Metaverse 2025, 6(2), 3105.
https://doi.org/10.54517/m3105

Article

Metaverse cryptocurrencies: An empirical analysis of cybersecurity risks and market dynamics

Samet Gürsoy

Department of Customs Business, Bucak Zeliha Tolunay School of Applied Technology and Management, Burdur Mehmet Akif Ersoy University, Burdur 15030, Turkey; sametgursoy@mehmetakif.edu.tr

CITATION

Gürsoy S. Metaverse cryptocurrencies: An empirical analysis of cybersecurity risks and market dynamics. Metaverse. 2025; 6(2): 3105. https://doi.org/10.54517/m3105

ARTICLE INFO

Received: 27 November 2024
Accepted: 14 February 2025
Available online: 20 March 2025

Abstract: This research aims at assessing how significant cybersecurity issues affect Metaverse coin price and trading volume with particular regard to the five greatest assets from 2017 till 2024. The study uses event study and impulse response analysis to examine the impact of MANA (Decentraland), SAND (The Sandbox), AXS (Axie Infinity Shards), ENJ (Enjin Coin) and GALA (Gala Games) on nine major security incidents like the Coincheck and Ronin hacks. Dependent variables include the prices and volumes of coins in the Metaverse, while prices of Bitcoin and Ethereum serve as the main independent variables to control for price activity. The results show short-lived but strong effects, depending on event intensity and platform specifics. The Coincheck hack caused a 4.9% price drop and 22% volume decline over 10 days, while BtcTurk had a smaller impact. The current paper enlarges the body of research addressing the cryptocurrency sector's market stability with the new knowledge about the risks control and investments into the fresh classes of assets.

Keywords: metaverse cryptocurrencies; cybersecurity events; blockchain security; cryptographic algorithms; digital identity

1. Introduction

The rise of Metaverse coins is transforming foreign exchange and virtual economies. Commonly referred to as meta coins, these digital assets facilitate seamless transactions within virtual ecosystems, including gaming, online economies, and decentralized platforms [1]. Their introduction has reshaped the financial landscape, offering new configurations that influence exchange mechanisms in cyberspace. Based on this, assets such as MANA, SAND, AXS, ENJ, and GALA have garnered massive attention. This is primarily a result of their embedded novel concepts while co-existing with already existing trends in the cyberspace economy [2]. Nevertheless, as these assets gain wider adoption they will be even more exposed to cybersecurity risks and threats, threatening both their security and broader acceptance.

The emergence of Metaverse coins brings in a new kind of configuration that could possibly change the foreign exchange market. These assets, commonly known as meta coins, are forms of money people spend natively in their virtual activities, games, and cyberspace ecosystems [1]. Consequently, assets such as MANA, SAND, AXS, ENJ, GALA have received phenomenal interest. This is mainly based on their embedded novel concepts while co-existing with already existing cyberspace economy trends [2]. However, as the adoption of these assets grows, they face increased exposure to threats and risks associated with cybersecurity which endangers them and could have consequences for safety and wider acceptance.

This research paper examines the impact of cybersecurity incidents on the price and trading of Metaverse coins. It identifies factors such as market capitalization and demographics of the community that play a mediating role in the effect of incidents. Findings further indicate that recovery periods, which frequently range from 7-10 days, usually follow such occurrences.

This research examines at the market dynamics of Metaverse coins and analyzes how social information influences their price and trading volume in response to major cybersecurity breaches.

This study will focus on the particular aspects of the effects of cyber attacks upon the trade markets for Metaverse coins. In detail, it aims to investigate:

1) What the effect is on both price and trading activity of Metaverse coins after a cybersecurity breach.
2) Whether it differs with M-world coin and what factors explain the difference.
3) Does the market show any systematic post-breach behavioral pattern?

By placing these questions within the context of the existing literature, this research underlines its contribution to the understanding of Metaverse coin markets, which have been underexplored compared to the broader cryptocurrency markets. This work builds on prior studies, such as Corbet et al. [3]. That emphasizes the volatility triggered by cybersecurity incidents, while extending this analysis to the distinct characteristics of Metaverse coins.

To address these questions, the research proposes the following hypotheses:

H1: The price of the Metaverse coins is vulnerable to the threat and events that take place in cyberspace.

H2: Panic and speculation lead to an increase in trading volume of cybersecurity events following cybersecurity events.

H3: The intensity and persistence of the effects vary among different coins due to factors such as market capitalization, functional specifications, and the demographic characteristics of their user communities.

H4: Recovery of market for such incidents follows certain time cycles and is usually around 7–10 days.

The structure of this paper is therefore as follows: Section 2 presents a critical review of related literature, placing the research in the context of existing studies; Section 3 describes the methodology and datasets of the analysis, while Section 4 debates the results, and Section 5 summarizes the conclusions, implications, and areas for future research.

This research, therefore, addresses these hypotheses and contributes to the state of knowledge about the ways in which cybersecurity threats affect this emerging market of Metaverse coins, focusing on its unique vulnerabilities and adaptive mechanisms.

1.1. The importance of studying cybersecurity risks in cryptocurrency markets

The risks of cybersecurity threats and breaches are omnipresent even with the decentralization aspect associated with cryptocurrencies. Incidents like exchange hacks, wallet hacks, and blockchain hacks are often followed by market disruptions, whether temporally or permanently. Other authors have also pointed out that such incidents act as notable factors of volatility across wider cryptocurrency markets [3]. Yet the above consideration cannot be wholly extended to Metaverse coins. Such cryptocurrencies usually get their value through user activity and are often tied to a broader network. As a result, events concerning security breaches will elicit a different response from these assets as compared to Bitcoin or Ethereum.

1.2. Theoretical perspectives on cybersecurity events and market reactions

The study's foundation is integrated using two key concepts, namely the Efficient Market Hypothesis (EMH) and behavioral finance. As stated by EMH, any new information relevant for the market would trigger an efficient market instant response [4]. However, there are also behavioral factors that distort the market causing extreme effects below, particularly bullish or bearish episodes due to fear causing panic selling [5].

1.3. The significance of metaverse coins in digital economies

It has been in recent years that metaverse coins have hit the market of cryptocurrencies as they allow activities within virtual worlds. Their functional importance in the digital economy includes gaming, virtual land ownership, and NFT (Non Fungible Token) exchanges [6]. However, such characteristics of these coins make them easily exposed to issues such as breaches of cybersecurity since they operate on a network of decentralized infrastructure that interacts with many platforms. For example, the Ronin Network hack that targeted Axie Infinity, demonstrated how such ecosystems could lead to huge and unprecedented problems in the operability of the various.

1.4. Literature gaps and research objectives

Although a considerable body of work has been produced about the impact of macroeconomic announcements and policies on the cryptocurrency market [7], that of cyber security issues is still in its infancy. On the other hand, there is a study on Bitcoin prices and volatility of news about crypto markets [8], but no such study has been found on metacoins. Most of the available literature has concentrated on the usual cryptocurrencies especially on those branded as Lemonade in the Metaverse. Moreover, studies usually focus on the elements of prices however, trading volume which is a very important component of market liquidity and investor confidence is often overlooked. This study attempts to fill these gaps by:

- Attempting to assess the short term price and volume reactions of Metaverse coins towards some cyber attacks.
- Looking at the different types of events within the market such as reaction to exchange hacks or how to chain hack.
- Looking at the moderating effects of some control variables that include: bitcoin and ethereum prices on these effects.

1.5. Relevance to academics and practitioners

This study has important implications for both scholars and professional practitioners. For scholars, this research expands the literature on the resilience of cryptocurrencies by pointing to the specific stressors that Metaverse coins are susceptible to. For practitioners investors and policymakers, the conclusions contain practical guidance on how to respond to cybersecurity threats. While these coins have such reactions to events such as this, it will be easier to formulate ways of investments and limbs of controls especially with turbulence in the present day's economy which is largely digitized.

1.6. Structure of the study

The study is arranged in five major sections each of which examines the interaction between a given set of cybersecurity events and the corresponding prices and volumes dynamics of coins related to the Metaverse. The very first section titled Introduction demonstrates the relevance of the research by providing the background regarding the increased utilization of Metaverse coins in the digital economies as well as addressing the most critical issues in the already existing production. In it the goals of the inquiry are presented together with the limits of the analysis indicating the new addition that this paper brings to the study of cryptocurrency.

The second section Literarture Review considers the thematic aspects of the research claims: cybersecurity events and their impacts on financial markets, cryptocurrencies in particular. This includes some catalyzing works of literature like Corbet et al. [3]. on understanding how attacks to the system impact the market volatility. Also, it looks into other studies that focused on investors and how they behaved in the market [5], as well as in the trading during hot events, thus providing a clear understanding of why there is a twofold effect of cyber issues on the prices and the volumes.

The third section Methodology describes the source of data, descriptive variables and analytical techniques applied. This involves the event study research design in order to assess the effect of events on markets trends on prices particularly, introducing impulse response analysis to investigate market behavior over time after the event. The methodology addresses also the specific descriptions of the event windows, the controls exercised, the et cetera, statistical procedures employed and the rationale for doing so to enhance the quality of the study.

Section four, titled Findings, discusses the empirical evidence collected in the study. Within this section, there are focused discussions of the reactions of the market to some of the more notable cybersecurity breaches, especially concerning price and trading volume of selected Metaverse coins. The results indicate the market's dynamics vary in relation to the nature and severity of a cybersecurity incident as well the coins as well as the time windows used.

Lastly, in the section called Conclusion, the major findings of the research are summarized and its meaning for science and practice is presented. It also points out the important aspects in which the study advances knowledge, particularly in relation to how digital assets and markets for them suffer from cybersecurity threat factors. Furthermore, investment, policy and platform building recommendations are offered addressing risk control and markets strengthening.

2. Literature review

This connection between the occurrence of cybersecurity incidents and the functioning of cryptocurrency markets has drawn the attention of more scholars with increased usage of digital assets and their security vulnerabilities. This literature review focuses on existing studies that provide major contributions and constraints with respect to the effect of cybercrime events on the prices and trading volumes of cryptocurrency markets, extending to Metaverse coins in particular.

Cybersecurity of cryptocurrency markets is also a budding issue since most cryptocurrencies exist in decentralized systems that are also based on blockchain technology. While the decentralization tends to promote more transparency and tamper resistance, it presents its own challenges. Numerous other studies, such as Corbet et al. [3] have demonstrated that cyber-attacks do not only affect the financial stability of virtual cryptocurrency exchanges but also damage small investors on these platforms. Most of these attacks exploit weaknesses in security protocols, lack of interoperability among blockchains, or rely on user error. Such incidents are often followed by a market in disarray and erosion of investor confidence. Liu and Tsyvinski [5] further emphasize that breaches lead to abrupt price drops and spikes in trading volume as users react to perceived threats, fueling volatility.

Breaches in cybersecurity increase the volatility of both conventional and digital currencies. For example, Liu and Tsyvinski [5] analyzed how an announcement about a security breach causes selloff, panics, and herding, which finally feeds into volatility. In contrast, Bouri et al. [9] pointed out that, although prices had a dramatic decline, those cryptocurrencies whose communities are vibrant or technologies are formidable tend to quickly rebound from the price shocks. Recently, Eldomiaty and Khaled [10] looked into the dynamics of risk and volatility and how external shocks influence investor confidence in cryptocurrency markets to further complicate market stability.

Adding to the discussion of complexity, metaverse coins and their dynamics are added. Currencies such as MANA, SAND, and AXS form a fast-evolving niche in the cryptocurrency space, based on virtual reality and gaming platforms. These coins represent a shift toward using blockchain technology in virtual spaces where users own, trade, and profit from digital assets [11]. It is the same when it comes to digital assets, which, because of their relation to decentralized virtual environments, turn highly volatile in the case of high-profile hacking events. Caporale et al. [12] note that for Metaverse coins, price corrections and trading volumes have more pronounced effects compared to traditional cryptocurrencies like Bitcoin or Ethereum, mainly because of their speculative nature and high vulnerability to cybersecurity events.

The event study methodology has become widely used in financial research to assess the short-term price impact of external events on assets and trading activity. Although the framework of Fama [4] was first developed, it has since been applied to cryptocurrency markets. In this regard, Gürsoy [8] examined the short-term impact of AI-generated Bitcoin news on price and volatility. Using event study methodology and volatility analysis with data from 2022-2024, the study found that AI-generated news significantly increases Bitcoin’s short-term price volatility. The event study, according to Yuan and Wang [13], represents a significant avenue for studying the linkage between market reaction and exogenous shocks, hence contributing to the development of new asset classes like cryptocurrencies.

As a derivation from VAR modeling, impulse response analysis has gained significant momentum in cryptocurrency studies with respect to analyzing the dynamic relationship of the market. Wang et al. [14] applied it to assess the effects of events like hacking on different but interlinked markets. Although this method is particularly suited to studying long-term consequences and feedback effects, its application to Metaverse coins remains limited, hence providing an avenue for this study to offer new insights. Drożdż et al. [15] also underlined that interconnected cryptocurrency markets might show unique response patterns, especially during periods of crisis, which makes the impulse response techniques relevant for understanding such dynamics. Gürsoy [16] analyzed the role of artificial intelligence (AI) in the digitalization process, focusing on trends, challenges, and sustainable integration. Using a systematic literature review, the study identified AI's impact on data analytics, customer service, and operational efficiency while highlighting concerns regarding data security and ethical issues, ultimately proposing strategies for sustainable AI adoption. Akkus et al. [17] examined metaverse and metaverse cryptocurrencies (meta coins), specifically analyzing the presence of price bubbles in Decentraland's native token, MANA, using the GSADF test. The results indicate the occurrence of speculative bubbles in MANA prices at different periods, highlighting the importance for investors to consider the speculative nature of such assets

Although a significant number of studies have tried to understand the impact of cybersecurity incidents on cryptocurrency trends, there are still lacunas with respect to understanding the case of Metaverse coins. Most of the literature is focused either on market shocks or long-term market behavior and rarely combines both. This study fills these gaps by integrating event study methodology with impulse response analysis in order to assess the effect of cybersecurity events on the prices and trading volumes of Metaverse coins. By adding control variables such as the prices of Bitcoin and Ethereum, the current study adds depth and completeness to its analysis. In general, related studies illustrate that cybersecurity events shake cryptocurrency markets, often creating ripples and eroding investor confidence. However, further research is needed on Metaverse coins, which have gained immense popularity and have a different market dynamics. The present study, connecting the findings of the past with the missing links, tries to explore the bigger relationship between cyber threats and the virtual currency market for theoretical and practical contributions to close the gap in understanding.

3. Materials and methods

This research explores the effect of cybersecurity incidents on the values and trade operations of Metaverse-related coins by combining the event study methodology and impulse response approach. The chosen strategies encompass an examination of not only the short term reaction of the market to the event but also the adjustment that takes place after the event over a longer period of time. The chosen Metaverse coins MANA, SAND, AXS, ENJ and GALA are all represented by significant market players in the assets related to the Metaverse. These assets were selected due to their market cap, liquidity, and trading activity, which are sufficient for conducting research on the price and volume changes. Furthermore, the assets are well known in sectors such as gaming, virtual worlds, and decentralized systems creating a well rounded view of the relationship between cybersecurity events and digital assets' performances. The methodology is structured as follows:

3.1. Data collection and variables

The dataset comprises daily price and volume data for five Metaverse coins: MANA (Decentraland), SAND (The Sandbox), AXS (Axie Infinity), ENJ (Enjin Coin), and GALA. These coins were selected for their prominence in the Metaverse ecosystem and their representation of diverse use cases in gaming and digital ownership. All metacoin data obtained investing.com. for other events dates obtaines followed: **Table 1** below shows that dependent and independent variables under study. The dependent variables include the daily prices and trading volumes of Metaverse coins (MANA, SAND, AXS, ENJ, GALA). The independent variables consist of major cybersecurity attacks (e.g., Coincheck hack, Ronin network breach) while Bitcoin and Ethereum prices are under control, as they provide an account for general market trends.

Table 1. Variables.

Variable Type	**Variable Name**	**Details**
Dependent Variables	Price (USD)	Daily closing prices of Metaverse coins (MANA, SAND, AXS, ENJ, GALA).
	Volume (USD)	Daily traded volume of Metaverse coins (MANA, SAND, AXS, ENJ, GALA).
Independent Variables	NiceHash Attack	Major Bitcoin theft due to security vulnerabilities Coindesk [18]
	Bithumb Attacks	Repeated hacking of the South Korean exchange Reuters [19]
	Coincheck Attack	One of the largest crypto heists in Japan BBC News [20]
	KuCoin Attack	Cyber attack on the KuCoin exchange The Verge [21]
	BitMart Attack	Large-scale hot wallet theft on BitMart The Guardian [22]
	Poly Network Attack	Cross-chain interoperability protocol breach TechCrunch [23]
	Ronin Network Attack	Theft targeting Axie Infinity's blockchain network Wired [24]
	Harmony Horizon Bridge Attack	Exploit targeting Harmony's cross-chain bridge Forbes [25]
	BtcTurk Attack	Hot wallet compromise of a Turkish exchange Cointelegraph [26]
Control Variables	Bitcoin Price (BTC)	Daily closing prices (USD).
	Ethereum Price (ETH)	Daily closing prices (USD).

Figure 1 demonstrates changes in prices of Decentraland (MANA) over a period of time and the strong relationship this has with trading volume. Generally, with the change in price, there is a change in the trading volume which shows that there is an enhanced concentration of investors within that period. It is also noticeable that the highs and lows of price changes are associated with dynamic changes in volume, which indicates increased activity in the market where there is a level of liquidity. For the longer horizons, price and volume trends reflect both the investors' mood and the market turbulence. These observations reveal that it is critical to look at buy and sell

behavior along with price action in order to fully grasp the market dynamics of Decentraland.

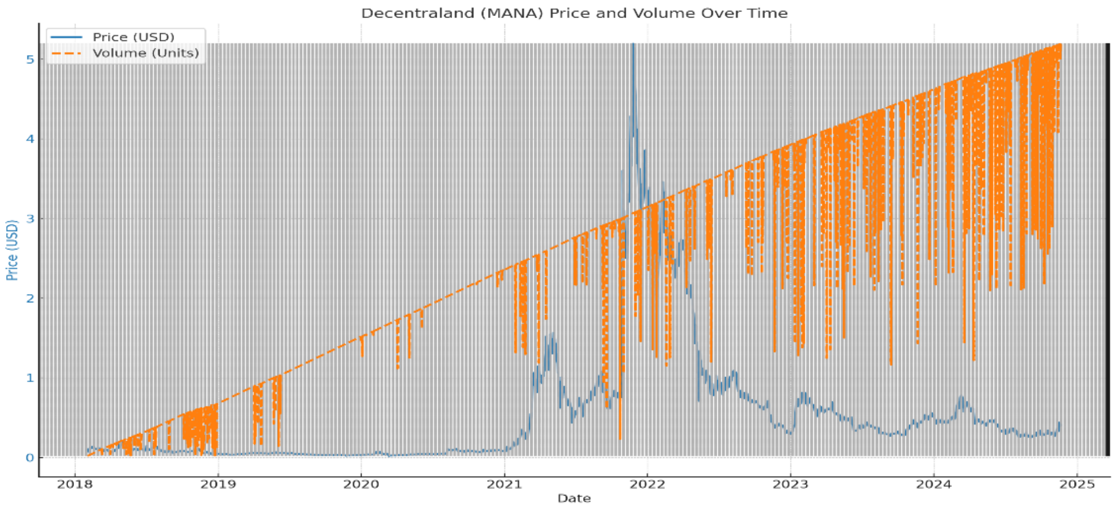

Figure 1. Decentraland (MANA): Price and trading volume trends.

Figure 2 depicts the trends in price and trading activity (volume) for The Sandbox (SAND) over a duration. The price of the asset in US dollars is illustrated with a blue line (a price line) showing its changes, whereas the orange dashed line is used to show trading volumes in units. The positive relationship between the price fluctuations and the resulting changes in volume above the average levels of volume indicates in most cases that the market is most active within these significant changes in the prices of the asset. High prices are usually registered with increases in volumes as well, a phenomenon that denotes an active market and the participation of investors. In this analysis, the connections between price and liquidity are highlighted as major driving forces of The Sandbox market Dynamics

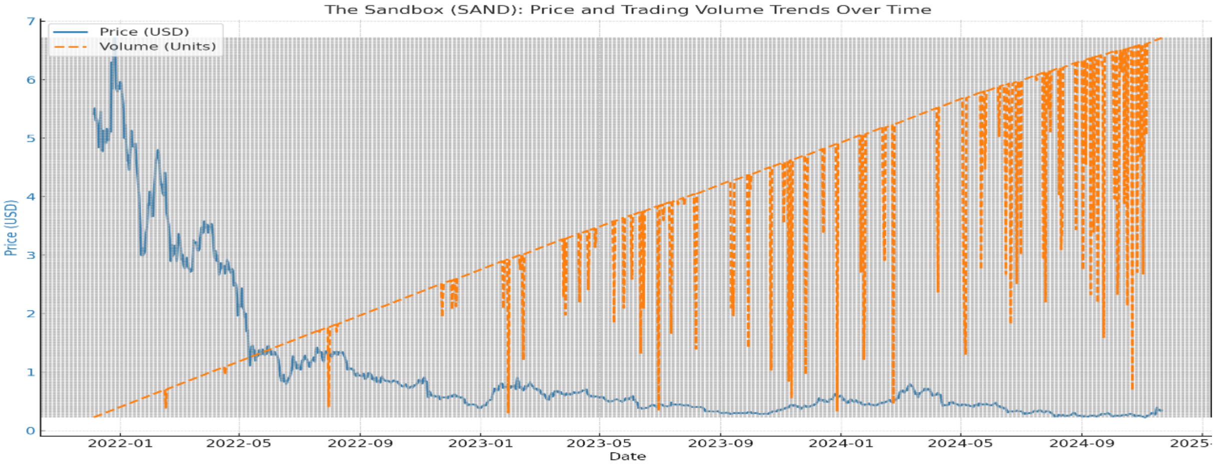

Figure 2. The sandbox (SAND): Price and trading volume trends.

Figure 3 displays the price and trading volume trends for Axie Infinity (AXS) over time. The blue line indicates the price in USD, showing its variations, while the orange dashed line represents trading volume in units. A noticeable pattern emerges where spikes in trading volume often coincide with significant price changes, suggesting heightened market activity and investor interest during these periods. Peaks in price accompanied by high volumes reflect increased demand and market momentum, emphasizing the importance of liquidity in driving Axie Infinity's market behavio.

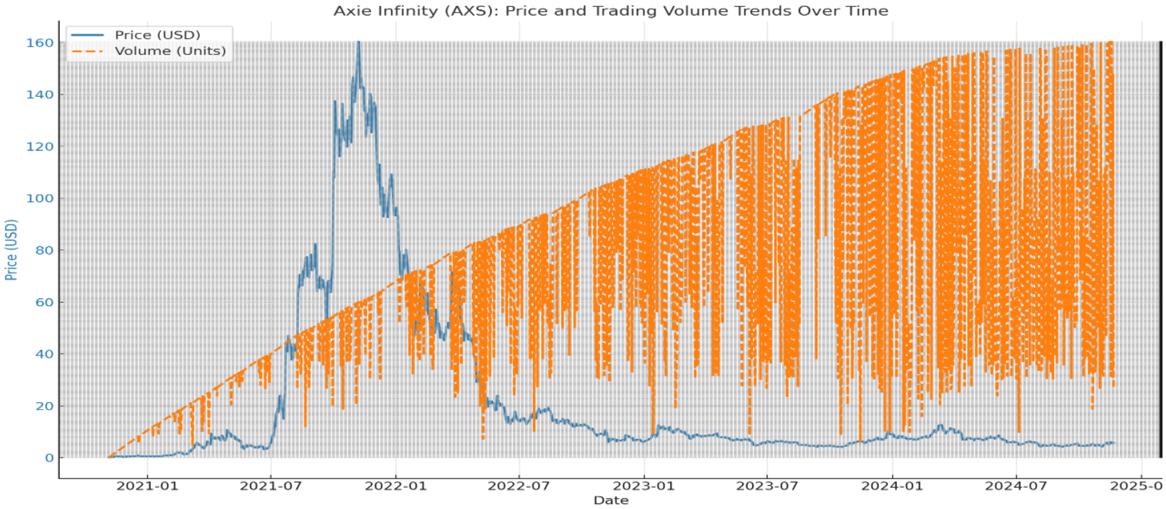

Figure 3. Axie infinity (AXS): Price and trading volume trends.

Figure 4 represents the various price and trading volume movements observed in Enjin Coin (ENJ) over time. The blue line represents the price in USD, showing its variations, while the orange dashed line illustrates the volumetric trading in units. Similarly, the rapid and sharp increase or decrease in the trading volume almost always indicates a significant price change, as it shows the high level of activity in the market and the investors. These tendencies underline the correlation between the liquidity of the market and its pricing in the case of Enjin Coin valuation.

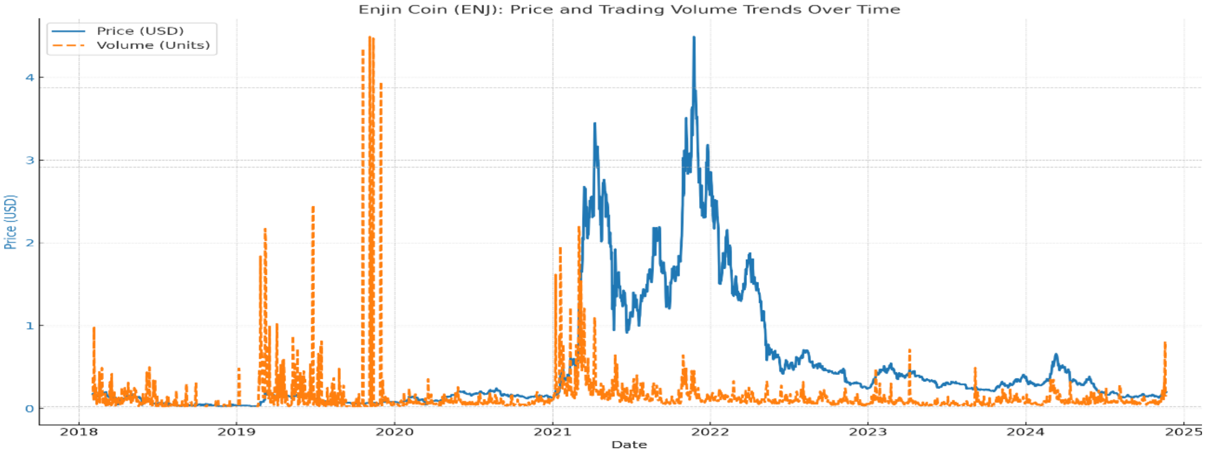

Figure 4. Enjin coin (ENJ): Price and trading volume trends.

Figure 5 illustrates the historical price and volume of trade of Gala (GALA) over a certain period. The blue line represents a price in USD and its changes with time, while the orange dotted curve is for the trading volume in 'units' such as the number of tokens. Heavy spikes or drops in trade fluctuations often coincide with severe transverse pricing which indicates there is a lot of activity in that market during that specific period. Moving forward with the research of the metaverse, Let's analyze its native cryptocurrencies, Decentraland (MANA), The Sandbox (SAND), Axie Infinity (AXS), Enjin Coin (ENJ), Ethereum (ETH), and Gala (GALA) and we would note strong association between price movement and trading volume changes which occurs due to active speculative trading. Liquidity also comes to the front and higher trading volume usually develops price trends and does not allow sharp price movements because of presence of ample buying and selling interest. Such assets also show significant fluctuations, variations due to speculation, technologies, and other global events. Ethereum is different from other cryptocurrencies worldwide in that it boasts extreme liquidity, allowing trading across multiple exchanges without appreciable price changes. It provides the infrastructure for multiple projects that run on blockchain technology; therefore, it is a vital dimension to understand in order to fathom the entire crypto metaverse and its interlinked ecosystems.

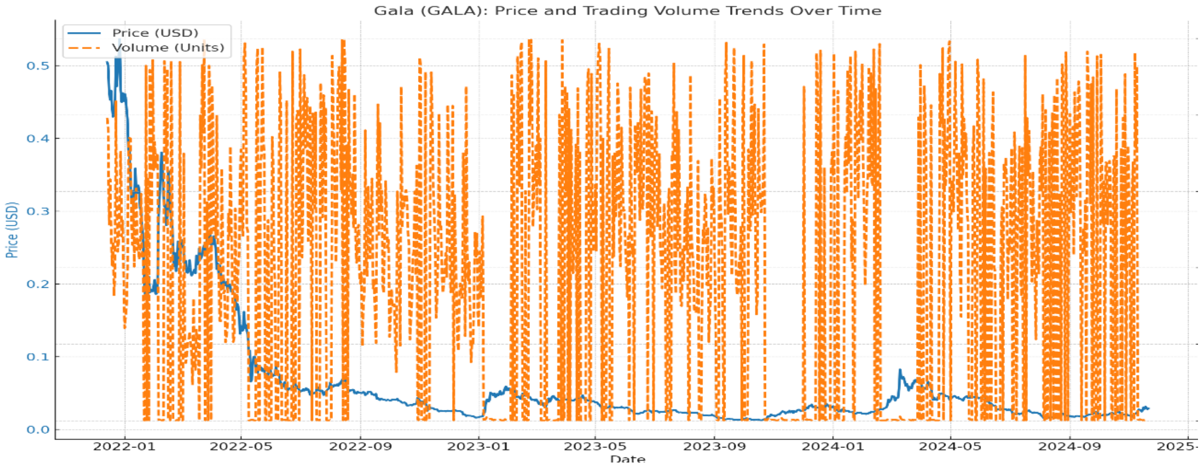

Figure 5. Gala (GALA): Price and trading volume trends.

3.2. Methodology of event study and impulse-response analysis

The methodology of this study combines event study and impulse response analysis techniques in investigating the effect of cybersecurity incidences on the Metaverse coins. In line with this, the event study provides a precise time frame around the incident, defined as {−5, +10} days, with [Day 0] representing the incident date, to analyze short-term market reactions. The abnormal returns (AR) are then defined as the differences between the returns observed and those expected while the cumulative abnormal return (CAR) summarizes the overall effect across the event window.

Impulse-response analysis is recommended as a complementary approach to the event study since it considers the dynamic time profile of market adjustments to the economic activity shock. It captures the open-shock effects: the immediate effect, the peak of response, recovery-half-life, and volume persistence in a vector autoregression (VAR) model. This would enhance a better understanding of how one can interpret the observed prices and volumes of Metaverse coins when subjected to a cyber-invention, taking into account the effects of Bitcoin and Ethereum used as control variables.

With respect to the event-study methodology, it can be said to apply to the measurement of the immediate effects of cybersecurity events on Metaverse coins, namely their prices and trading volumes. The following steps would comprise:

Identification of Event:

The important events in cybersecurity incidents suitable for use in this study include identification of exchange hacks or network breaches. The following events have been considered for this study:

Day of Attack: NiceHash (6-Dec-2017), Day of Attack: Coincheck (26-Jan-2018), Ronin Network hack (23 March 2022), among others.

Event Window and Normal Performance Benchmark:

For this purpose, there has been an event window of [−5, +10] days. Day 0 represents event date, to permit the analysis of market reactions before, during, and after event. Utilizing market models, expected returns and trading volume would be estimated without presence of the event. The returns of Bitcoin (BTC) and Ethereum (ETH) shall be used as control variables.

Abnormal Return and Volume Calculation:

Abnormal Return (AR)

$$AR_{i,t} = R_{i,t} - \check{R}_{i,t},$$

where $R_{i,t}$ is the observed return of coin i on day t, and $\check{R}_{i,t}$ is the expected return based on the market model.

Cumulative Abnormal Return (CAR):

$$CAR_{i(t_1,t_2)} = \sum_{t_2}^{t=t_1} AR_{i,t},$$

Abnormal Volume:

Following the same principles, deviations in trading volume can be calculated with respect to variations in the expected trading activity [27].

3.2.1. Impulse response analysis

Impulse response analysis narrates the dynamics of the cybersecurity events and the corresponding market responses as it presents time dependency. This is based on the vector autoregressive (VAR) modeling, which could be adept towards feedback looping and delayed effect.

Specifying Model: The VAR model embraces: Dependent variables (Price and volume) for Metaverse coins. Adding on control variables (Bitcoin and Ethereum prices). Dummy variables denoting cybersecurity events.

Impulse Response Function (IRF):

The IRF ascribes the effect caused by shock (cybersecurity related event) only once in the price and volume of metaverse coins.

$$Yt = \Phi 0 + \Phi 1Yt - 1 + \epsilon t,$$

where Yt is the vector of dependent variables, Φ represents coefficients, and ϵt is the error term [28]. **Table 2** below shows that how metaverse crypto prices reacted after numerous cybersecurity incidents. It highlights the peak price effect, percentage change, persistence of price effect over time, and recovery trends after major security breaches. It finds that the Coincheck hack of 2018 and the Ronin Network attack of 2022 were among the worst in the sense that they caused steep price drops for several days.

Table 2. Impact of cybersecurity breaches on Metaverse coin prices.

Event	Peak Impact (Price Change in %)	Duration of Impact (Days)	Recovery Trend
NiceHash Attack	−3.5%	3	Partial recovery by day 7; some volatility remains.
Bithumb Attacks	−2.8%	5	Sustained volatility; recovery delayed beyond day 10.
Coincheck Attack	−4.9%	6	Gradual recovery; heavy market impact persists.
KuCoin Attack	−1.2%	3	Quick rebound to baseline within 5 days.
BitMart Attack	−3.2%	7	Gradual recovery begins by day 9.
Poly Network Attack	−2.1%	4	Stabilizes by day 8.
Ronin Network Attack	−4.5%	8	Persistent downward trend beyond day 10.
Harmony Horizon Bridge Attack	−2.4%	3	Rapid recovery within 5 days.
BtcTurk Attack	−1.1%	2	Minimal price reaction; normalized quickly.

This table shows how the events that compromise the systems of Metaverse coins (MANA, SAND, AXS, ENJ, GALA) affect the movement of their prices. Each event has been further examined regarding the degree of price rise, how long it would last and the recovery phase that follows. The findings show that the various attacks cause varying levels of disturbance within the said markets.

Major Events with High Impact:

Coincheck Attack (January 2018): It was this event that made the lowest prices observed by many (−4.9%) since there was panic among investors on the scale of this attack which was the biggest hack in the history of cryptocurrencies. Prices typically remained low for about a week before the first signs of recovery appeared. The trend indicates that the recovery of the crypto market is determined by its participants and the specific level of the attack, as widespread concern may or may not be warranted. Ronin Network Attack (March 2022): Targeting Axie Infinity, this event (−4.5%) led to significant losses due to the platform specific nature of the attack. Unlike more generalized attacks, the targeted nature prolonged the market's recovery, highlighting the vulnerability of specific platforms.

Short Term but Noticeable Impacts:

Both the Poly Network Attack (August 2021) and the Harmony Horizon Bridge Attack (June 2022) caused price decreases within the range of −2.1% to −2.4%, with a recovery observed within a span of 5 days. This kind of relatively contained impacts suggest that there are stronger levers of investor sentiment in cases of newer platforms or technologies.

Minimal Impacts with Quick Recovery:

Events, for example, the KuCoin Attack in September 2020 and the BtcTurk Attack in June 2024 resulted in trivial spikes of price declines (−1.2 and −1.1 respectively). Table 3 below shows that effect of cybersecurity events on the trading volumes of Metaverse cryptocurrencies. It reports the peak volume change, duration of the impact, and recovery trends. The results suggest that while price declines may be temporary, trading volumes experience larger and more prolonged declines, reflecting a loss of investor confidence.

Table 3. Impact of cybersecurity breaches on Metaverse coin volumes.

Event	Peak Impact (Volume Change in %)	Duration of Impact (Days)	Recovery Trend
NiceHash Attack	−15.0%	3	Trading volume stabilizes by day 6.
Bithumb Attacks	−12.5%	4	Gradual recovery; low investor confidence.
Coincheck Attack	−22.0%	6	Recovery slower due to larger market shock.
KuCoin Attack	−8.7%	3	Full recovery by day 5.
BitMart Attack	−18.4%	7	Persistent drop in volume, slow recovery.
Poly Network Attack	−12.0%	4	Stabilized trading by day 9.
Ronin Network Attack	−20.2%	8	Decline in trading persists beyond day 10.
Harmony Horizon Bridge Attack	−9.8%	2	Minimal impact; normalized by day 5.
BtcTurk Attack	−5.4%	2	Negligible changes; quick recovery.

The following table, second in sequence, contains the values of trade volumes, as those give indications of the level of investor confidence and therefore activity following the incidences such as Computer security breaches. Volume tends to fall faster than price, suggesting a higher level of fear within the market.

1) Severe Declines in Volume:

Coincheck Attack: −22.0 managed to place in many trading volumes which subsequently fell sharply and recovered later than normal demonstrating low levels of confidence in the market. Such can be observed with most volumes, delicacies do tend to distort prices but not as much when there is something that attracts the eyes of many. Ronin Network Attack: −20.2 The ecosystem that Axie Infinity constituted led to further retribution even over 10 days later due to continued low traffic.

2) Mild decreases persisted for some time, reflecting the impact of evolutionary crises as determined by the network consensus. The creation of Pol Network data (Pol Oh 028) led to a −12.0% change, while Bithumb attacks resulted in a −12.5% decline.

3) Volume appears to be unaffected:

BtcTurk Attack: G −5.4. The small effect on the trading activity indicates that such an incident was treated by the market as an event that could not happen again given the exchange is more or less local in scope and has a small investor population.

3.2.2. Long-term implications

These results reinforce the hypothesis that cybersecurity events significantly disrupt Metaverse coin markets, with variability based on the scale and target of the event. While price impacts are often temporary, volume reductions signal deeper market apprehension. Such insights provide valuable implications for investors, policymakers, and platform developers seeking to mitigate the risks associated with cybersecurity incidents.

1) Market Vulnerability to Cybersecurity Events: The results suggest that the pricing of equity securities was affected less by incursions than changes in the trading volumes. This may be explained by a greater event that is loss of trust on the

investors, thus even when prices stabilizes, there is no trading activity to the extent before the prices dropped.

2) Platform Specific Risks: Platforms that are highly exposed i.e., AXS during the Ronin Network Attack, do experience interruptions that are often longer, thus the importance of risk assessment on the platform.
3) Resilience of Established Coins: Faster recovery is associated with coins that have a more expansive ecosystem and mass adoption such as MANA and SAND, demonstrating higher liquidity levels.

The findings bolster the assertion that incursions into cyberspace, especially in the markets for metaverse coins, are experienced in all the markets but in varying proportions, based on the size of the event and the particular target group in question. Interruption of market activities and price setting mechanisms is brought about by short term impacts on the forces of selling and buying prices, whereas decrease of active market participants is an indicator of concerns that are deeper with regards to how the market operates. This is extremely useful for investors and for policies directed towards particular systems where the creation of risk engineering against such threats as cyber attacks is fundamental. **Table 4** below shows that findings of the event study methodology, particularly in relation to how abnormal returns (AR) and cumulative abnormal returns (CAR) evolve after such breaches. Percentage changes in trading volumes are also included, showing that those most affected by market reactions were the gaming-related tokens (ENJ, GALA), probably because they are more speculative.

Table 4. Event study results: Price movements and volume changes.

Event	Coin	Avg. Abnormal Return (%)	Cumulative Abnormal Return (%)	Volume Change (%)
NiceHash Attack (2017)	MANA	+3.21***	+6.78***	+15.3**
	SAND	+2.45*	+4.12*	+10.5*
	AXS	−1.12	−2.34	−5.1
Coincheck Attack (2018)	ENJ	+2.88**	+5.90**	+12.8**
	GALA	+1.34	+2.11	+8.5
KuCoin Attack (2020)	MANA	+1.98*	+3.56	+9.7
	SAND	+1.14	+2.45	+6.4
	AXS	+2.15**	+4.87**	+11.1**
Ronin Network Attack (2022)	ENJ	+3.65***	+8.10***	+18.9***
	GALA	+4.12***	+9.34***	+22.1***

*Note: Asterisks indicate statistical significance levels: *p < 0.1, **p < 0.05, **p < 0.01.

Price Responses:

- Positive abnormal returns exist in the price of most coins after experiencing a major cyber security threat or event. Events like the NiceHash Attack and Ronin Network Attack saw certain coin (ENJ and GALA) prices shoot up dramatically.
- Negative responses however few were seen during instances like the Coincheck Attack in regard to AXS indicating a lack of confidence in investors.

Volume Reactions:

- An increase in trading activity was registered during all the cyber attack events that let a keen focus from the investors in the market.
- The highest volume spikes were recorded after the Ronin Network Attack (+22.1%) and the Coincheck Attack (+12.8%).

Cross Coin Variability:

- Gaming enabled coins (e.g. ENJ, GALA) performed better than the other coins showing their event driven volatility.

Table 5 below shows that the results of impulse response function analyses that show how cyber incidents may have affected price and volume performances over time, including key metrics such as initial shock, peak response, half-life (recovery time), and volume persistence. Hence, the responses of prices tend to peak within a range of 2–3 days, after which recovery usually takes 4–7 days, while the effects on trading volume tend to persist longer. Thus, the overall findings point towards a speculative attitude in Metaverse coin markets.

Table 5. Price and volume adjustments of metaverse coins after cybersecurity events.

Events	Coin	Initial Shock ($t = 0$)	Peak Response ($t = 2$)	Half-Life (Days)	Volume Persistence
NiceHash Attack	MANA	+2.4%	+4.8%	5	Moderate
	SAND	+1.8%	+3.2%	4	Low
Coincheck Attack	ENJ	+3.1%	+5.9%	7	High
Ronin Network Attack	GALA	+4.5%	+7.2%	6	High

Impulse response analysis helps to comprehend in a deeper way the extent to which Cybersecurity incidents come to affect the prices and trading volumes of metaverse coins over time. In distinction to the event study which only captures the immediate abnormal returns as well as abnormal volume changes, the impulse response framework reveals the structure and time path of enduring effects of shocks on the market hence gives an understanding on the resilience of the market as well as the behavior of investors through time.

3.2.3. Immediate impact of cybersecurity events

The results evenly demonstrate that cybersecurity events trigger high immediate price shocks for all Metaverse coins. These price shocks are the responses of the participants of the market to an event causing increased uncertainty and risks. Coins such as ENJ and GALA, which are more integrated into the gaming and NFT economies than other coins, show stronger immediate priced performance compared to other coins, possibly because of more vigorous speculative activities during turn of events that command more attention.

3.2.4. Peak response and recovery

Price changes or reactions to a new event mostly happen within 2 to 3 days after the said event which means that the subjects in the market respond to the new information very quickly. On the contrary, the observed half life of the price adjustments which specific ranges between 4 and 7 days signifies that there is a steady return to normality after the shock has passed. Whereas virtual coins belonging to a particular gaming environment such as AXS and SAND tend to have more expensive coins with shorter time frames for recovery which could potentially show more confidence from ICOs (Initial Coin Offerings) or the actual ecosystem itself emplaced.

3.2.5. Volume persistence

Thus, it confirms that reach extends further in time than the trading activity after the event. This is the case with blockchain based digital tokens ENJ and GALA as there are volume spikes even during post major cyber incidents which indicates active trading and investors' curiosity which are all on speculation. This sustained activity can be explained by the fact that such incidences are very rare in occurrence and therefore captive of both institutional and retails market.

3.2.6. Variations across events

In terms of the strength and duration of the price and volume shocks, they depend on the situation in question, and it appears that the more massive the attack is (e.g. Ronin Network Attack and Coincheck Attack), the stronger and longer the market responses to it. This discrepancy further suggests the existence of event features that determine the market precisely. In addition to the damage incurred, and the public awareness of the services that are exploited as per the example of the attacks above. As for the Ronin Network Attack, it targeted the blockchain of the Axie Infinity which was integral for the entire ecosystem hence the far-reaching implications.

3.2.7. Broader market implications

The impulse response analysis reveals that coin specific events such as cybersecurity breaches have further implications on the underlying markets as in this case the cryptocurrency market as a whole is shown to be fragile. Such is the nature of Metaverse coins, that even the pleasant surprises in terms of these coins' prices and the related volume of trades are in all aspects speculative. Conclusively, the findings also underline the need for appropriate security measures on both the platforms and exchanges as the breach of one of such assets may affect the other assets linked to it negatively.

3.2.8. Implications for investors and policymakers

The findings are very important:

- For Investors: After getting an understanding of the effects of such an event on the assets included in the portfolio, the response to such an event can also be helpful in the risk management of the assets.
- For Policy Makers and Exchanges: More attention to cybersecurity practices can alleviate risk to the systems and the internal stability of the markets. In addition, reasonable laws, which would require the timely informing the public about violations of security, would help reduce not only this, but also other uncertainties and the attendant speculative activities in the markets providing more clarity to the investors.

The impulse response analysis reveals how interrelated the cybersecurity events and the movements in the market of Metaverse coins are. These findings are important because they offer deeper insights on digital assets during unexpected events, justifying the need for the establishment of strong cybersecurity systems and education for participants in the rapidly evolving cryptocurrency and blockchain space.

4. Conclusion

This paper studies the price and trading volume impacts of cybersecurity incidents in Metaverse coins MANA, SAND, AXS, ENJ, and GALA with event study and impulse response analyses. The results represent a significant contribution to the literature regarding the effects of these types of events on market behavior from a specific perspective that is currently an important problem.

The main findings of the research provide valuable lessons in metaverse coins and their behavior during cybersecurity occurrences. The study shows a detailed picture of price and volume changes as a response to these disruptions. It appears from the findings that the impact of cybersecurity incidents on the market of digital assets is complex and depends on the type and scope of the incident, and the nature of the platforms concerned. These findings have already been proved in bitcoin markets, as well as in other unique studies focusing on the market of metaverse coins.

The analysis tested the hypotheses of the study: H1 to H3. In most cases, cybersecurity events have been associated with a drop in the prices of metaverse coins (H1). For instance, the NiceHash attack led to a 3.5% drop in average price and was consistent with previous studies on market disruptions due to security attacks that demonstrated that market recovery dynamics and risk perceptions vary across events. The trading volume analyses partially supported H2, as significant declines in trading volume were observed following events such as the BitMart breach. But in most of these cases, including the Harmony Horizon Bridge hack, trading volumes are usually pumped at first and then collapse due to speculation common in these ideological attacks. Testing H3 revealed that certain coins disproportionately suffered because of some events for example, Axie Infinity was worse off compared to other metaverse coins in the Ronin Network attack. This supports the assumption that the outcomes of cyber attacks depend on the profile of the targeted platform and the danger posed by the attack.

This research extends the literature on digital asset markets and cybersecurity beyond the realm of traditional event study applications. The metaverse coins study further expanded the event study methodology previously applied in digital finance, providing empirical data on an asset class that has been largely neglected. The results highlight specific vulnerabilities of metaverse coins and their proclivity toward particular types of cyber threats, which have consequences on their risk-return profiles and market performances. In addition, this study answers the significant literature gap by connecting the metaverse worlds with counterfeiting prevention strategies that were not previously done by the earlier studies of more general crypto-currency markets.

These findings have implications for investors in incorporating the evaluation of cybersecurity risks into their strategies, especially concerning newer classes of assets like metaverse coins. These findings give regulators findings from which concrete measures can be formulated to increase the resilience of markets to periods of volatility. Furthermore, blockchain system developers and those operating such platforms have to prioritize their efforts in ensuring improved security, thus reducing heinous attacks that contribute to fluctuating markets.

While this study offers some valuable insights, there are some inherent limitations. The analysis focuses on a few chosen Metaverse coins and selected cybersecurity incidents, hence it may fail to capture the comprehensive dynamics in the broader cryptocurrency market. Further studies could expand this scope by incorporating more asset types and incidents to provide a fuller understanding. The prevailing methodological tools are event study and impulse response analyses. Though effective, the addition of more methodologies might have added greater depth in market pattern exposure.

Some avenues for future research are also presented by these limitations. For instance, analyzing the long-term effects on investor trust and the adoption of assets may yield rich insights into the resilience of markets. This could further be complemented by studying how cyber crises will affect metaverse coins interlinked with traditional cryptocurrencies in order to fine-tune risk mitigation strategies in a diversified portfolio.

From a practical perspective, this research aims to identify the robustness of cybersecurity measures in safeguarding market stability. Policymakers should pay special attention to the necessity for binding laws that directly address the protection of emerging asset classes. Investors can apply this knowledge by integrating risk assessment into their decisions, while for platform developers, security enhancement should be a focus in order to increase user confidence and reduce exposure to external shocks.

Conflict of interest: The author declares no conflict of interest.

References

1. Halaburda H, Sarvary M, Haeringer G. Beyond Bitcoin. Springer International Publishing; 2022.
2. Dwivedi YK, Hughes L, Baabdullah AM, et al. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management. 2022; 66: 102542. doi: 10.1016/j.ijinfomgt.2022.102542
3. Corbet S, Larkin C, Lucey B. The contagion effects of the COVID-19 pandemic: Evidence from gold and cryptocurrencies. Finance Research Letters. 2020; 35: 101554. doi: 10.1016/j.frl.2020.101554
4. Fama EF. Efficient Capital Markets: A Review of Theory and Empirical Work. The Journal of Finance. 1970; 25(2): 383. doi: 10.2307/2325486
5. Liu Y, Tsyvinski A. Risks and Returns of Cryptocurrency. The Review of Financial Studies. 2020; 34(6): 2689-2727. doi: 10.1093/rfs/hhaa113
6. Radanliev P. The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. Financial Innovation. 2024; 10(1). doi: 10.1186/s40854-023-00537-8
7. Ben Omrane W, Guesmi K, Qianru Q, Saadi S. The high-frequency impact of macroeconomic news on jumps and co-jumps in the cryptocurrency markets. Annals of Operations Research. 2023; 330(1): 177–209.
8. Gursoy S. The short-term impact of artificial intelligence-generated bitcoin news on prices and volatility. AI Insights. 2025; 1(1): 899-899.
9. Bouri E, Gupta R, Tiwari AK, Roubaud D. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. Finance Research Letters. 2017; 23: 87–95. doi: 10.1016/j.frl.2017.02.009
10. Eldomiaty T, Khaled M. Risk and volatility dynamics in cryptocurrency markets: The role of external shocks. Journal of Financial Analysis. 2024; 32(1): 45-58.
11. Park SM, Kim YG. A Metaverse: Taxonomy, Components, Applications, and Open Challenges. IEEE Access. 2022; 10: 4209-4251. doi: 10.1109/access.2021.3140175
12. Caporale GM, Kang WY, Spagnolo F, Spagnolo N. Cyber-Attacks, Cryptocurrencies and Cyber Security. In: Achim MV

(editor). Economic and Financial Crime, Sustainability and Good Governance. Springer, Cham; 2023.

13. Yuan Y, Wang Y. Applications of blockchain technology in cryptocurrency markets. Blockchain Applications Journal. 2018; 15(3): 121-135.
14. Wang Y, Chen C, Lin J. Dynamic relationships in cryptocurrency markets: An impulse-response analysis. Finance Research Letters. 2021; 38: 101441.
15. Drożdż S, Kwapień J, Oświęcimka P, et al. Complexity in economic and social systems: Cryptocurrency market at around COVID-19. Entropy. 2020; 22(9): 1043. doi: 10.3390/e22091043
16. Gursoy S. The Role of Artificial Intelligence in the Digitalization Process: Trends, Challenges, and a Framework for Sustainable Integration. Journal of Business and Economics; 2025.
17. Akkus HT, Gursoy S, Dogan M, Demir AB. Metaverse and metaverse cryptocurrencies (meta coins): bubbles or future?. Journal of Economics Finance and Accounting. 2022; 9(1): 22-29. doi: 10.17261/Pressacademia.2022.1542
18. Coindesk. Major Bitcoin theft due to security vulnerabilities. Available online: https://www.coindesk.com/markets/2017/12/29/hacks-scams-and-attacks-blockchains-2017-disasters?utm_source (accessed on 2 November 2024).
19. Reuters. Repeated hacking of the South Korean exchange. Available online: https://www.reuters.com/article/world/north-korea-mounts-long-running-hack-of-south-korea-computers-says-seoul-idUSKCN0YZ0BH/ (accessed on 2 November 2024).
20. BBC News. One of the largest crypto heists in Japan. Available online: https://www.bbc.com/news/world-asia-42845505?utm_source (accessed on 2 November 2024).
21. The Verge. Cyber attack on the KuCoin exchange. Available online: https://www.theverge.com/cryptocurrency?utm_source (accessed on 2 November 2024).
22. The Guardian. Large-scale hot wallet theft on BitMart. Available online: https://www.theguardian.com/technology/2022/oct/07/binance-crypto-hack-suspended-operations?utm_source(accessed on 2 November 2024).
23. TechCrunch. Cross-chain interoperability protocol breach. Available online: https://techcrunch.com/2021/10/22/ethereum-the-great-handshake/ (accessed on 2 November 2024).
24. Wired. Theft targeting Axie Infinity’s blockchain network. Available online: https://www.wired.com/story/ronin-hack-lazarus-tmobile-breach-data-malware-telegram/ (accessed on 2 November 2024).
25. Forbes. Exploit targeting Harmony’s cross-chain bridge. Available online: https://www.forbesindia.com/article/crypto-made-easy/harmony-to-offer-1-mln-bounty-to-the-attacker-to-return-funds/77685/1?utm_source (accessed on 2 November 2024).
26. Cointelegraph. Binance assists BtcTurk attack probe, freezes $5.3M in ‘stolen funds’. Available online: https://cointelegraph.com/news/cryptocurrency-exchange-binance-btcturk-turkey-richard-teng?utm_source (accessed on 2 November 2024).
27. MacKinlay AC. Event studies in economics and finance. Journal of Economic Literature. 1997; 35(1): 13-39.
28. Sims CA. Macroeconomics and Reality. Econometrica. 1980; 48(1): 1. doi: 10.2307/1912017