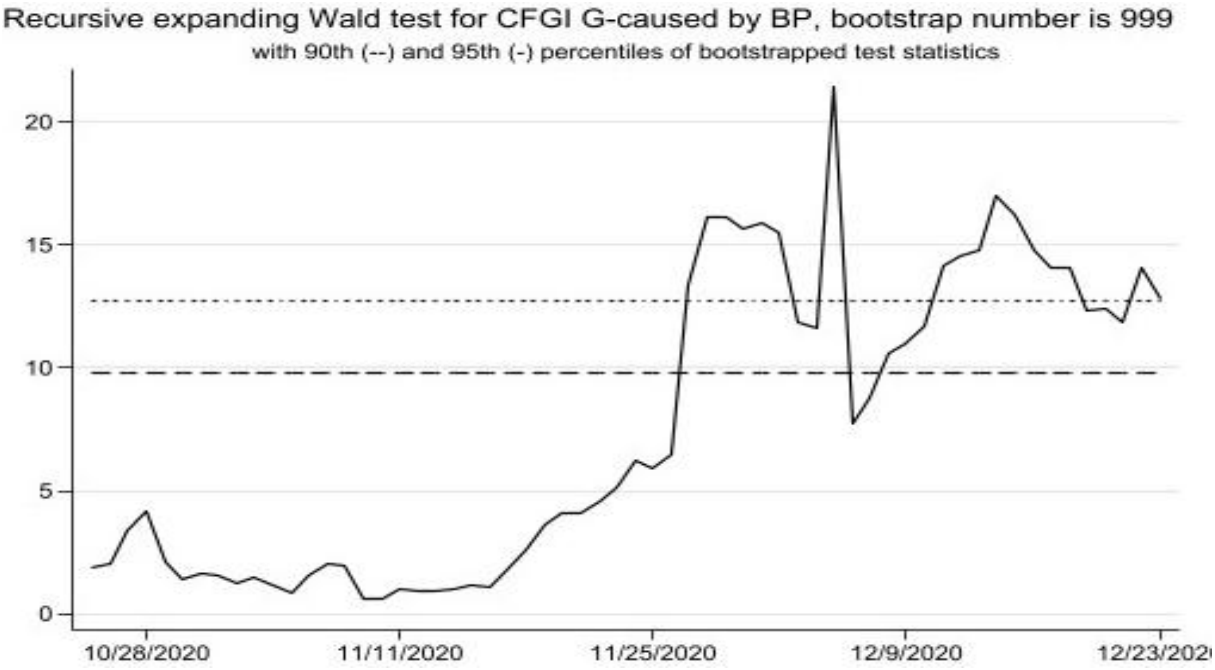
Figure 3.4: Time-varying Granger causality test results after the KuCoin exchange heist (window size = 30, using 30% of the sample, with 999 bootstrap repetitions)

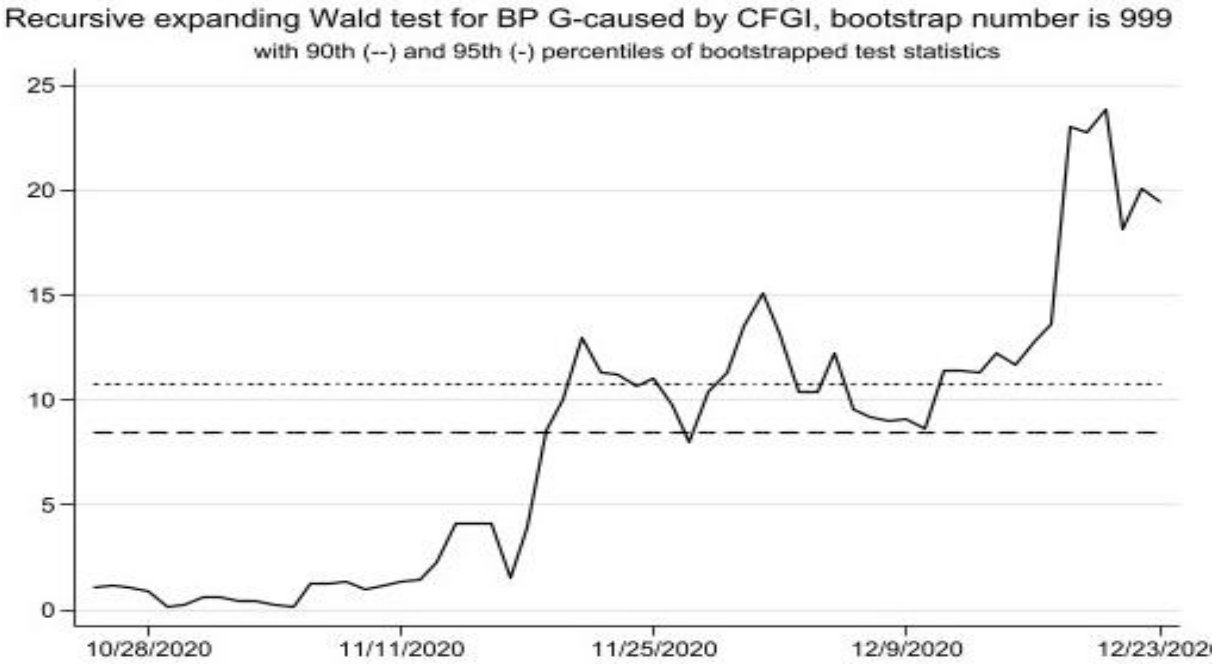





Rolling Wald test for BP G-caused by CFGI, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
15
10
5
0
10/28/2020
11/11/2020
11/25/2020
12/9/2020


Rolling Wald test for CFGI G-caused by BP, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
20
15
10
5
0
10/28/2020
11/11/2020
11/25/2020
12/9/2020





The rolling window size is 30, and the bootstrap repetition is 999. The dashed line represents the 95th percentile of the bootstrapped test statistics, while the dotted line corresponds to the 90th percentile. When the test statistic exceeds these critical values, the null hypothesis is rejected at the corresponding significance level, indicating that Bitcoin price Granger causes CFGI (or CFGI Granger causes Bitcoin price) during those periods.

The fluctuating predictive relationship between Bitcoin price and sentiment before and after the KuCoin exchange heist may be attributed to structural market changes triggered by the incident. Cryptocurrency heists are typically unforeseen incidents that generate significant market uncertainty. In such situations, investors often become apprehensive about future market trends, leading to shifts in behaviour. These behavioural changes can cause market

price fluctuations, as suggested by Shiller (2003). For instance, investors may reduce trading activity to mitigate risks, which impacts market liquidity. A decline in liquidity can have lasting consequences on market operations and structures. Additionally, market confidence often deteriorates in the aftermath of a cryptocurrency heist, raising investor concerns about regulations and security. This erosion of confidence can result in sell-offs and market turbulence. The recovery of market confidence tends to be prolonged, introducing structural shifts in the market. Before the KuCoin exchange heist, the market appeared relatively stable, with investors relying more on long-term trends than on sentiment. However, this heist marked a turning point as media coverage amplified negative sentiment. For example, reports suggested that the amount stolen might exceed initial estimates, and concerns about the security of cryptocurrency exchanges were raised (Jagati, 2020).

Although the KuCoin exchange heist did not compromise the Bitcoin blockchain itself, which is widely regarded as virtually hack-proof, it exposed security vulnerabilities in centralised trading platforms and severely damaged investor confidence. Bitcoin was the largest and most symbolic asset stolen in this incident. As the benchmark currency of the entire cryptocurrency market, it was central to the perceived stability of the system. Many retail investors do not clearly distinguish between "an exchange being hacked" and "Bitcoin itself being hacked," and may thus interpret such incidents as evidence of Bitcoin's insecurity. Furthermore, since exchanges are the primary gateways to Bitcoin liquidity, their security is closely tied to overall trust in the Bitcoin market (Fang et al., 2025). Consequently, the KuCoin exchange heist was perceived not merely as an incident of asset theft but as a shock to the stability and safety of the Bitcoin ecosystem, likely exerting a deeper influence on Bitcoin price and sentiment than cryptocurrency heists involving other tokens.

However, the influence of this heist on investor sentiment and its feedback on Bitcoin price does not materialise immediately. Comprehensive sentiment indicators such as the CFGI are constructed from multiple underlying components, including volatility, trading volume, and search trends, that adjust gradually to new information. Consequently, their response to sudden shocks tends to be delayed. From a behavioural finance perspective, sentiment evolution is also time-dependent: initial reactions are marked by uncertainty and observation, followed by collective emotional responses once the event's implications become widely discussed and internalised. This lagged adjustment process explains why the bidirectional predictive relationship between Bitcoin price and CFGI becomes significant only about a month after the heist. Moreover, the upward trend in the Wald statistics observed during this

period further indicates that the bidirectional predictive relationship between Bitcoin price and CFGI gradually strengthens over time, reflecting the progressive reinforcement of market feedback mechanisms.

In summary, this unease prompted sell-offs or reduced investments, which directly impact the Bitcoin price. Price volatility further fuels investor anxiety, encouraging emotional trading decisions that exacerbate price fluctuations (Bourghelle et al., 2022). These dynamics contributed to a stronger predictive relationship between Bitcoin price and CFGI in the aftermath of the KuCoin exchange heist. These findings are consistent with those of Cheung et al. (2015), Corbet et al. (2020b, 2020c), and Wang et al. (2020), further suggesting that structural breaks induced by external shocks reshape the dynamic predictive relationship between Bitcoin price and sentiment.

This chapter also provides robustness checks with a window size of 10 in Appendix 3.6 to examine whether the results are sensitive to the choice of window size. In general, the choice of window size reflects a trade-off between smoothness and responsiveness. A larger window smooths short-term fluctuations and highlights long-term trends but may obscure short-term variations in causal dynamics. In contrast, a smaller window is more sensitive to local changes and better captures short-term adjustments in relationships following sudden events. Therefore, comparing results across different window specifications helps verify the temporal robustness of the findings.

Figure 3.9 in the appendix presents the results of the time-varying Granger causality tests before the KuCoin exchange heist. The *RO* and *RE* algorithms indicate that Bitcoin price influences CFGI during certain periods, while CFGI affects Bitcoin price during others. However, the *FE* algorithm suggests that these short-term causal relationships are temporary, as no statistically significant long-term relationship is detected. This finding is consistent with the results obtained using a rolling window of 30, suggesting that before the KuCoin exchange heist, the interaction between Bitcoin price and investor sentiment remains weak and unstable.

Figure 3.10 in the appendix presents the results of the time-varying Granger causality tests after the KuCoin exchange heist. The *FE* algorithm indicates that the effects of Bitcoin price on CFGI and vice versa gradually strengthen over time. Moreover, compared with a window size of 30, the *RO* and *RE* algorithms reveal that using a smaller window size of 10 produces statistically significant bidirectional predictive relationships across a larger number of

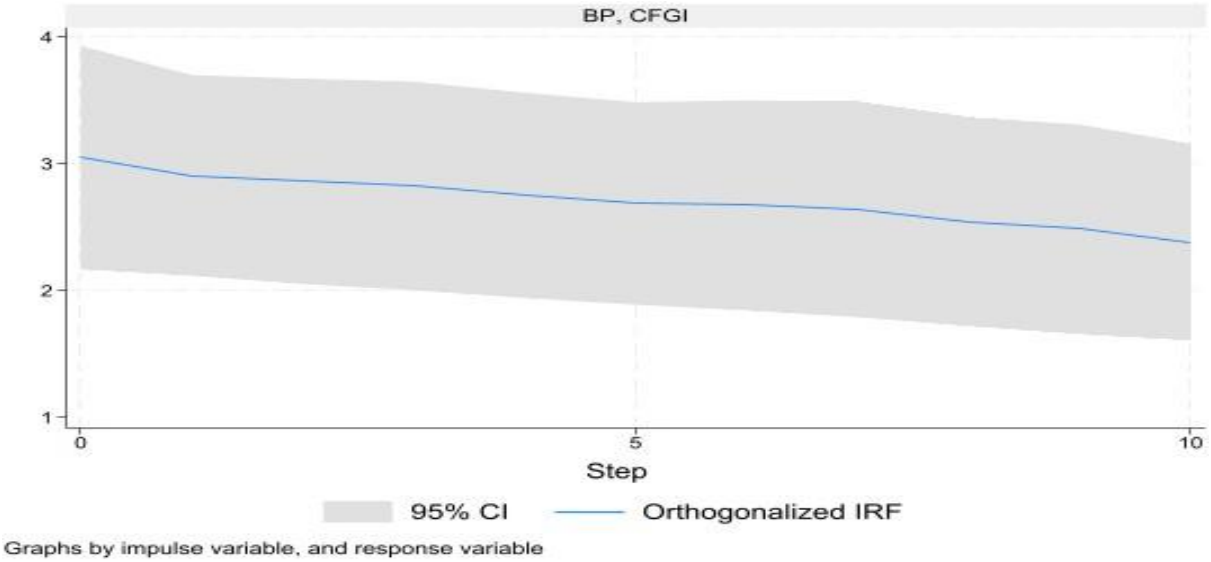
overlapping periods. This suggests that a smaller window can capture finer short-term dynamic adjustments. The incident heightened uncertainty, tightened liquidity, and intensified media attention, making the price–sentiment feedback more frequent and short-lived. Consequently, a smaller window is more sensitive to such high-frequency, short-horizon causal episodes and thus uncovers more significant predictive relationships after the heist, reflecting stronger behavioural responses and structural shifts triggered by the event.

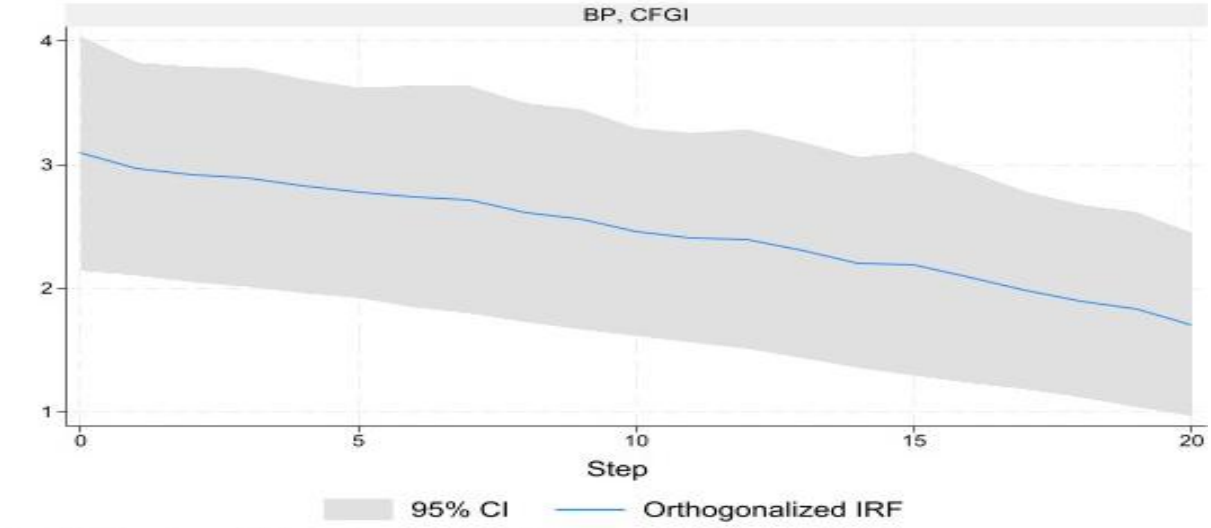
In summary, the robustness tests using different window sizes consistently support the main conclusion that, after the KuCoin exchange heist, there exists a statistically significant and gradually strengthening bidirectional predictive relationship between Bitcoin price and CFGI, whereas before the heist, this bidirectional predictive relationship is not statistically significant.

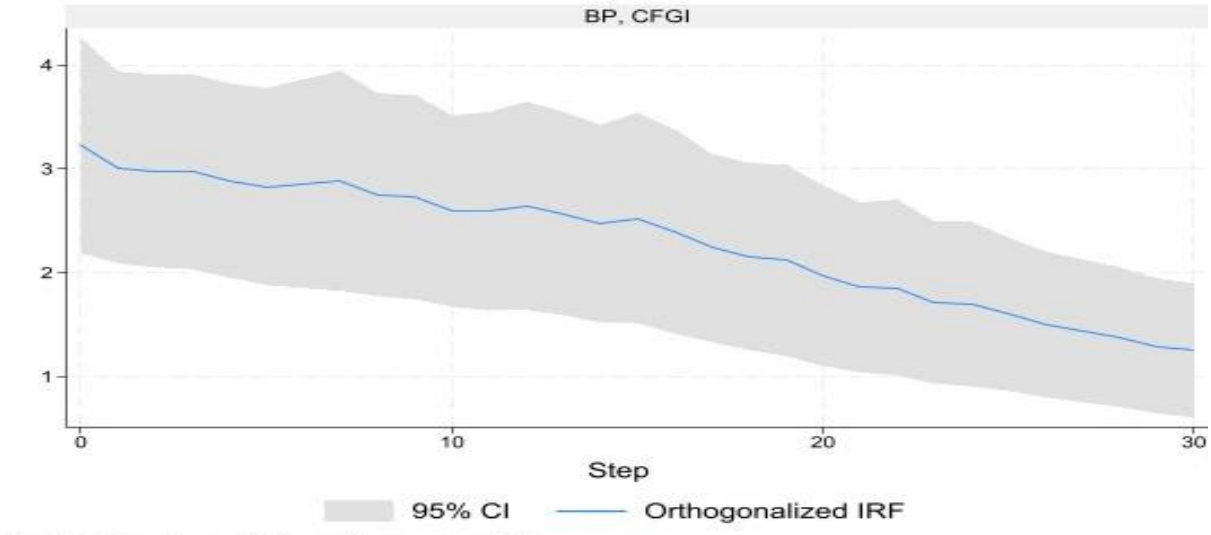
3.4.3 Local Projection Impulse Response Analysis

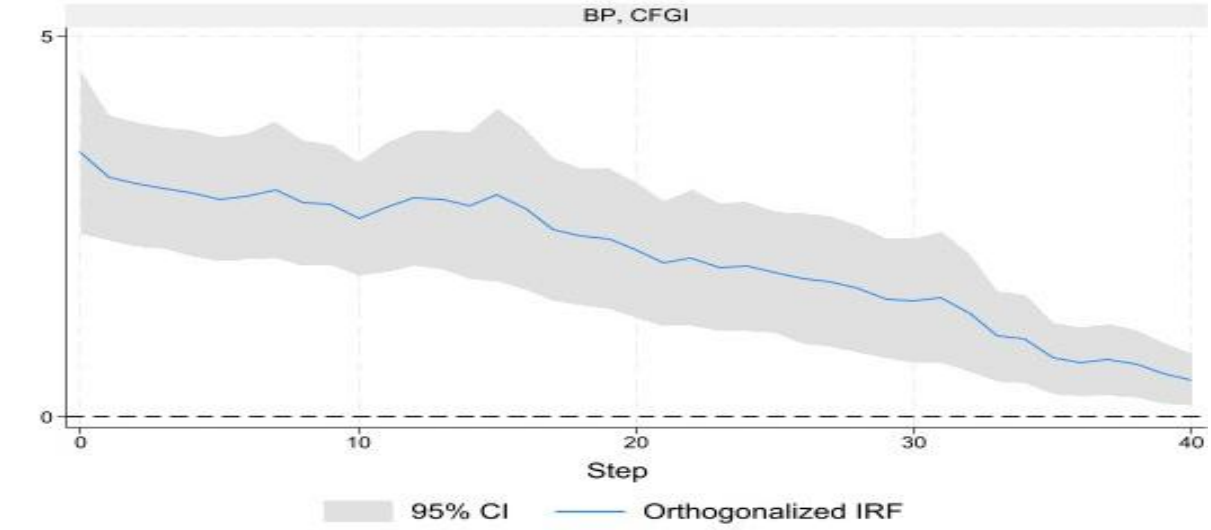
Next, this chapter uses local projection impulse response methods to investigate further the dynamic interaction between the Bitcoin price and the CFGI following the KuCoin exchange heist. This approach explores how price shocks (or market sentiment) propagate over time and influence changes in market sentiment (or prices). To ensure the robustness of our findings, this chapter conducts impulse response analyses with different forecast horizons (steps set at 10, 20, 30, and 40). The orthogonalized impulse response results presented in Figure 3.5 indicate that the Bitcoin price exerts a significant positive impact on CFGI, and similarly, CFGI has a significant positive effect on the Bitcoin price. This suggests that when the Bitcoin price (or CFGI) increases, CFGI (or Bitcoin price) also rises, and when the Bitcoin price (or CFGI) decreases, CFGI (or Bitcoin price) declines accordingly. Additionally, it observes that the impact of Bitcoin price on CFGI gradually weakens over time, stabilising around 40 days after the shock. In contrast, the influence of CFGI on Bitcoin price exhibits greater fluctuation, with an initial sharp increase reaching a peak around 30 days before gradually tapering off. These findings highlight the significant role of market sentiment in influencing Bitcoin price after the KuCoin exchange heist and reveal an asymmetric dynamic relationship between sentiment and price.

Figure 3.5: Local projected impulse responses of BP and CFGI

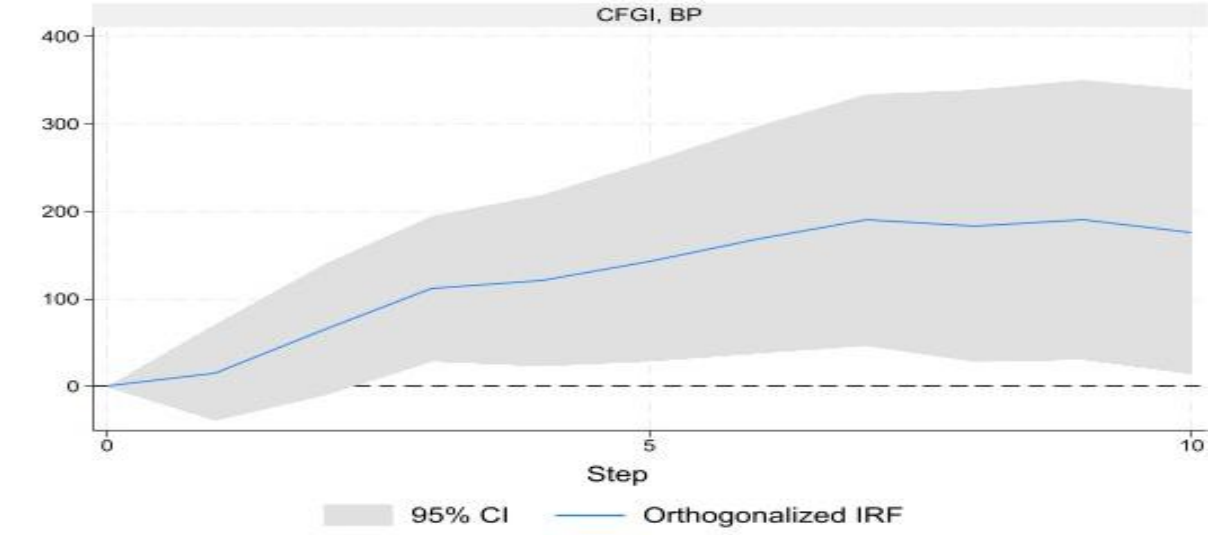




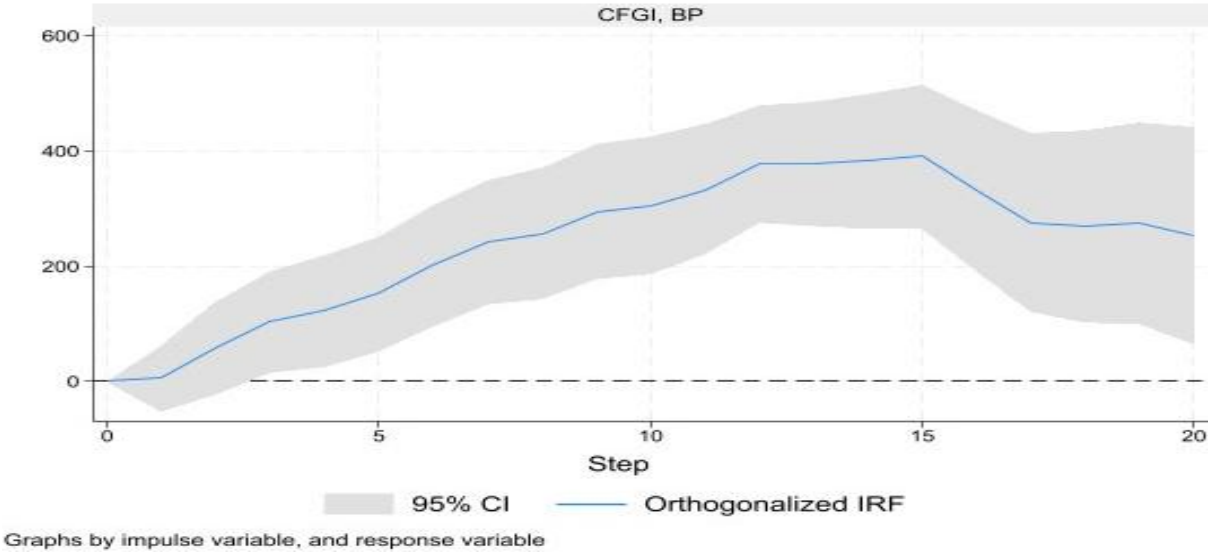




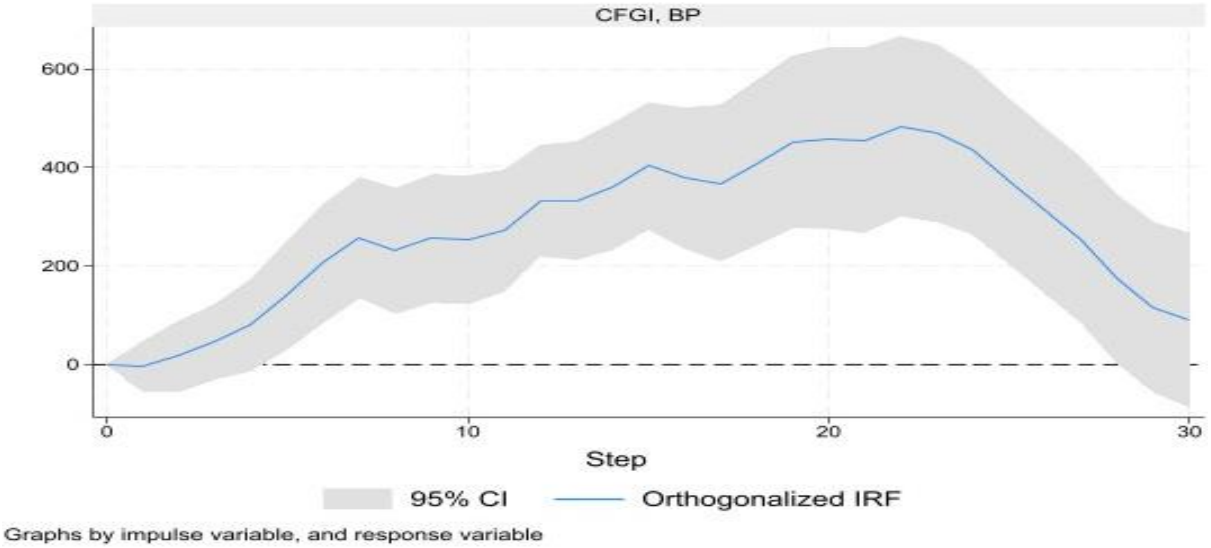
Graphs by impulse variable, and response variable

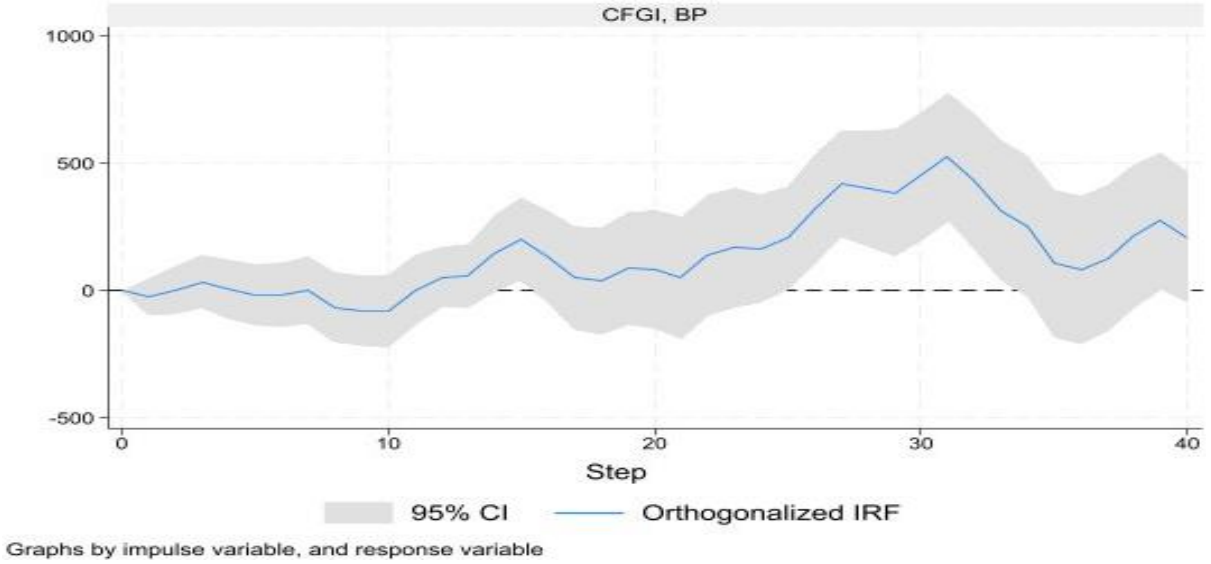


Graphs by impulse variable, and response variable



Graphs by impulse variable, and response variable





Firstly, the more decisive influence of market sentiment on prices can be attributed to the behavioural drivers of investor actions (Schmeling, 2009; Wang et al., 2021; Ballis & Verousis, 2022; Anamika et al., 2023). Following a cryptocurrency heist, investor panic or confidence directly shapes trading behaviours, amplifying market price volatility. For example, panic sentiment can trigger widespread sell-offs, further depressing prices. Moreover, market sentiment has a high degree of transmissibility and self-reinforcing characteristics. When panic spreads, it not only affects individual investors but also propagates through network effects to the entire market, leading to more pronounced price fluctuations (Bourghelle et al., 2022; Jia et al., 2022; Lin et al., 2023; Manahov & Li, 2024). In contrast, the feedback effect of price on market sentiment is typically slower and may be diluted by other market information or events during the transmission process. This asymmetry reflects a key characteristic of cryptocurrency markets: compared to traditional

financial markets, cryptocurrency markets are more sentiment-driven (Waghmare & Uike, 2023; Long et al., 2024). Due to their high volatility and lack of mature regulatory frameworks, cryptocurrency investors are more susceptible to external information (such as cryptocurrency heists) and sentiment swings, further exacerbating price volatility (Gupta et al., 2024). Finally, while sentiment may fluctuate rapidly in the short term, its overall trend (e.g. panic or confidence) usually takes longer to undergo fundamental changes (Chen et al., 2019). Conversely, price can change rapidly in the short term, but these changes may not immediately affect market sentiment (Gaies et al., 2023). During the recovery period following the incident, market sentiment may gradually adapt to price fluctuations and adjust expectations based on longer-term trends rather than reacting immediately to isolated price movements.

These findings are consistent with previous studies that emphasised the significant impact of sentiment on Bitcoin price (Kraaijeveld & De Smedt, 2020; Kapar & Olmo, 2021; Sabalionis et al., 2021; Bouteska et al., 2022; Gaies et al., 2023). However, this chapter's findings further highlight the asymmetric relationship between price and sentiment. This asymmetry underscores the central role of sentiment in shaping price movements in cryptocurrency markets while also revealing the complexities of feedback mechanisms in the sentiment-price relationship. These findings provide deeper insights into the intricate dynamics of cryptocurrency markets, particularly in the aftermath of disruptive incidents such as cryptocurrency heists, where sentiment and price fluctuations can amplify each other in unique and unpredictable ways.

In summary, the results of the time-varying Granger causality tests and local projection impulse response analysis support the hypothesis *H1*. The dynamic predictive relationship between Bitcoin price and CFGI highlights the significant impact of specific incidents on Bitcoin price and market sentiment. Following Bitcoin-specific heists, the bidirectional predictive relationship between Bitcoin price and CFGI becomes notably stronger. Investors can use CFGI to forecast price trends and market reactions during such incidents. Similarly, changes in Bitcoin prices can provide insights into future shifts in market sentiment, enabling investors to refine their Bitcoin trading strategies. This predictive relationship offers investors an additional source of information, helping them better navigate market volatility and mitigate potential losses (AlNemer et al., 2021).

3.4.4 Time-Varying Granger Causality Test between Bitcoin Price and CFGI during Other Cryptocurrency Heists

As of April 2024, there are more than 9,000 cryptocurrencies (CoinMarketCap, 2024). This diversity has expanded the range of potential target assets for cryptocurrency heists, with commonly stolen cryptocurrencies including Ethereum, Binance Coin, Ripple, and Tether. Although this chapter observes that in the KuCoin exchange heist, Bitcoin price influenced CFGI, and CFGI, in turn, influenced Bitcoin price, whether this bidirectional predictive relationship applies to heists targeting other cryptocurrencies still deserves further exploration. Considering CFGI's available data range, this chapter uses nine cryptocurrency heists discussed in Chapter 2 as a sample. Table 3.8 presents the data span for each cryptocurrency heist. To ensure consistency across cases, the same time frame as used in the KuCoin exchange heist analysis is applied, a 30-day period following each cryptocurrency heist.

Table 3.8: The scope of cryptocurrency heist data

Platform	Data range
PancakeBunny	May 20, 2021, to August 17, 2021
Poly Network	August 10, 2021, to November 07, 2021
Bitmart	December 4, 2021, to March 3, 2022
Wormhole	February 03, 2022, to May 03, 2022
Ronin Network	March 29, 2022, to June 26, 2022
Beanstalk	April 16, 2022, to July 14, 2022
Nomad	August 02, 2022, to October 30, 2022
Binance	October 07, 2022, to January 04, 2023
FTX	November 11, 2022, to February 08, 2023

The Bitcoin price (BP) data is sourced from CoinGecko, while the CFGI data is obtained from Alternative.me.

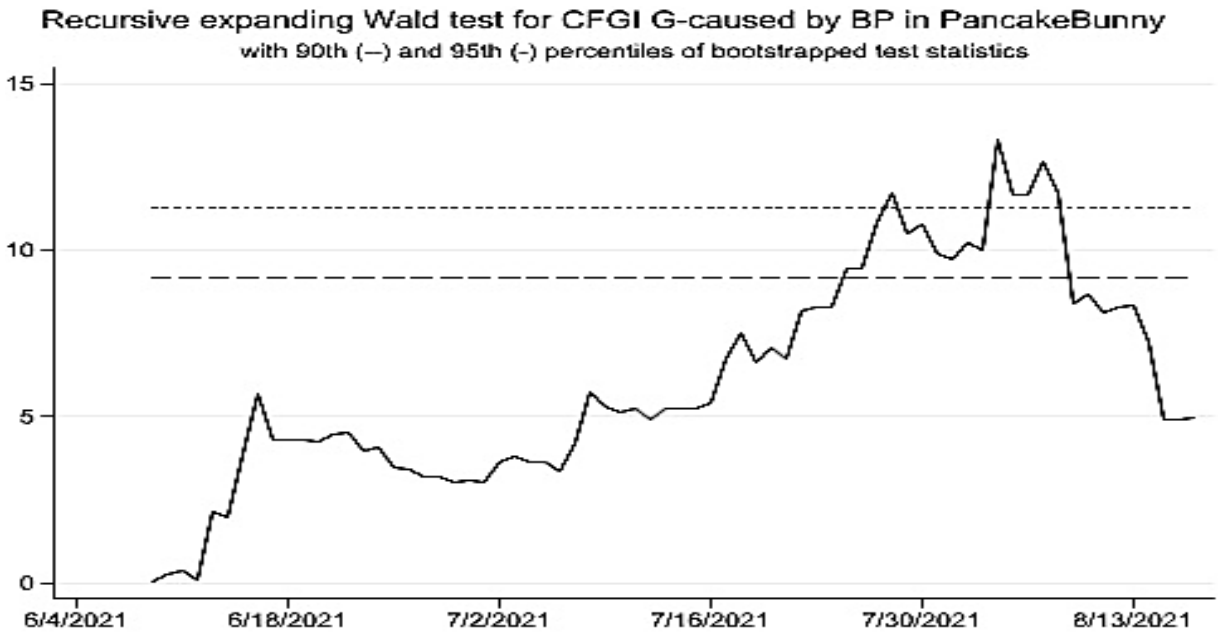
Since the *RE* algorithm integrates the strengths of both the *FE* and *RO* algorithms, which capture short-term dynamics and long-term trends simultaneously while demonstrating superior sensitivity to temporal instability (Baum et al., 2021), this chapter primarily presents results based on the *RE* algorithm. The results from the *FE* and *RO* algorithms are provided in Appendix 3.6 (Figure 3.11) as robustness checks. Figure 3.6 presents the results of the time-varying Granger causality test using the *RE* algorithm[4]. The findings indicate that, following most cryptocurrency heists, Bitcoin price has little to no statistically significant

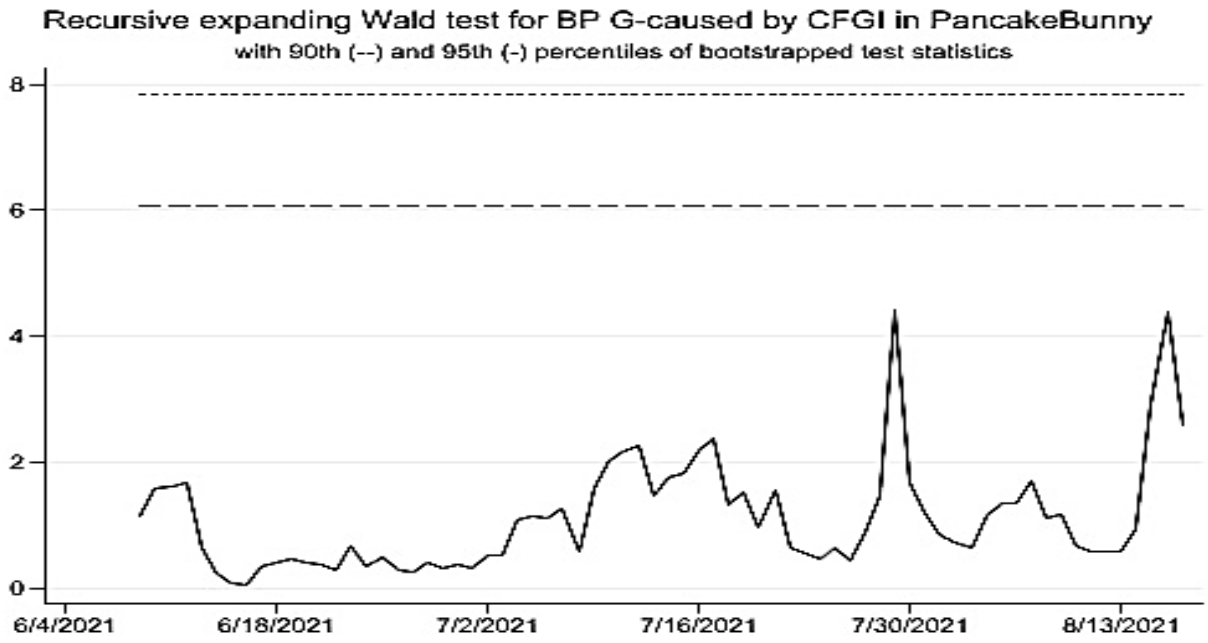
[4] The VAR model is constructed using the first-order differenced Bitcoin price (BP) and the CFGI series. Except for the Nomad protocol and Binance platform heists, where the optimal lag orders are 4 and 2, respectively, all other cryptocurrency heists adopt a lag order of 1. The rolling window size is set to 20, balancing the trade-off between capturing short-term fluctuations and maintaining estimation stability. 999 bootstrap repetitions are used. Wald statistics are computed to be robust to heteroskedasticity.

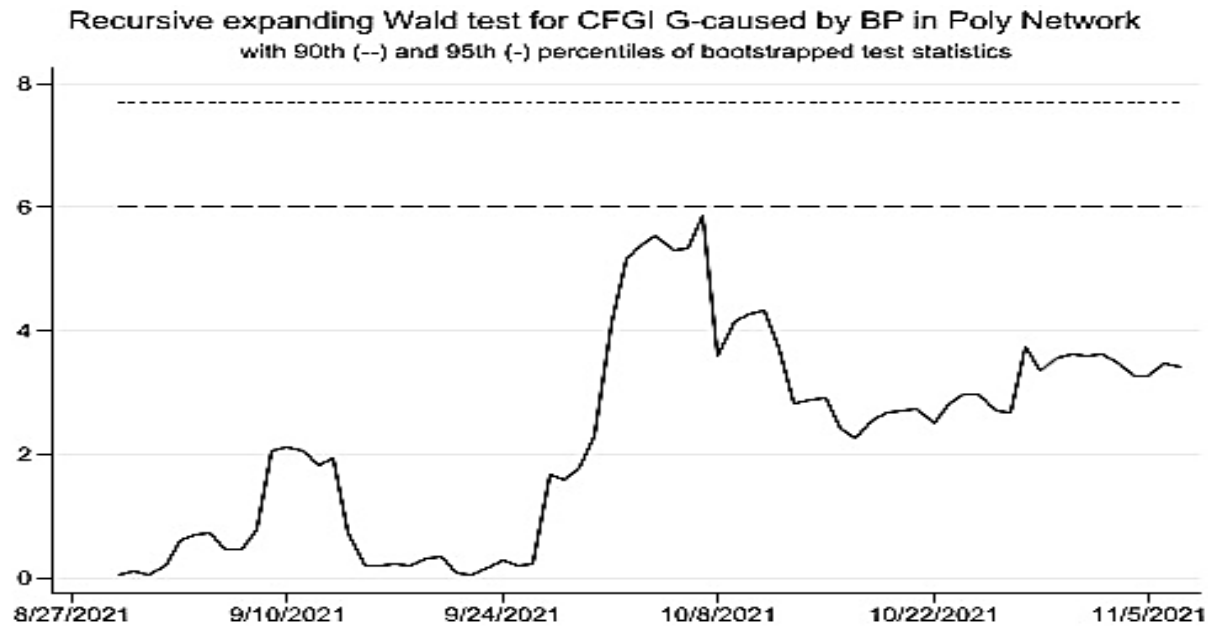
effect on CFGI. Likewise, CFGI shows limited statistically significant influence on Bitcoin price. This phenomenon is understandable, as CFGI primarily measures sentiment specific to the Bitcoin market, and Bitcoin itself is not directly targeted in these cryptocurrency heists. Typically, such heists trigger widespread market anxiety, but the concern is often concentrated on the affected tokens. Investors tend to monitor the markets of stolen tokens more closely, as these assets are directly associated with potential financial losses, leading to greater volatility in those markets.

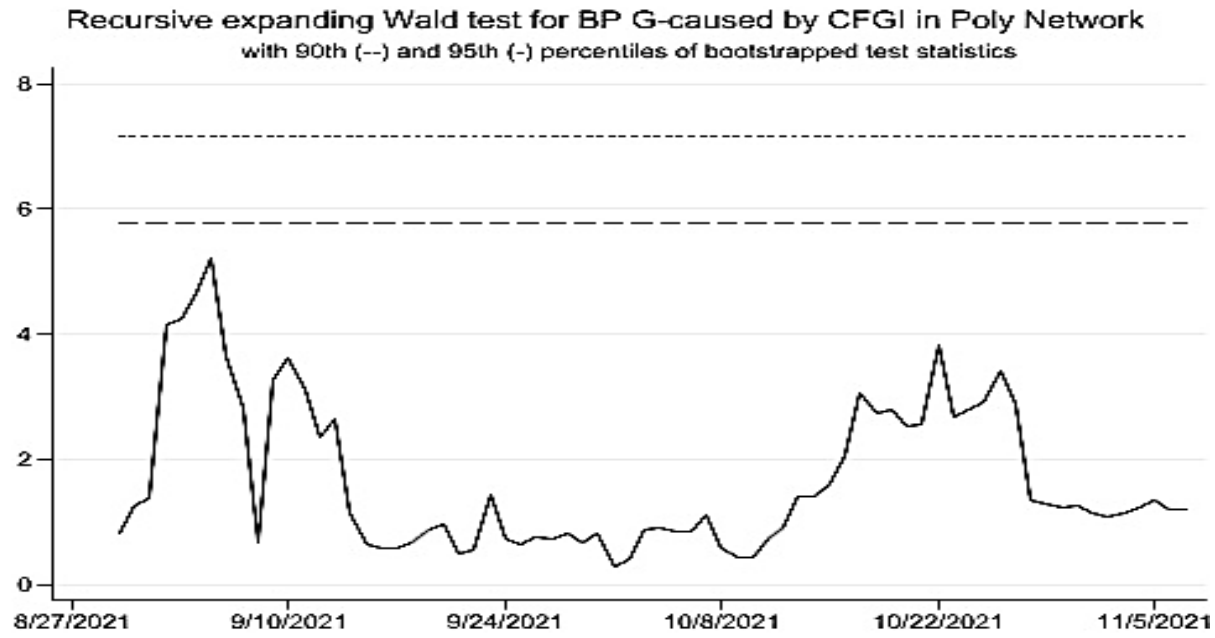
In contrast, unlike the dramatic fluctuations of the stolen tokens, Bitcoin may exhibit more stable price movements over the long-term following these cryptocurrency heists. As a result, the influence of Bitcoin price on Bitcoin market sentiment may not be significant. Furthermore, the speed and scope of sentiment diffusion in the cryptocurrency market may be constrained by prevailing market conditions (Vasudevan et al., 2024). Negative sentiment generated around stolen tokens may not immediately spill into the Bitcoin market. The relatively stable sentiment in the Bitcoin market may not significantly influence the Bitcoin price.

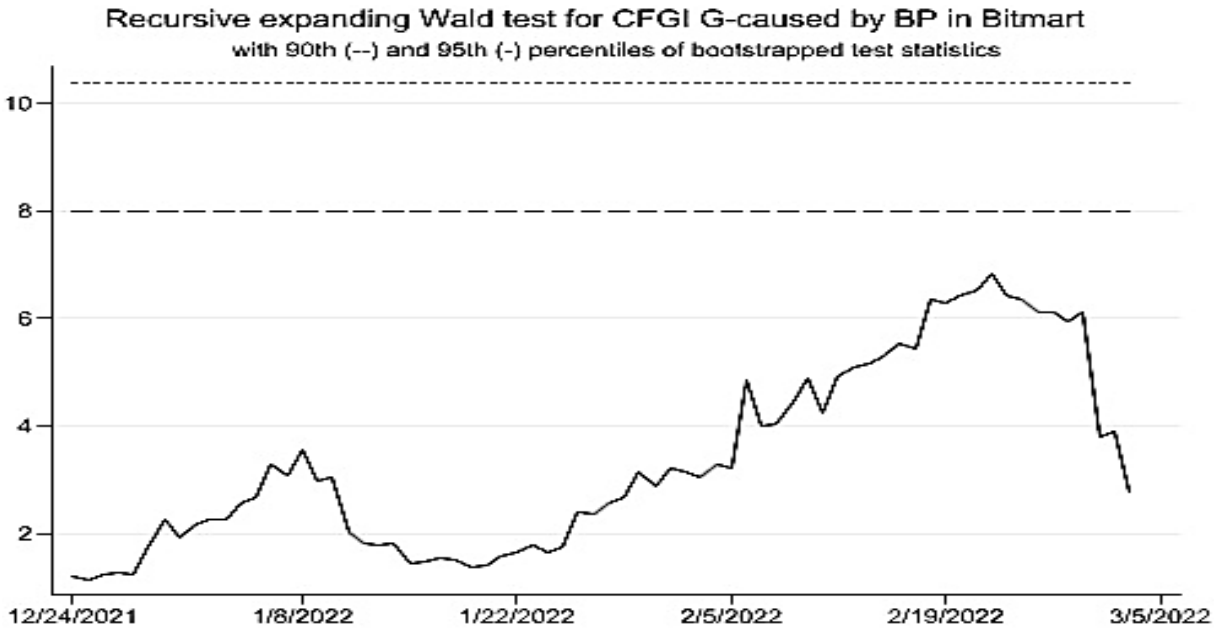
Figure 3.6: Time-varying Granger causality between BP and CFGI using the *RE* algorithm across nine cryptocurrency heists

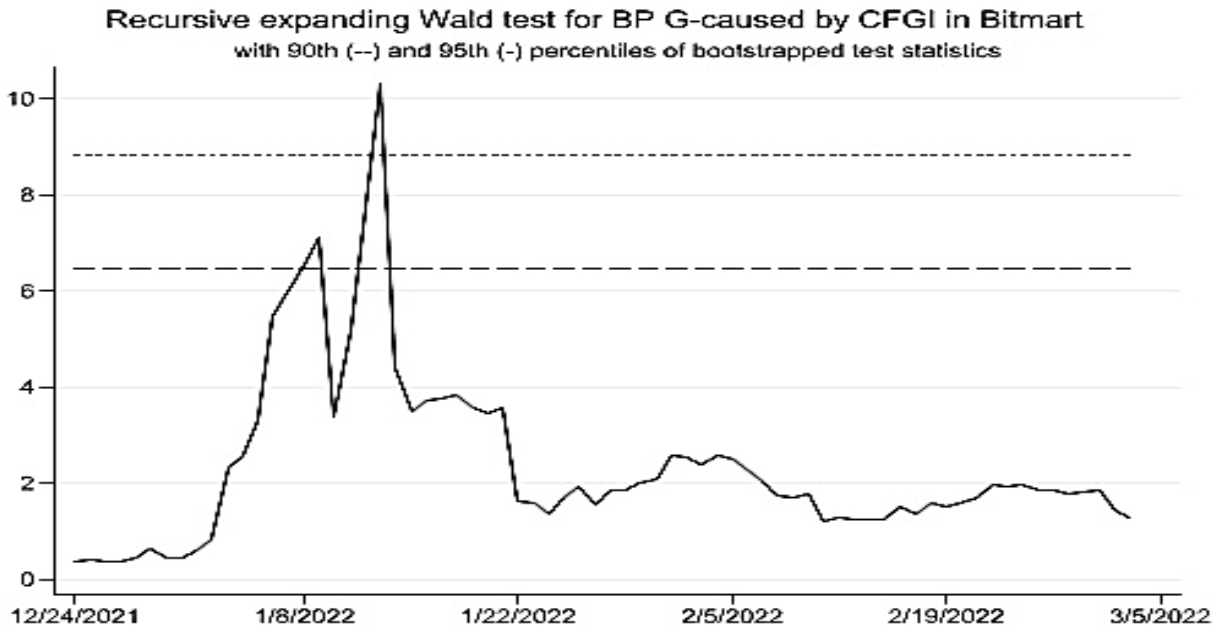


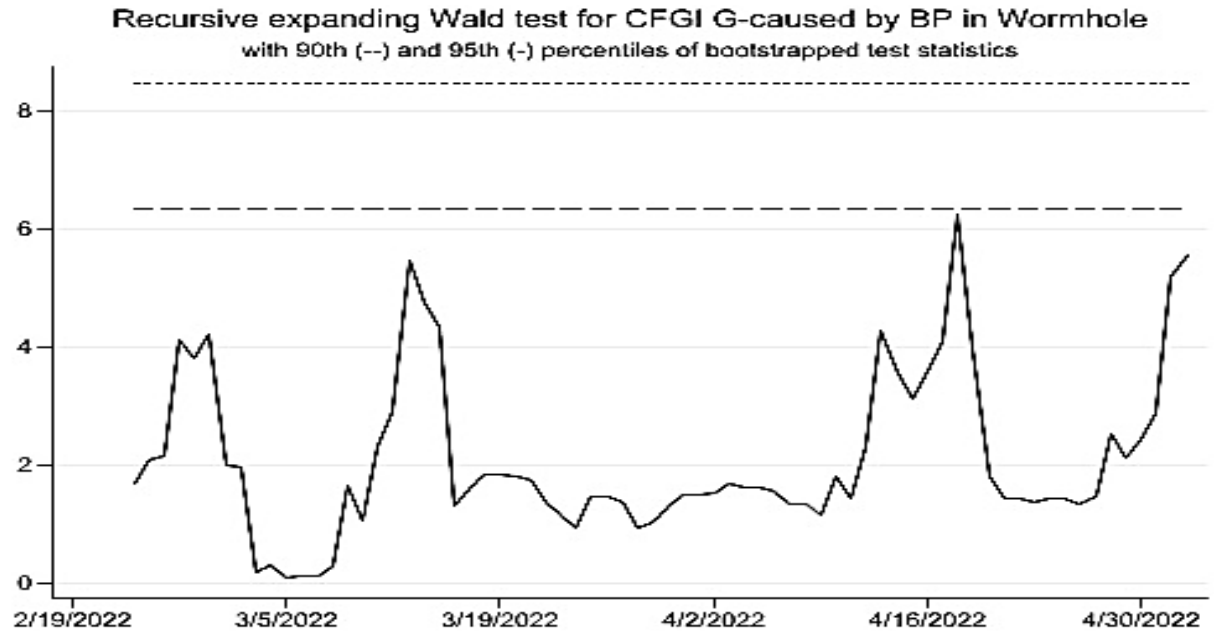

Recursive expanding Wald test for BP G-caused by CFGI in PancakeBunny
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
6/4/2021
6/18/2021
7/2/2021
7/16/2021
7/30/2021
8/13/2021

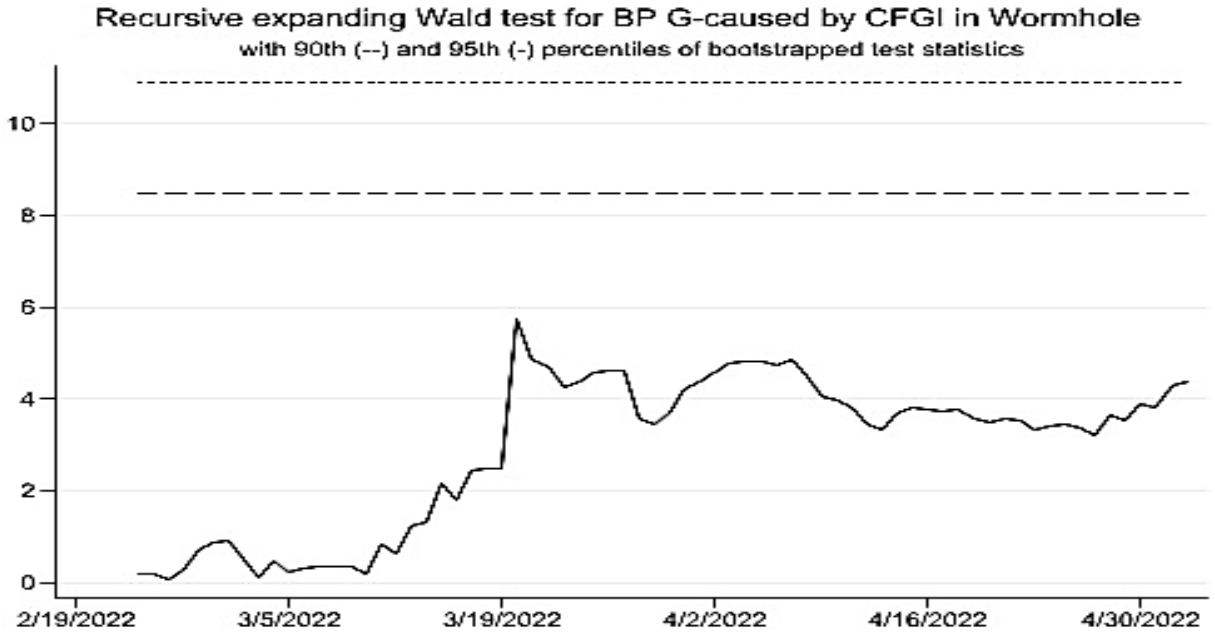

Recursive expanding Wald test for CFGI G-caused by BP in Poly Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
8/27/2021
9/10/2021
9/24/2021
10/8/2021
10/22/2021
11/5/2021

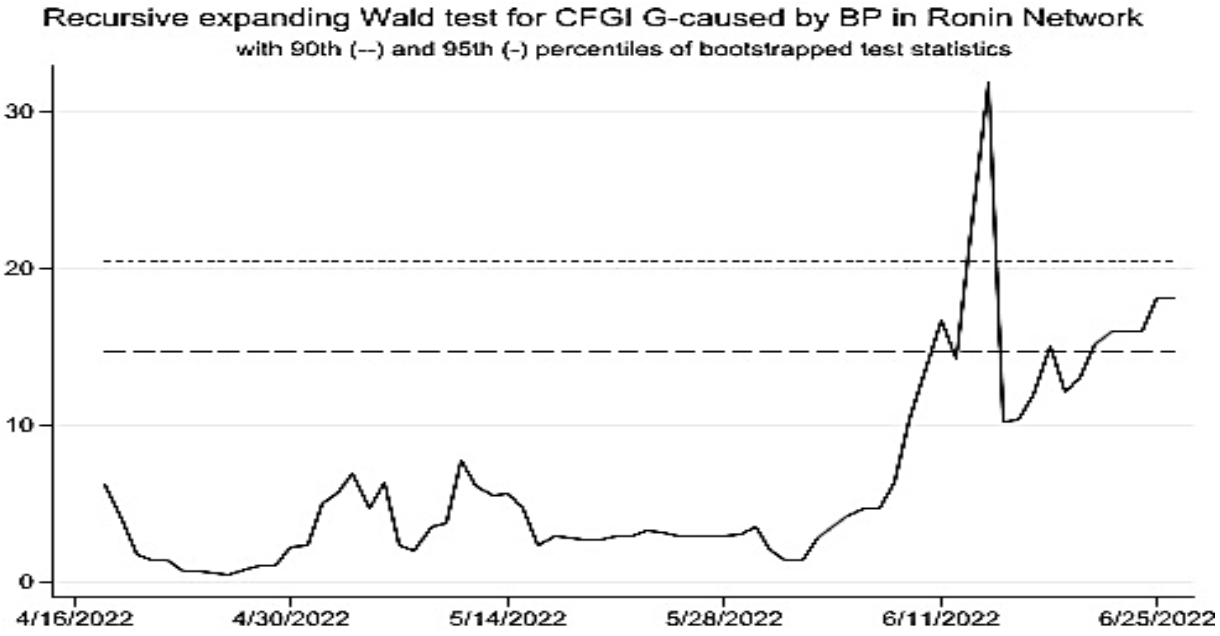

Recursive expanding Wald test for BP G-caused by CFGI in Poly Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
8/27/2021
9/10/2021
9/24/2021
10/8/2021
10/22/2021
11/5/2021

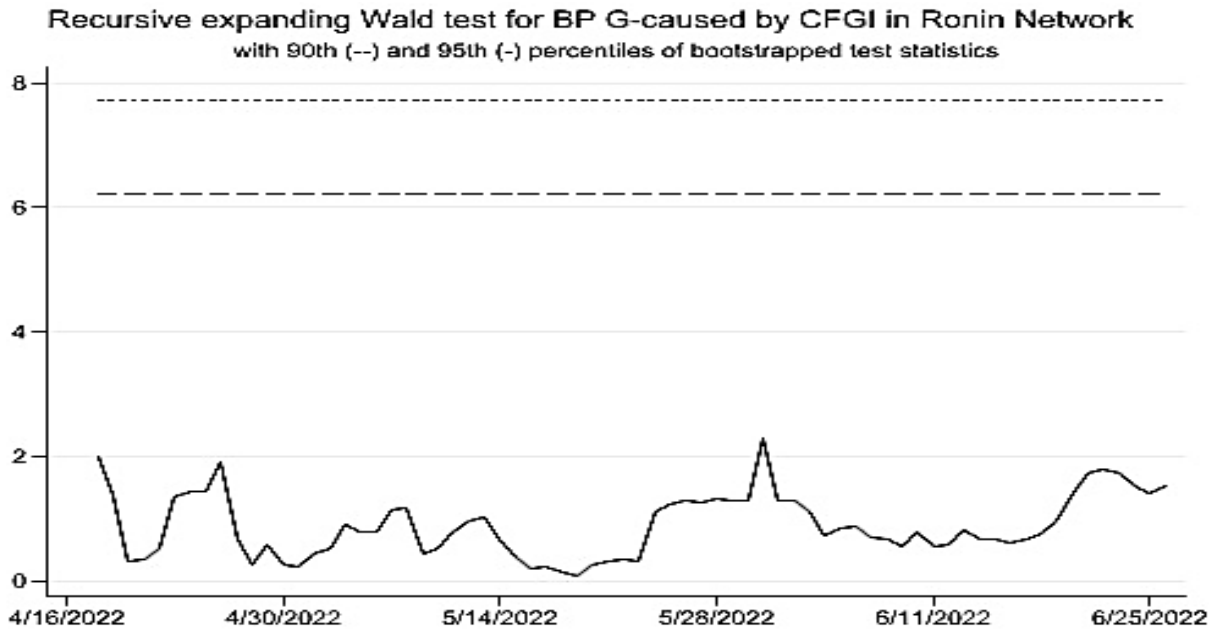

Recursive expanding Wald test for CFGI G-caused by BP in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

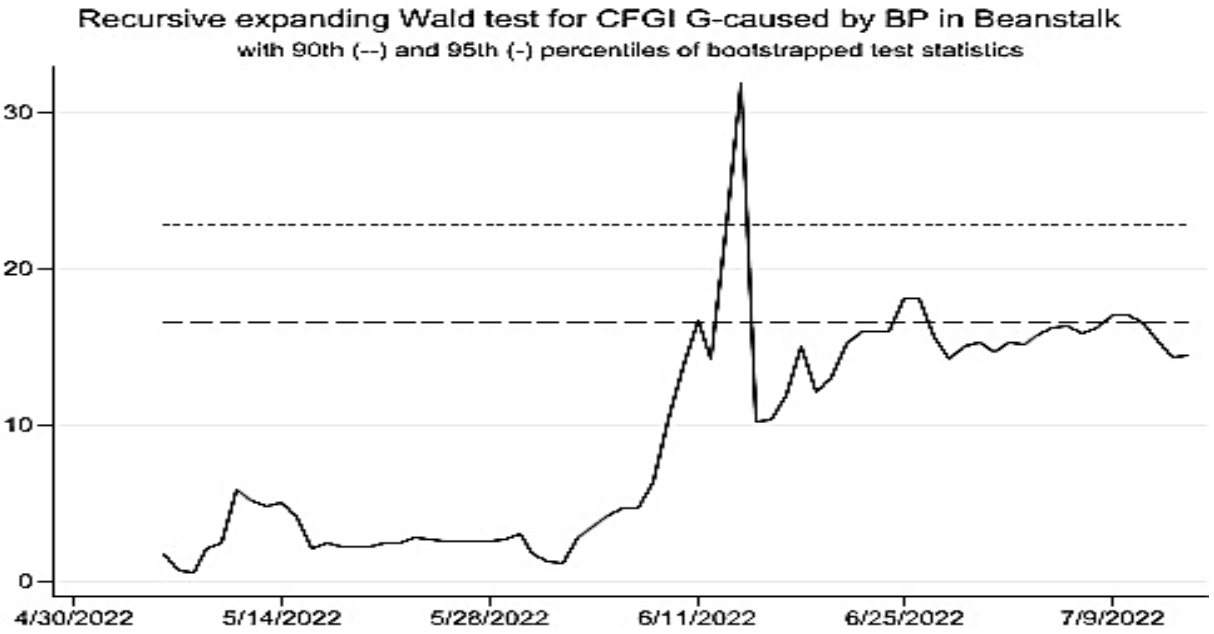

Recursive expanding Wald test for BP G-caused by CFGI in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
0
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

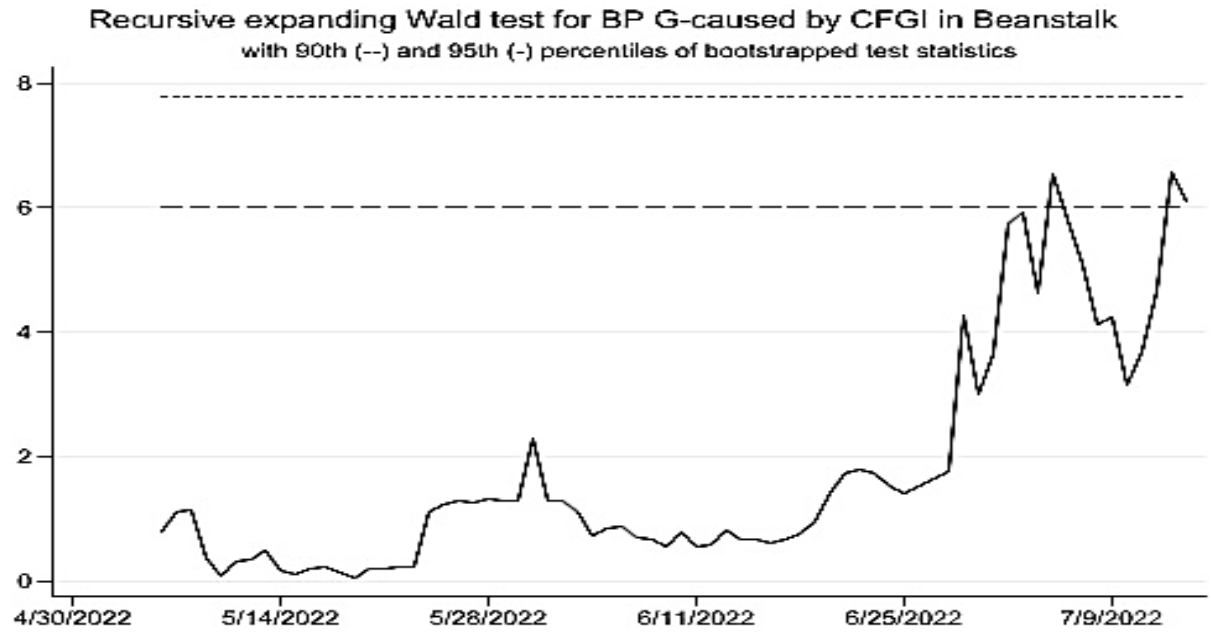

Recursive expanding Wald test for CFGI G-caused by BP in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

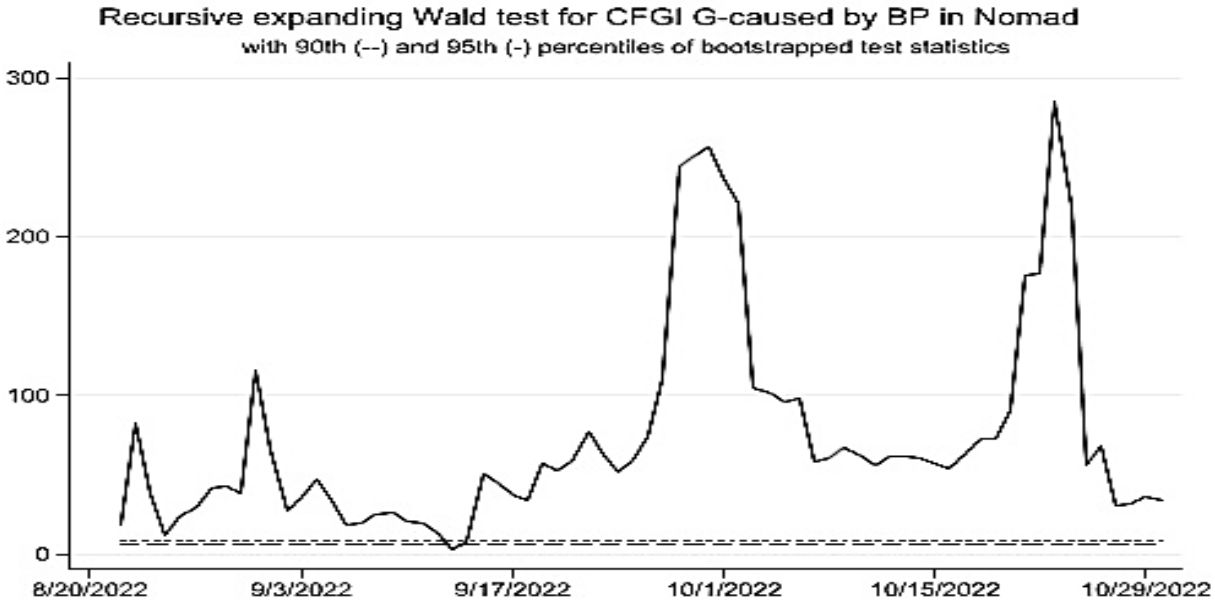

Recursive expanding Wald test for BP G-caused by CFGI in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
0
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

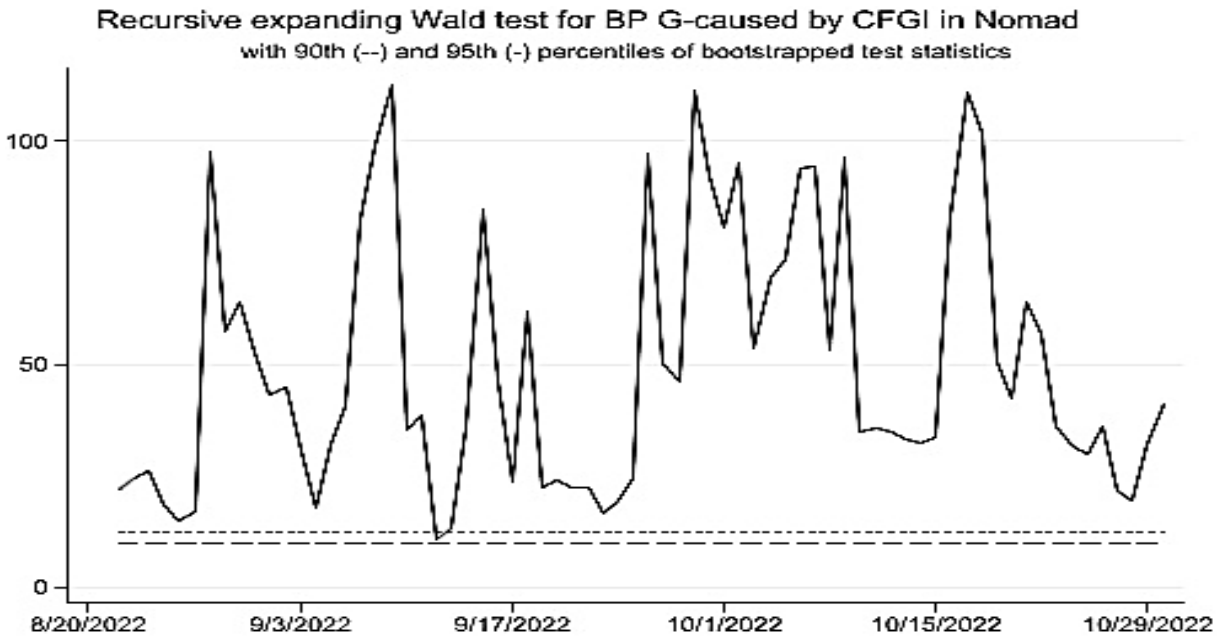

Recursive expanding Wald test for CFGI G-caused by BP in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

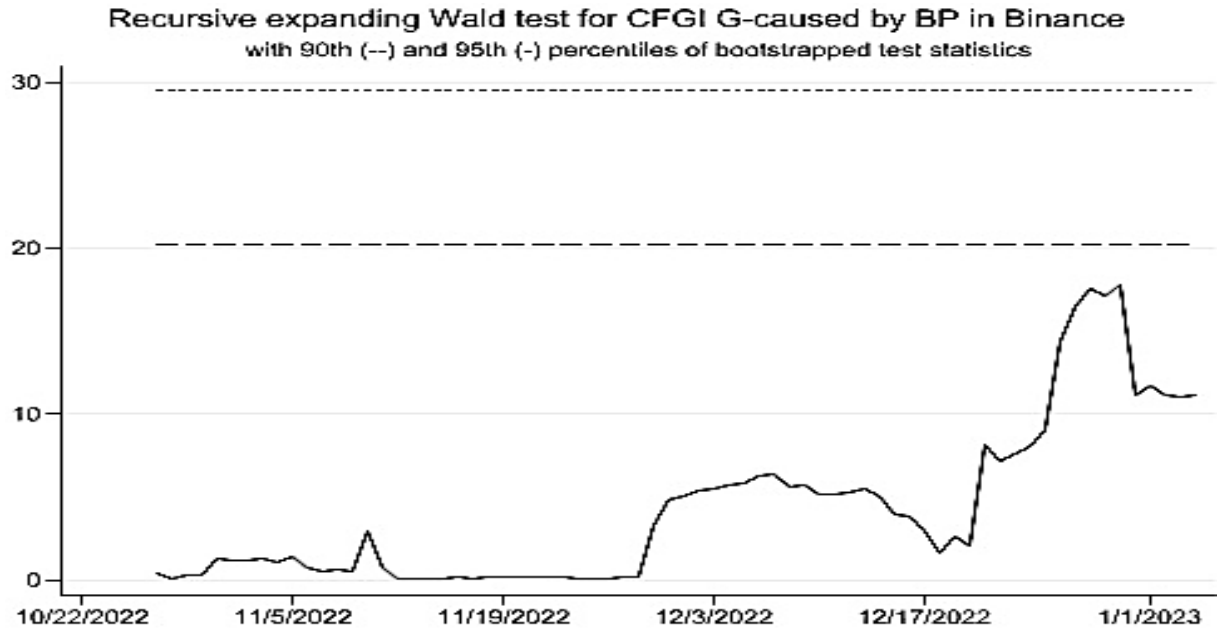

Recursive expanding Wald test for BP G-caused by CFGI in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

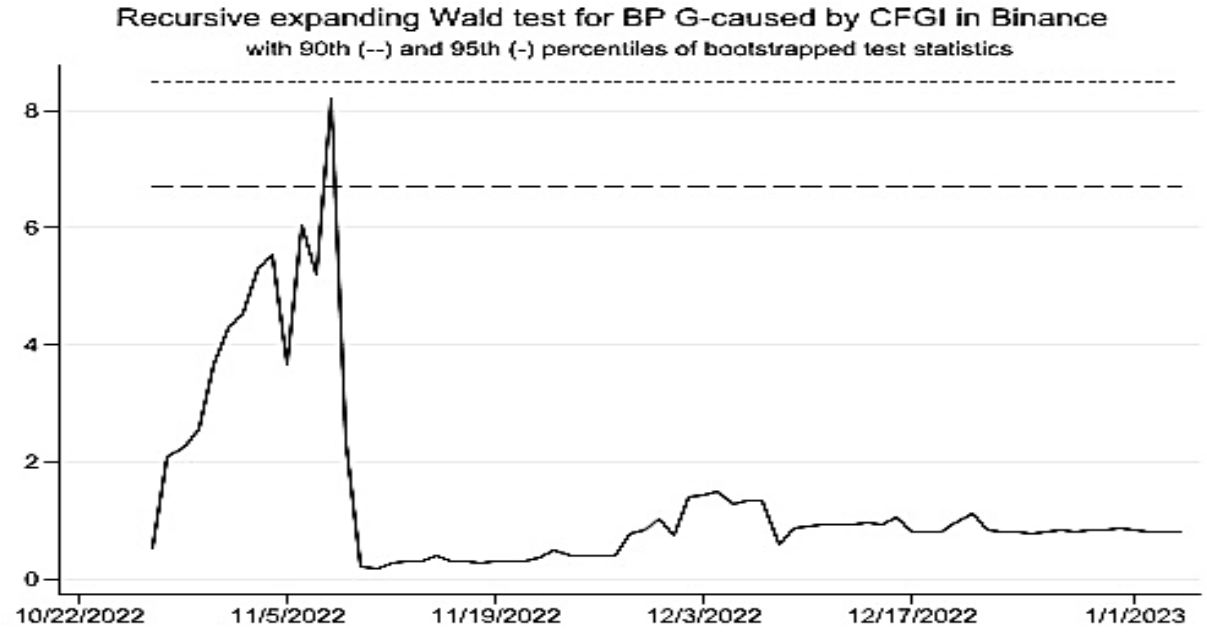

Recursive expanding Wald test for CFGI G-caused by BP in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

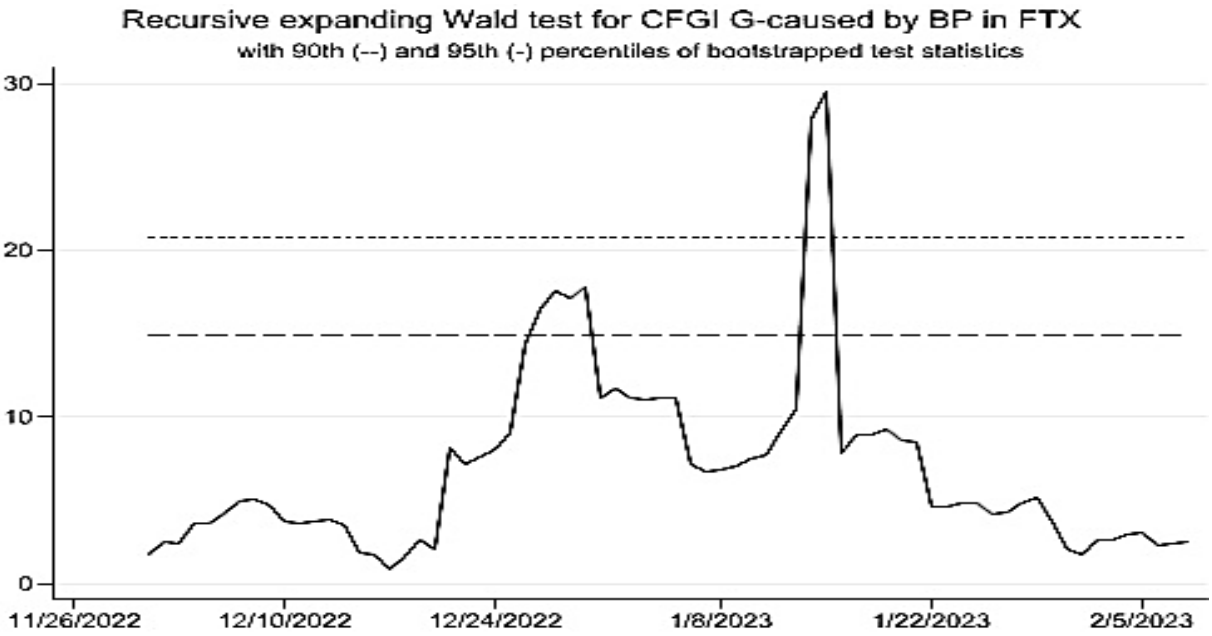

Recursive expanding Wald test for BP G-caused by CFGI in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

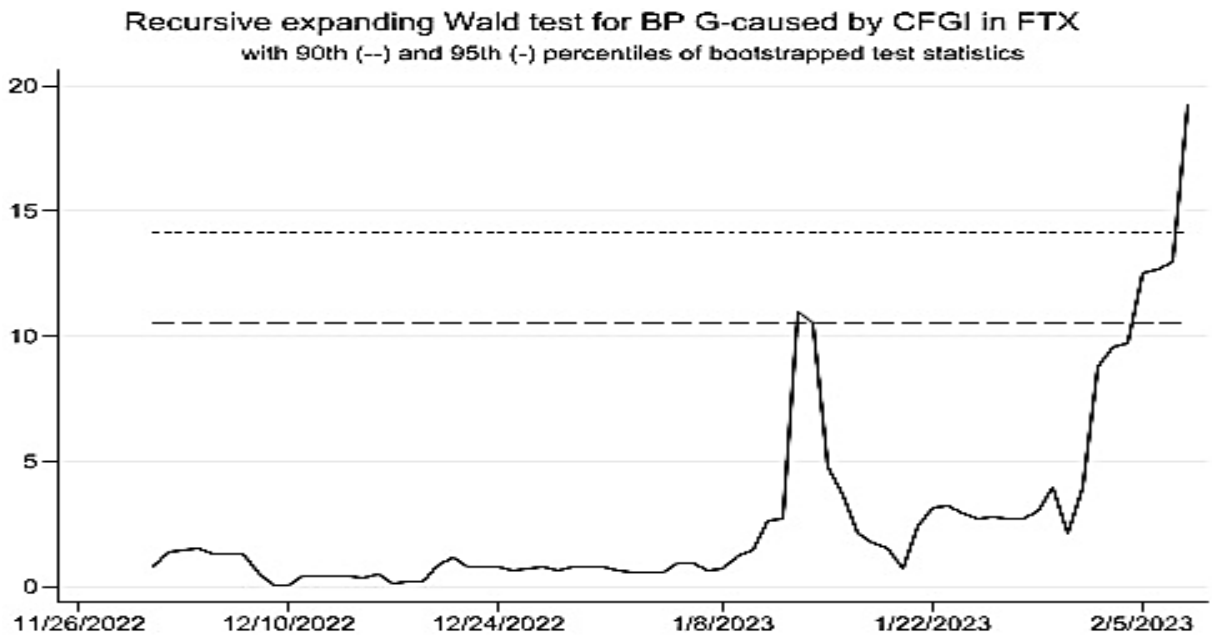

Recursive expanding Wald test for CFGI G-caused by BP in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
300
200
100
0
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022


Recursive expanding Wald test for BP G-caused by CFGI in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
100
50
0
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022


Recursive expanding Wald test for CFGI G-caused by BP in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023

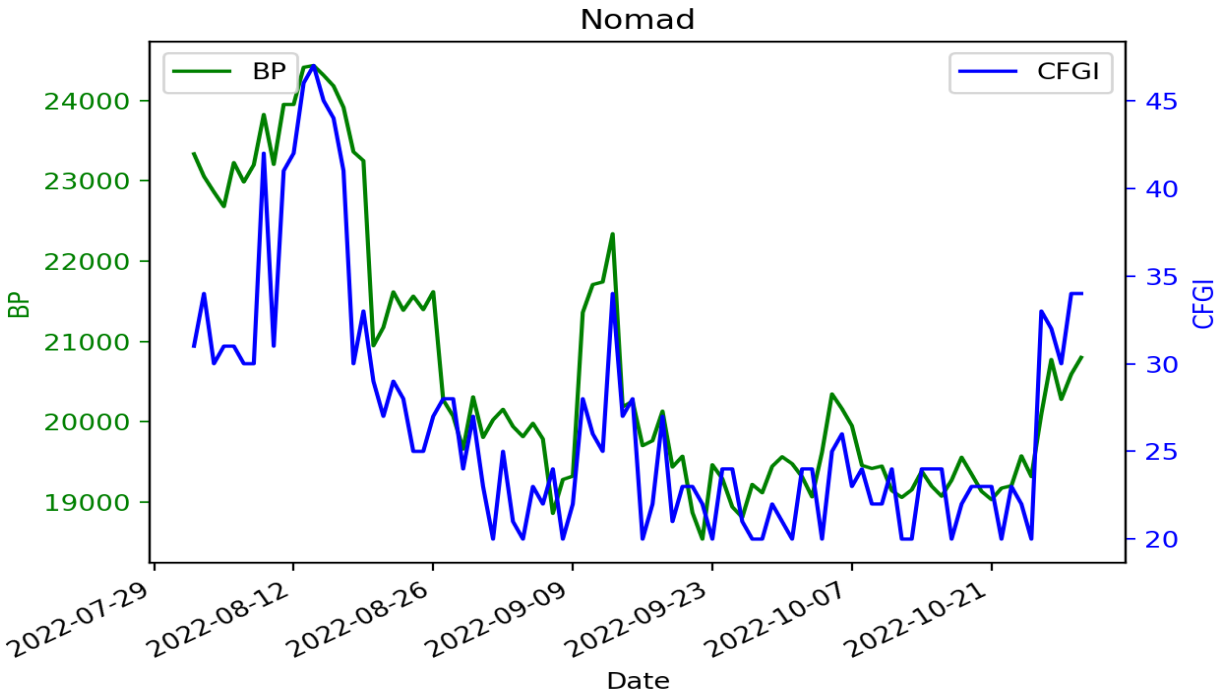

Recursive expanding Wald test for BP G-caused by CFGI in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023


Recursive expanding Wald test for CFGI G-caused by BP in FTX
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
11/26/2022
12/10/2022
12/24/2022
1/8/2023
1/22/2023
2/5/2023



The Nomad protocol heist is particularly noteworthy, as it represents a rare case where statistically significant bidirectional predictive relationship is observed between Bitcoin price and CFGI following the incident. Nomad is a cryptocurrency bridging service provider whose core smart contract contained a critical vulnerability in the past. This flaw allowed attackers to manipulate transactions, facilitating the widespread theft of tokens bridged through the protocol. Multiple parties rapidly exploited the vulnerability, resulting in the loss of substantial assets and making it one of the most chaotic and extensive hacks in cryptocurrency history. What distinguishes the Nomad protocol heist is its far-reaching impact. Unlike attacks targeting specific tokens, the vulnerability in the Nomad bridge affects all assets connected to its infrastructure, leading to significant disruptions across the cryptocurrency market and severely undermining investor confidence in bridging protocols. Figure 3.7 illustrates the changes in Bitcoin price and CFGI following the Nomad protocol heist, revealing a pronounced simultaneous decline in Bitcoin price and market sentiment. Although Bitcoin is not directly targeted, the exploitation of the Nomad protocol heightens investor perceptions of systemic risk in the cryptocurrency market. As the benchmark asset in the crypto space, Bitcoin experiences considerable volatility in both price and sentiment. The collapse of confidence in bridging protocols—critical for cross-chain transactions—raises broader concerns about the security of blockchain ecosystems. This erosion of trust leads to a decline in Bitcoin's price and poses major challenges to the recovery of market sentiment.

Figure 3.7: Trends of BP and CFGI after the Nomad protocol heist



The Bitcoin price data is sourced from CoinGecko, while the CFGI data is obtained from Alternative.me.

The results of the *FE* and *RO* algorithms presented in Appendix 3.6 (Figure 3.11) show consistent findings. In summary, the empirical evidence supports Hypothesis *H2*. Specifically, in Bitcoin-targeted heists, the predictive relationship between Bitcoin price and market sentiment is stronger. However, in broader cryptocurrency heists that do not directly involve Bitcoin, this predictability weakens. For investors, especially in an environment where cryptocurrency heists occur frequently, using the CFGI to formulate investment strategies after a cryptocurrency heist requires careful consideration of the incident's impact on the Bitcoin market. If a cryptocurrency heist severely disrupts the Bitcoin market, the CFGI may become highly valuable for forecasting Bitcoin price movements. Conversely, if the cryptocurrency heist has little direct effect on Bitcoin, relying solely on CFGI may lead to inaccurate predictions and suboptimal investment decisions.

3.4.5 The Impact of CFGI on Other Cryptocurrency Markets

As the most significant cryptocurrency market by capitalisation, Bitcoin's dynamics often profoundly impact the broader cryptocurrency ecosystem. However, whether the market panic triggered by Bitcoin thefts affects other cryptocurrency markets remains uncertain. Existing studies offer mixed findings regarding the spillover effects between cryptocurrency markets. Some studies suggested that Bitcoin, as a high-capitalisation cryptocurrency, serves

as a major source of returns and volatility spillovers to other cryptocurrency markets, with these effects intensifying over time (Katsiampa et al., 2019a; Kumar & Anandarao, 2019; Özdemir, 2022; Manahov & Li, 2024). In contrast, other studies indicated weak or non-existent volatility spillovers between Bitcoin and other cryptocurrency markets (Luu Duc Huynh, 2019; Zięba et al., 2019). These discrepancies imply that the relationships between cryptocurrency markets may inherently be dynamic, shaped by market sentiment, regulatory changes, and unexpected market events. In the previous analysis of the KuCoin exchange heist, this chapter finds that CFGI significantly influences the Bitcoin price after the heist. Next, it aims to investigate whether CFGI also influences other cryptocurrency markets. This chapter selects Ethereum and Binance Coin as representative assets. These two cryptocurrencies are among the most highly capitalised and particularly susceptible to hacker theft. Daily price data for Ethereum (EP) and Binance Coin (BCP) is also sourced from CoinGecko, and the data range is from September 25, 2020, to December 23, 2020.

This chapter employs a connectedness test based on the TVP-VAR model to examine the spillovers among CFGI, Bitcoin, Ethereum, and Binance Coin. By analysing their connectedness, this analysis investigates how much of the price volatility in Ethereum and Binance Coin can be attributed to fluctuations in CFGI, thereby revealing whether volatility in Bitcoin-related market sentiment affects other major cryptocurrencies. Table 3.9 reports the connectedness results among the variables following the KuCoin exchange heist. The total connectedness index (*TCI*) is relatively low, at 51.68, indicating that the spillover effects among CFGI, Bitcoin, Ethereum, and Binance Coin are moderate and that their fluctuations remain relatively independent. For CFGI, the largest volatility contribution it receives comes from Bitcoin (22.07%), while it receives much less from Ethereum (15.44%) and Binance Coin (11.98%). This indicates that Bitcoin volatility is the primary driver of CFGI, whereas Ethereum and Binance Coin play a more limited role in influencing it. Moreover, Bitcoin also receives a substantial volatility contribution from CFGI, amounting to 20.24%. This finding aligns with previous results showing that, after the KuCoin exchange heist, the predictive relationship between Bitcoin and CFGI strengthened, with each exerting a significant influence on the other.

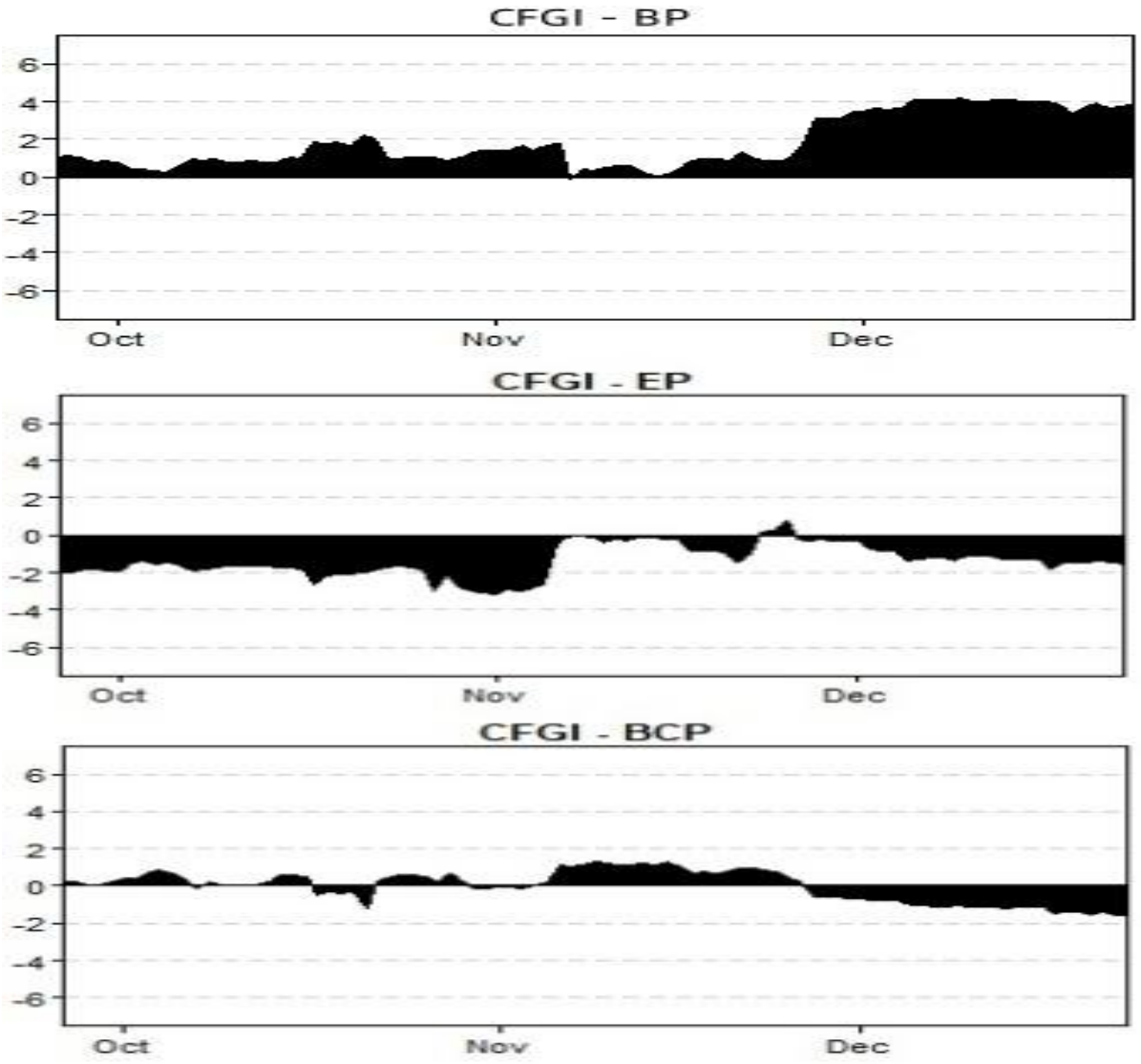
Table 3.9: Connectivity results between CFGI, BP, EP and BCP

	BP	CFGI	EP	BCP	FROM
BP	44.91	20.24	25.71	9.14	55.09
CFGI	22.07	50.51	15.44	11.98	49.49
EP	25.47	14.09	43.42	17.02	56.58
BCP	11.39	11.95	22.23	54.43	45.57
TO	58.92	46.28	63.39	38.14	206.73
NET	3.84	-3.21	6.81	-7.43	**TCI**
					51.68

The data for Bitcoin price (BP), Ethereum price (EP), and Binance Coin price (BCP) are obtained from CoinGecko, while the CFGI data is sourced from Alternative.me. The findings are derived from a TVP-VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each variable receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the variable is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. *TCI* represents the overall level of connectedness among the variables, while a lower *TCI* suggests weaker linkages and more independence among variables.

For Ethereum and Binance Coin, the volatility contribution they receive from CFGI is relatively modest, at only 14.09% and 11.95%, respectively. This indicates that while Bitcoin market sentiment plays a significant role in driving Bitcoin's price dynamics following the KuCoin exchange heist, its influence on other cryptocurrencies, such as Ethereum and Binance Coin, appears more limited. This may be attributed to investors' differing perceptions of cryptocurrencies, influenced by factors such as variations in blockchain technology. While the KuCoin exchange heist may raise security concerns for Bitcoin, it does not necessarily affect other cryptocurrencies. Moreover, the cryptocurrency market comprises thousands of tokens, each with its own ecosystem and community. Consequently, when a token is affected by a cryptocurrency heist, the impact tends to remain confined within its own market, exerting limited influence on others (Victor & Weintraud, 2021; Li et al., 2024). This fragmentation attenuates the linkage between Bitcoin sentiment and other cryptocurrency markets. Therefore, the sentiment and prices of different cryptocurrencies may remain stable in the aftermath of the KuCoin exchange heist, largely unaffected by negative sentiment in the Bitcoin market. Figure 3.8 illustrates the dynamic connectedness among CFGI, Bitcoin, Ethereum, and Binance Coin. The connection between Bitcoin and CFGI is considerably stronger than that between CFGI and either Ethereum or Binance Coin. This suggests that Bitcoin market sentiment exerts a relatively limited influence on Ethereum and Binance Coin, whose market volatility is primarily driven by endogenous factors.

Figure 3.8: Dynamic net connectedness plot between CFGI and BP, EP, and BCP



The data range is from September 25, 2020 to December 23, 2020.

In summary, the findings support Hypothesis *H3*. The connectedness test results continue to show that the predictive relationship between Bitcoin price and CFGI becomes stronger during cryptocurrency heists that specifically target Bitcoin. However, the predictive impact of CFGI on other major cryptocurrencies, such as Ethereum and Binance Coin, appears to be less pronounced. While CFGI can assist investors in making short-term trading decisions for Bitcoin during Bitcoin-specific heists, its applicability to other cryptocurrencies remains limited. Relying solely on CFGI may therefore lead investors with diversified cryptocurrency portfolios to draw misleading inferences.

3.5 Conclusion

Cryptocurrency heists expose platform vulnerabilities, undermine investor confidence, and destabilise markets. However, they offer a unique opportunity to examine the interplay between price dynamics and market sentiment. As Bitcoin is the largest cryptocurrency by market capitalisation, cryptocurrency heists targeting it are even more worthy of our attention.

This chapter uses the Crypto Fear & Greed Index (CFGI) as a proxy for market sentiment to examine the predictive relationship between Bitcoin price and sentiment, focusing on the KuCoin exchange heist, which involved the theft of a large amount of Bitcoin. The findings reveal a dynamic predictive relationship between Bitcoin price and sentiment, particularly during periods of market disruption. Before the KuCoin exchange heist, no statistically significant bidirectional predictive relationship is observed. However, in the aftermath, a statistically significant bidirectional predictive relationship emerges. While sentiment may have a limited influence on price under normal market conditions, it becomes a pivotal driver during crises. Furthermore, price fluctuations can amplify shifts in sentiment, creating a reinforcing feedback loop (Bourghelle et al., 2022). These findings underscore the importance of understanding this dynamic relationship, particularly for investors developing strategies to navigate potential market disruptions.

This chapter further examines nine additional cryptocurrency heists to assess whether the observed predictive relationship between Bitcoin price and CFGI represents a general pattern or one specific to events that directly affect the Bitcoin market. The results indicate that this predictive relationship largely depends on the extent to which a cryptocurrency heist impacts the Bitcoin market. When a heist has little or no influence on Bitcoin, no statistically significant bidirectional predictive relationship is observed between Bitcoin price and sentiment. In a market environment where cryptocurrency heists occur frequently, investors should carefully assess the extent to which such incidents affect the Bitcoin market before relying on CFGI to guide their investment strategies.

Additionally, this chapter examines the spillover effects of the CFGI on other cryptocurrency markets during the KuCoin exchange heist. The findings indicate that the turmoil in Bitcoin sentiment caused by the heist does not significantly affect other cryptocurrency markets, such as Ethereum and Binance Coin. This suggests that the negative sentiment in the Bitcoin market resulting from the heist may not immediately influence other cryptocurrencies, due to factors such as differences in investor perceptions of various cryptocurrencies and the

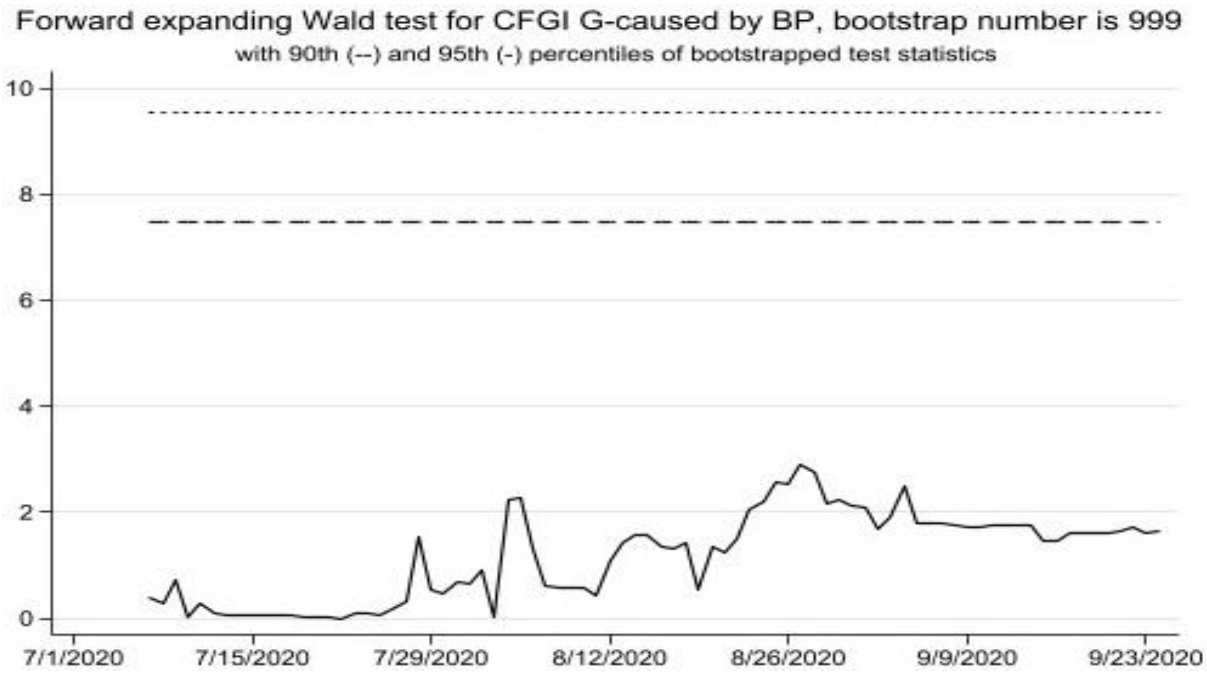
technological distinctions between blockchains (Victor & Weintraud, 2021; Li et al., 2024). The findings highlight that during Bitcoin-targeted heists, relying solely on CFGI may lead investors with diversified cryptocurrency portfolios to draw misleading conclusions.

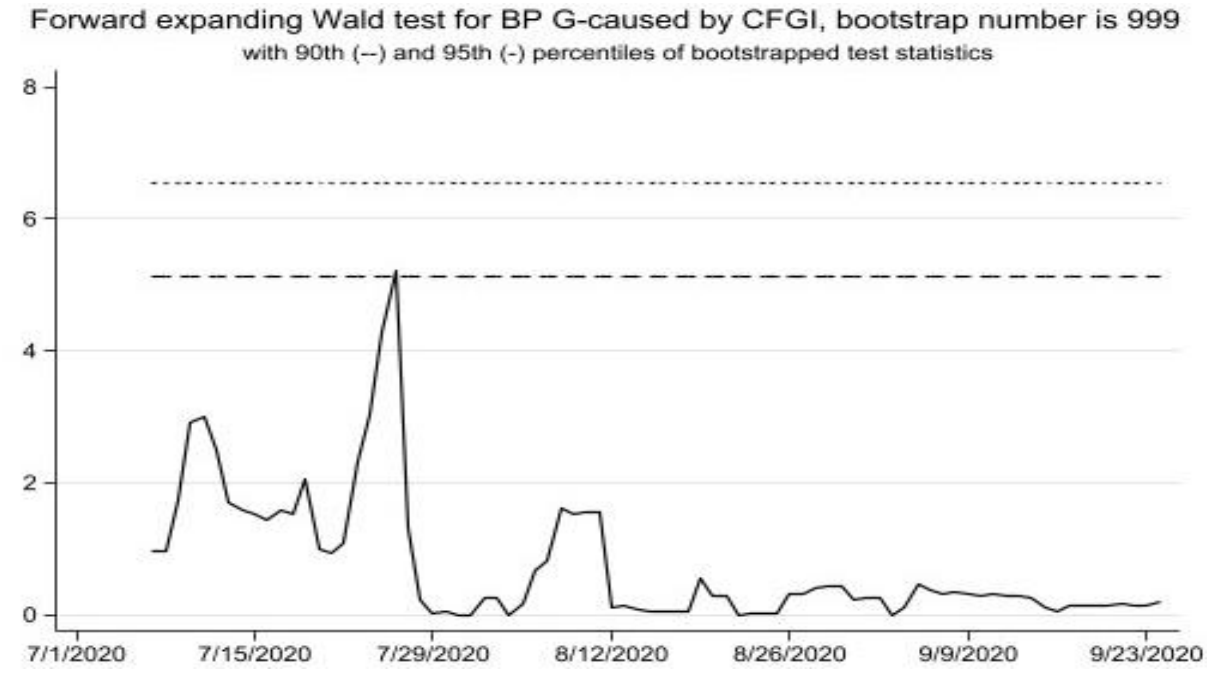
This study deepens our understanding of the predictive relationship between Bitcoin price and market sentiment under extreme market conditions. However, several limitations remain. First, although this chapter provides evidence of changes in the predictive relationship between Bitcoin price and CFGI following the KuCoin exchange heist, the Granger causality tests employed capture predictability rather than true economic causation. As the findings are based on a single cryptocurrency heist, future studies could examine multiple Bitcoin-related heists to validate the robustness and generalisability of the results. Second, although the CFGI is a comprehensive and widely used indicator of Bitcoin sentiment, it has inherent limitations. While it discloses the weights of its six components, Alternative.me does not release its numerical values, preventing component-level analysis. Consequently, it is difficult to identify which factors primarily drive sentiment changes during major events such as cryptocurrency heists. Distinguishing between market-based and non-market-based components represents a promising direction for future study, helping clarify whether market activity factors (e.g., volatility and trading volume) or behavioural factors (e.g., social media and search trends) dominate the predictive relationship between Bitcoin price and sentiment. Future studies could address this limitation by using sentiment measures that allow component-level analysis or by constructing decomposed sentiment indices to capture heterogeneous sentiment drivers.

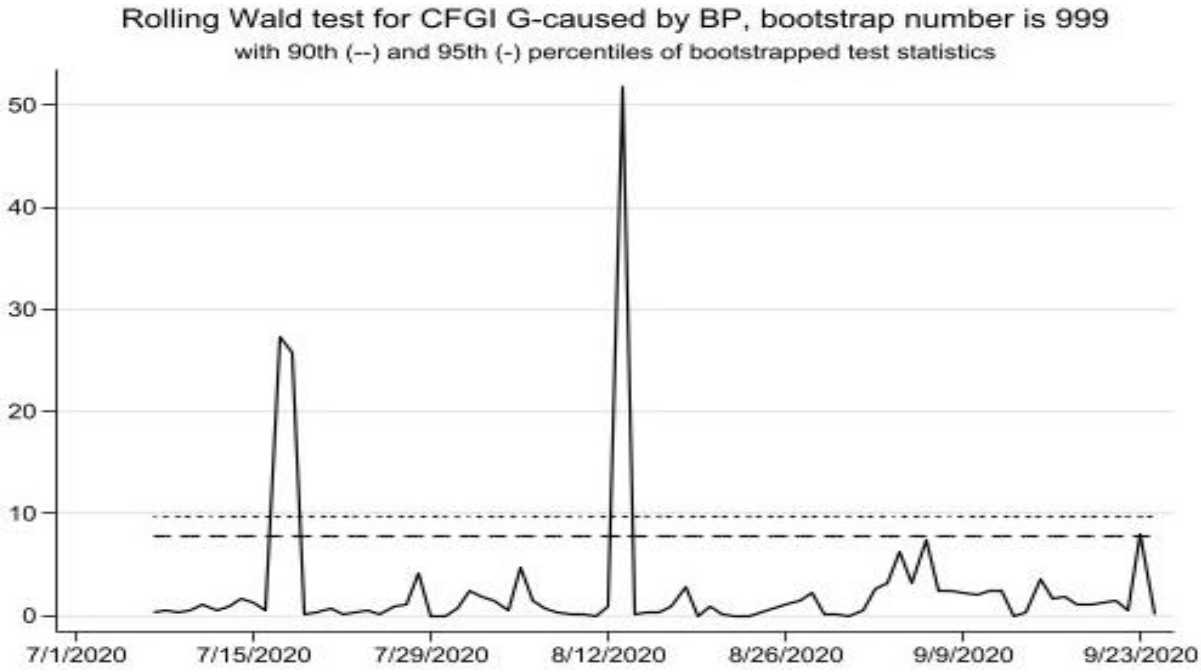
Moreover, future studies could explore alternative sentiment indicators. For instance, CoinMarketCap introduced the CMC Crypto Fear and Greed Index (CMC) in 2023, which measures sentiment across the entire cryptocurrency market rather than focusing solely on Bitcoin. Comparing the predictive performance of CMC and CFGI during extreme events would provide valuable insights. Finally, while this chapter focuses on the predictive relationship between CFGI and other cryptocurrencies during the KuCoin heist, future work could extend the analysis to other cryptocurrency heists to examine sentiment–price dynamics across a wider range of cryptocurrencies, offering a deeper understanding of sentiment's broader relevance in cryptocurrency markets.

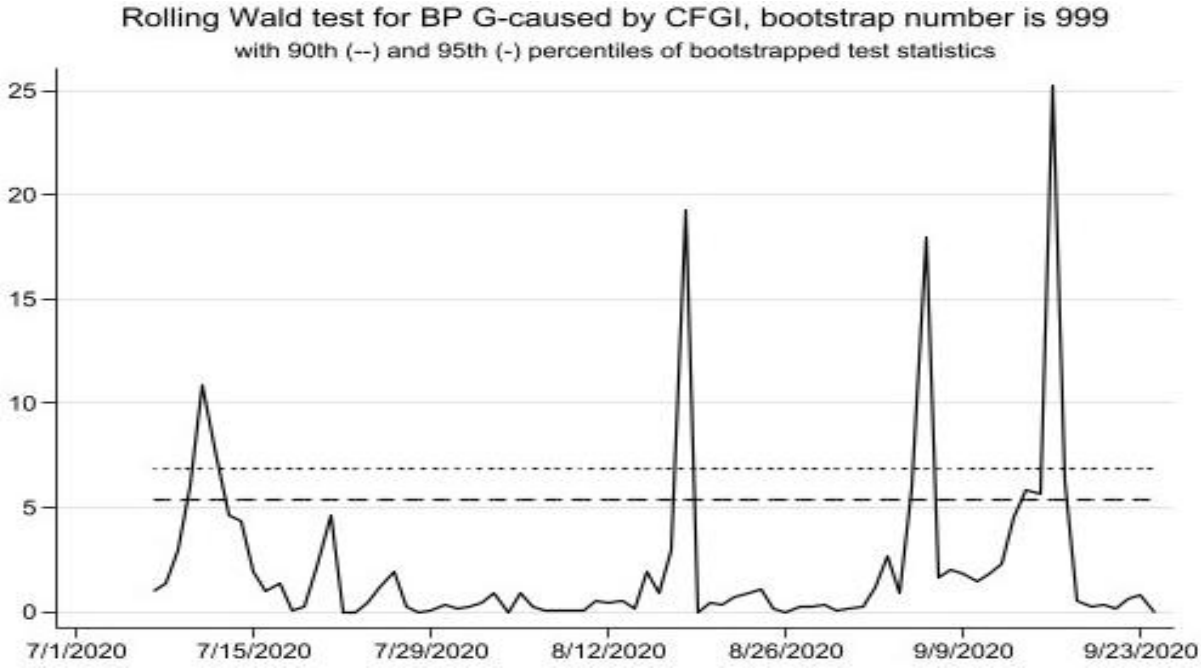
3.6 Appendix

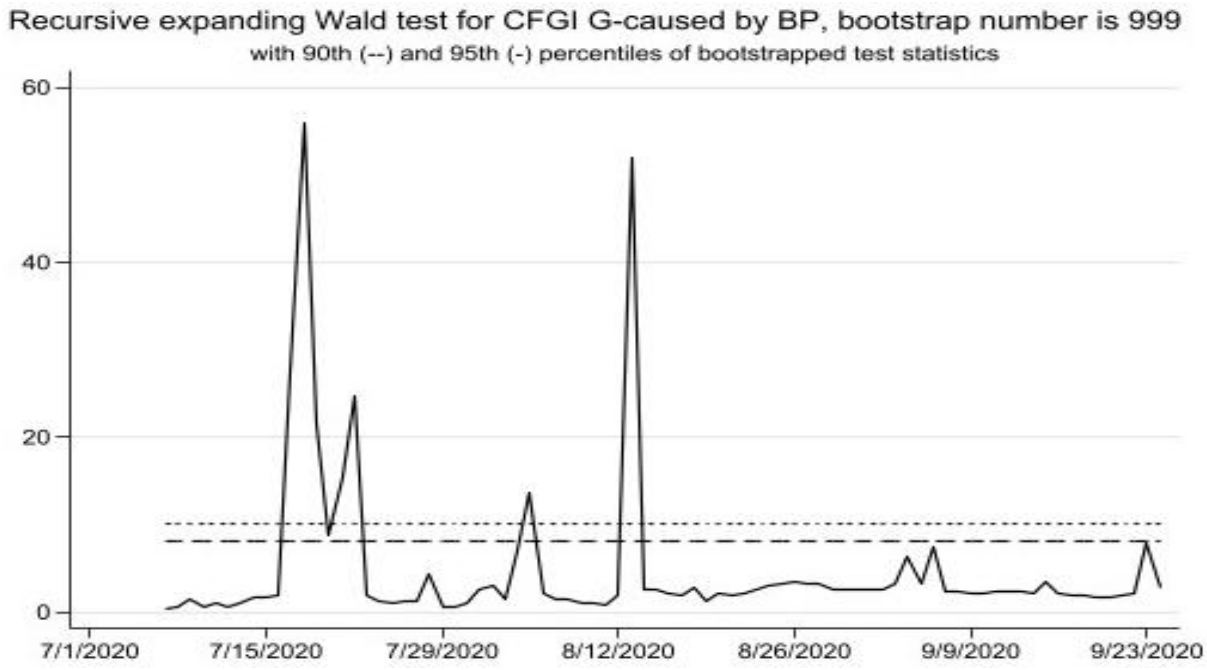
Figure 3.9: Time-varying Granger causality test results before the KuCoin exchange heist (window size = 10, using 10% of the sample, with 999 bootstrap repetitions)

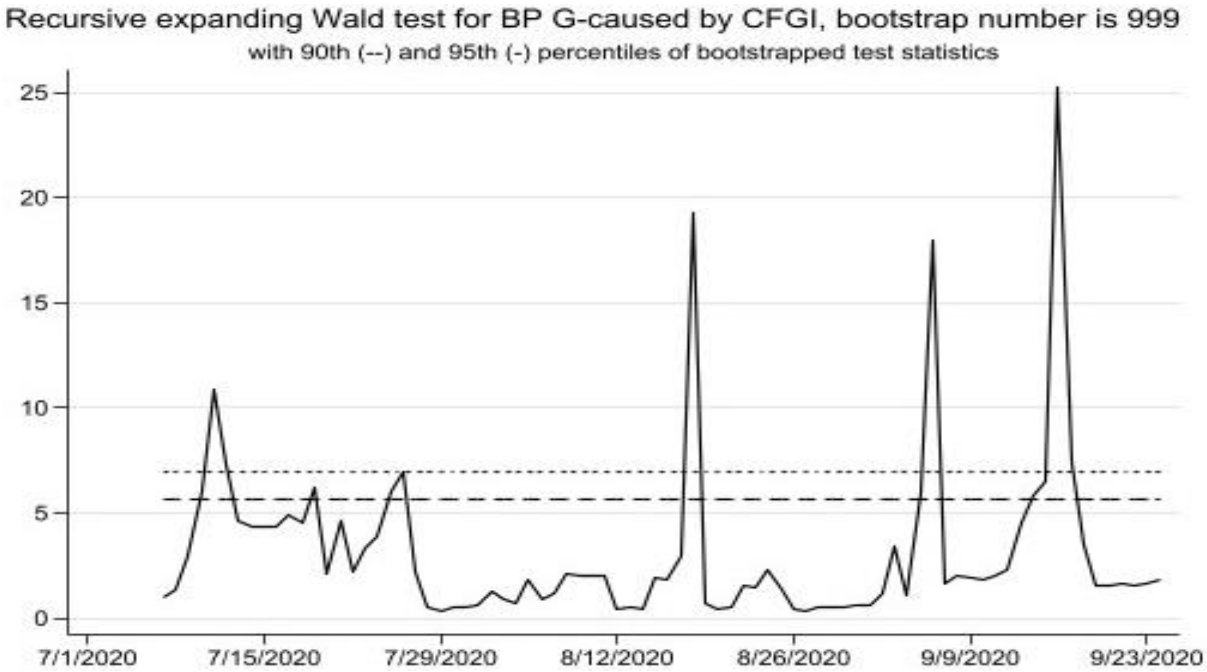





Rolling Wald test for CFGI G-caused by BP, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
50
40
30
20
10
0
7/1/2020
7/15/2020
7/29/2020
8/12/2020
8/26/2020
9/9/2020
9/23/2020

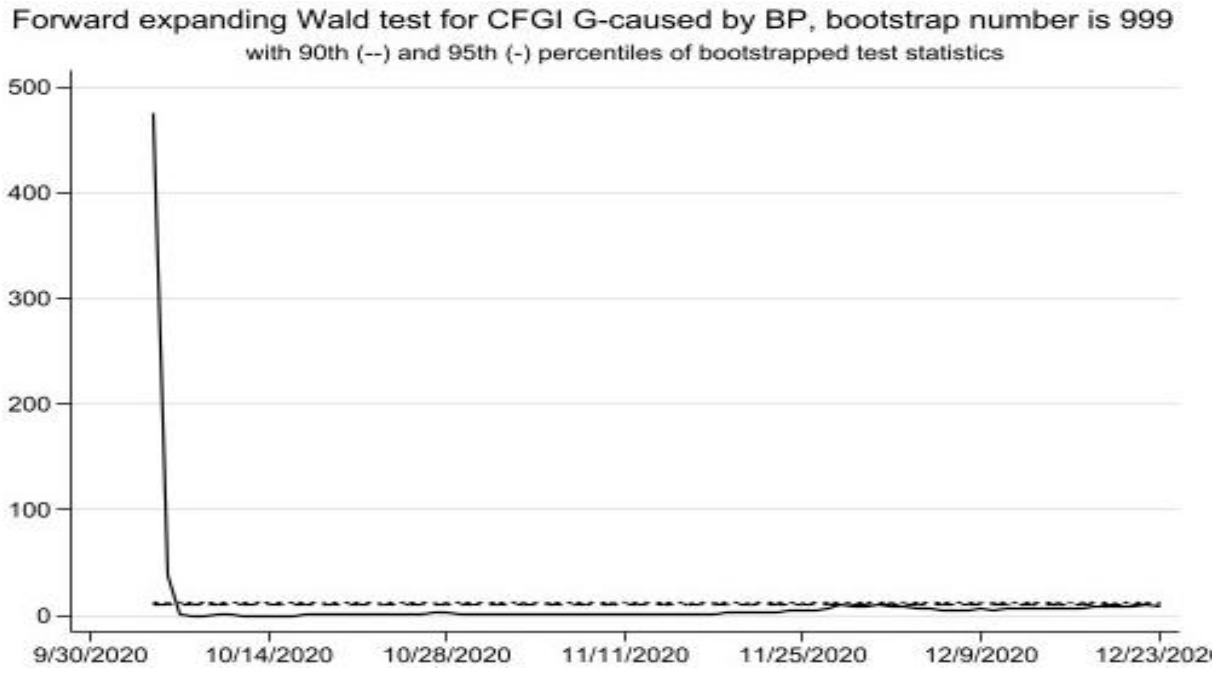

Rolling Wald test for BP G-caused by CFGI, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
25
20
15
10
5
0
7/1/2020
7/15/2020
7/29/2020
8/12/2020
8/26/2020
9/9/2020
9/23/2020

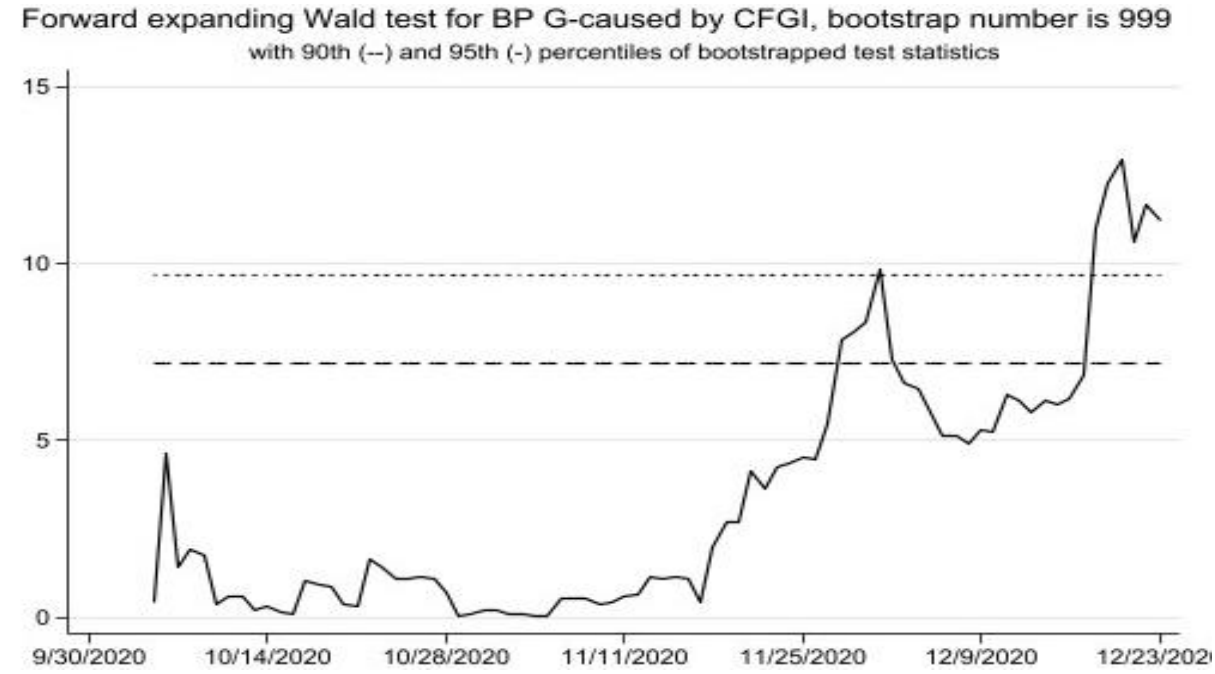


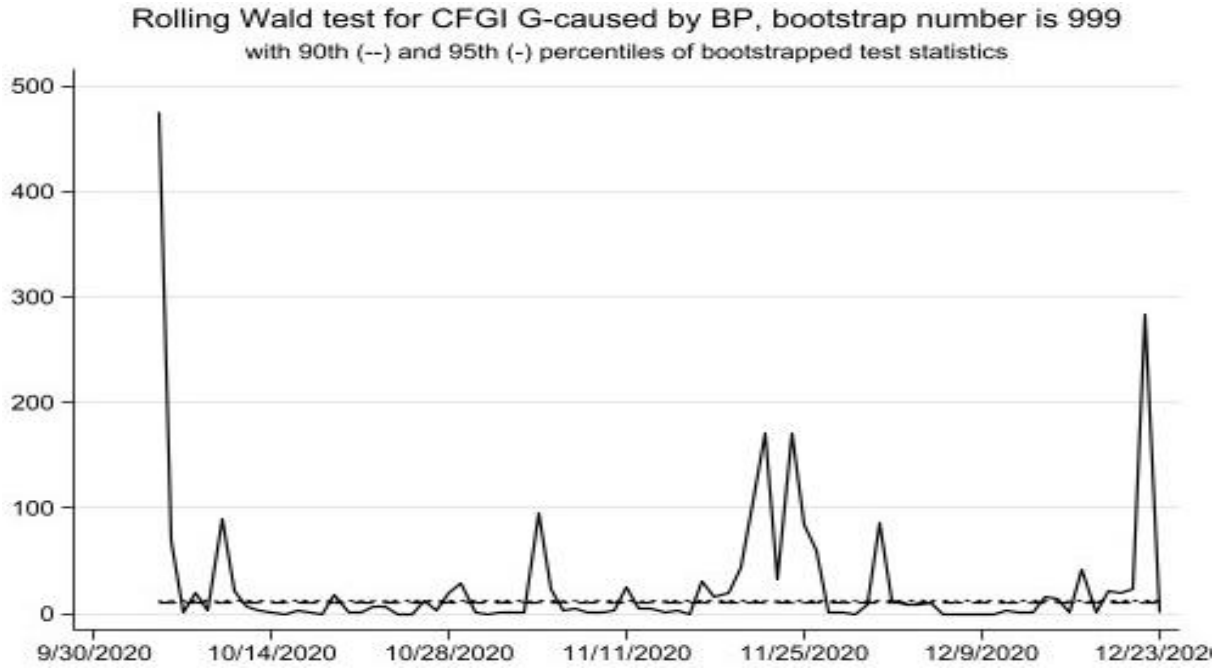


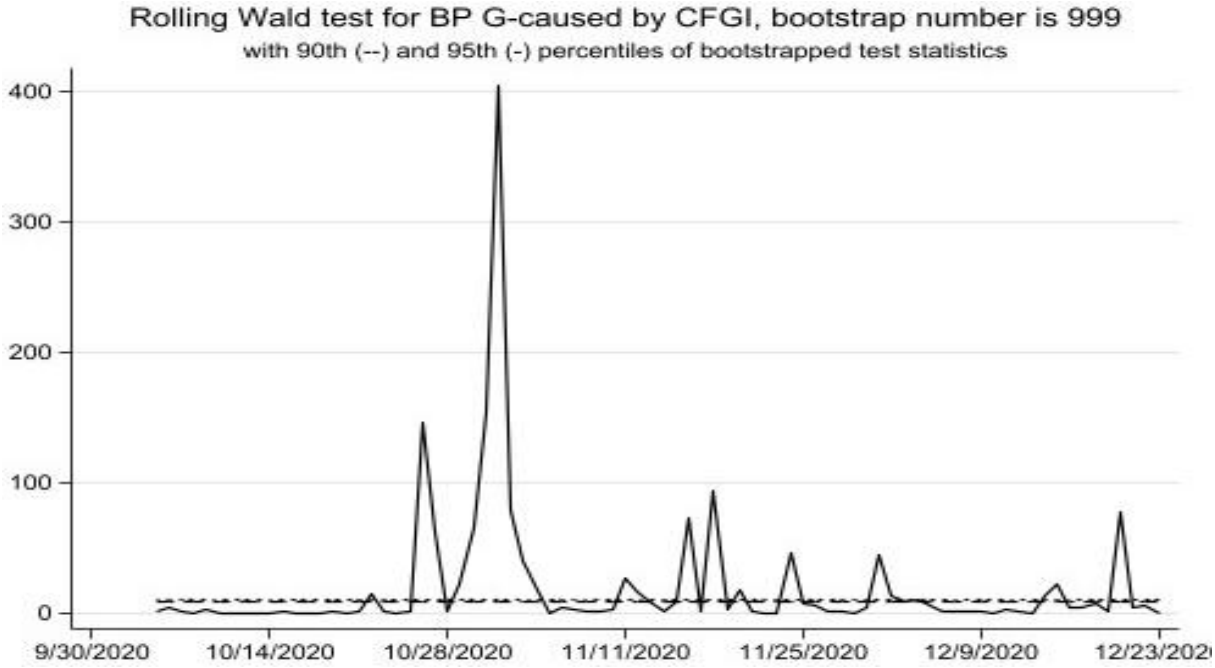
The rolling window size is 10, and the bootstrap repetition is 999. The dashed line represents the 95th percentile of the bootstrapped test statistics, while the dotted line corresponds to the 90th percentile. When the test statistic exceeds these critical values, the null hypothesis is rejected at the corresponding significance level, indicating that Bitcoin price Granger causes CFGI (or CFGI Granger causes Bitcoin price) during those periods.

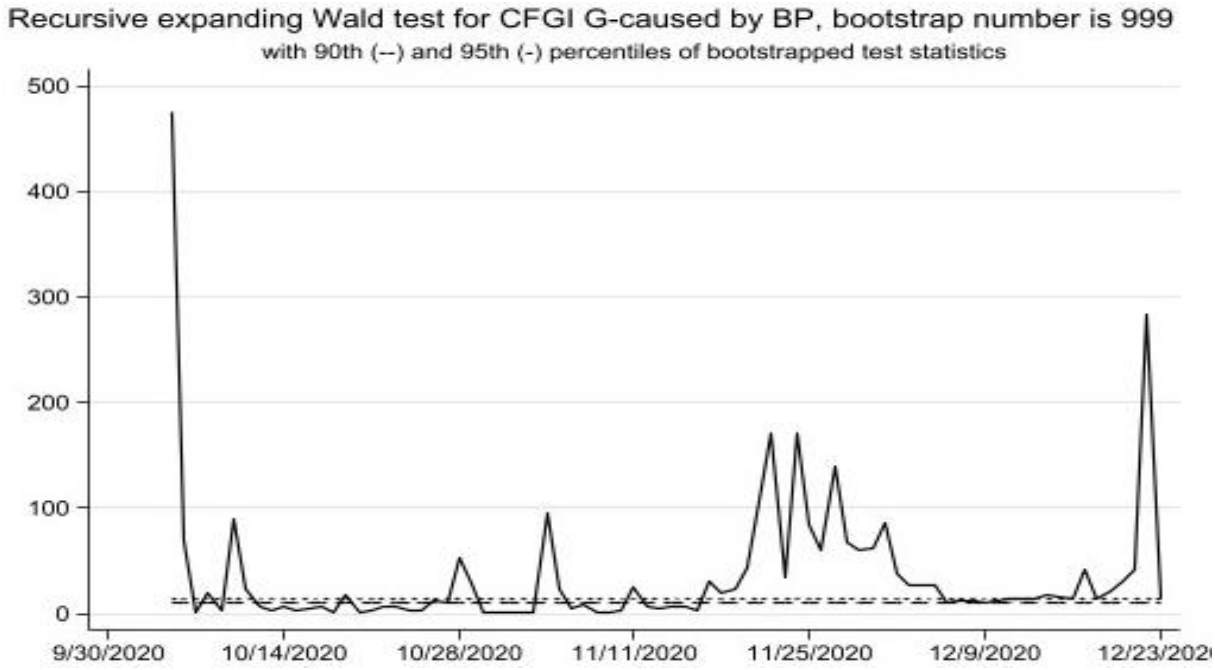
Figure 3.10: Time-varying Granger causality test results after the KuCoin exchange heist (window size = 10, using 10% of the sample, with 999 bootstrap repetitions)

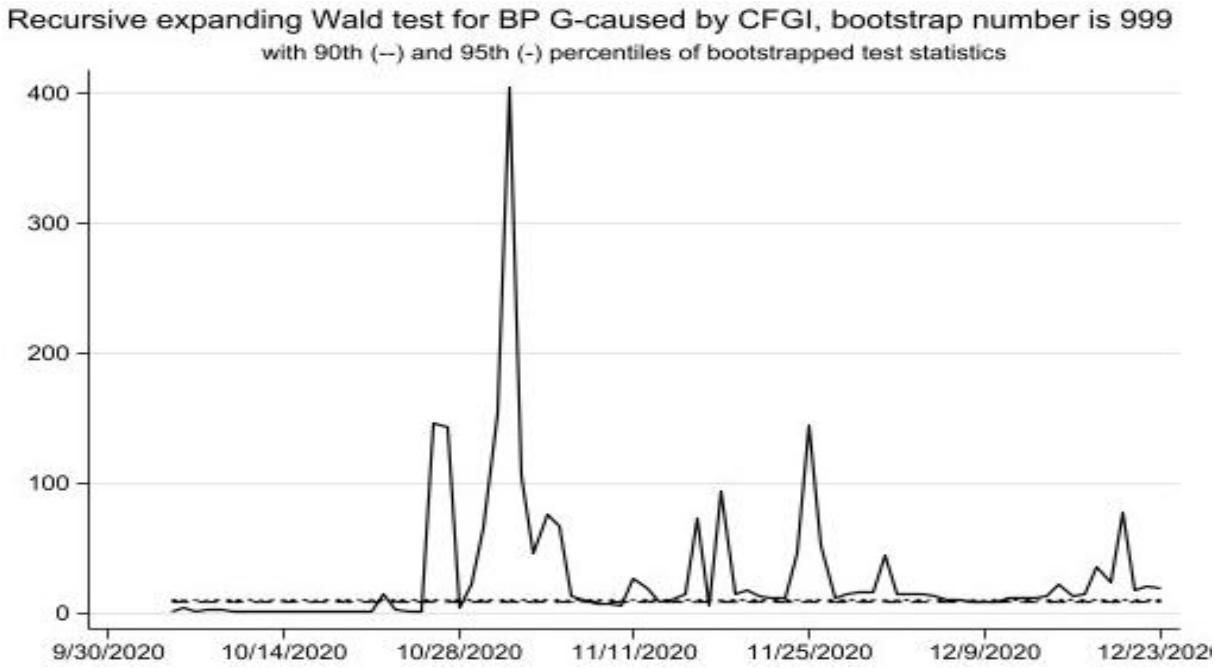





Rolling Wald test for CFGI G-caused by BP, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
500
400
300
200
100
0
9/30/2020
10/14/2020
10/28/2020
11/11/2020
11/25/2020
12/9/2020

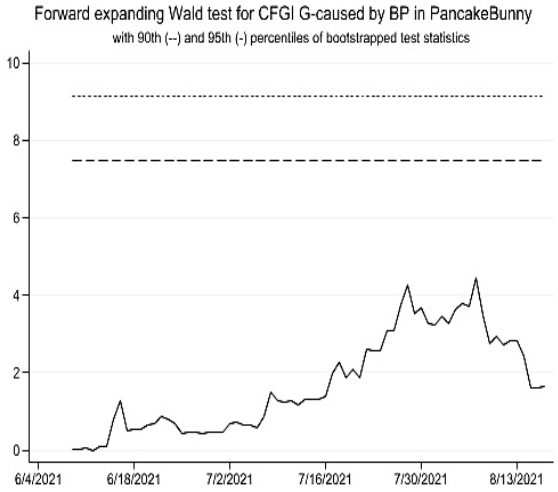

Rolling Wald test for BP G-caused by CFGI, bootstrap number is 999
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
400
300
200
100
0
9/30/2020
10/14/2020
10/28/2020
11/11/2020
11/25/2020
12/9/2020

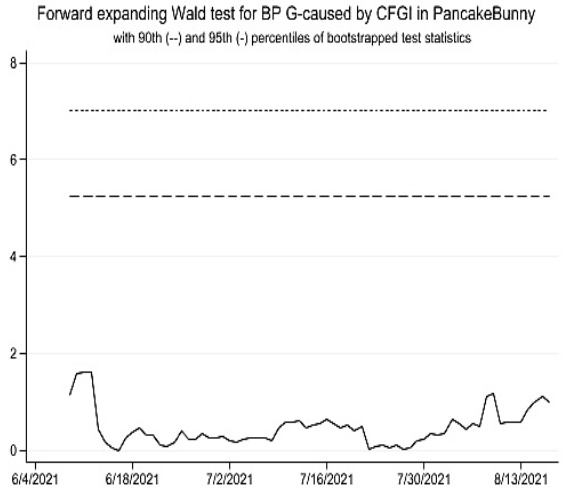


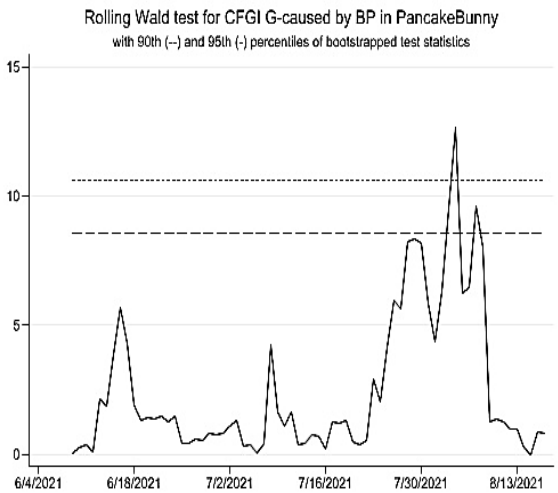


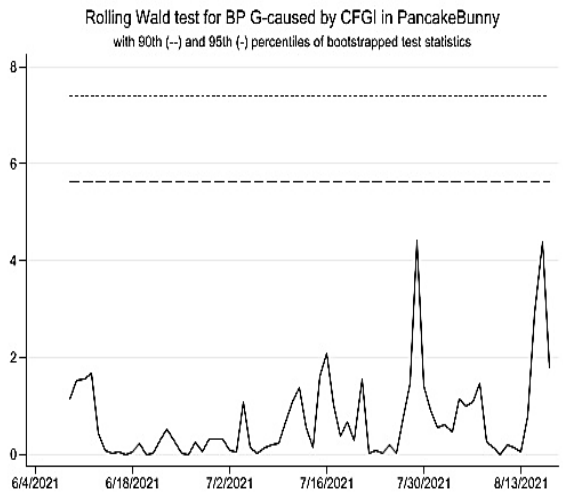
The rolling window size is 10, and the bootstrap repetition is 999. The dashed line represents the 95th percentile of the bootstrapped test statistics, while the dotted line corresponds to the 90th percentile. When the test statistic exceeds these critical values, the null hypothesis is rejected at the corresponding significance level, indicating that Bitcoin price Granger causes CFGI (or CFGI Granger causes Bitcoin price) during those periods.

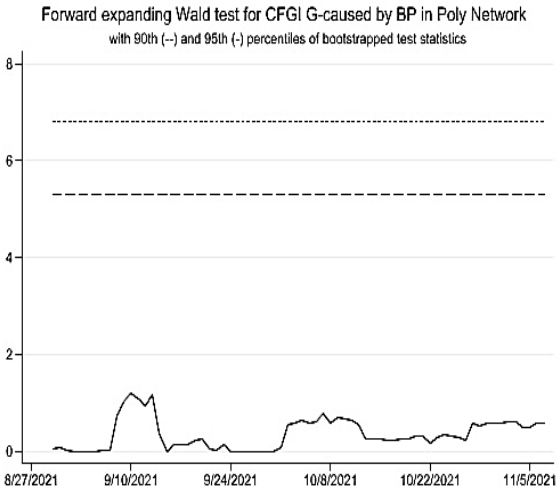
Figure 3.11: Time-varying Granger causality between BP and CFGI using the *FE* and *RO* algorithms across nine cryptocurrency heists

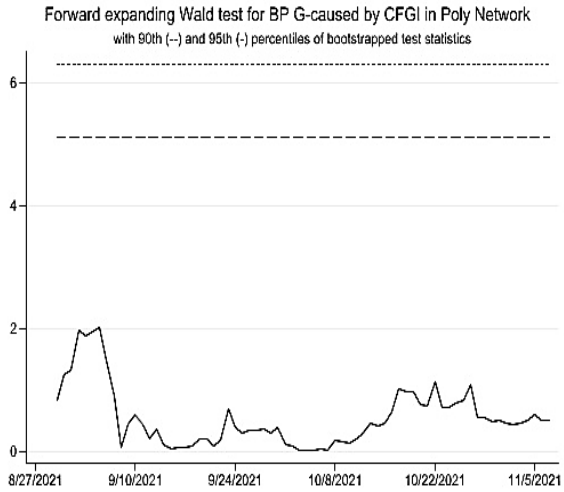


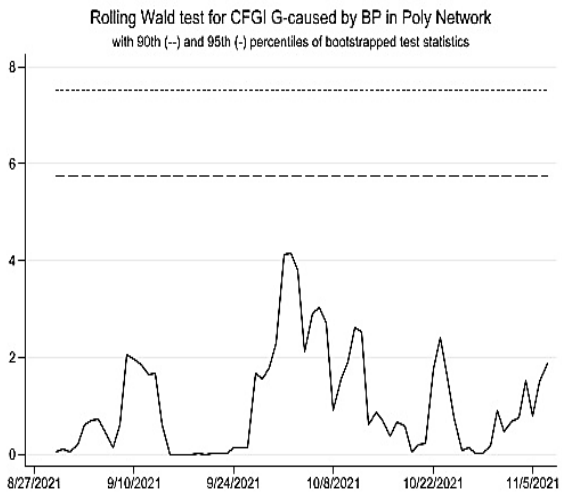


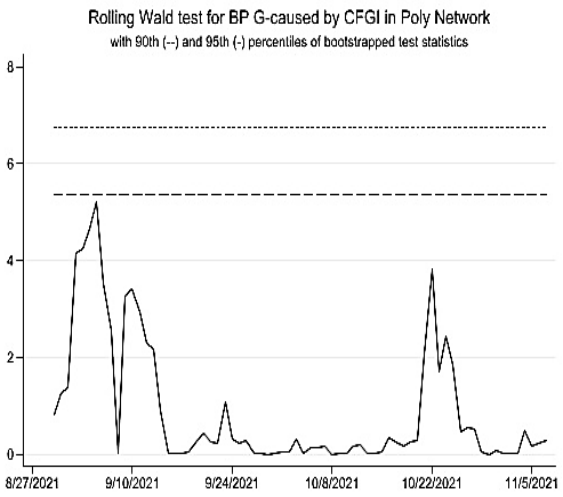


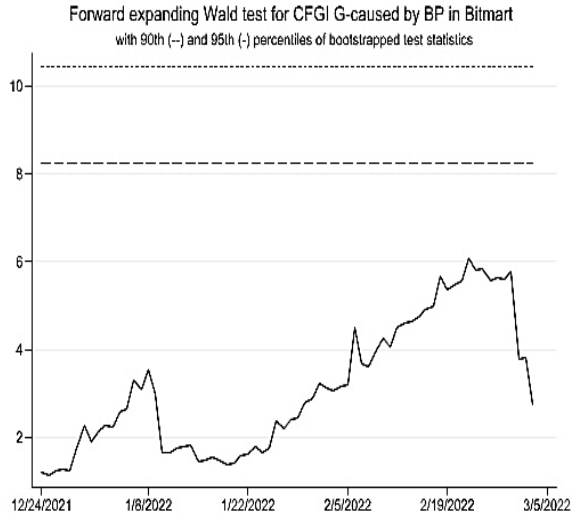


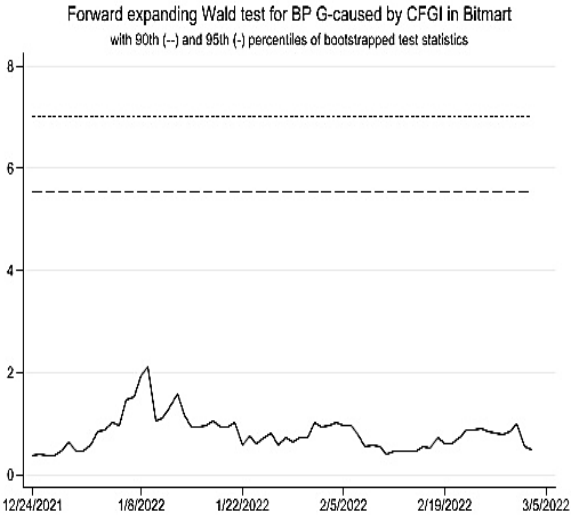


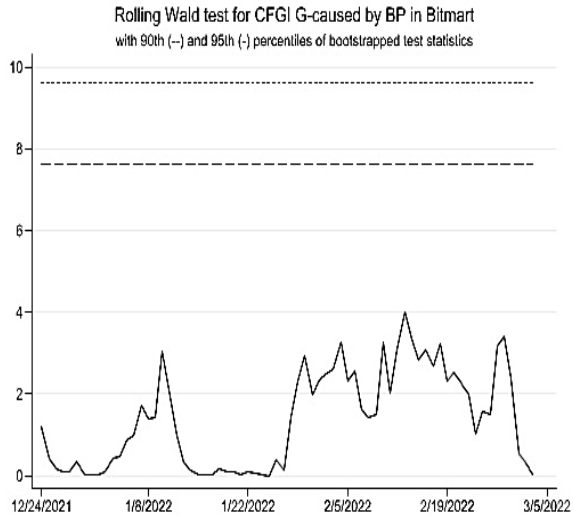


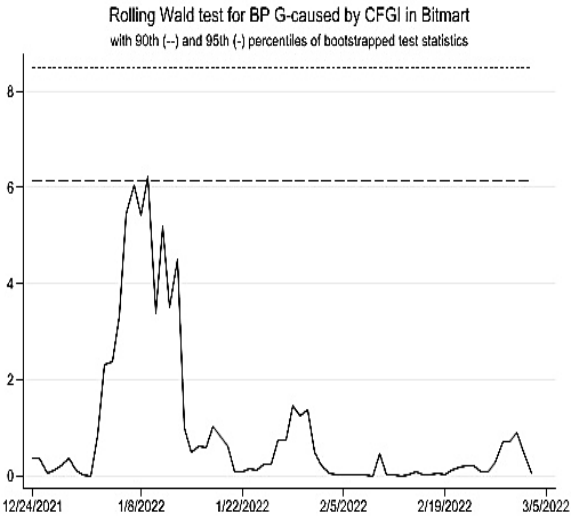

Rolling Wald test for CFGI G-caused by BP in Poly Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
8/27/2021
9/10/2021
9/24/2021
10/8/2021
10/22/2021
11/5/2021

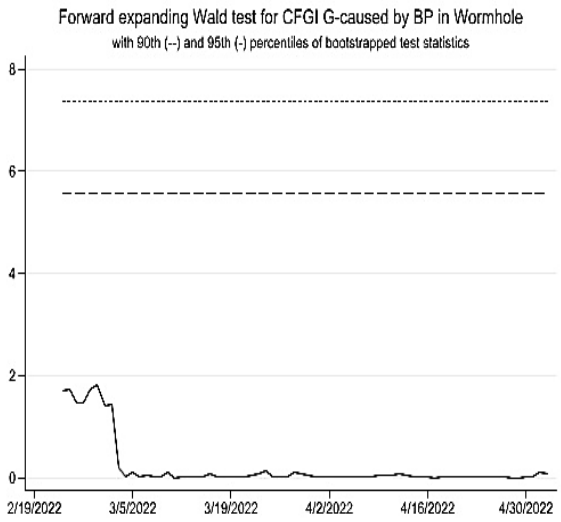

Rolling Wald test for BP G-caused by CFGI in Poly Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
8/27/2021
9/10/2021
9/24/2021
10/8/2021
10/22/2021
11/5/2021

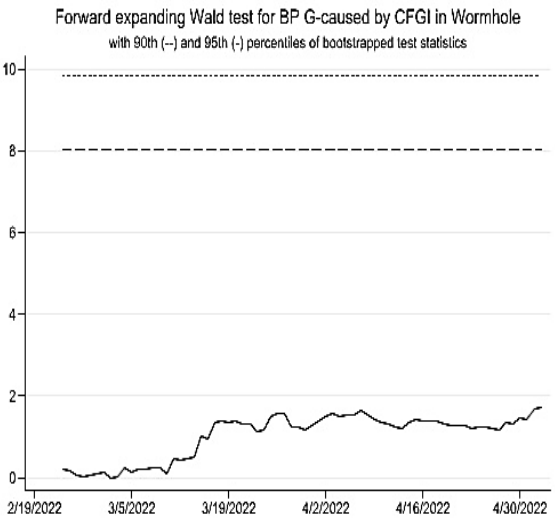

Forward expanding Wald test for CFGI G-caused by BP in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

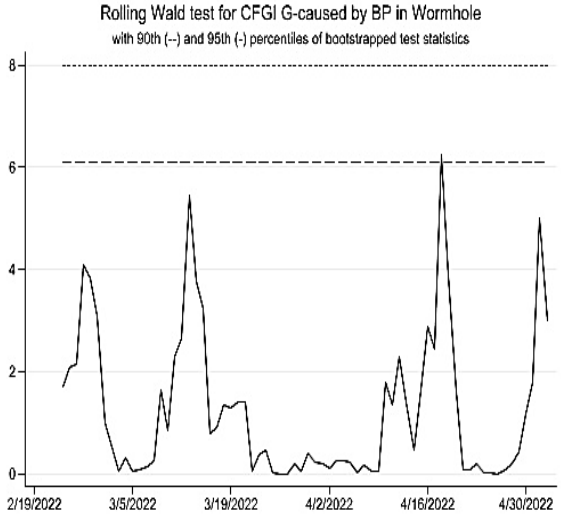

Forward expanding Wald test for BP G-caused by CFGI in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

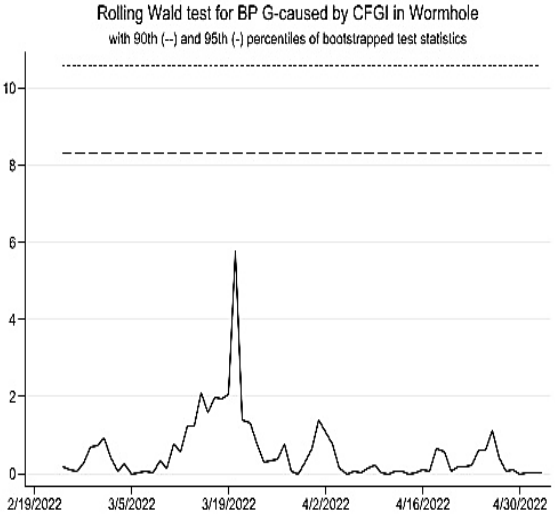

Rolling Wald test for CFGI G-caused by BP in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
10
8
6
4
2
0
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

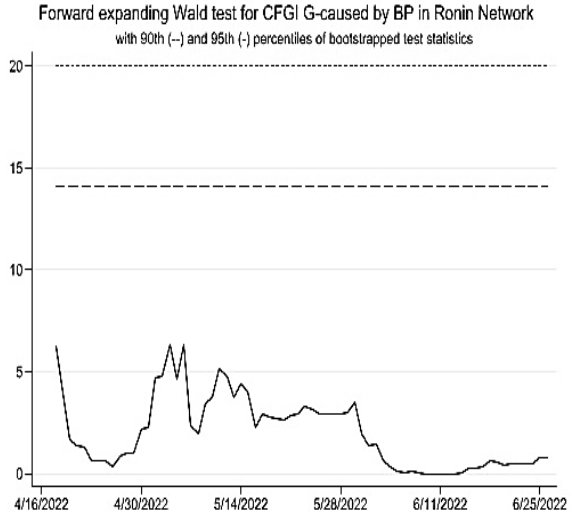

Rolling Wald test for BP G-caused by CFGI in Bitmart
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
12/24/2021
1/8/2022
1/22/2022
2/5/2022
2/19/2022
3/5/2022

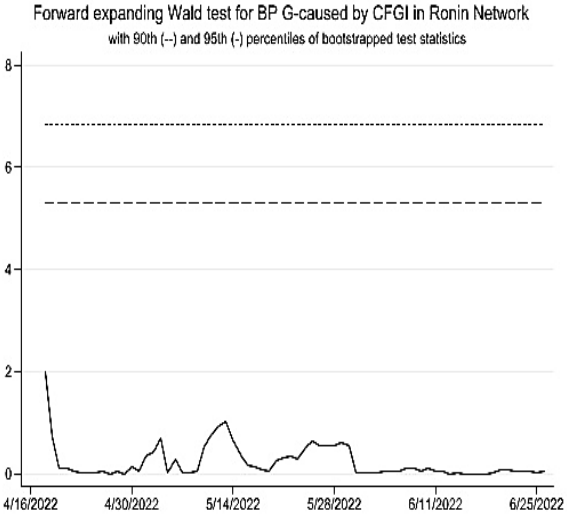

Forward expanding Wald test for CFGI G-caused by BP in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
2
4
6
8
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

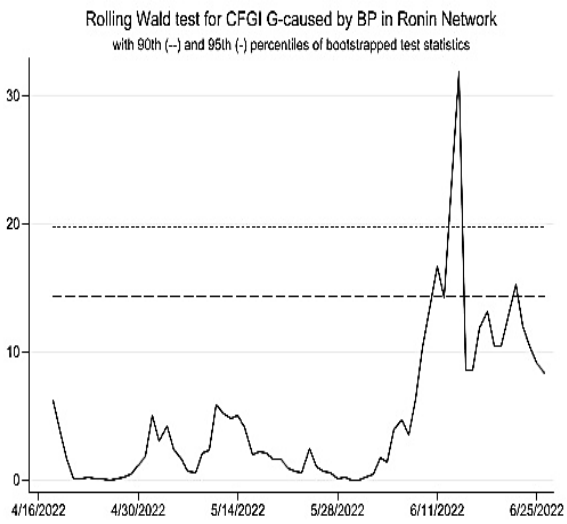

Forward expanding Wald test for BP G-caused by CFGI in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
2
4
6
8
10
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

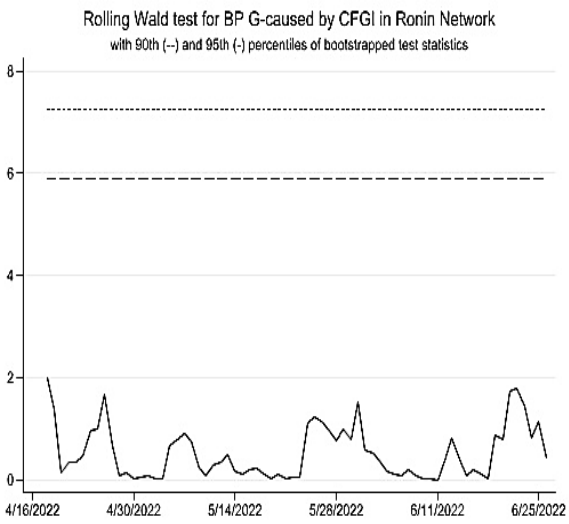

Rolling Wald test for CFGI G-caused by BP in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
2
4
6
8
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

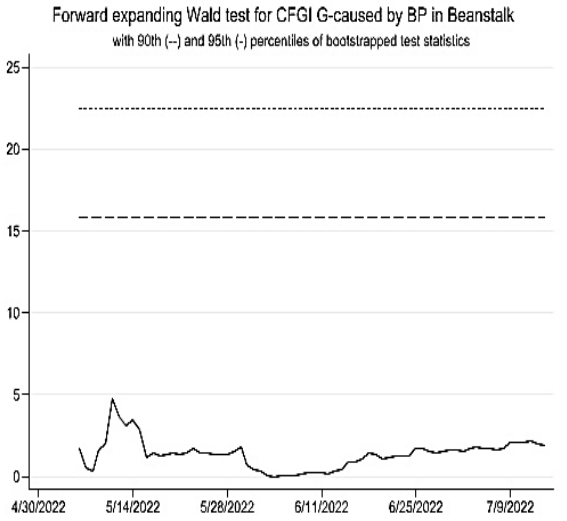

Rolling Wald test for BP G-caused by CFGI in Wormhole
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
2
4
6
8
10
2/19/2022
3/5/2022
3/19/2022
4/2/2022
4/16/2022
4/30/2022

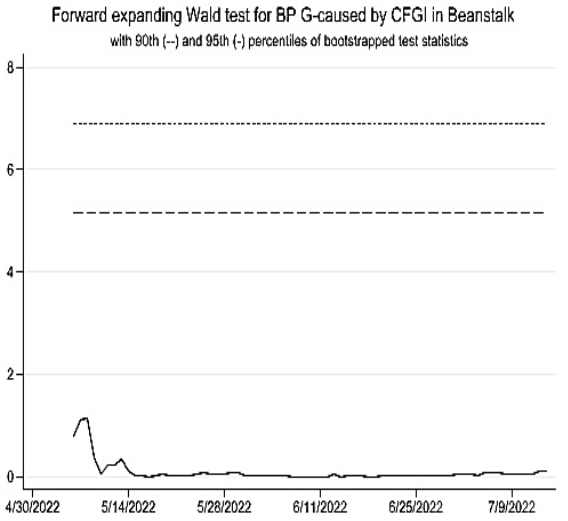

Forward expanding Wald test for CFGI G-caused by BP in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
5
10
15
20
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

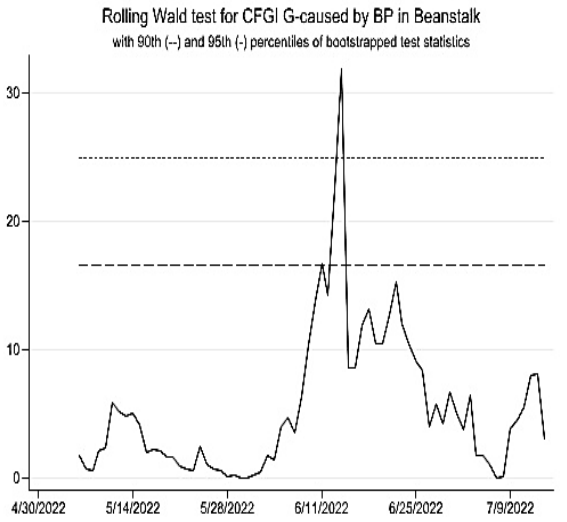

Forward expanding Wald test for BP G-caused by CFGI in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
0
2
4
6
8
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

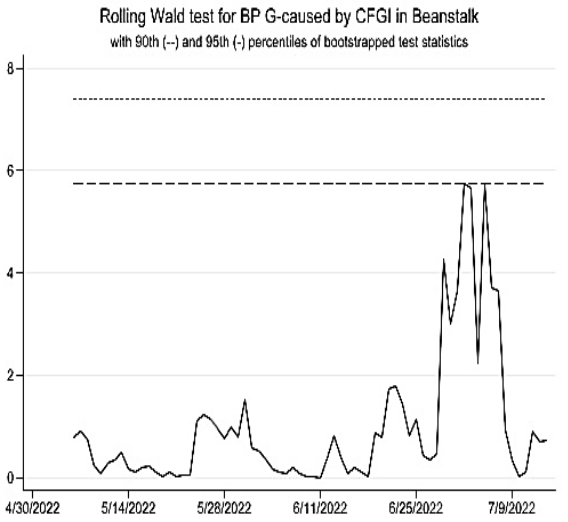

Rolling Wald test for CFGI G-caused by BP in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

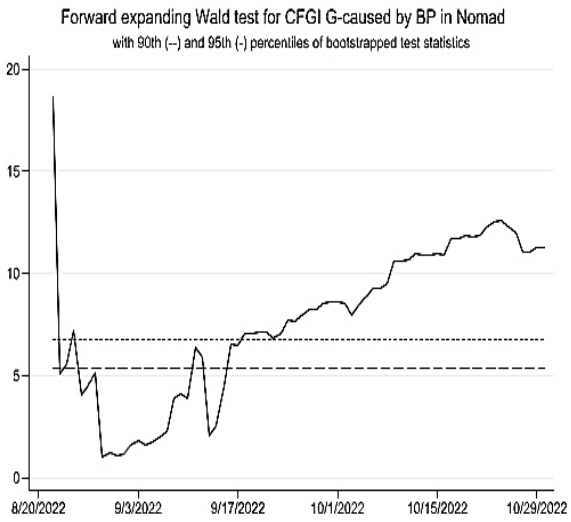

Rolling Wald test for BP G-caused by CFGI in Ronin Network
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
4/16/2022
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022

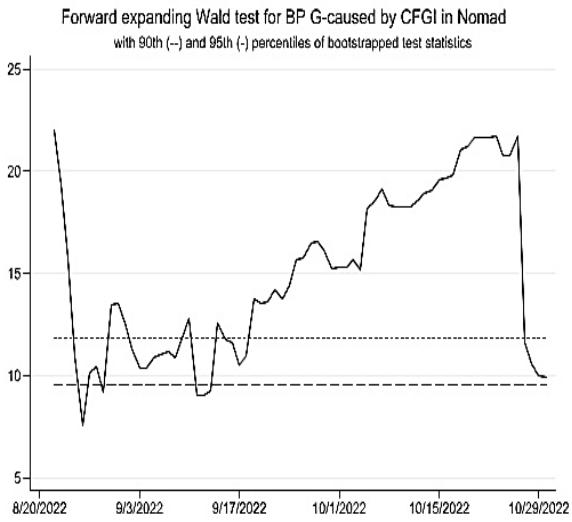

Forward expanding Wald test for CFGI G-caused by BP in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
25
20
15
10
5
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

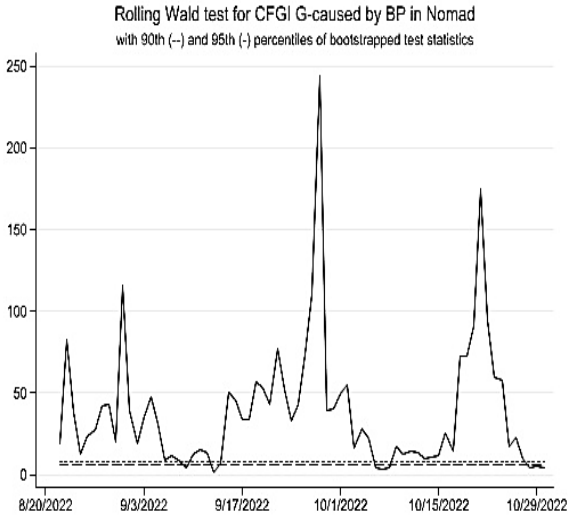

Forward expanding Wald test for BP G-caused by CFGI in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

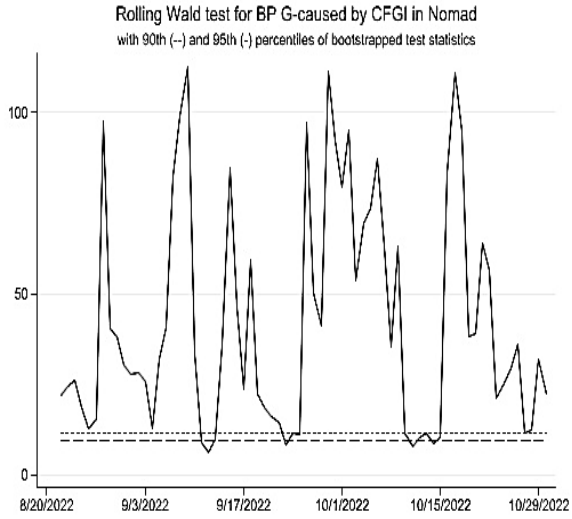

Rolling Wald test for CFGI G-caused by BP in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

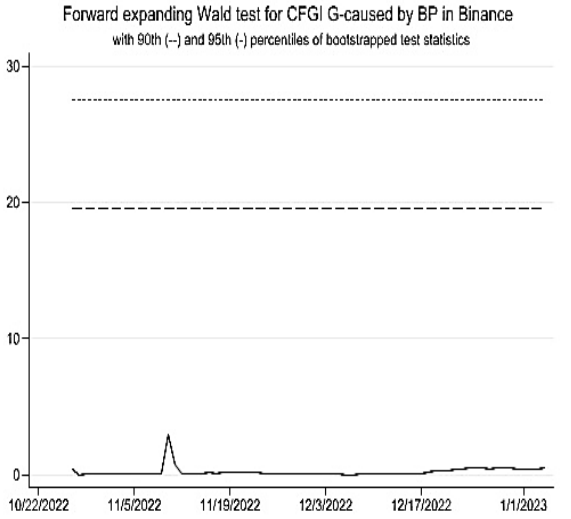

Rolling Wald test for BP G-caused by CFGI in Beanstalk
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
4/30/2022
5/14/2022
5/28/2022
6/11/2022
6/25/2022
7/9/2022

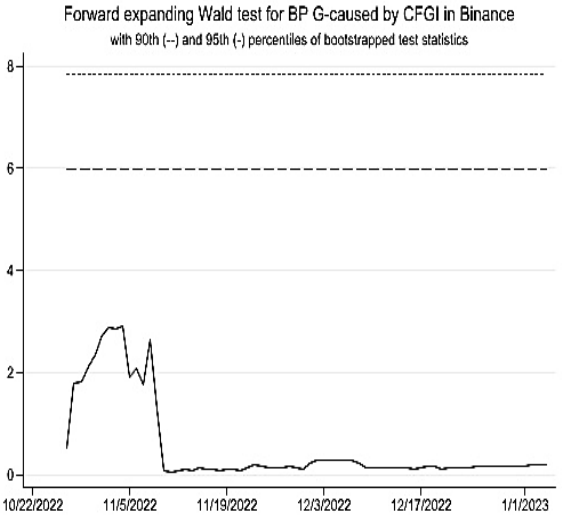

Forward expanding Wald test for CFGI G-caused by BP in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
20
15
10
5
0
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022

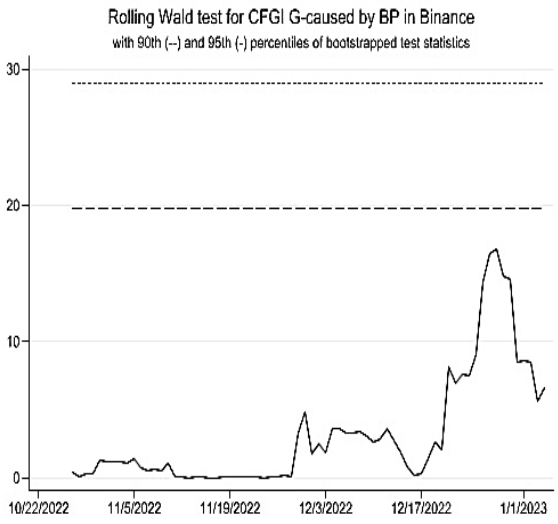

Forward expanding Wald test for BP G-caused by CFGI in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
25
20
15
10
5
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022

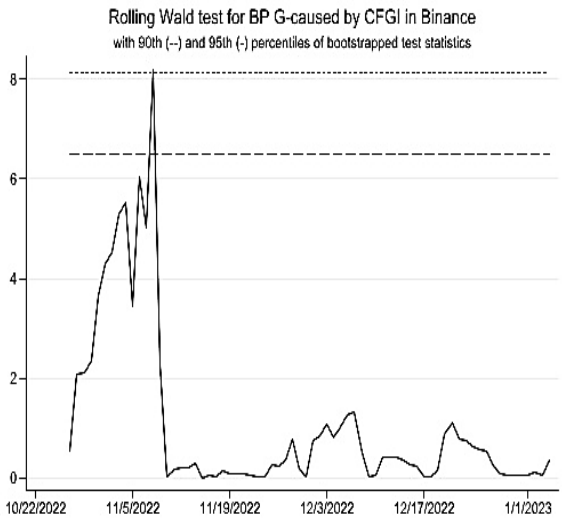

Rolling Wald test for CFGI G-caused by BP in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
250
200
150
100
50
0
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022

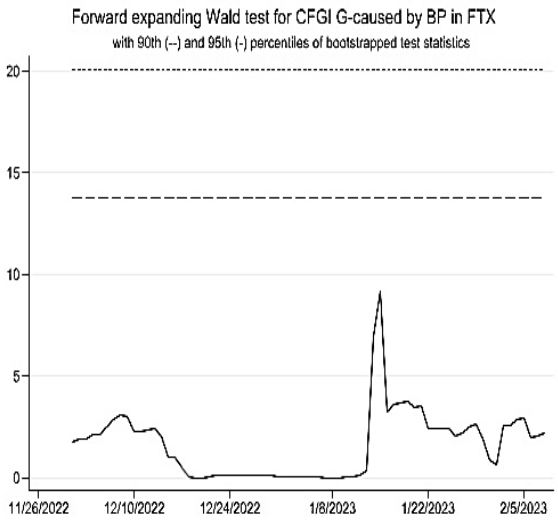

Rolling Wald test for BP G-caused by CFGI in Nomad
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
100
50
0
8/20/2022
9/3/2022
9/17/2022
10/1/2022
10/15/2022
10/29/2022

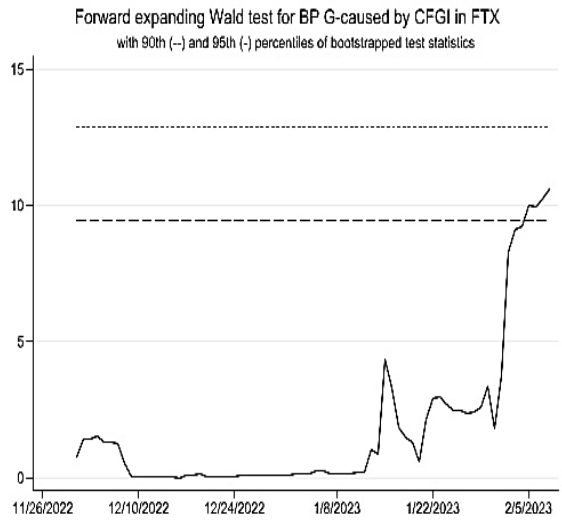

Forward expanding Wald test for CFGI G-caused by BP in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023

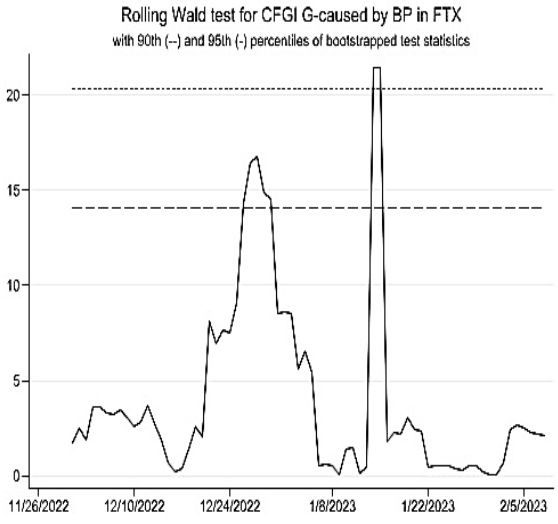

Forward expanding Wald test for BP G-caused by CFGI in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023

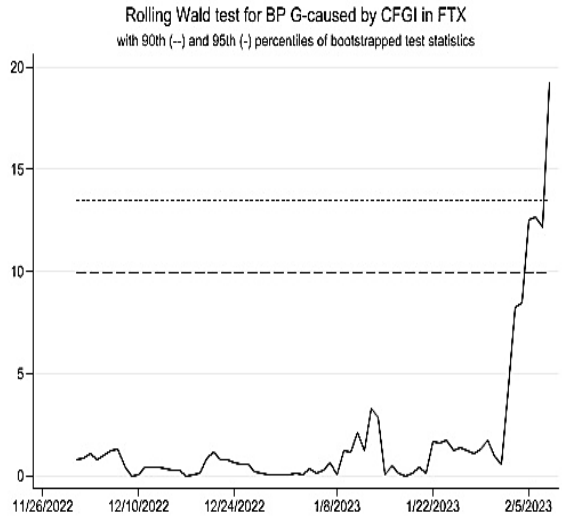

Rolling Wald test for CFGI G-caused by BP in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
30
20
10
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023


Rolling Wald test for BP G-caused by CFGI in Binance
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
8
6
4
2
0
10/22/2022
11/5/2022
11/19/2022
12/3/2022
12/17/2022
1/1/2023


Forward expanding Wald test for CFGI G-caused by BP in FTX
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
20
15
10
5
0
11/26/2022
12/10/2022
12/24/2022
1/8/2023
1/22/2023
2/5/2023


Forward expanding Wald test for BP G-caused by CFGI in FTX
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
15
10
5
0
11/26/2022
12/10/2022
12/24/2022
1/8/2023
1/22/2023
2/5/2023


Rolling Wald test for CFGI G-caused by BP in FTX
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
20
15
10
5
0
11/26/2022
12/10/2022
12/24/2022
1/8/2023
1/22/2023
2/5/2023


Rolling Wald test for BP G-caused by CFGI in FTX
with 90th (--) and 95th (-) percentiles of bootstrapped test statistics
20
15
10
5
0
11/26/2022
12/10/2022
12/24/2022
1/8/2023
1/22/2023
2/5/2023

Chapter 4 The Impact of Major DeFi Heists on DeFi Token Liquidity and Market Stability

4.1 Introduction

Decentralised Finance (DeFi) leverages the transparency, security, and decentralised nature of blockchain technology, combined with the use of cryptocurrencies, to facilitate financial transactions without the need for centralised institutions. Through peer-to-peer financial networks, DeFi provides online wallets, lending, spot trading, margin trading, market making, and derivatives (Chen & Bellavitis, 2019; Corbet et al., 2023). For example, users can borrow stablecoins using any cryptocurrency as collateral to place leveraged bets on certain cryptocurrencies; conversely, users can also earn interest by lending out stablecoins. Most DeFi protocols and applications are built on Ethereum, with users participating in DeFi through decentralised applications (dapps)[5]. DeFi applications cover various aspects of financial services, promising higher efficiency, lower costs, and greater inclusivity (Schär, 2021). By February 2025, the total value of assets locked in DeFi protocols reached $97.91 billion, a substantial increase from about $630 million at the beginning of 2020. This increase was not solely driven by rising cryptocurrency prices; the number of tokens locked also rose substantially. For example, the amount of Ethereum locked on the Ethereum chain increased from 4.73 million in early 2020 to 19.57 million in early 2025; the amount of Solana locked on the Solana chain rose from 10.4 million in early 2021 to 45.03 million in early 2025; and the amount of Avalanche locked on the Avalanche chain grew from 243,054 in early 2021 to 37.09 million in early 2025 (DeFiLlama, 2025). This dramatic growth demonstrates the exploding interest and confidence investors have in decentralised finance solutions, marking DeFi's significant position at the forefront of financial technology innovation (The Fintech Times, 2023; Alamsyah & Muhammad, 2024). With an increasing number of projects and capital flowing into this space, DeFi is expected to continue playing a key role in the global financial ecosystem, driving the decentralisation and digital transformation of traditional financial services (Alamsyah et al., 2024; Bakare et al., 2024).

[5] Decentralised applications (dapps) are autonomously running applications that typically operate on decentralised computing platforms, blockchains, or other distributed ledger systems through the use of smart contracts. Unlike traditional applications, dapps operate without human intervention and are not owned by any single entity. Instead, ownership is represented through the distribution of tokens to users, which are allocated based on programmed algorithms, thus diluting ownership and control of the dapps. As no single entity controls the system, the application remains decentralised (Wu et al., 2021).

DeFi tokens are a unique type of cryptocurrency utilised within the DeFi ecosystem, and the uses of different types of DeFi tokens vary greatly. Table 4.1 summarises the current common uses of DeFi tokens. These tokens are often based on blockchain platforms like Ethereum and follow standards such as ERC-20, facilitating easy trading and interoperability across the DeFi ecosystem (Harvey et al., 2021; Hertig, 2023). The innovation of DeFi tokens lies not just in their function as a medium of value transfer; they also empower users to participate in and influence the development of DeFi protocols. This marks a significant departure from traditional financial instruments like stocks or bonds, highlighting their unique position in the financial world (Metelski & Sobieraj, 2022).

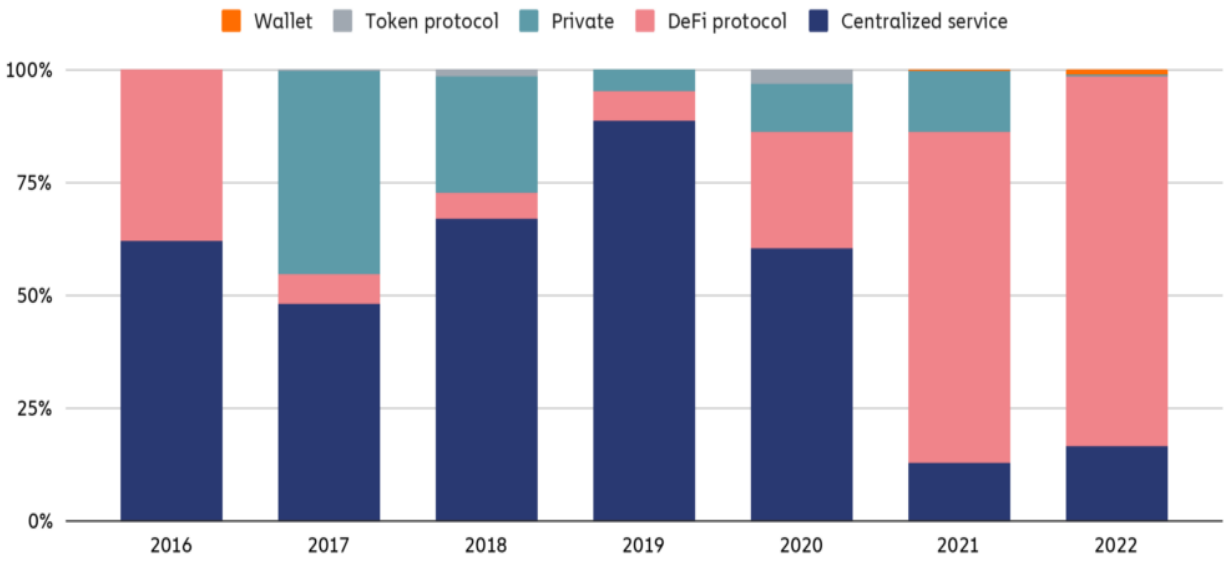
Table 4.1: Types and uses of DeFi tokens

Application	Details
Governance	Allows holders to vote on decisions affecting the DeFi protocol, participating in the decentralised governance of the protocol's future direction and updates.
Liquidity provider	Issued to users who deposit assets into liquidity pools to provide liquidity, these tokens represent their share of the deposit and can be redeemed at any time for the original deposit plus any earned transaction fees.
Loan	In certain DeFi lending platforms, depositing assets into a loan account earns tokens representing its loan balance. These tokens can track the borrower's debt or serve as collateral.
Yield farming	Engaging in yield farming activities (providing liquidity, lending, etc.) in some DeFi projects earns additional tokens as rewards, incentivising participation and support for the ecosystem.
Stablecoins	Though often considered a separate category of digital currency, stablecoins play a crucial role in the DeFi ecosystem by providing a stable medium of exchange, allowing users to avoid the volatility of the cryptocurrency market.
Wrapped	By creating equivalent tokens on different blockchains, cross-chain circulation and interoperability of assets are achieved while retaining their value and characteristics.

Source: https://www.coindesk.com/learn/what-are-defi-tokens/

Although DeFi is an emerging phenomenon, it also carries many risks. Its ecosystem is particularly vulnerable to bugs, hacking, and fraud. Figure 4.1 shows that 2021 and 2022 saw a significant uptick in cryptocurrency heists, largely driven by attacks on DeFi protocols, with cybercriminals making off with over $3.1 billion from DeFi hacks in 2022 alone, representing 82.1% of all crypto stolen that year.

Figure 4.1: Cryptocurrency stolen in hacks by victim platform type, 2016-2022



Source: https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/

Of the $3.1 billion stolen, 64% of the losses came from attacks on cross-chain bridge protocols (Chainalysis, 2023). Bridges are especially attractive to hackers because of their design: to transfer assets across blockchains, bridges lock tokens in a smart contract on the source chain and issue "wrapped" tokens on the destination chain. This creates large, concentrated pools of locked assets that act as collateral (Chainalysis, 2024b). As a result, any vulnerability in the underlying code can jeopardise the entire pool of collateral. The combination of high concentration and large transaction volumes means that a single exploit may yield extraordinary profits, making bridges a primary target for malicious actors. Moreover, the technical complexity of cross-chain interoperability increases the likelihood of overlooked bugs or design flaws, further amplifying their security risks (Belenkov et al., 2025). The attack vectors affecting DeFi are diverse and constantly evolving. Table 4.2 summarises the current methods of attacking DeFi. Overall, most DeFi hacks stem from flaws in the design and implementation of smart contracts, because a large proportion of DeFi protocols are either unaudited or insufficiently audited (Chainalysis, 2024a).

Table 4.2: Classification of DeFi attack methods

Attack method	Description
Protocol exploitation	Hackers exploit vulnerabilities in the blockchain components of the protocol (e.g. validator nodes, the protocol's virtual machine or mining layer related) to carry out attacks.
Insider attack	Protocol developers steal funds directly.
Phishing	Hackers replace the protocol to spend tokens on behalf of users or trick users into sending funds to malicious smart contracts.
Contagion	Hackers use the same vulnerability to attack across different protocols.
Compromised server	Hackers attack the protocol's servers, thereby preventing the protocol from running.
Wallet hack	Hackers steal wallet services hosted by protocols.
Price manipulation hack	When there is a vulnerability in a smart contract that prevents asset prices from accurately reflecting the situation, hackers exploit the vulnerability to manipulate token prices.
Smart contract exploitation	Embedding vulnerabilities in the development process of smart contracts to facilitate future attacks.
Compromised private key	Hackers directly steal users' private keys to heist.
Governance attacks	Hackers gain enough influence or voting power to push harmful proposals.
Third-party compromised	Hackers attack by using vulnerabilities in third-party programs under the protocol.

Source: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/#:~:text=In%202023%2C%20however%2C%20funds%20stolen,a%20drop%20in%20DeFi%20hacking

In addition to being vulnerable to hacker attacks, the decentralised nature of DeFi, which aims to automate the provision of financial services and reduce human dependence, makes it lack standardised regulation (Benson et al., 2024). What is more, when stablecoins are widely used as collateral for debt financing, the financial stability risk of the DeFi ecosystem will also increase accordingly (Darlin et al., 2022). Finally, many transactions in the DeFi market require confirmation of the user's private key, and the risk of private key loss is not uncommon in the DeFi market, which also raises concerns about the security of DeFi (Carter & Jeng, 2021).

Hence, despite the promising outlook of DeFi, it still has a considerable path to navigate. This chapter uses the event study method, focusing on the top six DeFi heists of 2022 (Table 4.3) as a backdrop, to examine the impact of increasingly frequent heists on the DeFi ecosystem.

This chapter aims to address the following two questions: How do the native DeFi tokens on the stolen platforms perform post-heists? Will these compromised platforms' DeFi tokens influence the entire DeFi market? This study is crucial and timely for two reasons: cryptocurrency hacks have become a widespread and formidable threat that demands attention, and DeFi is emerging as a key area in the crypto economy with vast potential for future growth. Previous studies have largely overlooked an in-depth analysis of the risk factor associated with cryptocurrency heists, and studies on DeFi have focused on its definition, regulation, advantages and disadvantages, and connections with other assets (Amler, 2021; Schueffel, 2021; Karim et al., 2022; Yousaf & Yarovaya, 2022; Corbet et al., 2023).

Table 4.3: Top six DeFi heists of 2022

Stolen platform (native token)	Date	Stolen amount ($)	Details
Qubit Finance (Qubit)	January 28, 2022	80 million	Hackers obtained large amounts of fake xEthereum collateral by attacking the QBridge protocol. This collateral is then used to replace all Binance Coins held in QBridge.
Ronin Network (Ronin)	March 29, 2022	620 million	Hackers obtained 5 private keys used to verify transactions and thus faked withdrawals, resulting in 173,600 Ethereum and $25.5 million in USD Coin being stolen from the Ronin Bridge in two transactions.
Beanstalk (Bean)	April 16, 2022	182 million	The hackers borrowed $80 million in cryptocurrency and deposited it into the project's silo, in exchange for receiving enough voting rights to transfer the vault's funds to themselves.
Maiar Exchange (Elrond)	June 5, 2022	113 million	Hackers exploited a smart contract vulnerability to withdraw approximately $113 million worth of Elrond and sold them on the Maiar Exchange, causing the value of Elrond to temporarily plummet 92%, which they then converted to Ethereum and traded on other exchanges.
Binance[6] (Binance Coin)	October 7, 2022	100 million	Hackers exploited a vulnerability in a smart contract to fake transactions, causing more Binance Coin to be minted on the network.
Mango Markets (Mango)	October 11, 2022	114 million	Hackers manipulated price oracle data to allow them to withdraw large loans without adequate collateral.

Source: https://shuftipro.com/blog/the-10-biggest-defi-hacks-of-2022-and-how-can-kyc-aml-compliance-help/; When selecting DeFi heists, this chapter only selects DeFi that have their own native tokens.

[6] Although Binance platform is primarily a centralised exchange, it also offers DeFi products through its Binance Smart Chain. Its native token, Binance Coin, enables participation in DeFi activities and access to decentralised exchanges. Thus, hacker attacks on Binance platform also affect its DeFi services.

Among various performance indicators, liquidity is particularly important in assessing the impact of DeFi heists on DeFi tokens. Unlike centralised financial markets, where liquidity is typically ensured by market makers and institutional investors, most DeFi markets are implemented via automated market makers (AMMs)-based decentralised liquidity pools funded by liquidity providers (LPs) (Shah et al., 2023). As a result, any disruption, such as a security breach, can severely affect the liquidity of DeFi tokens, leading to increased slippage, higher transaction costs, and reduced market depth (Hedera, 2025). Moreover, liquidity is a key determinant of price stability; lower liquidity levels can exacerbate price volatility, making assets more susceptible to manipulation and panic-driven sell-offs. Low liquidity also reduces the utility of the platform's native DeFi token within DeFi protocols, such as lending or staking, further diminishing the platform's attractiveness and preventing the formation of a healthy trading ecosystem (Financial Stability Board, 2023). Given these factors, this chapter evaluates the post-heist performance of stolen platforms' native DeFi tokens primarily through the lens of liquidity, as it provides direct insights into platform performance and investor confidence.

Due to the relative ease of obtaining token price and trading volume data, low-frequency liquidity indicators based on these variables have been widely used in cryptocurrency liquidity studies (Brauneis & Mestel, 2018). Brauneis et al. (2021) emphasised that among these low-frequency measures, the Amihud illiquidity ratio (Amihud, 2002) and the Kyle and Obizhaeva (2016) estimator are most effective in approximating benchmark liquidity levels. However, the Amihud illiquidity ratio, which measures the price impact per unit of trading volume, does not account for zero-volume trading days. To address this limitation, the Amivest liquidity ratio (Cooper et al., 1985; Amihud et al., 1997), which captures the amount of volume that can be absorbed per unit of price change, can serve as a complementary measure to the Amihud illiquidity ratio. Therefore, this chapter uses hourly price data of DeFi tokens and applies the above three low-frequency price impact measures as proxies for liquidity to investigate the changes in the liquidity of the stolen platforms' native DeFi tokens five days before and after DeFi heists. The results indicate that the liquidity of most stolen platforms' native DeFi tokens significantly deteriorates after the DeFi heists.

According to market microstructure theory by the Glosten-Milgrom model (Glosten & Milgrom, 1985), when information asymmetry exists, liquidity providers (market makers) tend to widen bid–ask spreads and reduce liquidity supply out of concern that they may trade against informed traders with superior information. Although the DeFi market relies on

AMMs and lacks traditional quote-driven mechanisms, LPs face similar concerns when deciding whether to continue supplying liquidity to pools. In the context of DeFi heists, hackers gain early knowledge of the stolen assets and their potential devaluation, and trade on this private information. Such early informed trading intensifies adverse selection pressures in the market, making it difficult for LPs to distinguish informed from uninformed traders. Consequently, they respond by withdrawing liquidity or widening effective spreads, which further exacerbates the deterioration of market liquidity. Furthermore, this chapter finds that the response speed and transparency of the victim platform play a crucial role in sustaining the liquidity of its native DeFi tokens. Faster responses and higher levels of transparency can mitigate market participants' informational disadvantages, reduce the risk of adverse selection, and thereby alleviate the negative impact of DeFi heists on liquidity.

This chapter also employs the Quantile Vector Autoregressive (QVAR) model to investigate the potential volatility spillover effects of DeFi heists. Unlike traditional VAR models that focus on average relationships, the QVAR framework allows for analysing dynamic interactions between variables across different points in the distribution. This is particularly important in cryptocurrency markets, where extreme events and asymmetric responses are common (Demiralay & Golitsis, 2021). The QVAR model captures both lower-tail and upper-tail dependencies, which provides more informative insights into market behaviour during stress periods or in response to highly positive or negative shocks (Jena et al., 2022). Therefore, the use of QVAR is well-suited for this study, as it allows for a more nuanced understanding of how DeFi-related shocks propagate across the market under DeFi heists.

This chapter selects the top five DeFi tokens by market capitalisation and uses the QVAR method to investigate whether the volatility of the stolen platform's native DeFi token spills over to these five mainstream DeFi tokens. The selection of the top five DeFi tokens by market capitalisation as a comparison benchmark is based on several considerations. First, these DeFi tokens represent the most established and widely traded assets within the DeFi ecosystem, providing a reliable measure of broader market trends. Due to their high liquidity and strong investor participation, they serve as a natural reference point for assessing the extent of volatility spillovers (Barchat, 2023). Second, larger DeFi tokens typically have more robust security mechanisms, governance frameworks, and diversified use cases, which may make them more resilient to external shocks. Comparing the impact of the stolen platforms' native DeFi tokens on these mainstream DeFi tokens allows us to determine whether the volatility induced by DeFi heist has broader market implications or remains

confined to the affected platform. At the same time, by comparing the effects of different forms of DeFi heists on mainstream DeFi tokens, it becomes possible to identify which type of attack generates more substantial and severe consequences. This issue has received limited attention in prior studies, yet it contributes to a deeper understanding of the heterogeneous impacts of different attack mechanisms on market stability. Such insights are highly relevant for the design of regulation, risk management, and governance structures in both current and future DeFi markets, and they also provide a central theme and research motivation for subsequent studies. Lastly, previous studies on DeFi market dynamics have predominantly focused on these major tokens due to their significant role in decentralised finance. By aligning with existing studies' samples, this study ensures consistency while addressing a novel research gap related to volatility spillovers.

The results indicate that while there is a high level of interconnectedness within the DeFi market, the spillover effects between different DeFi tokens vary. Specifically, mainstream DeFi tokens exhibit significant interconnectedness and mutual influence, but their interconnectedness on the smaller market-cap DeFi tokens from the stolen platforms is relatively limited. Consequently, although the native DeFi tokens of the stolen platforms cause some volatility spillover to mainstream DeFi tokens, the extent is minimal. The native DeFi tokens of the stolen platforms are often net receivers of volatility rather than transmitters. Furthermore, it finds that if investors develop broader concerns about the security of DeFi protocols with governance structures similar to those of the stolen platforms, the resulting fear and uncertainty lead to increased market volatility. In such cases, the native DeFi tokens of the stolen platforms become transmitters of volatility. In other words, attacks targeting the governance mechanisms of DeFi may generate more significant and severe impacts than other forms of DeFi heists. The findings underscore the importance of robust governance and security measures in maintaining market stability and protecting investor interests in the rapidly evolving DeFi environment.

Finally, drawing on the primary economic rationale of regulating financial intermediary activities, this chapter proposes several regulatory approaches for the future of DeFi to help it cope with the increasingly frequent DeFi heists. It recommends that policymakers enhance DeFi oversight by introducing third-party institutions, setting stringent risk management standards, implementing decentralised insurance protocols, and strengthening regulations on liquidity pools. These measures aim to protect both protocol developers and investors.

This chapter makes three key contributions to advancing knowledge in the field of DeFi risk. First, it systematically examines how major DeFi heists affect DeFi token liquidity and volatility spillovers, which is an area that remains underexplored in the existing literature. Second, it introduces the QVAR framework into the DeFi study, enabling the analysis of asymmetric spillover effects under extreme market conditions. Compared with traditional VAR or GARCH models, this approach provides a more nuanced understanding of risk transmission across different states of the market. Third, the study finds that DeFi heists related to governance mechanisms produce more severe and persistent effects than other types of attacks, highlighting the critical role of protocol design and information transparency in shaping market reactions. Overall, these contributions provide new empirical evidence, methodological innovation, and theoretical insights into how DeFi markets respond to severe security shocks.

In practical terms, the findings help market participants better understand how crypto hacks influence DeFi market dynamics, allowing them to develop more effective risk management strategies. The study also offers valuable guidance for policymakers in designing regulatory frameworks aimed at mitigating such risks. By promoting stronger security mechanisms and sustainable development, this study contributes to the long-term stability and resilience of the DeFi ecosystem. Finally, the insights gained from this study lay a foundation for future research into DeFi risk, governance, and market behaviour.

This chapter is structured as follows. The second section is the literature review, the third is the data and methodology, the fourth is the empirical research results, the fifth is the regulatory recommendations for DeFi, and the sixth is the conclusion.

4.2 Literature Review

4.2.1 Information Asymmetry and Liquidity

Liquidity is one of the core characteristics of financial markets, reflecting an asset's ability to be traded quickly without causing significant price changes. A highly liquid market facilitates price discovery, reduces transaction costs, enhances risk sharing, and improves market efficiency and investor confidence (Amihud & Mendelson, 1986; Pástor & Stambaugh, 2003). In contrast, illiquid markets often exhibit prices that deviate from fundamentals, greater trading frictions, and, in extreme cases, systemic instability (Brunnermeier & Pedersen, 2009). Therefore, liquidity serves not only as an indicator of market health but also as a key

dimension for understanding asset price dynamics and investor behaviour (Chordia et al., 2000).

In traditional financial studies, asset liquidity could be analysed through the lens of market microstructure theory. This theoretical framework examines how trading mechanisms, information asymmetry, order book depth, and market-making behaviour jointly shape price formation and liquidity provision. Among these contributions, the information asymmetry pricing model proposed by Glosten and Milgrom (1985) demonstrates that bid–ask spreads originate from adverse selection risks faced by market makers who interact with both informed and uninformed traders. Because market makers cannot distinguish between the two, they widen bid–ask spreads to compensate for potential losses when trading with informed participants. The model predicts that as information asymmetry increases or the proportion of informed traders rises, market makers set higher spreads to maintain zero expected profits, thereby raising transaction costs and reducing market liquidity. In this framework, liquidity is effectively modelled as a function of information asymmetry—markets become less liquid when private information disparities intensify.

Building on this foundation, numerous studies have extended the Glosten and Milgrom (1985) framework to explore the relationship between information asymmetry and liquidity. Stoll (1989) decomposed bid–ask spreads into order-processing, inventory-holding, and information asymmetry components, showing that information asymmetry could capture the intrinsic link between liquidity and information structure. Hasbrouck (1991) verified this decomposition using high-frequency data and found that the information component accounts for a substantial portion of spreads, especially during periods of intense information flow such as earnings announcements. Biais et al. (1995) demonstrated how dynamic quote adjustments and order book depth jointly determine liquidity. Huang and Stoll (1997) further developed a structural estimation approach to identify spread components across different markets and found that higher market transparency and competition improve liquidity. Collectively, these studies establish that information asymmetry is a central driver of liquidity fluctuations, while the bid–ask spread remains an effective measure of liquidity conditions.

With the rise of electronic trading and high-frequency data, scholars have expanded this framework to emerging markets and alternative asset classes. Chordia et al. (2000, 2001) found significant commonality in stock market liquidity, which tends to decline during periods of market stress, indicating that information asymmetry shocks can propagate across

assets through investor sentiment and funding constraints. Easley et al. (2002) introduced the Probability of Informed Trading (PIN) measure, providing a quantitative approach to assess information asymmetry. Brennan and Subrahmanyam (1996) and Pástor and Stambaugh (2003) integrated liquidity risk into asset pricing, demonstrating that information asymmetry not only affects trading efficiency but also generates a liquidity risk premium in expected returns.

In recent years, scholars have applied the Glosten and Milgrom information asymmetry mechanism to cryptocurrency markets to explain price volatility and liquidity variations. Due to decentralisation, anonymity, and the lack of mandatory disclosure, information asymmetry among cryptocurrency traders is particularly severe (Othman et al., 2019; Park & Chai, 2020; Alfieri et al., 2025). The study by Makarov and Schoar (2020) showed that market fragmentation across exchanges leads to cross-platform liquidity segmentation and frictions in information transmission, and that these information asymmetries result in frequent and sizable arbitrage opportunities across trading venues. Tiniç et al. (2023), using Bitfinex limit order book data, found that adverse selection costs account for approximately 10% of bid–ask spreads, confirming that information asymmetry plays a significant economic role in cryptocurrency pricing. Moreover, they showed that the adverse selection component is positively related to future return volatility but negatively related to liquidity indicators such as realised spreads, order book slope, and the Amihud illiquidity ratio, implying that increased information asymmetry amplifies volatility and reduces market liquidity. Manahov and Li (2025c) further found that information asymmetry between issuers and investors significantly reduces newly issued tokens' liquidity during hacker attacks in ICO markets, with the effect most pronounced for newly issued tokens on the same blockchain as the attacked assets. Overall, these studies establish information asymmetry as a key theoretical foundation for understanding low liquidity in cryptocurrency markets.

Despite these advances, studies on DeFi token liquidity remain limited. Existing studies have primarily focused on the liquidity of major cryptocurrencies such as Bitcoin and Ethereum. Most findings suggest that cryptocurrencies exhibit lower liquidity than traditional assets (Loi, 2018; Corbet et al., 2019a; Smales, 2019; Trimborn et al., 2020), although liquidity may improve under certain market conditions (Sensoy, 2019; Scharnowski, 2021; Brauneis et al., 2022; Leirvik, 2022). As a form of cryptocurrency, DeFi tokens are inevitably affected by both external market conditions and changes in information environments. DeFi hacking incidents represent sudden informational shocks that disrupt the distribution of information

among market participants. Although DeFi trading relies on AMMs rather than centralised market makers, the Glosten-Milgrom market microstructure model remains applicable. Compared with traditional financial markets, the decentralised and pseudonymous nature of DeFi, along with the lack of standardised disclosure mechanisms, amplifies the consequences of information asymmetry and makes liquidity provision more sensitive to external shocks. Therefore, this chapter adopts the theoretical framework of Glosten and Milgrom (1985) to investigate how information asymmetry affects DeFi token liquidity in the context of DeFi heists, thereby addressing an important gap in the existing literature.

4.2.2 Examining Relationships Between DeFi Tokens and Other Assets

Existing literature on DeFi primarily focuses on the interconnections between DeFi tokens and other assets, aiming to provide valuable insights for risk management and portfolio management. Spillover effect theory posits that shocks affecting one asset, market, or institution can propagate to others through various transmission mechanisms. These mechanisms include price co-movements, correlated investor sentiment, portfolio rebalancing activities, and liquidity linkages. Originally developed in the context of international finance to explain how a crisis in one country can influence others (Allen & Gale, 2000; Forbes & Rigobon, 2002), the theory has since been widely applied to analyse risk transmission across financial sectors, asset classes, and institutional networks (Diebold & Yilmaz, 2009, 2012; Acemoglu et al., 2015). In highly interconnected systems, spillover effects have the potential to transform localised disruptions into broader systemic risks. In the context of DeFi, this theoretical framework is particularly relevant. Although DeFi platforms operate independently from a technical standpoint, they are often tightly linked through shared user bases, token dependencies, and interoperable smart contracts. As a result, a security breach on one platform could trigger ripple effects that compromise the stability of the broader DeFi ecosystem.

Specifically, existing studies on the spillover effects of DeFi tokens can be broadly divided into two areas: (i) examining the relationships between DeFi tokens and other crypto assets and (ii) exploring the relationships between DeFi tokens and traditional assets.

In studying the relationship between DeFi tokens and other crypto assets, most studies indicate significant interconnectedness between DeFi tokens and other crypto assets. For example, Karim et al. (2022) explored the interconnectedness between NFTs, DeFi tokens, and cryptocurrencies. Using quantile connectedness techniques, they examined the

transmission of extreme risks in the blockchain market under median, extremely low, and extremely high volatility conditions. They found evidence of extreme risk transmission across different cryptocurrency markets. They noted that there is a positive spillover effect between DeFi tokens and mainstream cryptocurrencies under median and extremely low volatility conditions. Similarly, Qiao et al. (2023) employed the wavelet-based quantile causality method and reached similar conclusions. They also highlighted that within the DeFi token market, the volatility of yield farming DeFi tokens spills over to other types of DeFi tokens in both the short and long term. Furthermore, they observed that the density of downside risk networks within DeFi tokens increases over time.

Akkus and Dogan (2024) used the TVP-VAR model to study the dynamic interconnectedness among cryptocurrencies, NFTs, and DeFi tokens. Their results indicated the presence of volatility spillover relationships among these three types of crypto assets, with Ethereum and Chainlink transmitting volatility to other crypto assets. Kumar et al. (2023) also used the TVP-VAR model to study the changes in return and volatility spillovers between cryptocurrencies, NFTs, and DeFi tokens before and after the Russia-Ukraine conflict. They found significant spillover effects among them both before and after the conflict, but the receiver and transmitter roles of these assets changed in the pre- and post-conflict periods. Regarding return spillovers, they discovered that Ethereum, Chainlink, Bancor, Basic Attention Token, and Bitcoin consistently acted as net return spillover transmitters, while Decentraland, Maker, DigiByte, and XRP consistently served as net return spillover receivers. For volatility spillovers, only Chainlink and Basic Attention Token consistently acted as net volatility spillover transmitters, while Bitcoin and XRP consistently served as net volatility receivers. Additionally, they explored the return and volatility spillover effects within three subsystems: cryptocurrency-NFT, cryptocurrency-DeFi, and NFT-DeFi. The results indicated that cryptocurrencies play a significant role in absorbing volatility shocks from NFT and DeFi assets. Their findings are helpful for investors seeking to reduce the negative impact of geopolitical events on their portfolios. Assaf et al. (2024) aimed to investigate the impact of COVID-19 on the interconnectedness among crypto assets. They used the TVP-VAR model to study the relationships between cryptocurrencies and DeFi tokens before and after COVID-19 and found that the return spillover effects from cryptocurrencies were significantly larger, being the main drivers of most changes in DeFi returns. Specifically, cryptocurrencies like Bitcoin, Ethereum, Cardano, and Binance Coin, as well as the DeFi token Bancor, were the primary sources of return and volatility shocks to other

cryptocurrencies and DeFi tokens. They also noted that this interconnectedness varies over time, peaking during the COVID-19 period and subsequently declining. Therefore, investing in DeFi could offer diversification benefits during normal and low-uncertainty periods, but during extreme periods, the increased interconnectedness of crypto assets may reduce the diversification benefits of DeFi investments.

Huang and Hsu (2024) further used a GARCH–EVT–Copula model to analyse the dependence structure between eight leading DeFi tokens and Bitcoin and Ethereum. Their results showed that the dependence between DeFi tokens and Bitcoin and Ethereum is positive and time-varying, with DeFi tokens being more closely correlated with Ethereum than with Bitcoin. They also found that when Bitcoin and Ethereum returns rise, investors are willing to pay a premium to purchase DeFi tokens to gain governance rights, which in turn drives up the prices of DeFi tokens. However, when Bitcoin and Ethereum returns fall, the prices of DeFi tokens do not fall as sharply because their governance rights remain unchanged. Thus, they argued that DeFi tokens are strongly correlated with cryptocurrencies, and this correlation is more pronounced in the upper tail.

On the contrary, some studies have pointed out that the connection between DeFi tokens and other crypto assets is not strong. For example, Park et al. (2023) used Pearson's pairwise correlation coefficients to determine the correlation between the returns of DeFi tokens. They found that the returns of tokens classified as DeFi projects exhibit a persistent co-movement trend and have a higher degree of correlation compared to other cryptocurrencies. Corbet et al. (2023) used the Diebold-Yilmaz connectedness test and found volatility spillover effects between Ethereum and DeFi tokens, which may be attributed to Ethereum's dominant role in the DeFi market. However, they also noted that the volatility spillover effects from traditional cryptocurrencies like Bitcoin and Ethereum to the DeFi market are smaller than the spillover effects among DeFi tokens within the DeFi market itself. Therefore, they suggested that DeFi tokens should be considered a distinct asset class from traditional cryptocurrencies. Similarly, Mensi et al. (2024), using the same method, also found that the connection between DeFi tokens and mainstream cryptocurrencies is weak. They further discovered that within cryptocurrencies, the primary currency transmitting volatility to both the system and DeFi assets is Ethereum, followed by Bitcoin and Litecoin, but their influence is smaller compared to Ethereum. Therefore, they suggested that portfolio managers should consider DeFi tokens as diversification tools.

Different findings suggest that the correlation between DeFi tokens and other crypto assets may be dynamic. Under extreme market conditions, such as black swan events, the interconnections between DeFi tokens and other crypto assets may strengthen as investors react collectively to heightened uncertainty. However, during normal market conditions, DeFi tokens may exhibit weaker correlations with other crypto assets due to their unique market structures, liquidity mechanisms, and governance models, which often lead to idiosyncratic price movements driven by protocol-specific developments rather than broader market trends.

In studying the relationship between DeFi tokens and traditional assets, most studies indicate that the relationship between DeFi tokens and traditional assets is relatively weak. For example, Cevik et al. (2022) used time and frequency domain causality tests and cross-quantilogram methods to examine the interrelationship between DeFi tokens and natural resource assets, focusing on return and volatility spillovers as well as hedging effectiveness. Their results showed that during bear markets, the correlation between DeFi tokens and natural resources is generally negative, indicating that DeFi tokens could provide effective hedging for gold and oil investors.

Yousaf et al. (2022) used the TVP-VAR model to study the dynamic interconnectedness between DeFi tokens (Chainlink, Maker, Basic Attention Token, and Synthetix) and mainstream currencies (Renminbi, Yen, Euro, and Pound). Their spillover analysis results indicated a low interdependence between DeFi tokens and currency markets. Ali et al. (2023) also employed the same method to study the connections between precious metals, industrial metals, and DeFi tokens before and during COVID-19. Their findings suggested that the relationship between DeFi tokens and both precious and industrial metals is weak; adding DeFi tokens to metal-based portfolios helps achieve diversification. Yousaf et al. (2023) utilised both the TVP-VAR and DCC-GARCH models to study the dynamic interconnections between DeFi tokens and sectoral stock markets during COVID-19. Their study revealed that DeFi tokens had the lowest spillover indices. They highlighted that incorporating DeFi tokens into traditional portfolios could provide effective hedging against risks present in traditional assets.

4.2.3 Studies on the Impact of Cryptocurrency Heists on Crypto Assets

There are limited studies on the impact of cryptocurrency heists on crypto assets. Manahov and Li (2024, 2025a, 2025b) examined the effects of cryptocurrency heists on different types of tokens. They found statistically significant spillover effects between the stolen

cryptocurrencies and tourism, energy, and real estate tokens, indicating that cryptocurrency heists not only harm the targeted crypto assets but also transmit negative effects to other tokens. They also reported that these tokens suffered severe liquidity deterioration during heist periods, with Ethereum-based tokens being particularly affected when Ethereum itself was attacked. Furthermore, Manahov and Li (2025c) investigated whether newly issued tokens (ICO tokens) were influenced during cryptocurrency heists. Their results showed that within five trading days, ICO tokens experienced a significant decline in both market efficiency and liquidity, with those issued on the same blockchain as the attacked tokens being most severely impacted, highlighting the interconnected risks within blockchain ecosystems.

Mohamad and Dimitriou (2024) investigated nine cryptocurrency heists and fraud incidents that occurred between 2020 and 2022. Using a multivariate GARCH model, they found that cybercrime events have a significant impact on the volatility of specific cryptocurrencies. Additionally, they discovered that while hacking incidents are generally perceived as bad news, cryptocurrency investors seem to be less affected when the cybercrime involves less popular tokens. This may be attributed to the lower market integration and liquidity of these tokens.

In summary, existing studies suggest that DeFi tokens exhibit a certain degree of correlation with other crypto assets, and their level of interconnectivity may vary over time. The weak linkage between DeFi tokens and traditional assets adds value to DeFi tokens as hedge assets. However, as common targets of crypto attacks, there is a lack of studies on the impact of cryptocurrency heists on DeFi assets. Do DeFi heists affect the native DeFi tokens of the compromised platforms? If so, does this impact spill over to other DeFi tokens, causing broader effects? This chapter seeks to address these questions to help market participants better understand these risks, develop effective risk management strategies, and enhance their ability to respond to volatility in the DeFi market.

4.3 Data and Methodology

4.3.1 Data and Variable

To compare the performance of native DeFi tokens on stolen platforms before and after the DeFi heists, this chapter uses hourly price data to analyse their performance in the five days preceding and following each DeFi heist. Based on Table 4.3, which lists the DeFi heists and

the affected native DeFi tokens, the datasets are as follows: In the Qubit Finance platform heist, the affected native token is the Qubit, and the data range is from January 23, 2022, to February 1, 2022; In the Ronin Network heist, the affected native token is the Ronin, and the data range is from March 24, 2022, to April 2, 2022; In the Beanstalk protocol heist, the affected native token is the Bean, and the data range is from April 11, 2022, to April 20, 2022; In the Maiar Exchange heist, the affected native token is the Elrond, and the data range is from May 31, 2022, to June 9, 2022; In the Binance platform heist, the affected native token is the Binance Coin, and the data range is from October 2, 2022, to October 11, 2022; In the Mango Markets platform heist, the affected native token is the Mango, and the data range is from October 6, 2022, to October 15, 2022.

All DeFi tokens' price data comes from coincodex. The coincodex tracks over 400 cryptocurrency exchanges and thousands of trading pairs, and its token prices are calculated by averaging the cryptocurrency exchange rates on different cryptocurrency trading platforms to accurately reflect the average price of each token as much as possible. Figure 4.2 provides a more intuitive illustration of the impact of the DeFi heists on the prices of native DeFi tokens from affected platforms. Most of these DeFi tokens experienced substantial price declines following the incident. For instance, Qubit fell by approximately 70.6%, Ronin by 24.8%, Bean by 98%, Elrond by 17.3%, and Mango by 54.5%. In contrast, Binance Coin showed the smallest decline, dropping only 4%. These price movements highlight not only the negative effects of DeFi heists on platform-specific tokens but also suggest that different platforms may exhibit varying degrees of market sensitivity in response to such security breaches.

Figure 4.2: Price changes of the stolen platform's native Defi token

(a) Qubit Finance platform heist – January 28, 2022

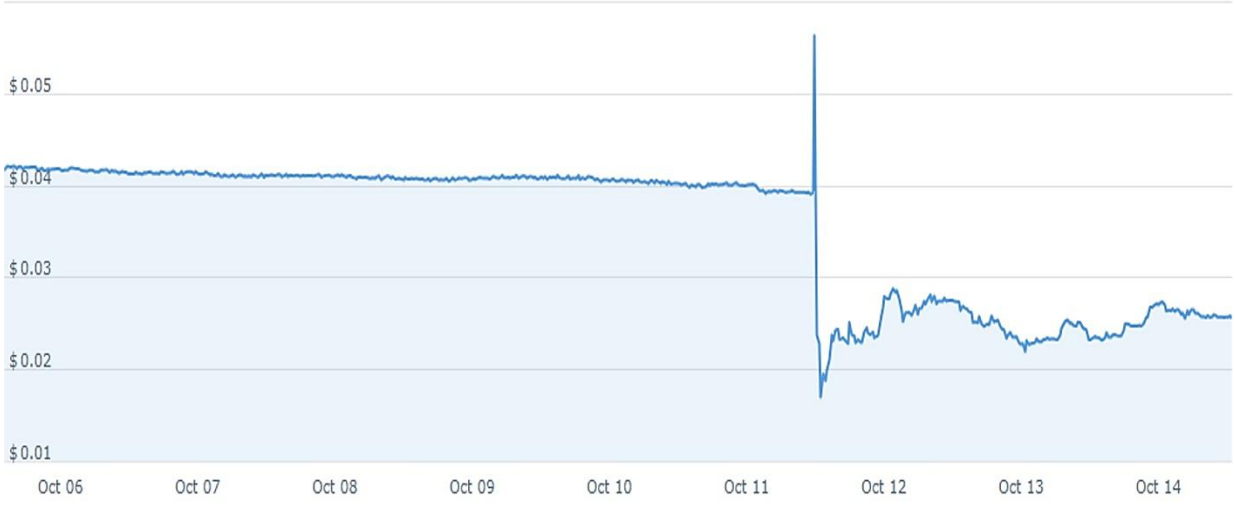
(b) Ronin Network heist – March 29, 2022

(c) Beanstalk protocol heist – April 16, 2022

(d) Maiar Exchange heist – June 5, 2022

(e) Binance platform heist – October 7, 2022

(f) Mango Markets platform – October 11, 2022



Source: coincodex

The hourly return of the DeFi token is calculated as:

$$R_t = Ln\left(\frac{P_t}{P_{t-1}}\right) \tag{25}$$

where R_t is the hourly return of the DeFi token, $Ln(P_t)$ and $Ln(P_{t-1})$ are the natural logs of DeFi token prices at time t and $t-1$. Table 4.4 presents the descriptive statistics of the returns for each DeFi token over the five days before and after the DeFi heists. The results indicate that, except for Binance Coin, the average returns of all other DeFi tokens decreased following the heists, suggesting that these incidents negatively affected the native DeFi tokens of the stolen platforms. Additionally, the standard deviations of most DeFi tokens increased, highlighting heightened volatility in the post-heist period. In particular, the standard deviation of Bean increased from 0.003 to 0.290, and that of Mango rose from 0.003 to 0.057. Furthermore, the returns for most DeFi tokens exhibited negative skewness and leptokurtosis after the heists, indicating the presence of more extreme negative returns. The Jarque–Bera (JB) test results confirm that the return distributions deviate from normality, while the Augmented Dickey–Fuller (ADF) test results demonstrate that the time series are stationary.

Table 4.4: Descriptive statistics of DeFi token returns in six DeFi heists

Panel A: Five days before the DeFi heists									
DeFi token	**Obs**	**Min**	**Max**	**Mean**	**S.Dev.**	**Skew**	**Kurt**	**JB**	**ADF**
Qubit	119	-2.275	2.299	0.000	0.298	0.116	55.311	15718.000***	-7.775***
Ronin	119	-0.043	0.040	0.001	0.010	-1.029	7.360	303.170***	-5.000***
Bean	119	-0.011	0.014	0.000	0.003	0.290	2.585	37.316***	-4.899**
Elrond	119	-0.037	0.042	-0.001	0.011	0.439	3.213	58.536***	-5.219***
Binance Coin	119	-0.018	0.009	0.000	0.003	-0.823	4.903	139.610***	-3.361*
Mango	119	-0.009	0.009	0.000	0.003	-0.041	-0.427	0.762	-6.557***
Panel B: Five days after the DeFi heists									
DeFi token	**Obs**	**Min**	**Max**	**Mean**	**S.Dev.**	**Skew**	**Kurt**	**JB**	**ADF**
Qubit	119	-0.235	0.034	-0.009	0.037	-4.377	21.818	2842.300***	-4.374**
Ronin	119	-0.208	0.026	-0.002	0.021	-7.977	75.515	30579.000***	-5.038***
Bean	119	-1.571	0.901	-0.028	0.290	-2.162	12.349	883.540***	-5.708***
Elrond	119	-0.104	0.034	-0.002	0.015	2.740	15.958	1467.000***	-6.683***
Binance Coin	119	-0.010	0.008	0.000	0.003	-0.791	2.215	39.054***	-5.235***
Mango	119	-0.485	0.150	-0.004	0.057	-5.174	45.152	9251.000***	-5.520***

The data source is from coincodex; **Skew:** Skewness, it is a measure of symmetry; **Kurt:** Kurtosis, it is a measure of whether the data are heavy-tailed or light-tailed relative to a normal distribution; **JB:** Jarque–Bera test; **ADF:** Augmented Dickey-Fuller test; *** At the 1% significance level; ** At the 5% significance level; * At the 10% significance level

4.3.2 Market Liquidity Test

Due to the complexity of the cryptocurrency market, obtaining and processing data on bid-ask spreads and order book dynamics is challenging. As a result, few studies have used full order book data to examine liquidity in cryptocurrency markets (Brauneis et al., 2021). Instead, price and trading volume data are more readily available, making low-frequency liquidity indicators based on these variables commonly used in cryptocurrency liquidity studies (Brauneis & Mestel, 2018). Among these low-frequency indicators, the most widely used are the Amihud illiquidity ratio (Amihud, 2002) and the Roll spread ratio (Roll, 1984). However, when the covariance of price changes is positive, the modified Roll spread ratio assigns the indicator value to zero, but a positive covariance of price changes does not necessarily indicate high liquidity.

Brauneis et al. (2021) emphasised that among these low-frequency indicators, the Amihud illiquidity ratio and the Kyle and Obizhaeva (2016) estimator best estimate the level of the liquidity benchmark measures. However, since the Amihud illiquidity ratio measures the price impact per unit of trading volume, it does not account for days with zero trading volume. To address this limitation, this chapter also incorporates the Amivest liquidity ratio (Cooper et al., 1985; Amihud et al., 1997), which evaluates the amount of trading volume that can be absorbed per unit of price change. Unlike the Amihud illiquidity ratio, the Amivest liquidity ratio considers days with zero trading volume but excludes trading days with zero returns. Given their complementary nature, these two indicators provide a more comprehensive assessment of market liquidity by considering both the impact of trading volume on price movements and the ability of price changes to absorb trading volume.

Since this chapter employs hourly data, three low-frequency price impact indicators are used as proxies for liquidity: the Amihud illiquidity ratio (*Amihud*), the Amivest liquidity ratio (*Amivest*), and the Kyle and Obizhaeva estimator (*Kyle*).

Amihud illiquidity ratio is used to assess the price changes caused by a unit of trading volume (Amihud, 2002). This ratio can be expressed as:

$$\text{Amihud illiquidity ratio} = \frac{1}{N}\sum_{t=1}^{N}\frac{|R_t|}{V_t} \tag{26}$$

where R_t is the return of the token at hour t, and V_t is the trading volume in USD at hour t. N is the total number of non-zero trading volume hours in the observation period. A higher ratio

indicates lower market liquidity, as price changes are more sensitive to trading volume. Conversely, a lower ratio suggests better market liquidity.

The Amivest liquidity ratio measures the volume of trades that the market can accommodate for a given price change, thereby reflecting the overall level of market liquidity. Unlike the Amihud illiquidity ratio, which emphasises the sensitivity of price changes to trading volume, the Amivest liquidity ratio focuses on the market's capacity to absorb trading volume under price fluctuations. It can be expressed as:

$$\text{Amivest liquidity ratio} = \frac{1}{N}\sum_{t=1}^{N}\frac{V_t}{|R_t|} \tag{27}$$

where R_t is the return of the token at hour t, and V_t is the trading volume in USD at hour t. N is the total number of non-zero return hours in the observation period. A higher ratio indicates greater trading volume for a given price change, indicating better liquidity (Cooper et al., 1985, Amihud et al., 1997; Berkman & Eleswarapu, 1998).

Kyle and Obizhaeva (2016) developed an illiquidity measure by calculating the ratio of an asset's volatility to its dollar trading volume within a specified time interval. It is defined as:

$$\text{Kyle and Obizhaeva estimator} = \left[\frac{\overline{\sigma_{t,i}^2(r)}}{\sum_{t=1}^{N} V_t}\right]^{\frac{1}{3}} \tag{28}$$

where $\overline{\sigma_{t,i}^2(r)}$ represents the mean of the squared returns of all subintervals i in interval t. V_t is the sum of trading volume in USD during the time interval t. A higher value of this estimator indicates greater price volatility but lower trading volume, suggesting poorer market liquidity. Conversely, a lower value signifies smaller price fluctuations accompanied by higher trading volume, indicating better market liquidity.

4.3.3 Quantile VAR Model

This chapter uses the Quantile Vector Autoregressive (QVAR) model to analyse the potential spillover effects of the DeFi heists. The QVAR model, as proposed by Ando et al. (2022) within the framework of graphical analysis for VAR models, employs quantile regression and factor structures to distinguish between common error components and idiosyncratic error components. Compared to traditional VAR models, the QVAR model captures dynamic relationships at different quantiles. This means that the QVAR model can capture

relationships between variables across different parts of the data distribution (e.g. high quantiles and low quantiles), providing deeper insights into extreme events and tail risks. According to the study by Jena et al. (2022), analyses conducted at the 5th and 95th quantiles using the QVAR approach are more valuable and informative for understanding the spillover effects of negative and positive news. Moreover, Ando et al. (2022) noted that the QVAR model differs from traditional conditional mean estimators, such as Ordinary Least Squares (OLS), because OLS regression suffers from omitted variable bias (Wilms et al., 2021). This bias occurs when an omitted third variable affects both the independent and dependent variables. The VAR framework addresses the potential for significant bias in network analysis that can arise from failing to account for sources of common variation (Khalfaoui et al., 2022).

Compared with DCC-GARCH or TVP-VAR models that are widely used to study volatility spillovers, QVAR offers distinct advantages. While DCC-GARCH effectively captures time-varying correlations in conditional variances, it primarily focuses on average dependence and neglects heterogeneity across different parts of the return distribution (Engle, 2002; Bouri et al., 2021b). Similarly, although TVP-VAR allows parameters to evolve, it remains centred on mean relationships, which may obscure asymmetric dynamics that arise during periods of market stress (Primiceri, 2005; Koop & Korobilis, 2013). Therefore, these estimators can only measure the average shock system. However, systemic shocks do not necessarily correspond to average shocks and may in fact be much larger, indicating the need to account for potential heterogeneous effects across the distribution of shock magnitudes (Bouri et al., 2021b). In contrast, QVAR explicitly estimates relationships at different quantiles, enabling the examination of whether spillover effects intensify in the tails (Ando et al., 2022).

This property is significant in DeFi markets. Unlike traditional financial systems, DeFi lacks circuit breakers and centralised stabilisers, meaning that once a DeFi heist occurs, shocks are sudden and accompanied by severe information asymmetry. Prices can fluctuate dramatically, and LPs' withdrawals may further amplify tail risks. In this context, a framework such as QVAR, which can uncover contagion effects in the tails rather than only at the mean, is highly appropriate. The key assumption of QVAR is that dependence structures among variables may differ across quantiles: spillover effects may be modest or insignificant in tranquil periods (e.g., at the 50th quantile), but become significantly stronger under extreme market conditions (e.g., at the 95th or 5th quantiles). Accordingly, QVAR results can be

interpreted as evidence of heterogeneous transmission mechanisms, whereby spillovers are limited in normal states but highly contagious during extremes (Bouri et al., 2021b).

Quantile regression allows us to estimate the relationship between y_t and x_t at each quantile τ of the conditional distribution $(y_t \mid x_t)$. This can be expressed as:

$$Q_\tau(y_t \mid x_t) = x_t\beta(\tau) \tag{29}$$

where Q_τ represents the τ-th conditional quantile function of y_t. $\tau \in (0,1)$ represents quantile index. x_t represents a vector of explanatory variables. $\beta(\tau)$ represents the dependence relationship between x_t and the τ-th conditional quantile function of y_t. Specifically, $\beta(\tau)$ is the parameter vector estimated at the τ-th conditional using the following expression:

$$\hat{\beta}(\tau) = \underset{\beta(\tau)}{a\arg\min} \sum_{t=1}^{T} \left(\tau - 1_{\{y_t < x_t\beta(\tau)\}}\right)|y_t < x_t\beta(\tau)| \tag{30}$$

Subsequently, the n-variable quantile VAR process p-th order is estimated as:

$$y_t = c(\tau) + \sum_{i=1}^{p} \Phi_i(\tau)y_{t-1} + e_t(\tau), t = 1, \dots, T \tag{31}$$

where y_t denotes the n-vector of dependent variable (In this chapter, it is volatility). $c(\tau)$ and $e_t(\tau)$ represent the n-vector of constants and residuals at quantile τ, respectively. $\Phi_i(\tau)$ denotes the matrix of lagged coefficients of the dependent valuable at quantile τ, with $i = 1, \dots, p$. The estimates $\hat{\beta}(\tau)$ and $\hat{c}(\tau)$ are obtained under the assumption that the residuals satisfy the population quantile restriction, $Q_\tau\left(e_t(\tau) \mid y_{t-1}, \dots y_{t-p}\right) = 0$. The population τ-th conditional quantile of the response variable y is given in Equation (32) below:

$$Q_\tau\left(y_t \mid y_{t-1}, \dots y_{t-p}\right) = c(\tau) + \sum_{i=1}^{p} \Phi_i(\tau)y_{t-1} \tag{32}$$

Next, it needs to calculate several return connectedness measures for each quantile τ. We represent equation (31) as an infinite-order vector moving average (MA) process:

$$y_t = \mu(\tau) + \sum_{s=0}^{\infty} A_s(\tau) e_{t-s}(\tau), t = 1, \dots, T$$
$$\mu(\tau) = \left(I_n - \Phi_1(\tau) - \cdots - \Phi_p(\tau)\right)^{-1} c(\tau) \quad (33)$$
$$A_s(\tau) = \begin{cases} 0, s < 0 : I_n, s = 0 \\ \Phi_1(\tau) A_{s-1} + \cdots + \Phi_P(\tau) A_{s-p}(\tau), s > 0 \end{cases}$$

where y_t is defined by the sum of the residuals $e_t(\tau)$.

Following Koop et al. (1996) and Pesaran and Shin (1998), the Generalized Forecast Error Variance Decomposition (GFEVD) quantifies the proportion of a variable's forecast error variance that can be attributed to shocks from different variables over a forecast horizon *H*:

$$\omega_{ij}^{g}(H) = \frac{\sigma_{jj}^{-1} \sum_{h=0}^{H-1} \left(e_i' A_s \sum e_j\right)^2}{\sum_{h=0}^{H-1} \left(e_i' A_s \sum e_j\right)} \quad (34)$$

where $\omega_{ij}^{g}(H)$ represents the contribution of the *j*-th variable to the forecast error variance of the i-th variable at horizon H. $\sum$ illustrates the variance matrix of the vector of errors. σ_{jj} denotes the *j*-th diagonal element of the $\sum$ matrix, and e_i is a vector with a value of one in the i-th position and zero otherwise.

We next normalise every entry of the variance decomposition matrix using the expression below:

$$\widetilde{\omega}_{ij}^{g}(H) = \frac{\omega_{ij}^{g}(H)}{\sum_{j=1}^{N} \omega_{ij}^{g}(H)} \quad (35)$$

Finally, we follow Diebold and Yilmaz (2012, 2014) to define the GFEVD connectedness measures at each quintile τ. The total directional spillover index (*SI*) from variable i to variables *j* at quintile τ is:

$$TO = SI_{i \to j}(\tau) = \frac{\sum_{j=1, i \neq j}^{N} \widetilde{\omega}_{ji}^{g}(\tau)}{\sum_{j=1}^{N} \widetilde{\omega}_{ji}^{g}(\tau)} \times 100 \quad (36)$$

The total directional spillover index (*SI*) from variables *j* to variable i at quintile τ is:

$$FROM = SI_{i \leftarrow j}(\tau) = \frac{\sum_{j=1, i \neq j}^{N} \widetilde{\omega}_{ij}^{g}(\tau)}{\sum_{j=1}^{N} \widetilde{\omega}_{ij}^{g}(\tau)} \times 100 \quad (37)$$

The net total directional spillover (*NSI*) index at quantile τ is:

$$NET = NSI = SI_{i\to j}(\tau) - SI_{i\leftarrow j}(\tau) = TO - FROM \tag{38}$$

A positive value indicates that the variable is a net transmitter of volatility, whereas a negative value indicates that the variable is a net receiver of volatility.

The total connectivity index (*TCI*) captures the overall level of interconnectedness within the system, reflecting the extent to which shocks are transmitted across the system. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower TCI suggests weaker linkages and more independence among the system. The *TCI* among the variables at quantile τ is:

$$TCI(\tau) = \frac{\sum_{i=1}^{N} \sum_{j=1, i\neq j}^{N} \widetilde{\omega}_{ij}^{g}(\tau)}{\sum_{i=1}^{N} \sum_{j=1}^{N} \widetilde{\omega}_{ij}^{g}(\tau)} \times 100 \tag{39}$$

4.4 Empirical Results

4.4.1 Impact of the DeFi Heists on the Liquidity of the DeFi Tokens

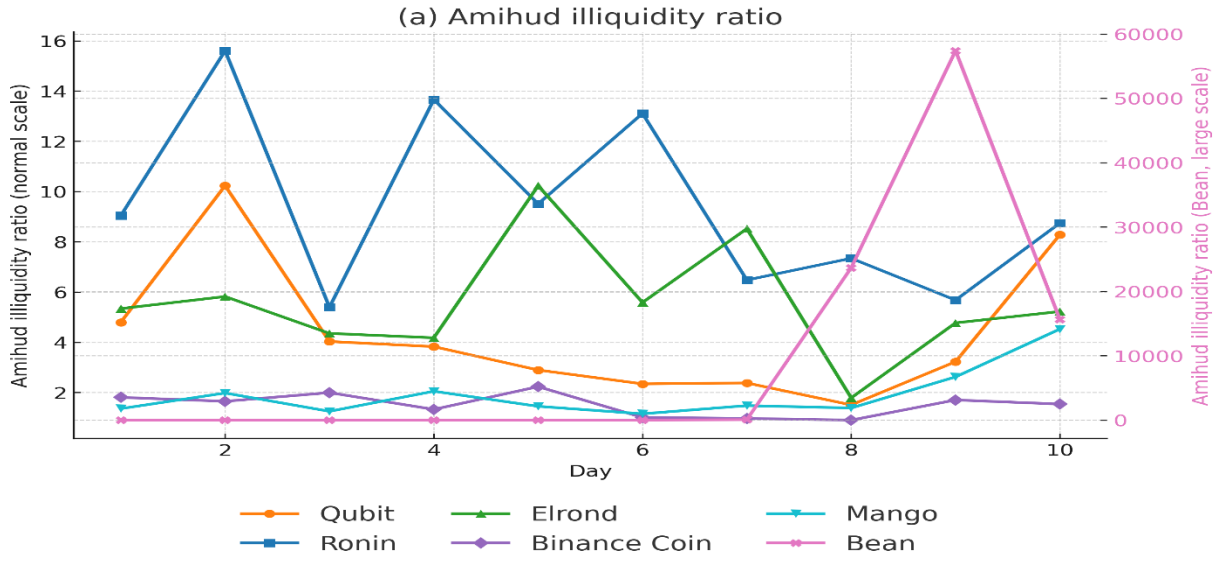
To examine the direct impact of price and trading volume fluctuations caused by DeFi heists on the liquidity of the native DeFi tokens on the affected platforms, this chapter uses the *Amihud*, the *Amivest*, and the *Kyle* indicators to estimate the liquidity. These indicators are used to measure the daily liquidity levels of DeFi tokens over a ten-day window, including the five days before and after each DeFi heist. This chapter collects the trading volume data for each DeFi token from coincodex, and the empirical results presented in Table 4.5 indicate that the impact of DeFi heists on DeFi token liquidity is not uniform. In some cases, a significant deterioration in liquidity is observed, whereas in others, the decline in liquidity is less pronounced. Figure 4.3 illustrates the trends of the three liquidity indicators, further demonstrating that DeFi heists have heterogeneous impacts on different DeFi tokens.

Specifically, the *Amihud* for Qubit increased from 2.343 to 8.279 over the five days following the heist, while the *Amivest* declined from 46.504 to 2.552. Although *Kyle* did not show a substantial increase after the heist, a noticeable rise was observed from 7.171 to 10.860 between the day before and after the heist (Days 5 to 7 in Table 4.5). These results indicate a significant deterioration in Qubit's liquidity. Similarly, Mango also experienced a decline in liquidity. Over the five days following the heist, the *Amihud* rose from 1.151 to 4.525, while the *Amivest* dropped from 4.296 to 2.677. Meanwhile, the *Kyle* increased from 1.481 to 3.705, further confirming the deterioration in liquidity.

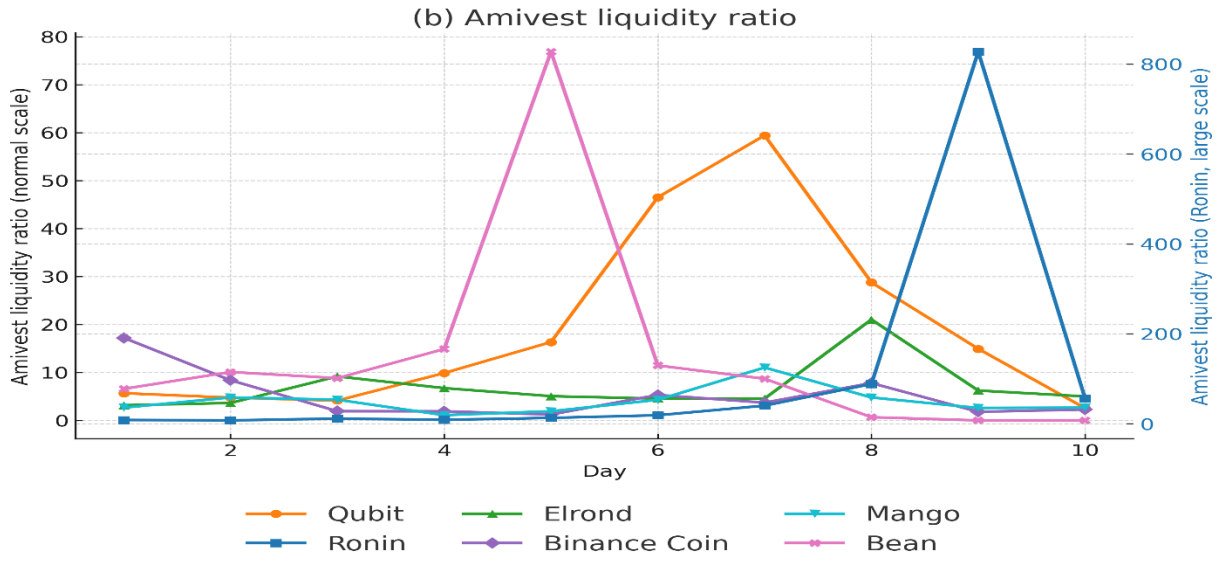
Table 4.5: Liquidity test results of Defi tokens

	1	2	3	4	5	6	7	8	9	10
Amihud illiquidity ratio (*Amihud*)										
Qubit	4.794	10.231	4.030	3.826	2.894	2.343	2.379	1.505	3.225	8.279
Ronin	9.035	15.602	5.392	13.660	9.509	13.107	6.476	7.341	5.677	8.743
Bean	3.572	3.252	2.009	2.739	1.898	1.821	79.065	23675.911	57397.295	15642.312
Elrond	5.339	5.819	4.353	4.177	10.231	5.853	8.519	1.787	4.770	5.224
Binance Coin	1.806	1.649	1.994	1.327	2.232	1.007	0.967	0.900	1.702	1.539
Mango	1.357	1.979	1.250	2.049	1.449	1.151	1.478	1.383	2.621	4.525
Amivest liquidity ratio (*Amivest*)										
Qubit	5.673	4.754	4.137	9.874	16.333	46.504	59.413	28.765	14.929	2.552
Ronin	8.384	7.391	11.428	8.653	12.984	18.821	40.230	88.370	827.546	56.290
Bean	6.577	10.092	8.809	14.880	76.866	11.454	8.690	0.672	0.006	0.022
Elrond	3.164	3.637	9.174	6.735	5.059	4.543	4.554	21.029	6.229	5.003
Binance Coin	17.217	8.373	1.923	1.904	1.234	5.319	3.704	7.786	1.794	2.284
Mango	2.661	4.787	4.320	1.101	1.912	4.296	11.024	4.786	2.598	2.677
Kyle and Obizhaeva estimator (*Kyle*)										
Qubit	6.696	8.976	5.703	5.602	7.171	9.705	10.860	7.419	6.426	5.203
Ronin	7.731	9.790	5.115	9.847	9.620	18.567	6.671	6.683	7.180	7.163
Bean	3.594	3.755	2.973	4.048	3.411	3.322	78.295	54.308	276.487	194.586
Elrond	3.245	3.587	2.518	2.641	4.281	2.279	4.251	2.052	2.973	3.695
Binance Coin	6.618	6.456	7.158	5.798	8.968	5.437	5.286	4.363	6.776	6.464
Mango	1.366	1.621	1.156	1.589	1.324	1.481	4.784	2.452	3.199	3.705

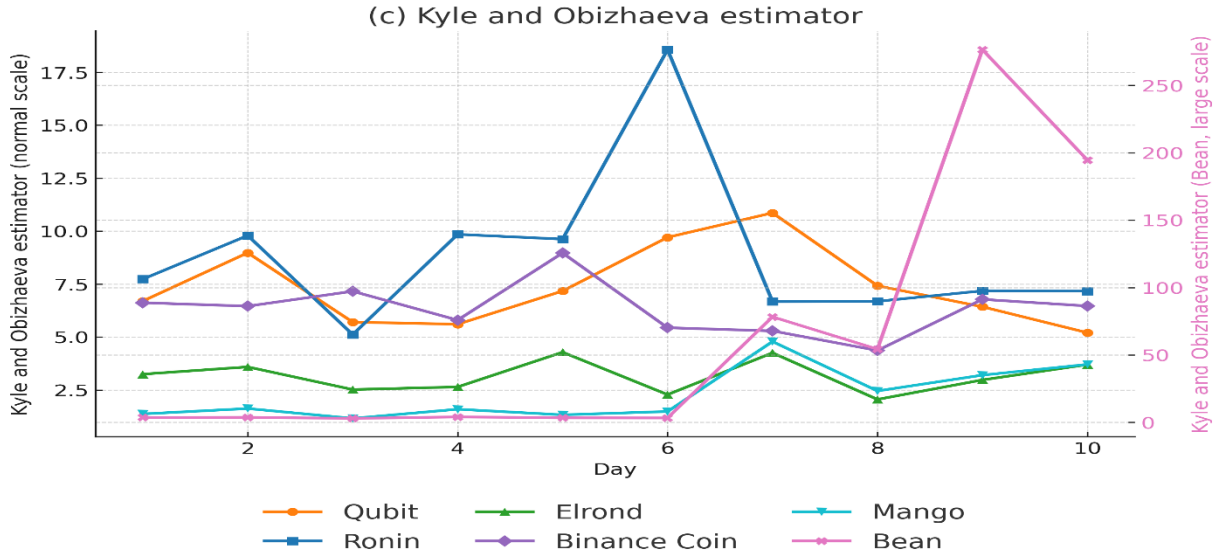
Figure 4.3: The trends of the three liquidity indicators



The larger the *Amihud* value, the worse the liquidity; Since Bean's *Amihud* values are substantially higher than those of the other DeFi tokens in the post-heist period, they are plotted on the right-hand Y-axis to allow for a clearer comparison of the changes across DeFi tokens; Each line represents one DeFi token around its own heist.



The smaller the *Amivest* value, the worse the liquidity; Since Ronin's *Amivest* values are substantially higher than those of the other DeFi tokens in the post-heist period, they are plotted on the right-hand Y-axis to allow for a clearer comparison of the changes across DeFi tokens; Each line represents one DeFi token around its own heist.



The larger the *Kyle* value, the worse the liquidity; Since Bean's *Kyle* values are substantially higher than those of the other DeFi tokens in the post-heist period, they are plotted on the right-hand Y-axis to allow for a clearer comparison of the changes across DeFi tokens; Each line represents one DeFi token around its own heist.

By comparison, the liquidity deterioration for Ronin and Elrond appeared to be shorter-lived. For example, Ronin's liquidity worsened most severely on the day of the heist (Day 6 in Table 4.5), with its *Amihud* surging from 9.509 to 13.107 and the *Kyle* increasing from 9.620 to 18.567. On the other hand, Elrond's liquidity significantly declined the day after the heist (Day 7 in Table 4.5), as its *Amihud* rose from 5.853 to 8.519, while its *Kyle* increased from 2.279 to 4.251. Both DeFi tokens' *Amihud* and *Kyle* suggest that trading volume exerted a stronger impact on price movements, leading to greater market instability, intensified price

shocks, and reduced market depth. However, *Amivest* did not provide evidence of declining liquidity. Therefore, while Ronin and Elrond faced short-term liquidity shocks, market participants were still able to trade, allowing investors to adjust more quickly to a new equilibrium, which explains why their liquidity levels improved in subsequent trading days. Despite the relatively short duration of the liquidity deterioration, Ronin and Elrond experienced significant price declines of 24.8% and 17.3%, respectively, during this period. This suggests that short-term liquidity shocks could still lead to substantial price fluctuations, increasing trading costs and liquidity risk for investors. Market sentiment deteriorated sharply following the heist, triggering panic selling and exacerbating the downward price movement. Although a few DeFi heists may take several days or even weeks to be detected (Carreras, 2022), the vast majority are identified within a short time. Since all transactions are recorded on-chain, blockchain monitoring tools, security firms, and community observers could often capture abnormal movements within a short time (Wang et al., 2021; Chainalysis, 2025), which can then be widely disseminated via social media, official announcements, or crypto news outlets.

The Glosten-Milgrom model (Glosten & Milgrom, 1985) of market microstructure helps further explain why liquidity deteriorates following a DeFi heist. Although DeFi relies on AMMs rather than centralised dealers, the same mechanism remains applicable. In a constant product AMM ($x \times y = k$), token prices are determined by the ratio of the two assets in the pool (Mohan, 2022). When a DeFi heist occurs, informed traders (usually the hacker), anticipating a decline in token value, rapidly sell tokens (x) into the pool in exchange for stablecoins or higher-quality assets (y). This process increases the pool's inventory of depreciating tokens, decreases its stablecoin reserves, and immediately incorporates the negative information into pool prices. LPs then face two types of risks: first, adverse selection, as they effectively transact at unfavourable prices against informed traders; and second, impermanent loss arising from price jumps and heightened volatility, where the pool's rebalancing shifts LPs' portfolios toward depreciating assets, generating losses relative to a passive benchmark (Del Monte et al., 2025). Because DeFi heists are often accompanied by sharp price declines and high volatility, these risks are amplified. Anticipating or observing such order flow, LPs' optimal response is typically to withdraw liquidity, which directly reduces pool depth. As pools become shallower, subsequent trades exert greater price impact, which is equivalent to a widening of bid–ask spreads. This further worsens market liquidity

and creates a negative feedback loop: informed selling induces LPs' withdrawals, which in turn magnify liquidity shocks (Pellicer, 2024).

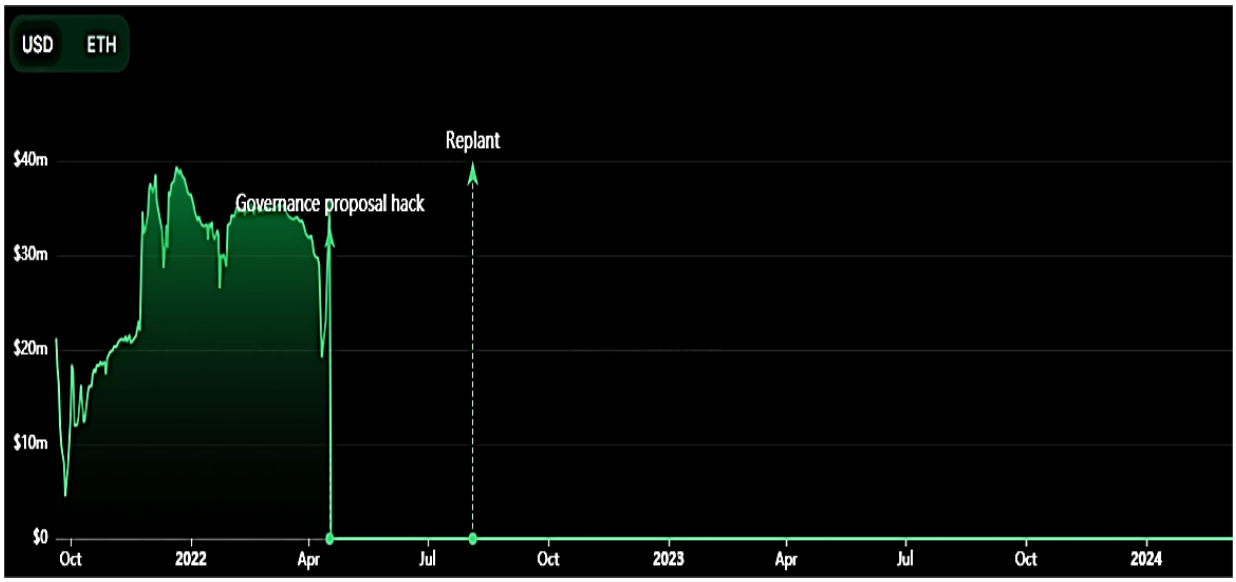
Beyond the adverse selection mechanism captured by the Glosten-Milgrom framework, investor sentiment plays a complementary role in amplifying liquidity shocks. Security breaches heighten concerns about platform safety and undermine confidence in native DeFi tokens. Overreacting investors engage in large-scale sell-offs while refraining from new investments, thereby depressing both trading activity and liquidity (Borgards & Czudaj, 2020; Jia et al., 2022; Wanidwaranan & Termprasertsakul, 2024). The study by Yao et al. (2024) also showed that abnormal attention exerts a persistent negative impact on liquidity, leading to excessive net buying pressure and buyer-side market congestion, which ultimately results in a sharp deterioration of market liquidity. In summary, this dual channel highlights that liquidity deterioration in DeFi markets stems not only from informed trading and liquidity withdrawals but also from heightened market fragility and sensitivity to shocks.

In the Binance platform heist, although *Amihud*, *Amivest*, and *Kyle* all suggest a decline in Binance Coin's liquidity five days after the heist, the magnitude of these changes was not substantial. Specifically, the *Amihud* and *Kyle* increased by only 52.83% and 18.89%, respectively, while the *Amivest* declined by 57.06%. Furthermore, Figure 4.2 indicates that Binance Coin's price drop during this heist was relatively modest. One possible reason why Binance Coin's liquidity did not experience a significant deterioration is the swift response of the Binance platform to the heist. Upon discovering that the exploit had been executed, the Binance platform immediately suspended network (Binance Smart Chain) operations, instructing all 44 validators to temporarily halt Binance Smart Chain activities to contain the losses. As a result, while approximately $137 million was successfully transferred by the attackers, the remaining funds were frozen on the Binance Smart Chain (Nansen, 2022). Additionally, the Binance platform promptly issued an official security response and conducted an on-chain governance vote to address the heist. From the perspective of the Glosten-Milgrom framework, the Binance platform's rapid disclosure and on-chain governance response effectively reduced information asymmetry in the aftermath of the attack. By narrowing the informational advantage of informed traders, these actions lowered adverse selection risk for LPs and mitigated the incentive to withdraw liquidity. Consequently, the expected widening of spreads and the severe deterioration of market liquidity were largely avoided. At the same time, this series of proactive measures reinforced investor confidence in

the platform and its native DeFi token, and alleviated market panic. As a result, investors did not withdraw from the Binance platform, preventing a significant decline in liquidity.

Another noteworthy DeFi heist is the Beanstalk protocol heist. Within five days of the heist, Bean's liquidity deteriorated significantly. For instance, its *Amihud* surged from 1.821 to 15,642.312, while the *Amivest* plummeted from 11.454 to 0.022. Similarly, the *Kyle* rose sharply from 3.322 to 194.586, indicating a near-total collapse in market liquidity. The severe liquidity deterioration in Bean could largely be attributed to the fact that this attack not only exposed a fundamental system vulnerability but also completely drained the protocol's Total Value Locked (TVL). TVL represents the total value of crypto assets locked within a DeFi platform and serves as a crucial metric for assessing its attractiveness and activity level. As shown in Figure 4.4, the Beanstalk protocol's TVL plunged to nearly zero following the attack, severely undermining investor confidence and destabilising the market environment for Bean.

Figure 4.4: TVL at Beanstalk protocol before and after the heist



Source: https://defillama.com/protocol/beanstalk?mcap=false

Concerns over protocol security further reduced trading activity in Bean, exacerbating the decline in market liquidity (Manahov et al., 2014; Ibikunle et al., 2016). Additionally, the Beanstalk protocol was shut down following the exploit, with no immediate recovery plan announced, leaving LPs and investors with limited information and heightened uncertainty regarding future risks. This lack of transparency intensified information asymmetry, further hindering the restoration of market liquidity (Barron & Qu, 2014; Hu & Prigent, 2019).

These findings are consistent with previous studies. Yue et al. (2021) applied four liquidity metrics to the top 100 cryptocurrencies and reported that negative news announcements impair liquidity within four days. Yao et al. (2024) found that crypto assets with smaller market shares and unique volatility attract fewer investors. These assets experience less trading activity, making their liquidity highly sensitive to changes in investor interest. Due to the magnifying effect of trading behaviour, increased attention from investors to these lesser-known cryptocurrencies could lead to significant liquidity fluctuations. Manahov and Li (2024) discovered that within two weeks of a cryptocurrency heist, the liquidity of three tourism tokens, Bitcoin, and Ethereum decreases, with smaller market cap tourism tokens exhibiting greater liquidity volatility than the larger market cap Bitcoin and Ethereum. In this chapter, except for Binance Coin, the market capitalisation of the studied DeFi tokens is relatively small, so DeFi heists are likely to have a more substantial impact on the liquidity of these small market-cap DeFi tokens. As a result, heists targeting DeFi platforms could lead to significant declines in the price and liquidity of the platform's native DeFi tokens.

In summary, *Amihud*, *Amivest*, and *Kyle* indicate that DeFi heists significantly reduce the liquidity of most DeFi tokens. This highlights the severe impact of security breaches on DeFi platforms, leading to substantial declines in the price and liquidity of their native DeFi tokens, and underscores the importance of robust security measures in maintaining market stability. The comparative study of the Binance platform and Beanstalk protocol heists emphasises the crucial role of timely response and increased transparency in preserving the liquidity of the platform's native DeFi tokens. The faster and clearer the disclosure, the smaller the informational advantage between informed traders and other participants. As this advantage diminishes, the adverse selection risk faced by LPs decreases, strengthening their incentive to remain in the pool and mitigating the decline in liquidity. Moreover, effective remedial measures for the project help investors maintain confidence and continue holding the tokens. Therefore, this study not only reveals the negative impact of DeFi heists on liquidity but also underscores the central role of disclosure mechanisms and response speed in shaping market reactions.

4.4.2 Impact of the DeFi Heists on the DeFi Market

Next, this chapter aims to investigate whether the volatility of the stolen platforms' native DeFi tokens will spill over to other mainstream DeFi tokens five days after the DeFi heists, thereby analysing the scope and extent of the DeFi heists' impact on the DeFi market.

According to market capitalisation data provided by CoinMarketCap, this chapter selects the top five DeFi tokens: Avalanche, Chainlink, Uniswap, Maker, and Stacks. The reasons for choosing these tokens are as follows: First, the top five DeFi tokens by market capitalisation typically have significant market influence and liquidity, with their price fluctuations reflecting the overall sentiment and trends of the DeFi market (Barchat, 2023). Second, these tokens represent different DeFi projects, including lending platforms, decentralised exchanges, and oracle services, providing strong representativeness. Tables 4.6-4.11 present the dynamic spillover results of the stolen platforms' native DeFi tokens and five major DeFi tokens across high, median, and low quantiles (i.e., the 95th, 50th, and 5th percentiles, respectively).

The results show that the *TCI* at both the extremely high and low quantiles are significantly large, and both exceed the *TCI* at the median quantile. This indicates that the volatilities of different DeFi tokens are highly correlated under extreme market conditions. When a single DeFi token experiences volatility, this fluctuation could easily spill over to other DeFi tokens, triggering a chain reaction. These findings are consistent with previous studies, which suggest that the cryptocurrency market is highly interconnected, and volatility within the same category of tokens is highly correlated (Canh et al., 2019; Katsiampa, 2019a; Katsiampa et al., 2019; Tiwari et al., 2020; Ante, 2022; Charfeddine et al., 2022; Dowling, 2022; Corbet et al., 2023; Aharon et al., 2024; Yousaf et al., 2024a). Therefore, the high interconnectedness within the DeFi market indicates a high level of risk, meaning the market's stability is poor and it is susceptible to external shocks (Baruník & Křehlík, 2018). Interestingly, it also finds that the interconnectedness among mainstream DeFi tokens is higher than their interconnectedness with the stolen platform's native DeFi token. For instance, in the Qubit Finance platform heist, the pairwise spillover effects between the Qubit and Avalanche during the high-volatility period (95th quantile) were 14.51% and 9.81%, respectively, while the pairwise spillover effects between the Chainlink and Avalanche were 17.07% and 18.90%, respectively. This indicates that although the overall connectedness within the DeFi market is high, this high interconnectedness is predominantly among mainstream DeFi tokens.

Table 4.6: Spillover connectedness between the Qubit and five mainstream DeFi tokens in the Qubit Finance platform heist

	Panel A: Spillover connectedness at the 95th quantile						
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	24.26	14.51	15.21	15.47	14.52	16.03	75.74
	Avalanche	9.81	19.18	18.90	18.49	15.48	18.14	80.82
	Chainlink	10.41	17.07	20.84	18.03	16.07	17.57	79.16
	Uniswap	10.32	18.06	18.74	19.97	15.51	17.42	80.03
	Maker	10.50	17.64	17.99	17.29	18.69	17.89	81.31
	Stacks	11.32	17.07	17.79	16.62	16.15	21.04	78.96
	TO	52.36	84.34	88.64	85.9	77.73	87.04	TCI
	NET	-23.38	3.53	9.47	5.87	-3.57	8.09	95.20
	Panel B: Spillover connectedness at the 50th quantile							
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	50.43	12.39	9.78	7.26	8.55	11.58	49.57
	Avalanche	6.40	33.63	18.89	14.69	12.93	13.46	66.37
	Chainlink	4.82	20.32	30.98	14.88	13.06	15.93	69.02
	Uniswap	4.69	18.84	19.23	28.03	14.47	14.74	71.97
	Maker	6.17	16.74	14.27	13.87	35.79	13.16	64.21
Qubit Finance	Stacks	7.90	16.64	18.08	13.2	11.93	32.24	67.76
	TO	29.99	84.93	80.25	63.9	60.94	68.88	TCI
	NET	-19.58	18.56	11.24	-8.07	-3.27	1.12	77.78
	Panel C: Spillover connectedness at the 5th quantile							
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	21.66	15.76	15.63	13.65	18.03	15.27	78.34
	Avalanche	15.06	19.86	17.61	14.11	18.01	15.34	80.14
	Chainlink	14.60	17.48	18.99	14.60	18.93	15.39	81.01
	Uniswap	14.98	17.86	16.23	17.21	18.80	14.92	82.79
	Maker	15.85	16.46	15.18	14.07	22.57	15.87	77.43
	Stacks	15.44	16.25	15.58	14.17	19.50	19.07	80.93
	TO	75.93	83.81	80.24	70.60	93.27	76.79	TCI
	NET	-2.41	3.67	-0.77	-12.19	15.85	-4.15	96.13

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.7: Spillover connectedness between the Ronin and five mainstream DeFi tokens in the Ronin Network heist

	Panel A: Spillover connectedness at the 95th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	20.12	14.82	16.58	16.49	18.50	13.49	79.88
	Avalanche	11.77	19.60	16.42	16.50	21.80	13.91	80.40
	Chainlink	12.21	17.90	18.16	16.78	21.46	13.50	81.84
	Uniswap	11.40	17.10	15.92	18.80	22.90	13.87	81.20
	Maker	12.99	17.20	15.71	16.09	24.84	13.17	75.16
	Stacks	12.39	17.07	17.32	17.22	19.28	16.72	83.28
	TO	60.76	84.10	81.95	83.08	103.95	67.93	TCI
	NET	-19.12	3.70	0.11	1.88	28.79	-15.36	96.35
	Panel B: Spillover connectedness at the 50th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	35.44	10.27	12.96	14.51	14.19	12.62	64.56
	Avalanche	6.68	27.80	15.69	17.97	15.30	16.55	72.20
	Chainlink	9.40	16.74	25.75	18.13	14.55	15.44	74.25
	Uniswap	7.33	16.26	15.72	28.78	16.06	15.85	71.22
	Maker	8.51	16.16	13.53	18.08	31.18	12.53	68.82
Ronin Network	Stacks	9.05	16.67	14.65	17.92	13.54	28.17	71.83
	TO	40.97	76.11	72.55	86.61	73.64	72.99	TCI
	NET	-23.59	3.91	-1.70	15.4	4.83	1.16	84.58
	Panel C: Spillover connectedness at the 5th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	21.35	15.26	15.34	18.31	13.69	16.05	78.65
	Avalanche	17.65	17.53	15.07	19.15	14.79	15.80	82.47
	Chainlink	16.66	16.32	16.99	18.86	14.67	16.50	83.01
	Uniswap	16.26	17.35	15.41	19.90	14.24	16.84	80.10
	Maker	17.62	16.07	15.14	19.16	15.61	16.41	84.39
	Stacks	17.12	16.57	15.36	18.56	13.29	19.09	80.91
	TO	85.32	81.56	76.32	94.04	70.68	81.60	TCI
	NET	6.67	-0.90	-6.69	13.94	-13.71	0.69	97.91

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.8: Spillover connectedness between the Bean and five mainstream DeFi tokens in the Beanstalk protocol heist

	Panel A: Spillover connectedness at the 95th quantile						
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	26.59	14.59	12.16	13.74	14.93	17.98	73.41
	Avalanche	15.78	19.10	13.38	15.99	15.62	20.14	80.90
	Chainlink	16.64	15.59	15.76	16.09	16.05	19.87	84.24
	Uniswap	15.98	14.63	14.07	18.08	16.82	20.41	81.92
	Maker	15.97	15.23	13.44	17.18	19.53	18.65	80.47
	Stacks	16.47	14.45	12.51	14.85	14.96	26.76	73.24
	TO	80.84	74.49	65.56	77.85	78.38	97.06	TCI
	NET	7.44	-6.41	-18.69	-4.07	-2.09	23.82	94.84
	Panel B: Spillover connectedness at the 50th quantile							
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	46.70	11.61	8.23	10.15	13.08	10.22	53.30
	Avalanche	10.86	29.01	14.68	17.35	15.23	12.87	70.99
	Chainlink	9.25	15.23	27.53	19.04	17.61	11.34	72.47
	Uniswap	9.89	17.26	16.32	26.24	18.17	12.11	73.76
	Maker	10.79	15.37	13.41	18.33	30.71	11.39	69.29
Beanstalk	Stacks	9.64	12.98	11.48	12.92	10.94	42.04	57.96
	TO	50.44	72.45	64.13	77.79	75.03	57.93	TCI
	NET	-2.86	1.46	-8.34	4.03	5.73	-0.03	79.55
	Panel C: Spillover connectedness at the 5th quantile							
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	21.28	13.28	12.74	16.64	16.64	19.42	78.72
	Avalanche	17.29	15.35	13.24	17.38	16.64	20.10	84.65
	Chainlink	17.74	13.40	14.70	17.03	16.80	20.33	85.29
	Uniswap	17.25	13.97	12.96	18.29	17.39	20.14	81.71
	Maker	16.5	14.32	13.38	18.14	18.38	19.28	81.62
	Stacks	17.00	13.82	12.91	16.62	16.60	23.05	76.95
	TO	85.77	68.79	65.23	85.81	84.06	99.26	TCI
	NET	7.06	-15.85	-20.06	4.10	2.45	22.31	97.79

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.9: Spillover connectedness between the Elrond and five mainstream DeFi tokens in the Maiar Exchange heist

	Panel A: Spillover connectedness at the 95th quantile						
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	20.24	14.49	19.01	14.66	13.85	17.74	79.76
	Avalanche	14.33	16.58	20.58	15.64	15.97	16.90	83.42
	Chainlink	14.40	15.29	21.22	16.66	15.33	17.10	78.78
	Uniswap	13.82	15.69	20.14	17.39	15.94	17.02	82.61
	Maker	14.47	14.92	20.29	16.39	16.25	17.68	83.75
	Stacks	15.56	14.37	19.32	15.94	15.38	19.42	80.58
	TO	72.58	74.77	99.34	79.30	76.47	86.45	TCI
	NET	-7.18	-8.66	20.56	-3.31	-7.28	5.86	97.78
	Panel B: Spillover connectedness at the 50th quantile						
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	33.28	14.88	14.91	12.56	12.74	11.63	66.72
	Avalanche	11.59	24.07	17.46	17.58	16.76	12.54	75.93
	Chainlink	8.73	14.96	31.24	17.25	15.26	12.56	68.76
	Uniswap	7.62	16.67	19.93	26.28	16.29	13.2	73.72
	Maker	10.29	17.64	16.95	17.13	25.35	12.63	74.65
Maiar Exchange	Stacks	9.23	15.71	16.29	15.52	15.84	27.41	72.59
	TO	47.47	79.86	85.54	80.04	76.88	62.56	TCI
	NET	-19.25	3.93	16.79	6.32	2.23	-10.02	86.47
	Panel C: Spillover connectedness at the 5th quantile						
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	23.89	17.75	16.22	13.83	14.54	13.76	76.11
	Avalanche	16.83	20.63	15.12	15.67	16.92	14.84	79.37
	Chainlink	16.75	17.63	20.56	15.25	15.32	14.48	79.44
	Uniswap	17.07	18.21	17.48	17.01	15.65	14.59	82.99
	Maker	17.59	17.65	15.99	15.07	18.95	14.75	81.05
	Stacks	16.48	17.85	16.92	15.30	15.73	17.72	82.28
	TO	84.73	89.10	81.73	75.12	78.15	72.42	TCI
	NET	8.62	9.73	2.30	-7.88	-2.90	-9.87	96.25

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.10: Spillover connectedness between the Binance Coin and five mainstream DeFi tokens in the Binance platform heist

	Panel A: Spillover connectedness at the 95th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	17.71	18.85	17.20	13.48	15.07	17.69	82.29
Avalanche	16.37	20.18	17.40	12.38	16.27	17.40	79.82
Chainlink	15.39	18.53	19.93	12.26	16.55	17.34	80.07
Uniswap	15.32	18.27	16.70	16.83	15.59	17.28	83.17
Maker	14.25	17.32	17.83	12.46	20.98	17.16	79.02
Stacks	14.77	18.60	16.82	12.89	17.10	19.82	80.18
TO	76.10	91.58	85.96	63.47	80.57	86.87	TCI
NET	-6.19	11.76	5.89	-19.69	1.54	6.69	96.91
	Panel B: Spillover connectedness at the 50th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	33.96	18.16	16.80	13.66	8.32	9.10	66.04
Avalanche	16.24	31.33	16.48	12.52	9.62	13.80	68.67
Chainlink	13.70	15.34	36.45	11.88	11.37	11.26	63.55
Uniswap	14.48	16.24	13.37	32.22	10.47	13.21	67.78
Maker	10.54	11.75	12.32	11.33	39.96	14.10	60.04
Binance Stacks	10.18	15.05	14.10	10.16	11.72	38.79	61.21
TO	65.14	76.54	73.07	59.56	51.51	61.47	TCI
NET	-0.90	7.87	9.52	-8.23	-8.53	0.27	77.46
	Panel C: Spillover connectedness at the 5th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	19.90	18.85	16.54	15.12	12.45	17.15	80.10
Avalanche	17.54	21.35	16.75	15.28	12.37	16.72	78.65
Chainlink	16.05	17.39	23.17	15.18	12.86	15.35	76.83
Uniswap	16.79	18.05	16.78	18.62	12.21	17.55	81.38
Maker	15.07	16.46	16.38	13.95	21.49	16.65	78.51
Stacks	16.06	17.76	14.12	15.32	12.02	24.72	75.28
TO	81.51	88.5	80.57	74.84	61.91	83.42	TCI
NET	1.41	9.85	3.74	-6.53	-16.6	8.14	94.15

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.11: Spillover connectedness between the Mango and five mainstream DeFi tokens in the Mango Markets platform heist

	Panel A: Spillover connectedness at the 95th quantile						
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	24.97	13.25	14.38	15.70	17.08	14.62	75.03
	Avalanche	15.64	16.02	17.30	16.63	18.25	16.16	83.98
	Chainlink	15.09	15.51	18.60	16.23	18.20	16.37	81.40
	Uniswap	16.45	14.69	16.81	19.12	17.07	15.85	80.88
	Maker	15.26	14.96	16.06	16.30	22.60	14.82	77.40
	Stacks	16.21	14.62	17.14	16.69	17.01	18.33	81.67
	TO	78.65	73.04	81.69	81.54	87.62	77.82	TCI
	NET	3.62	-10.94	0.28	0.66	10.22	-3.85	96.07
	Panel B: Spillover connectedness at the 50th quantile						
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	48.11	10.87	10.67	11.59	9.13	9.63	51.89
	Avalanche	10.00	25.58	17.67	16.92	12.42	17.41	74.42
	Chainlink	9.39	18.38	26.24	18.84	11.35	15.8	73.76
	Uniswap	9.40	16.25	16.04	29.46	13.91	14.95	70.54
	Maker	7.22	14.21	11.19	16.83	37.73	12.82	62.27
Mango Markets	Stacks	10.94	17.93	14.95	16.96	11.16	28.06	71.94
	TO	46.95	77.65	70.52	81.14	57.96	70.61	TCI
	NET	-4.95	3.23	-3.24	10.60	-4.31	-1.33	80.96
	Panel C: Spillover connectedness at the 5th quantile						
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	24.61	14.78	11.81	14.74	18.10	15.96	75.39
	Avalanche	15.76	19.13	13.22	15.81	17.64	18.45	80.87
	Chainlink	15.75	16.66	17.68	15.18	16.27	18.47	82.32
	Uniswap	14.27	17.44	12.87	18.26	16.61	20.55	81.74
	Maker	14.49	16.36	12.09	15.35	23.10	18.61	76.90
	Stacks	14.82	17.20	13.38	14.55	17.08	22.98	77.02
	TO	75.08	82.43	63.37	75.63	85.7	92.04	TCI
	NET	-0.31	1.56	-18.96	-6.11	8.79	15.02	94.85

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 20 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

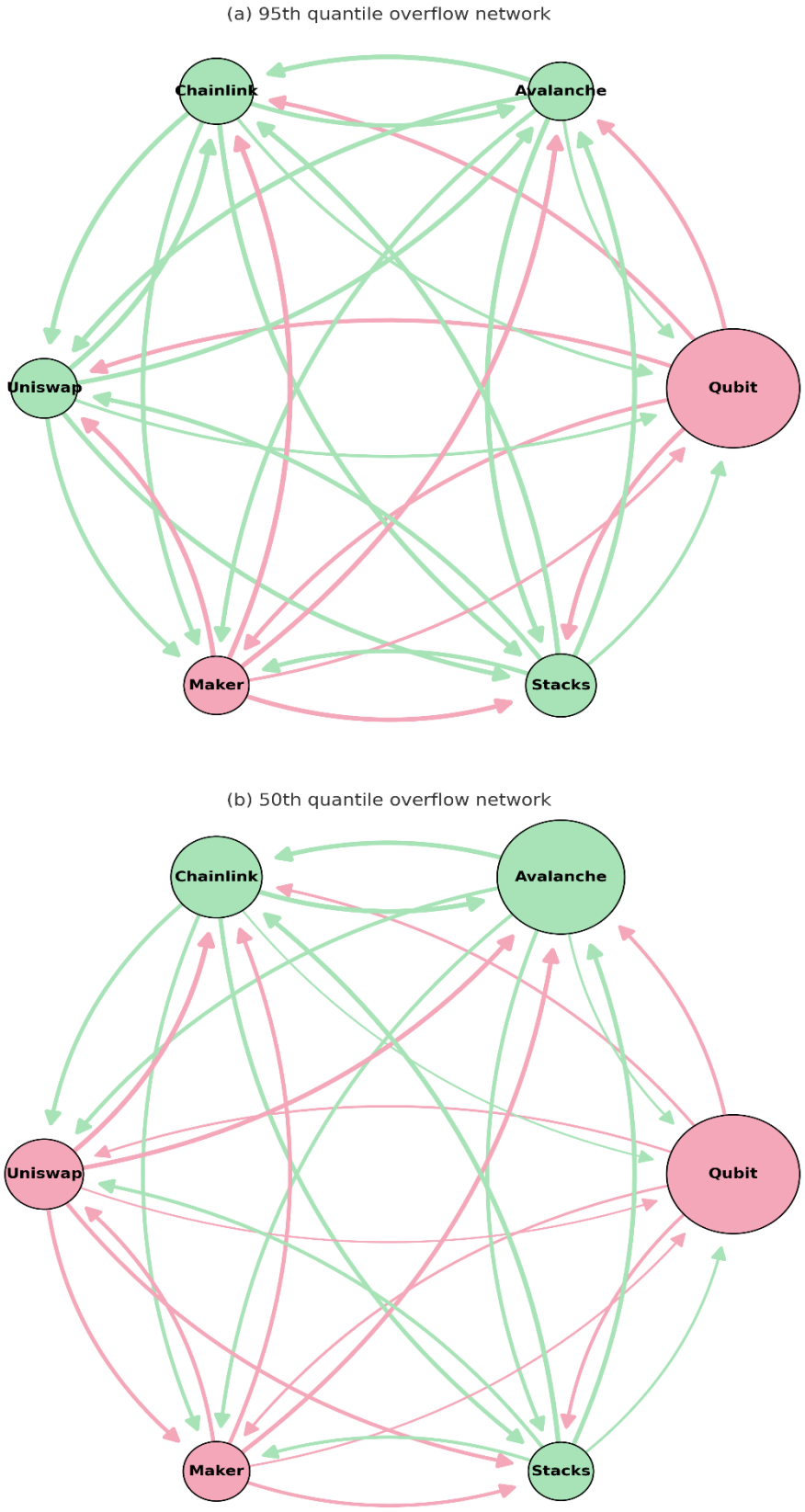
In the cryptocurrency market, large-cap tokens tend to be the initiators and receivers of volatility, which is related to their market capitalisation and high liquidity (Corbet et al., 2018b; Yi et al., 2018; Ji et al., 2019; Omane-Adjepong & Alagidede, 2019; Yousaf et al., 2024b). Mainstream DeFi tokens generally have larger market capitalisation and higher liquidity, which allows their market fluctuations to be more effectively transmitted to other

mainstream tokens. Additionally, mainstream DeFi tokens are widely used and integrated across multiple DeFi protocols and trading platforms, further enhancing their network effects and interconnectedness. The high degree of interconnectedness among mainstream DeFi tokens also reflects investor behaviour patterns. Investors tend to focus on and invest in tokens with larger market caps and higher liquidity (Hasan et al., 2022; Ozdamar et al., 2022), resulting in more frequent capital flows among these tokens and strengthening their volatility transmission effects. In contrast, the native DeFi tokens on the stolen platforms have smaller market capitalisations. Small-cap DeFi tokens, due to their lower market capitalisation, insufficient liquidity, and limited application and integration within the DeFi ecosystem, exhibit relatively weaker connectedness with mainstream DeFi tokens. These findings are consistent with previous studies by Corbet et al. (2019a) and Yarovaya and Zięba (2022), which observed that interconnectedness within the cryptocurrency market is primarily seen among leading cryptocurrencies and is stronger in the short term. Therefore, considering the *TCI* and the interconnectedness among various DeFi tokens, it is concluded that the interconnectedness is higher among mainstream DeFi tokens, while the connectedness between the native DeFi tokens of the stolen platforms and mainstream DeFi tokens is lower.

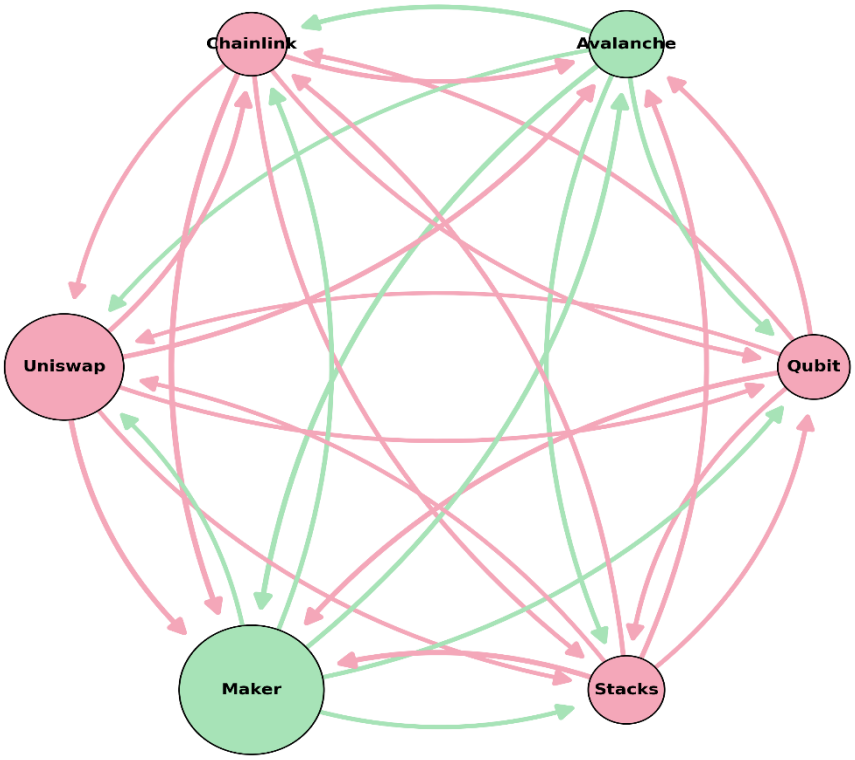
Next, although the native DeFi tokens of the stolen platforms exhibit spillover effects on other mainstream DeFi tokens (as indicated by positive *TO* values), a comparison of the *TO* values across tokens reveals that most of these native DeFi tokens have lower *TO* values than other mainstream DeFi tokens. Furthermore, as shown in the connectedness networks (Figures 4.5–4.10), most of the stolen platforms' native DeFi tokens are net receivers of volatility (red nodes represent receivers, whereas green nodes represent transmitters). This suggests that the volatility transmitted from the stolen platforms' native DeFi tokens to other mainstream DeFi tokens is smaller than the volatility they receive from them. In addition, the volatility received by mainstream DeFi tokens primarily originates from within their own network rather than from the native DeFi tokens of the stolen platforms[7].

[7] This can be seen from the interconnectivity value between DeFi tokens, which can be observed at the intersection of the rows and columns corresponding to two DeFi tokens in the spillover connectedness table.

Figure 4.5: Quantile overflow network between the Qubit and five mainstream DeFi tokens in the Qubit Finance platform heist

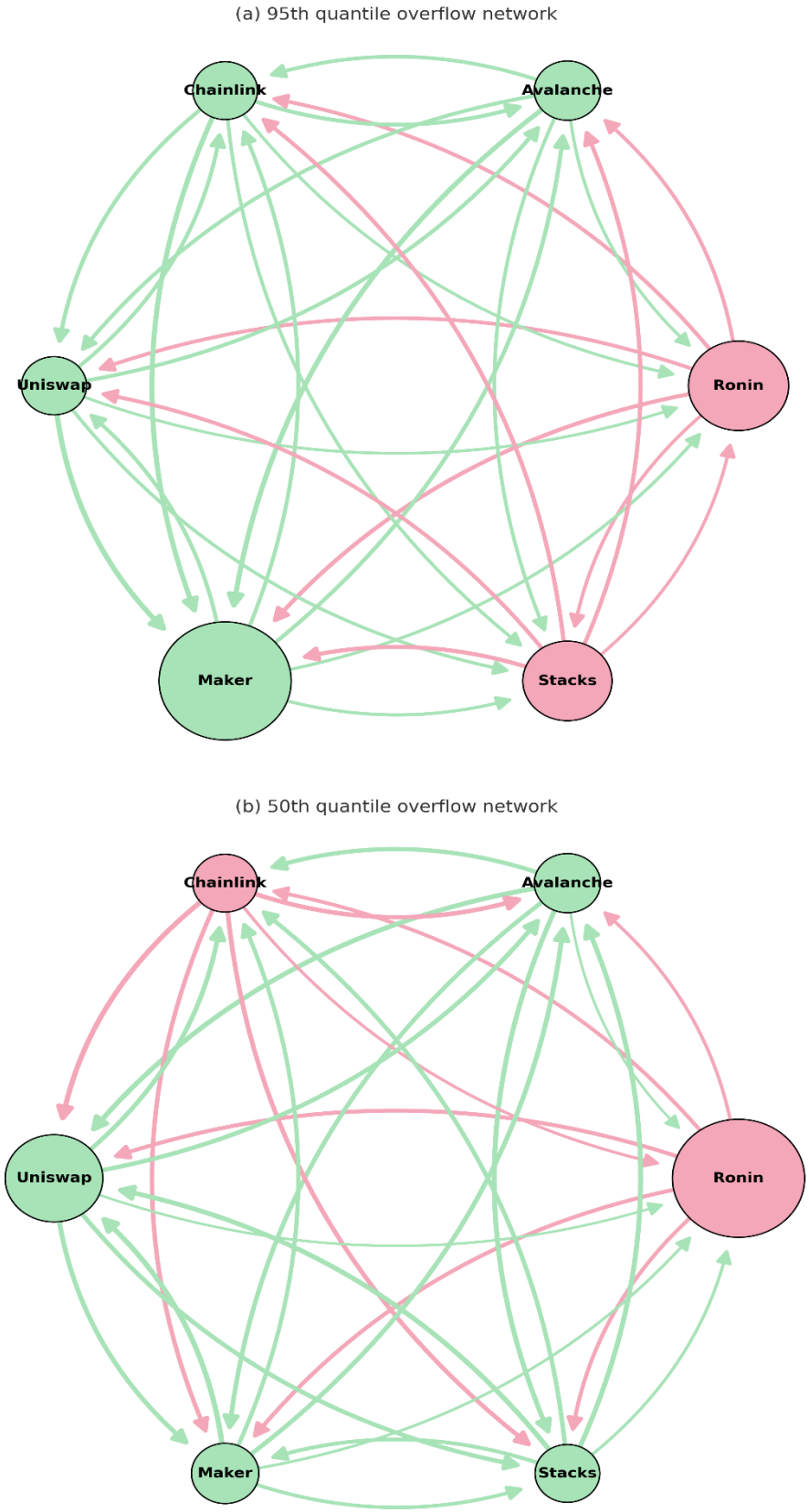


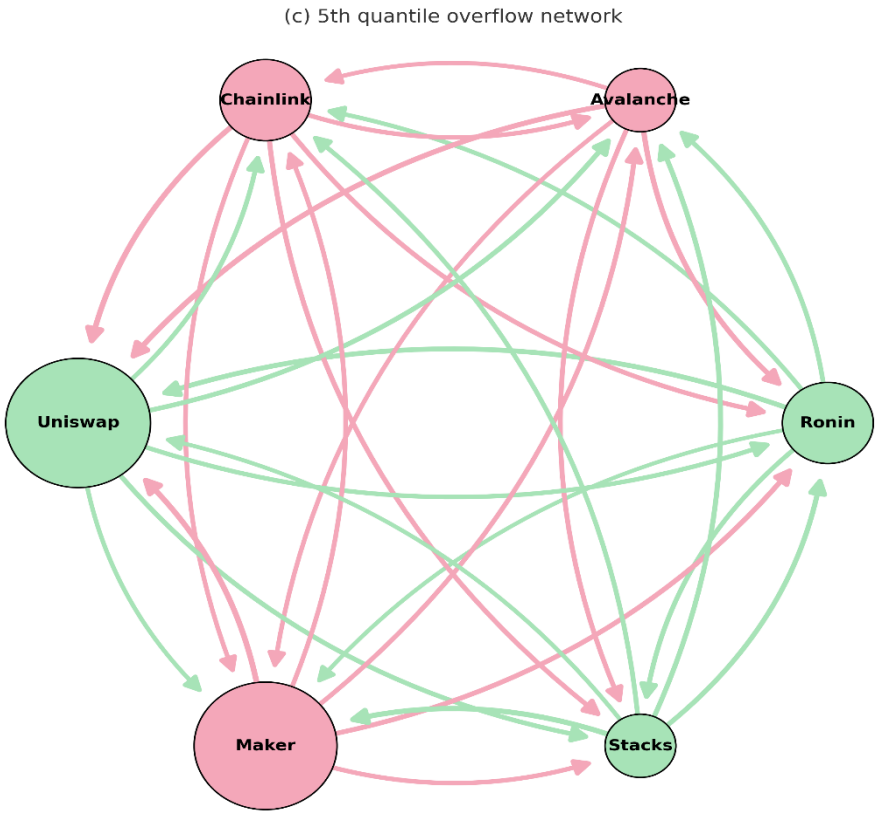
(c) 5th quantile overflow network



Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

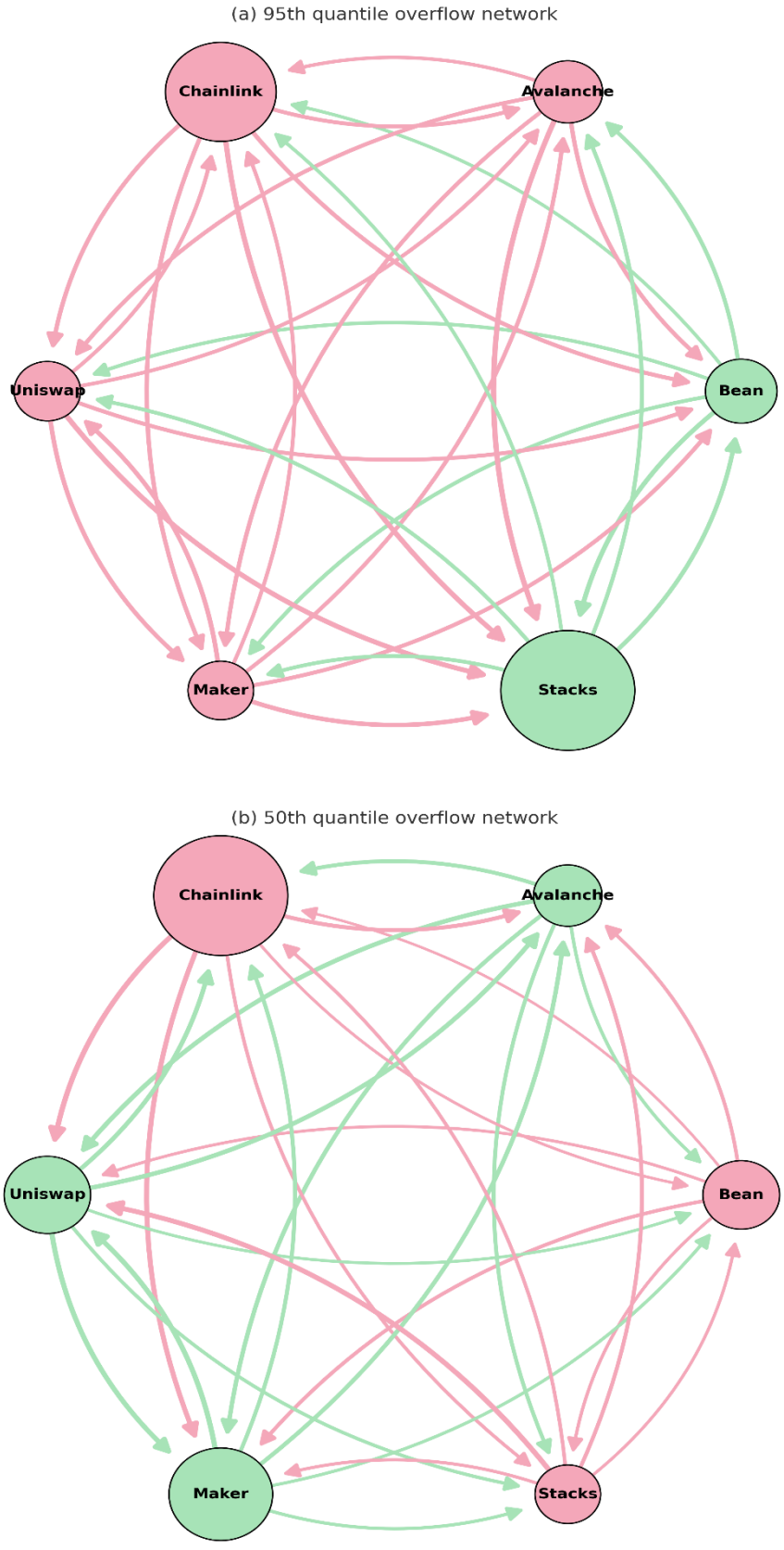
Figure 4.6: Net spillover between the Ronin and five mainstream DeFi tokens in the Ronin Network heist

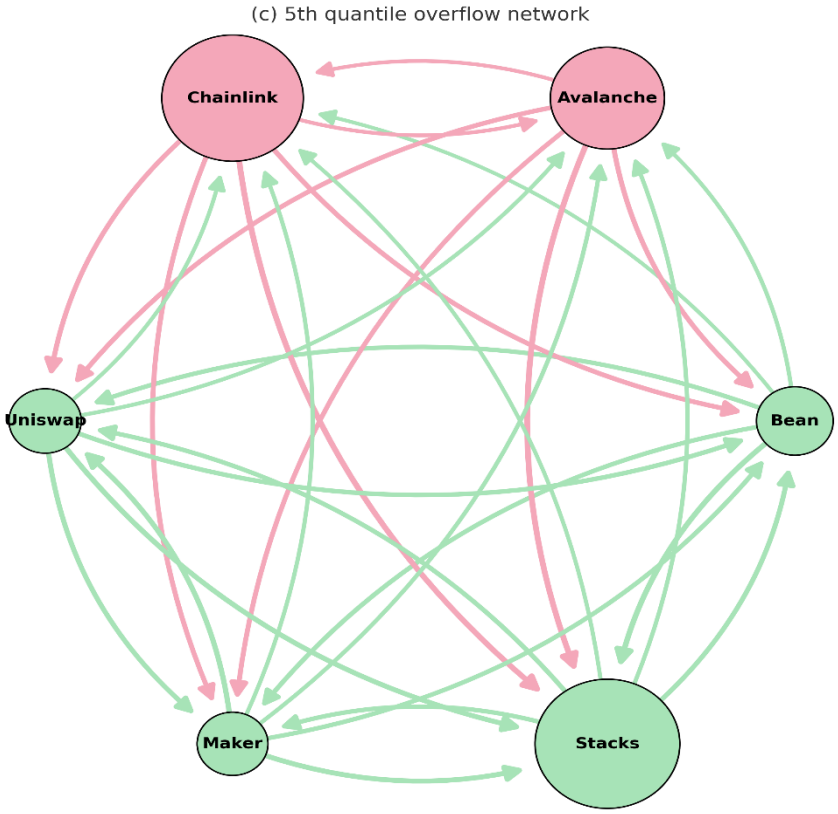




Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

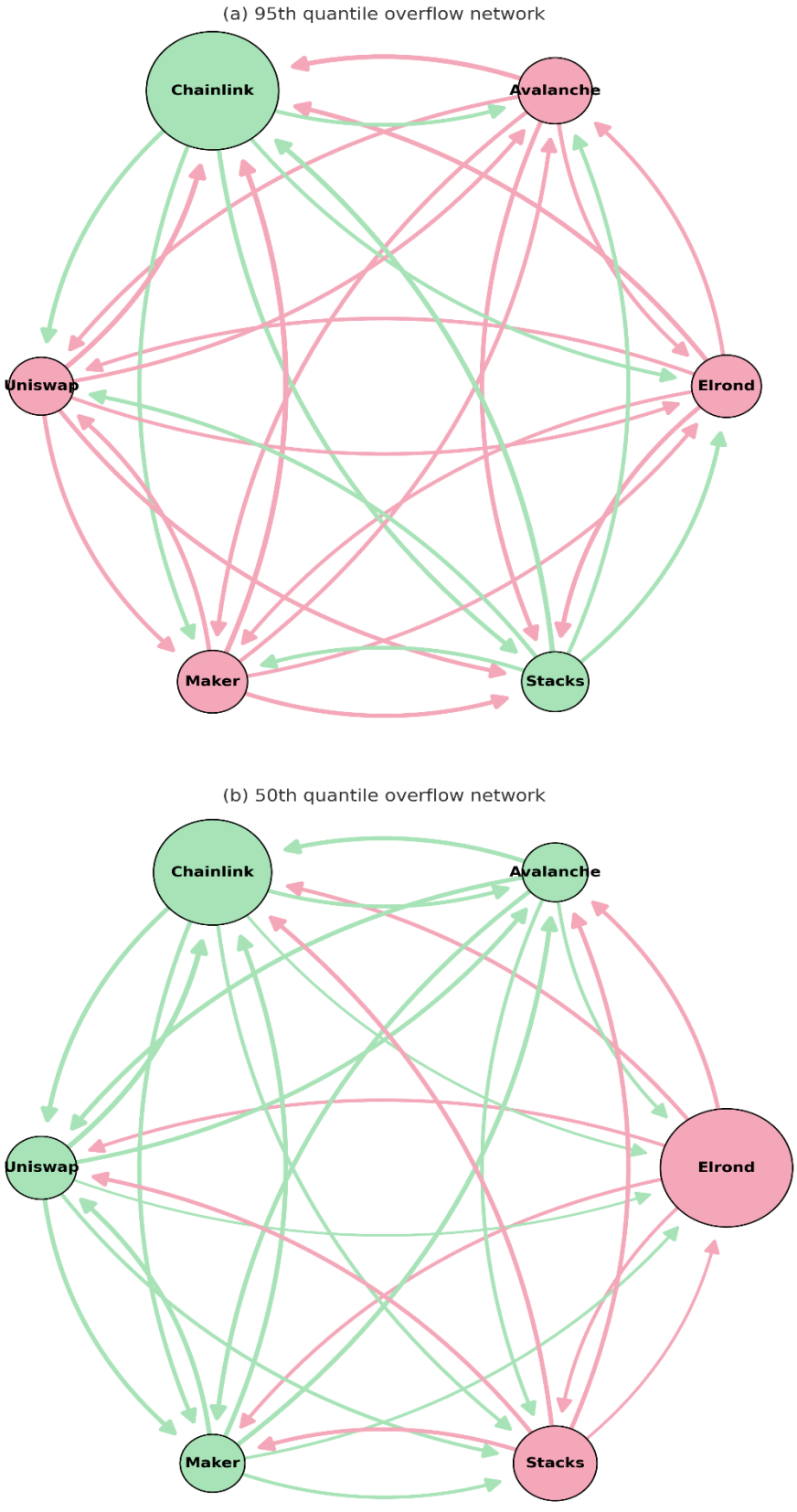
Figure 4.7: Net spillover between the Bean and five mainstream DeFi tokens in the Beanstalk protocol heist

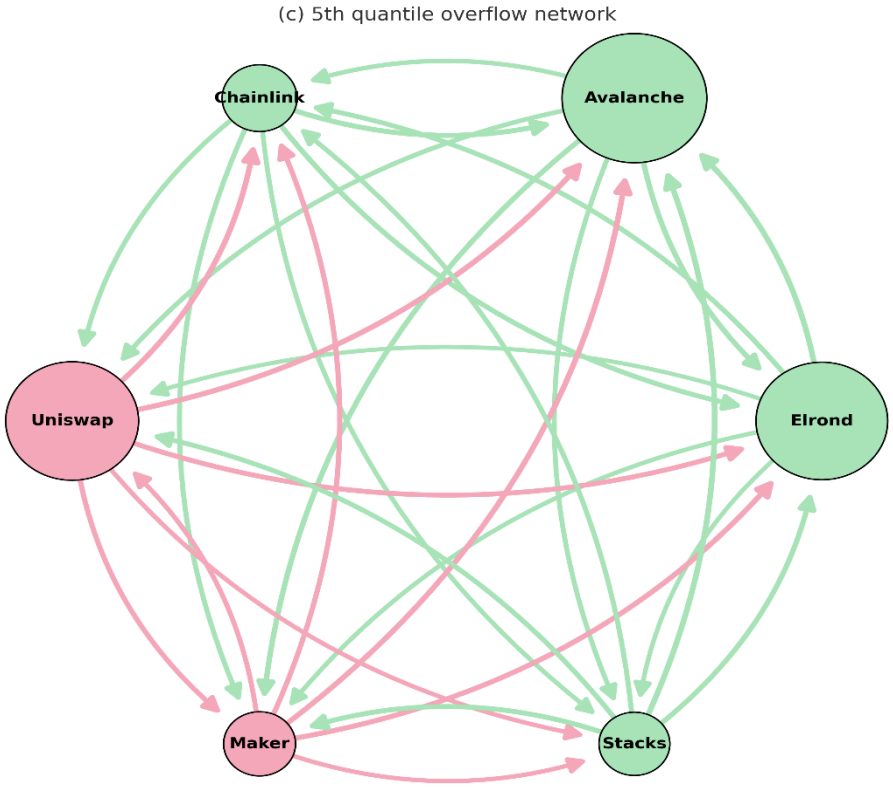




Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

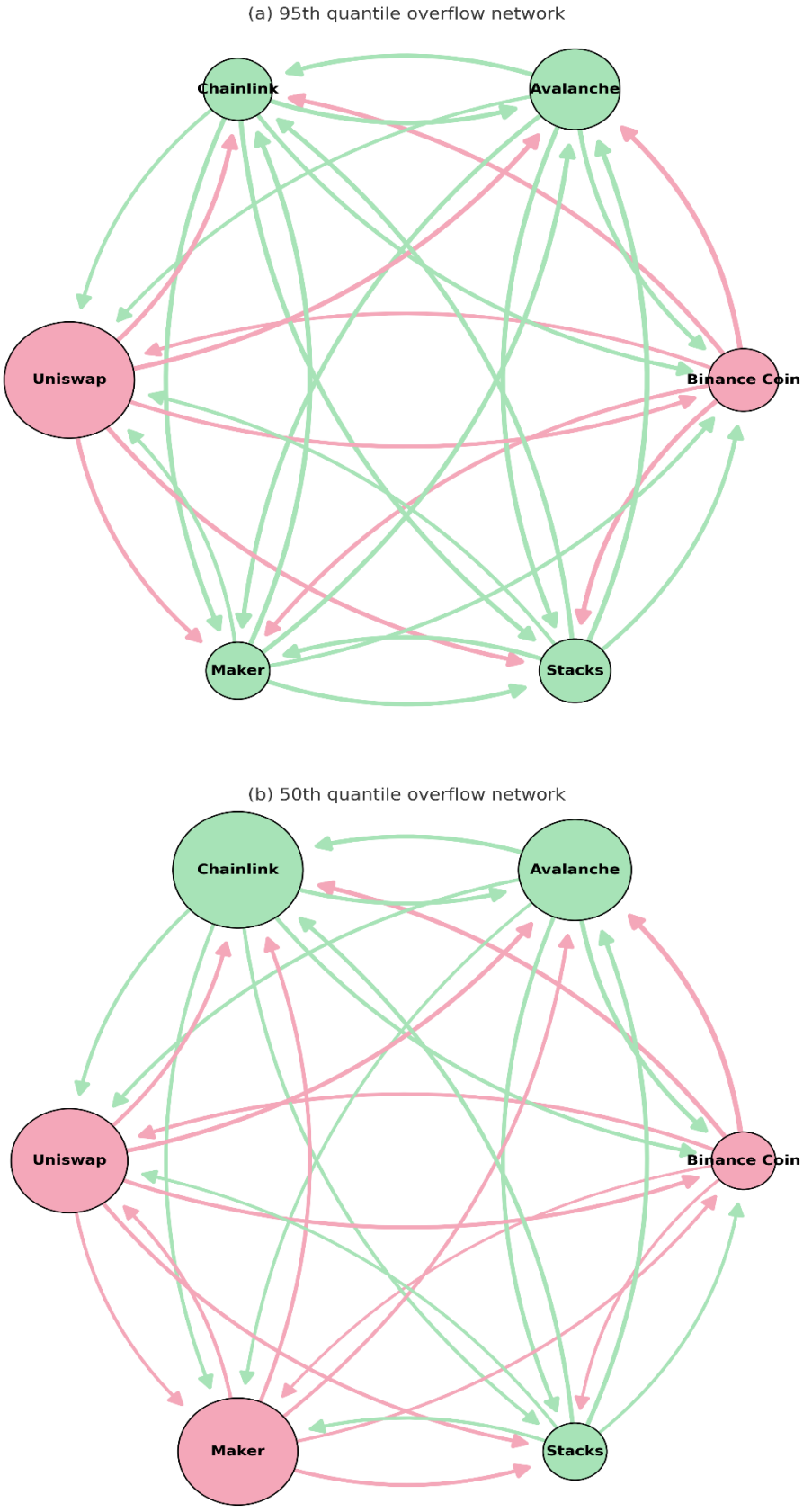
Figure 4.8: Net spillover between the Elrond and five mainstream DeFi tokens in the Maiar Exchange heist

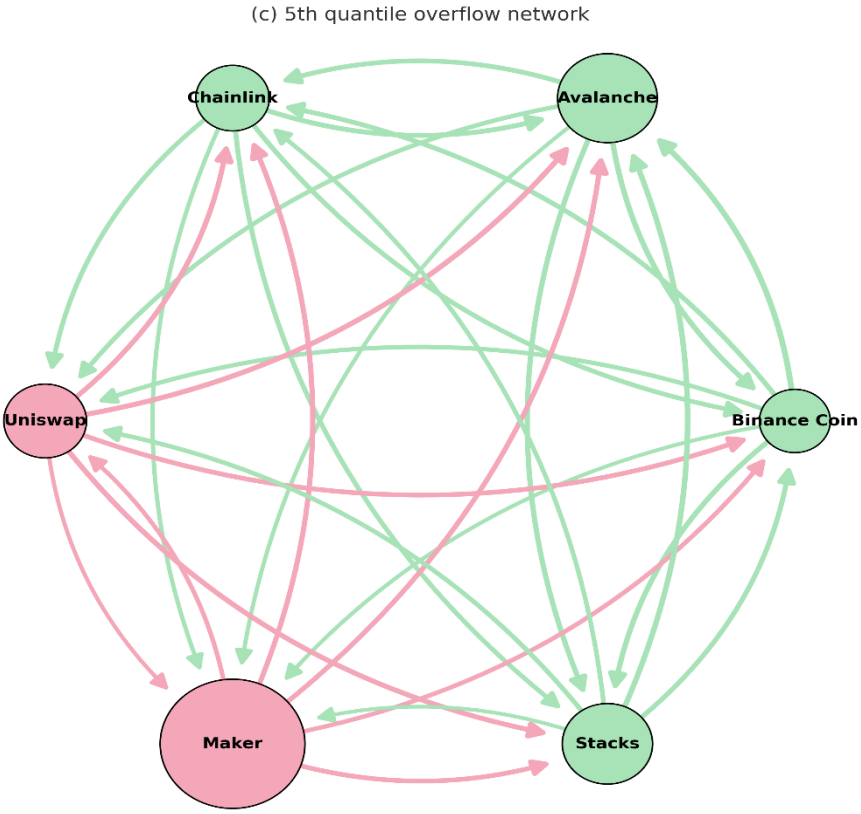




Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

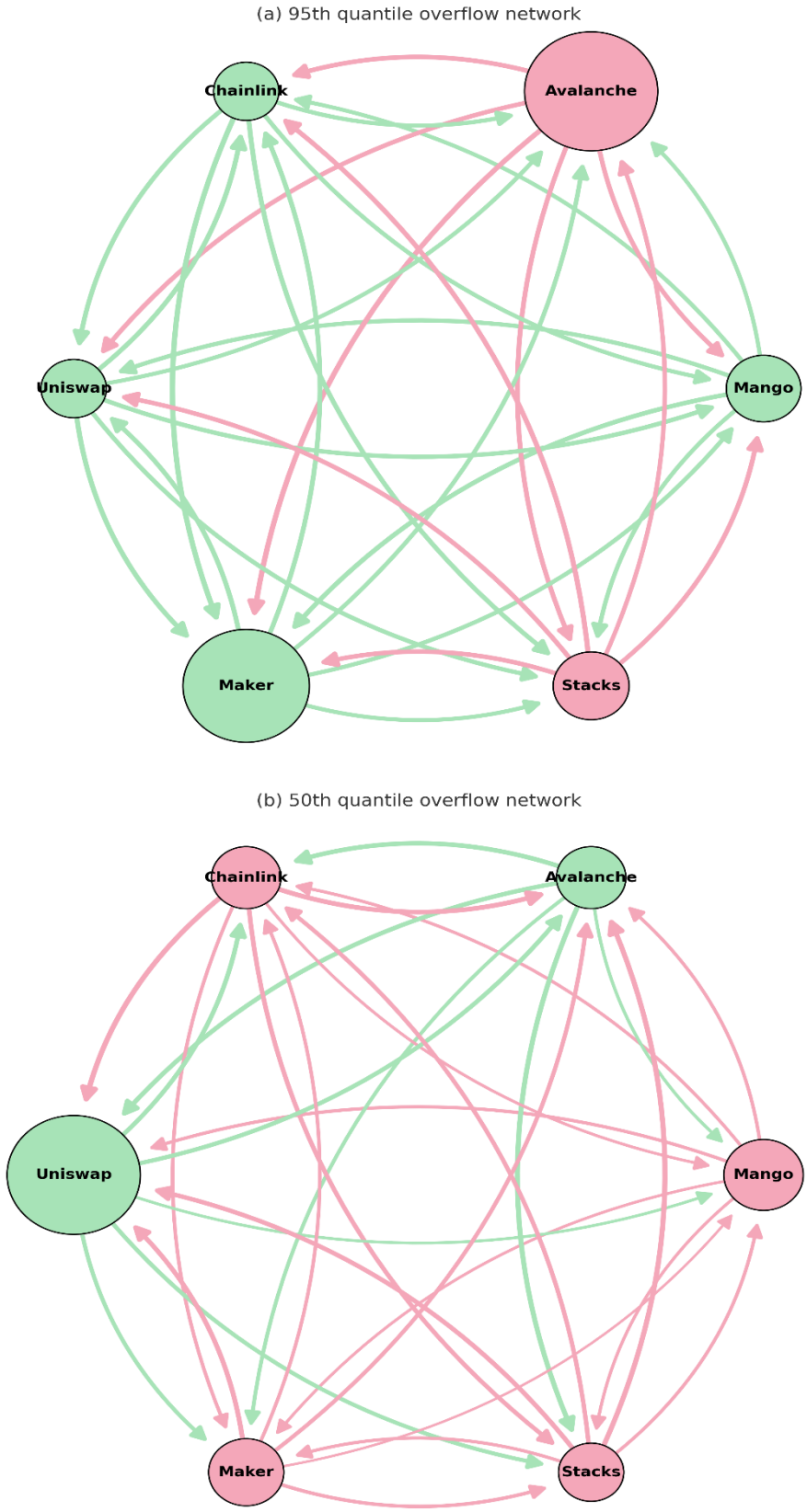
Figure 4.9: Net spillover between the Binance Coin and five mainstream DeFi tokens in the Binance platform heist

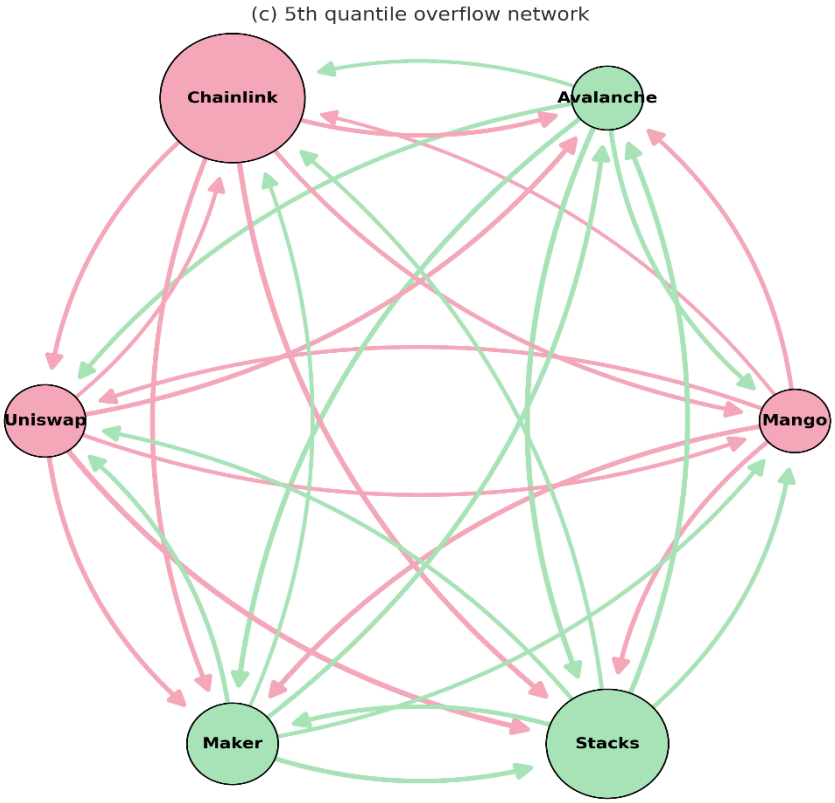




Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

Figure 4.10: Net spillover between the Mango and five mainstream DeFi tokens in the Mango Markets platform heist





Based on the full-sample QVAR model with a lag order of 1 and a forecast market dynamics 10 time steps into the future. Node colours represent the sign of the net spillover, with red indicating receivers of volatility and green indicating transmitters. Node sizes reflect the magnitude of the absolute net spillover. Arrows on the edges indicate the direction of spillovers, while edge widths capture the spillover intensity. To account for overlapping edges, curved edges are used in the visualisation.

While a heist targeting a specific DeFi platform could cause volatility in the platform's native DeFi token and transmit some of this volatility to other mainstream DeFi tokens, the contagion effect is relatively weak. This aligns with the previous analysis that the connectedness level between mainstream DeFi tokens and the native DeFi tokens of stolen platforms is low. The diversity of protocols and assets within the DeFi market helps absorb the impact of individual assets. Even if the native DeFi token of one platform is compromised, other platforms' DeFi tokens continue to support the DeFi market, mitigating the spread of negative effects (Metelski & Sobieraj, 2022). Furthermore, in this chapter, the most affected DeFi tokens hold a small market share within the DeFi market, limiting their impact on overall market volatility. Other mainstream DeFi tokens could stabilise the market environment and buffer the shocks potentially caused by DeFi heists (Kollias et al., 2011). Investors may also have developed certain psychological expectations and behavioural adaptations to DeFi heists. Given that most hacker attacks target DeFi protocols, investors might now consider them a normal occurrence within the DeFi investment space. According to Immunefi (2023), there were 155 attacks targeting DeFi in 2022 alone. Therefore, a single

DeFi heist does not trigger excessive market reactions, as investors have learned to incorporate such risks into their investment strategies, thereby reducing the overall market impact of these events.

In the Beanstalk protocol heist, the Bean exhibits significant spillover effects (high *TO* values and positive *NET* values) at extreme quantiles (Table 4.8 and Figure 4.7). This indicates that the impact of the Beanstalk protocol heist on the DeFi market is considerably greater than that of other DeFi heists that this chapter investigates. A possible explanation for this is that the attack exploited Beanstalk protocol's majority voting governance system, which is a core feature of many DeFi protocols. Like many other DeFi projects, the Beanstalk protocol incorporates a governance mechanism where participants can collectively vote on code changes. They receive voting power proportional to the value of the Bean they hold. According to Certik (2022), the attacker utilised a flash loan obtained through the decentralised protocol Aave to borrow nearly $1 billion in cryptocurrency assets. They then used these assets to acquire enough bean tokens to gain 67% voting power in the project. With this absolute majority, they were able to approve the execution of code that transferred the assets to their wallet. The attacker then immediately repaid the flash loan, netting $80 million in profit.

The vulnerability in the majority voting governance system raised concerns among investors about the security of other DeFi protocols. This incident highlighted the potential risks associated with governance mechanisms that allow significant control through token holdings, especially when such control can be quickly accumulated via flash loans. Chainalysis (2024a) reported that governance attacks result in an average loss of about $1 million, ranking second among all types of DeFi attack methods. The resulting fear and uncertainty may have had a broader impact on the DeFi market, as investors began to question the robustness and security of similar governance structures in other projects (Bouri et al., 2021a; Corbet et al., 2022). Investors losing confidence might decide to divest from these projects, leading to selling pressure and price declines. Additionally, in response to perceived risks, investors might reallocate their funds to what they consider safer assets, including more established cryptocurrencies or stablecoins, further increasing the selling pressure on DeFi tokens. Previous studies have also highlighted the vulnerability of decentralised governance in DeFi. Dotan et al. (2023) pointed out that the use of governance tokens exhibits a strong tendency toward centralisation, which may undermine the security of DeFi platforms. Gudgeon et al. (2020) proposed a novel strategy that exploits so-called flash loans, which in principle

enables a governance attack to be executed with only two transactions and without locking any assets, further underscoring how deficiencies in governance design can trigger crises in DeFi protocols.

To sum up, the analysis highlights the interconnectedness within the DeFi market and the varying degrees of spillover effects among different DeFi tokens. Mainstream DeFi tokens exhibit significant interconnectivity and mutual influence, but they tend to be less interconnected with smaller DeFi tokens from stolen platforms. The Beanstalk protocol heist, however, stands out due to its significant spillover effects, underscoring the vulnerabilities in governance mechanisms that can be exploited via flash loans. This incident has not only shaken investor confidence in Beanstalk protocol but also raised broader concerns about the security of DeFi protocols with similar governance structures. The resultant fear and uncertainty have led to increased market volatility, with investors reallocating funds to perceived safer assets, thereby exerting further selling pressure on DeFi tokens. These findings emphasise the importance of robust governance and security measures in maintaining market stability and protecting investor interests in the rapidly evolving DeFi landscape.

4.4.3 Robustness Tests of Liquidity Analysis and Volatility Spillover Effects

To mitigate the estimation instability caused by the limited number of hourly observations, this chapter reports the results of estimating the three liquidity indicators using a 6-hour rolling window in Appendix 4.7. The rolling-window approach incorporates overlapping samples from adjacent time intervals, helping to smooth out the influence of outliers and capture the dynamic evolution of liquidity over time. This method enhances the ability to detect structural changes in liquidity before and after DeFi heists, thereby improving the robustness and interpretability of the estimates. The corresponding results are presented in Figures 4.11–4.16 in Appendix 4.7.

Consistent with the earlier results, the liquidity of Qubit and Mango deteriorated significantly following the heists (Figures 4.11 and 4.16). This is reflected in the upward trend of the *Amihud* and *Kyle* after the heists, accompanied by a decline in the *Amivest*, indicating higher trading costs and reduced market depth. For Ronin and Elrond, liquidity deterioration was particularly severe on the day of the heists (Figures 4.12 and 4.14), as evidenced by the sharp increase in the *Amihud* and *Kyle* within on the day of the heists, suggesting a short-term liquidity shock. The liquidity dynamics of Bean (Figure 4.13) also point to substantial

deterioration, with *Amihud* and *Kyle* rising markedly in the post-heist period, while the *Amivest* declined significantly, highlighting sustained liquidity stress. In contrast, Binance Coin's liquidity showed no significant change before and after the heist (Figure 4.15), with only a slight deterioration on the day of the heist, followed by a quick recovery to its pre-heist level. Overall, the robustness checks confirm that DeFi heists exert significant negative impacts on the liquidity of the native DeFi tokens of the stolen platforms, while the magnitude and persistence of these effects vary across DeFi tokens.

Furthermore, Appendix 4.7 reports the robustness results obtained by re-estimating the QVAR model using a longer 80-hour rolling window while keeping the forecast horizon fixed at 10 steps, to test the sensitivity of the results to the choice of rolling window length. A longer window provides more effective observations at the tail of the sample, reducing estimation variance and yielding smoother and more stable quantile estimates. The robustness results presented in Tables 4.12–4.17 in Appendix 4.7 indicate that, even under extreme market conditions, the *TCI* continues to show a high degree of volatility synchronisation among DeFi tokens, with strong interconnectedness remaining concentrated among the major DeFi tokens. During the most DeFi heist periods, the volatility received by mainstream DeFi tokens mainly originates from within the mainstream DeFi token network rather than from the native DeFi token of the stolen platform. In the Beanstalk protocol heist, Bean still exhibits significant spillover effects at extreme quantiles, further indicating that this DeFi heist has a severe impact on the DeFi market due to its attack on the governance mechanisms. Overall, the findings are consistent with the previous results, suggesting that the choice of estimation window does not drive the conclusions.

In summary, the robustness tests on liquidity and volatility spillovers support the previous findings. First, regarding liquidity, the robustness checks of the three liquidity indicators consistently show that most stolen platforms' native DeFi tokens experience significant liquidity deterioration after the DeFi heists, further confirming the negative impact of DeFi heists on these DeFi tokens' liquidity. Second, in terms of volatility spillovers, the QVAR results re-estimated with a longer rolling window remain consistent with the baseline, indicating that under extreme market conditions, volatility across different DeFi tokens continues to move in a highly synchronised manner. However, the strongest interconnectedness is observed among mainstream DeFi tokens rather than the native tokens of the stolen platforms. This suggests that the overall impact of DeFi heists on the wider DeFi market is limited, with the negative effects concentrated mainly on the stolen platforms

themselves, thereby highlighting the resilience of the DeFi market in the face of such shocks. However, attacks targeting the governance mechanisms may trigger widespread concerns about the security of other DeFi protocols with similar structures, further amplifying market uncertainty. This highlights the need for future DeFi protocols to pay particular attention to vulnerabilities in their governance system.

4.5 Potential Regulatory Recommendations

In the face of increasingly frequent DeFi hacking attacks, implementing appropriate regulatory measures is urgent and crucial for protecting protocol developers and investors. Currently, the regulatory environment for DeFi remains uncertain and varies significantly across different jurisdictions. For example, the European Union finalised the Markets in Crypto-Assets Regulation (MiCA) in 2023, becoming the first jurisdiction to adopt a comprehensive regulatory framework for digital assets. MiCA provides legal clarity regarding the privacy, security, and transparency of crypto-assets, requiring issuers to publish approved white papers and obtain regulatory authorisation. Non-compliance may result in penalties (European Union, 2023a). However, MiCA excludes crypto-asset services that are offered in a fully decentralised manner without the involvement of any intermediaries. This has created ambiguity in the regulation of DeFi platforms, as MiCA equates decentralisation with the complete absence of intermediaries (European Union, 2023b). In reality, many DeFi ecosystems rely on critical intermediaries that play a pivotal role in the functioning and sustainability of the system. These are often referred to as systemically important crypto intermediaries (SICIs). As such, the key challenge for the European Union regulators lies in distinguishing between genuinely decentralised systems and those that merely reduce, but do not eliminate, intermediation.

Hong Kong has not yet introduced DeFi-specific legislation, but regulates DeFi-related activities through its existing financial regulatory framework. The Securities and Futures Commission (SFC) evaluates DeFi activities based on their actual operation under the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering Ordinance (AMLO). This functional approach follows the principle of “same business, same risks, same rules,” aiming to strike a balance between financial innovation and regulatory integrity (Financial Services and the Treasury Bureau, 2023). Meanwhile, the Hong Kong Monetary Authority (HKMA) has issued guidelines for banks on the risk management considerations associated with adopting distributed ledger technology (DLT), reflecting a growing interest in

integrating DLT into traditional finance (Hong Kong Monetary Authority, 2024). The key challenge in Hong Kong is maintaining regulatory transparency and accountability while fostering innovation.

In Singapore, the regulatory framework for digital assets is based primarily on the Payment Services Act of 2019 and the Financial Services and Markets Act of 2022, both overseen by the Monetary Authority of Singapore (MAS) (2019, 2022). While MAS has acknowledged the risks associated with DeFi and issued consumer advisories, the existing legislation does not comprehensively cover all forms of DeFi activity, particularly those involving decentralised governance and anonymous transactions. The main challenge for Singaporean regulators is to ensure financial stability and investor protection without stifling innovation in the DeFi space.

The United Kingdom is in the process of developing a comprehensive regulatory regime for digital assets. The Financial Conduct Authority (FCA) oversees crypto-asset activities under the Financial Services and Markets Act 2023, and regulations differentiate between digital securities, unbacked crypto-assets, and stablecoins. The HM Treasury (2023) has signalled that DeFi will be addressed under its future financial services regulatory framework, with a focus on eliminating regulatory arbitrage. The key regulatory challenge in the United Kingdom lies in defining legal boundaries for DeFi and designing flexible, yet enforceable, rules that can accommodate its diverse governance structures.

The United States adopts a fragmented regulatory model for digital assets, with oversight shared among multiple agencies, including the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Crimes Enforcement Network (FinCEN), and the Federal Deposit Insurance Corporation (FDIC) (Emmert, 2023). These agencies attempt to apply existing securities and commodities laws to DeFi protocols, often relying on enforcement actions due to a lack of unified regulatory guidance. The Financial Innovation and Technology for the 21st Century Act (FIT21) represents a recent attempt to establish a compliant pathway for decentralised networks, including computing and social networks, ensuring that digital assets receive appropriate and secure regulatory treatment (Gensler, 2024). The central challenge in the United States is how to establish clear and coherent compliance mechanisms for decentralised systems without undermining innovation or pushing projects offshore.

Overall, different jurisdictions have adopted diverse regulatory approaches to DeFi, reflecting varying interpretations of decentralisation and different balances between innovation and oversight. The European Union offers a unified framework but faces definitional challenges. Jurisdictions such as Hong Kong and Singapore pursue function-based, gradual approaches, while the United Kingdom is working to develop a forward-looking but structured regime. The United States, by contrast, exhibits fragmented enforcement with limited clarity. These regulatory divergences may lead to inconsistencies and jurisdictional arbitrage in the global DeFi ecosystem, while also opening the door for international cooperation in shaping future standards. This chapter attempts to propose some regulatory methods for the future of DeFi based on the primary economic rationale of regulating financial intermediary activities, thereby reducing the negative impact of DeFi heists.

The primary economic rationale for regulating financial intermediary activities is the existence of market failures, which could, in principle, be improved through policy intervention. Market failures can be categorised into two main types: (i) information problems and (ii) externalities (Aquilina et al., 2024).

4.5.1 How to Solve Information Problems

Information problems include both information insufficiency and information asymmetry (Aquilina et al., 2024). In the DeFi market, investors often lack adequate information. For instance, they may question whether they can fully trust the development team behind a dapp or whether specific smart contracts have vulnerabilities that hackers could exploit. Regarding information asymmetry, it is difficult for investors to distinguish between high-quality and low-quality projects in the DeFi market. Some low-quality projects may persist in the market for a long time and are more susceptible to hacker attacks due to a lack of robust security measures. Additionally, the structure of many Decentralised Autonomous Organisations (DAOs) that dapps rely on makes it challenging to understand where decision-making authority lies and who is accountable for the consequences of such decisions (Doerr et al., 2021). This complexity can leave investors unable to protect their interests in the event of a DeFi heist.

To mitigate issues of information insufficiency and asymmetry, regulatory authorities can require DeFi projects to introduce third-party platforms to monitor on-chain illegal activities and conduct third-party audits to assess and review the security of projects. Third-party platforms can monitor on-chain activities in real time, detect and report suspicious

transactions, and prevent the spread of illegal activities. Meanwhile, third-party audits can uncover vulnerabilities and security risks in smart contracts, helping development teams fix them promptly and prevent exploitation by hackers. For investors, the monitoring results and audit reports from third parties can help them differentiate between high-quality and high-risk projects, avoiding investments in the latter. Furthermore, the involvement of third parties could increase investor confidence in DeFi projects, knowing that these projects have been validated by independent entities.

There are many on-chain security monitoring and project auditing platforms, such as Hacken and Certik. Hacken provides these services to many clients, such as FTX and Gate.io, as well as data provider CoinGecko. The foundation has even partnered with the government of Ukraine to support its blockchain initiatives. Certik offers services to inspect project code security, identifying any vulnerabilities that hackers could exploit. Developers can fix issues before re-auditing, aiming for positive results (Rearick, 2022). However, the challenge is that auditing standards vary between firms, and their reliability remains unclear (Yuyama et al., 2023). Currently, most global regulatory efforts for DeFi focus primarily on centralised intermediaries, stablecoins, and AML/KYC compliance. Areas such as security auditing and technical transparency remain underregulated. Therefore, future regulatory efforts should aim to formalise and standardise third-party auditing practices within the regulatory framework. Doing so would help bridge the gap between voluntary self-regulation and formal oversight, thereby reducing the risk of DeFi projects being exploited by malicious actors.

4.5.2 How to Solve External Problems

In financial markets, the actions of one party in a financial transaction can significantly impact other entities and, in some cases, even affect the stability of the entire system. The most notable example of this is the 2008 subprime mortgage crisis in the United States (Brunnermeier et al., 2009; Aquilina et al., 2024). In the DeFi sector, whether through collateralisation, staking, or any other crypto-financial model, many DeFi protocols are interlinked. The advantage of this interconnectivity is that during periods of market stability and growth, the synergies between DeFi protocols can create a positive feedback loop, propelling the crypto industry upward. However, the same interconnectivity can lead to a ‘death spiral’ during market downturns, causing a chain reaction of negative effects. Although this chapter's findings indicate that the impact of smaller DeFi tokens from compromised platforms on mainstream DeFi tokens is minimal, we cannot overlook the broader

implications of heists on the DeFi ecosystem. As observed in the Beanstalk protocol heist, investors' broader concerns about the security of DeFi protocols with similar voting governance systems can exacerbate market volatility. This underscores the need for effective regulatory measures to mitigate external volatility in the DeFi market.

Aquilina et al. (2024) showed that in traditional financial markets, systemic externalities could be mitigated through four approaches: (i) prudential regulation of financial institutions; (ii) stringent risk management requirements; (iii) deposit insurance for deposit-taking institutions; and (iv) the central bank acting as the lender (or dealer) of last resort in extreme situations. The DeFi market could adopt these regulatory strategies from traditional financial markets to enhance its stability in the face of DeFi heists.

For example, (i) similar to addressing information problems, implementing regular audits and compliance checks in DeFi could ensure that projects adhere to security and operational standards. This could be achieved through third-party auditing firms that assess the robustness of smart contracts and the overall security framework of the platform. (ii) DeFi projects should set leverage limits, ensure adequate collateral for loans, and implement automated liquidation mechanisms to manage risks in real time. Specifically, if a DeFi platform sets a leverage limit, even if hackers attempt to exploit vulnerabilities to borrow large amounts, the leverage cap will restrict their borrowing capacity, thereby reducing potential losses. In terms of collateral, if a DeFi project requires 150% collateral for each loan, the collateral can cover the loan amounts even if hackers manipulate the market to cause significant price swings, reducing financial stress on the platform. Lastly, during a DeFi heist, automated liquidation mechanisms can quickly react to liquidate problematic loans, protecting the overall health of the platform and preventing larger financial losses.

(iii) DeFi projects could provide insurance to cover losses resulting from hacking incidents or smart contract failures. At present, almost all traditional financial institutions are unwilling to provide insurance coverage for crypto assets (Zhou & Zhang, 2025). As a result, the DeFi ecosystem has been compelled to develop its own insurance projects to meet the inherent demand for risk-sharing and loss mitigation through smart contracts. This could be achieved through decentralised insurance protocols that pool resources from multiple participants to provide coverage for specific risks. Nexus Mutual is one of the earliest and most prominent decentralised insurance protocols built on the Ethereum blockchain. Operating under a mutual insurance model, it allows members to pool capital to provide coverage against risks

such as smart contract vulnerabilities, exchange hacks, and, more recently, yield-bearing token risks. Claims are assessed and settled through a decentralised governance process, in which holders of the native Nexus Mutual token vote on the validity of claims, with economic incentives designed to reward accurate assessments and penalise dishonest behaviour. This design aims to create a market-based risk pricing mechanism that is transparent and community-driven (Walters, 2023).

Nadler et al. (2023) proposed a fully decentralised insurance protocol. Current protocols often rely on governance voting or external oracles, which introduce subjectivity, coordination problems, and capital inefficiencies. By contrast, their design is based on a tranche structure that splits pooled capital into senior (A) and junior (B) tokens. Losses are absorbed first by junior token holders, while senior tokens are affected only in extreme cases. This mechanism creates a market-based pricing system for risk, as the relative valuation of the two tranches reflects the perceived likelihood of protocol failure. Importantly, the model enables claims to be settled automatically on-chain without external inputs, thus eliminating the need for subjective assessment or governance intervention. The protocol also improves capital efficiency by allowing part of the collateral to be allocated to yield-bearing assets, while providing fallback mechanisms to ensure orderly redemption in the event of failure. Despite the emergence of more and more DeFi insurance, Zhou and Zhang (2025) also pointed out that the DeFi insurance market is still in its early stages of development and continues to face challenges such as actuarial difficulties and regulatory hurdles.

(iv) The decentralised nature of DeFi makes it challenging to have a central bank-like lender of last resort, which also makes it difficult for investors to recover their losses when a protocol fails. Additionally, Avgouleas and Seretakis (2023) pointed out that applying the lender-of-last-resort mechanism to the cryptocurrency market may create a moral hazard. Government implicit guarantees could turn these DeFi projects into another class of ‘too big to fail’ institutions. In the absence of a safety net provided by a lender of last resort mechanism, prudently regulating the liquidity pools of projects is a suitable way to mitigate the liquidity risks faced by DeFi platforms. Ensuring that decentralised liquidity pools can provide timely liquidity support when a DeFi platform encounters a hacking attack and users start large-scale withdrawals, thereby preventing the platform from becoming paralysed.

In conclusion, regulating DeFi is a complex issue that involves ensuring compliance and security while also maintaining the innovative nature of the services (Amler et al., 2021;

Yuyama et al., 2023). In the context of frequent DeFi heists, it is crucial to establish disclosure systems and enforcement frameworks tailored to the characteristics of DeFi and crypto assets. This chapter recommends the introduction of third-party institutions, the establishment of stringent risk management standards, the adoption of decentralised insurance protocols, and the strengthening of regulations on liquidity pools to safeguard the interests of both protocol developers and investors.

4.6 Conclusion

The continuous development of decentralised finance (DeFi) has brought an increasing number of DeFi tokens into the spotlight for investors. However, its ecosystem is particularly susceptible to vulnerabilities, hacks, and fraud, which have raised ongoing concerns about the security of DeFi. This chapter, set against the backdrop of the six largest DeFi heists in 2022, is the first to investigate the impact of DeFi heists on the DeFi market. Understanding whether DeFi heists affect the native DeFi tokens of hacked platforms and whether these impacts spill over to other DeFi tokens is crucial for grasping the risks and dynamics within the DeFi ecosystem.

This chapter uses three low-frequency price impact measures as proxies for liquidity to investigate the liquidity levels of the stolen platforms' native DeFi tokens five days before and after the DeFi heist. The findings reveal that DeFi heists significantly reduce the liquidity of most of the stolen platforms' native DeFi tokens. This underscores the critical impact of security breaches on DeFi platforms, highlighting the necessity of robust security measures for platform stability. Furthermore, the analysis shows that the speed and transparency of the compromised platform's response are crucial in preserving the liquidity of its native DeFi token. According to the Glosten-Milgrom model (Glosten & Milgrom, 1985), information asymmetry leads to wider bid–ask spreads and reduced liquidity. Although DeFi relies on automated market makers (AMMs) rather than traditional dealers, similar mechanisms apply: informed traders sell depreciating tokens into liquidity pools, while liquidity providers (LPs), facing adverse selection and impermanent loss, withdraw liquidity. This process reduces pool depth and magnifies price impacts, equivalent to a widening of bid–ask spreads. Therefore, a quicker response and higher transparency could help reduce the likelihood of the DeFi token's liquidity being adversely impacted by the DeFi heist.

Additionally, using the Quantile Vector Autoregressive (QVAR) model, it finds that mainstream DeFi tokens exhibit strong mutual influence and interconnectedness. However,

the interconnectedness between these mainstream DeFi tokens and the native DeFi tokens of compromised platforms is relatively weak. This indicates that while the volatility of native DeFi tokens from hacked platforms could cause some spillover to other mainstream DeFi tokens, the contagion effect is not very pronounced. This could be attributed to the diversity of protocols and assets within the DeFi market, which helps absorb the impact of individual assets. Even if a platform's native DeFi token is compromised, tokens from other platforms continue to support the market, mitigating negative effects. Mainstream DeFi tokens, with their large market capitalisations, could stabilise the market and buffer the shocks from DeFi heists. Notably, this chapter observes significant volatility spillover effects from the native DeFi token of hacked platforms to mainstream DeFi tokens in the Beanstalk protocol heist. If investors develop broader concerns about the security of DeFi protocols with governance structures similar to those of the compromised platforms, the resulting fear and uncertainty could exacerbate market volatility. Overall, these findings underscore the importance of robust governance and security measures for maintaining market stability and protecting investor interests in the rapidly evolving DeFi market.

For investors, the results suggest that caution is warranted when incorporating DeFi tokens into diversified portfolios, as frequent DeFi heists could lead to significant market volatility. Investors should favour larger market-cap DeFi tokens, as their size and better security features help buffer the impacts of DeFi heists. For policymakers, this study highlights the necessity of developing strong governance frameworks and security measures to maintain market stability and protect investor interests. Policymakers could focus on introducing third-party institutions, setting stringent risk management standards, implementing decentralised insurance protocols, and strengthening regulations on liquidity pools. These measures will enhance DeFi platforms' resilience to potential hacker attacks and ensure that governance mechanisms are not easily exploited. Overall, this chapter emphasises the need for continuous improvements in DeFi platform security and governance to ensure the sustainable growth of the DeFi ecosystem.

4.7 Appendix

Figure 4.11: Liquidity changes of the Qubit before and after the Qubit Finance platform heist

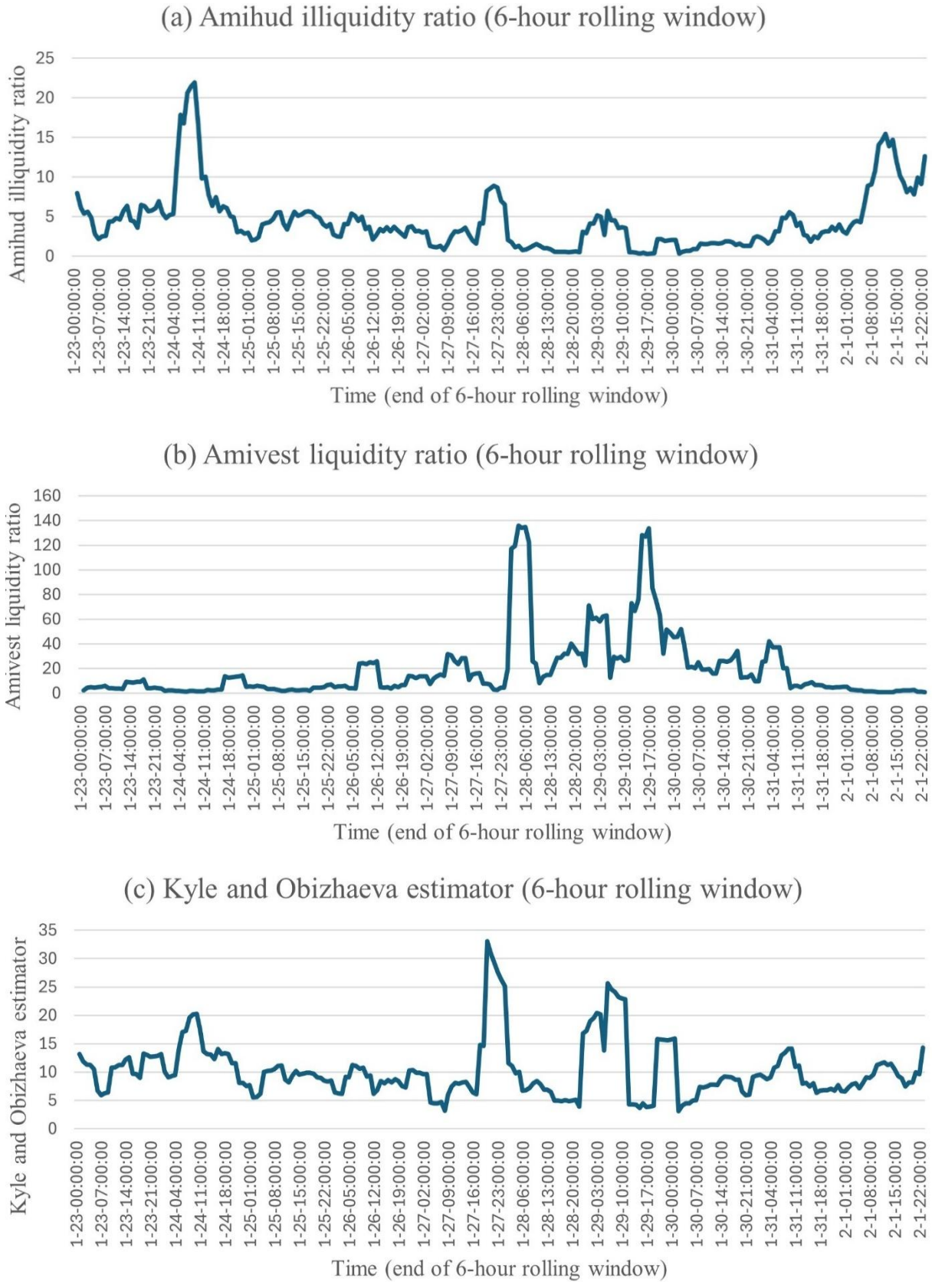


Figure 4.12: Liquidity changes of the Ronin before and after the Ronin Network heist

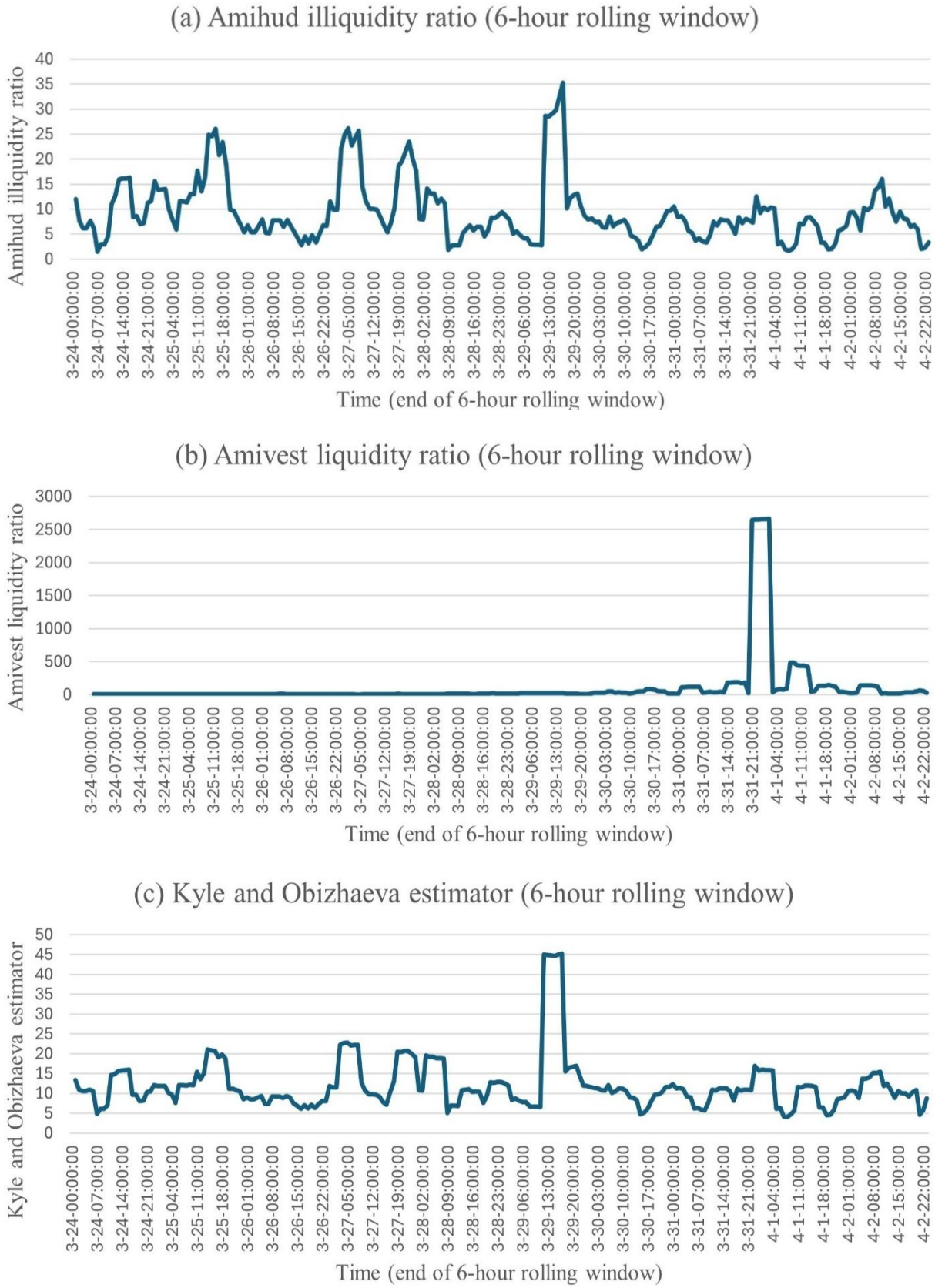


Figure 4.13: Liquidity changes of the Bean before and after the Beanstalk protocol during the heist

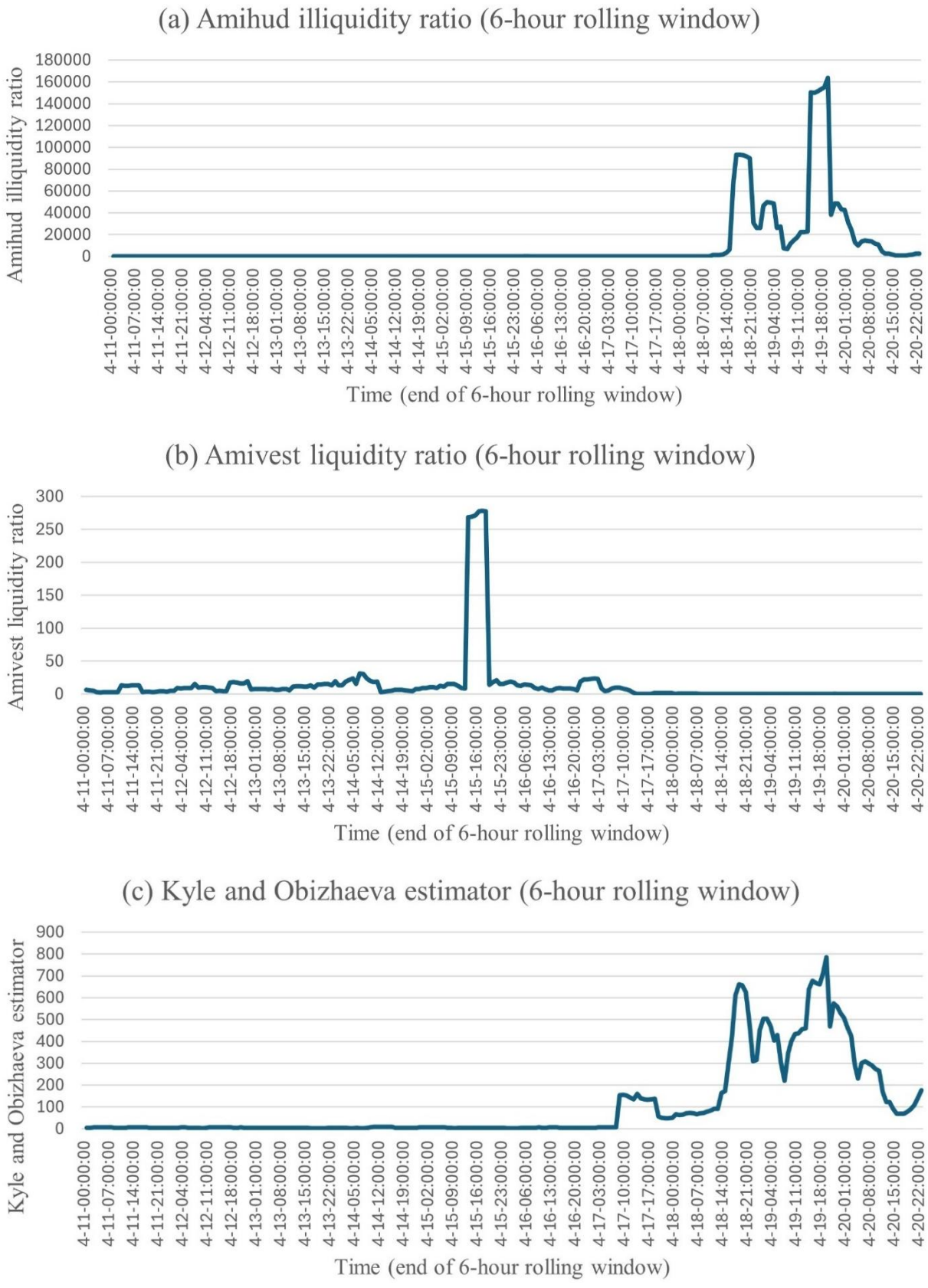


Figure 4.14: Liquidity changes of the Elrond before and after the Maiar Exchange heist

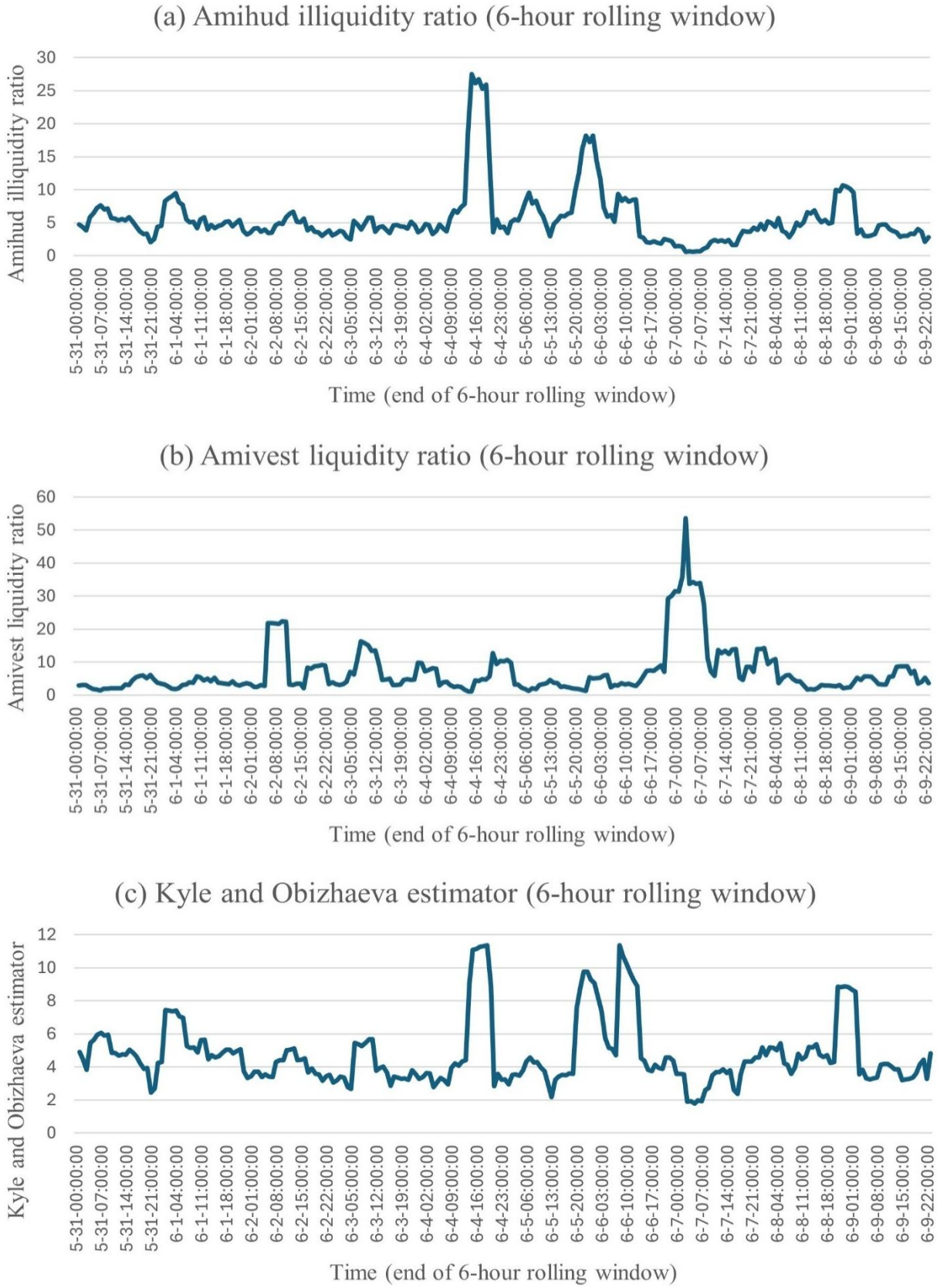


Figure 4.15: Liquidity changes of the Binance Coin before and after the Binance platform heist

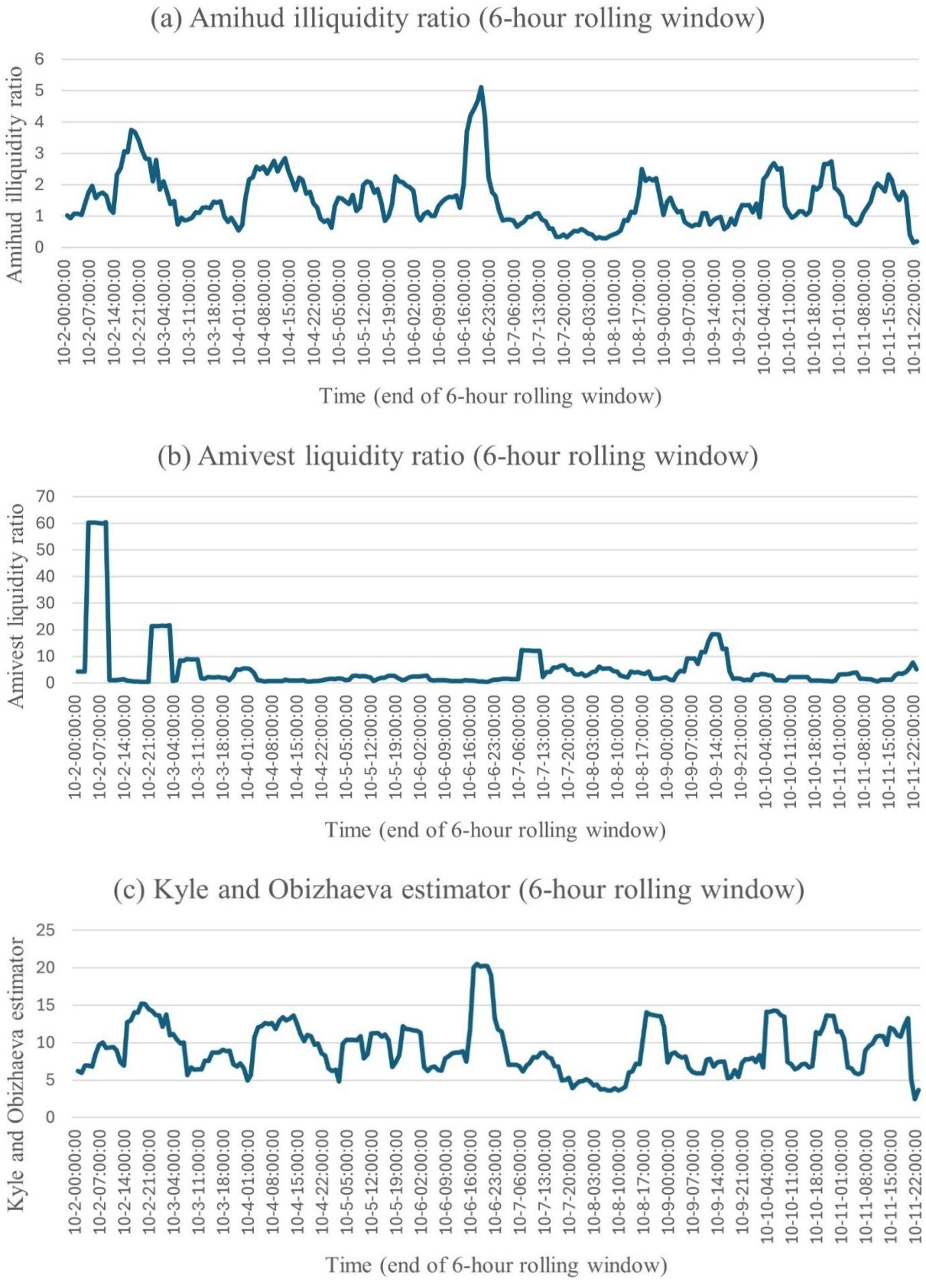


Figure 4.16: Liquidity changes of the Mango before and after the Mango Markets platform heist

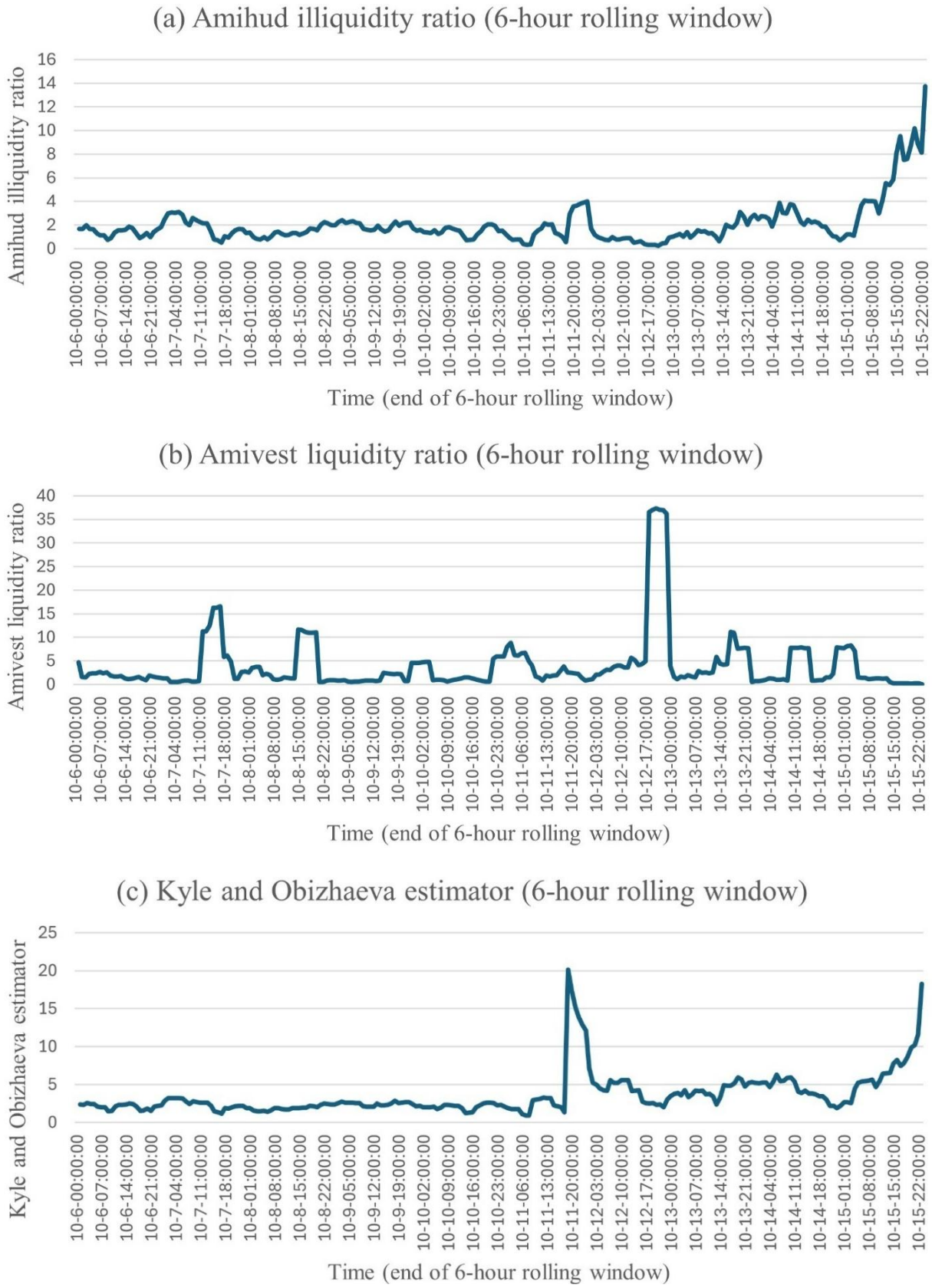


Table 4.12: Spillover connectedness between the Qubit and five mainstream DeFi tokens in the Qubit Finance platform heist

	Panel A: Spillover connectedness at the 95th quantile						
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	15.66	21.46	10.48	14.87	20.38	17.15	84.34
	Avalanche	9.58	23.97	9.94	16.92	21.24	18.34	76.03
	Chainlink	9.40	22.45	12.93	16.39	21.22	17.61	87.07
	Uniswap	9.42	20.16	13.64	18.90	20.33	17.55	81.10
	Maker	8.49	22.68	11.04	17.47	22.84	17.49	77.16
	Stacks	7.65	21.40	13.64	16.98	20.92	19.41	80.59
	TO	44.55	108.14	58.74	82.62	104.10	88.14	TCI
	NET	-39.79	32.12	-28.33	1.52	26.93	7.55	81.05
	Panel B: Spillover connectedness at the 50th quantile						
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	93.35	1.18	1.56	0.98	0.95	1.98	6.65
	Avalanche	0.28	35.87	18.96	18.52	11.87	14.49	64.13
	Chainlink	0.43	19.43	36.45	15.42	9.70	18.57	63.55
	Uniswap	0.32	19.47	16.60	37.92	11.92	13.76	62.08
	Maker	0.29	15.22	11.69	15.73	43.52	13.56	56.48
Qubit Finance	Stacks	1.49	15.77	20.25	13.02	10.99	38.47	61.53
	TO	2.82	71.07	69.06	63.67	45.44	62.35	TCI
	NET	-3.83	6.95	5.51	1.59	-11.05	0.82	52.40
	Panel C: Spillover connectedness at the 5th quantile						
		Qubit	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Qubit	16.89	28.79	13.20	14.51	9.68	16.92	83.11
	Avalanche	6.64	36.41	14.52	15.89	10.08	16.46	63.59
	Chainlink	7.55	25.80	19.47	15.30	13.09	18.79	80.53
	Uniswap	6.02	32.15	14.35	18.90	9.82	18.76	81.10
	Maker	8.61	25.20	14.77	13.86	20.18	17.38	79.82
	Stacks	6.94	24.63	16.11	16.45	12.18	23.68	76.32
	TO	35.76	136.58	72.95	76.02	54.86	88.30	TCI
	NET	-47.36	72.99	-7.58	-5.08	-24.96	11.99	77.41

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.13: Spillover connectedness between the Ronin and five mainstream DeFi tokens in the Ronin Network heist

	Panel A: Spillover connectedness at the 95th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	30.10	10.98	14.76	13.93	16.18	14.06	69.90
	Avalanche	10.49	20.60	17.91	17.52	19.57	13.92	79.40
	Chainlink	9.99	16.72	20.91	17.88	18.14	16.37	79.09
	Uniswap	8.76	17.08	17.27	21.97	17.17	17.74	78.03
	Maker	9.11	17.89	17.04	18.26	23.39	14.32	76.61
	Stacks	10.96	15.32	17.82	19.00	15.44	21.46	78.54
	TO	49.31	77.99	84.80	86.58	86.49	76.41	TCI
	NET	-20.59	-1.41	5.70	8.55	9.88	-2.14	76.93
	Panel B: Spillover connectedness at the 50th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	65.42	4.21	7.68	6.05	5.85	10.78	34.58
	Avalanche	1.46	32.72	18.39	16.88	15.79	14.77	67.28
	Chainlink	2.46	17.05	30.27	18.21	14.45	17.55	69.73
	Uniswap	1.28	15.46	18.00	30.86	16.07	18.33	69.14
	Maker	1.97	16.24	16.18	18.38	33.97	13.27	66.03
Ronin Network	Stacks	4.54	14.23	18.18	19.36	12.75	30.94	69.06
	TO	11.71	67.20	78.43	78.88	64.91	74.69	TCI
	NET	-22.86	-0.08	8.70	9.74	-1.12	5.63	62.64
	Panel C: Spillover connectedness at the 5th quantile						
		Ronin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Ronin	20.30	14.81	16.64	15.16	16.38	16.70	79.70
	Avalanche	8.68	20.97	17.83	17.08	18.44	17.00	79.03
	Chainlink	8.68	17.20	20.37	18.20	17.60	17.96	79.63
	Uniswap	7.17	17.24	18.49	20.40	18.27	18.44	79.60
	Maker	7.96	17.57	18.05	18.23	21.15	17.05	78.85
	Stacks	8.54	17.19	18.61	18.21	17.57	19.87	80.13
	TO	41.02	84.01	89.62	86.88	88.26	87.16	TCI
	NET	-38.68	4.98	9.99	7.28	9.40	7.03	79.49

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.14: Spillover connectedness between the Bean and five mainstream DeFi tokens in the Beanstalk protocol heist

	Panel A: Spillover connectedness at the 95th quantile						
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	26.96	10.77	12.51	13.89	12.35	23.51	73.04
	Avalanche	17.41	15.56	13.38	16.74	13.96	22.95	84.44
	Chainlink	16.79	11.98	16.12	16.52	13.03	25.57	83.88
	Uniswap	16.67	13.00	14.05	18.45	13.82	24.01	81.55
	Maker	17.43	12.38	12.67	16.20	17.92	23.41	82.08
	Stacks	17.09	12.30	13.02	15.69	12.37	29.53	70.47
	TO	85.40	60.43	65.63	79.04	65.52	119.45	TCI
	NET	12.36	-24.01	-18.25	-2.52	-16.56	48.98	79.25
	Panel B: Spillover connectedness at the 50th quantile						
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	74.62	5.85	3.64	5.19	6.23	4.47	25.38
	Avalanche	4.23	35.44	16.27	19.88	14.32	9.87	64.56
	Chainlink	3.91	16.03	35.82	19.70	16.51	8.03	64.18
	Uniswap	3.16	20.72	18.07	31.24	16.39	10.42	68.76
	Maker	4.01	16.67	13.79	19.84	39.58	6.11	60.42
Beanstalk	Stacks	4.29	12.27	10.15	10.85	5.77	56.68	43.32
	TO	19.60	71.53	61.92	75.46	59.22	38.90	TCI
	NET	-5.78	6.97	-2.26	6.70	-1.20	-4.42	54.44
	Panel C: Spillover connectedness at the 5th quantile						
		Bean	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Bean	25.57	17.06	12.47	14.06	15.31	15.53	74.43
	Avalanche	21.45	18.66	12.02	16.18	16.04	15.64	81.34
	Chainlink	20.00	17.29	14.11	16.20	16.55	15.84	85.89
	Uniswap	19.91	17.81	12.80	16.92	16.65	15.92	83.08
	Maker	18.93	18.00	12.87	16.89	19.25	14.06	80.75
	Stacks	20.04	16.93	12.15	15.77	16.89	18.23	81.77
	TO	100.32	87.09	62.31	79.11	81.44	76.99	TCI
	NET	25.89	5.75	-23.58	-3.97	0.69	-4.78	81.21

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.15: Spillover connectedness between the Elrond and five mainstream DeFi tokens in the Maiar Exchange heist

	Panel A: Spillover connectedness at the 95th quantile						
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	28.43	14.54	16.53	12.74	11.14	16.62	71.57
	Avalanche	10.27	20.54	19.19	16.37	15.62	18.01	79.46
	Chainlink	10.59	17.29	24.76	15.29	16.17	15.89	75.24
	Uniswap	10.79	18.11	18.80	19.51	16.43	16.37	80.49
	Maker	8.51	17.62	20.56	17.03	20.33	15.95	79.67
	Stacks	12.66	17.95	18.03	15.24	14.19	21.94	78.06
	TO	52.81	85.51	93.11	76.67	73.55	82.84	TCI
	NET	-18.76	6.05	17.87	-3.82	-6.12	4.78	77.42
	Panel B: Spillover connectedness at the 50th quantile							
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	73.09	5.16	4.34	4.94	5.59	6.88	26.91
	Avalanche	0.93	26.79	17.39	20.29	19.95	14.66	73.21
	Chainlink	0.60	18.78	29.06	19.89	17.96	13.71	70.94
	Uniswap	1.03	20.73	18.57	26.17	19.61	13.89	73.83
	Maker	1.25	19.40	16.99	20.23	27.08	15.04	72.92
Maiar Exchange	Stacks	1.46	16.62	15.02	16.17	18.42	32.32	67.68
	TO	5.27	80.69	72.30	81.52	81.53	64.18	TCI
	NET	-21.63	7.48	1.36	7.69	8.61	-3.50	64.25
	Panel C: Spillover connectedness at the 5th quantile							
		Elrond	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Elrond	19.16	18.66	16.23	12.53	16.07	17.35	80.84
	Avalanche	11.89	20.35	17.50	14.11	18.09	18.06	79.65
	Chainlink	12.13	18.70	19.39	14.94	17.04	17.80	80.61
	Uniswap	12.50	19.33	17.47	15.23	17.66	17.81	84.77
	Maker	12.10	19.68	17.46	14.09	18.80	17.88	81.20
	Stacks	12.58	19.36	17.13	13.78	17.57	19.58	80.42
	TO	61.19	95.73	85.80	69.44	86.43	88.89	TCI
	NET	-19.65	16.09	5.19	-15.33	5.22	8.48	81.25

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.16: Spillover connectedness between the Binance Coin and five mainstream DeFi tokens in the Binance platform heist

	Panel A: Spillover connectedness at the 95th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	24.09	18.35	17.23	17.81	9.82	12.70	75.91
Avalanche	14.58	20.20	17.90	16.41	17.66	13.25	79.80
Chainlink	17.27	18.22	26.07	16.55	10.94	10.95	73.93
Uniswap	16.48	17.50	16.90	23.79	12.22	13.11	76.21
Maker	11.23	13.96	15.18	14.74	30.80	14.08	69.20
Stacks	13.92	15.72	15.14	15.08	17.54	22.60	77.40
TO	73.49	83.75	82.37	80.59	68.17	64.07	TCI
NET	-2.42	3.95	8.44	4.38	-1.03	-13.32	75.41
	Panel B: Spillover connectedness at the 50th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	44.73	20.30	12.66	15.22	1.47	5.63	55.27
Avalanche	19.60	43.09	16.99	11.42	5.85	3.04	56.91
Chainlink	11.72	17.85	56.68	8.47	3.44	1.85	43.32
Uniswap	17.57	15.13	8.63	49.94	4.40	4.33	50.06
Maker	0.49	6.12	1.56	1.40	82.81	7.63	17.19
Binance Stacks	8.72	2.95	5.11	5.84	8.09	69.29	30.71
TO	58.08	62.35	44.96	42.34	23.25	22.49	TCI
NET	2.81	5.44	1.64	-7.72	6.05	-8.22	42.24
	Panel C: Spillover connectedness at the 5th quantile						
	Binance Coin	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
Binance Coin	22.54	15.52	17.71	17.09	12.38	14.76	77.46
Avalanche	17.54	21.38	17.67	18.20	11.09	14.13	78.62
Chainlink	15.46	16.13	24.24	14.75	14.77	14.64	75.76
Uniswap	18.74	15.84	16.56	23.40	11.70	13.76	76.60
Maker	11.87	13.41	13.36	13.42	30.22	17.72	69.78
Stacks	15.20	15.76	12.39	15.28	16.70	24.66	75.34
TO	78.81	76.66	77.69	78.74	66.63	75.02	TCI
NET	1.36	-1.96	1.93	2.14	-3.15	-0.32	75.59

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Table 4.17: Spillover connectedness between the Mango and five mainstream DeFi tokens in the Mango Markets platform heist

	Panel A: Spillover connectedness at the 95th quantile						
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	31.64	13.31	13.35	12.38	16.65	12.67	68.36
	Avalanche	9.45	19.15	19.39	17.24	16.08	18.69	80.85
	Chainlink	9.18	17.00	21.09	16.08	14.35	22.30	78.91
	Uniswap	8.19	17.42	18.39	21.36	15.33	19.31	78.64
	Maker	9.68	16.68	15.09	17.34	24.39	16.82	75.61
	Stacks	7.87	16.77	18.77	16.84	15.62	24.13	75.87
	TO	44.38	81.18	85.00	79.88	78.02	89.79	TCI
	NET	-23.98	0.33	6.09	1.24	2.41	13.92	76.37
	Panel B: Spillover connectedness at the 50th quantile							
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	94.44	1.99	1.19	0.95	0.62	0.82	5.56
	Avalanche	0.38	30.09	25.63	16.44	7.91	19.55	69.91
	Chainlink	0.34	23.41	33.43	15.92	7.09	19.82	66.57
	Uniswap	0.21	19.35	19.31	37.63	8.68	14.82	62.37
	Maker	0.18	12.88	9.25	12.52	54.77	10.40	45.23
Mango Markets	Stacks	0.42	21.73	21.11	15.10	6.06	35.57	64.43
	TO	1.53	79.35	76.48	60.94	30.36	65.40	TCI
	NET	-4.03	9.45	9.91	-1.43	-14.87	0.97	52.34
	Panel C: Spillover connectedness at the 5th quantile							
		Mango	Avalanche	Chainlink	Uniswap	Maker	Stacks	FROM
	Mango	17.55	17.99	16.87	16.38	17.01	14.20	82.45
	Avalanche	6.59	21.14	19.48	18.25	17.38	17.15	78.86
	Chainlink	6.96	20.36	21.04	18.17	16.68	16.80	78.96
	Uniswap	5.76	19.55	19.10	21.15	17.17	17.27	78.85
	Maker	6.49	19.21	17.75	18.39	21.60	16.56	78.40
	Stacks	5.88	19.51	19.39	18.41	17.42	19.40	80.60
	TO	31.67	96.61	92.59	89.60	85.67	81.98	TCI
	NET	-50.78	17.75	13.63	10.75	7.27	1.38	79.69

The findings are derived from a Quantile VAR method with a lag length of 1, determined by the Akaike Information Criterion (AIC). The rolling window size is 80 hourly observations, and forecast market dynamics 10 time steps into the future. *FROM* indicates the source of causal impacts that each DeFi token receives, while *TO* denotes the destination of these effects. *NET* equals *TO* minus *FROM*. Positive values of *NET* indicate that the DeFi token is a net transmitter of spillover impacts, whereas negative values suggest it is a net receiver. A higher *TCI* indicates stronger spillover effects and greater systemic interdependence, while a lower *TCI* suggests weaker linkages and more independence among DeFi tokens.

Chapter 5 Summary and Conclusion

The increasing prevalence of cryptocurrency heists has raised critical concerns regarding their broader impact on the cryptocurrency ecosystem. Despite the growing number of security breaches, academic studies have yet to fully explore how these events affect key market dynamics, such as market efficiency, investor sentiment, etc. Given Bitcoin's dominant position in the cryptocurrency market, this thesis primarily focuses on understanding how cryptocurrency heists influence Bitcoin's market efficiency and investor sentiment. Additionally, as DeFi platforms have become frequent targets of hacking attacks, this thesis extends its analysis beyond Bitcoin to investigate the impact of DeFi heists on the stolen platform's native DeFi tokens' liquidity and overall DeFi market stability. By systematically analysing these aspects, this thesis contributes to a deeper understanding of how security breaches disrupt cryptocurrency markets.

The second chapter of this thesis examines how cryptocurrency heists influence Bitcoin's market efficiency. Using the Adaptive Market Hypothesis (AMH) as a theoretical framework, this study applies the permutation entropy and the Complexity–entropy causality plane to assess efficiency changes across twelve major cryptocurrency heists (Mt Gox, Coincheck, KuCoin, PancakeBunny, Poly Network, Bitmart, Wormhole, Ronin Network, Beanstalk, Nomad, Binance and FTX). The findings indicate that Bitcoin's market efficiency declines significantly on the day of and immediately following these cryptocurrency heists. This decline is characterised by reduced permutation entropy and increased complexity, suggesting that security breaches introduce temporary inefficiencies into the Bitcoin market. Furthermore, tokens directly targeted by cryptocurrency heists exhibit even greater efficiency losses compared to Bitcoin, implying that investor attention is more focused on the affected tokens. These results underscore the disruptive nature of cryptocurrency heists and highlight the importance of improving market stability through enhanced security protocols and risk management measures.

The third chapter investigates the bidirectional predictive relationship between Bitcoin price and investor sentiment in the context of cryptocurrency heists. By employing the Cryptocurrency Fear & Greed Index (CFGI) as a proxy for sentiment, this study uses a time-varying Granger causality approach to examine sentiment-price dynamics before and after the KuCoin exchange heist, where large amounts of Bitcoin were stolen. The results reveal that no significant bidirectional predictive relationship exists between Bitcoin price and CFGI in

the 90 days preceding the heist. However, within 90 days following the heist, a strong feedback loop emerges, in which CFGI fluctuations significantly influence Bitcoin price movements and vice versa. This intensified sentiment-price interaction suggests that heightened uncertainty following a heist exacerbates investor reactions, potentially creating a cycle of price declines and market panic. Additionally, this study also finds that the bidirectional predictive relationship between price and CFGI does not always hold after cryptocurrency heists. Only cryptocurrency heists that directly impact Bitcoin exhibit a strong sentiment-price feedback mechanism, whereas those targeting other cryptocurrencies display a weaker relationship. This may be attributed to CFGI primarily measuring sentiment within the Bitcoin market, making it less reflective of fluctuations in other cryptocurrencies. Finally, this study finds that the bidirectional sentiment-price relationship is primarily confined to Bitcoin, with limited effects on other cryptocurrencies such as Ethereum and Binance Coin. This highlights the specificity of sentiment dynamics in the Bitcoin market and suggests that while CFGI is a useful indicator for predicting Bitcoin price movements during Bitcoin crisis periods, it may not be as effective for other cryptocurrencies.

The fourth chapter extends the analysis to the DeFi ecosystem, where security vulnerabilities have become an increasing concern. This chapter investigates six major DeFi heists in 2022 (Qubit Finance, Ronin Network, Beanstalk, Maiar Exchange, Binance and Mango Markets) and their impact on the liquidity of stolen platforms' native DeFi tokens as well as the broader DeFi market. Using low-frequency price impact measures and the Quantile VAR model, the findings show that the liquidity of the affected DeFi tokens declines sharply post-heist. However, the spillover effects on mainstream DeFi tokens are relatively limited, suggesting that while individual DeFi platforms suffer substantial liquidity shocks, the overall DeFi market exhibits a degree of stability. Nonetheless, if investor confidence in DeFi security deteriorates significantly, for example due to concerns about governance mechanisms, market-wide volatility may increase, posing systemic risks to the broader DeFi ecosystem. These findings highlight the importance of robust security mechanisms, transparent governance, and crisis management strategies in maintaining stability within the DeFi sector. Beyond its empirical findings, this chapter provides valuable implications for the design and safety of DeFi. Drawing on lessons from traditional financial systems, DeFi platforms could enhance systemic stability through four design dimensions: (i) regular security audits and compliance assessments to ensure protocol integrity and transparency; (ii) prudent risk management mechanisms, including leverage limits, adequate collateralisation

ratios, and automated liquidation processes to contain losses during attacks; (iii) the development of decentralised insurance frameworks to provide compensation for hacking incidents and smart contract failures, thus restoring investor confidence; and (iv) improved liquidity management within decentralised liquidity pools to prevent liquidity freezes during crisis events. Collectively, these design implications emphasise that building a secure and sustainable DeFi ecosystem requires balancing innovation with risk control, transparency, and accountability.

Overall, this thesis makes several key contributions to the understanding of cryptocurrency markets in the context of cryptocurrency heists. First, it provides empirical evidence that cryptocurrency heists may significantly impact Bitcoin's market efficiency, further supporting the notion that Bitcoin's market efficiency evolves in response to changes in the external market environment. Second, it reveals the crucial role of investor sentiment in shaping market reactions during periods of heightened uncertainty, demonstrating how sentiment-driven feedback loops can amplify price volatility. Third, it extends the scope of analysis beyond Bitcoin to the DeFi ecosystem, offering novel insights into how security breaches affect DeFi token liquidity and market stability.

These findings carry substantial implications for investors, policymakers, and academics operating within the rapidly evolving cryptocurrency ecosystem. For investors, the results reveal that cryptocurrency heists may lead to sudden and significant declines in market efficiency, particularly in the immediate aftermath of an attack. This volatility is not random but shaped by behavioural responses such as panic selling, herding, and overreaction to sentiment shocks. As such, investors should not only account for technological risks but also recognise the informational inefficiencies and emotional contagion that follow security breaches. The evidence also cautions against over-reliance on a single sentiment indicator such as CFGI, particularly during crisis periods when sentiment dynamics become asset-specific. To mitigate behavioural biases and manage short-term risks more effectively, investors should adopt a multi-indicator sentiment approach and consider event-driven strategies that factor in the nature and perceived severity of security incidents.

For policymakers, this thesis reveals critical regulatory blind spots, particularly in the governance and security infrastructure of DeFi platforms. Existing frameworks often overlook the systemic risks posed by decentralised protocols that lack standardised audits, transparent incident disclosures, and robust governance mechanisms. The findings suggest

that regulators should implement mandatory security audits, establish timely disclosure protocols for security breaches, and promote governance reforms tailored to decentralised organisational structures. Such interventions can help mitigate market disruptions and investor anxiety caused by cryptocurrency heists, while enhancing overall regulatory compliance and investor confidence in the digital asset market.

For academics, this thesis examines the impact of cryptocurrency heists on the cryptocurrency market through the lens of market microstructure theory, thereby extending the existing literature's understanding of market behaviour under extreme events. By conceptualising security breaches as endogenous shocks, this thesis reveals how information asymmetry, liquidity fragility, and market interconnectedness interact within the cryptocurrency market to influence market efficiency, investor sentiment, token liquidity, and risk transmission channels. This perspective not only applies market microstructure theory to the emerging cryptocurrency ecosystem but also enriches its applicability and explanatory power under conditions of high uncertainty, providing a suitable theoretical framework for understanding price discovery and information transmission in the cryptocurrency market.

Despite its contributions, this thesis is subject to several limitations that should be acknowledged. First, the empirical analysis focuses on a limited number of high-profile cryptocurrency heists, which may constrain the generalisability of the findings to the broader cryptocurrency ecosystem. Smaller-scale hacking incidents, insider frauds, or protocol-level vulnerabilities are not fully explored, even though they may trigger distinct market reactions. The heterogeneous nature of heist types, magnitudes, and timing suggests that different forms of security breaches could have varying effects on market dynamics. Second, the empirical models and indicators employed in this thesis could be further developed. The permutation entropy measure currently does not provide formal statistical significance testing, which presents a challenge for rigorously assessing the evolution of market efficiency. Moreover, although Alternative.me discloses the weighting scheme of the six components comprising the sentiment index, it does not release their exact numerical values, preventing a detailed component-level analysis. As a result, it remains difficult to identify which specific factors primarily drive fluctuations in market sentiment during major events such as cryptocurrency heists.

Third, the investigation of market efficiency and liquidity is largely confined to short-term responses surrounding heist events. While this focus effectively captures immediate

disruptions, it does not fully address the long-term adjustment process or the persistence of structural inefficiencies after market recovery. Moreover, the liquidity analysis relies on low-frequency measures, which, although widely used, may not adequately reflect the high-frequency dynamics of liquidity. Finally, given the global divergence in regulatory approaches, from the EU's harmonised MiCA framework to the fragmented enforcement-driven U.S. model and China's prohibition-based stance, which regulatory model—proactive and harmonised (EU), fragmented yet enforcement-driven (US), or prohibitive (China)—is most effective in maintaining market stability and protecting investors in the aftermath of major security incidents? This is important for global cryptocurrency governance and risk management.

Building on the limitations identified above, several clear avenues for future studies emerge, all centred on deepening understanding of how extreme security events shape cryptocurrency market dynamics through microstructural mechanisms. First, expanding the dataset of cryptocurrency heists to include a wider range of security incidents, such as smaller-scale attacks, protocol-level vulnerabilities, and insider fraud, would enable a more comprehensive understanding of how different types and magnitudes of breaches influence market dynamics. Such studies could further explore cross-sectional differences in market reactions across blockchain ecosystems and cryptocurrency classes. Second, future studies should seek to develop statistical methods capable of testing whether changes in permutation entropy measures are significant, so as to provide a more rigorous assessment of the evolution of market efficiency. Moreover, a valuable direction for future studies would be to disentangle the relative contributions of market-based components (e.g., volatility and trading volume) and behavioural components (e.g., social media activity and search intensity). Doing so would enhance understanding of whether sentiment shifts are primarily driven by objective market dynamics or by behavioural responses. Future studies could address this limitation by employing sentiment indices that allow component-level decomposition or by constructing new sentiment measures capable of isolating heterogeneous drivers of market sentiment.

Third, longitudinal analyses are needed to examine the long-term consequences of cryptocurrency heists. Future work could assess whether market efficiency and liquidity eventually recover to pre-attack levels or whether persistent inefficiencies arise due to structural distrust or technological vulnerabilities. Integrating high-frequency data and micro-level order book information would also help capture the real-time liquidity dynamics. Finally, given the global divergence in regulatory approaches, future studies could examine

how these differing regimes shape post-heist market stability, investor protection, and systemic safety.

In conclusion, this thesis provides a comprehensive investigation into how cryptocurrency heists impact Bitcoin's market efficiency, investor sentiment, and the DeFi market. By bridging gaps in the existing literature and offering new empirical insights, it contributes to a more nuanced understanding of the vulnerabilities within the cryptocurrency market and its influence. As the crypto industry continues to evolve, addressing security risks will be crucial in fostering greater market stability and investor confidence in digital asset markets.

References

Aalborg, H.A., Molnár, P. and de Vries, J.E., 2019. What can explain the price, volatility and trading volume of Bitcoin?. *Finance Research Letters*, *29*, pp.255-265.

Abraham, J., Higdon, D., Nelson, J. and Ibarra, J., 2018. *Cryptocurrency Price Prediction Using Tweet Volumes and Sentiment Analysis. SMU Data Sci Rev 1 (3)*

Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). Systemic risk and stability in financial networks. *American Economic Review*, *105*(2), 564-608.

Adelopo, I. and Luo, X., 2025. Interconnectedness among cryptocurrencies and financial markets: A systematic literature review. *Digital Finance*, pp.1-53.

Aharon, D.Y., Ali, S. and Brahim, M., 2024. Connectedness at extremes between real estate tokens and real estate stocks. *International Review of Financial Analysis*, *95*, p.103425.

Ahmed, W.M., 2022. Robust drivers of Bitcoin price movements: An extreme bounds analysis. *The North American Journal of Economics and Finance*, *62*, p.101728.

Akerlof, G.A., 1978. The market for "lemons": Quality uncertainty and the market mechanism. In *Uncertainty in economics* (pp. 235-251). Academic Press.

Akkus, H.T. and Dogan, M., 2024. Analysis of dynamic connectedness relationships between cryptocurrency, NFT and DeFi assets: TVP-VAR approach. *Applied Economics Letters*, *31*(21), pp.2250-2255.

Alamsyah, A., Kusuma, G.N.W. and Ramadhani, D.P., 2024. A review on decentralized finance ecosystems. *Future Internet*, *16*(3), p.76.

Alamsyah, A. and Muhammad, I.F., 2024. Unraveling the crypto market: A journey into decentralized finance transaction network. *Digital Business*, *4*(1), p.100074.

Alexander, C. and Dakos, M., 2020. A critical investigation of cryptocurrency data and analysis. *Quantitative Finance*, *20*(2), pp.173-188.

Alexander, C. and Heck, D.F., 2020. Price discovery in Bitcoin: The impact of unregulated markets. *Journal of Financial Stability*, *50*, p.100776.

Alfieri, E., Burlacu, R. and Enjolras, G., 2025. Cryptocurrency bubbles, information asymmetry and noise trading. *The Journal of Risk Finance*, *26*(2), pp.295-319.

Ali, S., Ijaz, M.S. and Yousaf, I., 2023. Dynamic spillovers and portfolio risk management between defi and metals: Empirical evidence from the Covid-19. *Resources Policy*, *83*, p.103672.

Ali, S., Shahzad, S.J.H., Raza, N. and Al-Yahyaee, K.H., 2018. Stock market efficiency: A comparative analysis of Islamic and conventional stock markets. *Physica A: Statistical Mechanics and Its Applications*, *503*, pp.139-153.

Allen, F., & Gale, D. (2000). Financial contagion. *Journal of political economy*, *108*(1), 1-33.

Almeida, J. and Gonçalves, T.C., 2024. Cryptocurrency market microstructure: a systematic literature review. *Annals of Operations Research*, *332*(1), pp.1035-1068.

AlNemer, H.A., Hkiri, B. and Khan, M.A., 2021. Time-varying nexus between investor sentiment and cryptocurrency market: new insights from a wavelet coherence framework. *Journal of Risk and Financial Management*, *14*(6), p.275.

Alvarez-Ramirez, J., Rodriguez, E. and Ibarra-Valdez, C., 2018. Long-range correlations and asymmetry in the Bitcoin market. *Physica A: Statistical Mechanics and its Applications*, *492*, pp.948-955.

Al-Yahyaee, K.H., Mensi, W., Ko, H.U., Yoon, S.M. and Kang, S.H., 2020. Why cryptocurrency markets are inefficient: The impact of liquidity and volatility. *The North American Journal of Economics and Finance*, *52*, p.101168.

Al-Yahyaee, K.H., Mensi, W. and Yoon, S.M., 2018. Efficiency, multifractality, and the long-memory property of the Bitcoin market: A comparative analysis with stock, currency, and gold markets. *Finance Research Letters*, *27*, pp.228-234.

Amihud, Y., 2002. Illiquidity and stock returns: cross-section and time-series effects. *Journal of financial markets*, *5*(1), pp.31-56.

Amihud, Y. and Mendelson, H., 1986. Asset pricing and the bid-ask spread. *Journal of financial Economics*, *17*(2), pp.223-249.

Amihud, Y., Mendelson, H. and Lauterbach, B., 1997. Market microstructure and securities values: Evidence from the Tel Aviv Stock Exchange. *Journal of financial Economics*, *45*(3), pp.365-390.

Amler, H., Eckey, L., Faust, S., Kaiser, M., Sandner, P. and Schlosser, B., 2021, September. Defi-ning defi: Challenges & pathway. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 181-184). IEEE.

Anamika, Chakraborty, M. and Subramaniam, S., 2023. Does sentiment impact cryptocurrency?. *Journal of Behavioral Finance*, *24*(2), pp.202-218.

Ando, T., Greenwood-Nimmo, M. and Shin, Y., 2022. Quantile connectedness: modeling tail behavior in the topology of financial networks. *Management Science*, *68*(4), pp.2401-2431.

Andrews, D.W., 1993. Tests for parameter instability and structural change with unknown change point. *Econometrica: Journal of the Econometric Society*, pp.821-856.

Andrews, D.W. and Ploberger, W., 1994. Optimal tests when a nuisance parameter is present only under the alternative. *Econometrica: Journal of the Econometric Society*, pp.1383-1414.

Ante, L., 2022. The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. *FinTech*, *1*(3), pp.216-224.

Antonakakis, N., Chatziantoniou, I. and Gabauer, D., 2019. Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. *Journal of International Financial Markets, Institutions and Money*, *61*, pp.37-51.

Aquilina, M., Frost, J. and Schrimpf, A., 2024. Decentralized finance (DeFi): a functional approach. *Journal of Financial Regulation*, *10*(1), pp.1-27.

Arora, V. and Shi, S., 2016. Energy consumption and economic growth in the United States. *Applied Economics*, *48*(39), pp.3763-3773.

Ashton, J.K., Gerrard, B. and Hudson, R., 2003. Economic impact of national sporting success: evidence from the London stock exchange. *Applied Economics Letters*, *10*(12), pp.783-785.

Ashton, J.K., Gerrard, B. and Hudson, R., 2011. Do national soccer results really impact on the stock market?. *Applied Economics*, *43*(26), pp.3709-3717.

Aslam, F., Memon, B.A., Hunjra, A.I. and Bouri, E., 2023. The dynamics of market efficiency of major cryptocurrencies. *Global Finance Journal*, *58*, p.100899.

Aslanidis, N., Bariviera, A.F. and Martínez-Ibañez, O., 2019. An analysis of cryptocurrencies conditional cross correlations. *Finance Research Letters*, *31*, pp.130-137.

Assaf, A., Demir, E. and Ersan, O., 2024. What drives the return and volatility spillover between DeFis and cryptocurrencies?. *International Journal of Finance & Economics*.

Avgouleas, E. and Seretakis, A., 2023. How should crypto lending be regulated under EU law?. *European Business Organization Law Review*, *24*(3), pp.421-438.

Aysan, A.F., Demir, E., Gozgor, G. and Lau, C.K.M., 2019. Effects of the geopolitical risks on Bitcoin returns and volatility. *Research in International Business and Finance*, *47*, pp.511-518.

Baek, C. and Elbeck, M., 2015. Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters*, *22*(1), pp.30-34.

Baele, L., 2005. Volatility spillover effects in European equity markets. *Journal of Financial and Quantitative Analysis*, *40*(2), pp.373-401.

Bakare, F.A., Omojola, J. and Iwuh, A.C., 2024. Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems. *World Journal of Advanced Research and Reviews*, *23*(3), pp.3075-3089.

Baker, H.K. and Ricciardi, V., 2014. How biases affect investor behaviour. *The European Financial Review*, pp.7-10.

Balcilar, M., Ozdemir, Z.A. and Arslanturk, Y., 2010. Economic growth and energy consumption causal nexus viewed through a bootstrap rolling window. *Energy Economics*, *32*(6), pp.1398-1410.

Ballis, A. and Verousis, T., 2022. Behavioural finance and cryptocurrencies. *Review of Behavioral Finance*, *14*(4), pp.545-562.

Bandt, C. and Pompe, B., 2002. Permutation entropy: a natural complexity measure for time series. *Physical review letters*, *88*(17), p.174102.

Banerjee, A.V., 1992. A simple model of herd behavior. *The quarterly journal of economics*, *107*(3), pp.797-817.

Barber, B.M. and Odean, T., 2008. All that glitters: The effect of attention and news on the buying behavior of individual and institutional investors. *The review of financial studies*, *21*(2), pp.785-818.

Barberis, N. and Thaler, R., 2003. A survey of behavioral finance. *Handbook of the Economics of Finance*, *1*, pp.1053-1128.

Barchat, C., 2023. *What is market cap? A guide to market capitalization in crypto.* MoonPay. Available at: https://www.moonpay.com/learn/cryptocurrency/what-is-market-capitalization [Accessed 24 May 2024].

Bariviera, A.F., 2017. The inefficiency of Bitcoin revisited: A dynamic approach. *Economics Letters*, *161*, pp.1-4.

Barnes, P., 2018. Crypto currency and its susceptibility to speculative bubbles, manipulation, scams and fraud. *Journal of Advanced Studies in Finance (JASF)*, *9*(2 (18)), pp.60-77.

Barron, O.E. and Qu, H., 2014. Information asymmetry and the ex-ante impact of public disclosure quality on price efficiency and the cost of capital: Evidence from a laboratory market. *The Accounting Review*, *89*(4), pp.1269-1297.

Bartels, R., 1982. The rank version of von Neumann's ratio test for randomness. *Journal of the American Statistical Association*, *77*(377), pp.40-46.

Baruník, J. and Křehlík, T., 2018. Measuring the frequency dynamics of financial connectedness and systemic risk. *Journal of Financial Econometrics*, *16*(2), pp.271-296.

Baum, C.F., Hurn, S. and Otero, J., 2021. The dynamics of US industrial production: A time-varying Granger causality perspective. *Econometrics and Statistics*.

Baur, D.G., Hong, K. and Lee, A.D., 2018. Bitcoin: Medium of exchange or speculative assets?. *Journal of International Financial Markets, Institutions and Money*, *54*, pp.177-189.

Bejaoui, A., Ben Sassi, S. and Majdoub, J., 2020. Market dynamics, cyclical patterns and market states: is there a difference between digital currencies markets?. *Studies in Economics and Finance*, *37*(4), pp.585-604.

Belenkov, N., Callens, V., Murashkin, A., Bak, K., Derka, M., Gorzny, J. and Lee, S.S., 2025. SoK: A review of cross-chain bridge hacks in 2023. *arXiv preprint arXiv:2501.03423*.

Benson, V., Adamyk, B., Chinnaswamy, A. and Adamyk, O., 2024. Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. *European Journal of Law and Economics*, *57*(1), pp.37-61.

Berkman, H. and Eleswarapu, V.R., 1998. Short-term traders and liquidity:: a test using Bombay Stock Exchange data. *Journal of financial Economics*, *47*(3), pp.339-355.

Bernile, G. and Lyandres, E., 2011. Understanding investor sentiment: The case of soccer. *Financial Management*, *40*(2), pp.357-380.

Bhatnagar, M., Taneja, S. and Rupeika-Apoga, R., 2023. Demystifying the effect of the news (shocks) on crypto market volatility. *Journal of Risk and Financial Management*, *16*(2), p.136.

Biais, B., Hillion, P. and Spatt, C., 1995. An empirical analysis of the limit order book and the order flow in the Paris Bourse. *the Journal of Finance*, *50*(5), pp.1655-1689.

Bikhchandani, S., Hirshleifer, D. and Welch, I., 1992. A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of political Economy*, *100*(5), pp.992-1026.

Black, F., 1976. Studies of stock price volatility changes. In *Proceedings from the American statistical association, business and economic statistics section* (p. 177).

Blau, B.M., Griffith, T.G. and Whitby, R.J., 2021. Inflation and Bitcoin: A descriptive time-series analysis. *Economics Letters*, *203*, p.109848.

Boehmer, E. and Kelley, E.K., 2009. Institutional investors and the informational efficiency of prices. *The Review of Financial Studies*, *22*(9), pp.3563-3594.

Borgards, O. and Czudaj, R.L., 2020. The prevalence of price overreactions in the cryptocurrency market. *Journal of international financial markets, institutions and money*, *65*, p.101194.

Bouoiyour, J. and Selmi, R., 2015. Bitcoin price: Is it really that new round of volatility can be on way?.

Bourghelle, D., Jawadi, F. and Rozin, P., 2022. *Do collective emotions drive bitcoin volatility? A triple regime-switching vector approach [Est-ce que les émotions collectives ont une influence directrice sur la volatilité?]* (No. hal-04412029).

Bouri, E., Azzi, G. and Dyhrberg, A.H., 2017. On the return-volatility relationship in the Bitcoin market around the price crash of 2013. *Economics*, *11*(1), p.2.

Bouri, E., Gabauer, D., Gupta, R. and Tiwari, A.K., 2021a. Volatility connectedness of major cryptocurrencies: The role of investor happiness. *Journal of Behavioral and Experimental Finance*, *30*, p.100463.

Bouri, E., Gupta, R. and Roubaud, D., 2019. Herding behaviour in cryptocurrencies. *Finance Research Letters*, *29*, pp.216-221.

Bouri, E., Saeed, T., Vo, X.V. and Roubaud, D., 2021b. Quantile connectedness in the cryptocurrency market. *Journal of International Financial Markets, Institutions and Money*, *71*, p.101302.

Bouteska, A., Mefteh-Wali, S. and Dang, T., 2022. Predictive power of investor sentiment for Bitcoin returns: Evidence from COVID-19 pandemic. *Technological Forecasting and Social Change*, *184*, p.121999.

Brauneis, A. and Mestel, R., 2018. Price discovery of cryptocurrencies: Bitcoin and beyond. *Economics Letters*, *165*, pp.58-61.

Brauneis, A., Mestel, R., Riordan, R. and Theissen, E., 2021. How to measure the liquidity of cryptocurrency markets?. *Journal of Banking & Finance*, *124*, p.106041.

Brauneis, A., Mestel, R., Riordan, R. and Theissen, E., 2022. Bitcoin unchained: Determinants of cryptocurrency exchange liquidity. *Journal of Empirical Finance*, *69*, pp.106-122.

Brennan, M.J. and Subrahmanyam, A., 1996. Market microstructure and asset pricing: On the compensation for illiquidity in stock returns. *Journal of financial economics*, *41*(3), pp.441-464.

Brini, A. and Lenz, J., 2024. A comparison of cryptocurrency volatility-benchmarking new and mature asset classes. *Financial Innovation*, *10*(1), p.122.

Broock, W.A., Scheinkman, J.A., Dechert, W.D. and LeBaron, B., 1996. A test for independence based on the correlation dimension. *Econometric reviews*, *15*(3), pp.197-235.

Brunnermeier, M., Crockett, A., Goodhart, C.A., Persaud, A. and Shin, H.S., 2009. *The fundamental principles of financial regulation* (Vol. 11). Geneva: ICMB, Internat. Center for Monetary and Banking Studies.

Brunnermeier, M.K. and Pedersen, L.H., 2009. Market liquidity and funding liquidity. *The review of financial studies*, *22*(6), pp.2201-2238.

Cachanosky, N., 2019. Can Bitcoin become money? The monetary rule problem. *Australian Economic Papers*, *58*(4), pp.365-374.

Cajueiro, D.O. and Tabak, B.M., 2004. Evidence of long range dependence in Asian equity markets: the role of liquidity and market restrictions. *Physica A: Statistical Mechanics and its Applications*, *342*(3-4), pp.656-664.

Calvo, G.A. and Mendoza, E.G., 2000. Capital-markets crisis and economic collapse in emerging markets: An informational-frictions approach. *American Economic Review*, *90*(2), pp.59-64.

Campbell, J.Y. and Hentschel, L., 1992. No news is good news: An asymmetric model of changing volatility in stock returns. *Journal of financial Economics*, *31*(3), pp.281-318.

Canh, N.P., Wongchoti, U., Thanh, S.D. and Thong, N.T., 2019. Systematic risk in cryptocurrency market: Evidence from DCC-MGARCH model. *Finance Research Letters*, *29*, pp.90-100.

Caporale, G.M., Kang, W.Y., Spagnolo, F. and Spagnolo, N., 2020. Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters*, *32*, p.101297.

Carreras, T., 2022. *$90M DeFi Hack Discovered Seven Months After the Fact*. Cryptobriefing. Available at: https://cryptobriefing.com/90m-defi-hack-discovered-seven-months-after-the-fact/ [Accessed 11 September 2025].

Carter, N. and Jeng, L., 2021. DeFi protocol risks: The paradox of DeFi. *Regtech, suptech and beyond: innovation and technology in financial services" riskbooks–forthcoming Q*, *3*.

Certik, 2022. *Revisiting Beanstalk Farms Exploit*. Certik. Available at: https://www.certik.com/zh-CN/resources/blog/6HaLMGIL5sI2fpfEZc0nzS-revisiting-beanstalk-farms-exploit [Accessed 2 March 2024].

Cevik, E.I., Gunay, S., Zafar, M.W., Destek, M.A., Bugan, M.F. and Tuna, F., 2022. The impact of digital finance on the natural resource market: Evidence from DeFi, oil, and gold. *Resources Policy*, *79*, p.103081.

Chainalysis, 2023. *2022 biggest year ever for crypto hacking with $3.8 billion stolen, primarily from DeFi protocols and by North Korea-linked attackers.* Chainalysis. Available at: https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/ [Accessed 4 March 2024].

Chainalysis, 2024a. *Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises*. Chainalysis. Available at: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/#:~:text=In%202023%2C%20however%2C%20funds%20stolen,a%20drop%20in%20DeFi%20hacking [Accessed 27 August 2025].

Chainalysis, 2024b. *Introduction to Cross-Chain Bridges*. Chainalysis. Available at: https://www.chainalysis.com/blog/introduction-to-cross-chain-bridges/ [Accessed 04 September 2025].

Chainalysis, 2025. *Preventing DeFi Hack Events with Chainalysis Hexagate Using Pattern Recognition and Machine Learning*. Chainalysis. Available at: https://www.chainalysis.com/blog/preventing-defi-hack-events-pattern-recognition-machine-learning-hexagate/#:~:text=In%20the%20early%20years%20of,Hexagate%20identified%20before%20exploits%20occurred [Accessed 11 September 2025].

Charfeddine, L., Benlagha, N. and Khediri, K.B., 2022. An intra-cryptocurrency analysis of volatility connectedness and its determinants: Evidence from mining coins, non-mining coins and tokens. *Research in International Business and Finance*, *62*, p.101699.

Chawki, M., 2022, March. Cybercrime and the Regulation of Cryptocurrencies. In *Future of information and communication conference* (pp. 694-713). Cham: Springer International Publishing.

Cheah, J.E.T., Luo, D., Zhang, Z. and Sung, M.C., 2022. Predictability of bitcoin returns. *The European Journal of Finance*, *28*(1), pp.66-85.

Chen, C.Y.H., Guo, L. and Renault, T., 2019. What makes cryptocurrencies special? investor sentiment and return predictability. *Investor Sentiment and Return Predictability (June 3, 2019)*.

Chen, L., Chen, J. and Xia, C., 2022. Social network behavior and public opinion manipulation. *Journal of Information Security and Applications*, *64*, p.103060.

Chen, Y. and Bellavitis, C., 2019. Decentralized finance: Blockchain technology and the quest for an open financial system. *Stevens Institute of Technology School of Business Research Paper*.

Chen, Y. and Bellavitis, C., 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, *13*, p.e00151.

Chen, Y.L., Chang, Y.T. and Yang, J.J., 2023. Cryptocurrency hacking incidents and the price dynamics of Bitcoin spot and futures. *Finance Research Letters*, *55*, p.103955.

Cheng, H.P. and Yen, K.C., 2020. The relationship between the economic policy uncertainty and the cryptocurrency market. *Finance Research Letters*, *35*, p.101308.

Cheung, A., Roca, E. and Su, J.J., 2015. Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, *47*(23), pp.2348-2358.

Chiu, J., Chung, H., Ho, K.Y. and Wu, C.C., 2018. Investor sentiment and evaporating liquidity during the financial crisis. *International Review of Economics & Finance*, *55*, pp.21-36.

Chordia, T., Roll, R. and Subrahmanyam, A., 2000 Commonality in liquidity. *Journal of financial economics*, *56*(1), pp.3–28.

Chordia, T., Roll, R. and Subrahmanyam, A., 2001. Market liquidity and trading activity. *The journal of finance*, *56*(2), pp.501-530.

Christie, A.A., 1982. The stochastic behavior of common stock variances: Value, leverage and interest rate effects. *Journal of financial Economics*, *10*(4), pp.407-432.

Chu, J., Zhang, Y. and Chan, S., 2019. The adaptive market hypothesis in the high frequency cryptocurrency market. *International Review of Financial Analysis*, *64*, pp.221-231.

Chundakkadan, R. and Nedumparambil, E., 2022. In search of COVID-19 and stock market behavior. *Global Finance Journal*, *54*, p.100639.

CoinGecko, 2024. *Bitcoin price*. Available at: https://www.coingecko.com/en/coins/bitcoin [Accessed March 24, 2024]

CoinMarketCap, 2024. *Crypto market overview*. Available at: https://coinmarketcap.com/charts/ [Accessed 13 February 2025].

Cooper, S.K., Groth, J.C. and Avera, W.E., 1985. Liquidity, exchange listing, and common stock performance. *Journal of Economics and Business*, *37*(1), pp.19-33.

Corbet, S. ed., 2021. *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies* (Vol. 2). Walter de Gruyter GmbH & Co KG.

Corbet, S., Cumming, D.J., Lucey, B.M., Peat, M. and Vigne, S.A., 2019b. Investigating the dynamics between price volatility, price discovery, and criminality in cryptocurrency markets. In *Aea Papers and Proceedings* (pp. 1-57).

Corbet, S., Cumming, D.J., Lucey, B.M., Peat, M. and Vigne, S.A., 2020a. The destabilising effects of cryptocurrency cybercriminality. *Economics Letters*, *191*, p.108741.

Corbet, S., Goodell, J.W. and Günay, S., 2022. What drives DeFi prices? Investigating the effects of investor attention. *Finance Research Letters*, *48*, p.102883.

Corbet, S., Goodell, J.W., Günay, S. and Kaskaloglu, K., 2023. Are DeFi tokens a separate asset class from conventional cryptocurrencies?. *Annals of Operations Research*, *322*(2), pp.609-630.

Corbet, S., Larkin, C., Lucey, B., Meegan, A. and Yarovaya, L., 2020b. Cryptocurrency reaction to fomc announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability*, *46*, p.100706.

Corbet, S., Larkin, C., Lucey, B.M., Meegan, A. and Yarovaya, L., 2020c. The impact of macroeconomic news on Bitcoin returns. *The European Journal of Finance*, *26*(14), pp.1396-1416.

Corbet, S., Lucey, B., Urquhart, A. and Yarovaya, L., 2019a. Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, *62*, pp.182-199.

Corbet, S., Lucey, B. and Yarovaya, L., 2018a. Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters*, *26*, pp.81-88.

Corbet, S., Meegan, A., Larkin, C., Lucey, B. and Yarovaya, L., 2018b. Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics letters*, *165*, pp.28-34.

Darbellay, G.A. and Wuertz, D., 2000. The entropy as a tool for analysing statistical dependences in financial time series. *Physica A: Statistical Mechanics and its Applications*, *287*(3-4), pp.429-439.

Darlin, M., Palaiokrassas, G. and Tassiulas, L., 2022, September. Debt-financed collateral and stability risks in the defi ecosystem. In *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 5-12). IEEE.

De Bondt, W.F. and Thaler, R., 1985. Does the stock market overreact?. *The Journal of finance*, *40*(3), pp.793-805.

DeFiLlama, 2025. *Total Value Locked*. Available at: https://defillama.com/ [Accessed 5 March 2025].

Del Monte, I.A., de Lucio, J.J. and Urban, M.A.S., 2025. Current Understanding of Impermanent Loss Risk in AMMs. *Blockchain: Research and Applications*, p.100360.

Demir, E., Gozgor, G., Lau, C.K.M. and Vigne, S.A., 2018. Does economic policy uncertainty predict the Bitcoin returns? An empirical investigation. *Finance Research Letters*, *26*, pp.145-149.

Demiralay, S. and Golitsis, P., 2021. On the dynamic equicorrelations in cryptocurrency market. *The Quarterly Review of Economics and Finance*, *80*, pp.524-533.

Dhanaraj, S., Gopalaswamy, A.K. and Babu M, S., 2013. Dynamic interdependence between US and Asian markets: an empirical study. *Journal of Financial Economic Policy*, *5*(2), pp.220-237.

Dias, I.K., Fernando, J.R. and Fernando, P.N.D., 2022. Does investor sentiment predict bitcoin return and volatility? A quantile regression approach. *International Review of Financial Analysis*, *84*, p.102383.

Diebold, F.X. and Yilmaz, K., 2009. Measuring financial asset return and volatility spillovers, with application to global equity markets. *The Economic Journal*, *119*(534), pp.158-171.

Diebold, F.X. and Yilmaz, K., 2012. Better to give than to receive: Predictive directional measurement of volatility spillovers. *International Journal of forecasting*, *28*(1), pp.57-66.

Diebold, F.X. and Yılmaz, K., 2014. On the network topology of variance decompositions: Measuring the connectedness of financial firms. *Journal of econometrics*, *182*(1), pp.119-134.

Doerr, J.F., Kosse, A., Khan, A., Lewrick, U., Mojon, B., Nolens, B. and Rice, T., 2021. DeFi risks and the decentralisation illusion. *BIS Quarterly Review*, *21*.

Donnelly, S., Ríos Camacho, E. and Heidebrecht, S., 2024. Digital sovereignty as control: The regulation of digital finance in the European union. *Journal of European Public Policy*, *31*(8), pp.2226-2249.

Dorofeyev, M., Kosov, M., Ponkratov, V., Masterov, A., Karaev, A. and Vasyunina, M., 2018. Trends and prospects for the development of blockchain and cryptocurrencies in the digital economy. *European Research Studies*, *21*(3), pp.429-445.

Dotan, M., Yaish, A., Yin, H.C., Tsytkin, E. and Zohar, A., 2023, November. The vulnerable nature of decentralized governance in defi. In *Proceedings of the 2023 workshop on decentralized finance and security* (pp. 25-31).

Dowling, M., 2022. Is non-fungible token pricing driven by cryptocurrencies?. *Finance Research Letters*, *44*, p.102097.

Dunham, L.M. and Garcia, J., 2021. Measuring the effect of investor sentiment on liquidity. *Managerial Finance*, *47*(1), pp.59-85.

Easley, D., Hvidkjaer, S. and O'hara, M., 2002. Is information risk a determinant of asset returns?. *The journal of finance*, *57*(5), pp.2185-2221.

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

El Montasser, G., Charfeddine, L. and Benhamed, A., 2022. COVID-19, cryptocurrencies bubbles and digital market efficiency: sensitivity and similarity analysis. *Finance Research Letters*, *46*, p.102362.

Elsayed, A.H., Gozgor, G. and Lau, C.K.M., 2022. Causality and dynamic spillovers among cryptocurrencies and currency markets. *International Journal of Finance & Economics*, *27*(2), pp.2026-2040.

Emmert, F., 2023. The regulation of cryptocurrencies in the United States of America. *European Journal of Law Reform*, *25*, pp.1-2.

Engle, R., 2002. Dynamic conditional correlation: A simple class of multivariate generalized autoregressive conditional heteroskedasticity models. *Journal of business & economic statistics*, *20*(3), pp.339-350.

Eom, C., Kaizoji, T., Kang, S.H. and Pichl, L., 2019. Bitcoin and investor sentiment: statistical characteristics and predictability. *Physica A: Statistical Mechanics and its Applications*, *514*, pp.511-521.

European Union, 2023a. *REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113 [Accessed 16 April 2025].

European Union, 2023b. *REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32023R1114 [Accessed 16 April 2025].

Fama, E.F., 1965. The behavior of stock-market prices. *The journal of Business*, *38*(1), pp.34-105.

Fama, E.F., 1970. Efficient capital markets. *Journal of finance*, *25*(2), pp.383-417.

Fang, Y., Chen, C.Y.H. and Jiang, C., 2025. A flight-to-safety from Bitcoin to stock markets: Evidence from cyber attacks. *International Review of Financial Analysis*, *103*, p.104093.

Fernandes, L.H., Bouri, E., Silva, J.W., Bejan, L. and de Araujo, F.H., 2022. The resilience of cryptocurrency market efficiency to COVID-19 shock. *Physica A: Statistical Mechanics and its Applications*, *607*, p.128218.

Financial Services and the Treasury Bureau, 2023. *Policy Statement on Development of Virtual Assets in Hong Kong*. Available at: https://gia.info.gov.hk/general/202210/31/P2022103000454_404805_1_1667173469522.pdf [Accessed 16 April 2025].

Financial Stability Board, 2023. *The Financial Stability Risks of Decentralised Finance*. Financial Stability Board. Available at: https://www.fsb.org/uploads/P160223.pdf [Accessed 27 February 2025].

Fisher, K.L. and Statman, M., 2000. Investor sentiment and stock returns. *Financial Analysts Journal*, *56*(2), pp.16-23.

Forbes, K.J. and Rigobon, R., 2002. No contagion, only interdependence: measuring stock market comovements. *The journal of Finance*, *57*(5), pp.2223-2261.

Fry, J., 2018. Booms, busts and heavy-tails: The story of Bitcoin and cryptocurrency markets?. *Economics Letters*, *171*, pp.225-229.

Gaies, B., Chaâbane, N. and Bouzouita, N., 2024. Navigating the storm: Time-frequency quantile dependence and non-linear causality between crypto-currency market volatility and financial instability. *The Quarterly Review of Economics and Finance*, *93*, pp.43-70.

Gaies, B., Nakhli, M.S., Sahut, J.M. and Schweizer, D., 2023. Interactions between investors' fear and greed sentiment and Bitcoin prices. *The North American Journal of Economics and Finance*, *67*, p.101924.

Gandal, N., Hamrick, J.T., Moore, T. and Oberman, T., 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, *95*, pp.86-96.

Garcia, D. and Schweitzer, F., 2015. Social signals and algorithmic trading of Bitcoin. *Royal Society open science*, *2*(9), p.150288.

Gensler, G., 2024. *Statement on the Financial Innovation and Technology for the 21st Century Act*. U.S. Securities and Exchange Commission (SEC). Available at: https://www.sec.gov/newsroom/speeches-statements/gensler-21st-century-act-05222024 [Accessed 16 April 2025].

Ghosh, A., Gupta, S., Dua, A. and Kumar, N., 2020. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, *163*, p.102635.

Gil-Alana, L.A., Abakah, E.J.A. and Rojo, M.F.R., 2020. Cryptocurrencies and stock market indices. Are they related?. *Research in International Business and Finance*, *51*, p.101063.

Giudici, P. and Abu-Hashish, I., 2019. What determines bitcoin exchange prices? A network VAR approach. *Finance Research Letters*, *28*, pp.309-318.

Glosten, L.R. and Milgrom, P.R., 1985. Bid, ask and transaction prices in a specialist market with heterogeneously informed traders. *Journal of financial economics*, *14*(1), pp.71-100.

Goczek, Ł. and Skliarov, I., 2019. What drives the Bitcoin price? A factor augmented error correction mechanism investigation. *Applied Economics*, *51*(59), pp.6393-6410.

Granger, C.W., 1969. Investigating causal relations by econometric models and cross-spectral methods. *Econometrica: journal of the Econometric Society*, pp.424-438.

Grobys, K., 2021. When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market. *Quantitative Finance*, *21*(8), pp.1267-1279.

Grobys, K., Dufitinema, J., Sapkota, N. and Kolari, J.W., 2022. What's the expected loss when Bitcoin is under cyberattack? A fractal process analysis. *Journal of international financial markets, institutions and money*, *77*, p.101534.

Gronwald, M., 2014. *The economics of bitcoins-market characteristics and price jumps* (No. 5121). CESifo Working Paper.

Grossman, S.J. and Stiglitz, J.E., 1980. On the impossibility of informationally efficient markets. *The American economic review*, *70*(3), pp.393-408.

Guégan, D. and Renault, T., 2021. Does investor sentiment on social media provide robust information for Bitcoin returns predictability?. *Finance Research Letters*, *38*, p.101494.

Gudgeon, L., Perez, D., Harz, D., Livshits, B. and Gervais, A., 2020, June. The decentralized financial crisis. In *2020 crypto valley conference on blockchain technology (CVCBT)* (pp. 1-15). IEEE.

Gupta, A., Pandey, G., Gupta, R., Das, S., Prakash, A., Garg, K. and Sarkar, S., 2024. Machine learning-based approach for predicting the altcoins price direction change from a high-frequency data of seven years based on socio-economic factors, bitcoin prices, twitter and news sentiments. *Computational Economics*, *64*(5), pp.2981-3026.

Gurdgiev, C. and O'Loughlin, D., 2020. Herding and anchoring in cryptocurrency markets: Investor reaction to fear and uncertainty. *Journal of Behavioral and Experimental Finance*, *25*, p.100271.

Hafner, C.M., 2020. Testing for bubbles in cryptocurrencies with time-varying volatility. *Journal of Financial Econometrics*, *18*(2), pp.233-249.

Hansen, B.E., 1992. Testing for parameter instability in linear models. *Journal of policy Modeling*, *14*(4), pp.517-533.

Härdle, W.K., Harvey, C.R. and Reule, R.C., 2020. Understanding cryptocurrencies. *Journal of Financial Econometrics*, *18*(2), pp.181-208.

Harvey, C.R., Ramachandran, A. and Santoro, J., 2021. *DeFi and the Future of Finance*. John Wiley & Sons.

Hasan, M., Naeem, M.A., Arif, M., Shahzad, S.J.H. and Vo, X.V., 2022. Liquidity connectedness in cryptocurrency market. *Financial innovation*, *8*, pp.1-25.

Hasbrouck, J., 1991. Measuring the information content of stock trades. *The Journal of Finance*, *46*(1), pp.179-207.

Hasbrouck, J., 1995. One security, many markets: Determining the contributions to price discovery. *The journal of Finance*, *50*(4), pp.1175-1199.

Hayes, A., 2024. *Blockchain facts: What is it, how it works, and how it can be used.* Investopedia. Available at: https://www.investopedia.com/terms/b/blockchain.asp [Accessed 13 February 2025].

He, Z., Zhou, F., Xia, X., Wen, F. and Huang, Y., 2019. Interaction between oil price and investor sentiment: nonlinear causality, time-varying influence, and asymmetric effect. *Emerging Markets Finance and Trade*, *55*(12), pp.2756-2773.

Hedera, 2025. *DeFi liquidity: Understanding liquidity in decentralized finance*. Hedera. Available at: https://hedera.com/learning/decentralized-finance/defi-liquidity [Accessed 27 February 2025].

Hertig, A., 2023. *What is the ERC-20 Ethereum token standard?* CoinDesk. Available at: https://www.coindesk.com/tech/2021/02/09/what-is-the-erc-20-ethereum-token-standard/ [Accessed 2 March 2024].

Hirshleifer, D. and Shumway, T., 2003. Good day sunshine: Stock returns and the weather. *The journal of Finance*, *58*(3), pp.1009-1032.

HM Treasury, 2023. *Future financial services regulatory regime for cryptoassets: Response to the consultation and call for evidence*. Available at: https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf [Accessed 16 April 2025].

Hong Kong Monetary Authority (HKMA), 2024. *Risk management considerations related to the use of distributed ledger technology*. Available at: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240416e1.pdf [Accessed 16 April 2025].

Hoque, H.A., Kim, J.H. and Pyun, C.S., 2007. A comparison of variance ratio tests of random walk: A case of Asian emerging stock markets. *International Review of Economics & Finance*, *16*(4), pp.488-502.

Hoque, M.E., Billah, M., Kapar, B. and Naeem, M.A., 2024. Quantifying the volatility spillover dynamics between financial stress and US financial sectors: Evidence from QVAR connectedness. *International Review of Financial Analysis*, *95*, p.103434.

Hou, Y., Liu, F., Gao, J., Cheng, C. and Song, C., 2017. Characterizing complexity changes in Chinese stock markets by permutation entropy. *Entropy*, *19*(10), p.514.

Hsu, Y.L. and Tang, L., 2022. Effects of investor sentiment and country governance on unexpected conditional volatility during the COVID-19 pandemic: Evidence from global stock markets. *International Review of Financial Analysis*, *82*, p.102186.

Hu, J., Luo, Q. and Zhang, J., 2020. The fluctuations of bitcoin price during the hacks. *International Journal of Applied Research in Management and Economics*, *3*(1), pp.10-20.

Hu, Y. and Prigent, J.L., 2019. Information asymmetry, cluster trading, and market efficiency: Evidence from the Chinese stock market. *Economic Modelling*, *80*, pp.11-22.

Huang, B.N., 1995. Do Asian stock market prices follow random walks? Evidence from the variance ratio test. *Applied Financial Economics*, *5*(4), pp.251-256.

Huang, C.C. and Hsu, C.C., 2024. Evaluating dependence between DeFi tokens and conventional cryptocurrencies. *Applied Economics Letters*, pp.1-7.

Huang, R.D. and Stoll, H.R., 1997. The components of the bid-ask spread: A general approach. *The Review of Financial Studies*, *10*(4), pp.995-1034.

Huang, Y.X., Xue, T. and Chunxiao-Zhang, J., 2024. How does the Bitcoin sentiment index of fear & greed affect Bitcoin returns?. *Corporate Ownership & Control*, *21*(2), pp.121-131.

Hull, M. and McGroarty, F., 2014. Do emerging markets become more efficient as they develop? Long memory persistence in equity indices. *Emerging Markets Review*, *18*, pp.45-61.

Hunter, M., 2024. *Mt. Gox: What we still don't know 10 years after the collapse.* CoinDesk. Available at: https://www.nasdaq.com/articles/mt.-gox:-what-we-still-dont-know-10-years-after-the-collapse [Accessed 13 February 2025].

Hurst, H.E., 1951. Long-term storage capacity of reservoirs. *Transactions of the American society of civil engineers*, *116*(1), pp.770-799.

Huynh, T.L.D., Ahmed, R., Nasir, M.A., Shahbaz, M. and Huynh, N.Q.A., 2024. The nexus between black and digital gold: evidence from US markets. *Annals of Operations Research*, *334*(1), pp.521-546.

Huynh, T.L.D., Nasir, M.A., Vo, X.V. and Nguyen, T.T., 2020. "Small things matter most": The spillover effects in the cryptocurrency market and gold as a silver bullet. *The North American Journal of Economics and Finance*, *54*, p.101277.

Huynh, T.L.D., Shahbaz, M., Nasir, M.A. and Ullah, S., 2022. Financial modelling, risk management of energy instruments and the role of cryptocurrencies. *Annals of Operations Research*, *313*(1), pp.47-75.

Ibikunle, G., Gregoriou, A., Hoepner, A.G. and Rhodes, M., 2016. Liquidity and market efficiency in the world's largest carbon market. *The British Accounting Review*, *48*(4), pp.431-447.

Immunefi, 2023. *CRYPTO LOSSES IN 2022*. Immunefi. Available at: https://assets.ctfassets.net/t3wqy70tc3bv/1ObYJk9jzWS4ExHICslYep/e2b5cee51268e47ee164c4dffbd78ad4/Immunefi_Crypto_Losses_2022_Report.pdf [Accessed 2 March 2024].

Jagati, S., 2020. *KuCoin hack unpacked: More crypto possibly stolen than first feared*. Shiraz Jagati's Blog. Available at: https://cointelegraph.com/news/kucoin-hack-unpacked-more-crypto-possibly-stolen-than-first-feared [Accessed 24 March 2024].

Japanese Financial Services Agency, 2022. *Regulatory framework for crypto-assets and stablecoins*. Financial Services Agency, the Japanese Government. Available at: https://www.fsa.go.jp/inter/etc/20220914-2/02.pdf [Accessed 16 May 2024].

Jena, S.K., Tiwari, A.K., Abakah, E.J.A. and Hammoudeh, S., 2022. The connectedness in the world petroleum futures markets using a Quantile VAR approach. *Journal of Commodity Markets*, *27*, p.100222.

Ji, Q., Bouri, E., Lau, C.K.M. and Roubaud, D., 2019. Dynamic connectedness and integration in cryptocurrency markets. *International Review of Financial Analysis*, *63*, pp.257-272.

Jia, B., Shen, D. and Zhang, W., 2022. Extreme sentiment and herding: Evidence from the cryptocurrency market. *Research in International Business and Finance*, *63*, p.101770.

Jiang, Y., Nie, H. and Ruan, W., 2018. Time-varying long-term memory in Bitcoin market. *Finance Research Letters*, *25*, pp.280-284.

Jin, X., 2016. The impact of 2008 financial crisis on the efficiency and contagion of Asian stock markets: A Hurst exponent approach. *Finance Research Letters*, *17*, pp.167-175.

Johansen, S., 1988. Statistical analysis of cointegration vectors. *Journal of economic dynamics and control*, *12*(2-3), pp.231-254.

Johansen, S., 1991. Estimation and hypothesis testing of cointegration vectors in Gaussian vector autoregressive models. *Econometrica: journal of the Econometric Society*, pp.1551-1580.

Kakinaka, S. and Umeno, K., 2022. Cryptocurrency market efficiency in short-and long-term horizons during COVID-19: An asymmetric multifractal analysis approach. *Finance Research Letters*, *46*, p.102319.

Kalyvas, A., Li, Z., Papakyriakou, P. and Sakkas, A., 2024. If you feel good, I feel good! The mediating effect of behavioral factors on the relationship between industry indices and Bitcoin returns. *The European Journal of Finance*, *30*(16), pp.1972-1983.

Kaminski, J., 2014. Nowcasting the bitcoin market with twitter signals. *arXiv preprint arXiv:1406.7577*.

Kamstra, M.J., Kramer, L.A. and Levi, M.D., 2000. Losing sleep at the market: The daylight saving anomaly. *American Economic Review*, *90*(4), pp.1005-1011.

Kang, H.J., Lee, S.G. and Park, S.Y., 2022. Information efficiency in the cryptocurrency market: The efficient-market hypothesis. *Journal of Computer Information Systems*, *62*(3), pp.622-631.

Kapar, B. and Olmo, J., 2021. Analysis of Bitcoin prices using market and sentiment variables. *The World Economy*, *44*(1), pp.45-63.

Karim, S., Lucey, B.M., Naeem, M.A. and Uddin, G.S., 2022. Examining the interrelatedness of NFTs, DeFi tokens and cryptocurrencies. *Finance Research Letters*, *47*, p.102696.

Karimi, P., Ghazani, M.M. and Ebrahimi, S.B., 2023. Analyzing spillover effects of selected cryptocurrencies on gold and brent crude oil under COVID-19 pandemic: Evidence from GJR-GARCH and EVT copula methods. *Resources Policy*, *85*, p.103887.

Katsiampa, P., 2019a. An empirical investigation of volatility dynamics in the cryptocurrency market. *Research in International Business and Finance*, *50*, pp.322-335.

Katsiampa, P., 2019b. Volatility co-movement between Bitcoin and Ether. *Finance Research Letters*, *30*, pp.221-227.

Katsiampa, P., Corbet, S. and Lucey, B., 2019. Volatility spillover effects in leading cryptocurrencies: A BEKK-MGARCH analysis. *Finance Research Letters*, *29*, pp.68-74.

Khalfaoui, R., Stef, N., Wissal, B.A. and Sami, B.J., 2022. Dynamic spillover effects and connectedness among climate change, technological innovation, and uncertainty: Evidence from a quantile VAR network and wavelet coherence. *Technological Forecasting and Social Change*, *181*, p.121743.

Khalik Salman, A. and Shukur, G., 2004. Testing for Granger causality between industrial output and CPI in the presence of regime shift: Swedish data. *Journal of Economic Studies*, *31*(6), pp.492-499.

Khuntia, S. and Pattanayak, J.K., 2018. Adaptive market hypothesis and evolving predictability of bitcoin. *Economics Letters*, *167*, pp.26-28.

Khursheed, A., Naeem, M., Ahmed, S. and Mustafa, F., 2020. Adaptive market hypothesis: An empirical analysis of time–varying market efficiency of cryptocurrencies. *Cogent Economics & Finance*, *8*(1), p.1719574.

Kim, A., Trimborn, S. and Härdle, W.K., 2021. VCRIX—A volatility index for crypto-currencies. *International Review of Financial Analysis*, *78*, p.101915.

Kim, H., Jang, S.M., Kim, S.H. and Wan, A., 2018. Evaluating sampling methods for content analysis of Twitter data. *Social media+ society*, *4*(2), p.2056305118772836.

Klein, T., Thu, H.P. and Walther, T., 2018. Bitcoin is not the New Gold–A comparison of volatility, correlation, and portfolio performance. *International Review of Financial Analysis*, *59*, pp.105-116.

Köchling, G., Müller, J. and Posch, P.N., 2019. Does the introduction of futures improve the efficiency of Bitcoin?. *Finance Research Letters*, *30*, pp.367-370.

Kollias, C., Manou, E., Papadamou, S. and Stagiannis, A., 2011. Stock markets and terrorist attacks: Comparative evidence from a large and a small capitalization market. *European Journal of Political Economy*, *27*, pp.S64-S77.

Koop, G. and Korobilis, D., 2013. Large time-varying parameter VARs. *Journal of Econometrics*, *177*(2), pp.185-198.

Koop, G., Pesaran, M.H. and Potter, S.M., 1996. Impulse response analysis in nonlinear multivariate models. *Journal of econometrics*, *74*(1), pp.119-147.

Kostika, E. and Laopodis, N.T., 2020. Dynamic linkages among cryptocurrencies, exchange rates and global equity markets. *Studies in Economics and Finance*, *37*(2), pp.243-265.

Kraaijeveld, O. and De Smedt, J., 2020. The predictive power of public Twitter sentiment for forecasting cryptocurrency prices. *Journal of International Financial Markets, Institutions and Money*, *65*, p.101188.

Kristoufek, L., 2013. BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, *3*(1), p.3415.

Kristoufek, L., 2015. What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. *PloS one*, *10*(4), p.e0123923.

Krückeberg, S. and Scholz, P., 2020. Decentralized efficiency? Arbitrage in bitcoin markets. *Financial Analysts Journal*, *76*(3), pp.135-152.

Kumar, A., Iqbal, N., Mitra, S.K., Kristoufek, L. and Bouri, E., 2022. Connectedness among major cryptocurrencies in standard times and during the COVID-19 outbreak. *Journal of International Financial Markets, Institutions and Money*, *77*, p.101523.

Kumar, A.S. and Anandarao, S., 2019. Volatility spillover in crypto-currency markets: Some evidences from GARCH and wavelet analysis. *Physica A: statistical mechanics and its applications*, *524*, pp.448-458.

Kumar, S., Patel, R., Iqbal, N. and Gubareva, M., 2023. Interconnectivity among cryptocurrencies, NFTs, and DeFi: evidence from the Russia-Ukraine conflict. *The North American Journal of Economics and Finance*, *68*, p.101983.

Kurka, J., 2019. Do cryptocurrencies and traditional asset classes influence each other?. *Finance Research Letters*, *31*, pp.38-46.

Kyle, A.S., 1985. Continuous auctions and insider trading. *Econometrica: Journal of the Econometric Society*, pp.1315-1335.

Kyle, A.S. and Obizhaeva, A.A., 2016. Market microstructure invariance: Empirical hypotheses. *Econometrica*, *84*(4), pp.1345-1404.

Lahmiri, S., Bekiros, S. and Salvi, A., 2018. Long-range memory, distributional variation and randomness of bitcoin volatility. *Chaos, Solitons & Fractals*, *107*, pp.43-48.

Lal, S., Nguyen, T.X.T., Bawalle, A.A., Khan, M.S.R. and Kadoya, Y., 2024. Unraveling investor behavior: The role of hyperbolic discounting in panic selling behavior on the global COVID-19 financial crisis. *Behavioral Sciences*, *14*(9), p.795.

Lamberti, P.W., Martin, M.T., Plastino, A. and Rosso, O.A., 2004. Intensive entropic non-triviality measure. *Physica A: Statistical Mechanics and its Applications*, *334*(1-2), pp.119-131.

Lee, C.F., Chen, G.M. and Rui, O.M., 2001. Stock returns and volatility on China's stock markets. *Journal of Financial Research*, *24*(4), pp.523-543.

Leirvik, T., 2022. Cryptocurrency returns and the volatility of liquidity. *Finance Research Letters*, *44*, p.102031.

Li, M., Manahov, V. and Ashton, J., 2024. The impact of cryptocurrency heists on Bitcoin's market efficiency. *International Journal of Finance & Economics*.

Lim, K.P., 2007. Ranking market efficiency for stock markets: A nonlinear perspective. *Physica A: Statistical Mechanics and its Applications*, *376*, pp.445-454.

Lin, X., Meng, Y. and Zhu, H., 2023. How connected is the crypto market risk to investor sentiment?. *Finance Research Letters*, *56*, p.104177.

Ljung, G.M. and Box, G.E., 1978. On a measure of lack of fit in time series models. *Biometrika*, *65*(2), pp.297-303.

Lo, A.W., 2004. The adaptive markets hypothesis: Market efficiency from an evolutionary perspective. *Journal of Portfolio Management, Forthcoming*.

Lo, A.W., 2005. Reconciling efficient markets with behavioral finance: the adaptive markets hypothesis. *Journal of investment consulting*, *7*(2), pp.21-44.

Lo, A.W. and MacKinlay, A.C., 1988. Stock market prices do not follow random walks: Evidence from a simple specification test. *The review of financial studies*, *1*(1), pp.41-66.

Loi, H., 2018. The liquidity of bitcoin. *International Journal of Economics and Finance*, *10*(1), pp.13-22.

Long, S.C., Xie, Y., Zhou, Z., Lucey, B.M. and Urquhart, A., 2024. From Whales to Waves: The Role of Social Media Sentiment in Shaping Cryptocurrency Markets. *Ying and Zhou, Zhengyuan and Lucey, Brian M. and Urquhart, Andrew, From Whales to Waves: The Role of Social Media Sentiment in Shaping Cryptocurrency Markets (January 25, 2024)*.

López-Cabarcos, M.Á., Pérez-Pico, A.M., Piñeiro-Chousa, J. and Šević, A., 2021. Bitcoin volatility, stock market and investor sentiment. Are they connected?. *Finance Research Letters*, *38*, p.101399.

López-Martín, C., 2023. Dynamic analysis of calendar anomalies in cryptocurrency markets: Evidences of adaptive market hypothesis. *Spanish Journal of Finance and Accounting/Revista Española de Financiación y Contabilidad*, *52*(4), pp.559-592.

Luther, W.J. and White, L.H., 2014. Can Bitcoin become a major currency?. GMU Working Paper in Economics No. 14-17. Available at: https://ssrn.com/abstract=2446604 [Accessed 19 February 2025].

Luu Duc Huynh, T., 2019. Spillover risks on cryptocurrency markets: A look from VAR-SVAR granger causality and student'st copulas. *Journal of Risk and Financial Management*, *12*(2), p.52.

Lyócsa, Š., Molnár, P., Plíhal, T. and Širaňová, M., 2020. Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin. *Journal of Economic Dynamics and Control*, *119*, p.103980.

Mai, F., Shan, Z., Bai, Q., Wang, X. and Chiang, R.H., 2018. How does social media impact Bitcoin value? A test of the silent majority hypothesis. *Journal of management information systems*, *35*(1), pp.19-52.

Makarov, I. and Schoar, A., 2020. Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics*, *135*(2), pp.293-319.

Malkiel, B.G., 2003. The efficient market hypothesis and its critics. *Journal of economic perspectives*, *17*(1), pp.59-82.

Manahov, V., Hudson, R. and Gebka, B., 2014. Does high frequency trading affect technical analysis and market efficiency? And if so, how?. *Journal of International Financial Markets, Institutions and Money*, *28*, pp.131-157.

Manahov, V. and Li, M., 2024. The implications of virtual money on travel and tourism. *Annals of Tourism Research*, *105*, p.103686.

Manahov, V. and Li, M., 2025a. A note on the relationship between digital assets and the energy markets: new evidence from the most prominent crypto heists. *The European Journal of Finance*, pp.1-37.

Manahov, V. and Li, M., 2025b. The digitalisation of the real estate market: New evidence from the most prominent crypto hacker attacks. *International Review of Financial Analysis*, *103*, p.104166.

Manahov, V. and Li, M., 2025c. The implications of crypto hacker attacks on financing new ventures. *Journal of Small Business Management*, pp.1-42.

Marczak, M. and Beissinger, T., 2016. Bidirectional relationship between investor sentiment and excess returns: New evidence from the Wavelet perspective. *Applied Economics Letters*, *23*(18), pp.1305-1311.

Marella, V., Kokabha, M.R., Merikivi, J. and Tuunainen, V., 2021, January. Rebuilding trust in cryptocurrency exchanges after cyber-attacks. In *Annual Hawaii International Conference on System Sciences* (pp. 5636-5646). Hawaii International Conference on System Sciences.

Mensi, W., Al-Yahyaee, K.H. and Kang, S.H., 2019a. Structural breaks and double long memory of cryptocurrency prices: A comparative analysis from Bitcoin and Ethereum. *Finance Research Letters*, *29*, pp.222-230.

Mensi, W., Al-Yahyaee, K.H., Al-Jarrah, I.M.W., Vo, X.V. and Kang, S.H., 2021. Does volatility connectedness across major cryptocurrencies behave the same at different frequencies? A portfolio risk analysis. *International Review of Economics & Finance*, *76*, pp.96-113.

Mensi, W., Gubareva, M. and Kang, S.H., 2024. Frequency connectedness between DeFi and cryptocurrency markets. *The Quarterly Review of Economics and Finance*, *93*, pp.12-27.

Mensi, W., Lee, Y.J., Al-Yahyaee, K.H., Sensoy, A. and Yoon, S.M., 2019b. Intraday downward/upward multifractality and long memory in Bitcoin and Ethereum markets: An asymmetric multifractal detrended fluctuation analysis. *Finance Research Letters*, *31*, pp.19-25.

Mensi, W., Rehman, M.U., Al-Yahyaee, K.H., Al-Jarrah, I.M.W. and Kang, S.H., 2019c. Time frequency analysis of the commonalities between Bitcoin and major Cryptocurrencies: Portfolio risk management implications. *The North American Journal of Economics and Finance*, *48*, pp.283-294.

Metelski, D. and Sobieraj, J., 2022. Decentralized finance (DeFi) projects: A study of key performance indicators in terms of DeFi protocols' valuations. *International Journal of Financial Studies*, *10*(4), p.108.

Meyer, E.A., Sandner, P., Cloutier, B. and Welpe, I.M., 2023. High on Bitcoin: Evidence of emotional contagion in the YouTube crypto influencer space. *Journal of Business Research*, *164*, p.113850.

Mills, L., 2024. *Crypto Usage Grows in Venezuela Despite Government Mismanagement*. Crypto Council for Innovation. Available at: https://cryptoforinnovation.org/crypto-usage-grows-in-venezuela-despite-government-

mismanagement/#:~:text=For%20several%20years%2C%20Venezuelans%20have,last%20year%20totaled%20%245.4%20billion [Accessed 13 February 2025].

Milunovich, G., 2018. Cryptocurrencies, mainstream asset classes and risk factors: A study of connectedness. *Australian Economic Review*, *51*(4), pp.551-563.

Mohamad, A. and Dimitriou, D., 2024. From scam to heist: the impact of cybercrimes on cryptocurrencies. *Applied Economics Letters*, pp.1-9.

Mohan, V., 2022. Automated market makers and decentralized exchanges: a DeFi primer. *Financial Innovation*, *8*(1), p.20.

Mokni, K., El Montasser, G., Ajmi, A.N. and Bouri, E., 2024. On the efficiency and its drivers in the cryptocurrency market: the case of Bitcoin and Ethereum. *Financial Innovation*, *10*(1), p.39.

Monetary Authority of Singapore, 2019. *Payment Services Act 2019*. Available at: https://www.mas.gov.sg/regulation/acts/payment-services-act [Accessed 16 April 2025].

Monetary Authority of Singapore, 2022. *Financial Services and Markets Act 2022*. Available at: https://www.mas.gov.sg/regulation/acts/financial-services-and-markets-act-2022 [Accessed 16 April 2025].

Nadarajah, S. and Chu, J., 2017. On the inefficiency of Bitcoin. *Economics Letters*, *150*, pp.6-9.

Nadler, M., Bekemeier, F. and Schär, F., 2023, May. DeFi risk transfer: Towards a fully decentralized insurance protocol. In *2023 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 1-9). IEEE.

Naeem, M.A., Bouri, E., Peng, Z., Shahzad, S.J.H. and Vo, X.V., 2021a. Asymmetric efficiency of cryptocurrencies during COVID19. *Physica A: Statistical Mechanics and its Applications*, *565*, p.125562.

Naeem, M.A., Mbarki, I. and Shahzad, S.J.H., 2021b. Predictive role of online investor sentiment for cryptocurrency market: Evidence from happiness and fears. *International Review of Economics & Finance*, *73*, pp.496-514.

Naeem, M.A., Mbarki, I., Suleman, M.T., Vo, X.V. and Shahzad, S.J.H., 2021c. Does Twitter happiness sentiment predict cryptocurrency?. *International Review of Finance*, *21*(4), pp.1529-1538.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto*.

Nansen, 2022. *BNB Chain's Cross-Chain Bridge Exploit Explained*. Nansen. Available at: https://www.nansen.ai/research/bnb-chains-cross-chain-bridge-exploit-explained#:~:text=frozen%20in%20BSC.-,How%20Did%20It%20Happen%3F,Binance%20Smart%20Chain%20(BEP20) [Accessed 13 February 2024].

Noda, A., 2021. On the evolution of cryptocurrency market efficiency. *Applied Economics Letters*, *28*(6), pp.433-439.

Nyblom, J., 1989. Testing for the constancy of parameters over time. *Journal of the American Statistical Association*, *84*(405), pp.223-230.

Omane-Adjepong, M. and Alagidede, I.P., 2019. Multiresolution analysis and spillovers of major cryptocurrency markets. *Research in International Business and Finance*, *49*, pp.191-206.

Othman, A.H.A., Alhabshi, S.M. and Haron, R., 2019. The effect of symmetric and asymmetric information on volatility structure of crypto-currency markets: A case study of bitcoin currency. *Journal of Financial Economic Policy*, *11*(3), pp.432-450.

Ozdamar, M., Sensoy, A. and Akdeniz, L., 2022. Retail vs institutional investor attention in the cryptocurrency market. *Journal of International Financial Markets, Institutions and Money*, *81*, p.101674.

Özdemir, O., 2022. Cue the volatility spillover in the cryptocurrency markets during the COVID-19 pandemic: evidence from DCC-GARCH and wavelet analysis. *Financial Innovation*, *8*(1), p.12.

Ozili, P.K., 2022. Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, *6*(2), pp.117-133.

Panagiotidis, T., Papapanagiotou, G. and Stengos, T., 2022. On the volatility of cryptocurrencies. *Research in International Business and Finance*, *62*, p.101724.

Panagiotidis, T., Stengos, T. and Vravosinos, O., 2019. The effects of markets, uncertainty and search intensity on bitcoin returns. *International Review of Financial Analysis*, *63*, pp.220-242.

Park, M. and Chai, S., 2020. The effect of information asymmetry on investment behavior in cryptocurrency market.

Park, S., Lee, S., Lee, Y., Ko, H., Son, B., Lee, J. and Jang, H., 2023. Price co-movements in decentralized financial markets. *Applied Economics Letters*, *30*(21), pp.3075-3082.

Pástor, Ľ. and Stambaugh, R. F., 2003. Liquidity risk and expected stock returns. *Journal of political economy*, *111* (3), pp.642–685.

Patil, A.C. and Rastogi, S., 2019. Time-varying price–volume relationship and adaptive market efficiency: A survey of the empirical literature. *Journal of Risk and Financial Management*, *12*(2), p.105.

Pellicer, J., 2024. Economic Risks in AMMs: A Comprehensive Risk Analysis. Medium. Available at: https://medium.com/sentora/economic-risks-in-amms-a-comprehensive-risk-analysis-02e993270570 [Accessed 21 August 2025].

Perry-Carrera, B., 2018. Effect of sentiment on Bitcoin price formation. *Economics in Trinity College of Duke University*, *49*.

Pesaran, H.H. and Shin, Y., 1998. Generalized impulse response analysis in linear multivariate models. *Economics letters*, *58*(1), pp.17-29.

Phillips, P.C., Shi, S. and Yu, J., 2015a. Testing for multiple bubbles: Historical episodes of exuberance and collapse in the S&P 500. *International economic review*, *56*(4), pp.1043-1078.

Phillips, P.C., Shi, S. and Yu, J., 2015b. Testing for multiple bubbles: Limit theory of real-time detectors. *International Economic Review*, *56*(4), pp.1079-1134.

Phillips, P.C., Wu, Y. and Yu, J., 2011. Explosive behavior in the 1990s Nasdaq: When did exuberance escalate asset values?. *International economic review*, *52*(1), pp.201-226.

Polat, A.Y., Aysan, A.F., Tekin, H. and Tunali, A.S., 2022. Bitcoin-specific fear sentiment matters in the COVID-19 outbreak. *Studies in Economics and Finance*, *39*(1), pp.98-110.

Primiceri, G.E., 2005. Time varying structural vector autoregressions and monetary policy. *The Review of economic studies*, *72*(3), pp.821-852.

Qiao, X., Zhu, H., Tang, Y. and Peng, C., 2023. Time-frequency extreme risk spillover network of cryptocurrency coins, DeFi tokens and NFTs. *Finance Research Letters*, *51*, p.103489.

Raddant, M. and Kenett, D.Y., 2021. Interconnectedness in the global financial market. *Journal of International Money and Finance*, *110*, p.102280.

Raimundo Júnior, G.D.S., Palazzi, R.B., Tavares, R.D.S. and Klotzle, M.C., 2022. Market stress and herding: a new approach to the cryptocurrency market. *Journal of Behavioral Finance*, *23*(1), pp.43-57.

Rearick, B. 2022. *5 Cybersecurity Cryptos to Bet on a Secure Future for Digital Money*. INVESTORPLACE. Available at: https://investorplace.com/2022/03/5-cybersecurity-cryptos-to-bet-on-a-secure-future-for-digital-money/ [Accessed 4 March 2024].

Rehman, M.U., 2020. Do bitcoin and precious metals do any good together? An extreme dependence and risk spillover analysis. *Resources Policy*, *68*, p.101737.

Rizvi, S.A.R., Dewandaru, G., Bacha, O.I. and Masih, M., 2014. An analysis of stock market efficiency: Developed vs Islamic stock markets using MF-DFA. *Physica A: Statistical Mechanics and its Applications*, *407*, pp.86-99.

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.

Roll, R., 1986. The hubris hypothesis of corporate takeovers. *Journal of business*, pp.197-216.

Ruan, Q., Meng, L. and Lv, D., 2021. Effect of introducing Bitcoin futures on the underlying Bitcoin market efficiency: A multifractal analysis. *Chaos, Solitons & Fractals*, *153*, p.111576.

Rudkin, S., Rudkin, W. and Dłotko, P., 2023. On the topology of cryptocurrency markets. *International Review of Financial Analysis*, *89*, p.102759.

Sabalionis, A., Wang, W. and Park, H., 2021. What affects the price movements in Bitcoin and Ethereum?. *The Manchester School*, *89*(1), pp.102-127.

Saffi, P.A. and Sigurdsson, K., 2011. Price efficiency and short selling. *The Review of Financial Studies*, *24*(3), pp.821-852.

Saleem, T., Yaqub, U. and Zaman, S., 2024. Twitter sentiment analysis and bitcoin price forecasting: implications for financial risk management. *The Journal of Risk Finance*, *25*(3), pp.407-421.

Samarakoon, L.P., 2011. Stock market interdependence, contagion, and the US financial crisis: The case of emerging and frontier markets. *Journal of International Financial Markets, Institutions and Money*, *21*(5), pp.724-742.

Sattarov, O., Jeon, H.S., Oh, R. and Lee, J.D., 2020, November. Forecasting bitcoin price fluctuation by twitter sentiment analysis. In *2020 international conference on information science and communications technologies (ICISCT)* (pp. 1-4). IEEE.

Schär, F., 2021. Decentralized finance: on blockchain and smart contract-based financial markets. *Review of the Federal Reserve Bank of St Louis*, *103*(2), pp.153-174.

Scharnowski, S., 2021. Understanding bitcoin liquidity. *Finance Research Letters*, *38*, p.101477.

Schmeling, M., 2009. Investor sentiment and stock returns: Some international evidence. *Journal of empirical finance*, *16*(3), pp.394-408.

Scholtens, B. and Peenstra, W., 2009. Scoring on the stock exchange? The effect of football matches on stock market returns: an event study. *Applied Economics*, *41*(25), pp.3231-3237.

Schueffel, P., 2021. Defi: Decentralized finance-an introduction and overview. *Journal of Innovation Management*, *9*(3), pp.I-XI.

Sensoy, A., 2019. The inefficiency of Bitcoin revisited: A high-frequency analysis with alternative currencies. *Finance Research Letters*, *28*, pp.68-73.

Shah, K., Lathiya, D., Lukhi, N., Parmar, K. and Sanghvi, H., 2023. A systematic review of decentralized finance protocols. *International Journal of Intelligent Networks*, *4*, pp.171-181.

Shahzad, S.J.H., Bouri, E., Ahmad, T., Naeem, M.A. and Vo, X.V., 2021. The pricing of bad contagion in cryptocurrencies: A four-factor pricing model. *Finance Research Letters*, *41*, p.101797.

Shanaev, S., Sharma, S., Ghimire, B. and Shuraeva, A., 2020. Taming the blockchain beast? Regulatory implications for the cryptocurrency Market. *Research in International Business and Finance*, *51*, p.101080.

Sharpe, W.F., 1964. Capital asset prices: A theory of market equilibrium under conditions of risk. *The journal of finance*, *19*(3), pp.425-442.

Shefrin, H. and Statman, M., 1985. The disposition to sell winners too early and ride losers too long: Theory and evidence. *The Journal of finance*, *40*(3), pp.777-790.

Shen, D., Urquhart, A. and Wang, P., 2020. A three-factor pricing model for cryptocurrencies. *Finance Research Letters*, *34*, p.101248.

Shiller, R.J., 1981. Do stock prices move too much to be justified by subsequent changes in dividends?.

Shiller, R.J., 2003. From efficient markets theory to behavioral finance. *Journal of economic perspectives*, *17*(1), pp.83-104.

Shleifer, A., 2000. Inefficient Markets: An Introduction to Behavioural Finance in Oxford University Press. *New York*.

Shynkevich, A., 2021. Impact of bitcoin futures on the informational efficiency of bitcoin spot market. *Journal of Futures Markets*, *41*(1), pp.115-134.

Sifat, I.M., Mohamad, A. and Shariff, M.S.B.M., 2019. Lead-lag relationship between bitcoin and ethereum: Evidence from hourly and daily data. *Research in International Business and Finance*, *50*, pp.306-321.

Simon, H.A., 1990. Bounded rationality. *Utility and probability*, pp.15-18.

Sims, C.A., 1980. Macroeconomics and reality. *Econometrica: journal of the Econometric Society*, pp.1-48.

Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *Ieee Access*, *9*, pp.13938-13959.

Siokis, F.M., 2018. Credit market Jitters in the course of the financial crisis: A permutation entropy approach in measuring informational efficiency in financial assets. *Physica A: Statistical Mechanics and its Applications*, *499*, pp.266-275.

Smales, L.A., 2019. Bitcoin as a safe haven: Is it even worth considering?. *Finance Research Letters*, *30*, pp.385-393.

Statista, 2025. *DeFi dominance, or DeFi market capitalization as a share of the overall crypto market cap, worldwide from June 2021 to March 2025*. Statista. Available at: https://www.statista.com/statistics/1262836/defi-dominance/ [Accessed 20 February 2025].

Stavroyiannis, S., 2018. Value-at-risk and related measures for the Bitcoin. *The Journal of Risk Finance*, *19*(2), pp.127-136.

Stoll, H.R., 1989. Inferring the components of the bid-ask spread: Theory and empirical tests. *the Journal of Finance*, *44*(1), pp.115-134.

Stosic, D., Stosic, D., Ludermir, T.B. and Stosic, T., 2019. Exploring disorder and complexity in the cryptocurrency space. *Physica A: Statistical Mechanics and its Applications*, *525*, pp.548-556.

Strych, J.O., 2022. The impact of margin trading and short selling by retail investors on market price efficiency: Empirical evidence from bitcoin exchanges. *Finance Research Letters*, *47*, p.102689.

Swanson, N.R., 1998. Money and output viewed through a rolling window. *Journal of monetary Economics*, *41*(3), pp.455-474.

Takaishi, T., 2018. Statistical properties and multifractality of Bitcoin. *Physica A: statistical mechanics and its applications*, *506*, pp.507-519.

Takaishi, T. and Adachi, T., 2020. Market efficiency, liquidity, and multifractality of Bitcoin: A dynamic study. *Asia-Pacific Financial Markets*, *27*, pp.145-154.

The Fintech Times, 2023. *Institutional Investors Show Growing Interest in DeFi Investments*. The Fintech Times. Available at: https://thefintechtimes.com/institutional-investors-show-growing-interest-in-defi-investments/ [Accessed 20 August 2025].

Thoma, M.A., 1994. Subsample instability and asymmetries in money-income causality. *Journal of econometrics*, *64*(1-2), pp.279-306.

Tiniç, M., Sensoy, A., Akyildirim, E. and Corbet, S., 2023. Adverse selection in cryptocurrency markets. *Journal of Financial Research*, *46*(2), pp.497-546.

Tiwari, A.K., Adewuyi, A.O., Albulescu, C.T. and Wohar, M.E., 2020. Empirical evidence of extreme dependence and contagion risk between main cryptocurrencies. *The North American Journal of Economics and Finance*, *51*, p.101083.

Tiwari, A.K., Jana, R.K., Das, D. and Roubaud, D., 2018. Informational efficiency of Bitcoin—An extension. *Economics Letters*, *163*, pp.106-109.

Trimborn, S., Li, M. and Härdle, W.K., 2020. Investing with cryptocurrencies—A liquidity constrained investment approach. *Journal of Financial Econometrics*, *18*(2), pp.280-306.

Tsihitas, T., 2025. *Worldwide cryptocurrency heists tracker (updated daily)*. Available at: https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/ [Accessed 13 February 2025].

Ullah, S., Attah-Boakye, R., Adams, K. and Zaefarian, G., 2022. Assessing the influence of celebrity and government endorsements on bitcoin's price volatility. *Journal of Business Research*, *145*, pp.228-239.

Umar, M., 2021. The impact of cyber-attacks on cryptocurrency price, return and liquidity: evidence from quantile-on-quantile regression. Available at: https://ssrn.com/abstract=3945849 [Accessed 05 November 2025].

Umar, M., 2025. The impact of cyber-attacks on different dimensions of cryptocurrency markets. *Technology in Society*, *81*, p.102865.

Urquhart, A., 2016. The inefficiency of Bitcoin. *Economics Letters*, *148*, pp.80-82.

Vasudevan, S., Piazza, A. and Ghinoi, S., 2024. Information diffusion in referral networks: an empirical investigation of the crypto asset landscape. *Quality & Quantity*, pp.1-18.

Victor, F. and Weintraud, A.M., 2021, April. Detecting and quantifying wash trading on decentralized cryptocurrency exchanges. In *Proceedings of the Web Conference 2021* (pp. 23-32).

Vidal-Tomás, D., 2021. An investigation of cryptocurrency data: the market that never sleeps. *Quantitative Finance*, *21*(12), pp.2007-2024.

Vidal-Tomás, D., 2022. Which cryptocurrency data sources should scholars use?. *International Review of Financial Analysis*, *81*, p.102061.

Waghmare, S. and Uike, D., 2023. Investor Sentiment Driving Crypto-Trade in India. *Fintech and Cryptocurrency*, pp.193-220.

Wald, A. and Wolfowitz, J., 1940. On a test whether two samples are from the same population. *The Annals of Mathematical Statistics*, *11*(2), pp.147-162.

Walters, S., 2023. *Nexus Mutual Review (NXM): Defi Smart Contract Insurance*. Coinbureau. Available at: https://coinbureau.com/review/nexus-mutual-nxm/ [Accessed 27 August 2025].

Wang, B., Liu, H., Liu, C., Yang, Z., Ren, Q., Zheng, H. and Lei, H., 2021, May. Blockeye: Hunting for defi attacks on blockchain. In *2021 IEEE/ACM 43rd international conference on software engineering: companion proceedings (ICSE-companion)* (pp. 17-20). IEEE.

Wang, J.N., Liu, H.C. and Hsu, Y.T., 2024. A U-shaped relationship between the crypto fear-greed index and the price synchronicity of cryptocurrencies. *Finance Research Letters*, *59*, p.104763.

Wang, L., Ma, F., Niu, T. and Liang, C., 2021. The importance of extreme shock: Examining the effect of investor sentiment on the crude oil futures market. *Energy Economics*, *99*, p.105319.

Wang, P., Li, X., Shen, D. and Zhang, W., 2020. How does economic policy uncertainty affect the bitcoin market?. *Research in International Business and Finance*, *53*, p.101234.

Wang, P., Zhang, W., Li, X. and Shen, D., 2019. Is cryptocurrency a hedge or a safe haven for international indices? A comprehensive and dynamic perspective. *Finance Research Letters*, *31*, pp.1-18.

Wanidwaranan, P. and Termprasertsakul, S., 2024. Herd behavior in cryptocurrency market: evidence of network effect. *Review of Behavioral Finance*, *16*(3), pp.406-423.

Wei, W.C., 2018. Liquidity and market efficiency in cryptocurrencies. *Economics Letters*, *168*, pp.21-24.

Wen, Y., Lu, F., Liu, Y. and Huang, X., 2021. Attacks and countermeasures on blockchains: A survey from layering perspective. *Computer Networks*, *191*, p.107978.

Weng, Z. and Lin, A., 2022. Public opinion manipulation on social media: social network analysis of Twitter bots during the COVID-19 pandemic. *International journal of environmental research and public health*, *19*(24), p.16376.

Wilms, R., Mäthner, E., Winnen, L. and Lanwehr, R., 2021. Omitted variable bias: A threat to estimating causal relationships. *Methods in Psychology*, *5*, p.100075.

Wronka, C., 2024. Crypto-asset regulatory landscape: a comparative analysis of the crypto-asset regulation in the UK and Germany. *Journal of Asset Management*, *25*(4), pp.417-426.

Wu, K., Ma, Y., Huang, G. and Liu, X., 2021. A first look at blockchain-based decentralized applications. *Software: Practice and Experience*, *51*(10), pp.2033-2050.

Wu, X., Wu, L. and Chen, S., 2022. Long memory and efficiency of Bitcoin during COVID-19. *Applied Economics*, *54*(4), pp.375-389.

Yang, Y. and Zhao, Z., 2021. Large cryptocurrency-portfolios: Efficient sorting with leverage constraints. *Applied Economics*, *53*(21), pp.2398-2411.

Yao, S., Sensoy, A., Nguyen, D.K. and Li, T., 2024. Investor attention and cryptocurrency market liquidity: a double-edged sword. *Annals of Operations Research*, *334*(1), pp.815-856.

Yarovaya, L., Brzeszczyński, J. and Lau, C.K.M., 2016. Intra-and inter-regional return and volatility spillovers across emerging and developed markets: Evidence from stock indices and stock index futures. *International Review of Financial Analysis*, *43*, pp.96-114.

Yarovaya, L. and Zięba, D., 2022. Intraday volume-return nexus in cryptocurrency markets: Novel evidence from cryptocurrency classification. *Research in International Business and Finance*, *60*, p.101592.

Yermack, D., 2024. Is Bitcoin a real currency? An economic appraisal. In *Handbook of digital currency* (pp. 29-40). Academic Press.

Yi, E., Ahn, K. and Choi, M., 2022. Cryptocurrency: Not far from equilibrium. *Technological Forecasting and Social Change*, *177*, p.121424.

Yi, S., Xu, Z. and Wang, G.J., 2018. Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?. *International Review of Financial Analysis*, *60*, pp.98-114.

Yousaf, I., Ali, S., Bouri, E. and Dutta, A., 2021. Herding on fundamental/nonfundamental information during the COVID-19 outbreak and cyber-attacks: Evidence from the cryptocurrency market. *Sage Open*, *11*(3), p.21582440211029911.

Yousaf, I., Assaf, A. and Demir, E., 2024a. Relationship between real estate tokens and other asset classes: Evidence from quantile connectedness approach. *Research in International Business and Finance*, *69*, p.102238.

Yousaf, I., Jareño, F. and Tolentino, M., 2023. Connectedness between Defi assets and equity markets during COVID-19: A sector analysis. *Technological Forecasting and Social Change*, *187*, p.122174.

Yousaf, I., Nekhili, R. and Gubareva, M., 2022. Linkages between DeFi assets and conventional currencies: Evidence from the COVID-19 pandemic. *International Review of Financial Analysis*, *81*, p.102082.

Yousaf, I., Pham, L. and Goodell, J.W., 2024b. Dynamic spillovers between leading cryptocurrencies and derivatives tokens: insights from a quantile VAR approach. *International Review of Financial Analysis*, *94*, p.103156.

Yousaf, I. and Yarovaya, L., 2022. Herding behavior in conventional cryptocurrency market, non-fungible tokens, and DeFi assets. *Finance Research Letters*, *50*, p.103299.

Yue, W., Zhang, S. and Zhang, Q., 2021. Asymmetric news effects on cryptocurrency liquidity: an event study perspective. *Finance Research Letters*, *41*, p.101799.

Yuyama, T., Katayama, K. and Brigner, P., 2023, May. Proposal of principles of defi disclosure and regulation. In *International Conference on Financial Cryptography and Data Security* (pp. 141-164). Cham: Springer Nature Switzerland.

Zanin, M., 2008. Forbidden patterns in financial time series. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *18*(1).

Zanin, M., Zunino, L., Rosso, O.A. and Papo, D., 2012. Permutation entropy and its main biomedical and econophysics applications: a review. *Entropy*, *14*(8), pp.1553-1577.

Zargar, F.N. and Kumar, D., 2019. Informational inefficiency of Bitcoin: A study based on high-frequency data. *Research in International Business and Finance*, *47*, pp.344-353.

Zeng, T., Yang, M. and Shen, Y., 2020. Fancy Bitcoin and conventional financial assets: Measuring market integration based on connectedness networks. *Economic Modelling*, *90*, pp.209-220.

Zhang, G., Xu, L. and Xue, Y., 2017. Model and forecast stock market behavior integrating investor sentiment analysis and transaction data. *Cluster Computing*, *20*, pp.789-803.

Zhang, X., Zheng, X. and Zeng, D.D., 2017. The dynamic interdependence of international financial markets: An empirical study on twenty-seven stock markets. *Physica A: Statistical Mechanics and its Applications*, *472*, pp.32-42.

Zhou, P. and Zhang, Y., 2025. Major conundrums and possible solutions in DeFi insurance. *International Journal of Finance & Economics*.

Zięba, D., Kokoszczyński, R. and Śledziewska, K., 2019. Shock transmission in the cryptocurrency market. Is Bitcoin the most influential?. *International Review of Financial Analysis*, *64*, pp.102-125.

Zouaoui, M., Nouyrigat, G. and Beer, F., 2011. How does investor sentiment affect stock market crises? Evidence from panel data. *Financial review*, *46*(4), pp.723-747.

Zunino, L., Bariviera, A.F., Guercio, M.B., Martinez, L.B. and Rosso, O.A., 2012. On the efficiency of sovereign bond markets. *Physica A: Statistical Mechanics and its Applications*, *391*(18), pp.4342-4349.

Zunino, L., Tabak, B.M., Serinaldi, F., Zanin, M., Pérez, D.G. and Rosso, O.A., 2011. Commodity predictability analysis with a permutation information theory approach. *Physica A: statistical mechanics and its applications*, *390*(5), pp.876-890.

Zunino, L., Zanin, M., Tabak, B.M., Pérez, D.G. and Rosso, O.A., 2009. Forbidden patterns, permutation entropy and stock market inefficiency. *Physica A: Statistical Mechanics and its Applications*, *388*(14), pp.2854-2864.

Zunino, L., Zanin, M., Tabak, B.M., Pérez, D.G. and Rosso, O.A., 2010. Complexity-entropy causality plane: A useful approach to quantify the stock market inefficiency. *Physica A: Statistical Mechanics and its Applications*, *389*(9), pp.1891-1901.