ISSN 0974-763X
UGC-CARE Listed Journal

# SOUTH ASIAN JOURNAL OF MANAGEMENT RESEARCH (SAJMR)

Volume 15, Issue No.1 January, 2025

## CHHATRAPATI SHAHU INSTITUTE OF BUSINESS EDUCATION AND RESEARCH (CSIBER), KOLHAPUR, MAHARASHTRA, INDIA

(An Autonomous Institute)
University Road, Kolhapur - 416004, Maharashtra State, India.

website : www.siberindia.edu.in
E-mail : editorsajmr@siberindia.edu.in

# Chhatrapati Shahu Institute of Business Education and Research (CSIBER)

# South Asian Journal of Management Research (SAJMR)

**Volume 15, Issue No. 1, January, 2025**

**Editor: Dr. Pooja M. Patil**

**Publisher**

**CSIBER Press**

**Central Library**

Chhatrapati Shahu Institute of
Business Education & Research (CSIBER)
University Road, Kolhapur – 416004, Maharashtra, India.
Phone: 91-231-2535706/07, Fax: 91-231-2535708,
Website: www.siberindia.edu.in
Email: csiberpress@siberindia.edu.in
Editor Email: editorsajmr@siberindia.edu.in

**Address:**
**CSIBER Press**
Central Library Building
Chhatrapati Shahu Institute of Business Education and Research (CSIBER),
University Road Kolhapur, Maharashtra - 416004, India.



**ISSN: 0974-763X**

**Price: INR ₹ 1,200/-**

**Editor: Dr. Pooja M. Patil**

**Distributed By**

**CSIBER Press**

**Central Library**

Chhatrapati Shahu Institute of
Business Education & Research (CSIBER)
University Road, Kolhapur – 416004, Maharashtra, India.
Phone: 91-231-2535706/07, Fax: 91-231-2535708,
Website: www.siberindia.edu.in
Email: csiberpress@siberindia.edu.in

# Influence of News and Different Hacking Events on Bitcoin and Ethereum using Garch Models

**Dr. Parminder Singh**
Assistant Professor,
Department of Commerce, Akal University,
Talwandi Sabo, Bathinda, Punjab, India

**Mrs. Megha Rewal**
Research Scholar,
Department of Commerce, Akal University,
Talwandi Sabo, Bathinda, Punjab, India

**Abstract**

Millions of bitcoins were stolen during August 2018 to September 2023. The societal impact of criminal activity in the cryptocurrency market is exemplified by the fact that with the average Bitcoin price standing at $7,572 in 2018, the monetary losses amounted to a substantial $8.9 billion. This study underscores the substantial impact of hacking events on cryptocurrency returns, notably highlighting the pronounced influence on Bitcoin. The study tested that there is a significant difference between the effect of good news and bad news on the point of bitcoin and Ethereum. Upon investigating how hacking incidents impact the uncertainty of Bitcoin and Ethereum returns. The findings of the study reveal two distinct responses following a hacking incident at day t = 1, there is an immediate increase in volatility. However, this heightened volatility is not a short-lived effect; it resurfaces once again at day t + 3. Moreover, there is also an effect of hacking incidents within Bitcoin and Ethereum market with a time lag of three days.

**Keywords:** Cryptocurrency, Bitcoin, Ethereum, Volatility.

## Introduction

The rise of cryptocurrencies has illuminated a crucial concern. The implications of security breaches, notably the escalating instances of hacking. This study delves into the profound societal implications stemming from criminal activities within the cryptocurrency market. It aims to unravel the intricate relationship between these breaches and the consequential shifts in market dynamics, contextualized against transformative cryptocurrencies like Bitcoin and Ethereum, lauded for their decentralized and secure transactional frameworks. However, between August 2018 and September 2023, a notable surge in cyber-attacks underscored the urgent need to comprehend the profound impact of these breaches. This urgency becomes evident when considering the theft of substantial Bitcoin reserves, amounting to staggering financial losses estimated at approximately $8.9 billion based on the average 2018 Bitcoin price of $7,572. This context underscores the pressing necessity to thoroughly comprehend the multifaceted effects of hacking incidents on the cryptocurrency market. This research aims to precisely explore the nuanced repercussions stemming from both positive and negative news events concerning the valuation of Bitcoin and Ethereum. It endeavors to discern potential divergences in market dynamics between these leading cryptocurrencies. Additionally, it seeks to delve into the specific contributions of hacking events towards the uncertainty and volatility of returns for Bitcoin and Ethereum, placing a keen emphasis on understanding the temporal intricacies of market responses following such events.

Previous studies have typically highlighted immediate spikes in volatility post-security breaches. However, this study aspires to uncover any potential delayed or prolonged effects. Utilizing GARCH models, the research endeavors to precisely quantify the temporal impact of hacking events on the volatility of returns for Bitcoin and Ethereum. This nuanced understanding assumes pivotal importance in deciphering the underlying market dynamics and inherent risk factors within the continually evolving realm of digital assets.

The inception of cryptocurrencies marked a significant departure from traditional financial systems, introducing decentralized digital currencies powered by blockchain technology. Bitcoin, the trailblazing cryptocurrency that emerged in 2009, offered a decentralized system for peer-to-peer transactions secured by cryptographic protocols. Subsequently, Ethereum, introduced in 2015, expanded the capabilities of blockchain by enabling smart contracts and decentralized applications, further diversifying the cryptocurrency landscape. The inherent features of Bitcoin and Ethereum have positioned them at the forefront of the cryptocurrency revolution. Their decentralized nature, cryptographic security, and transparent transactional protocols have garnered widespread attention and investment interest, propelling them into the limelight of global financial markets. However, among their sudden rise, the cryptocurrency market has grappled with persistent challenges, notably security vulnerabilities. The period between August 2018 and September 2023 witnessed a distressing surge in cyber-attacks targeting cryptocurrency exchanges, wallets, and trading platforms. These breaches resulted in substantial financial losses, estimated at approximately $8.9 billion in stolen Bitcoin reserves based on the average Bitcoin price in 2018. Such incidents underscored the vulnerability of digital assets to malicious activities and raised profound concerns about their security and stability within financial ecosystems. The

impact of these security breaches extended beyond financial losses, permeating societal and market dynamics. Investor confidence wavered, regulatory scrutiny intensified, and market volatility surged in the wake of these events. Understanding the nuanced effects of these incidents on the valuation and volatility of Bitcoin and Ethereum holds paramount significance in navigating the intricate landscape of cryptocurrency markets.

Moreover, the research aims to unravel the intricate relationship between hacking events and the volatility of returns for Bitcoin and Ethereum. Prior studies have often highlighted immediate spikes in market volatility post-security breaches. However, this study endeavors to comprehensively explore the temporal dimensions of market responses, aiming to uncover any delayed or prolonged effects stemming from these incidents. Leveraging GARCH models enables a granular examination of volatility patterns and temporal dynamics following hacking events, facilitating a nuanced understanding of the unique market reactions of Bitcoin and Ethereum.

T-GARCH and E-GARCH models used to check whether there is an impact of the incidents on the variables or not. T-GARCH tested that whether there is an impact of any news which can affect the returns- the coins of the cryptocurrency market in this study. The significant results of T- GARCH relates the impact of both the news (whether it is positive or negative) for the further proceedings to the E-GARCH model for calculating the overall impact of the news. This study noted the hacking events (negative news) in the cryptocurrency market for both the investors and the market by taking these days as a dummy for the further analysis.

Comprehending the temporal implications of hacking incidents on cryptocurrency market dynamics are essential in comprehensively assessing associated risks and uncertainties. While immediate volatility spikes may be evident, scrutinizing the prolonged effects and their duration becomes imperative to gauge the resilience and adaptability of Bitcoin and Ethereum within the evolving landscape of digital assets.

GARCH models, renowned for their efficacy in capturing volatility patterns and conditional variance in financial time series data, form the backbone of this research. By employing these sophisticated econometric tools, this study aims to quantify and analyze the temporal impacts of hacking events on the volatility of returns for Bitcoin and Ethereum. This detailed analysis will provide deeper insights into the temporal intricacies of market responses, aiding in comprehending the dynamic relationships between hacking incidents and cryptocurrency market dynamics.

**Literature Review**

The expanding realm of cryptocurrency has reaped a significant attention across various studies, each shedding light on distinct facets of this rapidly evolving landscape.

Manahov, V. (2024) noted a sudden and drastic downturn in the cryptocurrency market led to a sharp decline in 95 out of the top 100 digital currencies due to market crash in 2018. The behavior of the more prominent cryptocurrencies, particularly Bitcoin, was pivotal in triggering the market crash. Moreover, the smaller cryptocurrencies tended to follow the lead of their larger counterparts, exacerbating the downward spiral.

Yu-Lun, Chen. et.al (2023) analysed that cryptocurrency hacking is a significant issue that has been affecting the development and price dynamics of cryptocurrencies such as Bitcoin. Hacking incidents and the theft of funds have been found to decrease the returns and increase the volatility of bitcoin spot and futures.

Chawki, M. (2022) examined the link between cybercrime and cryptocurrency regulation. The study highlighted the challenges posed by cybercriminal activities in the realm of digital assets and suggests regulatory strategies to counter these issues. Additionally, it focused on the role of technological solutions in tracking illicit activities. By offering actionable recommendations, the study aims to bolster regulatory frameworks, creating a more secure environment while fostering responsible innovation in the cryptocurrency space.

Ferri (2022) found that hacking attacks have a significant and persistent impact on the volatility of cryptocurrency markets, but the impact varies depending on the size and reputation of the exchange that is hacked. Larger and more reputable exchanges tend to experience a smaller and less persistent impact on volatility.

Chawki (2022) discussed the relationship between cybercrime and cryptocurrencies, and the challenges that law enforcement and regulators face in addressing this issue. The author argues that a balanced approach is needed, focusing on targeting criminal activity while not stifling innovation in the cryptocurrency sector.

Grobys, K. (2021) discussed the vulnerabilities and uncertainties present in the cryptocurrency market, with a specific focus on the security of block chain technology and the occurrence of hacking incidents. It delves into the potential risks associated with these factors and their implications for the cryptocurrency market.

Corbet, S et.al. (2020) investigated the implications of cybercriminal involvement in cryptocurrency, emphasizing its potential to disrupt the economic landscape. The research delves into the destabilizing effects such activities may have on financial systems and their consequential impact on the broader economy.

Makarov and Schoar (2020) explored the dynamics of cryptocurrency prices and the existence of arbitrage opportunities in these markets. Additionally, it analysed the trading strategies utilized by market participants and the influence of these strategies on market efficiency. By providing insights into the functioning of cryptocurrency markets, this research sheds light on the significance of trading and arbitrage in these markets.

Kethineni and Cao (2020) investigated the growing popularity of cryptocurrency and its correlation with criminal activities. Different types of criminal behavior associated with cryptocurrency- money laundering, fraud, and illicit transactions are explored. Difficulties faced by law enforcement agencies when investigating and prosecuting cryptocurrency-related crimes. By providing valuable insights into the relationship between cryptocurrency and criminal activity, this study emphasizes the importance of implementing effective regulatory measures in this emerging field.

Twomey and Mann (2020) argued that cryptocurrency markets are particularly vulnerable to fraud and manipulation due to lack of regulation, anonymity, and complexity. They identify a number of specific types of fraud and manipulation that are common in these markets, including pump-and-dump schemes, wash trading, spoofing, hacking, and exit scams. The activities pose a significant threat to the integrity of cryptocurrency markets and call for greater regulation and investor education.

Mauro et.al (2018) examined Bitcoin's security and privacy aspects, different components, vulnerabilities, and existing solutions. It covered the system's structure, including block chain and the PoW consensus protocol, while highlighting potential security threats. Additionally, it assesses current security solutions, addresses anonymity concerns, and suggests future research directions for enhancing bitcoin's security and privacy measures.

Tony Klein (2018) found that bitcoin and gold possess distinct asset properties and relationships with equity markets. Unlike gold, Bitcoin exhibits an inverse correlation, rising when markets decline. Gold serves as a haven in financial turmoil, while bitcoin lacks consistent hedging qualities in portfolios. Bitcoin, as a part of the broader cryptocurrency index CRIX, doesn't offer stable hedging capabilities similar to Gold, apart from a unique response in variance during market fluctuations.

Katsiampa, P. (2017) examined the Bitcoin's volatility using different GARCH models with a comparative analysis to assess their performance in capturing the volatility of Bitcoin. The findings of this research offer valuable insights into the volatility dynamics of Bitcoin and shed light on the effectiveness of different GARCH models in accurately measuring its volatility.

Bouoiyour and Selmi (2016) delved into the potential of Bitcoin as a significant milestone in the evolution of digital currencies. The study thoroughly analyzed the characteristics and implications of Bitcoin, such as its decentralized nature, security features, and potential effects on traditional financial systems. The findings offer valuable insights into the opportunities and challenges that come with the adoption and development of Bitcoin as a novel form of currency.

David, Yermack (2014) observed the gold standard tied to convertibility that declined from 1920s to 1970s due to factors like financing wars and limited gold production. Fiat currencies, dependent on public trust in government or central bank control, emerged after this collapse in most major economies. Bitcoin aims to address the shortcomings of both gold-backed and fiat currencies by positioning itself as an "algorithmic currency" with a predictable supply and growth controlled by cryptographic rules.

This study builds upon the existing literature by examining the impact of hacking events on cryptocurrency returns, particularly focusing on Bitcoin and Ethereum. Previous research primarily highlighted the negative effects of hacking incidents on investor confidence and market stability (e.g., Böhme et al., 2015; Catalini & Gans, 2016). However, contrary to these findings, this study reveals a positive correlation between hacking events and cryptocurrency returns, suggesting that investors may view hacks as an opportunity to hedge against future risks by increasing their investments in Bitcoin and Ethereum. This finding extends the literature by presenting a different perspective on investors' behavior during security breaches, showing that such events may not always lead to market downturns. The results offer valuable insights into how market participants react to perceived risks and contribute to the understanding of short-term market dynamics in the cryptocurrency market.

**Objectives of the Study**

- To study the impact of hacking events on Cryptocurrency returns.
- To evaluate market flexibility and implications of hacking incidents.
- To assess the influence of market attitude and volatility on Cryptocurrency returns.

**Data and Methodology**

The research conducted is based solely on data obtained from secondary sources spanning the timeline from April 2019 to March 2024. The primary source of information regarding cryptocurrency coins is derived from Coinmarket.com, a reputable platform known for providing comprehensive data and insights into various cryptocurrencies' market performance. This data includes a wide array of information such as daily returns, trading volumes, market capitalization, and other relevant metrics associated with different cryptocurrencies during the specified period. For the aspect related to hacking events in the cryptocurrency domain, the data is sourced from chainsec.io/exchange-hacks, a platform specifically dedicated to documenting and cataloguing cryptocurrency exchange breaches or hacking incidents. Only incidents that have well-documented dates and precise information regarding the amounts compromised within the specified timeframe of the study are

incorporated into the analysis. The focus is on analyzing and including hacking events that occurred within the stipulated period, ensuring a thorough and precise examination of these occurrences and their potential impact on the cryptocurrency market.

The research methodology relies on the consolidation and rigorous examination of these datasets, carefully selecting and utilizing information that meets the study's criteria for accuracy, reliability, and relevance. By exclusively considering verified and well-documented hacking events alongside cryptocurrency market data from reputable sources, the study aims to provide a comprehensive and credible analysis of the relationship between hacking incidents and cryptocurrency returns within the specified timeframe.

**Analysis and Interpretation**

**Table 1- Descriptive Statistics of Bitcoin Return with Hack and Hack+3 Days**

| | $BTC_{RETURN}$ | $BTC_{HACK\ DAY}$ | $BTC_{H+3}$ |
|---|---|---|---|
| **Mean** | 0.0015 | 0.0000 | 0.0002 |
| **Median** | 0.0008 | 0.0000 | 0.0000 |
| **Maximum** | 0.1722 | 0.0454 | 0.1603 |
| **Minimum** | -0.4650 | -0.1519 | -0.1519 |
| **Std. Dev.** | 0.0358 | 0.0043 | 0.0075 |
| **Observations** | 1827 | 1827 | 1827 |

**Source**- Prepared by author in E-Views

$BTC_{RETURN}$ shows daily Bitcoin returns whereas $BTC_{HACK}$ and $BTC_{H+3}$ show Bitcoin returns for hack day and 3 days after the hack respectively by taking hack as a dummy (1 if there was a hack on that day, 0 otherwise). The table interprets that Bitcoin returns have averaged 0.15% per day. The median of hacks is 0.0000 and the minimum of $BTC_{HACK}$ is -0.1519 which indicates that that there have been more days with no hacks than days with hacks. The largest daily Bitcoin return has been 17.22%. The maximum $BTC_{HACK}$ is 0.0454, which means that there has only been one hack on a given day. The standard deviation of $BTC_{RETURN}$ is 0.0358, indicating that Bitcoin returns have been very volatile. The standard deviation of $BTC_{H+3}$ is 0.0075, which means that Bitcoin returns 3 days after a hack has been less volatile than daily Bitcoin returns. The standard deviation of $BTC_{HACK}$ is 0.0043, which means that the number of hacks per day has been relatively stable. Overall, the table shows that Bitcoin returns are very volatile. This means that Bitcoin investors should expect large swings in both $BTC_{HACK}$ and $BTC_{H+3}$

**Table 2- Descriptive Statistics of Ethereum Return with Hack and Hack+3 Days**

| | $ETH_{RETURN}$ | $ETH_{HACK}$ | $ETH_{H+3}$ |
|---|---|---|---|
| **Mean** | 0.0017 | 0.0001 | 0.0002 |
| **Median** | 0.0012 | 0.0000 | 0.0000 |
| **Maximum** | 0.2307 | 0.0528 | 0.1449 |
| **Minimum** | -0.5500 | -0.1355 | -0.1683 |
| **Std. Dev.** | 0.0451 | 0.0041 | 0.0082 |
| **Observations** | 1827 | 1827 | 1827 |

**Source-** Prepared by author in E-Views

Ethereum (ETH) exhibits notable volatility and unpredictability in its daily returns, portraying significant fluctuations within its market performance. On average, the daily return for Ethereum stands at 0.17%. However, the standard deviation, calculated at 0.0451, indicates a substantial likelihood of extreme returns, highlighting the inherent volatility within ETH's market behavior. This volatility suggests that Ethereum's value experiences significant shifts, making it susceptible to rapid and sizable price movements. The standard deviation of 0.0041 emphasizes the unpredictability of these events. Specifically, Ethereum tends to experience negative returns on the day of a hack and in the subsequent three days. The average return on the day of the hack is notably lower at -0.1683%, followed by an average return of -0.1355% in the three days following the hack. This consistent pattern suggests that hacking incidents significantly impact Ethereum's short-term performance, resulting in decreased returns immediately post-hack and persisting negativity for a short period thereafter. Overall, these findings underline Ethereum's susceptibility to extreme market movements, coupled with its vulnerability to the effects of hacking incidents. The negative impact of hacks on short-term returns indicates the market's sensitivity to such security breaches, emphasizing the need for vigilant monitoring and strategic measures to mitigate the adverse effects on Ethereum's value and investor confidence.

**Table 3- Unit Root test for Bitcoin and Ethereum Returns**

| Unit Root Test | | |
|---|---|---|
| **Augmented Dickey-Fuller test statistic** | | |
| | **t-statistic** | **Prob.** |
| **Bitcoin** | -44.9670 | 0.0001 |
| **Ethereum** | -45.6862 | 0.0001 |

**Source**- Prepared by author in E-Views

Both Bitcoin and Ethereum hold considerable significance at a statistical level. The t-statistics for Bitcoin and Ethereum, standing at -44.9670 and -45.6862 respectively, coupled with their low p-values of 0.0001, strongly reject the null hypothesis of a unit root within their time series data. This rejection indicates that both Bitcoin's and Ethereum's data exhibit stationarity, implying a lack of a unit root in their price movements. This absence of a unit root suggests that Bitcoin and Ethereum showcase more volatility and unpredictability compared to stationary time series data. Additionally, the findings imply that conventional technical analysis tools, which often rely on the assumption of stationarity, may not be as effective in accurately predicting future price movements for Bitcoin and Ethereum due to their non-stationary nature. Therefore, their distinct behavior challenges the efficacy of traditional analytical tools typically applied in financial markets.

**Table 4 – List of Hacking Events**

| Date | Amount stolen | Exchange |
|---|---|---|
| **01-04-2019** | 1,30,00,000 | Bithumb |
| **27-06-2019** | 42,00,000 | Bitrue |
| **12-07-2019** | 3,20,00,000 | BITPoint |
| **27-11-2019** | 4,90,00,000 | Upbit |
| **06-02-2020** | 73,000 | Altsbit |
| **08-09-2020** | 54,00,000 | Eterbase |
| **26-09-2020** | 28,00,00,000 | KuCoin |
| **01-02-2021** | 45,000 | Cryptopia |
| **19-08-2021** | 8,00,00,000 | Liquid |
| **05-12-2021** | 15,00,00,000 | BitMart |
| **11-12-2021** | 7,80,00,000 | AscendEX |
| **09-01-2022** | 68,00,000 | LCX |
| **01-11-2022** | 2,80,00,000 | Deribit |
| **10-04-2023** | 1,30,00,000 | GDAC |

**Source**- https://chainsec.io/exchange-hacks

To date, the cryptocurrency industry has experienced 55 significant hacking incidents, resulting in cumulative losses of approximately $2.4 billion. The most devastating breach occurred in 2014, when Mt.Gox suffered a massive hack, leading to the theft of $661,348,000, which remains the largest single loss. These security breaches have resulted in substantial financial losses, highlighting the ongoing challenges and vulnerabilities in the digital currency space. The table 4 catalogues 14 cryptocurrency exchange hacks spanning from 2019 to 2024, delineating the date, stolen amount, and targeted exchange. Notably, the majority of these substantial breaches have predominantly focused on exchanges based in Asia, likely attributed to the region's significant position as a cryptocurrency trading hub. The collective value pilfered in these hacking incidents surpasses a staggering $1 billion. Among these breaches, the largest occurred during the KuCoin hack in September 2020, resulting in a staggering $280 million theft, while the smallest breach transpired during the Cryptopia hack in February 2021, amounting to $45,000 in losses. The table underscores a consistent rise in both the frequency and magnitude of cryptocurrency exchange hacks in recent years. This escalating trend is presumed to be a consequence of the surging popularity of cryptocurrencies coupled with the increasing valuation of digital assets. Cryptocurrency exchanges, being reservoirs of substantial digital wealth, become prime targets for hackers seeking unauthorized access. The fallout from a cryptocurrency exchange hack reverberates significantly for investors who bear the brunt of such incidents, facing the perilous loss of their digital assets. These breaches not only result in immediate financial losses but also inflict a substantial shock to investor confidence within the cryptocurrency industry, increasing the far-reaching impacts of these cybercrimes.

$$BTC_{RETURN} = \beta_0 + \beta_1 * BTC_{HACK} + \varepsilon \quad (1)$$

Where,

$BTC_{RETURN}$ is the dependent variable (the return of Bitcoin)
$BTC_{HACK}$ is the independent variable (a binary variable that is 1 if there was a Bitcoin hack on that day and 0 otherwise)
$\beta_0$ is the intercept
$\beta_1$ is the slope coefficient
$\varepsilon$ is the error term
The equation represents a simple linear regression model used to examine the impact of Bitcoin hacking events ($BTC_{HACK}$) on Bitcoin returns ($BTC_{RETURN}$). $BTC_{RETURN}$ serves as the dependent variable, indicating the return on Bitcoin, while $BTC_{HACK}$ acts as the independent variable, taking a binary form (1 for a day with a Bitcoin hack and 0 otherwise). The coefficient $\beta_1$ quantifies the relationship between Bitcoin returns and hacking events, elucidating the change in returns associated with a unit change in $BTC_{HACK}$. The intercept $\beta_0$ signifies the expected Bitcoin return in the absence of hacking events. The model aims to understand how Bitcoin returns are influenced by the occurrence of Bitcoin hacks, offering insights into the potential impact of hacking incidents on Bitcoin's financial performance.

$$\mathbf{BTC_{RETURN} = \beta_0 + \beta_1 * BTC_{H+3} + \varepsilon} \quad \textbf{(2)}$$

Where,
$BTC_{RETURN}$ is the dependent variable (the return of Bitcoin)
$BTC_{H+3}$ is the independent variable (a binary variable that is 1 if there was a Bitcoin hack in the past 3 days and 0 otherwise)
$\beta_0$ is the intercept
$\beta_1$ is the slope coefficient
$\varepsilon$ is the error term
The equation provided represents a linear regression model aimed at examining the relationship between Bitcoin returns ($BTC_{RETURN}$) and the occurrence of Bitcoin hacks within a three-day window ($BTC_{H+3}$). $BTC_{RETURN}$ stands as the dependent variable, representing the return on Bitcoin. $BTC_{H+3}$ functions as the independent variable, taking on a binary form (1 if a Bitcoin hack occurred within the past three days, and 0 otherwise). The coefficient $\beta_1$ quantifies the impact of Bitcoin hacking events within this three-day period on Bitcoin returns, illustrating the change in returns associated with the presence of a recent hacking incident. The intercept $\beta_0$ signifies the expected Bitcoin return when there have been no hacking events in the past three days. This model seeks to elucidate how Bitcoin returns are influenced by the occurrence of Bitcoin hacks within this defined temporal window, providing insights into the potential short-term impact of recent hacking incidents on Bitcoin's financial performance.

**Table 5 – Regression of Bitcoin Return with Hackings**

| Variable | Coefficient | Std. Error | t-Statistic | Prob. |
|---|---|---|---|---|
| $BTC_{RETURN}$ | 0.0015 | 0.0008 | 1.7795 | 0.0753 |
| $BTC_{HACK}$ | 0.9966 | 0.1951 | 5.1083 | 0.0000 |
| | | | | |
| **Variable** | **Coefficient** | **Std. Error** | **t-Statistic** | **Prob.** |
| $BTC_{RETURN}$ | 0.0013 | 0.0008 | 1.6021 | 0.1093 |
| $BTC_{H+3}$ | 0.9951 | 0.1098 | 9.0644 | 0.0000 |

**Source-** Prepared by author in E-Views

The conducted regression analysis aimed to evaluate the effect of hacking events on Bitcoin returns. The model integrated dummy variables representing both the day of the hack and the subsequent three days following the event. The coefficients within the table interpret the influence of each variable on Bitcoin returns. For instance, the coefficient attributed to $BTC_{Hack}$ stands at 0.9966, indicating that a Bitcoin hack event correlates with a noteworthy 0.9966 increase in Bitcoin returns. This impact holds significant statistical relevance, evident from the p-value of 0.0000. Conversely, the coefficient associated with Bitcoin Return (3 days after hack) is 0.0013, signifying that Bitcoin returns on the hack day slightly influence a mere 0.0013 increase in returns three days later. This influence lacks statistical significance, as indicated by the p-value of 0.1093. Collectively, the outcomes derived from the regression analysis suggest a positive impact of Bitcoin hacks on Bitcoin returns. The findings underscore the intricate relationship between hacking events and the market dynamics of Bitcoin, unveiling a notable shift in investor behavior in response to security vulnerabilities within the cryptocurrency landscape.

$$\mathbf{ETH_{RETURN} = \beta_0 + \beta_1 * ETH_{HACK} + \varepsilon} \quad \textbf{(3)}$$

Where,
$ETH_{RETURN}$ is the dependent variable (the return of Ethereum)
$ETH_{HACK}$ is the independent

$\beta_0$ is the intercept
$\beta_1$ is the slope coefficient
$\varepsilon$ is the error term
The equation presented represents a linear regression model investigating the relationship between Ethereum returns ($ETH_{RETURN}$) and the occurrence of Ethereum hacking events ($ETH_{HACK}$). In this context, $ETH_{RETURN}$ serves as the dependent variable, signifying the return on Ethereum, while $ETH_{HACK}$ operates as the independent variable, taking on a binary form (1 denoting the presence of a hacking event and 0 otherwise). The coefficient $\beta_1$ encapsulates the impact of Ethereum hacking incidents on Ethereum returns, depicting the change in returns associated with the occurrence of a hacking event. The intercept $\beta_0$ symbolizes the expected Ethereum return when there are no hacking events. This model aims to unveil how Ethereum returns are affected by the presence or absence of hacking incidents, providing insights into the potential influence of such events on Ethereum's financial performance.

$$\mathbf{ETH_{RETURN} = \beta_0 + \beta_1 * ETH_{H+3} + \varepsilon} \quad \textbf{(4)}$$

Where,
$ETH_{RETURN}$ is the dependent variable (the return of Ethereum)
$ETH_{H+3}$ is the independent variable
$\beta_0$ is the intercept
$\beta_1$ is the slope coefficient
$\varepsilon$ is the error term
The provided equation constitutes a linear regression model exploring the relationship between Ethereum returns ($ETH_{RETURN}$) and the occurrence of Ethereum hacking events within a three-day timeframe ($ETH_{H+3}$). In this context, $ETH_{RETURN}$ signifies the dependent variable, representing the return on Ethereum, while $ETH_{H+3}$ serves as the independent variable, taking a binary form (1 if a hacking event occurred within the past three days, and 0 otherwise). The coefficient $\beta_1$ characterizes the impact of Ethereum hacking events within this three-day period on Ethereum returns, highlighting the change in returns associated with recent hacking incidents. The intercept $\beta_0$ represents the anticipated Ethereum return when there have been no hacking events within the specified timeframe. This regression model seeks to unveil how Ethereum returns are influenced by the occurrence of recent hacking events, shedding light on the potential short-term impact of these incidents on Ethereum's financial performance.

**Table 6 – Regression of Ethereum Return with Hackings**

| Variable | Coefficient | Std. Error | t-Statistic | Prob. |
|---|---|---|---|---|
| $\mathbf{ETH_{RETURN}}$ | 0.0017 | 0.0011 | 1.5859 | 0.1129 |
| $\mathbf{ETH_{HACK}}$ | 0.9946 | 0.2588 | 3.8434 | 0.0001 |
| | | | | |
| **Variable** | **Coefficient** | **Std. Error** | **t-Statistic** | **Prob.** |
| $\mathbf{ETH_{RETURN}}$ | 0.0015 | 0.0010 | 1.4612 | 0.1441 |
| $\mathbf{ETH_{H+3}}$ | 0.9954 | 0.1263 | 7.8785 | 0.0000 |

**Source-** Prepared by author in E-Views

A regression analysis was performed to examine the impact of hacking days on Ethereum returns. The model included dummy variables for the day of the hack and the three days following the hack. . The coefficient for $ETH_{HACK}$ is 0.9946, which is statistically significant (p-value = 0.0001). This means that a hack event is associated with a 0.9946 increase in Ethereum returns on the day of the hack. The coefficient for $ETH_{H+3}$ is also statistically significant (p-value = 0), meaning that a hack event is associated with a 0.9954 increase in Ethereum returns on the three days following the hack. Overall the results of the regression analysis show that both the day of the hack and the three days following the hack have a statistically significant impact on Ethereum price returns. In other words, hacking events can have a negative impact on Ethereum prices. This is likely because hacking events erode investor confidence in the security of the Ethereum network. In short, the table suggests that hacking events have a statistically significant negative impact on Ethereum price returns.

In a nutshell, both Bitcoin and Ethereum hacks have a positive and statistically significant impact on their respective cryptocurrency returns, both on the day of the hack and 3 days later. This suggests that investors seek to hedge their bets against future hacks by buying more Bitcoin and Ethereum after a hack. It is important to note that these are just observational studies, and they cannot prove that cryptocurrency hacks cause cryptocurrency prices to increase. However, the results do suggest that there is a strong correlation between cryptocurrency hacks and cryptocurrency price movements.

$$\mathbf{BTC_{RETURNt} = \mu + \alpha(BTC_{RETURNt-1}) + \beta(BTC_{RETURNt-2}) + \varepsilon_t} \quad \textbf{(5)}$$

$$\mathbf{\sigma^2_t = \omega + \alpha\varepsilon^2_t + \beta\sigma^2_{t-1}} \quad \textbf{(6)}$$

Equation (5) is for the ARIMA and Equation (6) is for Garch Where,
$BTC_{RETURNt}$ is the Bitcoin return at time t
$\mu$ is the constant term

α is the AR(1) coefficient
β is the AR(2) coefficient
$\varepsilon_t$ is the white noise error term, which is assumed to follow a Student's t-distribution with ν degrees of freedom
$\sigma^2_t$ is the conditional variance of the Bitcoin return at time t
ω is the constant term in the GARCH equation
Equation (5) outlines an Autoregressive Integrated Moving Average (ARIMA) model that predicts Bitcoin returns at time't'. This model incorporates the Bitcoin returns from the previous two days,'t-1' ($BTC_{RETURNt-1}$) and't-2' ($BTC_{RETURNt-2}$), denoted as α and β, respectively. Additionally, it includes a constant term (μ) and an error term ($\varepsilon_t$) following a Student's t-distribution with degrees of freedom (ν). This predictive model aims to capture and utilize past returns to forecast the current return for Bitcoin, utilizing a combination of autoregressive and moving average components.
Equation (6) delineates a Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model for the conditional variance ($\sigma^2_t$) of Bitcoin returns at time't'. This model incorporates a constant term (ω) and factors in the conditional variance based on the preceding variance ($\sigma^2_{t-1}$) and the squared error term derived from the ARIMA model. This GARCH model accounts for the volatility clustering observed in Bitcoin returns, acknowledging that past variances and squared errors impact the current volatility, thus illustrating how volatility tends to persist in the cryptocurrency's returns over time.

**Table 7 – TGARCH on Bitcoin Returns**

| | **Coefficient** | **Std. Error** | **z-Statistic** | **Prob.** |
|---|---|---|---|---|
| **$BTC_{RETURN}$** | 0.0015 | 0.0008 | 1.7761 | 0.0757 |
| **AR(2)** | -0.0489 | 0.4106 | -0.1190 | 0.9053 |
| **MA(2)** | 0.0929 | 0.4092 | 0.2271 | 0.8204 |
| **Variance Equation** | | | | |
| **$BTC_{RETURN}$** | 0.0001 | 0.0000 | 9.0123 | 0.0000 |
| **$RESID(-1)^2$** | 0.0837 | 0.0137 | 6.1256 | 0.0000 |
| **$RESID(-1)^2$*(RESID(-1)<0)** | 0.1285 | 0.0137 | 9.3809 | 0.0000 |
| **GARCH(-1)** | 0.8022 | 0.0157 | 51.0269 | 0.0000 |

**Source-** Prepared by author in E-Views
The table shows the results of a GARCH(1,1) model fitted to the daily returns of Bitcoin. The coefficients in the ARIMA section of the table represent the impact of past Bitcoin returns ($BTC_{RETURN}$), second-order autocorrelation (AR(2)), and second-order moving average (MA(2)) on current Bitcoin returns. The coefficients in the GARCH section of the table represent the impact of past squared Bitcoin returns ($BTC_{RETURN}^2$), past volatility ($RESID(-1)^2$), and past leverage effect ($RESID(-1)^2$*(RESID(-1)<0)) on current volatility. The AR(2) and MA(2) coefficients are not significant, indicating that there is no evidence of second-order autocorrelation or moving average in Bitcoin returns. The $(BTC\ RETURN)^2$, $RESID(-1)^2$, and $RESID(-1)^2$*(RESID(-1)<0) coefficients are all significant, indicating that past squared Bitcoin returns, past volatility, and the past leverage effect all have a positive impact on current volatility. The value 0.1285 indicates that any news rather it is bad or good, it can effect the prices of the Bitcoin returns.

$$\mathbf{ETH_{RETURNt} = \mu + \alpha(ETH_{RETURNt-1}) + \beta(ETH_{RETURNt-2}) + \varepsilon_t} \quad \mathbf{(7)}$$

$$\mathbf{\sigma^2_t = \omega + \alpha\,(ETH_{RETURNt-1})^2 + \beta\sigma^2_{t-1} + \gamma\varepsilon^2_t} \quad \mathbf{(8)}$$

Equation (1) is for the ARIMA and Equation (2) is for Garch where,
$ETH_{RETURNt}$ is the Ethereum return at time t
μ is the constant term
α is the AR(1) coefficient
β is the AR(2) coefficient
$\varepsilon_t$ is the white noise error term
$\sigma^2_t$ is the conditional variance of the Ethereum return at time t
ω is the constant term in the GARCH equation
γ is the ARCH coefficient
Equation (7) outlines an Autoregressive Integrated Moving Average (ARIMA) model applied to Ethereum returns at time 't'. This model utilizes Ethereum returns from the prior two days, 't-1' ($ETH_{RETURNt-1}$) and 't-2' ($ETH_{RETURNt-2}$), represented as predictors (α and β respectively) influencing the current return. Alongside these predictors, the model includes a constant term (μ) and a white noise error term ($\varepsilon_t$). By incorporating past returns, the ARIMA model aims to forecast the current Ethereum return using a combination of autoregressive and moving average components.
Equation (8) delineates a Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model, illustrating the conditional variance ($\sigma^2_t$) of Ethereum returns at time 't'. This model involves a constant term (ω) and considers several factors: the previous variance ($\sigma^2_{t-1}$), the squared value of Ethereum returns at 't-1'

($\alpha(ETH_{RETURNt-1})^2$), and the squared error term ($\varepsilon^2_{t-1}$) weighted by a coefficient γ. The inclusion of these components addresses an Autoregressive Conditional Heteroskedasticity (ARCH) effect, signifying volatility clustering observed in Ethereum returns. This GARCH model provides insights into how past variances, squared returns, and error terms collectively contribute to understanding the current volatility dynamics within Ethereum's return framework.

**Table 8 - TGARCH on Ethereum Returns**

| | **Coefficient** | **Std. Error** | **z-Statistic** | **Prob.** |
|---|---|---|---|---|
| **$ETH_{RETURN}$** | 0.0018 | 0.0010 | 1.8110 | 0.0701 |
| **AR(2)** | -0.0593 | 0.2413 | -0.2457 | 0.8060 |
| **MA(2)** | 0.1103 | 0.2408 | 0.4580 | 0.6469 |
| **Variance Equation** | | | | |
| **$ETH_{RETURN}$** | 0.0001 | 0.0000 | 7.3421 | 0.0000 |
| **$RESID(-1)^2$** | 0.1043 | 0.0133 | 7.8451 | 0.0000 |
| **$RESID(-1)^2$*(RESID(-1)<0)** | 0.0260 | 0.0116 | 2.2448 | 0.0248 |
| **GARCH(-1)** | 0.8647 | 0.0106 | 81.4417 | 0.0000 |

**Source**- Prepared by author in E-Views

The $ETH_{RETURN}$ coefficient is significant, indicating that past Ethereum returns have a positive impact on current Ethereum returns. It means autocorrelation exists. The AR(2) coefficient is positive and significant, indicating that there is second-order autocorrelation in Ethereum returns. This means that the current return is positively correlated with the two previous returns. The MA(2) coefficient is negative and significant, indicating that there is a second-order moving average in Ethereum returns. This means that the current return is negatively correlated with the two previous moving averages of the returns. The $RESID(-1)^2$ coefficient is positive and significant, indicating that past volatility has a positive impact on current volatility. This is the GARCH effect. The $RESID(-1)^2$*(RESID(-1)<0) coefficient is positive and significant, indicating that there is a leverage effect in Ethereum returns. The value 0.0260 suggests that both positive and negative news can impact Ethereum returns.

The T-Garch model reveals that both Bitcoin and Ethereum returns are influenced by market news. However, to determine whether these returns are more affected by positive or negative news, the E-Garch model is employed. The E-Garch model captures the leverage effect of shocks, which means it assesses how market data responds to news, whether it's positive or negative. This model is an extension of the T-GARCH model, allowing for an asymmetric impact of positive and negative shocks on volatility.

The equation for the EGARCH model is as follows:

$$\ln(\sigma^2_t) = \omega + \alpha(\varepsilon^2_t - \gamma|\varepsilon_t|) + \beta \ln(\sigma^2_{t-1}) \quad (9)$$

where,

$\sigma^2_t$ is the conditional variance of the Bitcoin return at time t

ω is the constant term

α is the ARCH coefficient

$\varepsilon^2_t$ is the squared innovation at time t

γ is the leverage coefficient

β is the GARCH coefficient

Equation (9) presents a logarithmic transformation of the conditional variance ($\sigma^2_t$) of Bitcoin returns at time 't', formulated within a GARCH (Generalized Autoregressive Conditional Heteroskedasticity) model. This equation entails a constant term (ω) and incorporates the effect of squared innovations ($\varepsilon^2_t$) and the absolute value of innovations ($|\varepsilon_t|$) weighted by the leverage coefficient (γ) and ARCH coefficient (α) respectively. The GARCH coefficient (β) signifies the impact of the logarithm of the previous conditional variance ($\ln(\sigma^2_{t-1})$) on the current variance. This formulation aims to capture the time-varying volatility in Bitcoin returns by considering both squared and absolute innovations and their influence on the evolving conditional variance, offering insights into the clustering of volatility in Bitcoin returns over time.

**Table 9- E Garch on Bitcoin Returns**

| | **Coefficient** | **Std. Error** | **z-Statistic** | **Prob.** |
|---|---|---|---|---|
| **BTC RETURN** | 0.0015 | 0.0008 | 1.8675 | 0.0618 |
| **AR(2)** | -0.0657 | 0.4261 | -0.1541 | 0.8775 |
| **MA(2)** | 0.0643 | 0.4273 | 0.1505 | 0.8804 |

| Variance Equation | | | | |
|---|---|---|---|---|
| **C(4)** | -0.6911 | 0.0667 | -10.3684 | 0.0000 |
| **C(5)** | 0.2480 | 0.0216 | 11.4624 | 0.0000 |
| **C(6)** | -0.0722 | 0.0095 | -7.5891 | 0.0000 |
| **C(7)** | 0.9228 | 0.0085 | 108.1529 | 0.0000 |

Source- Prepared by author in E-Views

The model presents insightful coefficients for Bitcoin's returns and volatility. BTC $_{RETURN}$ coefficient signifies a marginal influence on Bitcoin returns. However, the autoregressive term (AR(2)) exhibits a substantial positive impact, indicating the significance of past returns on the current outcome. Conversely, the moving average term (MA(2)) shows a notable negative effect, suggesting a dampening effect on returns. Transitioning to the variance equation, coefficients C(4), C(5), and C(6) signify the impact of different news events on Bitcoin's volatility. C(4) and C(6) display negative coefficients, highlighting the stronger influence of adverse news, while C(5) portrays a positive impact. Notably, C(7) stands out with a significantly strong positive effect, pointing to a particular type of news strongly driving Bitcoin's volatility. Overall, the model underscores the interplay of past returns and diverse news factors in shaping both Bitcoin returns and its volatility.

$$\ln(\sigma^2_{t+1}) = \omega + \alpha(ETH_{RET}{}^2_t - \gamma|ETH_{RETt}|) + \beta \ln(\sigma^2_t) \quad (10)$$

where:

$\sigma^2_t$ is the conditional variance of the Ethereum return at time t

$\omega$ is the constant term

$\alpha$ is the ARCH coefficient

$ETH_{RET}{}^2_t$ is the squared Ethereum return at time t

$\gamma$ is the leverage coefficient

$\beta$ is the GARCH coefficient

Equation (10) represents a GARCH (Generalized Autoregressive Conditional Heteroskedasticity) model, featuring a logarithmic transformation of the conditional variance ($\sigma^2_{t+1}$) of Ethereum returns at time 't'. This equation incorporates various components to model the evolving variance: a constant term ($\omega$), the impact of squared Ethereum returns ($ETH_{RET}{}^2_t$) and the absolute value of Ethereum returns ($|ETH_{RETt}|$) weighted by the leverage coefficient ($\gamma$) and ARCH coefficient ($\alpha$) respectively, and the effect of the logarithm of the previous conditional variance ($\ln(\sigma^2_t)$) indicated by the GARCH coefficient ($\beta$). By considering both squared and absolute Ethereum returns, this model aims to capture and characterize the time-varying volatility in Ethereum returns, providing insights into the patterns of volatility clustering within the Ethereum market.

**Table 10- E Garch on Ethereum Returns**

| Variable | Coefficient | Std. Error | z-Statistic | Prob. |
|---|---|---|---|---|
| **$ETH_{RETURN}$** | 0.0017 | 0.0010 | 1.8091 | 0.0704 |
| **AR(2)** | -0.0527 | 0.2052 | -0.2568 | 0.7973 |
| **MA(2)** | 0.0913 | 0.2064 | 0.4424 | 0.6582 |
| **Variance Equation** | | | | |
| **C(4)** | -0.3504 | 0.0377 | -9.3068 | 0.0000 |
| **C(5)** | 0.2092 | 0.0169 | 12.3694 | 0.0000 |
| **C(6)** | -0.0240 | 0.0068 | -3.5063 | 0.0005 |
| **C(7)** | 0.9681 | 0.0045 | 215.8061 | 0.0000 |

**Source**- Prepared by author in E-Views

The provided model offers valuable insights into Ethereum's returns and volatility. ETH $_{RETURN}$ demonstrates a relatively modest impact on Ethereum's returns. However, the autoregressive (AR(2)) and moving average (MA(2)) terms indicate substantial influences. AR(2) suggests a noteworthy positive effect of past returns, while MA(2) reflects a significant negative impact on current returns. Transitioning to the variance equation, coefficients C(4), C(6), and C(7) illustrate the influence of various news events on Ethereum's volatility. Negative coefficients in C(4) and C(6) highlight the stronger impact of adverse news, whereas C(5) indicates a positive effect. Notably, C(7) stands out with a significantly strong positive impact, indicating a specific type of news strongly driving Ethereum's volatility. Overall, past returns and distinct news factors notably shape both Ethereum's returns and its volatility in this model.

The negative coefficient (C(6)) in both E-GARCH models for Bitcoin and Ethereum returns suggests a noteworthy influence of negative news compared to positive news on their returns. This implies that negative news events exert a more pronounced impact on the volatility of Bitcoin and Ethereum returns than positive

news. The model indicates that adverse or unfavorable news developments tend to have a stronger association with increased volatility in both cryptocurrencies, potentially prompting larger and more persistent market reactions compared to positive news events.

**Conclusion**

The study underscores the substantial impact of hacking events on cryptocurrency returns, notably highlighting the pronounced influence on Bitcoin. It stresses the necessity of acknowledging cryptocurrencies' asymmetric reactions to positive and negative news, outlining the complexities of forecasting their price movements due to inherent volatility and non-stationary behavior. The research outcomes indicate persistent and asymmetric volatility in Bitcoin and Ethereum returns. This implies that previous volatility positively influences current volatility, and negative shocks exert a more pronounced impact on volatility compared to positive shocks of similar magnitude. These findings shed light on the different dynamics of cryptocurrency markets, emphasizing the challenges associated with volatility forecasting and the significance of external events, like hacking incidents, in shaping their performance.

**Implication of the Study**

This study provides valuable insights for various stakeholders. Investors and traders can use the findings to refine strategies by understanding how news impacts Bitcoin and Ethereum prices. Policymakers can develop better regulations based on market behavior after hacking events, while cybersecurity experts can improve security measures for digital assets. Academically, the study deepens the understanding of cryptocurrency market responses to cyber-attacks. Overall, the research promotes public trust in cryptocurrency by showcasing market resilience and contributing to long-term stability.

**References**


**Ali, G. (2013).** EGARCH, GJR-GARCH, TGARCH, AVGARCH, NGARCH, IGARCH and APARCH models for pathogens at marine recreational sites. Journal of Statistical and Econometric Methods, 2(3), 57-73.

**Ausloos, M., Zhang, Y., & Dhesi, G. (2020).** Stock index futures trading impact on spot price volatility. The CSI 300 studied with a TGARCH model. Expert Systems with Applications, 160, 113688.

**Bouoiyour, J., & Selmi, R. (2016).** Bitcoin: A beginning of a new phase? Economic Bulletin, 36(3), 1430-1440.

**Caporale, G. M., Kang, W. Y., Spagnolo, F., & Spagnolo, N. (2023).** Cyber-Attacks, Cryptocurrencies and Cyber Security. In Economic and Financial Crime, Sustainability and Good Governance (pp. 347-381). Cham: Springer International Publishing.

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

**Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. (2019).** Investigating the dynamics between price volatility, price discovery, and criminality in cryptocurrency markets. Price Discovery, and Criminality in Cryptocurrency Markets (May 3, 2019).

**Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020).** The destabilising effects of cryptocurrency cybercriminality. Economics Letters, 191, 108741.

**David, Yermack. (2014).** Is Bitcoin a Real Currency? An Economic Appraisal. Social Science Research Network, doi: 10.2139/SSRN.2361599

**FERRI, R. (2022).** Modeling crypto's volatility after a hacking attack.

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

**Grobys, K. (2021).** When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market. Quantitative Finance, 21(8), 1267-1279.

**Harrell, F. E. (2017).** Regression modeling strategies. Bios, 330(2018), 14.

**Katsiampa, P. (2017).** Volatility estimation for Bitcoin: A comparison of GARCH models. Economics Letters, 158, 3-6.

**Kethineni, S., & Cao, Y. (2020).** The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325-344.

**Lawless, H. T., Heymann, H., Lawless, H. T., & Heymann, H. (2010).** Descriptive analysis. Sensory evaluation of food: Principles and practices, 227-257.

**Le Tran, V., & Leirvik, T. (2020).** Efficiency in the markets of crypto-currencies. Finance Research Letters, 35, 101382.

**Makarov, I., & Schoar, A. (2020).** Trading and arbitrage in cryptocurrency markets. Journal of Financial Economics, 135(2), 293-319.

**Manahov, V. (2024).** The great crypto crash in September 2018: why did the cryptocurrency market collapse?. Annals of Operations Research, 332(1), 579-616.

**Mauro, Conti., E., Sandeep, Kumar., Chhagan, Lal., Sushmita, Ruj. (2018).** A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys and Tutorials, 20(4):3416-3452. doi: 10.1109/COMST.2018.2842460

**Nunez, E., Steyerberg, E. W., & Nunez, J. (2011).** Regression modeling strategies. Revista Española de Cardiología (English Edition), 64(6), 501-507.

**Pham, H., Nguyen Thanh, B., Ramiah, V., & Moosa, N. (2022).** The effects of hacking events on bitcoin. Journal of Public Affairs, 22, e2744.

**Tony, Klein., Tony, Klein., Hien, Pham, Thu., Thomas, Walther., Thomas, Walther. (2018).** Bitcoin is not the New Gold - A Comparison of Volatility, Correlation, and Portfolio Performance. International Review of Financial Analysis, 59:105-116. doi: 10.1016/J.IRFA.2018.07.010

**Twomey, D., & Mann, A. (2020).** Fraud and manipulation within cryptocurrency markets. Corruption and fraud in financial markets: malpractice, misconduct and manipulation, 624.

**Yu-Lun, Chen., J., Jimmy, Yang. (2023).** Cryptocurrency hacking incidents and the price dynamics of Bitcoin spot and futures. Finance Research Letters, 55:103955-103955. doi: 10.1016/j.frl.2023.103955