VILNIUS UNIVERSITY

FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

FINANCE AND BANKING

Ugnė Sauliūnaitė

MASTER THESIS

KIBERNETINIŲ NUSIKALTIMŲ ĮTAKOS KAINŲ SVYRAVIMUI KRIPTOVALIUTŲ RINKOSE TYRIMAS	**INVESTIGATING IMPACT OF CYBERCRIMINALITY ON PRICE VOLATILITY IN CRYPTOCURRENCY MARKETS**

Supervisor Prof. Dr Alfreda Šapkauskienė

(scientific, pedagogical titles of the supervisor, supervisor's name, surname)

Vilnius, 2023

TABLE OF CONTENTS

INTRODUCTION

The Internet has played a vital role in international communication for more than two decades and is becoming increasingly incorporated into the lives of people all over the world. Because to innovations and cheap costs in this field, the Internet's availability, use, and performance have considerably risen, and the Internet now has over 3 billion users globally. The Internet has established a massive worldwide network that contributes billions of dollars to the global economy each year. The majority of economic, commercial, cultural, social, and political operations and relations of countries are now conducted in cyberspace at all kinds, involving people, government, and governmental institutions. Most critical and sensitive information is transported to this space or has been produced in this space, and vital and sensitive infrastructures and systems are either a part of cyberspace itself or are controlled, managed, and exploited through this space. The majority of media activities are shifted to this area, as are the majority of financial transactions, and a considerable amount of individuals' time and activities are spent interacting in this space.

However, cyberspace has posed new security challenges for nations. Threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage have emerged from both strong and weak performers, including governments, organized and terrorist groups, and even individuals, due to the low cost of entry, anonymity, uncertainty of the threatening geographical area, dramatic impact, and lack of public transparency in cyberspace.

Many commercial firms and government agencies throughout the world are currently dealing with cyber-attacks and the dangers of wireless communication technology. Analysts have been debating the potential repercussions of cyber-attacks for more than a decade. There are different scenarios for harsh and sometimes prevalent physical or economic damage, such as the function of a virus that attacks an economic system's financial documents or disrupts a country's stock market, or the function of a virus that sends an incorrect message, causing the country's power plant to stop and fail, or even the function of a virus that disrupts the air traffic control system, causing air accidents.

The availability of a complete definition of a cyber-attack will surely have a direct influence on the legal environment, making it more difficult to continue and identify the repercussions of this sort of assault. Until now, academics from all over the globe have offered a variety of ways for preventing cyber-attacks or reducing the harm they do. Some of the approaches are in use, while others are still being researched. The many sorts of new descendant assaults are discussed in depth.

The history of early-generation cyber-security approaches are described together with standard security frameworks.

This topic is relevant because cryptocurrencies have grown in popularity as a result of their ability to offer efficient payment systems via a decentralized distributed ledger that is not reliant on a political process or governmental regulatory structure. Cryptocurrency prices are volatile and cybercriminality is one of the key reasons. Hackers can take electronic identities and shift funds from lawful accounts if they have access to the public's credentials. Phishing attacks are when a hacker imitates the appearance of a trustworthy source in order to gain credentials. Direct security breaches may allow hackers to steal much more information.

The continuing expansion of cryptocurrencies and the underlying exchanges on which they trade has created a great deal of pressure to learn more about a product that has been identified as a potential augmentation to and replacement for traditional cash as we know it. When compared to more established rivals, much research continues to show that this asset class has extraordinarily high levels of volatility. Thus, cryptocurrencies as a new asset class are not without significant drawbacks, notably in terms of providing a platform for criminal activity and, in some cases, massive cybercrime events. While there is great dispute about how this commodity should be regulated, there are numerous ways through which criminality might flourish and prosper. Because of the increased potential for illegality and malpractice, regulatory organizations and policymakers have viewed the emergence of cryptocurrencies with some skepticism. Therefore, it is unclear, what is the relationship between price volatility and cyberattacks in cryptocurrency markets?

The main aim of the Master thesis is to identify characteristics of cyberattacks and examine its impact on price volatility in cryptocurrency markets.

To achieve this aim, the following objectives are set:

- Review the literature of cybercrime and cryptocurrency market concepts and discuss connection between cybercrime and cryptocurrency market price fluctuation.
- Build a methodology to investigate dynamics and cryptocurrency price’s response to the cyberattacks.
- Based on constructed methodology, conduct a study to analyse and describe results and discuss limitations, suggest improvements for future work.

Chosen method for this research is based on previous experiments (Katsiampa, 2017; Corbet, Meegan, Larkin, Lucey, & Yarovaya, 2018). As this research heavily depends on statistical and numerical analysis, the major method of data collection is quantitative. The Generalized AutoRegressive Conditional Heteroskedasticity (GARCH) is selected for this research due to its capability to assess the return volatility of stocks, bonds, and other financial instruments as well as estimate the volatility of financial markets model approach is why I chose it. The GARCH process offers a more accurate structure when forecasting the values and rates of financial products than other models. The GARCH approach is used to accomplish the aim of this research. 13 variables with daily data from September 1, 2017, to October 31, 2022, are included in the analysis.

The thesis is structured as follows: in the literature review section, the literature related to the topic of the study and the conducted research methods are analysed; in the methodology section, an in-depth explanation of the incorporated research methods and the limitations arising from them is provided; in the results section, I conduct an in-depth analysis of the data and discuss upon the data source and detailed explanation of the results generated from the conducted analysis is provided; the conclusions and recommendations section focus on summarizing the findings of the study and proposing recommendations for future work.

1. THEORETICAL CONCEPTS ABOUT CYBERCRIMINALITY AND PRICE VOLATILITY IN CRYPTOCURRENCY MARKETS

In this section, I explore the existing literature related to cyberattacks definitions and fundamental concepts, cyberspace risks and cyberattacks events in cryptocurrency markets, price volatility in cryptocurrency markets. While the literature related to analysing the effects of the cyberattacks on price volatility in cryptocurrency markets is very limited as of this moment, there is a vast selection of conducted research related to the latter problems related to cyberattacks and causes of price volatility.

1.1. Concepts of cyberattack

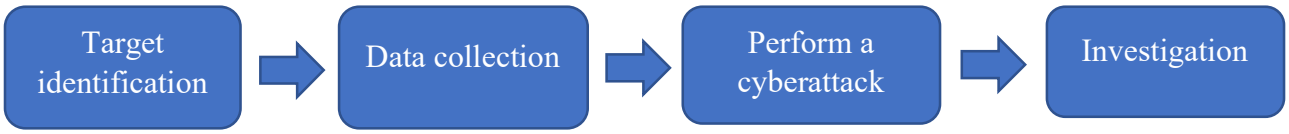
Cyber-attacks are a larger category than what has typically been referred to as information operations. Information operations combine the primary abilities of cyberwarfare, psychological warfare, computer systems, military trickery, and security operations in cooperation with specific assistance and relevant abilities to penetrate, stop, destroy, or hijack human decisions, and it is one of national institutions' decision-making processes (Hart et al., 2020). The anatomy of a cyber-attack is depicted in Figure 1. According to the USNM Cyberspace Operations Strategy, computer network operations include attack, protection, and utilization allowing (Ma et al., 2021). The latter differs from network assaults and network defense in that it emphasizes on gathering and analysing data rather than disrupting networks, and it may be used as a precursor to an attack. These activities can be used to disseminate information and spread propaganda (Thomson, 2015). Operations that enable computer network exploitation can also be carried out with the goal of stealing crucial computer data. Trap Sniffers and Doors are useful tools for cyber security in this situation (Liu et al., 2021). Trap Doors allow an external user to access software at any moment without the computer user's awareness. Sniffers are devices that may be used to steal usernames and passwords (Karbasi and Farhadi, 2021). The main definitions and principles of cyberspace are listed in Table 1. Cyber warfare can have the following repercussions (Khan et al., 2020; Furnell and Shah, 2020):

- The overthrow of the political system or a major danger to national security;
- Synchronous physical warfare initiation and facilitation of physical warfare beginning in the near future;

- Catastrophic devastation or harm to the country's worldwide reputation;
- Catastrophic devastation or harm to the country's political and economic relationships;
- Human casualties in large numbers or a threat to public health and safety;
- Internal disturbance;
- Considerable instability in the country's government;
- Putting the public's faith in religious, national, and ethnic convictions in jeopardy;
- Irreparably harming the national economy;
- Destruction of the functioning of national cyber assets on a large scale.

Figure 1

Structure of cyberattack



Source: made by author

In addition, five cyber warfare situations can be taken into account: (1) Government-sponsored cyber intelligence gathering to collect information for future cyber-attacks, (2) a cyber-attack aiming at planting the seeds of instability and public revolt, (3) disabling equipment and encouraging physical assault are the goals of a cyber-attack, (4) as a counterpart to physical hostility, cyber-attacks are being used, (5) The ultimate purpose of a cyber-attack is to cause widespread destruction or disruption (cyber warfare) (Alibasic et al., 2016). Encryption is one kind of cyber-attack. Encryption is a reversible process of encrypting and decrypting data that necessitates the use of a key. Encryption can be used in conjunction with encryption to give an additional layer of security. Encryption is the practice of encrypting and decrypting data in such a way that it can only be decoded by particular people. The encryption system is a mechanism for encrypting and decrypting data. Encryption is a strong tool for securing vital and private information from strangers and criminals, as well as for concealing illegal activity from law enforcement. Cryptographic algorithms must be continuously consolidated to avoid insecurity as computers become faster and failure mechanisms become more secure (Zou et al., 2020). It is important to note that there is a distinction to be made between cyber-crime, cyber-warfare, and cyber-attacks in general. The distinction between cyber-crime, cyber-

warfare, and cyber-attack is described in figure 2 and table 2, which establishes the conceptual distinction between them. Various definitions of cyber-attack have been proposed by legal and technological experts. There are four most prominent definitions of cyber-attack, which I discuss below.

Table 1

Basic definitions and concepts of cyberspace (Bullock et al., 2021)

Title	Definition
Cyber space	Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings forthe purpose of production, processing, storage, exchange, retrieval and exploitation of information.
Cyber capital belonging to a country.	A vital (or sensitive) infrastructure of a country, a vital cyber system, a key information, or individuals
Cyber vulnerability	Vulnerability refers to a weakness within an asset, security procedures or internal controls, or the implementation of thatnational cyber asset that can be exploited or activated by internal or external threats to conduct cyber warfare.
Cyber threats	Any event with the ability to strike a blow to missions, tasks, images, national cyber assets or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of(disruptive) service delivery.
Cyber threat level	Cyber threats are able to affect national cyber assets at the transnational, national, institutional, provincial, critical, andcritical levels of infrastructure.
Probability of cyber threats	Very high (imminent), high (probable), low (unlikely) and very low (very unlikely)
Intensity of cyber threat very low (security incident)	Very high (disaster), high (crisis), moderate (major security incident), low (security incident) and
Cyber attack	Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional useof a cyber-weapon against an information system in a manner that causes a cyber-incident is also considered cyber-attack.
Cyber weapon	A cyber weapon is a system designed and manufactured to damage the structure or operation of other cyber systems. These systems include bot networks, logic bombs, cyber vulnerability exploitation software, malware, and traffic generation systems to prevent service attacks and distributed service.
Cyber warfare	Cyber warfare is the highest level and most complex type of cyber-attack (cyber operation) that is carried out against thenational cyber interests of countries and will have the most severe consequences.
Cyber warfare origin	The cyber force of the aggressor country or groups organized under the aggressor states, cyber weapons controlled orabandoned by these forces
Cyber defense	Utilization of all unarmed cyber and non-cyber facilities of a country, to create deterrence, prevention, prevention, timelydetection, effective and deterrent response to any cyber attack
Cyber biome	Cyber biome refers to the formation of a native and dynamic cyber environment that is supportive for a country in variousfields.
Virus	A virus is a self-replicating program that spreads to other documents and other programs by duplicating itself, and may cause programs to malfunction. A computer virus acts like a biological virus that spreads through its reproduction to cells inthe host body. Some of the popular viruses are: NIMDA, SLAMMER, and SASSER.
Hacker	A person who enters a system without permission or who increases his/her access to information to browse, copy, replace,delete or destroy it.

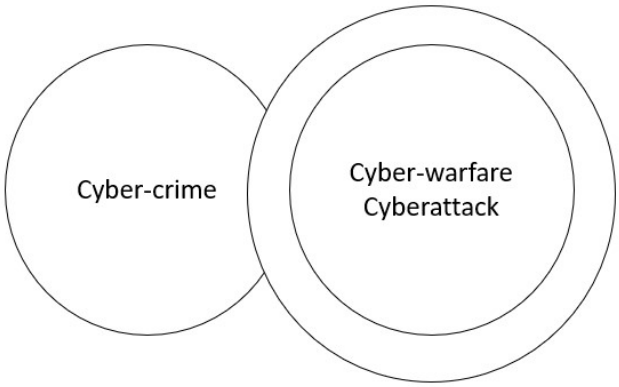
Source: made by author

First expert is Richard Clark and there are authors who did research based on Richard's Clark definition. According to the author (Motsch et al., 2020), Cyber-attacks are activities conducted by countries to breach a country's or other countries' computers or computer networks in order to cause harm or disruption. The three aspects of the attack, namely the perpetrator, the purpose, and the intention of the attack, have been utilized as criteria in the study and critique of this term, without considering the forms of disruption (Cao et al., 2019). Furthermore, only countries are stated in general when it comes to the perpetrator of the crime. Individuals and non-governmental and private groups acting against a third country in the context and geographical area under the control and jurisdiction of a country (cyberspace of networks under the control of countries) will essentially fall outside the scope of the mentioned definition and will not be included. As a result, there should be a legal gap in the coverage of such attacks. Given this position, it is reasonable to conclude that the previous definition is completely inadequate, since it excludes a considerable portion of assaults carried out by private and non-governmental organizations, resulting in a void.

Second expert is Michael Hayden and there are authors who did research based on Michael's Hayden definition. Any attempt to deliberately damage or destroy the computer networks of another country (Robinson et al., 2015). Clearly, this term is also quite broad and makes no distinction between cybercrime, cyber-attacks, and cyber warfare, and the line between their detection is hazy. The lack of such a distinction influences the actions of observers and policymakers. The broad structure of the rules of war leaves internet open, which can have harmful and negative effects for the development of war and country's aggressiveness (Edgar and Manz, 2017). Thus, the above definition's fundamental flaw is that definition is very general, which leads to a lack of success as a definition. The first definition limited the perpetrators of the attack to government aggressors. Unlike the first definition, the second definition is broad enough to be easily interpreted and, as previously stated, can be dangerous, have negative consequences, and cause confusion in bilateral relations, ultimately posing a threat to international peace.

Figure 2

Distinction between cyber-crime, cyber-warfare, cyberattack



Source: made by author

Table 2

Distinction between cyber-crime, cyber-attacks, and cyber-warfare (Dash et al., 2021)

Type of cyber action	Nature
Cyber-crime	Cyber actions taken only by non-governmental attackers. The cyber action is carried out by a computer system and is merely in violation of criminal law.
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network. The attack must have political or security purposes.
Cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an armed attack.

Source: made by author

Third expert is Martin Libicki and there are authors who did research based on Martin's Libicki definition. Virtual attacks on computer systems make the systems appear normal, but they actually produce and deliver false responses (Quigley et al., 2015). In truth, this definition of cyber-attacks excludes a wide range of possible risks to a country's national security if its cyber infrastructure has been targeted but not yet reached the degree and threshold of substantial attacks. The fact is that these threats have the potential to harm the target country's computer systems and

networks. As a result, any definition of a cyber-attack that excludes the abovementioned will inevitably be insufficient and lacking in comprehensiveness.

Tallinn Manual Group states that a cyber-attack is an offensive or defensive cyber activity that can result in personal injury or death, as well as property damage or destruction. The findings and impacts obtained are what makes this definition so odd. According to the authors of this definition, a cyberattack is of the kind of an attack if it causes personal and financial harm (Bullock et al., 2021). Thus, rather than the attacks themselves, the fundamental reason for defining this group is the result-oriented character of cyberattacks. Therefore, if this type of attack leaves objective and tangible effects and consequences of violence, it will be classified as an attack, and the rules of international law in related areas and fields (the right to appeal to coercion, the law of war, and the law of international responsibility) will be actionable.

The scale of global cyberspace, of course, creates overlapping and overlapping zones of control for national players with varying legal and cultural perspectives, as well as varying geopolitical goals. Countries all around the world have become so reliant on cyberspace for communications and real-world control that it is nearly difficult to remove themselves from it. As a result, cyberspace is progressively affecting each country's security tasks and functions (Zhao et al., 2020). It is impossible to establish guarantees in the product supply chain process due to worldwide software and hardware production. The cyber domain is fundamentally different due to its scalability. In the most extreme conditions, a bomb has a limited physical range; but cyber-threats have a vast range of consequences, therefore we have a system that can affect real-world operations. Cyberspace activities, like many other areas of knowledge, are governed by a limited group of people. Users have no control over or modification of the software or hardware they utilize. It is no surprise that just a few people are capable of properly controlling or managing cyber warfare (Zhang et al., 2021). The scattered nature of the cyber domain, despite the necessary concentration and specialized knowledge, prohibits a single person or group of individuals from gaining complete control.

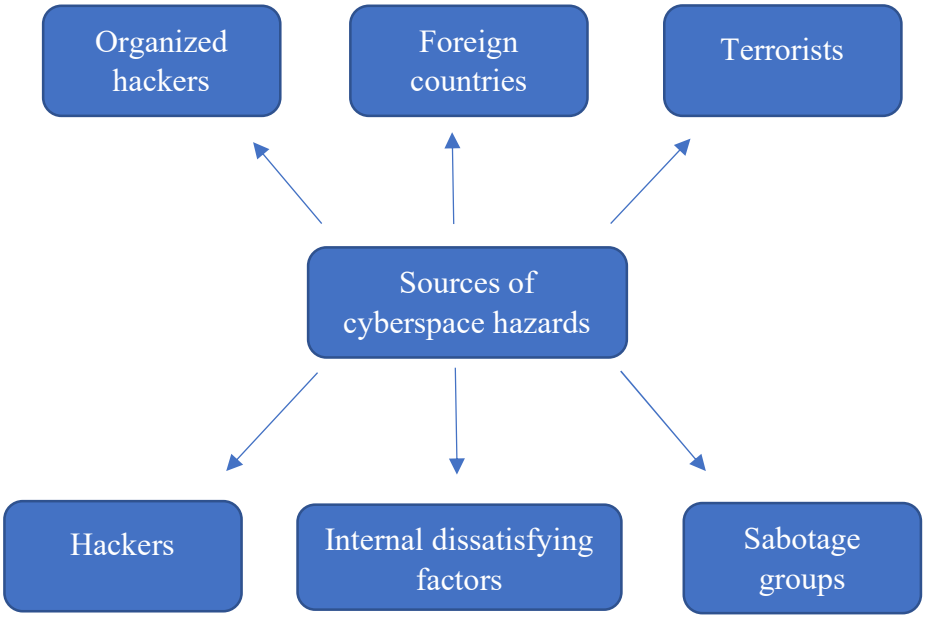
Changes in the cyber field happen quickly and are based on the continuous advancement of computing and communication technology. This velocity is accelerated by cyber cohesiveness. Each shift brings in a new period of vulnerability and reaction. Cyberspace is far from stagnant, and it is virtually constantly changing (Varga et al., 2021). Cyber assets are widely distributed across all types of organizations, ranging from closed and government-controlled systems to systems owned by the

commercial sector of society, all of which have various resources and facilities, as well as different capacities and concerns (Zhao et al., 2021). Due to the nature of cyberspace, there is currently no technical capability to confidently assign activities to individuals, groups, or organizations. Foreign threats, internal threats, threats in the supply chain of products and services, and risks owing to weak operational competence of local forces are the most common cyber threats (Al-Ghamdi, 2021).

Cyber tools are used by foreign intelligence services to carry out part of their intelligence collecting and spying activities. The misuse and destruction of countries' information infrastructures has been recorded in several cases around the world. Information infrastructures include computer systems, Internet information networks, and processors and controllers integrated in essential sectors. Groups of people that target cyber systems for monetary gain are another source of attacks, and these groups' attacks are rising (Beechey et al., 2021). Other organizations (hackers) also use the network to promote themselves occasionally. In the current environment, infiltrating networks with a minimum of knowledge and abilities is achievable by getting the appropriate tools and protocols from the Internet and utilizing them against other websites. Meanwhile, a politically motivated gang (dubbed Hacktivism) targets popular web pages or e-mail servers.

Figure 3

Sources of cyberspace hazards



Source: made by author

These groups typically raise the demand on e-mail servers, and they broadcast their political statements via infiltrating websites (Solomon, 2017).

However, inner unsatisfied agents operating within the organization are the primary source of cybercrime, and these agents do not require extensive knowledge of cyber-attacks because their target system awareness typically grants them unlimited access to hit the system or steal the organization's data. Terrorists are another source of danger, attempting to destroy, disable, or intentionally exploit essential infrastructure in order to jeopardize national security, inflict large losses, harm the country's economy, and erode public faith (Saxena and Gayathri, 2021). The sources of cyber risks are depicted in Figure 3.

Denial of service, logical bombs, abuse tools, Sniffer, Trojan horse, Virus, Worm, Send spam, and Botnet are some of the most common cyber-attack methods. Authorized users' access to the system and vice versa is denied using the Denial-of-Service approach. Indeed, the attacker begins by bombarding the target systems with diverse messages and obstructing the legitimate flow of data from a single point. This makes it impossible for any system to connect to the Internet or communicate with other computers (Topping et al., 2021). Instead of launching an assault from a single source, they strike from a huge number of spread systems at the same time, which is known as widespread Denial of Service. This is frequently accomplished by spreading worms over numerous computers in order to assault the target. Publicly available abuse tools can find and penetrate weaknesses in networks at various skill levels. A logic bomb is a sort of attack in which a programmer inserts code into a computer that, in the occurrence of a specified event, causes the program to do a harmful action automatically (Li et al., 2021; Marefati et al., 2018). Moreover, Sniffer is a software that tries to spy on routed data and examines each item in the data stream for particular information such as passwords (Patel et al., 2021). A Trojan horse is a malicious software that disguises itself as a useful application that the user is ready to run (Al Shaer et al., 2020). A virus can also contaminate system files, which are regularly used applications, by injecting a duplicate of itself into such files. These versions execute by loading infected files into memory, allowing the virus to infect other files. Viruses, unlike worms, need human assistance to spread. Contrary to virus, the worm is a self-replicating system software that copies itself from one computer to another on the network (Aziz and Amtul, 2019). Finally, a botnet is a collection of compromised remote control devices that are used to spread malware, coordinate assaults, spam, and steal data. Botnets are often installed discreetly on the target computer,

allowing an unauthorized user to remotely manipulate the machine in order to accomplish their malevolent intentions. Electronic warriors are another name for botnets (Kharlamova et al., 2021).

Qiu et al. (2021) used an unique scale to analyse spoofing data from two scales to investigate the impact and danger of cyber security in WAMS-based FFR (Fractional flow reserve) regulation. They also looked towards a cyber-security defensive architecture for the FFR system based on time–frequency. With genuine synchrophasor data, the outcome exhibited greater accuracy and robustness. Lee et al. (2021) created a knowledge-based hidden Makrove modeling technique for a unified cyber-attack response procedure. They also used updated HMMs to investigate a security state approximation approach. A case study was used to illustrate the validity of the established strategy. Zhang and Malacaria (2021) developed a cyber-security decision-making system that allows users to choose the best security portfolio for defending against multistage cyber-attacks. A LM was used to detect ongoing assaults, and the system contained both online and preventative improvements. They discovered that selecting effective solutions on the internet was a Bayesian STACKELBERG game. The cyber-attack potential factors for NPPs were investigated by Kim et al. (2020). In addition, AHP and FA were used to measure the comparative relevance of NPP potential factors. They discovered that the Korean cyber security approach had a higher preference for being used. Tosun (2021) demonstrated that cyber-attacks cause rapid negative shocks to a company's popularity. Furthermore, financial markets react to business security breaches by decreasing the total its return value. Furthermore, due to increasing selling pressure and higher liquidity, the trading rate climbed. Long-term, R&D and dividends decline, but target companies continue to compensate CEOs.

1.2. Cyber-security and its policy

Cyber security is a critical component of every company's or organization's infrastructure. In brief, a cyber security-focused firm or organization can attain high status and many achievements, because this success is founded on the company's capacity to secure private and consumer data from a rival. Customers and people are subjected to abuse by businesses and rivals. First and foremost, a firm or organization must give this protection in order to create and grow (Rodríguez-deArriba et al., 2021). Practical ways to secure information, networks, and data from internal and external threats are included in cyber-security. Networks, servers, intranets, and computer systems are all protected by cyber-security specialists. Only authorized personnel have access to the information, thanks to cyber-security (Ahmed Jamal et al., 2021). Knowing the different forms of cyber security is crucial for better

protection. Security on the Internet: Network security safeguards a computer network against threats such as virus and hacking. Network security refers to a collection of tools that allow businesses to keep computer networks safe from hackers, coordinated attacks, and viruses (Zhang, 2021). Application security is achieved by the use of hardware and software (such as antivirus applications, encryption, and firewalls) to secure the system from external dangers that might obstruct application development (Alkatheiri et al., 2021). Information security guards against unauthorized access, disclosure, misuse, unauthorized alterations, and deletion of physical and digital data (Ogbanufe, 2021). Processes and decisions taken to regulate and secure data are included in operational security. For instance, user permissions while accessing the network, or procedures that determine when and where information may be saved or exchanged (Ogbanufe, 2021). Cloud Security: Protects data on the cloud (based on software) and monitors to eliminate the possibility of on-site assaults (Krishnasamy and Venkatachalam, 2021). User training: This term refers to the unpredictability of cybersecurity, specifically individual users. A virus can be introduced into the security system by unintentionally. Any company's corporate security plan should include training on how to eliminate suspicious files from emails, how to avoid connecting to anonymous USBs, and other crucial concerns (Krishnasamy and Venkatachalam, 2021).

Any unlawful action involving a system, equipment, or network is considered cybercrime. There are two sorts of cybercrime: crimes that employ a system as a target and crimes that a system unwittingly contributes to. Cybercriminals utilize a variety of strategies. Any organization's security is founded on three principles: confidentiality, integrity, and availability. The security triangle, or CIA, is a set of three principles that have stood as the gold standard for system security from the earliest computer systems (Palmieri et al., 2021). Only authorized sources have access to sensitive information and functions, according to the concept of confidentiality. Example of confidentiality is military secrets. Only authorized persons and resources can alter, add, or remove sensitive information and functions, according to the integrity standards. For instance of integrity, a user inserts inaccurate data into a database. According to the Availability Principles, systems, functions, and data must be accessible on demand within agreed-upon parameters based on a service level agreement (SLA) (Nguyen and Golman, 2021). The most effective cybersecurity strategies go beyond the above-mentioned concepts. This simple protection can be bypassed by any experienced hacker. Cyber-security gets increasingly complex as an organization expands. Another cyber-security restriction is dealing with the expanding number of participants in the virtual and real worlds of data interchange. The lack of qualified workers to undertake the job is a significant barrier in cyber-security. Many

people with broad capabilities are at the lower end of the cyber-security vision. Coverage of cyberspace is a big topic. A comprehensive approach considers all of these factors and ensures that none are overlooked (Alzubaidi, 2021). The world's key infrastructure functions as a cyber–physical system. This amazing building provides us with several advantages. Using an online system, on the other hand, introduces a new susceptibility to hacking and cyber-attacks. The impact of assaults on an organization's performance must be included into the decision-making process. The security of online apps is viewed as the weakest location for assaulting an organization by several of the top new hackers. Excellent encryption is the foundation of app security. Every plan must be tailored to the specific needs of each company and implemented in a unique way. Hacking and penetrating information is thus made more difficult. Cyber-security is growing more complicated. Organizations must approach cyber-security from a "security perspective." As a result, to stay one step ahead of hackers, you must always maintain a high level of protection. Investment in cyber-security systems and services is increasing as a result of increased security efforts. McAfee, Cisco, and Trend Micro are the three corporations involved in this industry (Chandra and Snowe, 2020).

Over time, cyber has boosted the community's yield and successfully transmitted information. Increased output has always been considered, regardless of the application or industry cyber is employed in. Fast data transit to cyberspace reduces the overall security of the system. Security indicators often conflict with progress for technology professionals working to improve manufacturing because prevention indicators restrict, prohibit, or postpone user access, consume indicators that identify critical system resources, and react to management attention (Katrakazas et al., 2020). The system is upgraded to a more suitable and rapid system. Along with the cyber-security policy, there is a contradiction between the security situation and the desire for cyber performance. The term "policy" refers to information dissemination laws and regulations, private sector aims for data conservation, and system operations methods for technological control in a range of cyber-security contexts. Nevertheless, the phrase cyber-security policy is used for a variety of objectives in this subject. There is no established definition for cyber-security policy, just as there is no fixed definition for "cyberspace," but when this idea is used as an adjective in the field of policy, a common concept is intended (Tam et al., 2021).

The regulatory framework accepts the cyber-security policy, which is then applied solely to the regulator's relevant regions. The components of security policies differ depending on the policy spectrum (Cheng et al., 2020). For example, a national cyber-security policy covers all citizens and

maybe international businessmen working in the area, whereas corporate cyber-security only covers personnel who are employed or have a formal contract with the company and are expected to manage their behavior toward the organization. Unless a written contract is in place, it is impossible to expect resource suppliers who rely solely on one customer to comply to the customer security policy (Alghamdi, 2021). The aims of the applicable regulatory authority dictate the content of the security policy. The aims of national security differ significantly from those of business security. The implementing organizations will establish how the policy will be interpreted and registered, and the regulatory board and the components involved will decide how the policy will be approved. The method by which goals become policies and the process by which policies are enacted into legislation are two distinct processes in government. However, it is typical in businesses to have a centralized security section in control of cyber-security policy, standards, and solutions. The standards and solutions of a company's security section become the regulations' guidance. Since security is a key concern for the organization, the various internal units of the basic components wing issue cyber-security policies. Various shared components can occasionally reveal policy inconsistencies that arise from attempting to address these challenges at the same time (Quigley et al., 2015).

The country's cyber policy is now integrated into its national security strategy. Even if a country's cyber-security strategy is aligned with economic policy, these laws and regulations do not have the same level of sovereignty as the constitution. In reality, policy is developed and presented in papers and lectures after a series of deliberations and debates. Policies are made to help guide and make decisions about laws and regulations. The policy is not governed by any rules or laws. At their best, laws, agreements, and norms represent sound policy. Cyber-security enforcement orders, rules, and regulations, on the other hand, can be issued without the creation of a cyber-security policy (Sakhnini et al., 2021).

Different sections in the corporate environment are expected to respect the regulations for fear of penalty, which will continue until the delinquent sector closes. Human resource, civil, and costing regulations, for example, are coded to the point where non-compliance with notification rules terminates the appropriate area. Middle managers are expected to implement communication policies into departmental activities and produce indicators at the departmental level to assess policy compliance, as well as to support processes such as employing personnel or submitting expenses. Any sort of organizational subdivision in the public sector encounters governance constraints (Baig et al., 2017). There are some exceptions, such as when different sections of the information classification

are regarded extremely seriously, but the business security policy provided by the CEO applies to the entire firm, whereas the security policy issued by the CEO is confined to the domain. Personnel in the field of technology is useful. One of the most recent modifications in the organizational range is the hiring of a senior data security manager or a senior manager who is in charge of selecting various aspects of an organization's security condition. Furthermore, one of the disadvantages of corporate cyber-security policy vs human capital or legal policy is that it is entrusted to managers. When the danger of disclosure of private information is significant, information should not be shared without carefully analysing the recipient's ability to maintain information security, according to cyber-security policy (Arend et al., 2020). This policy delegated data risk assessment to a manager who may wish to cut expenses by outsourcing information flow to the office and using persons outside the office to conduct data analysis. Perhaps the same boss wants to avoid examination in order to save money. Such a circumstance may arise as a result of miscalculations of information duties toward someone who isn't a security professional, or the risk may be borne by the culture of the company in question. In every situation, task separation is critical. Because cyber-security measures have not progressed as far as accounting or human resource indicators, these scenarios become more complicated and difficult.

1.3. Price volatility in cryptocurrency markets

Bitcoin is a digital payment mechanism based on open source software. In reaction to perceived government and central bank failings during the 2008 global financial crisis and the European sovereign debt crisis (ESDC) of 2010–2013, its reputation among professionals and economic actors has surged. Whereas central banks and governments guarantee or control traditional currencies, Bitcoin is completely decentralized and relies on a complex system that controls transactions, manages supply, and prevents destructive behaviors that might jeopardize the system. All activities are electronically saved and documented in blockchain, a distributed ledger data technology. While the Bitcoin algorithm is a strong deterrent to counterfeiting, the system has been exposed to criminal activity, such as the large loss of 350 million USD worth of Bitcoins from the Mt. Gox market in February 2014. Dwyer (2015) describe the fundamentals of Bitcoin. Bitcoin was the very first cryptocurrency to be created. Other cryptocurrencies, such as Ethereum and XRP, have since emerged, but Bitcoin has managed to preserve its dominance in cryptocurrency market. Bitcoin's market capitalization surpassed $10 billion USD at the end of June 2016 (coinmarketcap.com), accounting for more than 80% of the total value of all cryptocurrencies on the market.

The concept of Bitcoin, its workings, its hazards, and its market history are all covered in this section. In 2008, Satoshi Nakamoto (2008) published a paper that served as the foundation for the first cryptocurrency, Bitcoin.

The major distinction between cryptocurrencies like Bitcoin and earlier digital currencies is the presence of a third party that verifies transactions (via the mining process) and prevents what is known as double-spending. Nevertheless, since bitcoin is decentralized (there is no need for a central bank), a peer-to-peer network may do this validation cryptographically using a proof-of-work mechanism that can be verified, trusted, and is irreversible.

A current bitcoin owner can transfer their holdings to another owner by recording the historical transaction history of those bitcoins and the new owner's public key in a digital ledger. Blockchain, which ensures that the transfer of Bitcoins is managed by a chain of transactions, records every transaction in a public ledger. When a transaction completes, it is collected into blocks that the peer-to-peer network software, which is intended to solve a cryptographic difficulty that arises as part of the proof-of-work system, nodes (anyone with the software and hardware may become a node), validate. This system makes it incredibly difficult and time-consuming to locate the solution to a problem. As a result, each time a node finds a solution, a new block is added to the blockchain, the only chain that contains all of the verified blocks and the only source of truth that can prevent double spending. An intriguing finding in the Bitcoin market is that the currency is notorious for its price volatility, which results in significant spikes in the current price followed by smaller but still significant losses.

The finance and economics debate on Bitcoin has escalated, in addition to the considerable literature on the legal and technical aspects of Bitcoin. According to Kristoufek (2014), Bitcoin is a one-of-a-kind asset that combines the characteristics of a traditional financial asset with those of a speculative asset. Popper (2015), on the other hand, views Bitcoin to be virtual gold, while Bouri et al. (2017) point out some of the benefits of Bitcoin as an asset. Some research have been interested in Bitcoin's 'moneyness,' regardless of whether it is a monetary or speculative asset, digital gold, or a commodity. Bitcoin, according to Yermack (2013), has no fundamental value and acts more like a speculative asset than a currency because its market capitalization is large in comparison to the economic transactions it supports. The author also finds that Bitcoin's utility as a currency is harmed by its volatility. According to Glaser et al. (2014), the majority of interest in Bitcoin stems from its

'asset' element rather than its monetary aspect. Hanley (2013) also claims that Bitcoin's pure market price vs conventional currencies is based on no intrinsic merit. Woo et al. (2013), on the other hand, suggest that Bitcoin has some fair value because of its money-like features. According to Garcia et al. (2014) and Hayes (2016), the expense of mining a Bitcoin adds some intrinsic worth to Bitcoins. Woo et al. (2013), on the other hand, suggest that Bitcoin has some fair value because of its money-like features. According to Garcia et al. (2014) and Hayes (2016), the expense of mining a Bitcoin adds some intrinsic worth to Bitcoins. Other research has looked into the Bitcoin market's price determination. According to Kristoufek (2013), there is a strong bidirectional causation between Bitcoin values and Bitcoin search searches on Google Trends and Wikipedia. Bouoiyour and Selmi (2015) show that a delayed Google search for the word "Bitcoin" plays a substantial role in describing the Bitcoin price, whereas Bitcoin velocity as defined by transaction data fails to explain the Bitcoin price. Polasik et al. (2015) reveal similar findings on the involvement of the two above-mentioned factors (the frequency of daily Bitcoin queries on the Internet and the amount of Bitcoin transactions) in determining the Bitcoin price. In the same way, Kristoufek (2014) discovers that the trade-exchange ratio is crucial in determining Bitcoin price changes in the long run. The exchange-trade ratio is used by Bouoiyour et al. (2015) to evaluate the relationship among Bitcoin price and transactions. In the short and medium term, the authors discover that Bitcoin price Granger causes an exchange-trade ratio. Similar to Kristoufek (2014), they demonstrate that rising the usage of Bitcoin in the exchange-trade ratio raises the value of Bitcoin in the long run. Authors also indicate a strong correlation between the exchange-trade ratio and the Bitcoin price. Ciaian et al. (2016) published an article on the factors that influence Bitcoin price volatility. It indicates that the overall number of distinct Bitcoin exchanges per day (a demand side variable) has a greater influence on Bitcoin price than the amount of Bitcoins (a supply side variable). As the Bitcoin is considered to be the most popular cryptocurrency, there are more other cryptocurrencies and cryptocurrency market is growing everyday.

The continuing expansion of cryptocurrencies and the fundamental markets on which they are traded has increased our awareness. It is urgent to understand a product that has been highlighted as a potential improvement to and replacement for traditional cash as we know it. One significant area of research focuses on the connections between cryptocurrencies and other more traditional financial markets, as our knowledge of FinTech grows (Goldstein et al., 2019) and the expanding importance of blockchain (Chen et al., 2019). Urquhart and Zhang (2019) examined the link between Bitcoin and currencies on an hourly basis and discovered that Bitcoin may be used as an intraday hedge for the

CHF, EUR, and GBP, but it can also be used as a diversifier for the AUD, CAD, and JPY. The authors also discovered that Bitcoin operates as a safe haven for the CAD, CHF, and GBP during instances of significant market turbulence. This backs up Sensoy's (2019) findings that both markets have gotten more informationally efficient over time, as well as Vidal-Tomás and Ibaez's (2018) study of Bitcoin's semi-strong efficiency in the Bitstamp and Mt.Gox exchanges. Guesmi et al. (2019) investigated the conditional cross effects and volatility spillovers between Bitcoin and other financial assets, demonstrating that Bitcoin can provide investors with diversification and hedging opportunities, whereas Ciaian et al. (2018) used an Autoregressive Distributed Lag model to investigate interconnections within the cryptocurrency market. Bouri et al. (2017) used data from July 2011 to December 2015 to see if Bitcoin might operate as a hedge and safe haven for key international stock indexes, bonds, oil, gold, the general commodities index, and the US dollar index using a dynamic conditional correlation model. They discovered that Bitcoin is a poor hedge and should only be used for diversification. Corbet et al. (2018) discovered evidence of these assets' relative isolation from financial and economic assets, as well as the possibility that cryptocurrencies might provide diversity benefits for investors with short investment horizons. External economic and financial shocks cause changes in the connections over time. Corbet et al. (2018) believe that the introduction of Bitcoin futures and the ability to trade them would have led to reduction in the variation of Bitcoin prices, or allowed hedging methods that may have alleviated pricing risk in the spot market. According to the authors, Bitcoin might have served as a unit of account, bringing it closer to becoming a currency.

Market efficiency can be defined by a variety of factors; however, the market efficiency of cryptocurrencies can be measured by a number of progressive factors, such as the existence of a new futures exchange, liquid cross-currency indices, and the relative reduction of intra-day volatility, though daily volatility remains high. In this section, we divide market inefficiency into two categories: product efficiency and pricing efficiency. Bouoiyour and Selmi (2015) employ ARDL bounds testing to demonstrate Bitcoin's highly speculative behavior, as well as its limited use in trade transactions, while ignoring its reliance on the Shanghai Stock Exchange and hash rate. The authors found no evidence that Bitcoin provides a safe haven, but Roth (2015) used the Systems Modelling Language to study the architectural structure of Bitcoin using a functional analysis (SysML). Urquhart (2016) was the first to look at the market efficiency of Bitcoin, and he discovered that it was inefficient in a series of tests, however it was growing less inefficient with time. Biais et al. (2019) discovered that splits can result in abandoned blocks and persistent deviation, which can be caused by a variety of circumstances such as information delays and software updates. Bariviera et al. (2017), Brauneis and

Mestel (2018), Sensoy (2019), Tiwari et al. (2018), and Vidal-Tomás and Ibaez (2018) are examples of follow-up research that employed a variety of various testing methodologies and data sets to support the finding of Bitcoin's inefficiency. Urquhart (2018) discovered that realised volatility and the amount of Bitcoin transacted, both controlled for Bitcoin fundamentals, are both major drivers of the next day's interest for Bitcoin using a large database spanning 2010 to 2017. Volume cannot assist predict the volatility of Bitcoin returns at any point on the conditional distribution, according to Balcilar et al. (2017), but volume can predict returns, excluding Bitcoin, bull, and bear market regimes. Furthermore, Corbet et al. (2018), using Phillips et al. (2011)'s bubble detection approach, discovered clear evidence of occasions when Bitcoin and Ethereum suffered bubble phases.

Hu et al. (2018) investigated the price clustering of non-fiat cryptocurrency exchange rate pairings to look at intra-day price behavior of Bitcoin, Litecoin, and Ripple. The data show strong price clustering at the round numbers 00, 000, and 0000, supporting the negotiating hypothesis that more clustering indicates higher pricing and price volatility. Further, Koutmos (2018) discovered that a one standard deviation shock to transaction activity results in a return gain of little over 0.30 percent on the third day after the shock. However, on the sixth day following the shocks, the data show a turnaround in this tendency. During bubbles, Fry and Cheah (2016) looked for contagion and discovered a spillover from Ripple to Bitcoin. The latter research, on the other hand, solely looked at Bitcoin and Ripple. Ardia et al. (2018) also demonstrated the existence of structural breakdowns in Bitcoin volatilities, using a two-regime MSGARCH model that used in-sample forecasting performance with an inverted leverage effect in low- and high-volatility regimes. In terms of liquidity, Wei (2018) provided evidence that return predictability decreases in cryptocurrencies with significant market liquidity, adding to the disputes about cryptocurrency efficiency and liquidity. Although there is minimal study on the correlations between traditional financial market work hours or trading times and the volatility of cryptocurrency markets, also there is a gap in research on day-of-week impacts within those new digital assets.

1.4. Impact of criminality on price volatility in cryptocurrency markets and GARCH model

However, cryptocurrencies as a new asset class are not without significant drawbacks, notably in terms of providing a platform for criminal activity and, indeed, massive cybercrime incidents.

While there is great dispute about how this commodity should be controlled, there are several ways through which crime might flourish and prosper. It is seen a number of quite clever, high-value

hacking instances, both at the exchange level and with individual cryptocurrencies. Each occurrence erodes trust and confidence in this asset class even further. Moreover, the very structure of cryptocurrencies has created a unique and efficient route via which both illegal finances and, indeed, criminal cross-border transactions may be readily carried out, despite the fact that traditional assets have flaws. Due to the general increased potential for criminality and malpractice, regulatory organizations and policymakers have viewed the emergence of cryptocurrencies with some skepticism. According to Foley et al. (2019), bitcoin is involved in roughly $76 billion in criminal behavior each year (46 percent of bitcoin transactions). This is thought to be in the same location as the illicit drug marketplaces in the United States and Europe, and is known as 'black e-commerce.' While Chu et al. (2017) and Phillip et al. (2018) investigated the volatility of cryptocurrency price returns, the possibility for market manipulation appears to have been widely discovered in cryptocurrency cross-correlations and market interdependencies. Griffins and Shams (2018) examined at whether Tether affected Bitcoin and other cryptocurrency values, and discovered that Tether purchases were timed to coincide with market downturns, resulting in considerable rises in the price of Bitcoin. Furthermore, fewer than 1% of the hours during which Tether had substantial transactions are linked to 50% of the increase in Bitcoin prices and 64% of the growth in other prominent cryptocurrencies, implying that Tether was utilized to offer price support and influence cryptocurrency prices. Gandal et al. (2018) also recognized the influence of unusual trading behavior on the Mt.Gox Bitcoin exchange hack, which resulted in the theft of around 600,000 Bitcoins. The authors showed that suspicious trading was most likely to blame for the price surge in late 2013 from $150 to $1,000, which was most likely driven by a single individual. These two important studies have narrowed the attention of regulators, policymakers, and academics alike, as the future expansion of cryptocurrencies cannot be supported while such critical problems of irregularity remain unaddressed.

Whereas these harmful researches continue to grow and highlight significant difficulties within the cryptocurrency markets, we also take into account the findings of several assessments of harmful manipulation tactics based on traditional financial markets. 'Pump-and-dumps' and 'spoofing,' both listed under the criteria of unlawful price manipulation as defined by Kyle and Viswanathan (2008), have been noted as two of the most troublesome concerns when concentrating on cybercriminality and the questionable market interactions that exist. According to Putnins (2012), there are three distinct routes on which we should develop in order to minimize risks from market manipulations: 1) more complete data collection, 2) detection controlled estimating approaches, and

3) controlled tests. Sabherwal et al. (2011) looked at the material on stock message boards to see whether they could uncover evidence of the most typical manipulation pattern for tiny businesses with weak financials, and they found significant evidence of a two-day boost followed by a two-day drop manipulation pattern. The attitude on internet forums has been discovered to be a significant predictor of trading-related activity.

Clarkson et al. (2006) evaluate the market response to acquisition speculation posts on the Hotcopper Internet Discussion Site (IDS) using an intra-day study. They show anomalous returns and trade volumes during ten-minute reporting periods, as well as unusual trade in the ten minutes prior to the announcement. The results demonstrate that the marketplace has expected and reacted to the announcement. It is an instance of a 'pump-and-dump,' which is a plan that aims to increase the price of a stock by making suggestions based on inaccurate or deceptive claims. The criminals are more likely to have a long position in the company's shares and sell it once the excitement has caused the stock price to rise. They have been found to be exceedingly harmful to the financial market's operation. When mining, it's vital to note that Chiu and Koeppl (2019) forecast net increases of 1-4 basis points for US corporate debt market yields. Diaz et al. (2011) address the difficulties of using data mining tools to discover stock value manipulations and expands prior findings by including intra-day transaction price research. Additionally to closing prices for the analysis of exchange-based manipulations, the authors extend earlier conclusions on the topic by analysing empirical proof in regular and manipulated hourly data. They also look at the specific peculiarities of intra-day trading that occur during suspicious hours. According to Zaki et al. (2011), a study on detecting fraud via data mining algorithms helps analysts discover suspected cases of bragging depending on spam messages. Their studies clearly indicate that knowing the cumulative impact of 'stock touting' spam emails is critical to understanding the patterns of manipulation involved with touting email campaigns. In addition, authors‘ findings suggest that data mining techniques can be utilized to speed up spam email fraud investigations. Spoofing is a kind of fraud in which an attacker pretends a user in order to gain unauthorized access to the victim's system or information. The main goal is to deceive the user into disclosing sensitive information in order to get access to the user's bank account, personal computer, or private information such as passwords. This approach may happen on a variety of platforms and products; however, little research has been done on bitcoin marketplaces to date. Lee et al. (2013) look at how traders spoof the financial markets by placing orders that have a low likelihood of being filled but fool other traders into believing there is an order book imbalance. In a proprietary data set, the researchers use intra-day transaction and transaction data from the Korea Exchange (KRX) to

accurately identify accounts. Investors carefully place spoofing orders, which, given the KRX's order-disclosure requirement at the time, generates the appearance of a significant order book discrepancy, with the purpose to affect following prices, according to the findings. There are two more studies that look into the effects of issues like spoofing. Cumming et al. (2011) examines the exchange market rules based on the market fraud, insider trading, and broker-agency disputes. While O'Hara (2015) investigates large market microstructure and dynamics.

Furthermore, key dangers to bitcoin are described. Hackers, fraud, and malware pose the biggest and most significant external threat to Bitcoin. An example is the aforementioned Mt. Gox disaster, which involved hackers forcing the company to close and declare bankruptcy. Additionally, the absence of national and international regulation of Bitcoin creates room for fraud and other illicit activity. The total number of 21 million Bitcoins is a significant risk. As more Bitcoins are created, the number of transactions would decline, which would lower the fees that miners are paid, diminishing their incentive and raising the potential of what are known as "attacks from history-revision." There might be a significant issue of losing your Bitcoins and not being able to get them back. This can take place if you misplace your Bitcoin electronic wallet, or it can also occur when e-wallet management providers make mistakes.

Theoretical knowledge of a comparatively recent financial instrument is frequently linked with significant contradicting evidence. The asset class of cryptocurrencies is no exception. Nevertheless, many studies, such as Corbet et al. (2018), continues to demonstrate that when compared to more proven alternatives, this asset class has extraordinarily high levels of volatility. The cause of this cryptocurrency market volatility is critical to understand, especially as regulators, policymakers, and experts attempt to assess, control, and determine on the cryptocurrency‘s future viability. Cybercriminality has been cited as one of the fundamental concerns eroding the viability of digital currency as 'the future of finance' (Corbet et al. (2018); Gandal et al. (2018)). There are known flaws at the exchange level, in the underlying technology, and, most dangerously, in the trading structures of these assets, such as 'spoofing' and 'pump-and-dumps.' After identifying both volatility and non-volatility effects, we set out to see if cybercrime is one of the key driving causes behind cryptocurrency volatility. Furthermore, I am seeking to see if cryptocurrency investors place different values on different types of cybercrime.

The literature statistically analysing price volatility in cryptocurrency markets is substantial. However, there appears to be little literature on GARCH modeling of cryptocurrencies, with the exception of Bitcoin. Chu et al. (2017) focus on the seven most popular cryptocurrencies which are the subject of the first GARCH modeling. In their research, each cryptocurrency is fitted with twelve GARCH models, which are evaluated according to five criteria. The best-fit models, projections, and acceptability of value-at-risk estimations are used to derive conclusions. In terms of modeling the volatility in the most popular and largest cryptocurrencies, they find that the IGARCH and GJRGARCH models provide the greatest matches.

The Bitcoin market, in particular, has experienced tremendous growth lately. Because Bitcoin is mostly used for investing, determining its volatility is critical. Katsiampa (2017) studied the ability of multiple competing GARCH-type models to explain Bitcoin price fluctuations. Author discovered evidence that the AR-CGARCH is the best model for data goodness-of-fit, implying the relevance of having both a short-run and long-run component of conditional variance.

Moreover, Baek and Elbeck (2015) use daily return data from Bitcoin and the S&P 500 Index to assess relative volatility using detrended ratios. The drivers of Bitcoin market returns are then studied by modeling Bitcoin market returns with specified economic variables. Using core economic variables, authors perform a regression analysis. Heteroscedasticity and autocorrelation consistent (HAC) covariance estimator by Newey–West are included into the research. Bitcoins are 26 times more volatile than the S&P 500 Index, according to their data. They also look at the factors that influence Bitcoin market returns. The regression results show that Bitcoin returns are driven internally by buyers and sellers and are not influenced by macroeconomic factors. However, as Bitcoin adoption develops, lower volatility and increased market and economic influence, resulting in a more balanced internally and externally driven investment vehicle is anticipated. Thus, there is a solid evidence that Bitcoin volatility is driven internally (by buyers and sellers), leading to the conclusion that the Bitcoin market is now highly speculative.

2. METHODOLOGY FOR RESEARCHING THE IMPACT OF CYBERATTACKS ON PRICE VOLATILITY IN CRYPTOCURRENCY MARKETS

In this section, the methodology and models used for the analysis are explained. The analysis of scientific literature carried out in the first part showed that in order to solve this price volatility in cryptocurrency markets due to cybercriminality scientific problem, the most suitable research method is Generalized AutoRegressive Conditional Heteroskedasticity (GARCH). GARCH model approach is chosen due to its ability to calculate the return volatility of stocks, bonds, and other financial instruments and to estimate the volatility of financial markets. When projecting the values and rates of financial instruments, the GARCH process provides a more precise framework than other models. My aim is to investigate the features of cyberattacks and their influence, dynamics on cryptocurrency market price volatility. To achieve this aim, GARCH methodology is chosen. The analysis includes thirteen variables measured daily data from September 1st 2017 to Ocotber 31st 2022.

2.1. Aim and hypotheses of the research

The main aim of this thesis is to research the characteristics of cyberattacks and how they affect the dynamics of the price volatility in the cryptocurrency market. In other words, the main interest is to identify the elements of cyberattacks and investigate how price volatility in the cryptocurrency market is impacted by cybercriminality. To achieve the aim, the following hypothesis for testing are set:

H1: Has there been a significant difference in cryptocurrency volatility during moments of traditional market volatility?

H2: Is there a significant shift in cryptocurrency market volatility as a result of cybercrime?

H3: Is cryptocurrency volatility affected by the seriousness of a cybercrime?

H4: Do conditional relationships between cryptocurrency markets alter significantly as a result of cybercrime events?

2.2. Data of the research description

This section presents the data of the analysis while also referencing its sources. In this research, I am focusing on cryptocurrencies and five traditional financial markets. In total thirteen different variables are used. In order to execute the analysis, the eight most liquid cryptocurrencies are decided to use: Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Monero, Cardano, and Bitcoin Cash. The same cryptocurrencies are also chosen by the other authors. I include the five following variables, which represent traditional financial markets, into analysis: 1) GBP/USD; 2) VIX; 3) Gold; 4) the S&P500; and 5) Oil as measured by West Texas Intermediate. The final choice of traditional financial market assets was based on giving a broad representation of equities, commodities, currencies, and options, while examining an extremely large number of goods. As a result, variable GBP/USD is chosen to represent cryptocurrencies and broad currency markets, the S&P500 selected to represent stock market performance, gold and oil (as measured by West Texas Intermediate, WTI oil markets) to represent commodity markets, and the VIX (CBOE volatility index) used to represent options markets and implied volatility, respectively.

Bitcoin is included in the analysis because it is the biggest blockchain-based digital asset. Those that are interested in cryptocurrencies and speculators find it to be incredibly popular. This digital asset has attracted significant investment from rich businesspeople and entrepreneurs. Ethereum is taken into consideration in the analysis since it allows flexibility and increases its functionality. The ETH project was developed to expand functionality and provide for versatility on a blockchain, allowing for the decentralized programming of various smart contract types in the ETH system. Because of the flexibility that ETH smart contracts provided, ETH drew a lot of developers, users, and investors, making it the second most popular cryptocurrency. ETH is a result and not meant to be used as money. Each updated member in the blockchain verifies the execution of a contract. This is done in order to ensure that the blockchain's consensus process is carried out correctly. Ethereum and Bitcoin are essentially distinguished by the Turing programming language, which enables anybody to construct contracts for any purpose. In terms of market value, the cryptocurrency Ripple, commonly known as XRP, is the fourth largest cryptocurrency on the market and it is one of the reason why ripple is chosen. An open-source Internet program called XRP enables users to send payments across international borders in several currencies in a relatively simple manner. As a result,

XRP has the benefit of providing additional currencies in addition to its own cryptocurrency for use in transactions. Additionally, the XRP protocol makes use of a distributed ledger, a group of up-to-date financial accounts, to enable users of XRP to send payments across borders that are quicker, less expensive, and more effective than conventional payments. The key distinction between bitcoin and Ripple is that although payments in Ripple are made from a single account as input, transactions in Bitcoin can be completed from several accounts.

It is crucial to include variable S&P 500 in the model sincet the 500 largest publicly traded firms in the United States make up the S&P 500 stock index, which is weighted based on each company's market capitalization. The term S&P 500 stands for the Standard & Poor's corporation. It is weighted using a float weighting method, which means that the market capitalization of each firm is modified in accordance with the quantity of shares that are offered for public trade. Additionally, the index is regarded as the strongest predictor of large capitalization equities in the United States, and as a result, numerous funds are established to monitor the behavior.

Moreover, research incorporates variable gold. The reason is that over time, gold has developed into a traded asset that retains its worth during unrest, making it a safe haven of value. Some of the main elements that influence the price of gold include: national interest rates, as gold prices tend to fall as they rise. Also, geopolitical events also have an impact on gold's price; during times of global unrest, investors tend to purchase the metal in order to have a high level of protection in uncertain times. Additionally, industrial production has an impact on gold prices as well since as production rises, so does demand, and vice versa. hase the commodity during times of international tension in order to have a high level of security.

Furthermore, the Cboe Volatility Index (VIX) is a real-time index that gauges the level of risk or anxiety in the market by reflecting estimates for volatility over the next thirty days. It is important to realize that it calculates volatility over the following 30 days. In other words, it measures prospective volatility rather than previous volatility. Low values of the indicator are known to result in periods of market tranquillity and long-lasting upward trends. High readings, on the other hand, signify panicky periods where a long-term downturn or downtrend is accelerated. It serves as a better gauge of investors' dread of potential declines than it does of their complacency during a market upturn. Generally, the VIX and the stock market are inversely related. The VIX increases as stock prices decline and vice versa. Consequently, a rise in equities will be viewed as having a lower risk

factor. Conversely, if it is bearish and equities decline, the danger is greater. The volatility increases in direct proportion to perceived danger. Therefore, this volatility is more sensitive to market direction.

Table 3

Selected variables for the analysis

Variable	Description	Source
BTC	Bitcoin	CoinMarketCap
ETH	Ethereum	CoinMarketCap
LTC	Litecoin	CoinMarketCap
XRP	Ripple	CoinMarketCap
XLM	Stellar	CoinMarketCap
XMR	Monero	CoinMarketCap
ADA	Cardano	CoinMarketCap
BTC_cash	Bitcoin Cash	CoinMarketCap
GBP/USD	GBP/USD	National Association of Securities Dealers Automated Quotations (NASDAQ)
VIX	CBOE Volatility index	Chicago Board Options Exchange (CBOE)
Gold	Gold	Chicago Board Options Exchange (CBOE)
S&P500	The S&P 500	S&P Dow Jones Indices LLC
Oil	Oil measured by West Texas Intermediate (WTI)	U.S. Energy Information Administration

Source: made by author

Volatility rises as a result of a downward shift or fall. The VIX typically has a level between 20 and 30. Below 20, investors get complacent and unconcerned. A reading of greater than 30 denotes market nervousness, or panic.

All chosen variables for the research are summarized table 3. Table 3 reports variables, descriptions and sources.

As for the frequency and time frame, I select daily data and the time interval from September 1st, 2017 through October 31st, 2022 as the period of interest for measuring the cryptocurrencies volatility and effects of the cyberattacks on cryptocurrency market. This time period was chosen because it provided the greatest amount of observations across all of our markets. The 1st of September, 2017 is selected as a starting point based on other authors‘ researches. The chosen period incorporates and reflects some of the biggest crypto hacking events. I believe the selected time period and frequency generates a sufficient amount of datapoints in the analysis.

The primary method of collecting data is quantitative, as this paper relies on statistical and numerical analysis. To describe the cryptocurrency market and impact on it of cybercriminality, descriptive method is used, also analysing and comparing results. I use software EViews for all calculations, estimations and figures.

The cryptocurrency data used for the study is sourced from the one if the four most popular cryptocurrency market database CoinMarketCap. CoinMarketCap is well-known database of cryptocurrency and token prices for being the source to go to monitor the price of cryptocurrencies and tokens. Binance, an international cryptocurrency exchange founded by Changpeng Zhao in China in 2017, just acquired CoinMarketCap. In the CoinMarketCap, the daily closing values of various cryptocurrencies are accessible to the general public and US dollars are used to list the prices. CoinMarketCap database was selected due to availability of providing data for free on numerous listed coins, including their price, available supply, trade volume, and market capitalization. Prices are obtained by weighting the prices at the major exchanges. In other words, results are provided by the website based on price computation using the volume-weighted average of values from several exchange marketplaces. Price is multiplied by total supply to calculate market capitalisation. The variables reflecting selected traditional financial markets were collected from these sources: VIX and Gold from Chicago Board Options Exchange (CBOE), Oil is sourced from U.S. Energy Information Administration, S&P 500 from S&P Dow Jones Indices LLC and GBP / USD is from National

Association of Securities Dealers Automated Quotations (NASDAQ) Stock Market. The above mentioned sources are selected for the traditional financial markets variables due to being trusted, largest and most reliable markets in the world.

2.3. The GARCH model

Based on the literature review in the first part and other authors‘ researches, in this thesis, GARCH methodology developed by Bollerslev (1986) is applied. The GARCH(1,1) model was determined to have the best fit for estimating volatility effects through the inclusion of dummy variables that signify both the time of day and times of significant conventional market volatility in specification tests. Additionally, the GARCH (1,1) model was found to be the best fit for estimating volatility impacts after industrial incidents for publicly traded companies in specification tests. For each of the time series variables, a GARCH is used to estimate expected return and conditional volatility. Moreover, GARCH models explain financial markets in which volatility fluctuates, becoming more volatile during financial crises or global events and becoming less volatile during periods of relative calm and stable economic growth. Additionally, advantages of using GARCH models are simplicity, generating volatility clustering and heavy tails (high kurtosis). On the other hand, there is no ideal econometric model. Some of the weaknesses of GARCH include symmetricity between positive and negative prior returns and restriction. However, the component GARCH structure has the advantage of being easier to interpret than the GARCH(2,2) model, making it easier to come up with suitable initial values for the parameters.

The aim is to obtain volatility fluctuations in the immediate aftermath of a significant cybercrime incident involving cryptocurrency markets. I have chosen this model because GARCH(1,1) processes are often used to represent daily financial returns and estimate volatility. I examine whether periods of high volatility in traditional financial markets have had an impact on cryptocurrency volatility. The GARCH specification is created to incorporate lagged conditional variance terms as autoregressive terms. The general GARCH (p,q) model has the following form:

$$R_t = a + b_0 X_t + \varepsilon_t, \text{ where } \varepsilon_t | \Omega_t \sim iidN(0, h_t) \quad (1)$$

$$h_t = \omega + \sum_{i=1}^{p} \alpha_i h_{t-i} + \sum_{j=1}^{q} \beta_j \varepsilon^2_{t-j} \quad (2)$$

This form indicates that the value of the variance scaling parameter h_t now depends on both the past value of the shocks, which is described by the lagged square residual terms, and the past value of itself, which is recorded by the lagged h_t terms. International impacts must also be mitigated, which may be done by include the returns of traditional financial instruments in the mean equation of the GARCH(1,1) technique. In the volatility estimation of the chosen structure, the volatility sourced in shocks that are included in the returns of traditional financial markets is taken into account. Thus, I reduce foreign effects by including traditional financial product returns. Five markets have been chosen to reflect traditional financial markets: 1) GBP/USD; 2) VIX; 3) Gold; 4) the S&P500; and 5) Oil as measured by West Texas Intermediate. Traditional financial markets are included in the mean equation of the GARCH(1,1) methodology, which takes the form:

$$R_t = a_0 + b_j R_{t-j} + b_2 £/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + \sum_{i=1}^{17} D_i + \varepsilon_t \quad (3)$$

$$\varepsilon_t | \Omega_t \sim iidN(0, h_t) \quad (4)$$

$$h_t = \omega + \alpha_i h_{t-i} + \beta_1 u^2_{t-1} \quad (5)$$

R_{t-j} represents the lagged value of cryptocurrency returns, n observations before R_t is observed. $b_2 £/\$_t$ represents the interaction between the selected cryptocurrency returns and £/$, while $b_3 VIX_t$ describes th value of VIX in the hour that the estimate R_t was observed. Moreover, $b_5 S\&P_t$ and $b_6 Oil$ represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through West Texas Intermediate (WTI). $\sum_{i=1}^{17} D_i$ is included to provide a coefficient relating to the included dummy variables indicating cybercriminality. Bollerslev (1986) demonstrated that parameters for positivity can be restricted and the wide-sense stationarity condition, $\alpha+\beta<1$. Nelson (1990) proved that the GARCH (1,1) process is uniquely stationary if where Bougerol and Picard (1992) generalise this for any GARCH (p,q) order model.

Thus, GARCH type models are popular when investigating Bitcoin and other cryptocurrency price volatility. Because GARCH(1,1) processes are commonly used to depict daily financial returns and assess volatility, this model is chosen in this thesis. I investigate whether extreme volatility in traditional financial markets, which reflect the periods of cyberattacks, has influenced cryptocurrency volatility.

Also, a DCC-GARCH model developed by Engle and Sheppard in 2001 will be used to examine the dynamic correlations. Since the full conditional matrix of variance and covariance of a specific portfolio can be calculated using the conditional correlations and the conditional volatility, this sort of model is a frugal choice to model portfolios with a large number of assets.

Table 4

Cryptocurrency hacking events used to investigate the differences in price volatility

Hack	Date	Time	Amount	Market	Description
1	November 7, 2017	11:51	$280 m	Ethereum	The money were essentially frozen when a user tinkering with the Parity multisig wallet library contract activated its kill mechanism.
2	November 21, 2017	04:15	$30 m	Tether	$30,950,010 USDT, according to Tether, was transmitted to an unauthorized bitcoin address.
3	December 6, 2017	10:45	$64 m	Bitcoin	NiceHash suffers a service breach and a hack.
4	December 18, 2017	21:35	$37 m	Bitcoin	Youbit's official website posted a notice stating that at about 4:34 a.m. local time, an external hack caused the loss of roughly 17% of all assets.
5	January 13, 2018	12:00	$0.4 m	Stellar	Hackers have taken Stellar Lumen (XLM) currencies worth $400,000 without the owner's consent from wallets hosted by Blackwallet.co as a result of a DNS hijack.
6	January 26, 2018	15:00	$532.6 m	NEM	Coincheck halted all NEM deposits on their exchange on January 26th.
7	January 31, 2018	20:22	$0.9 m	BeeToken	The cryptocurrency firm BeeToken was compromised while phishing assaults were used to target its ICO.
8	February 5, 2018	17:00	$1.8 m	Ethereum	Investors in the Seele ICO were defrauded of roughly $2 million by fictitious administrators.
9	February 8, 2018	12:00	$ 195 m	Nano	Exchange fraud.
10	February 15, 2018	09:00	$50 m	Bitcoin	Over a three-year span, a big swindle generated $50 million in cryptocurrencies.
11	March 4, 2018	17:41	$50 m	Bitcoin	BTC Global was a fraud that trader Steven Twain, who claimed to be well-known, started in September 2017.
12	April 5, 2018	12:00	$300 m	Bitcoin	GainBitcoin started as a multi-level marketing (MLM) scam in 2015 and attracted over 100,000 investors who were all given the assurance that they would get monthly returns of 10% on their investment.
13	April 9, 2018	12:00	$650 m	Initial Coin Offering (ICO)	Two blockchain companies, Ifan and Pincoin, are accused of pulling off the biggest alleged ICO fraud in Vietnam.
14	April 19, 2018	09:00	$20 m	Bitcoin	The scam was founded in 2015 by two men, who then created a multi-level business by promising investors large profits by investing in bitcoin.
15	June 10, 2018	17:00	$40 m	Pundi X (NPXS)	Conrail claimed that it had halted operations as a result of the theft of ERC-20 tokens from the platform.
16	June 16, 2018	07:33	$31.5 m	Ethereum	Bithumb recently observed unusual access, therefore it transferred a significant quantity of ethereum to its cold wallet.
17	July 9, 2018	21:35	$23.5 m	Ethereum	A security flaw at Bancor's hot wallet that was used to update smart contracts on its exchange led to the loss of almost $23.5 million worth of Ethereum.

Source: made by author. Seventeen biggest cryptocurrency hacking events

The DCC-GARCH is expressed:

$$r_t = \mu_t + a_t,\ a_t = H_t^{1/2} z_t \qquad (6)$$

$$\boldsymbol{H_t = D_t R_t D_t} \qquad (7)$$

where, $\mathbf{r}_t$ is the n x 1 vector of log returns of n assets at time t, $\boldsymbol{a_t}$ the k x1 vector of mean-corrected returns of n assets at time t, i.e. $E[\boldsymbol{a_t}] = 0$. $Cov[\boldsymbol{a_t}] = \mathbf{H}_t$, μ_t the k × 1 vector of the expected value of the conditional r_t, $\mathbf{H}_t$ the k × k matrix of conditional variances of $\boldsymbol{a_t}$ at time t, $H_t^{1/2}$ any k × k matrix at time t such that $\mathbf{H}_t$ is the conditional variance matrix of $\boldsymbol{a_t}$, $\mathbf{D_t}$ the k × k, diagonal matrix of conditional standard deviations of $\boldsymbol{a_t}$ at time t, $\mathbf{R_t}$ the k × k conditional correlation matrix of $\boldsymbol{a_t}$ at time t, and z_t the k × 1 vector of IID errors such that $E[\mathbf{z_t}]=0$ and $E[\mathbf{z_t z_t^T}] = I$.

It is important to note that the GARCH models have different orders; normally, the GARCH (1,1) model is the simplest and is the most suited. The ARCH effect means short-term persistence of the "shock" in the profitability of asset. A crucial technique for studying the temporal dynamics of the second moments is the ARCH test (i.e. conditional variance). The opposite is also true: a significant ARCH effect identifies time-varying conditional volatility, volatility clustering (or mean reversion), and, as a result, the presence of a fat-tailed distribution.

In this methodology part, data and arguments for choosing and using the variables are presented. Also, sources are described and I outline the model and present the process of the research.

3. IMPACT OF CYBERCRIMINALITY ON PRICE VOLATILITY IN CRYPTOCURRENCY MARKETS

In this part, data and summary statistics are presented and described. Furthermore, the impact of cybercriminality on price volatility in cryptocurrency market is analysed through four different hypotheses, which are described in the methodology part. It is investigated into whether cryptocurrency volatility behaves differently during periods of significant volatility in traditional financial markets. As a result, I analyse H1, which is bolstered by the DCC-GARCH analysis of volatility transfers that follows. H2 is analysed to examine whether there is a substantial shift in the price volatility of the cryptocurrency market as a result of cybercrime. H3 is investigated to discover if the severity of a cybercrime is a determinant in cryptocurrency price volatility. Furthermore, H4 is tested to determine whether the conditional linkages between cryptocurrency markets change dramatically as a result of cybercrime incidents.

3.1. Data and summary statistics

This part consists of providing essential descriptive statistics, conducting data quality analysis, and discussing the results of the latter.

Analysis includes thirteen different variables: eight cryptocurrency variables and five variables, representing traditional financial markets. Chosen cryptocurrencies are Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Monero, Cardano, Bitcoin Cash while variables reflecting traditional financial market are GBP/USD, VIX, Gold, the S&P 500 and Oil as measured by West Texas Intermediate. Table 5 displays descriptive and summary statistics of selected variables for the study. Table 5 shows that the variables were not stable during the chosen period because the minimum and maximum values were significantly different between each other. From table 5, I can highlight that lowest exchange rate of cryptocurrency is Stellar (0.0106) while highest exchange rate is a Bitcoin (67527.9) which is much higher than other cryptocurrency. The reason Bitcoin is so much more expensive than other cryptocurrencies is due to scarcity: the maximum supply of Bitcoin is 21 million. There will never be more than 21 million Bitcoin in existence. According to many analysts, the restricted supply, or scarcity, is a significant contribution to Bitcoin's value. The number of observations is higher for cryptocurrencies (1887) while for traditional financial markets variables the

number of observations is lower (1294). The reason is that traditional financial markets are open on weekdays and closed on weekends while cryptocurrency markets are always open and traded on weekdays and weekends. Cryptocurrency markets operate around the clock, 365 days a year. This is due to unlike stocks and commodities, the cryptocurrency market is a decentralized network of computers rather than a controlled exchange.

Table 5

Descriptive statistics of selected variables

	Observations	Mean	Median	Maximum	Minimum	Std. Dev.
Bitcoin	1887	19630.0256	10342.1	67527.9	3228.7	17000.0615
Ethereum	1887	1093.8335	446.840	4808.38	83.81	1194.9018
Litecoin	1887	100.6824	74.1	386.82	23.124	63.6714
Ripple	1887	0.5133	0.3770	2.78	0.136	0.3536
Stellar	1887	0.1872	0.1278	0.886	0.0106	0.1376
Monero	1887	146.9570	124.169	483.687	32.107	86.725
Cardano	1857	0.4855	0.1416	2.9652	0.0185	0.6303
Bitcoin Cash	1887	486.5152	341	3708.9	78.35	427.2529
GBP / USD	1294	1.3066	1.3099	1.4338	1.0684	0.0646
VIX	1294	20.5648	18.81	82.690	9.14	8.7274
Gold	1294	15.8713	15.42	48.980	8.88	5.0595
S&P 500	1294	3379.8127	3131.29	4796.56	2237.4	684.6487
Oil	1294	63.6638	61.48	123.64	-36.98	19.9054

Source: calculated and prepared by the author using data from CoinMarketCap, NASDAQ, CBOE, S&P Dow Jones Indices LLC, U.S. Energy Information Administration

Additionally, table 5 shows the mean of VIX is 20.5648 while it also has reached maximum of 82.690. Interpretation is that a typical VIX value ranges from 20 to 30, below which investors become comfortable. A number of 30 or above implies that there is fear or anxiety in the market.

Since it can be seen that the VIX's mean hovers around 20, it can be concluded that on many days, the VIX value was above 30, indicating that there was trepidation and fear in the market, and given the selected period, this could be linked to the Covid-19 pandemic. Taking into account that this is the mean, which means that it is doing an average of all the values during the selected period, we can notice that many enormous values had to be encountered in the data set to obtain this mean.

Table 6 shows correlation between variables. It is seen that cryptocurrencies are positively correlated. After taking into consideration the volatility of cryptocurrencies, there is some positive correlation between cryptocurrency and stock prices. The same elements that influence stock values also influence the price of cryptocurrencies. Prices tend to follow the same trends because investors and traders approach cryptocurrencies the same way they do equities. Moreover, highest cryptocurrency correlations are bertween Bitcoin and Bitcoin Cash (0.99), Bitcoin and Ethereum (0.928).

Table 6

Correlation between variables

	Cardano	Bitcoin	Bitcoin Cash	Ethereum	Litecoin	Stellar	Monero	Ripple	GBP / USD	Gold	Oil	S&P 500	VIX
Cardano	1.000												
Bitcoin	0.893	1.000											
Bitcoin Cash	0.203	0.099	1.000										
Ethereum	0.927	0.928	0.153	1.000									
Litecoin	0.700	0.714	0.661	0.679	1.000								
Stellar	0.667	0.635	0.600	0.615	0.839	1.000							
Monero	0.735	0.691	0.709	0.708	0.919	0.861	1.000						
Ripple	0.734	0.616	0.626	0.697	0.816	0.857	0.877	1.000					
GBP / USD	0.593	0.548	0.479	0.541	0.695	0.738	0.753	0.626	1.000				
Gold	0.094	0.229	-0.287	0.146	-0.077	-0.117	-0.054	-0.119	-0.220	1.000			
Oil	0.530	0.513	0.206	0.627	0.414	0.451	0.489	0.511	0.454	-0.330	1.000		
S&P 500	0.837	0.912	-0.103	0.897	0.502	0.436	0.524	0.485	0.459	0.265	-0.516	1.000	
VIX	-0.036	0.049	-0.323	0.013	-0.200	-0.183	-0.180	-0.197	-0.292	0.836	-0.386	0.062	1.000

Source: calculated and prepared by the author using data from CoinMarketCap, NASDAQ, CBOE, S&P Dow Jones Indices LLC, U.S. Energy Information Administration

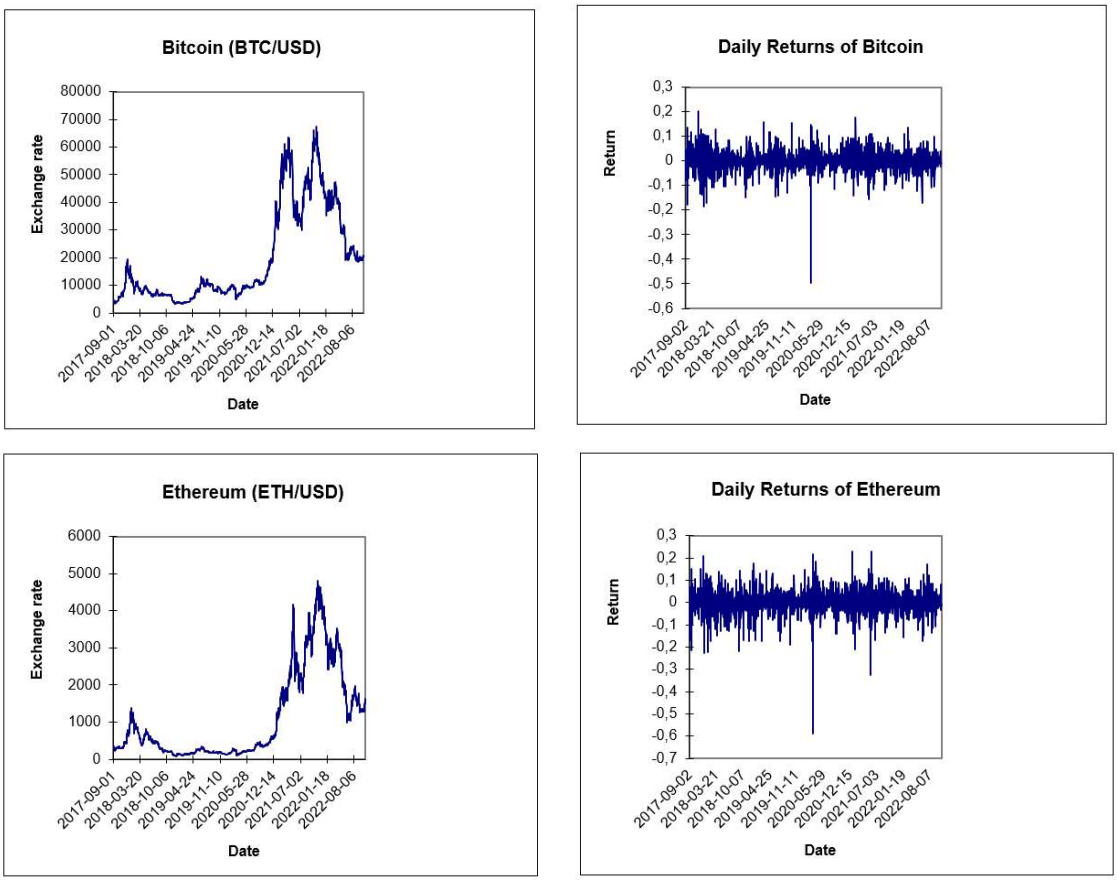
Moreover, daily returns for the variables in this study will be used, as was already indicated. Returns can be determined in a number of different ways. However, adopting the continuous compounding method is one of the most popular ways to do so when evaluating financial data (Ruppert, 2014). Thus, compound returns are used to calculate each cryptocurrency's daily price

returns. The model used to transform each cryptocurrency's daily pricing into logarithmic returns is represented by the following equation: $rt=\ln(P_t)-\ln(P_{t-1})$, where ln (P_t) and ln (P_{t-1}) represent the natural logarithms of the closing prices in USD of cryptocurrencies on days t and days t-1, respectively. As a result, Ruppert's (2014) recommendations for independently and identically distributed (i.i.d.) and normally distributed log returns are followed.

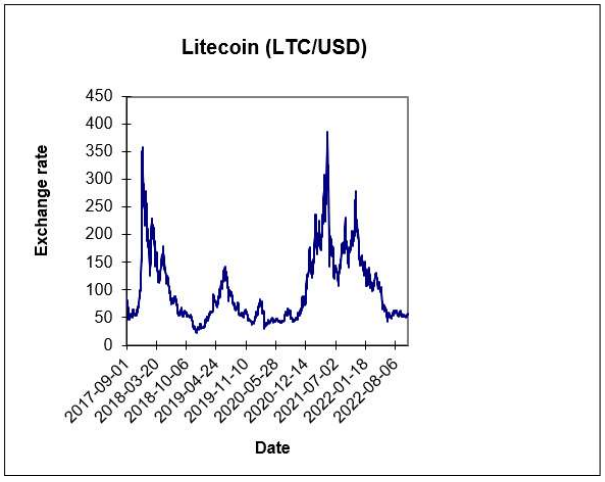
The variables' exchange rates and returns time series are depicted in figure 4. The graphs show that the patterns are similar, the trends are not very different, and at first glance it appears like all of them have a surge in March at the beginning of 2020. The Ripple graph, which displays a larger rise near the end of 2020 in December, makes this surge less obvious. Between 2019 and 2022, Bitcoin and Ethereum appear to change more, whilst Ripple returns have been more consistent. Ripple, however, had greater fluctuation beginning in November than Bitcoin and Ethereum. Graphs displays the price spikes in March for Bitcoin and Ethereum and December for Ripple, which coincided with the announcement of the Covid-19 epidemic and the beginning of the third wave of the pandemic.

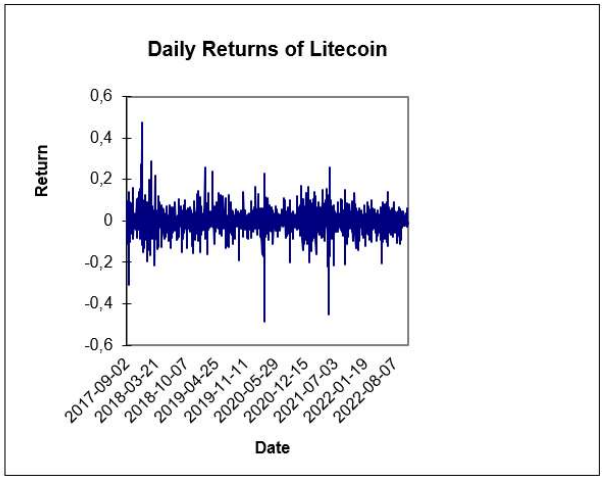
Figure 4

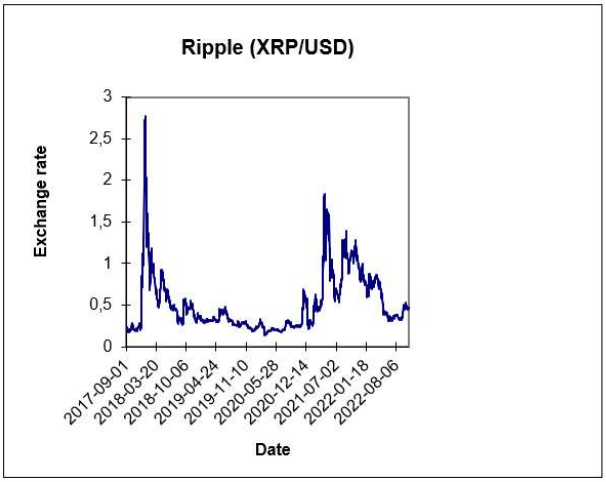
Exchange rates and daily log returns of cryptocurrencies prices

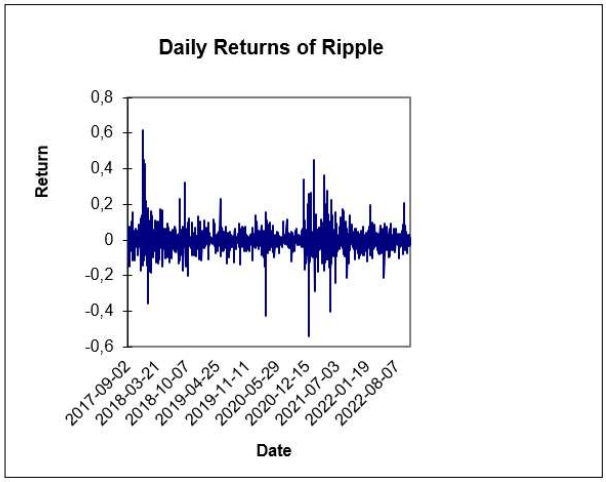


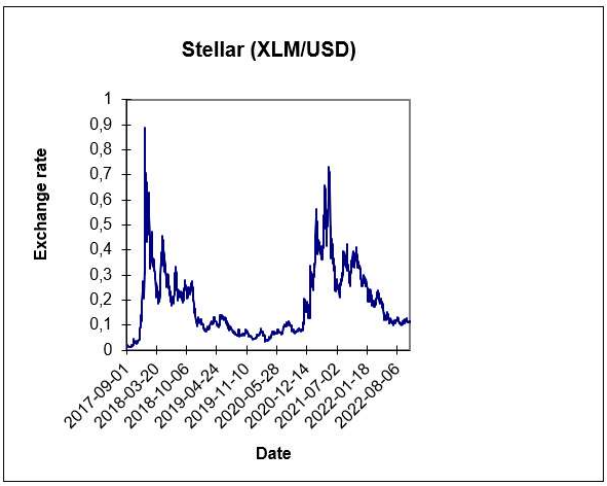
Continuation of figure 4

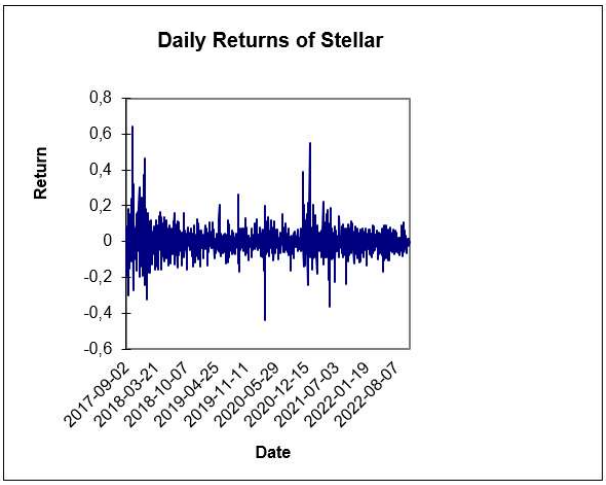




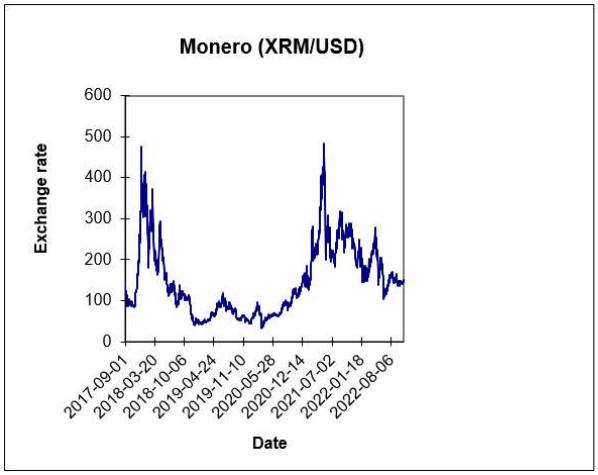


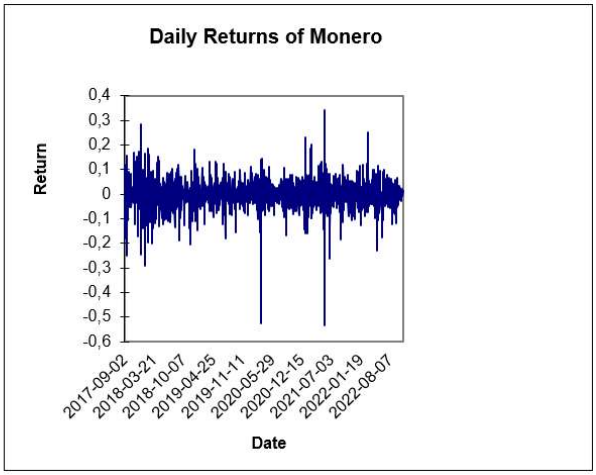


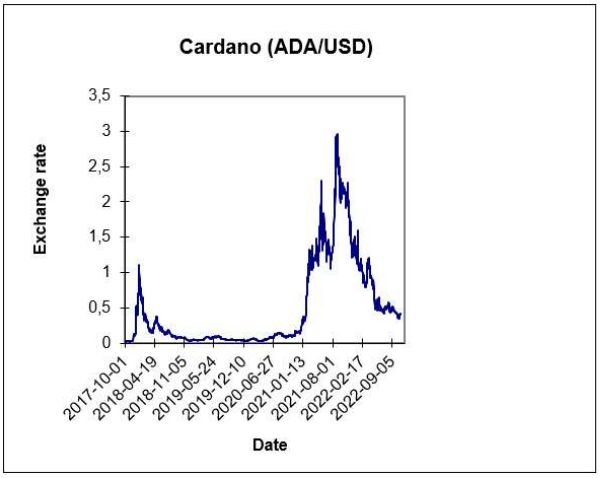


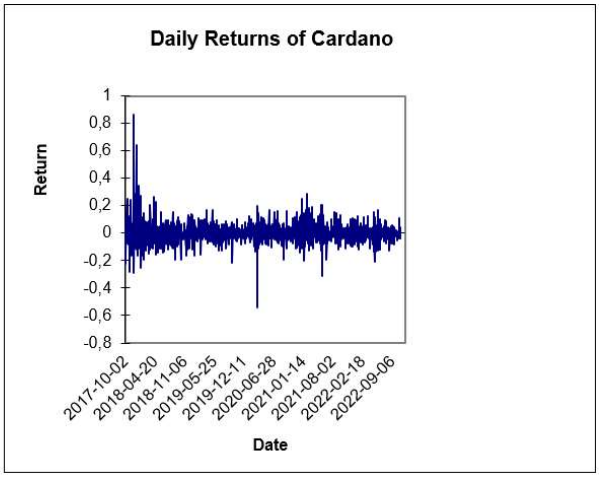


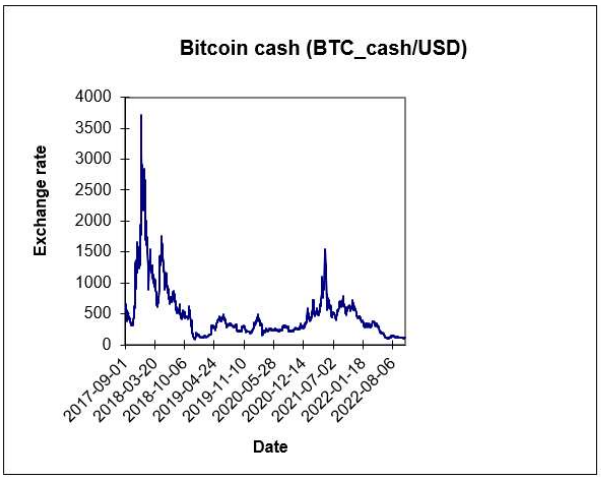
Continuation of figure 4

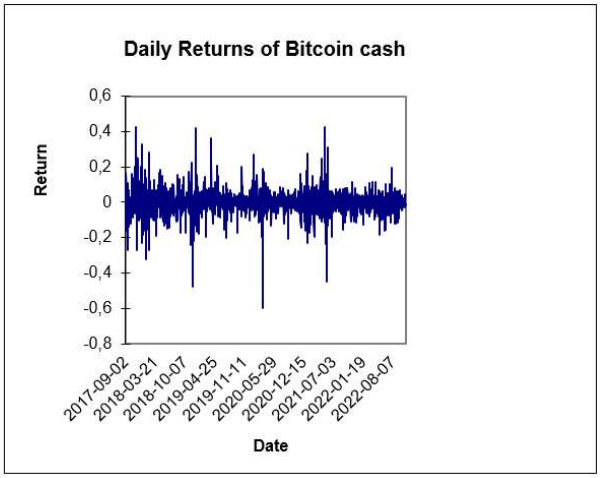












Source: prepared by the author using Eviews

Moreover, the daily cryptocurrency return time-series plot in figure 4 demonstrates that there are intervals of low volatility followed by periods of high volatility (some serene periods as well as turbulent ones), which suggests volatility clustering and supports the ARCH effect.

This part of the study, describes and summarizes the data. Also, methods and tools to achieve the described aim are explained.

3.2. Testing hypotheses and describing results

H1. Is there a major difference in cryptocurrency volatility during times of traditional market volatility?

This research of volatility yields a number of fascinating findings. With the exception of Cardano, there are rarely substantial correlations between individual cryptocurrency markets and different periods of low to high volatility in the VIX, S&P500, and gold markets. Despite this lack of confidence, all differentials between high and low differential GARCH-calculated volatility are positive, with the exception of the link between Cardano and the VIX. However, I notice some very substantial linkages and behavioural differences between our chosen cryptocurrency markets and both the oil and GBP/USD markets. There are interactions between the selected factors and times of low and below-average volatility in the markets for Bitcoin, Ethereum, Litecoin, Monero, and Cardano, whereas high volatility periods are related with a considerable rise in volatility. The size of such volatility differentials is greatest in the Bitcoin, Litecoin, and Cardano markets. The correlation As a result, H1 can be failed to reject based on the evidence presented, which shows that periods characterized by strong volatility in the oil and GBP/USD markets are similarly related with sharp, significant increases in the volatility of cryptocurrency markets.

Table 7

Price volatility of cryptocurrencies during various typical financial market volatility regimes

	Bitcoin	Bitcoin Cash	Ethereum	Litecoin	Ripple	Stellar	Monero	Cardano
Oil Volatility								
Low Vol.	0.00015	0.0008	-0.00001	-0.00029	+0.00166**	0.00085*	0.00071	-0.00016
Below Average Vol.	0.00093**	0.00065	0.00054	0.00051	0.00097	0.00143***	0.00089	0.00025
Above Average Vol.	0.00069	0.0011	0.00056*	0.00023	-0.00065	0.00043	0.00114**	-0.00007
High Vol.	0.00116***	0.00149	0.00071**	0.00089**	0.00097	-0.00011	0.00153**	0.00139***
High-Low Difference	0.00103	0.00071	0.00071	0.00119	-0.00069	0.00095	0.00082	0.00157
S&P500 Volatility								
Low Vol.	-0.00071	-0.00115	-0.00129**	-0.00105	-0.00008	-0.00188***	0.00004	-0.00115*
Below Average Vol.	0.00018	0.00068	-0.00003	0.00011	0.00120*	0.00071	-0.00002	0.00011
Above Average Vol.	0.00044	-0.00048	0.00002	0.00037	0.00008	0.00045	-0.00014	-0.0003
High Vol.	-0.00035	-0.00094	-0.00019	-0.00059	0.00053	0.00059	0.00068	-0.00046
High-Low Difference	0.00038	0.00023	0.00108	0.00048	0.00061	0.00246	0.00063	0.00069
GBP/USD Volatility								
Low Vol.	-0.00140***	-0.00251***	-0.00109**	-0.00114**	-0.00084	-0.00067	-0.00183***	-0.00105**
Below Average Vol.	-0.00119***	-0.00120**	-0.00080*	-0.00083	-0.00065	-0.00114***	-0.00120**	-0.00119***
Above Average Vol.	-0.00107***	-0.00133**	-0.00074	-0.00054	-0.00187***	-0.00156***	-0.00145***	-0.00085**
High Vol.	-0.00067***	-0.00126*	-0.00091**	-0.00063	-0.00043	-0.00135***	-0.00138**	-0.00135***
High-Low Difference	0.00072	0.00125	0.00018	0.00051	0.00042	-0.00068	0.00045	-0.00031
Gold Volatility								
Low Vol.	0.00001	-0.0005	0.00005	-0.00054	-0.00021	-0.00075	-0.00023	+0.00196***
Below Average Vol.	-0.00018	-0.0006	-0.00004	-0.00107*	-0.00084	0.00018	-0.00103	-0.00045
Above Average Vol.	-0.00026	-0.00003	-0.00009	-0.00041	0.00046	-0.00055	0.00009	-0.00073
High Vol.	0.00073*	-0.00044	0.00102*	0.00083	0.00003	-0.00041	0.00043	0.00093
High-Low Difference	0.00072	0.00006	0.00098	0.00137	0.00024	0.00034	0.00067	-0.00104
VIX Volatility								
Low Vol.	-0.00056	-0.00065	-0.00071	-0.0001	-0.00136*	0.00041	-0.0005	0.00194***
Below Average Vol.	0.00035	0.00097*	0.00012	+0.00082*	0.00036	0.00062	0.00058	0.00112**
Above Average Vol.	0.00051	0.00061	0.00026	0.0008	-0.00223***	0.00103**	0.00147**	0.00295***
High Vol.	-0.00015	0.00066	0.00004	0.00067	-0.00001	0.00195***	0.00051	0.00016
High-Low Difference	0.00042	0.00132	0.00075	0.00077	0.00135	0.00154	0.00101	-0.00178

Source: compiled and obtained values by the author using Eviews

This suggests that the same news and sentiment that affects the GBP/USD and oil markets may also cause considerable volatility in cryptocurrency markets, demonstrating the products' and exchanges' continuing progress.

I set out to determine the source of this volatility after noticing a number of stylized features its interconnections with volatility in traditional financial markets. There have been multiple cases of

serious cybercriminality that have harmed the reputation and credibility of both individual cryptocurrencies and the broader exchanges on which they trade in the relatively short time that they have existed. It is critical to examine how cryptocurrency investors behaved before and after such instances. The investigation begins with a look at broad volatility changes and volatility transfer in the aftermath of cybercrime. The second step analyses how the information content of such pricing has changed as a result of the occurrence.

H2. What price volatility dynamics have emerged as a result of cryptocurrency cybercrime?

The first round of the investigation focuses into how the volatility dynamics of the chosen cryptocurrencies changed before and after cybercrime activities. Furthermore, H2 is analysed, which examines whether there is a significant change in cryptocurrency volatility in the aftermath of cybercrime. I utilize a multivariate-GARCH analysis to focus on direct volatility changes, but DCC-GARCH methodology is also employed to concentrate on changes in dynamic correlations. The multivariate-GARCH methodology, whose results are reported in table 8, is based on three sources of data, one of which being the inclusion of historical data via lagged cryptocurrency returns. Table 9 further provides robustness by estimating GARCH calculated volatility over the entire period in which cybercriminality incidents are denoted. With the exception of Ethereum, I find that lagged returns are considerable in all of the cryptocurrencies that were looked into. The traditional assets: GBP/USD, VIX, gold, S&P500, and oil are included in the multivariate-GARCH methodology to account for international effects. With the exception of the approach relating to Bitcoin itself, Bitcoin is utilized as a control variable in the analysis of our selected cryptocurrencies because it is the most well-known and market-leading cryptocurrency in terms of market price. With the exception of Bitcoin and both Stellar and Cardano, there is a very significant and positive link between Bitcoin and our analysed cryptocurrencies. While Bitcoin, with the exception of oil, has a positive association with traditional asset returns, it is extremely similar to the market linkages discovered in Ripple. Both Ethereum and Litecoin, however, have primarily unfavorable associations with traditional assets when compared to the other major capitalization cryptocurrencies. The correlations between cryptocurrencies with medium and low market capitalization are largely non-standard, with the VIX and Bitcoin having uniformly favorable relationships. Across all separate techniques, the cumulative ARCH and GARCH coefficients are determined to be below unity and significant at the 1% level.

Table 8

Cryptocurrency response to hacking incidents using the multivariate GARCH approach

Variable	Stellar	Ethereum	Litecoin	Bitcoin	Bit. Cash	Ripple	Cardano	Monero
R1	-0.2628***	-0.0447	-0.0558**	-0.1896***	-0.0060	-0.1736***	-0.2760***	-0.1499***
	-6.48	(-1.74)	-2.39	(-4.21)	-0.27	-8.44	-8.84	-5.06
R2	0.0345	-0.0131	-0.0727***	-0.0488	-0.0504**	-0.2037***	-0.0709*	-0.0137
	1.17	(-0.62)	-3.67	(-1.57)	-2.11	-10.14	-1.72	-0.44
R3	-0.1813***	-0.0059	-0.0472*	0.0460	-0.0216	0.0579**	0.0761**	0.0774***
	-11.08	(-0.24)	-1.91	(1.52)	-0.88	2.44	2.11	2.86
R4	-0.0393*	-0.0168	-0.0656***	-0.0930***	-0.0063	-0.0092	-0.0828***	-0.0192
	-1.78	(-0.86)	-4.02	(-3.34)	-0.25	-0.40	-3.03	-0.74
R5	-0.1823***	-0.0192	-0.0283	-0.0103	-0.0341	-0.0217	-0.0078	-0.0653**
	-9.04	(-0.95)	-1.43	(-0.42)	-1.62	-0.98	-0.25	-2.40
GBP/USD	-0.2349***	-0.4719	0.2629	0.2395	-0.7563	0.7008	-0.1159	0.0365
	-3.89	(-1.23)	0.52	(0.38)	-1.00	0.75	-0.09	0.05
VIX	0.0191	-0.0122	-0.0177	0.0152	0.0109	0.0141	0.0237	0.0153
	0.88	(-0.75)	-1.00	(0.88)	0.48	0.61	0.96	0.92
Gold	-0.5614*	-0.1741	-0.0458	0.2286	-0.6397*	0.3451	0.0896	-0.0373
	-1.78	(-0.68)	-0.20	(0.67)	-1.91	0.83	0.16	-0.11
S&P500	0.1625	0.0130	0.2417	0.1595	-0.0808	0.4752	0.1235	0.1028
	0.56	(0.06)	1.01	(0.56)	-0.23	1.24	0.39	0.36
Oil	-0.2540*	-0.0506	-0.0124	-0.1174	0.1365	-0.1537	0.3203*	0.1124
	-1.71	(-0.60)	-0.16	(-1.04)	0.96	-1.08	1.73	0.90
Bitcoin	0.1717***	0.8062***	0.8968***	-	0.8665***	0.5907***	0.0424	0.7511***
	4.72	(31.98)	29.78	(-)	25.62	17.35	1.03	19.66
D1	0.0011	0.0010	0.0016	-0.0011	0.0023	0.0007	0.0019	0.0030*
	0.38	(0.92)	1.22	(-1.60)	1.53	0.42	1.54	1.90
D2	0.0016	-0.0015***	-0.0006	-0.0005	0.0002	-0.0012	-0.0004	-0.0003
	0.43	(-4.19)	-0.63	(-0.67)	0.12	-1.20	-0.43	-0.27
D3	0.0002	-0.0021***	-0.0013	0.0033***	-0.0010	0.0008	0.0003	-0.0003
	0.04	(-2.54)	-1.32	(2.89)	-0.70	1.02	0.13	-0.18
D4	0.0053***	-0.0016	-0.0010	-0.0031***	-0.0051**	0.0023	-0.0002	-0.0068***
	2.59	(-1.59)	-0.49	(-2.62)	-2.38	1.43	-0.16	-6.52
D5	-0.0016	-0.0013	-0.0019	-0.0020*	-0.0030*	-0.0033*	-0.0009	-0.0009
	-0.83	(-1.02)	-1.33	(-1.69)	-1.90	-1.68	-0.60	-0.50
D6	-0.0011	0.0005	-0.0001	-0.0010	-0.0003	-0.0002	-0.0006	-0.0008
	-1.13	(0.50)	-0.13	(-0.98)	-0.23	-0.17	-0.65	-0.68
D7	0.0056***	-0.0003	0.0032***	-0.0008	-0.0016	0.0106***	0.0019**	-0.0011
	9.23	(-0.27)	2.47	(-0.83)	-1.17	17.34	2.41	-0.76
D8	0.0010	0.0033*	0.0029	0.0025	0.0054**	0.0042***	0.0011	0.0053**
	0.87	(1.91)	1.38	(1.37)	2.39	2.49	0.90	2.31
D9	0.0000	-0.0008	-0.0002	-0.0004	-0.0009	0.0008	-0.0006	-0.0013
	0.05	(-0.71)	-0.11	(-0.26)	-0.44	0.39	-0.50	-0.69

Continuation of table 8

D10	-0.0004	0.0003	-0.0003	0.0008	0.0028***	0.0020***	-0.0002	0.0021
	-0.44	(0.29)	-0.19	(0.87)	2.75	2.77	-0.44	1.61
D11	0.0017**	-0.0018**	-0.0012	-0.0027***	-0.0020**	-0.0041***	-0.0010	-0.0028***
	2.50	(-2.33)	-1.41	(-6.74)	-2.09	-4.72	-0.98	-3.18
D12	0.0002	0.0010	0.0000	-0.0005	-0.0002	0.0001	0.0009	-0.0005
	0.31	(0.99)	0.00	(-0.86)	-0.19	0.05	1.08	-0.62
D13	0.0011	0.0017*	0.0009	0.0091***	0.0016	0.0013	0.0008	0.0010
	1.19	(1.65)	0.95	(4.52)	1.27	0.67	1.50	0.81
D14	0.0000	0.0020*	0.0011	0.0008	0.0065***	0.0018	0.0000	0.0027**
	-0.03	(1.91)	1.08	(1.13)	5.19	1.22	-0.01	2.12
D15	0.0001	-0.0021**	-0.0023**	-0.0023***	-0.0015	-0.0008	0.0016***	-0.0053***
	0.10	(-2.36)	-2.63	(-4.68)	-1.04	-0.50	2.68	-8.39
D16	0.0000	0.0004	0.0002	0.0002	0.0001	-0.0001	-0.0003	0.0000
	-0.07	(0.50)	0.25	(0.25)	0.08	-0.09	-0.50	0.03
D17	0.0099***	-0.0007	-0.0003	-0.0009	-0.0007	-0.0008	0.0101***	-0.0013
	50.18	(-0.67)	-0.28	(-1.17)	-0.42	-0.39	52.61	-1.08
ARCH	0.1039***	0.1160***	0.1122***	0.0600***	0.0960***	0.1922***	0.1693***	0.0882***
	50.27	(27.26)	33.59	(38.31)	28.32	44.28	36.53	26.06
GARCH	0.8927***	0.8457***	0.8682***	0.9287***	0.8803***	0.7401***	0.8273***	0.9025***
	447.46	(166.53)	244.46	(547.03)	211.51	126.58	207.79	265.69

Source: compiled and obtained values by the author using Eviews

T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

While there are a variety of responses, there appear to be no significantly uniform responses across all markets analysed, implying that all markets have different volatility responses to the cybercrime events under investigation. However, for hacks 4, 7, 8, 10, 14, and 15, there are a variety of responses. Hacks 4 and 15 are both linked to a cybercrime that took place within an exchange (Coincheck and Coinrail, respectively), which exchanged a wide range of cryptocurrencies and so had a theoretically possible impact on a wide range of items. Hacks 7, 8, 10, and 14 are linked to ICO-related scams and cybercriminality. Such findings suggest that cryptocurrencies have a wide range of volatility responses, with data pointing to significant instability created by exchange hacking and ICO fraud, both of which may be seen to be significantly reliant on perceptions of stability and financial safety. Any danger to such stability is observed to elicit widespread responses across a large number of cryptocurrencies, rather than on a per-coin basis. Based on the market that has been directly targeted by such cybercrime, there is also evidence of cryptocurrency-specific volatility.

Table 9

A continuous variable indicating cryptocurrency cybercriminality used in a multivariate GARCH technique

Variable	Stellar	Ethereum	Litecoin	Bitcoin	Bit. Cash	Ripple	Cardano	Monero
GBP/USD	-0.3563***	-0.4136	0.1857	0.2603	-0.6414	0.7232	-0.1867	-0.0840
	(-6.40)	(-1.08)	(0.38)	(0.48)	(-0.86)	(0.80)	(-0.14)	(-0.11)
VIX	0.0246	-0.0121	-0.0087	0.0243	0.0196	0.0406	0.0224	0.0019
	(1.03)	(-0.74)	(-0.45)	(1.36)	(0.89)	(1.45)	(0.68)	(0.09)
Gold	-1.6722***	-0.1161	-0.1151	0.3161	-0.6468**	0.1236	-0.1227	-0.0055
	(-4.82)	(-0.50)	(-0.64)	(1.17)	(-2.01)	(0.30)	(-0.19)	(-0.02)
S&P500	0.1936	0.0204	0.2712	0.1495	0.0368	0.3528	0.3369	0.1635
	(0.64)	(0.10)	(1.02)	(0.52)	(0.10)	(0.94)	(0.94)	(0.47)
Oil	-0.3224***	-0.0510	0.0233	-0.0817	0.1202	0.1251	0.0385	0.0667
	(-1.89)	(-0.63)	(0.31)	(-0.79)	(0.86)	(0.73)	(0.28)	(0.45)
Bitcoin	0.1332***	0.7866***	0.9286***	-	0.8162***	0.7733***	-	0.8394***
	(3.62)	(33.39)	(28.83)	(-)	(23.12)	(26.12)	(-)	(25.87)
Volatility Change	1.2265*	0.4297	1.2624***	1.3916***	0.8512	3.2872**	0.7668	1.4947***
	(1.87)	(0.66)	(3.40)	(5.22)	(1.52)	(2.29)	(0.15)	(8.82)
ARCH	0.2846***	0.1879***	0.2309***	0.2924***	0.3532***	0.4030***	0.4629***	0.2607***
	(8.55)	(8.15)	(7.32)	(4.35)	(7.79)	(18.43)	(6.13)	(2.64)
GARCH	0.9218***	0.7866***	0.7598***	0.5062***	0.6280***	0.5845***	0.5750***	0.4477***
	(13.75)	(9.84)	(10.92)	(7.50)	(7.54)	(13.91)	(10.45)	(4.42)

Source: compiled and obtained values by the author using Eviews

T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Such proof was discovered in the Bitcoin market during hack 3 (+0.0033), hack 4 (-0.0031), and hack 11 (-0.0027), as well as in the Ethereum market during hack 8. (0.0033). The remaining attacks are determined to be quite geographically and product-specific, including cryptocurrencies that were not included in our pick owing to a variety of variables, including data availability and illiquidity.

H3. Has the nature and scope of cybercrime have a direct impact on cryptocurrency volatility?

Use dummy variables to represent the time period during which the stated hack in table 4 occurs to analyse H3, which explores whether the severity of each occurrence is related to the level of volatility that is experienced.

Table 10

Based on the predicted monetary amount taken, a multivariate GARCH technique was used to examine the impacts of bitcoin cybercrime

Variable	Stellar	Ethereum	Litecoin	Bitcoin	Bit. Cash	Ripple	Cardano	Monero
GBP/USD	-0.3523***	-0.4272	0.1704	0.2547	-0.6585	0.6072	-0.1965	-0.0297
	(-5.25)	(-1.12)	(0.34)	(0.46)	(-0.89)	(0.70)	(-0.14)	(-0.04)
VIX	0.0262	-0.0113	-0.0098	0.0231	0.0168	0.0326	0.0237	0.0083
	(1.11)	(-0.68)	(-0.52)	(1.31)	(0.79)	(1.19)	(0.71)	(0.45)
Gold	-1.6372***	-0.1311	-0.1053	0.3161	-0.6576**	-0.0039	-0.0862	0.0011
	(-4.58)	(-0.56)	(-0.55)	(1.09)	(-2.05)	(-0.01)	(-0.13)	(0.00)
S&P500	0.2316	0.0380	0.2759	0.1698	0.0163	0.2700	0.3542	0.2174
	(0.75)	(0.18)	(1.05)	(0.58)	(0.05)	(0.71)	(0.92)	(0.65)
Oil	-0.3233**	-0.0549	0.0204	-0.0963	0.1244	0.1685	0.0422	0.0402
	(-1.90)	(-0.68)	(0.27)	(-0.95)	(0.88)	(1.07)	(0.30)	(0.28)
Bitcoin	0.1329***	0.7856***	0.9311***	-	0.8191***	0.7792***	-	0.8471***
	(3.57)	(32.94)	(28.63)	(-)	(23.00)	(23.62)	(-)	(25.52)
Volatility Change	0.0609	0.0289	0.0640***	0.0705***	0.0434	0.1460***	0.1190	0.0866***
	(1.60)	(0.82)	(2.87)	(4.41)	(1.29)	(2.77)	(0.13)	(7.24)
ARCH	0.2821***	0.1810***	0.2226***	0.2860***	0.3767***	0.4549***	0.4521***	0.2804***
	(8.50)	(7.97)	(7.14)	(4.15)	(7.83)	(14.73)	(6.08)	(2.79)
GARCH	0.9239***	0.7946***	0.7621***	0.5221***	0.6292***	0.5813***	0.5834***	0.4649***
	(13.72)	(9.74)	(10.72)	(7.58)	(7.50)	(15.33)	(10.72)	(4.39)

Source: compiled and obtained values by the author using Eviews

T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

I include the estimated financial value lost during the cybercrime occurrence in this manner. The scale of the loss in each market analysed is represented by a continuous dummy variable in the results. Table 10 shows that four markets have considerable evidence that volatility is connected with the size of a cybercriminality occurrence (Bitcoin, Litecoin, Ripple and Monero). Although the results of four markets are minor, all of the outcomes in this research are favorable, with Cardano demonstrating a strong positive link between the dollar-valued scale of cybercriminality and the GARCH-calculated volatility measure.

H4. Do the conditional relationships between cryptocurrency markets change significantly as a result of cybercrime?

Next, a DCC-GARCH approach is used to examine the dynamic correlations between chosen cryptocurrencies in order to analyse H4, specifically if such dynamic correlations alter following cybercrime incidents. Table 11 summarizes the findings. The average dynamic correlation between each cryptocurrency pair in our dataset is shown in table 11. The strongest cross-cryptocurrency correlations found are between Litecoin and Bitcoin, Litecoin and Ethereum, Ripple and Ethereum, Monero and Ethereum, Ripple and Ethereum, Monero and Litecoin, Bitcoin Cash and Litecoin, Monero and Ripple, and finally Bitcoin Cash and Monero. The estimations of the same dynamic correlation relationship in the period preceding each hacking incident are then provided. This study presents a variety of intriguing findings. First, while comparing the cross-correlations between bigger and smaller capitalization cryptocurrencies, it is seen that smaller capitalization cryptocurrencies have lower estimates. This applies not just to dynamic correlations between smaller cryptocurrencies, but also to interactions between smaller and bigger cryptocurrencies. Second, it is possible to define two distinct periods during which cross-cryptocurrency correlations have risen steadily, as measured by each hacking event. The highest persistent increase in cross-cryptocurrency correlations was seen between hack 3 and hack 5 (6 December 2017 and 13 January 2018). During hack 4, cross-correlations are at their highest (18th of December 2017). These developments overlap with Nicehash's service breach and hacking, Youbit's bankruptcies because to an external hack, and Blackwallet.co's DNS takeover, which resulted in the remote loss of $400,000 in Stellar Lumer (XLM). The total loss from these three cyber incidents is around $103.4 million, which is less than other single hacking incidents.

Table 11

Dynamic relationships between chosen cryptocurrency markets during hacking incidents

	MO-BT	LT-BT	RI-BT	ET-BT	Bc-BT	ST-BT	Bc-ET	RI-LT	MO-ET	ST-ET	LT-ET	RI-ET
Total	0.01	0.02	0.01	0.01	0.01	0.00	0.01	0.02	0.02	0.01	0.02	0.02
D1	0.01	0.02	0.01	0.01	0.01	0.01	0.02	0.02	0.01	0.00	0.02	0.01
D2	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.01	0.01
D3	0.04	0.02	0.01	0.01	0.01	0.01	0.02	0.01	0.04	0.02	0.02	0.01
D4	0.17	0.25	0.19	0.16	0.12	0.05	0.13	0.33	0.16	0.07	0.24	0.20
D5	0.10	0.13	0.13	0.10	0.11	0.07	0.12	0.19	0.10	0.07	0.14	0.17
D6	0.02	0.02	0.02	0.02	0.02	0.00	0.02	0.02	0.02	0.00	0.01	0.02
D7	0.04	0.06	0.04	0.04	0.03	0.02	0.03	0.07	0.04	0.02	0.06	0.05
D8	0.02	0.02	0.03	0.02	0.02	0.00	0.02	0.03	0.02	0.00	0.02	0.03
D9	0.02	0.02	0.03	0.02	0.02	0.01	0.02	0.03	0.02	0.01	0.02	0.03
D10	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.00	0.01	0.01
D11	0.03	0.03	0.02	0.03	0.03	0.00	0.02	0.02	0.03	0.00	0.02	0.02
D12	0.02	0.02	0.02	0.02	0.02	0.00	0.02	0.02	0.02	0.01	0.02	0.02
D13	0.02	0.02	0.02	0.02	0.02	0.00	0.02	0.03	0.02	0.00	0.02	0.03
D14	0.01	0.00	0.00	0.01	0.01	0.00	0.01	0.01	0.01	0.00	0.01	0.01
D15	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.02	0.01	0.01	0.01
D16	0.01	0.00	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.00	0.01	0.01
D17	0.01	0.00	0.01	0.00	0.00	0.00	0.01	0.01	0.01	0.00	0.01	0.01
	MO-RI	Bc-LT	CA-LT	MO-LT	Bc-RI	ST-RI	Bc-MO	CA-MO	CA-ST	Bc-ST	CA-RI	MO-ST
Total	0.02	0.02	0.00	0.02	0.01	0.01	0.02	0.01	0.01	0.00	0.01	0.01
D1	0.00	0.03	0.00	0.01	0.01	0.00	0.00	0.00	0.01	-0.02	0.00	0.01
D2	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.00	0.00	0.01
D3	0.02	0.04	0.02	0.05	0.01	0.01	0.05	0.02	0.06	0.04	0.01	0.05
D4	0.19	0.18	0.05	0.25	0.12	0.17	0.17	0.02	0.06	0.04	0.06	0.08
D5	0.10	0.16	0.03	0.14	0.13	0.11	0.15	0.03	0.04	0.10	0.04	0.09
D6	0.02	0.02	0.00	0.02	0.02	0.00	0.02	0.00	0.00	0.00	0.00	0.00
D7	0.04	0.05	0.04	0.06	0.03	0.03	0.03	0.02	0.02	0.02	0.03	0.02
D8	0.03	0.02	0.00	0.02	0.02	0.01	0.02	0.00	0.01	0.00	0.01	0.00
D9	0.03	0.02	0.00	0.02	0.02	0.01	0.02	0.00	0.00	0.00	0.01	0.01
D10	0.01	0.01	0.00	0.01	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
D11	0.02	0.02	0.00	0.02	0.02	0.00	0.03	0.00	0.00	0.00	0.00	0.00
D12	0.02	0.02	0.00	0.01	0.02	0.01	0.02	0.00	0.00	0.01	0.00	0.00
D13	0.03	0.02	0.00	0.02	0.03	0.01	0.02	0.00	0.01	0.00	0.01	0.00
D14	0.01	0.01	0.00	0.01	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
D15	0.02	0.01	0.01	0.02	0.01	0.01	0.02	0.02	0.01	0.01	0.01	0.01
D16	0.01	0.01	0.00	0.01	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
D17	0.01	0.01	0.00	0.01	0.01	0.00	0.00	0.01	0.12	0.00	0.01	0.01

Source: compiled and obtained values by the author using Eviews

Note: For presentation purposes, the names of the selected cryptocurrencies have been shortened. They are now presented as BT (Bitcoin), ET (Ethereum), LT (Litecoin), RI (Ripple), ST (Stellar), MO (Monero), Bc (Bitcoin Cash), and CA (Cardano).

Furthermore, significant crosscorrelations in some connections persist beyond the period of attack 6, which marks the second biggest loss of investor capital the largest particular hacking incident in the sample. However, it appears that the four incidents' continued international coverage resulted in a significant loss of trust in the cryptocurrency market at this period, as seen by the vast cross-correlations of both the largest and smallest cryptocurrencies. Thus, hypothesis H4 is failed to reject in general.

The second separate phase of increased cross-correlations occurs between the 4th of March and the 9th of April 2018, corresponding to the theft of roughly $300 million during the multi-level-marketing strategy generated by GainBitcoin and the ICO fraudulent activities inspired by Ifan and Pincoin that resulted in a loss of $650 million. Surprisingly, in the bulk of cross-cryptocurrency connections, there are two distinct periods that result in increased correlations. The first occurred on September 5, 2017, during a time of heightened correlations closely tied to hack 11, followed by a substantial spike in correlations on March 18, 2018, and the days after. The earlier occurrence appears to coincide with the first time Bitcoin dipped below $4,400 in a big sell-off that sparked widespread concern across the cryptocurrency sector, while the later event happens in the midst of two major announcements. The first was Google's decision to prohibit cryptocurrency advertisements, implying that even legal businesses would be unable to market their services, similar to Facebook's decision. The failed robbery on the Binance exchange, where hackers had manipulated the market before attempting to pay out, was the second major news item that sparked such widespread cryptocurrency comovement. Because the attack was unsuccessful, it is not included in the list of cybercrime incidents. In addition, the exchange offered $250,000 for information that may lead to the hackers' arrest, and set aside $10 million in a fund for future bounty awards to deter similar attempts.

It is necessary to quickly explore the relationships between selected cryptocurrencies while analysing the findings of the aforementioned DCC-GARCH research. Because Bitcoin and Litecoin have the same structure as peer-to-peer networks, it is not unreasonable to expect some parallels in their volatility responses as investors study their structure, dynamics, and reaction mechanism to shocks in the same way. Cardano is based on smart contracts, similar to Ethereum. Stellar is an open-source, decentralized system for transferring digital currencies to fiat currencies that enables for cross-border transactions between any two currencies. It was invented by the same guy who built the Mt. Gox exchange and co-founded Ripple, and it has many of the same qualities as Ripple (Jed McCaleb).

Table 12

An overview of the study hypotheses that were rejected or failed to reject

Hypothesis	Description	Result	Notes
H1	Has there been a significant difference in cryptocurrency volatility during moments of traditional market volatility?	Fail to reject	I find evidence that times marked by large volatility in the markets for oil and the GBP/USD are also marked by rapid, significant spikes in the volatility of cryptocurrency markets.
H2	Is there a significant shift in cryptocurrency market volatility as a result of cybercrime?	Fail to reject	During cybercrime occurrences, there is evidence of rapid volatility responses in cryptocurrency markets, which appear to be rationally targeted at the cryptocurrencies directly implicated as well as the larger cryptocurrency industry if the cybercrime event is systemically destructive.
H3	Is cryptocurrency volatility affected by the seriousness of a cybercrime?	Fail to reject	Although the results of four markets are minor, all of the outcomes in this research are favorable, with Cardano demonstrating a strong positive link between the dollar-valued scale of cybercriminality and the GARCH-calculated volatility measure.
H4	Do conditional relationships between cryptocurrency markets alter significantly as a result of cybercrime events?	Fail to reject	There are two main findings: smaller capitalization cryptocurrencies have lower estimated cross-correlations than their bigger counterparts, and smaller capitalization cryptocurrencies have lower estimated cross-correlations. Second, we can pinpoint two distinct periods during which cross-cryptocurrency correlations have risen steadily, as measured by each hacking event.

When compared to the other seven cryptocurrencies, Monero is found to be relatively isolated because it uses a Proof of Work mechanism to issue new coins and incentivize miners to secure the network and validate transactions through an obfuscated public ledger, which means anyone can broadcast or send transactions but no outside observer can tell the source, amount, or destination. These varied design qualities and interconnections add to the support for the various conclusions that have been uncovered.

A lot of intriguing findings emerge from the combination of the preceding multivariate GARCH and DCC-GARCH analyses. The research results show and identify that during cybercrime events, there are sharp volatility responses in cryptocurrency markets, which appear to be rationally targeted at the cryptocurrencies directly involved as well as the broader sector of cryptocurrencies if

the cybercrime event is systemically damaging. This is especially noticeable during cybercrime incidents involving wallet theft, which proponents claim is one of the primary security characteristics of virtual currencies, and assaults on cryptocurrency exchanges that trade various cryptocurrencies. Furthermore, evidence of widespread comovement in cryptocurrency markets at times of acute stress and significant reputational harm is discovered, supporting the hypothesis that these relatively young markets have evolved to behave similarly to traditional financial assets during times of crisis.

CONCLUSIONS AND RECOMMENDATIONS

Cryptocurrencies are a worldwide phenomena that is frequently and prominently discussed by the media, venture capitalists, banking, and governmental institutions. The Bitcoin market, in particular, has experienced tremendous growth recently. Because Bitcoin is primarily used for investment purposes, determining its volatility is critical. This research looked at GARCH type model to explain Bitcoin price volatility and its relationship th cybercriminality. In terms of modeling the volatility in the most popular and largest cryptocurrencies, GARCH model is used due to GARCH models are considered to be the most accurate.

There are suggestions that cryptocurrencies should now be viewed as more than just a curiosity, given the growing demand and interest in them. Some cryptocurrencies, such as Bitcoin, Ethereum, Litecoin, and Ripple, have had more recent growth than others. However, there is still debate over whether cryptocurrencies, particularly Bitcoin, should be classified as currencies, assets, or investment vehicles, which is a major topic in and of itself. Most often cryptocurrencies are considered as financial assets, with the majority of users trading them for investment purposes: either as a long-term investment in innovative technologies or as a way to earn a quick buck. In terms of financial investment, such as hedging or pricing instruments, investigating the volatility of cryptocurrencies is critical. As a result, findings are valuable in terms of portfolio and risk management, as well as in assisting others in making better-informed decisions about financial investments and the possible benefits and drawbacks of using cryptocurrencies. Bitcoin is unlike any other financial asset, which opens up new opportunities for stakeholders in terms of risk management, portfolio analysis, and consumer sentiment analysis. As a result, it could be a beneficial tool for portfolio and risk management, and our findings could aid investors in making better judgments.

Furthermore, cryptocurrencies have gained appeal as a result of their capacity to provide efficient payment systems through a decentralized distributed ledger that is not reliant on a political process or state regulatory structure. Cryptocurrency values are unpredictable for a variety of reasons, one of which being cybercrime. If hackers acquire access to the public's credentials, they can steal electronic identities and divert payments from legitimate accounts. Phishing attacks occur when a hacker impersonates a trusted source in order to obtain credentials. Hackers may be able to get a lot more information if there are direct security breaches.

Power dissipation is a phenomena caused by the features of cyberspace, such as cheap entry fees, anonymity, susceptibility, and asymmetry. This indicates that if governments have thus far split the game of power among themselves, other players, such as private enterprises, organized terrorist and criminal organizations, and people, must be playing a part, despite governments continue to play a key one. Cyber attacks are intermittent, multifaceted, and extremely damaging due to their association with important networks and infrastructure.

The study's main aim of study examined into the link between hacks and price volatility in cryptocurrency marketplaces has been accomplished. The goals have been fulfilled. Within an exchange that traded a wide range of cryptocurrencies, there are widespread volatility responses for cybercrime occurrences, indicating that such cybercrime has sector-wide volatility consequences.

• Examined the literature on cybercrime and cryptocurrency market concepts, as well as the relationship between cybercrime and price fluctuations in the cryptocurrency market.

• Build a methodology to evaluate the influence of cybercrime on bitcoin price volatility using the GARCH model.

In the conclusion of analysis of scientific literature, the term "cyber-attack" refers to any illegal cyber conduct intended to violate the security policy of a cyber-asset and result in harm, disruption of services, or access to information related to the said national cyber asset. Cyber-attacks are also defined as the deliberate use of a cyber-weapon against an information system in a way that results in a cyber-incident. A cyber-attack aims to disable and impair a computer network's functionality. There must be a political or security motive for the attack. The biggest and most important external threat to cryptocurrency is from hackers, fraud, and malware. Furthermore, the lack of national and international regulation of Bitcoin makes it easier for fraud and other illegal activities to occur.

The main results of research and analysis, suggest several key conclusions regarding price volatility in cryptocurrency markets and impact of cyberattacks. There is evidence that periods of high volatility in the oil and GBP/USD markets are also accompanied by sharp increases in volatility in the cryptocurrency markets. Moreover, there is evidence of quick volatility reactions in the cryptocurrency markets during cybercrime incidents. These reactions seem to be logically directed at the cryptocurrencies directly involved as well as the greater cryptocurrency industry if the cybercrime event is systemically harmful. Cardano shows a substantial positive relationship between the dollar-

valued scale of cybercriminality and the GARCH-calculated volatility measure, despite the fact that the results of four markets are modest. The two key conclusions are that smaller capitalization cryptocurrencies have lower estimated cross-correlations than their larger equivalents, and vice versa. Second, each hacking event allows us to identify two separate times when cross-cryptocurrency correlations have been continuously increasing.

Based on the findings, several recommendations are provided. While the literature related to analysing the effects of the cyberattacks on price volatility in cryptocurrency markets is very limited as of this moment, there is a vast selection of conducted research related to the latter problems related to cyberattacks and causes of price volatility. Since the knowledge and literature on the impacts of cyberattacks is still quite scarce, most of the research done regarding the topic focuses on bigger hacking events and shorter period, various determinants of price volatility in cryptocurrency markets. This study, among other studies done on the latter topic, should influence researchers to analyse the recent cyberattacks on various cryptocurrencies. A future work is to fit another multivariate GARCH-type models to describe the joint behavior of the hacking events and bigger number of chosen cryptocurrency. This would necessitate both methodological and empirical advancements.

REFERENCES

Alibasic, A., Al Junaibi, R., Aung, Z., Woon, W. L., & Omar, M. A. (2016, September). Cybersecurity for smart cities: A brief review. *In International Workshop on Data Analytics for Renewable Energy Integration* (pp. 22-30). Springer, Cham. https://doi.org/10.1007/978-3-319-50947-1_3

Ardia, D., K. Bluteau, and M. Ruede (2018). Regime changes in bitcoin garch volatility dynamics. Finance Research Letters (Forthcoming). https://doi.org/10.1016/j.frl.2018.08.009

Baek, C., Elbeck, M., 2015. Bitcoins as an investment or speculative vehicle? A first look. Appl. Econ. Lett. 22(1), 30-34. https://dx.doi.org/10.1080/13504851.2014.916379

Balcilar, M., E. Bouri, R. Gupta, and D. Roubaud (2017). Can volume predict bitcoin returns and volatility? a quantiles-based approach. Economic Modelling 64, 74–81. 10.1016/j.econmod.2017.03.019

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019). The blockchain folk theorem. The Review of Financial Studies 32 (5), 1662–1715. 10.1093/rfs/hhy095

Bouoiyour, J. and R. Selmi (2015). What does bitcoin look like? Annals of Economics & Finance 16 (2).

Bouri, E., Molnár, P., Azzi, G., Roubaud, D., & Hagfors, L. I. (2017). On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? Finance Research Letters, 20, 192-198. https://doi.org/10.1016/j.frl.2016.09.025

Brauneis, A. and R. Mestel (2018). Price discovery of cryptocurrencies: Bitcoin and beyond. Economics Letters. https://doi.org/10.1016/j.econlet.2018.02.001

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2021). 8-Cybersecurity and Critical Infrastructure Protection. *Bullock JA, Haddow GD, Coppola DP, Introduction to Homeland Security. Sixth ed. Butterworth-Heinemann, Boston,* 425-497.

Cao, Y., Huang, Z., Ke, C., Xie, J., & Wang, J. (2019). A topology-aware access control model for collaborative cyber-physical spaces: Specification and verification. *Computers & security, 87*, 101478. https://doi.org/10.1016/j.cose.2019.02.013

Chicago Board Options Exchange, CBOE Gold ETF Volatility Index [GVZCLS], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/GVZCLS, May 23, 2022.

Chicago Board Options Exchange, CBOE Volatility Index: VIX [VIXCLS], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/VIXCLS, May 22, 2022.

Chiu, J. and T. V. Koeppl (2019). Blockchain-based settlement for asset trading. The Review of Financial Studies 32 (5), 1716–1753. https://doi.org/10.1093/rfs/hhy122

Chu, J., S. Chan, S. Nadarajah, and J. Osterrieder (2017). Garch modelling of cryptocurrencies. Journal of Risk and Financial Management 10 (4), 17. 10.3390/jrfm10040017

Ciaian, P., & Rajcaniova, M. (2018). Virtual relationships: Short-and long-run evidence from BitCoin and altcoin markets. Journal of International Financial Markets, Institutions and Money, 52, 173-195. https://doi.org/10.1016/j.intfin.2017.11.001

CoinMarketCap, Cryptocurrencies. Retrieved from https://coinmarketcap.com/ , November 1st, 2022.

Corbet, S., C. Larkin, B. Lucey, A. Meegan, and L. Yarovaya (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. Economics Letters 165 (1), 28–34. https://doi.org/10.1016/j.econlet.2018.01.004

Dash, N., Chakravarty, S., & Satpathy, S. (2021). An improved harmony search based extreme learning machine for intrusion detection system. *Materials Today: Proceedings.*

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. Journal of financial stability, 17, 81-91. https://doi.org/10.1016/j.jfs.2014.11.006

Edgar, T. W., & Manz, D. O. (2017). Science and cyber security. *Research Methods for Cyber Security; Syngress Publishing, Inc.: Rockland, MA, USA*, 33-62.

Foley, S., J. R. Karlsen, and T. J. Putnins (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32 (5), 1789–1853. 10.1093/rfs/hhz015

Fry, J. and E.T. Cheah (2016). Negative bubbles and shocks in cryptocurrency markets. International Review of Financial Analysis 47, 343–352. https://doi.org/10.1016/j.irfa.2016.02.008

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness? *Computer fraud & security, 2020*(8), 6-12. https://doi.org/10.1016/S1361-3723(20)30084-1

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics, 95, 86-96. https://doi.org/10.1016/j.jmoneco.2017.12.004

Guesmi, K., Saadi, S., Abid, I., & Ftiti, Z. (2019). Portfolio diversification with virtual currency: Evidence from bitcoin. International Review of Financial Analysis, 63, 431-437. https://doi.org/10.1016/j.irfa.2018.03.004

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security, 95,* 101827. https://doi.org/10.1016/j.cose.2020.101827

Karbasi, A., & Farhadi, A. (2021). A cyber-physical system for building automation and control based on a distributed MPC with an efficient method for communication. *European Journal of Control.* https://doi.org/10.1016/j.ejcon.2021.04.008

Katsiampa, Paraskevi. 2017. Volatility estimation for Bitcoin: A comparison of GARCH models. Economics Letters 158: 3–6. https://doi.org/10.1016/j.econlet.2017.06.023

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention, 148,* 105837. https://doi.org/10.1016/j.aap.2020.105837

Koutmos, D. (2018). Bitcoin returns and transaction activity. Economics Letters 167, 81–85. 10.1016/j.econlet.2018.03.021

Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security, 102*, 102138. https://doi.org/10.1016/j.cose.2020.102138

Ma, L., Zhang, Y., Yang, C., & Zhou, L. (2021). Security control for two-time-scale cyber physical systems with multiple transmission channels under DoS attacks: the input-to-state stability. *Journal of the Franklin Institute.* https://doi.org/10.1016/j.jfranklin.2021.05.017

Motsch, W., David, A., Sivalingam, K., Wagner, A., & Ruskowski, M. (2020). Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems. *Procedia Manufacturing, 51*, 1748-1754. https://doi.org/10.1016/j.promfg.2020.10.243

Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System. Journal for General Philosophy of Science.

National Association of Securities Dealers Automated Quotations (NASDAQ), GBP/USD, retrieved from https://www.nasdaq.com/market-activity/currencies/gbpusd/historical , November 2st, 2022.

Phillip, A., J. Chan, and S. Peiris (2018). A new look at cryptocurrencies. Economics Letters 163, 6–9. https://doi.org/10.1016/j.econlet.2017.11.020

Phillips, P. C., Y. Wu, and J. Yu (2011). Explosive behavior in the 1990's nasdaq: When did exuberance escalate asset values? International Economic Review 52 (1), 201–226. http://dx.doi.org/10.2139/ssrn.1091830

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly, 32*(2), 108-117. https://doi.org/10.1016/j.giq.2015.02.001

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security, 49*, 70-94. https://doi.org/10.1016/j.cose.2014.11.007

Roth, N. (2015). An architectural assessment of bitcoin: using the systems modeling language. Procedia Computer Science 44, 527–536. https://doi.org/10.1016/j.procs.2015.03.066

Ruppert, D. (2004). Statistics and finance: An introduction (Vol. 27). New York: Springer.

S&P Dow Jones Indices LLC, S&P 500 [SP500], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/SP500, May 22, 2022.

Sensoy, A. (2019). The inefficiency of Bitcoin revisited: A high-frequency analysis with alternative currencies. Finance Research Letters, 28, 68-73. https://doi.org/10.1016/j.frl.2018.04.002

Thomson, J. R. (2015). *High integrity systems and safety management in hazardous industries*. Butterworth-Heinemann.

Tiwari, A. K., R. Jana, D. Das, and D. Roubaud (2018). Informational efficiency of bitcoinâATan extension. Economics Letters 163, 106–109. https://doi.org/10.1016/j.econlet.2017.12.006

U.S. Energy Information Administration, Crude Oil Prices: West Texas Intermediate (WTI) - Cushing, Oklahoma [DCOILWTICO], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/DCOILWTICO, November 1st, 2022.

Urquhart, A. (2016). The inefficiency of Bitcoin. *Economics Letters, 148*, 80-82.

Urquhart, A. (2018). *What causes the attention of Bitcoin? Economics Letters, 166*, 40-44.

Urquhart, A., & Zhang, H. (2019). Is Bitcoin a hedge or safe haven for currencies? An intraday analysis. International Review of Financial Analysis, 63, 49-57. https://dx.doi.org/10.2139/ssrn.3758512

Vidal-Tomás, D., & Ibaez, A. (2018). Semi-strong efficiency of Bitcoin. Finance Research Letters, 27, 259-265. https://doi.org/10.1016/j.frl.2018.03.013

Wei, W. C. (2018). Liquidity and market efficiency in cryptocurrencies. Economics Letters 168, 21–24. 10.1016/j.econlet.2018.04.003

Zhang, X., Xu, M., Da, G., & Zhao, P. (2021). Ensuring confidentiality and availability of sensitive data over a network system under cyber threats. Reliability Engineering & System Safety, 214, 107697. https://doi.org/10.1016/j.ress.2021.107697

Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. (2020). TIMiner: Automatically extracting and analysing categorized cyber threat intelligence from social data. *Computers & Security, 95*, 101867. https://doi.org/10.1016/j.cose.2020.101867

Zhao, Z. G., Ye, R. B., Zhou, C., Wang, D. H., & Shi, T. (2021). Control-theory based security control of cyber-physical power system under multiple cyber-attacks within unified model framework. *Cognitive Robotics, 1*, 41-57. https://doi.org/10.1016/j.cogr.2021.05.001

Zou, T., Bretas, A. S., Ruben, C., Dhulipala, S. C., & Bretas, N. (2020). Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. *Electric power systems research, 187,* 106490. https://doi.org/10.1016/j.epsr.2020.106490

KIBERNETINIŲ NUSIKALTIMŲ ĮTAKOS KAINŲ SVYRAVIMUI KRIPTOVALIUTŲ RINKOSE TYRIMAS

UGNĖ SAULIŪNAITĖ

Magistro baigiamasis darbas

Finansų ir Bankininkystės programa

Vilniaus universiteto Ekonomikos ir verslo administravimo fakultetas

Darbo vadovas – Dr. Alfreda Šapkauskienė

Vilnius, 2023

Santrauka

62 puslapiai, 4 paveikslai, 12 lentelių, 55 šaltiniai.

Šiuo akademiniu darbu buvo siekiama ištirti, kaip kibernetinės atakos veikia kainų svyravimus kriptovaliutų rinkose. Tikslai apima literatūros peržiūrą ir kibernetinių nusikaltimų bei kriptovaliutų rinkų sampratų aptarimą, tyrimo metodo pasirinkimą ir analizę, skirtą kriptovaliutų kainų dinamikai ir atsakui į kibernetines atakas ištirti. Magistro baigiamąjį darbą sudaro trys pagrindinės dalys: mokslinės literatūros analizė, tyrimo metodai ir tyrimo rezultatų apžvalga.

Literatūros analizė atlikta siekiant apžvelgti pagrindines kibernetinio nusikalstamumo sąvokas ir jo ryšį su kriptovaliutomis, aptarti kainų svyravimus kriptovaliutų rinkose ir ištirti kitų autorių naudojamus GARCH modelius.

Metodikos dalyje pristatoma trylika pasirinktų kintamųjų ir septyniolika įsilaužimo įvykių, skirtų analizuoti kibernetinių atakų įtaką kainų svyravimui kriptovaliutų rinkose 2017-2022 m. Metodikos dalyje aprašomas ir pristatomas pasirinktas GARCH modelis.

Tyrimo rezultatų skyriaus apžvalgoje ir analizėje pateikiama bendra pasirinktų aštuonių kriptovaliutų ir penkių tradicinių finansų rinkų apžvalga su aprašomomis lentelėmis ir skaičiais.

Empirinė analizė taip pat nurodo dienos kriptovaliutų grąžos laiko eilučių diagramas, kurios palaiko ARCH efektą ir siūlo nepastovumo grupavimą. Tai leidžia autoriui naudoti modelį ir sėkmingai interpretuoti rezultatus. Pagrindiniai tyrimų ir analizės rezultatai leidžia daryti keletą esminių išvadų dėl kainų svyravimo kriptovaliutų rinkose ir kibernetinių atakų poveikio. Naudojant daugiamačius GARCH ir DCC-GARCH metodus, yra įrodymų, kad kibernetinių nusikaltimų incidentų metu kriptovaliutų rinkose greitai reaguojama į nepastovumą. Atrodo, kad šios reakcijos yra racionaliai nukreiptos į tiesiogiai susijusias kriptovaliutas, taip pat į didesnę kriptovaliutų pramonę, jei kibernetinio nusikaltimo įvykis yra sistemiškai žalingas. Be to, yra teigiamų rezultatų, rodančių, kad kriptovaliutų nepastovumui įtakos turi kibernetinių nusikaltimų rimtumas. Taip pat tikrinama, ar sąlyginiai ryšiai tarp kriptovaliutų rinkų labai keičiasi dėl kibernetinių nusikaltimų incidentų. Galiausiai apibendrinami rezultatai ir pateikiamos rekomendacijos.