FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION
VILNIUS UNIVERSITY

FINANCE AND BANKING MASTER PROGRAMME

Karolina Maciulevičiūtė

MASTER THESIS

KRIPTOVALIUTŲ KAINŲ KINTAMUMO SĄSAJOS SU NUSIKALSTAMUMU KRIPTOVALIUTŲ RINKOSE TYRIMAS	**INVESTIGATING DYNAMICS BETWEEN PRICE VOLATILITY AND CRIMINALITY IN CRYPTOCURRENCY MARKETS**

Master degree student_____

Supervisor_____
Assoc. prof. PhD Alfreda Šapkauskienė

Date of submission of Master Thesis: _____
Ref. No. _____

Vilnius, 2022

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

The usage of cryptocurrencies in the financial sector has been recently increasing worldwide. Blockchain technology together with cryptocurrencies are representatives of digital development through the global economy. However, with the increasing usage, there is still a lot of discussion about the extent to which cryptocurrencies are being exploited for criminal purposes. Having certain benefits, the cryptocurrency market brings out significant threats. Specific issues have been presented in the context of crimes related to cryptocurrencies, in particular their use for money laundering, terrorist financing, cyber-attacks, fraud or payment for illegal goods and services in Darknet markets. The development of cryptocurrencies in terms of their usage for different financial transactions is a recent and potentially profound innovation. The anonymity of cryptocurrency users determines the use for a variety of lawful and illicit activities.

Since cryptocurrencies became better known worldwide, the price dynamics of cryptocurrencies become a questionable matter. While other innovations can be described as exponentially growing in the long term, cryptocurrency markets are highly volatile, which affects their further development. Accordingly, in recent years, the nature of cryptocurrencies and their volatility have been widely studied by investors, policymakers and business analysts. While it is known that cryptocurrencies take part in illicit activities, the impact of criminal activity on cryptocurrency price remains uncertain. There are not many studies providing evidence or detailed analysis of the topic; therefore, the research on the influence of criminal activity on the cryptocurrency market is an essential step in economics.

To date, little research has been carried out on price volatility in terms of criminal activity. Subsequently, the literature on cryptocurrencies is generally focused on investigating the dynamics of their prices. Researchers mostly focus on price drivers (Corbet et al, 2019; Goczek et al., 2019; Guindy, 2021; Kristoufek, 2015; Liu et al., 2019; Phillips and Gorse, 2018; Polasik et al. 2015), price volatility affected by the media (Alkhazali et al., 2018; Azqueta-Gavaldon, 2020; Gurrib et al., 2019; Hakim das Neves, 2020; Park et al., 2020; Zhu et al., 2017), cryptocurrency usage for illicit activities (Albrecht et al., 2019; Foley et al., 2019; Gandal et al., 2018; Goldsmith et al., 2020; Kamps et al, 2018; Kethineni et al., 2018) and the impact of cyber-attacks on cryptocurrency prices (Bejaoui et al., 2019; Bouveret, 2018; Caporale et al., 2020; Caporale et al., 2021; Corbet et al, 2019; Giovanni et al., 2020).

It turns out that cryptocurrency price dynamics is quite a controversial topic, still, there are clear indications that criminal activity is affecting its economy. The technical shortcomings and the lack of a central government issuing and controlling this digital currency make it vulnerable. Considering high price fluctuations, such as THE Bitcoin price crash in December 2017, when

Bitcoin price fell 45% from its peak five days prior to the crash. Similar examples of Bitcoin price bubbles were repeated in early 2021. As a result of that, the cryptocurrency market has been associated with controversy over frequent incidents, such as hacks, theft, scams and illegal use, which have had an impact on its ecosystem since it became popular. Moreover, the current global financial situation caused by COVID-19 is actually the time to test cryptocurrencies of their safe heaven properties since their inception. There are several ways in which COVID-19 has increased the risk of illegal activities. The pandemic has provided new criminal opportunities not only in the medical equipment supply chain but also in fraud and hacking. For example, the increase in the number of online transactions, coupled with the growing number of inexperienced users has led to a rapid increase in online financial fraud. At the same time, the global economic slowdown and rising unemployment may have led to a greater propensity for crime to compensate for economic insecurity and lost revenue. For cybercriminals, the lockdown was primarily an opportunity to increase the effectiveness of attacks. As a result of that, there is a trend that cryptocurrency-related crime is growing year by year, in particular scams, such as Ponzi schemes. However, as there is a lack of empirical research in regard to the impact of different criminal activities on cryptocurrency prices, such investigation helps to improve market transparency.

The aim of the research. The purpose of this research is to investigate the dynamics between the price volatility of cryptocurrencies in order to determine whether there is a link between criminal activity and cryptocurrency price volatility.

The main objectives of the research:

1. To theoretically analyze the impact of criminal activity in cryptocurrency markets on cryptocurrency prices;
2. To identify and analyze research methods applied in the literature to investigate cryptocurrency price volatility and its factors and develop a research methodology for an investigation of cryptocurrency price dynamics affected by criminal activity;
3. To estimate the actual impact of criminal activity on cryptocurrency prices based on the developed methodology.

Research methods. Related scientific studies were gathered and systemized in order to examine and compare contribution of already existing methods and findings. Therefore, literature analysis was engaged as a part of the methodology to support and validate empirical models. Based on the literature review, Multivariate Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model was selected as the first and the second research method to investigate direct volatility changes immediately after criminal incidents in the cryptocurrency market. As a third research model that aims to analyze changing correlations between cryptocurrencies due to criminal incidents, the Dynamic Conditional Correlation (DCC) GARCH model was employed.

All research models were developed by using software “OxMetrics” together with “Matlab” and “Eviews” which were used for descriptive statistics and analysis of the initial data.

Structure of the research. The thesis consists of three main parts. The first part covers the theoretical aspects of the use of cryptocurrencies for criminal activities, the types of criminal activities that take part in the cryptocurrency market and their impact on the price, an overview of the main price drivers of cryptocurrencies and the key differences between cryptocurrencies. In addition, this part involves the analysis of methods and variables used in related literature. The methodology section provides a detailed analysis of multivariate GARCH and DCC-GARCH models as well as selected variables, data period and formulated hypotheses. The third part represents the results of empirical analysis of dynamics between the price volatility of cryptocurrencies caused by criminal activity in cryptocurrency markets.

1 THEORETICAL ASPECTS OF CRYPTOCURRENCY USAGE FOR CRIMINAL ACTIVITIES AND ITS IMPACT ON PRICES

The purpose of this chapter is to identify and analyze specific aspects of cryptocurrency economics in relation to criminal activity and to clarify the purpose of the research. It seeks to develop the theoretical base and to define the main purpose of the study in an appropriate context. First of all, the role of different types of criminal activities in the cryptocurrency ecosystem is discussed. The second part explains the impact of different types of criminal activity on cryptocurrency prices. In the third part, the other drivers of cryptocurrency price and the reasons of its volatility are identified. Lastly, this chapter represents the summary of the literature regarding cryptocurrency price volatility and its factors.

1.1 The role of criminal activities in the cryptocurrency ecosystem

In recent year, the cryptocurrency market has encountered quick growth. This market permits organizations to increase funds without cooperating with venture capital investors and be traded without listing on a stock exchange (Liu, Tsyvinski and Wu, 2019). Cryptocurrencies are based on blockchain technology, which was primarily created for Bitcoin in 2009, by an unrecognized programmer who has the pseudonym Satoshi Nakamoto. Moreover, Blockchain is based on a digital distributed ledger technology, meaning that the separate parts of a chain are stored in a decentralized network of digital devices. Since there is no single authority, it is impossible to modify or manipulate blockchain, hence this can be identified as the most significant advantage of blockchain. By resolving a mathematical riddle, cryptocurrencies, such as Bitcoin are “mined”, therefore there is a limit on the number of cryptocurrencies issued (Seele, 2018).

Blockchain technology operates in such a way that the coin records all the transactions made in the past using the chain. As all the transactions are recorded in the blockchain, theoretically it should be transparent. However, in practice, the user and most of the legal authorities are not able to review the information in the blockchain, therefore it is possible to conduct anonymous transactions, similarly with cash. In general, the potential transparency of the whole blockchain technology makes it possible to carry out the most convenient illicit transactions worldwide, regardless of national borders, warehousing or transportation problems. Due to the mentioned advantages, blockchain is used by criminals in order to protect themselves from law enforcement (Caporale et al., 2020; Seele, 2018).

Technological progress provokes changes in economy, both in developed and undeveloped countries that affect most people. Blockchain technology adoption implementing cryptocurrencies to the economy also cause risks. Advanced technologies such as Fintech are especially vulnerable

to cyber-attacks, considering their dependence on technology. Increasingly frequent cyber-attacks carried out by criminals from underground web communities (e.g., Darknet) is a significant issue that resulted from substantial reliance on information technology (Benjamin, Valacich and Chen, 2019; Bouveret, 2018). Given the staggering rise in prices in recent years, cryptocurrencies have been accused of price bubbles. Cryptocurrency markets experience some well-known problems such as regulatory oversight, the possibility of illegal use through anonymity in an underdeveloped market and infrastructure breaches affected by the growth of cybercrime (Corbet et al., 2019).

Several authors (Albrecht et al., 2019; Foley et al., 2019; Gandal et al., 2018; Goldsmith et al., 2020; Kamps et al, 2018; Kethineni et al., 2018) identify the flexibility, anonymity, easy access to the online markets and lack of legal enforcement as the key factors bringing conventional criminals to the internet. The regulatory and legal uncertainty, as well as frequent system issues concerned to Bitcoin security such as hacking, thefts and illegal usage, may have a negative impact on the trust of the user for a particular cryptocurrency. The decrease of user's trust can directly influence its value (Caporale et al., 2020; Kethineni and Cao, 2020; Koerhuis, Kechadi & Le-Khac, 2019). Based on the research conducted by Sovbetov (2018), there is a statistically significant effect of cryptocurrency market factors such as total market price, trading volume and volatility on the Bitcoin, Ether, Dash, Litecoin and Monero cryptocurrencies in the long and short term, respectively. The market fluctuations have a higher impact on these cryptocurrencies in the long term.

Furthermore, digital currency-related crimes are rising since cryptocurrencies are more often used as payment form for online transactions of illicit items, for example, counterfeit identification cards, weapons, and illegal medications (Kethineni et al., 2020). Such cryptocurrencies as Bitcoin and Monero lead to new models for criminals to defraud a lot of individuals from Ponzi schemes to drug trafficking, money laundering and tax evasion. Based on a recent study provided by Foley et al. (2019), around 25% of all bitcoin users and 44% of all transactions are related to illicit activities. According to Foley et al. (2019), the total value of illicit Bitcoin transactions per year is estimated at approximately USD 72 billion. However, other studies have found that less than 1% of Bitcoin transactions processed by exchange services may be considered illegal (Fanusie and Robinson, 2018). Similar to 2019, 2020 was a year full of fraud and cybercrime as approximately USD 4,26 trillion was stolen from cryptocurrency exchanges.

Given the range of specific features of blockchain technology, some cryptocurrencies can be described as facilitating their usage for illicit activities. As Bitcoin was the primary cryptocurrency in the ecosystem, the developers of the later introduced cryptocurrencies purposely reproduced its supreme features such as decentralized peer-to-peer exchange and shared public ledger to be able to compete with Bitcoin, which is considered as the market leader. The main

focus was to improve speed, robustness and privacy features. Other cryptocurrencies are commonly called altcoins as an alternative to Bitcoin. Although the basic structures of altcoins are similar to Bitcoin, they traded in part based on their outstanding differences from Bitcoin. In addition, some of the later altcoins were developed mainly for niche constituencies (White, 2015).

As the best-known cryptocurrency in the world, Bitcoin can also be described as a cryptocurrency that accounts for more than half of the market capitalization of all cryptocurrencies, has the largest trading volume and provides liquidity to other cryptocurrencies (Saiedi, Brostrom & Ruiz, 2020). The potential role and partial replacement for conventional financial services and currencies as well as by its role in illegal activities caused Bitcoin growth worldwide. It is important to highlight the fact that although no cryptocurrency has reached Bitcoin usage rates or market capitalization, the market capitalization of each of the top 12 cryptocurrencies exceeds 1 billion USD, indicating that altcoins are an attractive alternative for consumers frustrated with Bitcoin. However, the variability is large, making it impossible to estimate whether this growth will continue.

Despite recent changes in the cryptocurrency market, such as the emergence of several more privacy-oriented cryptocurrencies, Bitcoin is still considered the main cryptocurrency for illegal or criminal activities on the dark web (Silfversten et al., 2020). Given the substantial volume of Bitcoin transactions, criminal and illegal activities are unlikely to be detected. Apart from Bitcoin, there are other quite popular cryptocurrencies such as Ether, Ripple and Litecoin. Bitcoin was first developed as a primary payment mechanism, while other cryptocurrencies, such as Ethereum, offered a wider range of blockchain programs useful for complex transactions, Initial Coin Offering (ICO) fraud, and market manipulation (Silfversten et al., 2020).

Ether is the second-largest cryptocurrency within the market given the liquidity and market capitalization. Ethereum is described as an ICO platform because it supports applications and other cryptocurrency operations. Developers of the application are able to establish their own cryptocurrencies and carry out ICOs using Ethereum to increase funds. Similarly to Ripple, the value of Ether value derives partially from the service of Ethereum as the ICO platform (Li & Whinston, 2020). Ethereum supports contingent contracts, also known as smart contracts, that are stored and executed through the blockchain only after the required conditions met. The publicly available consensus of the writers of the Ethereum blockchain examine the conditions and validates the execution of the contracts (Li & Whinston, 2020). Sovbetov (2018) identified that Bitcoin and Ether have a higher sensitivity to the market in the short run.

According to Phillips et al. (2018), there is a significant similarity between Bitcoin and Litecoin cryptocurrencies as Litecoin was created based on Bitcoin infrastructure. However, Litecoin offers faster transaction confirmations, i.e., 2,5 minutes versus 10 minutes (White, 2015).

Ripple is a cryptocurrency developed by the technology company Ripple Labs and does not rely on a mining protocol. In order to ensure the stability of Ripple coin, the system is following the example of Bitcoin by using a shared public ledger. The payment network of Ripple validates transactions through a consensus protocol which is able to verify transactions in 5 seconds instead of 1-10 minutes (if using mining protocols). According to Brada and Sedlaček, (2017), Ripple does not use blockchain and use a public database called RippleNet instead. The popularity of Ripple is driven by the fact that it is used as an intermediary in regular international currency transfers.

Considering Bitcoin as the most popular cryptocurrency used in Darknet marketplaces, other altcoins, such as Ether due to its popularity or Monero due to improved anonymity have occasionally been adopted in Darknet marketplaces (Foley, 2019). Brada and Sedlaček (2017) emphasize that Monero (launched in 2014) was developed mostly focusing on privacy, decentralization and scalability. The entire design of Monero is significantly different from Bitcoin. As the public addresses are not recorded in the blockchain, Monero does not provide the ability to query other user's public address on the blockchain in order to review their transactions and balance (Koerhuis, Kechadi & Le-Khac, 2019).

Given the growing concern that most popular cryptocurrencies, especially Bitcoin, do not have as strong guarantees of anonymity and privacy, several alternative cryptocurrencies such as Dash, Monero, Litecoin and Zcash have been developed having privacy-enhancing and protecting features. Dash and Litecoin claim that they have a faster verification process, which shortens their operations.

Zcash is a digital currency released as a code derivative of Bitcoin in 2016 which allows choosing a privacy structure. Therefore, the funds can be transparent or protected and the user is able to choose between two options. Transparent funds have similar privacy features to Bitcoin and protected funds are designed with more stringent privacy attributes to ensure that personal and transactional data remains completely confidential. The purpose of privacy coins such as Zcash is to provide greater protection for the privacy of legitimate users who do not intend to disclose their financial information to the public (Silfversten et al., 2020). The protection provided by Zcash to its users is an important factor, especially for criminals wishing to use Zcash for money laundering or major illegal activities. In addition, Zcash benefits by better protecting its users from cyber-attacks compared to other privacy coins (Silfversten et al., 2020).

Dash is a cryptocurrency launched in 2014, previously named Darkcoin. Dash has some features like Bitcoin, but also has additional attributes such as instant and private transactions, as well as decentralized governance (Brada and Sedlaček, 2017). In line with this, Dash provides greater anonymity to its users comparing with Bitcoin. While each transaction and the address of

its user is publicly represented in the Bitcoin ledger, the information of Dash transactions is not public (White, 2015). According to a recent study, Dash and Ripple were discovered to be sustainable safe haven investments during the crisis in the financial markets (Jeribi et al., 2021).

Wei (2018) identifies Tether as the largest coin within the cryptocurrency ecosystem which is also most stable. Stable coins allow pricing cryptocurrencies in US dollars without a requirement to open a USD bank account. Thus, it is mostly used for online crypto exchanges. Given such features, the investor is mainly seeking to convert and exchange as stable coin into another cryptocurrency, especially on exchanges where the standard fiat currencies are not accepted. This results in Tether being used for the exchange of a particular cryptocurrency to another. Wei (2018) also emphasizes that as Tether is not mined, unlike other cryptocurrencies, it has outstanding control over the size and timing of emissions. Silfversten et al. (2020) highlight that more stable cryptocurrencies are likely to be preferred for illegal activities that require long term planning, particularly money laundering, considering destabilization of the funds' movement caused by significant value fluctuations.

To conclude, the nature of cryptocurrencies provides a specific and effective channel through which illegal funds as well as illegal cross-border transactions could be executed. Anonymity, flexibility, speed of transactions and the lower fees compared to traditional payment systems as well as easy access to the online markets and lack of legal enforcement are the main factors behind the cryptocurrency-related crime are growing worldwide. Furthermore, as the altcoins were introduced to the cryptocurrency ecosystem after Bitcoin, they mainly focused on improving the speed of the transactions and privacy. The most well-known privacy-oriented cryptocurrencies are Monero, Dash and Zcash. Stable cryptocurrencies such as Tether are likely to be preferred for illegal activities. In addition, criminal activity damages the credibility of the cryptocurrency market and have continued to grow in both scale and complexity.

1.2 The impact of different types of criminal activity on cryptocurrency prices

As it was previously discussed in section 1.1, cryptocurrencies are often used in criminal activities due to their features, especially anonymity. However, here are different types of criminal activity that uses cryptocurrencies for individual purposes. Figure 1 summarizes the most analyzed types of criminal activities in relation to cryptocurrency based on the literature analysis.

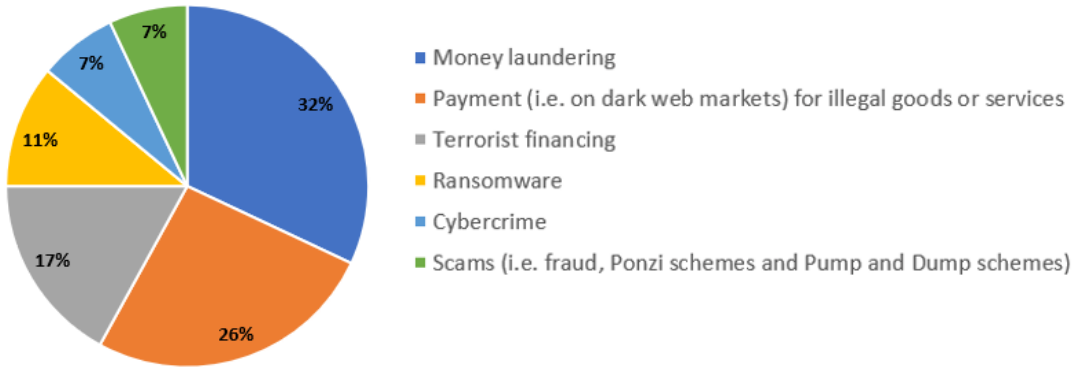

Figure 1. The most analyzed types of criminal activities

Source: Compiled by an author

The main and most examined topic of literature related to cryptocurrency usage for illicit activities is money laundering (Albrecht et al., 2019; Anika, 2019). Money laundering can be described as a method using by criminals to conceal and protect their wealth, which was originated illegally in order to avoid the consequences determined by the law (Anika, 2019). Money laundering has historically been conducted mainly through traditional banking institutions. The intensification of the fight against cross-border crime and money laundering is leading to new methods of carrying out illegal activities. As a result of a new requirement for banking and financial institutions to report suspicious or substantial financial activities and to examine new and existing customers regarding the verification of their identities as well as the source of funds, money launderers are looking for alternatives of less regulated measures to conceal the source of the income gained through their crimes. As cryptocurrency markets remain unregulated, this regulatory gap provides an opportunity for those who want to engage in money laundering and other illegal activity. It is true because cryptocurrencies represent a lack of traditional banking features, for example, it includes non-person to person virtual banking, is decentralized, and has no formal oversight. In 2021, European Commission proposed changes to EU law that would make cryptocurrencies more traceable and would help stop money-laundering and the financing of terrorism by prohibiting the provision of anonymous cryptocurrency wallets. However, the proposals could take two years to become law.

Money laundering basically is a transfer of property, which was obtained as a result of crime, in order to conceal or disguise the illegal origin of the property as well as to help any individual who is involved in this activity to avoid the legal consequences of the actions. There are a lot of factors that attract people to use cryptocurrencies in money laundering schemes, but the main factor is anonymity. Anonymity allows to conduct any transaction using a nickname or pseudonym, therefore there is no need for cryptocurrencies to pass through a regulated bank or

even a third party and it is possible to transfer money without a reason or legitimacy of the payments (Forgang, 2019).

It is important to note that since financial institutions do not issue cryptocurrencies, they are not subject to the same regulations. Without the need for a financial intermediary, individuals can freely trade cryptocurrencies, therefore it is simple to use cryptocurrencies in money laundering schemes. Trading platforms provide an opportunity to legitimately exchange cryptocurrencies. For example, to exchange one cryptocurrency for another or to convert traditional money into cryptocurrency. However, even though anti-money laundering policies and procedures are implemented, it is still possible to find weaknesses to be exploited. There are many examples globally that the largest and most extremely regulated financial institutions can be susceptible to money laundering (Albrecht et al., 2019). In terms of COVID-19 impact, travel restrictions have forced changes to smuggling methods, preventing the use of drug mules and making it harder to physically move cash overseas. Therefore, the pandemic may have reinforced or accelerated pre-existing trends whereby criminals were seeking to use cryptocurrencies to launder funds.

Unlike conventional money laundering mechanisms, cryptocurrency money laundering has the advantage of circumventing geographical constraints, exploiting gaps and overlaps in heterogeneous regulatory systems. The main advantages of cryptocurrency laundering are faster implementation than traditional money laundering, and no authentication is required, as opposed to the Know Your Customer (KYC) obligations of traditional financial institutions (Desmond, Lacey & Salmon, 2019). Based on the forensic analysis of privacy-oriented cryptocurrencies (e.g., Monero and Verge) conducted by Koerhuis et al. (2019), criminals use cryptocurrencies that incorporate anonymity and privacy features in order to eliminate the possibility to trace funds to a particular user using a variety of malware to launder money. Based on the recent events in the markets, the indirect impact of criminal activity could be also identified. For example, due to money laundering and terrorist financing risks, the government of China decided to prohibit supporting digital currency transactions through the banks and payments platforms. The result of such prohibitions led to Bitcoin price to fall below $30,000 in 2021 for the first time in more than five months. Since reaching an all-time high of $64,870 in April, Bitcoin has lost more than half of its value.

One of the costliest types of crimes related to cryptocurrencies is exchange hacks (Goldsmith et al., 2020). Cryptocurrencies provide additional confidentiality, defined by its anonymity, therefore markets that operate on the Darknet (internet website which can be accessed only with specific authorization), use Bitcoin as a channel of exchange (Kethineni et al., 2018). Cryptocurrencies are widely used as a payment mechanism for buying illegal goods and services

in dark online markets (Silfversten et al., 2020). Darknet is a network like which can only be accessible by using certain communication protocols that ensure greater anonymity. Darknet markets are particularly used for selling and buying illegal goods and services as Darknet hides the identities of buyers and sellers (Foley et al., 2019). Bitcoin ensures additional confidentiality to a Darknet market already characterized by its anonymity; hence Bitcoin is commonly used in many of these markets as a medium of exchange (Kethineni et al., 2018). Benjamin et al. (2019) It is also important to highlight that cybercriminals are usually co-operated through Darknet communities such as web forums, creating a valuable data repository.

Silk Road that started in 2011 was the best-known Darknet marketplace, mostly used the sale of drugs, having Bitcoin as the only accepted currency. In 2013, Silk Road was shut down by the U.S. Federal Bureau of Investigation (FBI). However, after it shut down, other Dark markets have emerged (Kethineni et al., 2018). Moreover, a study by Gurrib, Kweh, Nourani and Ting (2019) showed the relation of transactions in the Bitcoin blockchain to the previous sales in darknet markets. Gandal et al. (2018) identified that suspicious trading activity is the cause of Bitcoin fluctuations, especially in late 2013. According to the research results, Bitcoin prices rose by approximately 80% during the days when suspicious trading activity prevailed. Therefore, such activity in the Mt. The Gox exchange was strongly linked to the increase in the Bitcoin price.

Furthermore, cryptocurrencies as an instrument of terrorist financing, are still at a very early stage compared to other criminal activities. Cryptocurrencies can be used to raise funds from and for sponsors and to conduct fundraising activities (Silfversten et al., 2020). Potential users value the same characteristics of cryptocurrencies as money launderers. However, the high volatility of cryptocurrencies acts as a constraint on terrorist financing, as these activities require a reliable source of large funds that cryptocurrencies could not ensure due to constant price fluctuations. Considering fast international transfers all over the world, cryptocurrencies are still a valuable instrument to conduct terrorist financing (Ciupa, 2019).

Cryptocurrencies have also become popular among hackers as a new form of bribery in the event of ransomware attacks since hackers began asking for cryptocurrencies. Unlike traditional forms of cybercrime that thrive unnoticed, ransomware attacks require victim attention and action (Lee et al., 2021). After blocking access to the files, hackers requested to pay in cryptocurrencies, mainly in Bitcoin, Ether and Bitcoin Cash. The reasons for requesting cryptocurrencies rather than conventional financial instruments are due to their global nature which means that the hacker does not have to pay high costs for currency exchange or international transfer operations. Also, by having an anonymous or pseudo-anonymous cryptocurrency, a hacker is able to conceal his identity more effectively. In the case of ransomware attacks, hackers prefer to use cryptocurrencies with lower volatility for more stable profits (Ciupa, 2019).

Another common type of illicit activity is cybercrime. In recent years, cyber attackers have been particularly interested in cryptocurrency. As a result of the spread of cryptocurrencies, it is becoming both a target and an instrument for cybercriminals (Gandal, et al., 2018). In such cases, cryptocurrencies behave more like a commodity or a bearer of securities whose value responds to the changes in regulated financial markets. If the value of certain cryptocurrencies is increasing, it causes a growing appetite to conduct an illicit activity as the potential benefit increased. In general, Caporale et al. (2020) research outcomes propose the presence of significant negative impacts of cyber-attacks on the likelihood for cryptocurrencies to remain in the low volatility regime. This shows the significance of gaining a more profound understanding of the mentioned type of crime and of the measures used by cybercriminals to restrain potentially disturbances to markets.

Furthermore, one of the main problems with cryptocurrencies is security. The media often highlights the usage of Bitcoin for illegal activities. There are a lot of hacking attacks target all component of the Bitcoin system infrastructure, such as merchants accepting Bitcoins, payment processors, digital wallet service providers, and trading platforms. The lack of technical knowledge of users and weak security of intuitional users in the system causes a danger. Due to the irreversibility of Bitcoin operations, it is practically impossible to recover losses (Polasik et al., 2015). Cyber-attacks are considered a significant risk factor by both small and large "miners", whose task is to aggregate unconfirmed transactions into new blocks and add them to the blockchain (Caporale et al., 2021). In addition, Caporale et al. (2021) emphasize that even in the presence of cyber-attacks, stronger cyber security is beneficial in enhancing the risk adjusted returns of cryptocurrencies and trading activity.

According to Scheau et al. (2020), the relation between cybercrime and cryptocurrency is becoming stronger and the consequences are directly connected to the level of development of a particular type of criminal activity. Furthermore, some studies (Corbet et al. 2019; Corbet et al. 2020) identified destabilizing effects of cyber criminality and cryptocurrency by analyzing financial market effects of recent cybercrime events that occurred in cryptocurrency markets. The results of the research showed that the volatility and cross-cryptocurrency correlations of the eight most liquid cryptocurrencies were increased by the hacking events. In addition, the discovered fluctuations are hack-specific and have a different impact on all currencies. Authors also identified that depending on the particular case, abnormal returns associated with the hacks can be from -2% and -24%. The abnormal returns are detected 4 hours prior to the hacking incident and at the time when the hack is announced, abnormal returns revert to zero (Corbet et al., 2019). One possible solution for an investor after a particular hacking event would be to trade from an affected market in other currencies, which would increase volatility and correlation in the markets. For this reason,

cryptocurrency hacking systematically undermines cryptocurrency markets in general. Moreover, small and large miners, responsible for grouping unvalidated transactions into new blocks and entering them in a blockchain describe cyber-attacks as one of the operational risk factors. A study carried out by Phillips et al. (2018) identified that relationships between selected factors and the cryptocurrency price in the short run is affected by specific events in the market (e.g., cyber-attacks and security breaches). In addition, the price of a cryptocurrency fluctuates over time, depending on the impact of the factor on the price. However, media news and market developments also affect the correlations between different cryptocurrencies.

According to Scheau et al. (2020), attackers' preferences are the storage and processing of information spaces as well as the lack of regulation. Only a few organizations protect against the risk of data corruption or privacy breaches, in the same way as only a few organizations anticipate the risk of cryptocurrency volatility. Examples of possible features of financial market manipulation are illegal data leakage and direct counterfeiting. Scheau et al. (2020) emphasize that if the money has already been sent to a cryptocurrency wallet, it is most likely gone. Scammers can simply withdraw funds by buying and selling cryptocurrency. However, notifying the wallet provider can sometimes help stop the transfer, but this practice is rarely successful. Giovanni et al. (2020) suggest that the lagged values in the volume of Bitcoin transactions in the short run have a significant impact on current data breaches and will therefore also affect potential data breaches in the future. However, Conrad et al. (2018) emphasize that investigation on crime-related statistics do not explain the volatility of Bitcoin, despite a popular press release on the specific topic.

Focusing on cybercrime and its impact on the market, some authors (Corbet et al., 2019; Kamps et al., 2018) have identified pump-and-dump schemes as one of the key issues. Pump-and-dump schemes, known since the 18th century can be defined as fraudulent price manipulations that spread misinformation (Kamps et al., 2018). Initially, criminals usually collect a certain product over a period of time and artificially increase the price by spreading false information before selling the product - an action defined as pumping. The sale of collected goods at a higher price resulting from the dissemination of false information is defined as dumping. Because the price has been raised artificially, it tends to fall, resulting in losses to buyers who have purchased the product by disseminating misinformation. Due to technological innovations in the trade in cryptocurrencies, the problem of disinformation has become more relevant in a shorter period of time. Given the lack of regulation and literature on the analysis of pump-and-dump schemes, cryptocurrencies are extremely vulnerable to such market manipulations. Furthermore, the usage of virtual payment methods has increased in the context of investment fraud and Ponzi schemes (Silfversten, 2020).

Considering other scams within the cryptocurrency market, Ponzi schemes are defined as a more complex type of fraud within the cryptocurrency ecosystem with a significant proportion of the volume of cryptocurrency market. Moore, Han and Clayton (2012) define High-Yield Investment Programs (HYIPs) as an online instrument for traditional financial scammers, where people are promised an extremely high return on their investments and interest rates often exceed 1% per day. Ponzi schemes are based on relatively high payouts from a large number of consumers.

To conclude, money laundering is the most examined topic of literature related to cryptocurrency usage for criminal activities. However, there is still little evidence regarding the direct impact of money laundering on cryptocurrency prices. One of the most expensive types of crime involving cryptocurrencies is exchange hacks. Cryptocurrencies are widely used to buy illegal goods and services in Darknet markets. Some authors identified that illegal trading activity caused fluctuations in the price of Bitcoin. Moreover, cryptocurrencies are also popular among hackers in the field of ransomware attacks. Even if Bitcoin shows tremendous potential to challenge traditional payment networks through advances in its technological architecture, the Bitcoin ecosystem has become a common target of attacks by cybercriminals. Based on the literature analysis, hacking events have a direct influence on the volatility and cross-cryptocurrency correlations. In terms of scams, cryptocurrencies are frequently used in fraud, pump-and-dump or Ponzi schemes. Due to the lack of regulation and literature on the analysis of Pump-and-Dump schemes, the cryptocurrency ecosystem is extremely vulnerable to such market manipulations. In addition, Ponzi schemes, defined as a more complex type of fraud, has a significant proportion of the cryptocurrency market volume. It is important to note that the consequences of any criminal activity are directly related its level of development. The increasing value of certain cryptocurrencies increases the appetite for criminal activity as the potential benefits increase. However, the illegal use of cryptocurrencies and criminal activities have a negative impact on user's trust, which can directly affect its value.

1.3 Other drivers of cryptocurrency price

As the impact of criminal activities on cryptocurrency prices was previously analyzed, it is necessary to identify the main drivers of cryptocurrency price. For instance, the price of Bitcoin can be defined as having extremely high volatility in a short term, which reduces its ability to represent an efficient unit of account (Ciaian et al., 2016). Ultimately, price volatility is the one with the greatest differences against major world currencies, such as US dollar, Euro, Yen, British Pound, among all Bitcoin features (Ciaian, Rajcaniova & Kancs, 2016).

Existing literature studies (Kristoufek, 2013; Bouoiyour and Selmi, 2015; Hakim das Neves, 2020) indicate three types of factors determining the price formation of Bitcoin: supply and demand of Bitcoin market forces, the attractiveness of cryptocurrencies as increased interest in certain assets is reflected in their year-on-year appreciation and global macroeconomic and financial factors such as the dollar exchange rate and the stock market index.

Demand and supply. Buchholz et al. (2012) state that the relationship between supply and demand of Bitcoin on the Bitcoin market is one of the main factors of Bitcoin price. For example, Bitcoin supply is measured by the total amount of Bitcoin circulating. The demand for Bitcoins is reflected in the scale of the Bitcoin economy (i.e., its usage in exchanges) and the speed of Bitcoin circulation. Bitcoin speed refers to the frequency at which one unit of Bitcoin is used to purchase goods and services. Quantitative theory suggests that as bitcoin speeds and inventories increase, the price of bitcoin falls, but rises along with the scale and overall price of Bitcoin economy. level (Ciaian, et al., 2016). Demand for Bitcoin is largely determined by its value as a medium of exchange. As a commodity currency such as the gold standard, Bitcoin does not have intrinsic value. The main difference between gold and Bitcoin is that the demand for Bitcoin depends only on its future exchange value, while the demand for commodity currency is determined only by its intrinsic value and the future exchange value (Ciaian, et al., 2016). The supply of Bitcoin is generated by the total number of units issued, which is publicly disclosed and recorded over a long period of time. Although the supply of Bitcoin is exogenous, the supply of gold is endogenous because it responds to changes in processing technology and returns. Given the exogenous nature of Bitcoin's supply, demand shocks are likely to be the main factor in its price volatility. Such shocks to demand could cause significant fluctuations in the price of Bitcoin, changing expectations for future use in exchanges (Ciaian, et al., 2016). In addition, Bouoiyour et al. (2015) emphasize that in the short run, the price of Bitcoin is mainly influenced by the volume variable.

Attractiveness. Several specific Bitcoin variables determine its demand, in addition to main currency price determinants, such as market supply and demand. This is mainly due to the relatively recent creation of Bitcoin and to the complexity of the currency (Buchholz et al., 2012; Kristoufek, 2013; Bouoiyour et al., 2015). First of all, the risk and uncertainty of the entire Bitcoin system could affect its price. Since Bitcoin is a fiat currency and thus, ultimately, it does not have an intrinsic value derived from consumption or its use in production processes and is useless (such as gold). The value of a fiat currency is based on optimism that it will still be useful in the future and will be accepted as a medium of exchange. Trust and acceptance expectations are crucial for Bitcoin, which is a relatively recently released currency and which is expanding its market share, building trust among market participants. Bitcoin is more vulnerable to cyber-attacks than traditional currencies, which can disrupt the entire Bitcoin system and ultimately cause Bitcoin to

breakdown (Moore and Christin, 2013). Third, Bitcoin attractiveness can impact its price as an investment opportunity for future investors. The decisions of potential investors may be affected by an increase or decrease in news media coverage (Guindy, 2021). With many potential investment opportunities and positive search costs, information plays a vital role. Given that investment demand depends on the additional cost of searching for information on potential investments, such as on stock exchanges, investors may prefer those investment opportunities that the media pays special attention to because they reduce search costs. Increased demand to invest in Bitcoin can put pressure on its price (Ciaian, et al., 2016). Ciaian, et al. (2016) describe such evidence for Bitcoin when high price cycles result from changes in positive and negative news. This means that depending on the news that is currently dominating the media, focused investment activity can have a positive or negative impact on the price of Bitcoin. According to Bouoiyour and Selmi (2016) and Polasik et al. (2015), Bitcoin price dynamics are driven more by negative shocks (e.g., bad news) than positive announcements.

Moreover, Hakim das Neves (2020) states that the price and number of searches on Google for the first two terms are cointegrated. Azqueta-Gavaldon (2020) investigated the causal relationship between media coverage and cryptocurrency prices and found a strong correlation between cryptocurrency prices and investment and regulatory-related news. However, media reports on technology and security affect prices, but not the other way around. This can be explained by the fact that technological developments or security issues should not be influenced by price. Overall, this study shows a link between media news and cryptocurrency prices. It is also emphasized that price fluctuations in the short term do not affect criminal activity or technological innovation. A study performed by Park and Park (2020) identified positive cross-correlation between web traffic, social networking features and cryptocurrency performance indicators. The findings suggest that indicators such as the number of top-level domains and the centralization of multiple social networks are useful in measuring cryptocurrency market capitalization, trading volume, and price.

In line with this, Bejaoui, Ben Sassi and Majdoub (2019) compared the dynamics of Bitcoin, Litecoin, Ether and Ripple daily returns and volatilities. The authors found a significant influence of speculative trading behavior of investors in the mentioned cryptocurrencies. By choosing to invest, as well as by imitating a specific investor in the cryptocurrency market (such as the Bitcoin market), they cause price fluctuations and thus market dynamics in the short term. According to Phillips and Gorse (2018), the correlation between social media factors and price intensifies during the bubble series regime. Several authors (Polasik et al. 2015; Sovbetov, 2018; Urquhart, 2018) observed that the attractiveness of cryptocurrencies, expressed in terms of

realized volatility and the volume of Bitcoin sold, are key factors in attracting attention to Bitcoin the next day.

Macroeconomic factors. Some researchers point out that the price of Bitcoin is not significantly influenced by macroeconomic and financial variables in the long run (Icellioglu et al., 2019; Gurrib et al., 2019; Ciaian et al., 2016; Zhu et al., 2017). Bouoiyour et al. (2015) and Alkhazali et al. (2018) comparatively explored that the price of gold is not related to Bitcoin pricing, even if it is generally compared to Bitcoin. Considering the short term, Zhu et al. (2017) present the US dollar exchange rate as evidence that economic factors have a significant influence.

A study conducted by Zhu et al. (2017) on how macroeconomic factors affect the price of Bitcoin using the same variables that affect gold prices found that the price of Bitcoin expressed in US dollar would be depreciated during the appreciation of the US dollar. For example, during the tested period (2014), the US dollar index rose steadily due to the recovery of the US economy, while the price of Bitcoin fell sharply.

Ciaian, et al. (2016) highlighted the role of global macroeconomic and financial growth in Bitcoin prices driven by variables such as stock indices and exchange rates. The macroeconomic and financial indicators can affect the price of Bitcoin through several channels. Stock exchange indices, for instance, can represent the global economy's general macroeconomic and financial developments. Other indicators reflecting significant macroeconomic and financial trends are inflation and price indices. The exchange rate may also show an increase in inflation and therefore have a positive effect on the price of Bitcoin.

The price of cryptocurrencies and macro-financial indicators may also have a negative correlation. If the prices of the stock decrease, it causes a sale of foreign investors' financial assets. While this situation leads to a depreciation of the underlying currency, it can also increase the price of Bitcoin if investors are willing to invest in Bitcoin instead of investing in stocks. The investor's return on the stock exchange will typically reflect the opportunity cost of investing in Bitcoin. This scenario represents a positive relationship between stock indexes and the price of Bitcoin. However, Alkhazali, Bouri and Roubaud (2018) identified that Bitcoin has a weak association with macroeconomic growth because it is difficult to predict Bitcoin returns and volatility after news related to macroeconomic surprises.

According to Icellioglu et al. (2019), due to price interactions with cryptocurrencies, they tend to behave as an investment rather than as a currency, and their prices interact with significant macroeconomic and financial indicators. Economic and financial variables in the model analyzed by Icellioglu et al. (2019) may explain about 70% of Bitcoin price fluctuations. On the contrary, a study by Gurrib et al. (2019) represents that the volatility of cryptocurrencies may not always be affected by macroeconomic news. Although significant changes in returns were observed during

the investigated period, there was no significant news on the same day as the fluctuations occurred. As the long-term relationship was found to be positive, this suggests that price volatility is related to news on social networks in the long run. This can be explained by the growth of active users, e. g. the increasing number of active users leads to greater interest in the cryptocurrency market and vice versa. The use of Bitcoin in trading and stock exchanges may be driven by favorable macroeconomic and financial developments, which will increase its demand, which may have a positive effect on the price of Bitcoin. In addition, Conrad et al. (2018) identified that the volatility of the S&P 500 has a significant negative impact on the long-term volatility of Bitcoin.

To summarize, the existing literature identifies three main factors that determine the supply and demand for pricing, attractiveness, and global macroeconomic indicators such as the dollar exchange rate and the stock market index. Cryptocurrency supply is measured by the total circulation while the demand is determined by cryptocurrency usage in exchanges and the speed of circulation. Some authors argue that Bitcoin price in the short run is largely influenced by volume. Risk and uncertainty can also affect the price. The trust and expectations of acceptance are crucial for Bitcoin as it is currently developing its market, building the confidence of market participants. As the authors claim that the attractiveness of a cryptocurrency affects its price, the decisions of potential investors can be influenced by media coverage. As a consequence, attention-driven investments could have a positive or negative effect on the price of Bitcoin. Some authors emphasize that the dynamics of Bitcoin prices are driven more by negative than positive news. Macro-financial indicators affect the price of a cryptocurrency through stock market indices, inflation, price indices and exchange rates. The price of cryptocurrency and macro-financial indicators may also have a negative relationship, as the volatility of the S&P 500 has a significant negative impact on the long-term volatility of Bitcoin. It has also been found that economic and financial variables can explain around 70% of Bitcoin price fluctuations. On the other way, macroeconomic news may not always affect the volatility of cryptocurrencies.

1.4 The summary of the literature regarding cryptocurrency price volatility and its factors

Based on the literature analysis, the most widely used models for volatility modelling are Autoregressive Distributed Lag (ARDL), Autoregressive–moving-average model (ARMA), Convergent Cross Mapping (CCM), Generalized Autoregressive Conditional Heteroskedasticity (GARCH), Markov switching non-linear specification, Seemingly Unrelated Regressions (SUR), Stochastic volatility (SV), Vector autoregressive (VAR) and Vector Error Correction (VEC) models. The table below summarizes the authors and the key topics where the models were applied.

Sovbetov (2018) investigated factors influencing the prices of the five most commonly used cryptocurrencies such as Bitcoin, Ether, Dash, Litecoin, and Monero, in the short and long-term over the period from 2010 to 2018 using the Autoregressive Distributed Lag (ARDL) technique on weekly basis. However, the ARDL technique is more preferable for a small sample size having a single long-term relationship between the underlying variables.

Bejaoui et al. (2019) applied the MS-ARMA model on Bitcoin, Ether, Ripple and Litecoin daily returns. MS-ARMA model allowed to consider the mean and variance of the regime shift based on the latent state variable St, that acquired a finite number of values.

Table 1

Quantitative methods used for investigation of price volatility and its factors

Author(s) \ Methods	**ADRL**	**ARMA**	**CCM**	**GARCH**	**Markov switching**	**SUR**	**SV**	**VAR**	**VEC**
Alexander et al. (2020)				X					
Alkhazali et al. (2018)				X					
Azqueta-Gavaldon (2020)			X						
Bauwens et al. (2014)				X					
Bejaoui et al. (2019)		X							
Bouoiyour et al. (2016)				X					
Caporale et al. (2020)					X				
Chu et al. (2017)				X					
Corbet et al. (2019)				X					
Corbet et al. (2020)				X					
Giovanni et al. (2020)								X	
Goczek et al. (2019)									X
Gurrib et al. (2019)								X	
Hakim das Neves (2020)									X
Icellioglu et al. (2019)						X			
Liu et al. (2019)				X					
Sovbetov (2018)	X								
Tiwari, Satish (2019)							X		
Zhu et al. (2017)									X

Source: Compiled by an author

Azqueta-Gavaldon (2020) applied the CCM model to examine the causal relationship between narratives and cryptocurrency prices. CCM is a statistical test used for the cause-and-effect relationship between two time series variables that aims to solve a problem whose correlation does not imply a causal relationship. CCM is based on the theory of dynamic systems and can be used in systems with causal variables and having a synergistic effect. CCM model draws conclusions from data templates and associations rather than using a set of parametric equations, which can be impractical when the exact mechanisms are unknown or too complex to be explained by existing data sets. CCM is generated for weakly coupled dynamic systems: time series systems that interact (are linked) as well as their relationships are able to change (are dynamic) over time (Azqueta-Gavaldon, 2020).

The GARCH framework was adopted in a lot of studies in the case of volatility modelling for cryptocurrencies. Bouoiyour et al. (2016) applied numerous GARCH extensions to properly assess Bitcoin price dynamics. Liu et al. (2019) used GARCH-in-mean (GARCH-M) models in order to investigate dynamics between volatility and returns of Bitcoin, Ether and Litecoin. Several authors, such as Alexander et al. (2020) and Bauwens et al. (2014) applied not only a standard GARCH model, but its modifications: GARCH with an asymmetric leverage effect GJR-GARCH and EGARCH. Just like Autoregressive Conditionally Heteroskedastic ARCH(p) model is Autoregressive AR(p) model applied to the variance of a time series, GARCH (p, q) is an ARMA (p,q) model applied to the variance of a time series. The AR(p) models the variance of the residuals or in other words, the time series squared. The Moving Average MA(q) portion models the variance of the process. According to Alkhazali et al. (2018), the standard GARCH (1,1) model best fitted for the data analysis of gold while the most suitable model for Bitcoin data was EGARCH (1,1) with a normal distribution. EGARCH (1,1) model was also applied by Alkhazali et al. (2018) to identify the impact of positive as well as negative macroeconomic news on the returns and volatility of Bitcoin prices over the period from 19 July 2010 to 7 February 2017. Bouoiyour et al. (2016) applied component with multiple Threshold (CMT)-GARCH model and GJR-GARCH specification and Corbet et al. (2020) GARCH and DCC-GARCH for Bitcoin price volatility estimation affected by COVID-19 pandemic. Conrad et al. (2018) used the GARCH-MIDAS model to identify volatility components of cryptocurrencies in both the long and short term. The Mixed Data Sampling (MIDAS) technique allows examining macroeconomic and financial variables sampled at a lower frequency. Particularly, the two-component GARCH-MIDAS model incorporates both a short-term and a long-term component. Chu et al. (2017) applied different GARCH specifications with different distributions for the innovation process (e.g., SGARCH, EGARCH, GJR-GARCH, APARCH, IGARCH, CSGARCH, GARCH, TGARCH) model for Bitcoin, Dash, Dogecoin, Litecoin, Monero and Ripple using daily global

price indices over the period from 22 June 2014 to 17 May 2017. It was found that IGARCH and GJRGARCH models are best suited for modelling the volatility of the most popular and largest digital currencies. As standard GARCH models may provide biased results during breaks (Bauwens, Backer & Dufays, 2014), Ardia et al. (2018) propose Markov-Switching GARCH (MS-GARCH) models. According to the discrete latent variable, the parameters of these models are able to vary over time. However, based on the analysis of the related studies, GARCH (1,1) model is the most suitable and easily adaptable for different time series by including variables in the price dynamic analysis.

Bouveret (2018) suggests an empirical model for a quantitative assessment of cyber risk and losses based on the standard Value-at-Risk (VaR) framework. Caporale and Zekokh (2019) discovered that standard GARCH models might provide comparatively inaccurate predictions of Value-at-Risk (VaR) and Expected-Shortfall (ES) for the four most well-known cryptocurrencies, such as Bitcoin, Ether, Ripple and Litecoin. enabling asymmetry and regime change, as suggested by the authors, could remedy the mentioned shortcomings.

A study by Caporale et al. (2020) applies the Markov switching non-linear specification in order to examine the impact of cyber-attacks on the returns of four cryptocurrencies such as Bitcoin, Ether, Litecoin and Stellar from 2015 to 2019. Using the Markov switching non-linear specification, the authors were able to identify a significant negative effect of cyber-attacks on the likelihood of cryptocurrencies would remain in a low-volatility regime.

Icellioglu et al. (2019) explained the price volatility of cryptocurrencies by macroeconomic indicators, the effects of S&P 500 stock market index, gold price, oil price, 2-year benchmark US bond interest rate and US dollar index on the prices of Bitcoin, Litecoin, Ethereum, and Ripple over the period from August 2016 to April 2019 using Seemingly Unrelated Regressions (SUR) model. The SUR Model allows to interpretation of the units separately. Therefore, the author has generated regression models for Bitcoin, Litecoin, Ether and Ripple and the effect of independent variables on cryptocurrency prices is obtained on a unit-by-unit basis.

Tiwari et al. (2019) compared a number of GARCH and SV models by examining the price returns of Bitcoin and Litecoin in order to determine which model is more suitable for the mentioned cryptocurrencies. The results showed that the most suitable model for Bitcoin is SV and GARCH for Litecoin. According to Tiwari et al. al (2019), SV models are more resistant to poor specifications and radical data changes because, in many cases, SV models outperform GARCH models.

The purpose of the VAR model is to identify how historical data impacts the values of the dependent variable in the present. The VAR model was applied by Hakim das Neves (2020) to examine the return characteristics of cryptocurrencies in order to determine whether

macroeconomic news affects returns. Hakim das Neves (2020) also emphasizes that dependent variables are endogenous. The VAR model was adopted by Giovanni et al. (2020) in a cointegration analysis of data breaches and Bitcoin-related variable relationship.

Zhu, Dickinson and Li (2017) used a VAR model to examine the long-term (data period from 2010 to 2014) dynamic relationship between Bitcoin price and seven other variables using the Johansen test. In addition, the authors built a VEC model based on the VAR model and used a Granger causality test to identify a causal relationship between Bitcoin and other variables. The VEC model can be described as a specific case of the VAR model for variables that are stationary in their differences and can be determined using the specific formation of VAR parameters (Hakim das Neves, 2020). The Granger causality test can verify the existence of a causal relationship between the two variables (Zhu et al., 2017).

The main difference between the VEC model and the VAR model is the significance of the error correction term in measuring how the system responds to long-term equilibrium deviations caused by a variable shock. The advantage of the VEC model is the examination of the economic behavior of the analyzed variables, as it allows to study the dynamics of the variables in both the long and short term, as well as because it aims not to exclude interactions between variables that may be ignored in the course of differentiation. Zhu et al. (2017) also emphasize that the VEC model has the ability to account for any integrated variable relationships.

However, it is also important to highlight that the choice of volatility model is highly dependent on the data source as well as the investigation period and model parameters (Alexander et al., 2020). Although the selection of an appropriate model is one of the key attributes of volatility investigation, the selection of variables included in the model also plays a significant role in achieving accurate results. The different types of variables represent certain markets that affect cryptocurrency markets in a particular way. Table 2 presents the variables mostly used by researchers analyzing cryptocurrency volatility.

Based on Table 2, authors who investigated the dynamics of cryptocurrency price volatility and its factors mostly incorporated the prices of gold, S&P 500 index, oil and Dow Jones Industrial Average (DJIA) index in their volatility models. Corbet et al. (2020) included the Dow Jones Industrial Average in the volatility model as a measure of international financial performance, West Texas Intermediate oil and gold as a representation of commodity markets. The results presented negative correlations of Bitcoin with international stock exchanges.

Sovbetov (2018) incorporated S&P 500 index, Gold, EUR/USD and Effective Federal Funds Rate as the control variables. According to the results of the study, in the Bitcoin, Ether, and Litecoin models, the S&P 500 index shows a weak form of positive significant coefficient (level 10%). Although these positive long-term relationships appear uncertain, they disappear altogether in the

short term because a negative estimate that is statistically significant (10% significance) is only predicted by the Bitcoin model. This confirms that an increase in the S&P 500 index may strengthen the USD against other fiat currencies (including cryptocurrencies).

Table 2

The most used variables in the cryptocurrency market volatility analysis

Variables	Bauwens et al. (2014)	Corbet et al. (2019)	Corbet et al. (2020)	Goczek et al. (2019)	Icellioglu et al. (2019)	Liu et al. (2019)	Sovbetov (2018)	Zhu et al. (2017)
S&P 500	X	X		X	X	X	X	
Gold	X	X	X	X	X		X	X
Oil		X	X	X	X			
VIX		X						
GBP/USD		X						
EUR/USD							X	
US dollar Index					X			X
Consumer Price Index								X
Dow Jones Industrial Average	X		X	X				X
Effective Federal Funds Rate						X	X	X
US Bond interest rate					X			

Source: Compiled by an author

According to the results of the research conducted by Icellioglu et al. (2019), the rise in the S&P 500 index, gold and oil prices increases cryptocurrency prices, while the rise in US bond interest rate and US dollar rate and the 2-year benchmark lead cryptocurrency prices to a fall. The inverse effect of the US dollar index and US Bond interest rate on the cryptocurrency prices suggests that investors prefer alternative investment instruments when the US dollar depreciates, and US bond yields decline. The author discovered that cryptocurrencies demonstrate similar trend as the overall market indicators, such as the stock market index, gold price and oil price. Therefore, cryptocurrencies are more an investment than a currency and prices of such financial assets

interact with major macroeconomic indicators. The economic and financial variables in the model can explain approximately 70% of the Bitcoin price movements.

Moreover, in order to discover volatility in different markets Corbet et al. (2019) included the CBOE Volatility Index, known as VIX symbol. It is a popular measure of the stock market's expectation of volatility implied by S&P 500 index options, calculated and published by the Chicago Board Options Exchange (CBOE). Corbet et al. (2019) identified few significant relationships between separate cryptocurrency markets (with the exception of Cardano) and different periods when in the markets for VIX, the S&P500 and gold are highly volatile. However, high volatility periods of GBP/USD and oil are associated with a significant increase in volatility in the Bitcoin, Ether, Litecoin, Monero and Cardano markets. The relationship between GBP/USD and cryptocurrency market volatility differences is much stronger. The largest differences were found in the Bitcoin and Bitcoin Cash markets, while other significant positive differences were found in the volatility of the Ether and Monero markets. However, Zhu et al. (2017) identified that the US dollar index has the greatest impact on the price of Bitcoin and the price of gold has the least.

Based on the analysis of quantitative methods used to determine cryptocurrency price volatility and its factors, most authors applied the GARCH framework and in particular, GARCH (1,1) model to conduct their investigation. The key benefit of the GARCH model is the large number of specifications that can be adapted to the purpose of the research and the variables selected. The analysis of the variables included in the volatility investigation shows that gold, S&P 500 index, oil and Dow Jones Industrial Average index are used the most widely used. Furthermore, all selected variables were applied to the GARCH models except Dow Jones Industrial Average index. Based on the conducted literature analysis, Dow Jones Industrial Average index was applied in two studies using the GARCH model and the other two using VEC model. However, the scale of studies on cryptocurrency price dynamics is growing rapidly and researchers have already introduced interesting insights. The conducted literature analysis is the basis for the development of a methodology for the investigation of the dynamics between price volatility and criminality in cryptocurrency markets.

2 METHODOLOGY OF INVESTIGATION OF THE DYNAMICS BETWEEN PRICE VOLATILITY AND CRIMINALITY IN CRYPTOCURRENCY MARKETS

The second chapter of the research describes the structure and the process of the statistical research models and provides a detailed plan of methodology (section 2.1). This section includes the construction and substantiation of methods that were applied. For this reason, a detailed methodology was prepared in order to perform the analysis based on the literature analysis conducted in the first chapter. As a result of that, the methodology of this research takes great account of the various methods and variables commonly used by researchers in the related scientific literature. Given the short period existence of cryptocurrencies, many significant price changes have been observed, together with broad structural changes and substantial criminality. Therefore, it is essential to investigate the different behaviors of cryptocurrency investors in the periods before and after criminal incidents. Based on data availability, examined literature, and trends in empirical financial studies, the GARCH method is considered the most suitable way to examine cryptocurrency volatility affected by illegal activities. This chapter begins by introducing the overview of the research structure and by providing a visual scheme of the prepared methodology along with hypotheses, variables and investigation period. The subsequent sections 2.3 and 2.4 impart a construction of separate research models (two multivariate GARCH and DCC GARCH models) by providing justification and formulas of each model. The analysis is set out to determine whether criminal activity is one of the main drivers of cryptocurrencies volatility.

2.1 The research structure for the analysis of cryptocurrency volatility affected by criminal incidents

The methodology, which focuses on the impact of criminal activity in cryptocurrency markets, is divided into two areas. First, the direct volatility changes are examined using multivariate GARCH analysis in order to identify the presence of differing pricing behaviour in the period immediately after criminal incidents in the cryptocurrency market. Secondly, based on the literature focusing on the co-movement of asset prices during periods of crises (Hakim das Neves, 2020 and Corbet et al., 2019) a DCC-GARCH analysis is applied to analyze changing correlations between cryptocurrencies through the inclusion of variables representing traditional financial market products and dummy variables representing criminal incidents in cryptocurrency markets. The structure of the research which provides an overview of methods used is presented in Figure 2. Each component of the methodology is described in more detail further below.

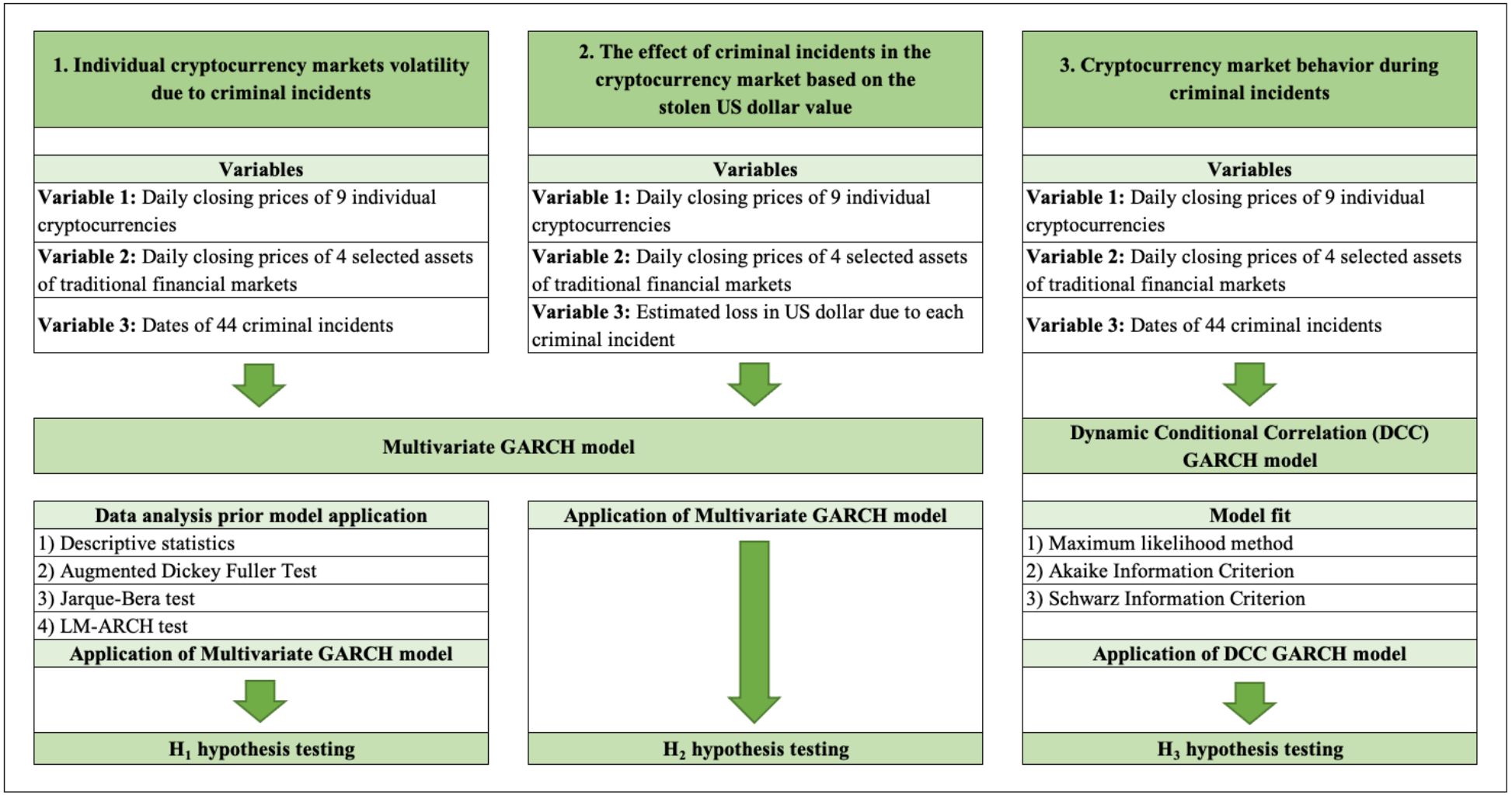

Figure 2. Structure of the investigation of cryptocurrency price dynamics due to criminal incidents

Source: Prepared by an author

Considering the analysis of related scientific studies and the gaps identified in the recent studies, the following three hypotheses were set out in order to analyze the volatility of cryptocurrencies affected by criminal activities:

– H_1: Does cryptocurrency market volatility change significantly in the aftermath of a criminal incident?

– H_2: Does the cryptocurrency volatility vary by severity of criminal incident?

– H_3: Do the conditional correlations between cryptocurrency markets change significantly after criminal incidents?

Each of the hypotheses covers separate parts of the investigation, therefore the results of all three hypotheses are presented in the third part, respectively.

The first part of the analysis employs a multivariate GARCH methodology in order to examine the relationships between the dependent variable (prices of the individual cryptocurrencies) and dummy variables (criminal incidents in the cryptocurrency markets). Multivariate GARCH specification was chosen because of its suitability for multivariate analysis. The development of the first model begins with the selection of individual cryptocurrency markets and dummy variables representing the criminal incidents that have occurred in cryptocurrency markets and the variables that best represent traditional financial markets based on analyzed literature and the determination of investigation period. Furthermore, in line with the analysis of descriptive statistics and correlation matrix between individual cryptocurrencies and traditional financial assets, several statistical tests such as the Augmented Dickey-Fuller Test, Jarque-Bera and LM-ARCH test are conducted prior to model application. A Multivariate GARCH analysis is also applied in the second part to test the second hypothesis.

The third part of the investigation employs DCC-GARCH specification. The focus of the second model is to investigate how the criminal incidents in cryptocurrency markets affect the correlations between cryptocurrencies. This model includes the same variables as the first multivariate GARCH model. The main question analyzed in the second part: do the conditional correlations between cryptocurrency markets change significantly in the aftermath of criminal incidents. Therefore, the DCC-GARCH specification is chosen as the second model of this research to analyze the dynamic behavior of the time series of individual cryptocurrency markets. Moreover, to check model fitting and reliability both Akaike information criterion (AIC) and Bayesian information criterion (BIC) to define optimal variable lag length are employed together with the method of maximum likelihood.

The investigation period and a description of the variables included in all three GARCH models is provided further below.

2.2 Variables used to investigate cryptocurrency volatility affected by criminal incidents

In order to compile a reliable volatility model, the variance equation includes dependent and independent variables. Table 3 provides a summary of all variables used in three separate parts of the investigation.

Table 3

Description of the variables included in the investigation

Variable	Description	Variable type
BTC	Bitcoin daily closing prices in US dollars	Dependent
ETH	Ethereum daily closing prices in US dollars	Dependent
LTC	Litecoin daily closing prices in US dollars	Dependent
XRP	Ripple daily closing prices in US dollars	Dependent
ADA	Cardano daily closing prices in US dollars	Dependent
USDT	Tether daily closing prices in US dollars	Dependent
XMR	Monero daily closing prices in US dollars	Dependent
ZEC	Zcash daily closing prices in US dollars	Dependent
DASH	Dash daily closing prices in US dollars	Dependent
S&P 500	S&P 500 stock market index daily closing prices in US dollars	Independent
Gold	Gold daily closing prices in US dollars	Independent
VIX	VIX (CBOE volatility index) daily closing prices in US dollars	Independent
USD	US dollar index daily closing prices in US dollars	Independent
44 dummy variables	Dates and estimated losses in US dollar of 44 separate criminal incidents occurred in cryptocurrency market during the investigated period	Independent

Source: Prepared by an author

According to Table 3, dependent variables are daily closing prices in US dollar of the five most liquid cryptocurrencies: Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Ripple (XRP), Cardano (ADA), Tether (USDT) and three privacy-oriented cryptocurrencies: Monero (XMR), Zcash (ZEC), Dash (DASH). Daily closing prices from CoinMarketCap.com were collected for the selected data period: from 1 January 2018 to 31 March 2021. Cryptocurrency markets operate 24 hours a day, seven days a week, therefore it provides 1182 daily observations over a selected time period.

Independent variables incorporated in the variance equations include traditional financial assets as well as dates and estimated losses in US dollars of 44 separate criminal incidents that occurred in the cryptocurrency market during the investigated period. Based on the literature analysis, the final selection of traditional financial market assets was based on a broad presentation of stocks, commodities, currencies and options. For this reason, the US dollar index was selected to represent interactions between cryptocurrencies, the S&P500 represents a stock market performance, gold – commodity markets and the VIX (CBOE volatility index) as a representation of options markets and implied volatility respectively. Data representing daily closing prices of selected traditional financial markets for the same time period were collected from Yahoo Finance. However, gold which represents the most infrequently traded commodity has 807 observations, whereas the US dollar index – 808, S&P 500 and VIX – 816 observations of each asset. For the daily closing prices of the selected financial products, the log return for each period, $r_t = \ln(P_t/P_{t-1})$ is estimated.

The investigation incorporates forty-four dummy variables denoteing cryptocurrency criminal incidents that occurred in the cryptocurrency market from 1 January 2018 to 31 March 2021. The list of criminal incidents covers a number of unique situations that focus on hacking and money laundering events, Ponzi schemes, ICO exit scams, frauds, thefts and incidents in Darknet marketplaces. The mentioned data was collected from a variety of publicly available sources without the use of a specific data source. Furthermore, only the incidents that were determined as significant, e. g. the loss is more than one million in US dollars have been included in the list. Table 4 represents the list of 10 criminal incidents included in the price volatility investigation that caused the greatest loss to the markets. A full list of forty-four criminal incidents is provided in Annex 1.

The selected forty-four criminal incidents mostly include incidents that occurred in specific exchanges (25 in total), 11 incidents are associated with cryptocurrency scams, 5 are related to ICO and 3 are related to money laundering. The largest estimated loss was from a cryptocurrency investment scam in the PlusToken platform. On 30 June 2019, early indications of trouble began as users started reporting delays in fund withdrawals. Some users complained of their failure to receive their funds on the Chinese social media website "Weibo," despite the follow-up after 35 hours of the withdrawal request. On 30 July 2020, 109 individuals involved in the PlusToken scheme with have been arrested by the Ministry of Public Security. The scammers have left the scheme by withdrawing more than $3 billion in Bitcoin, Ether and EOS together with leaving message "*sorry we have run*".

Table 4

10 criminal incidents in the cryptocurrency markets that caused the most losses to the markets

No.	Date	Amount	Market	Description
1	2018-01-26	$530m	NEM	26 January 2018, all deposits were suspended in NEM on the Coincheck exchange. Once the hack was confirmed by the exchange, it was then revealed that the hack resulted in a loss of 523 mln. NEM coins, worth approx. $532.6 mln 26 January. The coins were stolen via several unauthorized transactions from a hot wallet.
2	2018-02-08	$195m	Nano	The hack is assumed to have taken place on 8 February 2018, but Nano's developers argue it was insolvent long before February and claim that now they have a reason to believe that Firano misled Nano Core team and the community for a significant period of time in respect of solvency of the BitGrail exchange.
3	2018-04-05	$300m	Bitcoin	GainBitcoin started in 2015 as a multi-level marketing system (MLM) which brought together over 100,000 investors, all of whom promised 10 percent monthly returns. Amit Bhardwaj, who had set up the scheme, moved his base of operations to Dubai while continuing operations in India when the authorities caught up.
4	2018-04-09	$650m	ICO	Two blockchain companies, Ifan and Pincoin, have pulled of the largest alleged ICO scam in Vietnam. Both companies have reportedly duplicated 32,000 investors with some 15 trillion VND ($660 million) in investment. Even though Ifan is registered in Singapore and Pincoin is registered in Dubai, both companies in Vietnam have approached the same company (Modern Tech) in order to announce their projects to potential investors.
5	2018-10-08	$660m	ICO	After pulling an ICO exit scam, the Pincoin operators came out with a $660 million trader fund, which was unsurprising given the 48 percent return the company promised to investors. The cryptocurrency known as Pincoin (PIN) was released back on 12 January. That was the beginning of a scam.
6	2019-05-22	$200m	Bestmixer	Bestmixer.io started operating in May 2018. Just a month later, police started to investigate the mixing service, which found that the so-called leading world crypto mixing service managed to launder on behalf of its customers for at least $200 million in cryptocurrency over the course of the year. On May 22, Bestmixer.io was seized by European police.
7	2019-07-30	$6b	Bitcoin, Ether, EOS	PlusToken allegedly carried out an exit scam, with deposits estimating to $2.9 billion. More than 100 people suspected of engaging in the PlusToken investment scam were arrested by Chinese police. Investors were based mainly in China and in South Korea, who stored Bitcoin, Ether and EOS on the platform.
8	2020-02-13	$300m	Bitcoin	An Ohio man has been arrested for operating the Helix Bitcoin mixing service. It is estimated that the mixer laundered approx. $300 million.
9	2020-06-24	$200m	CryptoCore	Researchers reported that over $200 million cryptocurrency has been stolen from online exchanges by the CryptoCore hacking group.
10	2020-11-03	$1b	Bitcoin	Thousands of Bitcoins that worth $1 billion at the time were seized by law enforcement which was reported as the biggest seizure of cryptocurrency in the history of agency. Justice Department seized the 70,000 bitcoins generated in revenue from drug sales on the Silk Web marketplace from a hacker, named as "Individual X," who moved the cryptocurrency from Silk Road into a wallet the hacker controlled.

Source: Prepared by an author using public sources

In 2020, the local media named Chain News identified that the stolen amount could be closer to $6 billion. In addition, PlusToken was accused of having caused Bitcoin prices to fall in 2019 as stolen funds were sold through Bitcoin Over the Counter (OTC) brokers.

Further details on the methods applied and all formulas for both models are explained in sections 2.3 and 2.4. Finally, the results are composed of literature analysis and the findings of both models.

2.3 Multivariate GARCH analysis for cryptocurrency market volatility due to criminal incidents

According to the structure of the research presented in section 2.1, the response of individual cryptocurrency markets to criminal incidents is examined using a multivariate GARCH model. There are two types of GARCH models: a univariate model that explains the persistence and volatility shock on itself and a multivariate that focuses on analyzing the volatility spillover of a variable on another variable. Therefore, a multivariate GARCH (1,1) methodology is used in the investigation in order to examine the dynamics of volatility in the aftermath of major crimes in the cryptocurrency markets. The GARCH specification was developed by Bollerslev (1986) as an extension of the Autoregressive Conditional Heteroskedasticity (ARCH) model, which includes a moving average component along with an autoregressive component. By introducing a moving average component, the model can design the relative change in variance over time and modifications in time-dependent variance (Chu, Chan, Nadarajah, & Osterrieder, 2017). The general form of the GARCH (p,q) model that includes a parameter p which denotes the total amount of lag variance terms and parameter q indicating the number of lag residual errors to be included in the GARCH model, is as follows:

$$R_t = a + bX_t + \varepsilon_t, \ where\ \varepsilon_t|\Omega_t \sim iidN(0, h_t) \quad (1)$$

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

The formulas presented above indicate that the value of the variance scaling parameter h_t depends on the past value of the shocks obtained by the lagged square residual terms, and on past values of itself, which are acquired by the lagged h_t terms.

Corbet (2019) found that the multivariate GARCH (1,1) model is the most suitable to investigate volatility effects through the use of dummy variables that denote both the day and also periods of significant volatility in traditional markets. Therefore, the multivariate GARCH (1,1) model is employed in further investigation. Furthermore, according to Corbet (2019), it is also

important to minimize foreign impacts that can be achieved by including traditional financial products in the mean equation of GARCH (1,1) specification. Therefore, the volatility caused by shocks that are incorporated into the returns of traditional financial markets is taken into account in the estimation of the volatility of the selected structure. The variance equation also incorporates dummy variables that are denoted as unity in the first five days after the criminal incident and zero otherwise. The multivariate GARCH (1,1) methodology used in this investigation has the following form:

$$R_t = a_0 + b_1 S\&P_t + b_2 Gold_t + b_3 VIX_t + b_4 USD_t + b_5 Bit_t + \varepsilon_t \quad (3)$$

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

$$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{44} D_i \quad (5)$$

$b_1 S\&P_t$ and $b_2 Gold$ indicate the relationship between cryptocurrency returns and the returns of the S&P500 and Gold. $b_3 VIX_t$ indicates the value of the VIX of the day when the estimate R_t is observed, while $b_4 USD_t$ indicates the relationship between the selected cryptocurrency returns and the US dollar index. Finally, $b_5 Bit_t$ indicates the returns of Bitcoin as a representation of cryptocurrency market dynamics (the methodology that analyzes Bitcoin individually, b_5 is denoted as zero). In order to provide a coefficient representing forty-four dummy variables described in Table 4 (full list provided in Annex 1), $\sum_{i=1}^{44} D_i$ is included in the variance equation. The list of criminal events includes a number of unique situations that targeted either the exchange on which cryptocurrencies are traded, the blockchain supporting a specific cryptocurrency or wallets of cryptocurrency investors.

Bollerslev (1986) argued for restrictions on the parameters for positivity, $\omega > 0$, $\alpha \geq 0$ and $\beta \geq 0$, and the broad-sense stationarity condition, $\alpha + \beta < 1$. Furthermore, Nelson (1990) provided evidence that the GARCH (1,1) specification is uniquely stationary if $E[\log(\beta + \alpha\varepsilon^2_t)] < 0$. Bougerol and Picard (1992) generalized such condition for any GARCH (p,q) order model.

Furthermore, based on the research structure presented in section 2.1, the multivariate GARCH methodology is also employed in order to analyze the impact of criminal incidents on the cryptocurrency market based on estimated loss in US dollars. The multivariate GARCH (1,1) methodology applied in the second part has the following form:

$$R_t = a_0 + b_1 S\&P_t + b_2 Gold_t + b_3 VIX_t + b_4 USD_t + b_5 Bit_t + \varepsilon_t \quad (6)$$

$$\varepsilon_t|\Omega_t \sim iidN(0, h_t) \tag{7}$$

$$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + D_{USD\$_i} \tag{8}$$

$b_1 S\&P_t$ and $b_2 Gold$ indicate the relationship between cryptocurrency returns and the returns of the S&P500 and Gold. $b_3 VIX_t$ indicates the value of the VIX of the day when the estimate R_t is observed, while $b_4 USD_t$ indicates the relationship between the selected cryptocurrency returns and the US dollar index. Finally, $b_5 Bit_t$ indicates the returns of Bitcoin as a representation of cryptocurrency market dynamics (the methodology that analyzes Bitcoin individually, b_5 is denoted as zero). Additionally, in order to provide a coefficient relating to the included forty-four dummy variables described in Table 4 (full list provided in Annex 1), the variance equation includes a continuous variable that represents the natural logarithm of the estimated value stolen in US dollars due to criminal incidents.

As a methodology for the first model and the second models is already discussed, the realization of the multivariate GARCH model analysis for the investigation of individual cryptocurrency markets response to criminal incidents and the impact of criminal incidents on the cryptocurrency market based on estimated losses in US dollars is presented in sections 3.1 and 3.2 respectively.

2.4 DCC-GARCH analysis for cryptocurrency market behavior during criminal incidents

A multivariate GARCH analysis is a beneficial starting point for analyzing changes to the volatility of cryptocurrencies due to criminal events. In line with this, the analysis also investigates whether the co-movement of cryptocurrency returns has increased significantly. During periods of financial crises, significant increases in co-movement and the correlation of the returns on traditional financial markets have been observed. Based on the analysis of the past market crashes, Corbet et al. (2019) stress that correlation coefficients depend on market volatility. Therefore, the presence of such co-movements in cryptocurrency markets is first examined, followed by the Dynamic Conditional Correlation – DCC-GARCH methodology, to specifically investigate their response during criminal events.

DCC-GARCH method, first introduced by Engle (2002), enable correlations to change over time rather than requiring them to be constant. The main concept of conditional variance and conditional correlation modeling is that the covariance matrix of a vector of returns, h_t, can be decomposed into the conditional standard deviations, D_t and a correlation matrix, R_t. In the DCC-GARCH model, both R_t and D_t are time-varying. The estimation of Engle's DCC-GARCH model has the following form:

$$h_t = D_t R_t D_t \quad (9)$$

It is important to note that two conditions must be considered when defining the type of the conditional correlation matrix R_t. First of all, the covariance matrix h_t has to be positive. Thus, R_t has to be positive definite (D_t is positive definite since the variance in the univariate GARCH models is all positive in the diagonal elements). Secondly, all elements must be equal or less than the unit within the conditional correlation matrix R_t.

The maximum likelihood method is also applied for model fitting. In order to maximize log-likelihood, the DCC model is estimated through a two-stage approach. If the parameters in R_t, e. g. D_t and ϑ are denoted as θ, the log-likelihood function is:

$$l_t(\theta, \vartheta) = \left[-\frac{1}{2}\sum_{t=1}^{T} nlog(2\pi) + log|D_t|^2 + \varepsilon_t^{'} D_t^{-2} \varepsilon t\right] + [\sum_{t=1}^{T} log|R_t| z_t^{'} R_t^{-1} z_t - z_t^{'} z_t] \quad (10)$$

According to Engle (2002), the DCC-GARCH model is developed to allow the estimation of two-stage conditional variance matrix h_t. During the first stage, univariate GARCH (1,1) volatility models are fitted for each of the return residuals and $\sqrt{h_{it}}$ estimates are derived. In the second stage, return residuals are transformed by their estimated standard deviations from the first stage as $z_{it} = \frac{\epsilon_{it}}{\sqrt{h_{it}}}$. Lastly, the standardized residual z_{it} is applied for the estimation of the correlation parameters.

The first part of the log-likelihood function is volatility, which represents the sum of the separate GARCH likelihoods. In the first stage, the log-likelihood function can be maximized over the parameters D_t. By having parameters estimated in the first stage, the correlation component of the likelihood function in the second stage is maximized to estimate the correlation coefficients. Finally, the change in DCC-GARCH model before and after the criminal incident in cryptocurrency markets occur is examined. In the first part of the analysis, the impact of external shocks on the features of dynamic conditional correlation is estimated using the following time-varying correlation model:

$$\rho_{ij,t} = \omega_{ij} = \sum_{p=1}^{p} \varphi_p p_{ij,t-p} + \sum_{k=1}^{2} \alpha_k DM_{k,t} + \varepsilon_{ij,t} \quad (11)$$

$p_{ij,t-p}$ denotes the pair-wise conditional correlation coefficient between the cryptocurrency i and cryptocurrency j. DM_1 is a dummy variable representing the date of the criminal incident. For the period after the criminal incident, the value of the dummy variable is equal to unity in the first five days after the criminal incident and zero otherwise. The conditional

variance equation is following a GARCH (1,1) specification along with a dummy variable that represents the exact day of the criminal incident, DM_k (k = 1):

$$h_{i,t} = A_0 + A_1\varepsilon_{t-1}^2 + B_1 h_{i,t-1} + \sum_{k=1}^{2} d_k DM_{k,t} \quad (12)$$

Where $A_0 > 0$, $A_1 \geq 0$, $B_1 \geq 0$ and $A_1 + B_1 < 1$.

In the mean equation, coefficient d_1 is statistically significant in all the investigated incidents. Further, in order to estimate the appropriate lag length, both the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) is used.

The AIC according to Akaike (1974) is defined by the following formula:

$$AIC = 2k - 2\ln(\hat{L}) \quad (13)$$

Where k denotes the number of estimated parameters in the model and $\hat{L}$ denotes the maximum value of the likelihood function for the model.

The BIC according to Schwarz (1978) is defined by the following formula:

$$BIC = k\ln(n) - 2\ln(\hat{L}) \quad (14)$$

Where *k* denotes the number of estimated parameters in the model, *n* denotes the number of observations, or the sample size and $\hat{L}$ denotes the maximum value of the likelihood function of the model.

To sum up, the methodology part covered the construction of three research models and presented the statistical tests that should be performed in order to compose a reliable analysis. Moreover, this part also included a detailed explanation and sequence of methodology application that is further used in chapter 3. Therefore, as methods, variables, datasets and hypotheses were examined and introduced, the third part can be implemented, results analyzed, overview and recommendations proposed.

3 INVESTIGATION OF THE DYNAMICS BETWEEN PRICE VOLATILITY AND CRIMINALITY IN CRYPTOCURRENCY MARKETS

As already discussed in earlier chapters, this research is based on two models – multivariate GARCH and DCC-GARCH. First of all, the multivariate GARCH model was applied to analyze individual cryptocurrency markets volatility due to criminal incidents and then to investigate the impact of criminal incidents based on estimated losses US dollar value of nine cryptocurrencies such as Bitcoin, Ether, Litecoin, Ripple, Cardano, Tether, Monero, Zcash and Dash. Further, the DCC-GARCH model was applied to investigate the co-movements in the same cryptocurrency markets in order to analyze their response during criminal incidents. The implementations of the models and the results of three separate investigations, together with the general overview, are presented further below.

3.1 Individual cryptocurrency markets volatility due to criminal incidents

This part first presents the analysis of changes in price volatility and the transfer of volatility in the aftermath of the criminal incident. Particularly, the multivariate GARCH model was employed to analyze how individual cryptocurrency markets behave in the periods after criminal incidents. The model was performed by applying several statistical tests to estimate the model fit as described in section 2.1. The main statistical tests employed before the model application are Augmented Dickey-Fuller Test, Jarque-Bera and LM-ARCH test. First of all, the results of the applied statistical tests are presented by providing tables and explanations. The results of the research presented further below were obtained using “Matlab”, “Eviews” and “OxMetrics”.

The first analysis model includes three groups of variables: (1) daily closing prices of Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Ripple (XRP), Cardano (ADA), Tether (USDT), Monero (XMR), Zcash (ZEC) and Dash (DASH) in US dollars; (2) daily closing prices of S&P 500 index, gold, VIX and US dollar index in US dollars (3) dates of 44 separate criminal incidents (presented in Annex 1) that occurred in the cryptocurrency market between 1 January 2018 and 31 March 2021. Figure 3 represents the price changes of Bitcoin, Ether, Litecoin, Ripple, Cardano, Tether, Monero, Zcash and Dash that were included into the further analysis.

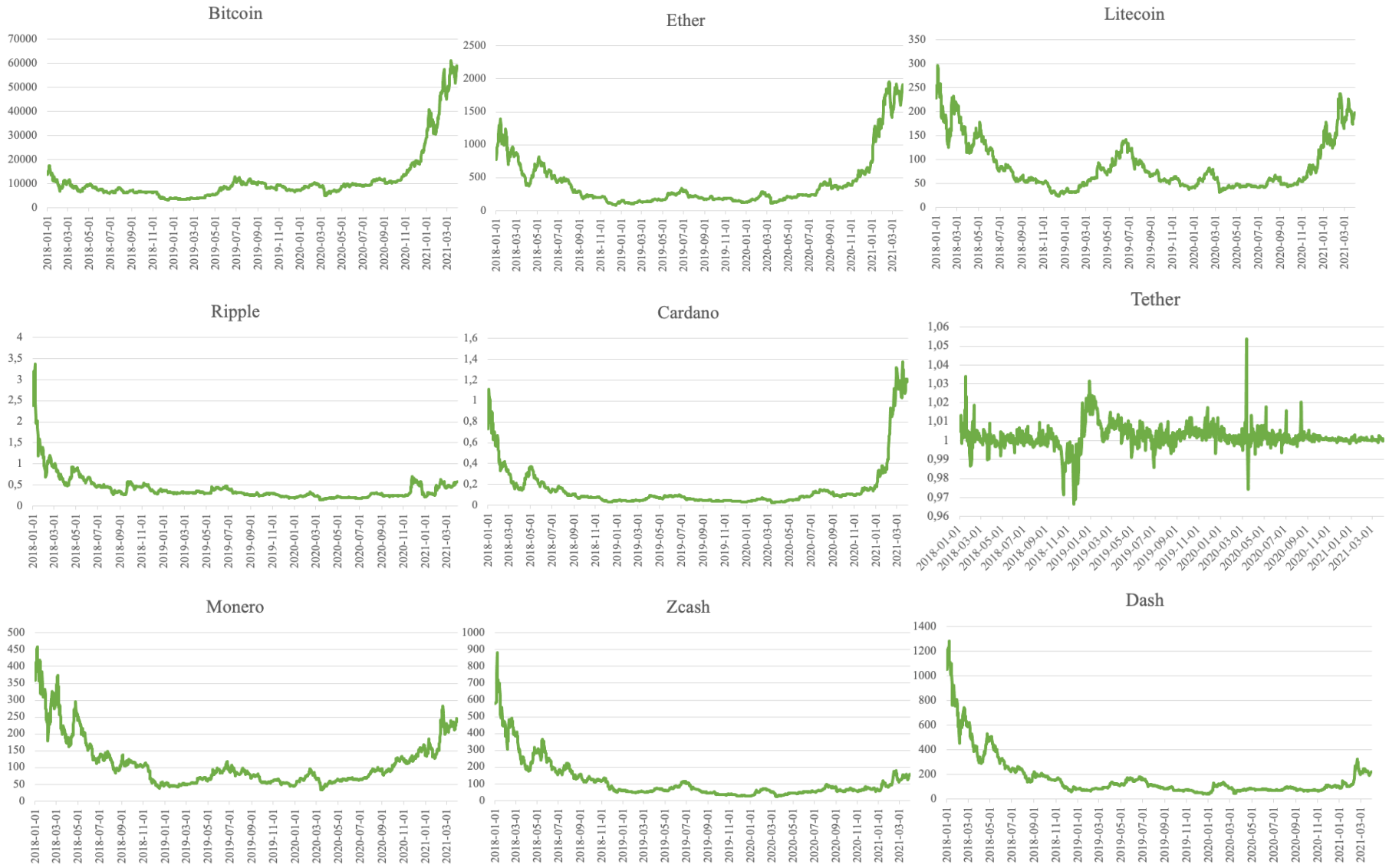

Figure 3. Price trends of cryptocurrencies included in the analysis in the period from 1 January 2018 and 31 March 2021

Source: Prepared by an author according to data from coinmarketcap.com

According to the graphs provided above, there are very large and frequent price fluctuations in some cryptocurrency markets. Especially Litecoin, Monero and Tether. However, as the analyzed period is longer than 3 years, the graphs present only the largest fluctuations of this period. It can therefore be assumed that the market shocks are persistent. Moreover, according to the graphs of cryptocurrency price volatility, all cryptocurrency markets follow similar patterns meaning that Bitcoin and altcoin markets are interrelated. As such effects might be mutual, the relationship between price volatility and criminal incidents in cryptocurrency markets is further investigated in the empirical analysis.

Descriptive statistics. Table 5 presents the descriptive statistics of the selected traditional assets and cryptocurrencies. Overall, 1182 time series of cryptocurrency markets, 816 times series of S&P 500 and VIX, 807 times series of Gold and 806 time series of USD Index are used from 1 January 2018 and 31 March 2021. VIX is the most volatile of the selected traditional financial markets as denoted with daily returns of +0,0009%. All cryptocurrencies reveal a daily average return over S&P 500, the next most volatile traditional asset.

Table 5

Descriptive statistics of the traditional financial assets and cryptocurrencies

	Count	Mean	Variance	St Dev	Skew	Kurt	Min	Max
S&P 500	816	0,0005	0,0002	0,0145	-1,0158	19,1150	-0,1277	0,0897
Gold	807	0,0003	0,0001	0,0099	-0,1322	9,0059	-0,0511	0,0578
VIX	816	0,0009	0,0081	0,0897	1,7496	12,1960	-0,2662	0,7682
USD Index	808	0,0000	0,0000	0,0037	0,2127	4,4635	-0,0163	0,0158
Bitcoin	1182	0,0012	0,0016	0,0404	-1,3408	19,8422	-0,4647	0,1718
Ether	1182	0,0008	0,0027	0,0517	-1,2294	15,5301	-0,5507	0,2307
Litecoin	1182	-0,0001	0,0028	0,0528	-0,2957	9,8616	-0,4491	0,2906
Ripple	1182	-0,0012	0,0036	0,0596	-0,2405	18,3613	-0,5505	0,4448
Cardano	1182	0,0004	0,0038	0,0617	-0,0590	8,8800	-0,5036	0,3218
Tether	1182	0,0000	0,0000	0,0049	0,2793	30,3117	-0,0526	0,0534
Monero	1182	-0,0003	0,0028	0,0528	-0,8859	11,2830	-0,4942	0,2268
Zcash	1182	-0,0011	0,0033	0,0574	-0,2642	7,4747	-0,4129	0,2607
Dash	1182	-0,0013	0,0033	0,0578	0,4559	13,9447	-0,4593	0,4513

Source: Prepared by an author using MATLAB

According to Table 5, Cardano is the most volatile cryptocurrency with a variance of 0,0038 and a standard deviation of 0,0617. The largest increase in price returns occurred in the market for Dash (+45,13%), while the biggest daily loss took place in the Ether market (-55,07%). Kurtosis measures whether the data are heavy-tailed or light-tailed relative to a normal

distribution. As the kurtosis for a standard normal distribution is 3, most of the cryptocurrency markets tend to have heavy tails, or outliers, meaning that these markets are not normally distributed. USD index has the closest value to 3, which is 4,4635. As the skewness of a normal distribution is 0, any symmetric data should have a skewness to be close to 0. According to Table 5, only the skewness of Cardano is the closest to 0.

Table 6 presents the correlation matrix for all of the selected variables used in the investigation.

Table 6

Correlation matrix between traditional financial assets and cryptocurrencies

	S&P 500	**Gold**	**VIX**	**USD Index**	**BTC**	**ETH**	**LTC**	**XRP**	**ADA**	**USDT**	**XMR**	**ZEC**	**DASH**
S&P 500	1,000												
Gold	0,085	1,000											
VIX	-0,709	-0,015	1,000										
USD Index	0,008	-0,709	0,042	1,000									
Bitcoin	-0,093	0,049	0,059	0,082	1,000								
Ether	-0,070	0,060	0,059	0,060	0,825	1,000							
Litecoin	-0,060	0,038	0,039	0,101	0,812	0,836	1,000						
Ripple	-0,046	0,061	0,040	0,102	0,600	0,670	0,648	1,000					
Cardano	-0,086	0,064	0,074	0,087	0,698	0,782	0,727	0,647	1,000				
Tether	-0,004	0,014	-0,026	0,010	-0,035	-0,076	-0,055	-0,068	-0,058	1,000			
Monero	-0,042	0,039	0,023	0,099	0,776	0,761	0,762	0,600	0,685	-0,031	1,000		
Zcash	-0,084	0,024	0,064	0,065	0,694	0,734	0,727	0,621	0,660	-0,015	0,754	1,000	
Dash	-0,071	0,039	0,048	0,076	0,707	0,727	0,734	0,607	0,641	-0,061	0,766	0,814	1,000

Source: Prepared by an author using MATLAB

Based on Table 6, there are three distinct areas of focus, such as the correlations between traditional financial assets and cryptocurrencies separately and the correlations between the two selected asset classes. Intra-cryptocurrency returns correlations present strong co-movement of cryptocurrencies and Bitcoin, except for the correlation with Tether (-0.035). Given the traditional financial market correlations, VIX presents a negative relationship with the S&P500 (-0.709), while Gold shows a relatively low, but still positive correlation with equity markets (+0.085). Before concluding the models, statistical tests of data suitability are performed. First of all, the stationarity of variables is verified by the Augmented Dickey-Fuller test.

Table 7 below shows that none of the variables has a unit root since individual ADF values are higher than their critical values of 5% and 10%, therefore null hypotheses were rejected. For example, ADF for BTC is -36,112, which is higher than -2,864 and -2,568 (stationary at 1st difference). ADF for S&P500 is the lowest compared to the ADF parameters of the other variables, but still higher than -2,865 and -2,569 (stationary at 1st difference).

Table 7

Augmented Dickey-Fuller Test for cryptocurrencies and traditional financial assets

	S&P 500	Gold	VIX	USD Index	BTC	ETH	LTC	XRP	ADA	USDT	XMR	ZEC	DASH
Prob.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
ADF statistic	-8,340	-28,808	-31,853	-26,333	-36,112	-36,125	-36,733	-33,960	-35,205	-21,314	-38,532	-23,195	-35,494
Test critical values													
1% level	-3,438	-3,438	-3,438	-3,438	-3,436	-3,436	-3,436	-3,436	-3,436	-3,436	-3,436	-3,436	-3,436
5% level	-2,865	-2,865	-2,865	-2,865	-2,864	-2,864	-2,864	-2,864	-2,864	-2,864	-2,864	-2,864	-2,864
10% level	-2,569	-2,569	-2,569	-2,569	-2,568	-2,568	-2,568	-2,568	-2,568	-2,568	-2,568	-2,568	-2,568

Source: Prepared by an author using Eviews

Table 8 summarizes the results of the other three statistical tests for all cryptocurrencies used in the further investigation. Traditional financial assets are included as independent variables in the individual equations in order to perform statistical tests. Based on the summarized results, Jarque-Bera statistics show that the normality assumption of the sample data is less than 5% for all cryptocurrencies, which implies that the cryptocurrency returns are likely to follow a non-normal distribution. Furthermore, the LM test shows that the residuals of all cryptocurrency returns have no serial correlation with exception of Tether and Monero as the LM statistics are less than 5%. In case there is no serial correlation, the data can be used for model application and further analysis.

Table 8

Results of statistical tests applied for cryptocurrencies

	BTC	ETH	LTC	XRP	ADA	USDT	XMR	ZEC	DASH
Probability > 0,05									
Jarque-Bera	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000
LM test	0,0979	0,0509	0,2068	0,9187	0,3544	0,0000	0,0260	0,0850	0,9975
ARCH	0,0887	0,0691	0,0117	0,0000	0,0666	0,0000	0,3841	0,0041	0,0004

Source: Prepared by an author using Eviews

In addition, ARCH test performed to verify heteroscedasticity reveals that Litecoin, Ripple, Tether, Zcash and Dash have a p-value of less than 5%. Therefore, the variance of the residuals is unequal over a range of measured values. As cryptocurrencies are generally more volatile than traditional financial assets, the reason for heteroscedasticity is that the observations included are either small or large compared to other observations.

As it was emphasized in the methodology of the investigation, the multivariate GARCH (1,1) model is the most suitable for investigating volatility effects through the use of dummy variables that represent the day and also periods of significant volatility in traditional markets. In the multivariate GARCH (1,1) equation applied in the first part of the investigation, international effects are incorporated through the inclusion of the traditional assets: S&P500, gold, VIX and USD index. Moreover, Bitcoin, as the market-leading cryptocurrency in terms of market capitalization, is used as a control variable in the investigation of selected cryptocurrencies, with the exception of the methodology related to Bitcoin itself. Due to the specific features of the "Oxmetrics" software, the multivariate GARCH (1,1) model applied for each investigated cryptocurrency market followed a normal distribution. Therefore, the outcome of the applied model is considered reliable. The results of volatility analysis affected by each of 44 criminal incidents that occurred during the investigation period using multivariate-GARCH methodology are presented in Table 9. Graphical presentation of the volatility shocks in nine cryptocurrency markets is provided in Figure 4.

Table 9

Volatility of individual cryptocurrency markets due to criminal incidents

Variable	BTC	ETH	LTC	XRP	ADA	USDT	XMR	ZEC	DASH
S&P 500	0,1278	0,1365	0,1219	0,1243	0,1318	0,1204	0,1276	0,1460	0,1110
Gold	0,0999	0,0692	0,0731	0,0555	0,0543	0,1649	0,0724	0,0610	0,0825
VIX	-0,1352	-0,1552	-0,1753	-0,1396	-0,1317	0,1347	-0,1510	-0,1503	-0,1170
USD Index	-0,0631	0,0511	0,0743	0,0359	-0,0460	-0,9775	0,1038	0,1018	-0,0259
Bitcoin	-	0,8289	0,8109	0,6775	0,7055	-0,1582	0,7428	0,7031	0,7347
D_1	0,0010	0,0026	0,0026	0,0058	0,0029	0,0008	0,0016	0,0013	0,0012
D_2	0,0009	-0,0013	0,0021	0,0045	-0,0016	0,0002	0,0007	0,0073	-0,0010
D_3	-0,0023	-0,0009	0,0025	0,0019	-0,0016	-0,0004	-0,0003	-0,0011	-0,0012
D_4	-0,0002	-0,0003	-0,0021	-0,0003	-0,0001	-0,0002	-0,0005	0,0001	-0,0007
D_5	0,0016	-0,0006	0,0001	0,0026	-0,0001	0,0006	0,0014	0,0010	0,0009
D_6	0,0069	0,0005	-0,0006	-0,0012	-0,0015	-0,0005	0,0005	0,0008	0,0003
D_7	-0,0006	-0,0006	-0,0002	0,0019	-0,0006	0,0010	0,0005	0,0018	0,0001
D_8	-0,0003	-0,0004	-0,0001	0,0001	-0,0004	-0,0001	0,0005	-0,0002	0,0004
D_9	-0,0004	-0,0006	0,0003	0,0029	0,0010	0,0001	-0,0001	0,0005	-0,0001
D_{10}	-0,0002	-0,0006	-0,0004	-0,0001	-0,0004	-0,0002	0,0002	0,0059	-0,0001
D_{11}	0,0008	0,0008	0,0002	-0,0005	0,0012	0,0004	0,0005	0,0009	0,0003

Continuation of Table 9

D_{12}	**-0,0003**	**-0,0002**	**0,0003**	**0,0033**	**-0,0010**	**0,0001**	**0,0007**	**0,0014**	**0,0005**
D_{13}	0,0002	0,0021	-0,0001	-0,0006	-0,0001	0,0000	0,0000	-0,0008	-0,0003
D_{14}	0,0001	0,0018	-0,0004	0,0001	0,0002	0,0000	0,0004	0,0006	-0,0002
D_{15}	-0,0002	-0,0007	-0,0005	-0,0018	-0,0011	-0,0008	0,0002	-0,0003	0,0071
D_{16}	0,0004	0,0000	-0,0002	0,0048	0,0004	-0,0002	-0,0003	-0,0003	-0,0003
D_{17}	-0,0013	0,0008	0,0004	0,0039	0,0006	-0,0001	0,0002	-0,0001	0,0004
D_{18}	-0,0009	-0,0009	-0,0006	-0,0006	-0,0009	-0,0005	-0,0006	-0,0008	-0,0003
D_{19}	0,0010	-0,0008	0,0016	0,0007	0,0006	0,0003	0,0005	-0,0007	0,0004
D_{20}	0,0008	0,0007	0,0014	0,0010	0,0006	0,0004	0,0006	0,0003	0,0004
D_{21}	0,0008	0,0008	0,0008	0,0003	0,0016	0,0004	0,0008	0,0004	0,0006
D_{22}	-0,0001	-0,0005	0,0001	-0,0010	-0,0003	-0,0001	-0,0005	-0,0002	-0,0008
D_{23}	0,0000	-0,0003	-0,0001	-0,0008	-0,0002	0,0000	-0,0002	-0,0003	0,0001
D_{24}	0,0048	0,0009	0,0008	0,0093	0,0024	0,0007	0,0013	0,0007	0,0006
D_{25}	-0,0036	0,0004	0,0009	-0,0042	-0,0022	0,0004	0,0009	0,0002	0,0006
D_{26}	0,0009	0,0013	0,0007	0,0007	0,0001	0,0001	0,0004	0,0034	0,0015
D_{27}	0,0001	-0,0004	-0,0005	0,0082	0,0001	0,0000	-0,0001	0,0000	-0,0004
D_{28}	-0,0006	-0,0006	-0,0005	-0,0006	-0,0006	-0,0006	-0,0004	-0,0006	-0,0006
D_{29}	-0,0009	-0,0009	-0,0004	-0,0004	-0,0004	-0,0004	-0,0004	-0,0009	-0,0009
D_{30}	-0,0003	0,0028	0,0006	0,0007	-0,0006	-0,0003	0,0002	-0,0006	-0,0001
D_{31}	0,0001	0,0001	0,0001	-0,0002	-0,0001	0,0000	0,0002	0,0003	0,0005
D_{32}	0,0056	0,0031	-0,0004	-0,0006	-0,0005	0,0005	0,0002	-0,0008	-0,0002
D_{33}	0,0064	0,0077	0,0032	-0,0001	0,0033	0,0006	0,0063	0,0009	0,0005
D_{34}	0,0002	-0,0004	0,0002	-0,0005	-0,0001	0,0004	-0,0003	-0,0002	-0,0002
D_{35}	-0,0002	-0,0004	-0,0003	0,0000	-0,0005	0,0000	-0,0003	-0,0002	-0,0004
D_{36}	-0,0008	-0,0008	-0,0002	-0,0003	0,0002	-0,0002	-0,0004	-0,0003	-0,0001
D_{37}	-0,0002	-0,0023	-0,0002	-0,0006	-0,0011	-0,0002	-0,0003	-0,0006	-0,0005
D_{38}	-0,0001	-0,0001	-0,0003	-0,0006	0,0003	-0,0001	-0,0001	-0,0003	-0,0001
D_{39}	-0,0010	-0,0015	-0,0002	-0,0004	-0,0006	-0,0001	0,0001	0,0003	-0,0001
D_{40}	-0,0001	-0,0002	-0,0001	-0,0006	-0,0004	-0,0035	-0,0001	-0,0007	-0,0003
D_{41}	0,0004	0,0001	0,0006	-0,0003	0,0003	0,0001	0,0000	0,0017	0,0002
D_{42}	0,0004	0,0000	0,0008	-0,0003	0,0003	0,0001	0,0000	-0,0016	0,0004
D_{43}	-0,0016	-0,0003	-0,0003	-0,0008	-0,0005	-0,0002	-0,0004	-0,0007	0,0002
D_{44}	-0,0001	-0,0002	-0,0001	0,0017	0,0014	-0,0002	-0,0003	-0,0005	-0,0004
ARCH	0,1440	0,1069	0,0573	0,6275	0,1135	0,1535	0,1083	0,1746	0,2134
GARCH	0,8077	0,8066	0,8847	0,3702	0,8101	0,7915	0,8549	0,6323	0,7535

Source: Prepared by an author using OxMetrics

Based on the results presented in Table 9 and graphical visualization provided in Figure 4, there is a strong significant and positive relationship between Bitcoin and the cryptocurrencies analyzed, with the exception of Bitcoin and Tether (-0,1582).

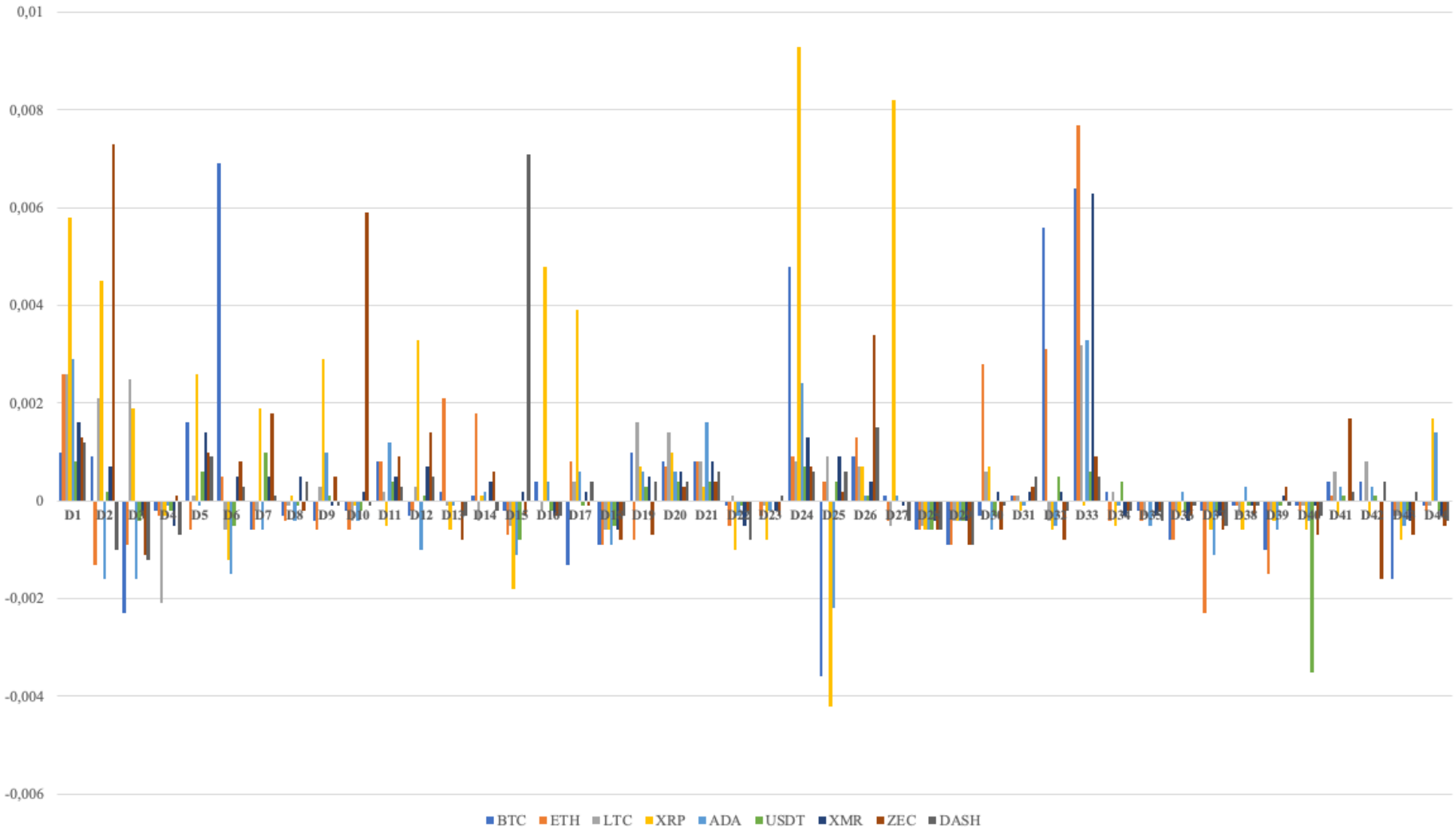

Figure 4. Volatility shocks of individual cryptocurrency markets in the aftermath of the criminal incidents

Source: Prepared by an author

While all the analyzed cryptocurrencies present positive relationships with returns of the traditional assets such as the S&P 500 and gold, VIX shows a negative relationship with cryptocurrencies, with the exception of Tether. Moreover, Tether presents a significant negative relationship with the USD index (-0,9775). This is the case because Tether is pegged to the value of a US dollar. Bitcoin, Cardano and Dash also have a negative relationship with the USD index, but it is not as significant. The cumulative ARCH and GARCH coefficients presented at the bottom of Table 9 were found to be less than unity throughout all individual cryptocurrency markets.

Although there are many different responses, the results in all analyzed markets appear to be not significantly uniform and indicate that responses of all markets to the investigated criminal incidents differ in terms of volatility. However, there are broad responses for criminal incidents 1, 3, 6, 10, 24, 27 and 33. Criminal incidents 1 and 3 are related to a cybercrime event within an exchange (Coincheck and BitGrail respectively), which traded a broad number of cryptocurrencies, thus presenting a theoretical possibility to influence different cryptocurrency markets. Furthermore, incidents 6, 24, 27 and 33 are associated with cryptocurrency scams and incident 10 is related to criminal activity that has taken place at the time of the ICO. Such findings suggest that there are broad differences in volatility changes of cryptocurrencies that support significant instability generated through cyber-attacks in exchanges and ICO fraud, which can be considered strongly dependent on perceptions of stability and financial safety. Any threat to such stability has been found to provoke a broad response in many cryptocurrency markets rather than at the individual level.

The investigation also revealed evidence of market-based cryptocurrency volatility that has been directly targeted by the specific criminal incident. Such evidence is identified in the market of Bitcoin in criminal incident 6 (0,0069), Ether during criminal incident 13 (0,0021), 14 (0,0018), 30 (0,0028) and 37 (-0,0023), Ripple incident 23 (-0,0008) and 25 (-0,0042) and Tether incident 40 (-0,0035). In addition, some of the unmentioned criminal incidents are found to be quite geographically specific and market-specific, relating to cryptocurrencies that are not included in the investigation due to their low liquidity. Despite many alternative specifications of investigation, there is a number of differing cases where the levels of GARCH-calculated volatility for individual cryptocurrencies are high. Considering the sharp volatility responses during criminal incidents that appear to be targeted at cryptocurrencies directly involved and the wider sector of cryptocurrencies, the first hypothesis is accepted throughout the investigated cryptocurrency markets.

3.2 The impact of criminal incidents on the cryptocurrency market based on estimated losses

This part presents the analysis of price volatility due to criminal incidents in the cryptocurrency market based on the stolen value in US dollars. Similar to the analysis presented in section 3.1, the multivariate GARCH model was employed to analyze the second hypothesis: whether the severity of each criminal incident is related to the level of volatility incurred during that time. The second analysis model includes three groups of variables: (1) daily closing prices of Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Ripple (XRP), Cardano (ADA), Tether (USDT), Monero (XMR), Zcash (ZEC) and Dash (DASH) in US dollars; (2) daily closing prices of S&P 500 index, gold, VIX and US dollar index in US dollars and (3) estimated loss in US dollars due to each of 44 separate criminal incidents (presented in Annex 1) that occurred in the cryptocurrency market during 1 January 2018 and 31 March 2021. The results of the second analysis are presented using a continuous dummy variable denoting the scale of the loss in each cryptocurrency market investigated. The parameters of each established model and research results obtained using "OxMetrics" are presented in Tables 10 and 11 below.

Table 10

Parameters of the multivariate GARCH (1,1)

Parameters	BTC	ETH	LTC	XRP	ADA	USDT	XMR	ZEC	DASH
ARCH	0,13609	0,10613	0,03008	0,19247	0,10968	0,14930	0,10850	0,10190	0,11360
GARCH	0,80805	0,80759	0,87053	0,79893	0,81452	0,78720	0,85480	0,81640	0,81360
Mean	0,00123	0,00077	-0,00013	-0,00120	0,00042	-0,00001	-0,00032	-0,00110	-0,00131
Skewness	-1,34280	-1,23135	-0,29619	-0,24114	-0,05900	0,27972	-0,88749	-0,26481	0,45645
Variance	0,00163	0,00266	0,00278	0,00354	0,00379	0,00002	0,00278	0,00328	0,00332
Kurtosis	19,909	15,582	9,895	18,424	8,910	30,414	11,321	7,500	13,992
Log Likelihood	1292,350	1880,548	1167,748	1868,235	1102,757	3421,664	1304,353	1217,813	1213,085
Alpha+Beta	0,94414	0,91372	0,90061	0,99140	0,92420	0,93650	0,96330	0,91830	0,92720
Unconditional variance	0,00203	0,00280	0,00277	0,05673	0,00392	0,00198	0,00247	0,00149	0,00198

Source: Prepared by an author: OxMetrics software output

According to Table 10, Bitcoin presents the highest mean while the market of Dash presents the lowest. The parameters unconditional variance shows that Ripple has the highest unconditional variance, indicating the variance that does not change over time. On the other hand, Zcash has the lowest unconditional variance parameter. The unconditional variance measures the overall uncertainty. While the skewness of a normal distribution is 0, therefore any symmetric data

should have a skewness near 0. According to Table 10, the skewness of Cardano is the closest to 0. Such a result is similar to the descriptive statistics presented in Table 5. However, the processed parameters of the multivariate GARCH (1,1) model have different values. The model of Tether has the highest kurtosis and Zcash has the lowest, meaning that the Zcash model is closest to the normal distribution compared to other cryptocurrency markets because the kurtosis for a standard normal distribution is 3. Although some cryptocurrency markets have skewness significantly greater or lower than 0 and the kurtosis parameters are greater than 3, OxMetrics software output indicates that all established models follow a normal distribution. As $E[\log(\beta + \alpha\varepsilon^2_t)]$ is less than 0, the GARCH (1,1) specification is uniquely stationary. Moreover, positivity constrains (alpha(L) / [(1 – beta(L)] >=0) for the GARCH (1,1) models is also observed. The sum of the parameters alpha and beta is less than 1. It is important to note that OxMetrics software automatically applies the maximum likelihood method for model fitting. For this reason, Table 10 presents the maximum possible log likelihoods for each market investigated. The values of independent variables and volatility trends are presented in Table 11 below.

Table 11

Volatility of individual cryptocurrency markets based on the stolen value in US dollars

Variable	BTC	ETH	LTC	XRP	ADA	USDT	XMR	ZEC	DASH
S&P 500	-0,2505	0,3809	0,0008	0,4644	0,4397	0,5566	-0,3228	0,3632	0,1096
Gold	0,1304	0,0275	-0,1004	0,0452	0,1383	0,0151	-0,2156	0,0710	-0,0208
VIX	-0,0695	-0,0096	-0,0183	0,0258	0,0005	0,0074	-0670	-0,0605	-0,0551
USD Index	0,0001	0,3924	-0,2422	0,3731	0,2575	0,7551	-0,4119	-0,0659	0,4199
Bitcoin	-	0,7505*	0,9132*	0,7696*	0,2351*	0,0382*	0,8593*	0,1734*	0,0941*
Volatility before	0,1489	0,1124	0,0848	0,0516	0,0118	0,0343	0,0457	0,0148	0,0153
Volatility after	0,2450	0,2908	0,3330	0,1756	0,2038	0,2503	0,1772	0,1115	0,0738
Volatility change	0,0961*	0,1784*	0,2482*	0,1240*	0,1920	0,2160	0,1315*	0,0967	0,0585

Source: Prepared by an author using OxMetrics

The total amount of losses incurred as a result of the 44 criminal incidents selected for investigation is $10,7 billion. Losses due to criminal incidents 27 and 41 account for more than half of the total loss as the criminal incident 27 caused losses of approximately 6 billion and incident 41 – $1 billion. Based on the results of the analysis presented in Table 10, five markets present significant evidence indicating that volatility is correlated with the size of the criminal incident (Bitcoin, Ether, Litecoin, Ripple and Monero) as *indicate significance at 10%. Bitcoin was specifically involved in 15 criminal incidents (e. g. 4, 5, 6, 8, 9, 15, 16, 21, 24, 26, 28, 32, 33,

39 and 41) of 44 criminal incidents that were selected for this investigation, making losses of approx. 4 billion US dollar. 11 criminal incidents e. g. 2, 13, 14, 15, 26, 27, 29, 30, 32, 37 and 39) resulted in approx. 2,3 billion US dollar in losses were specifically related to Ether. Litecoin was particularly stolen only during criminal incident 26. Ripple was specifically involved in 4 criminal incidents (e. g. 20, 23, 25 and 26) that resulted in approx. $33 million in losses. Monero, on the other hand, was not particularly involved in any of 44 criminal incidents. However, in practice, Monero is often used in various criminal activities from Ponzi schemes to drug trafficking, money laundering and tax evasion due to privacy-enhancing and protecting features.

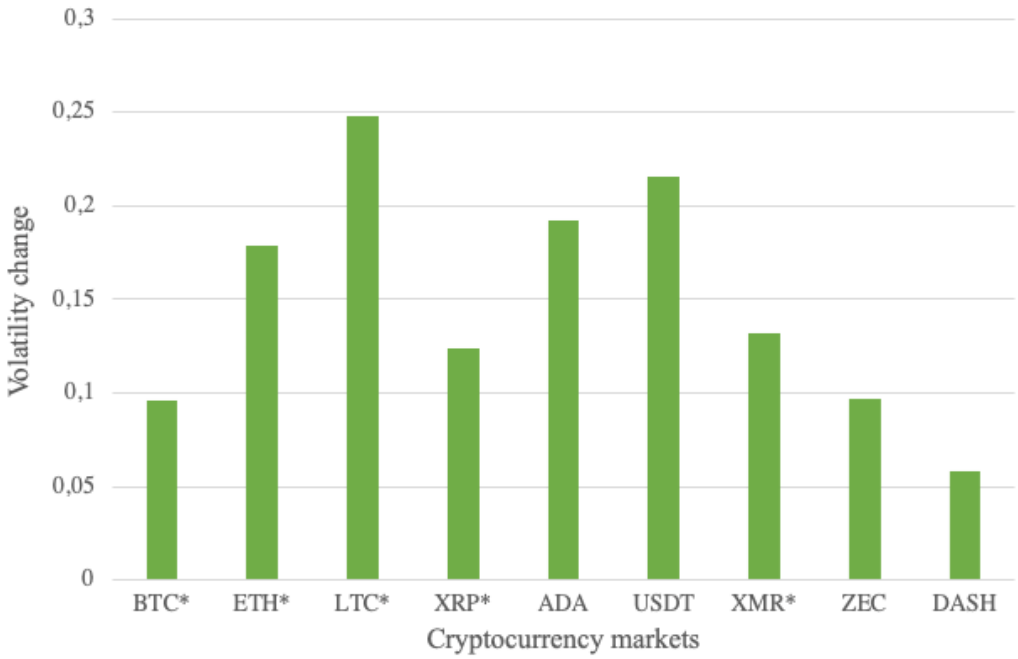

Figure 5. Volatility changes of individual cryptocurrency markets based on the stolen value in US dollars

Source: Prepared by an author

Figure 5 presents the volatility changes of nine cryptocurrency markets due to the scale of losses caused by 44 criminal incidents. It is important to note that although the results of five markets remain insignificant, the results for all investigated markets are positive throughout this analysis. Cardano and Tether present evidence of a significant relationship between the dollar-valued scale of criminal incidents and the GARCH-calculated volatility measure. In the case of Cardano, there is only one criminal incident (criminal incident 25) that specifies the theft of this cryptocurrency. However, the losses are insignificant compared to other criminal incidents because only 2,5 million in Cardano (approx. $4 million) were stolen from the hot wallet registered in Bitrue, a Singaporean exchange. It is also important to note that Cardano is also highly sensitive to the high volatility of the broader cryptocurrency market. Its token fell by almost 90% in less

than two months at the beginning of 2018, as the regulatory environment led the emerging industry to a bear market, which lasted for many years.

Tether is commonly known as a stable coin, typically backed by a fiat currency like the US dollar or the Euro. The primary purpose of a stable coin like Tether is to maintain its value of $1 all the time. Since each USDT is backed by the reserves held by the Tether Treasury, maintaining that value should be simple. However, the value of Tether's asset has fluctuated over years. For example, in July 2018, the Tether reached a record high of $1,32. The price fluctuations occur when demand for a token change. Due to specific features that enable Tether to ensure stability, it is commonly used in online crypto exchanges for converting and exchanging stable coins into another cryptocurrency, especially on exchanges where the standard fiat currencies are not accepted. Furthermore, more stable cryptocurrencies, such as Tether are likely to be preferred for illegal activities that require long term planning (e.g., money laundering). A criminal incident 40 may have had a substantial influence on such result. During criminal incident 40, the hacker stole approx. $24 million worth of cryptocurrency from Harvest Finance, a web portal that allows users to invest cryptocurrencies and then manipulate variations in price to achieve small profits. Specifically, the hacker stole $11 million worth of Tether and $13 million worth of USD Coin (USDC). It is worth mentioning that the hacker returned $2,5 million to the platform two minutes after the attack, but the reason for such action remains unclear. Further, in October 2021, Tether settled allegations that it misled about its digital currency being backed by fiat currencies by paying a fine of $41 million to the US Commodity Futures Trading Commission. Tether committed to submit periodic attestations and audits of its reserves that were discovered to be stored in high-risk assets, including loans and other cryptocurrencies rather than cash or cash equivalents. However, due to the fact that Tether is backed by the US dollar, results may present a significant relationship between the criminal incidents and estimated changes of volatility, as losses are scaled in the US dollars.

To conclude, although the results of five cryptocurrency markets remain insignificant, all the estimates are positive throughout this analysis, with Cardano and Tether demonstrating a substantial positive relationship between the dollar-valued scale of criminal incidents and GARCH-calculated volatility measure, therefore the second hypothesis is accepted: cryptocurrency volatility varies by the severity of the criminal incident.

3.3 Cryptocurrency market behavior during criminal incidents

This part first represents the analysis of dynamic correlations between selected cryptocurrencies using a DCC-GARCH methodology to analyze the third hypothesis investigating whether such dynamic correlations change after criminal incidents. The third analysis model includes three groups of variables: (1) daily closing prices of Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Ripple (XRP), Cardano (ADA), Tether (USDT), Monero (XMR), Zcash (ZEC) and Dash (DASH) in US dollars; (2) daily closing prices of S&P 500 index, gold, VIX and US dollar index in US dollars and (3) dates of 44 separate criminal incidents (presented in Annex 1) that occurred in the cryptocurrency market during 1 January 2018 and 31 March 2021.

Given estimates of the same dynamic correlation relationship in the period surrounding each criminal incident, this investigation presents a variety of interesting findings. First of all, it is observed that cryptocurrency estimates for smaller capitalizations are lower compared to the cross-correlation between their larger counterparts. This applies not only to dynamic correlations between smaller cryptocurrencies but also to relationships between smaller and larger cryptocurrencies.

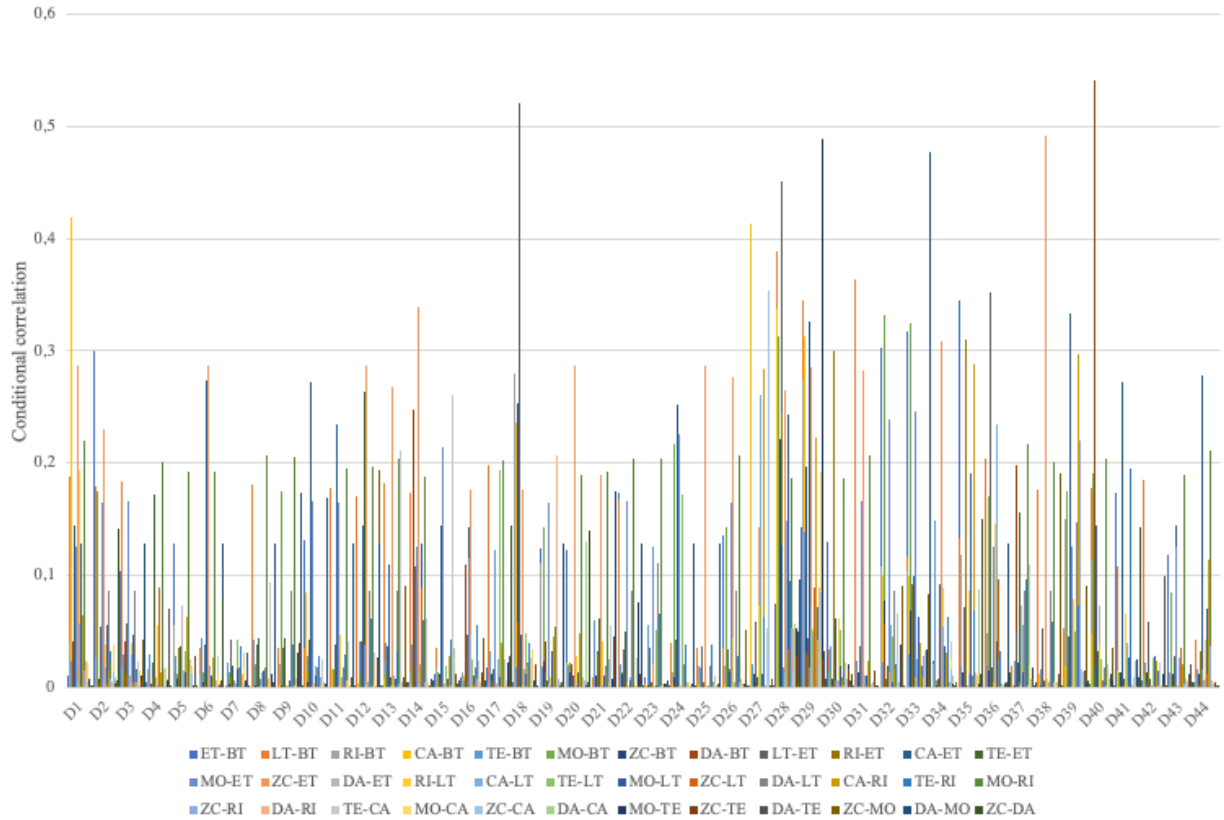

Figure 6. Dynamic conditional correlations between cryptocurrency markets during criminal incidents

Source: Prepared by an author

Figure 6 shows the tendency of how the dynamic correlations between cryptocurrency markets changed during particular criminal incidents. Considering the average dynamic correlation between each cryptocurrency pair included in the analysis, the highest cross-correlations for cryptocurrencies were found to be based on the relationships between Ether and Bitcoin, Litecoin and Bitcoin, Cardano and Bitcoin, Monero and Bitcoin, Litecoin and Ether, Cardano and Ether, Zcash and Ether, Monero and Ripple, and finally Dash and Monero (all estimates of average dynamic correlations are calculated as +0,05).

For presentation purposes, Table 12 presents only the main findings of dynamic correlations between the selected cryptocurrencies during criminal incidents. All the results of dynamic correlations between selected cryptocurrencies at the time of each criminal incident are presented in Annex 2.

Table 12

Main findings of dynamic conditional correlations between cryptocurrency markets during criminal incidents

Findings	**Criminal incident number**	**Criminal incident date**	**Counterparties**	**Change in cross-correlations (at peak)**
1	1 through 3	26th of January 2018 through 8th of February 2018	Ether and Bitcoin Monero and Bitcoin	0,3001; 0,1747
2	17 through 19	8th of October 2018 through 27th of March 2019	Litecoin and Ether Ripple and Bitcoin, Cardano and Bitcoin Zcash and Bitcoin	0,5213; 0,2797; 0,2361; 0,2527
3	23 through 25	1st of June 2019 through 27th of June 2019	Cardano and Ether Monero and Bitcoin	0,2173; 0,2522
4	27 through 29	30th of July 2019 through 9th of November 2019	Litecoin and Ether Monero and Bitcoin Ripple and Ether Cardano and Bitcoin	0,4512; 0,3132; 0,2447; 0,4137
5	28 through 30	28th of October 2019 through 27th of November 2019	Cardano and Ether Monero and Tether Monero and Cardano Litecoin and Bitcoin	0,3262; 0,4893; 0,1915; 0,3881
6	30 through 32	27th of November 2019 through 5th of February 2020	Litecoin and Bitcoin Zcash and Ripple	0,3644; 0,0283
7	31 through 33	12th of December 2019 through 14th of February 2020	Monero and Bitcoin	0,3323

Continuation of Table 12

8	**32 through 33**	**5th of February 2020 through 14th of February 2020**	**Ether and Bitcoin Monero and Bitcoin**	**0,3176; 0,3323**
9	32 through 34	5th of February 2020 through 18th of April 2020	Dash and Monero	0,4775
10	34 through 36	18th of April 2020 through 24th of June 2020	Ether and Bitcoin Ripple and Bitcoin Ripple and Bitcoin	0,3454; 0,3106; 0,1184
11	37 through 39	10th of September 2020 through 26th of September 2020	Zcash and Ether	0,4912
12	39 through 41	26th of September 2020 through 3rd of November 2020	Zcash and Bitcoin Dash and Bitcoin	0,3655; 0,5410

Source: Prepared by an author based on OxMetrics software output

The criminal incidents 12, 27, 28, 29, 36, 37, 38, 39 and 40 had the greatest impact on cross-correlations in several markets simultaneously. For instance, due to criminal incident 28 occurred 28th of October 2019, 10 dynamic correlations changed by more than 15%, e.g., Litecoin and Bitcoin, Ripple and Bitcoin, Cardano and Bitcoin, Monero and Bitcoin, Zcash and Bitcoin, Litecoin and Ether, Ripple and Ether, Zcash and Ether, Monero and Litecoin, Monero and Ripple. The combined loss from these incidents is approximately $6,5 billion representing the majority of all losses due to the criminal incidents selected for investigation.

Figures 7, 8 and 9 further supports the above-mentioned results by presenting the evidence of the spikes in cross-cryptocurrency correlations corresponding to the time of the selected criminal incidents.

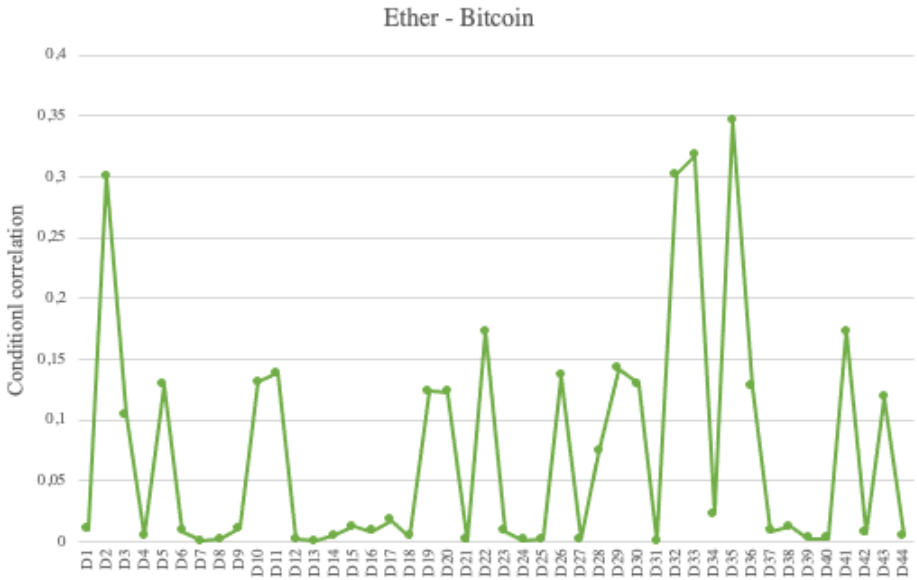

Figure 7. Dynamic conditional correlations between Ether and Bitcoin

Source: Prepared by an author

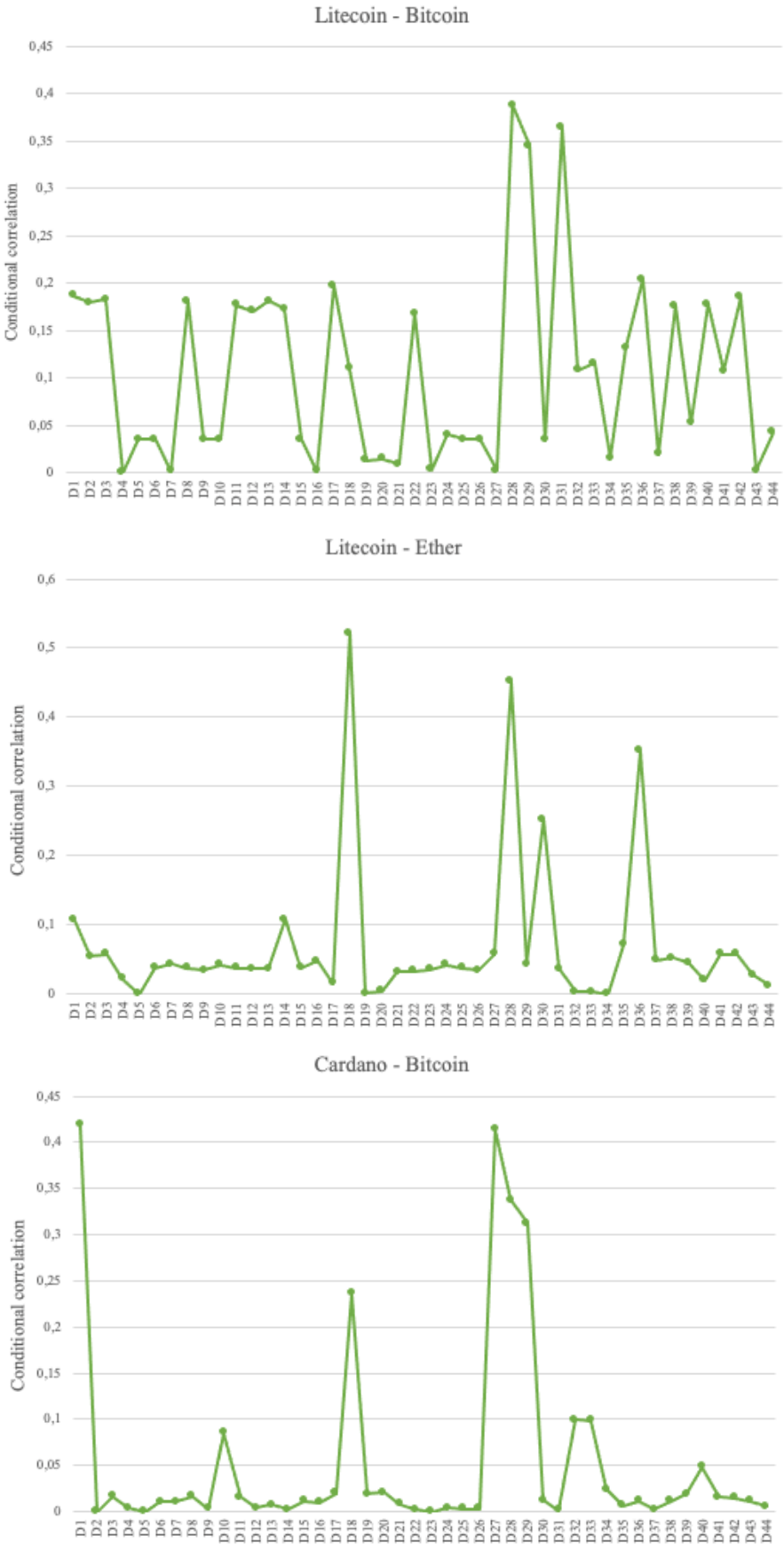

Figure 8. Dynamic conditional correlations between Litecoin and Bitcoin, Litecoin and Ether; Cardano and Bitcoin during criminal incidents

Source: Prepared by an author

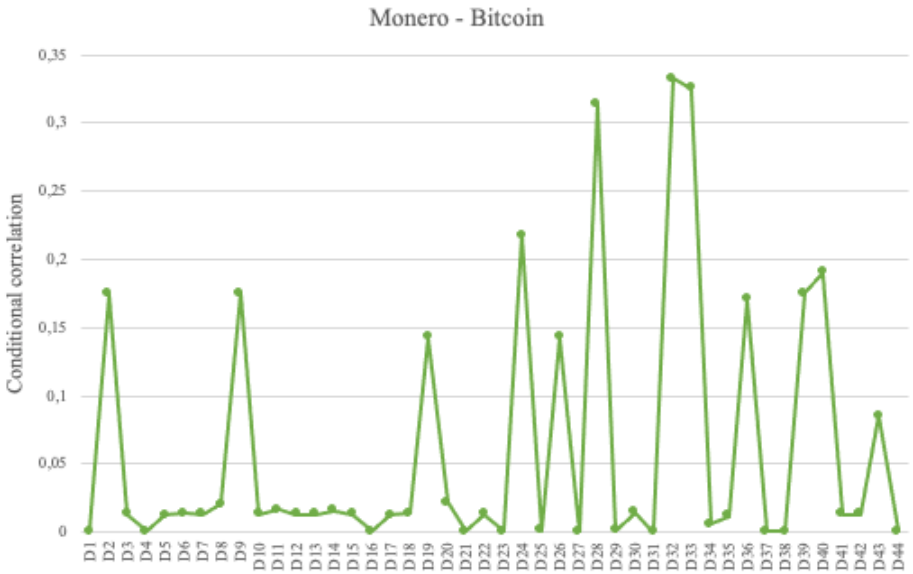

Figure 9. Dynamic conditional correlations between Monero and Bitcoin during criminal incidents
Source: Prepared by an author

Moreover, twelve distinct periods of sustained increase in cross-cryptocurrency correlations as controlled for each criminal incident were identified. Because all selected cryptocurrencies differ in terms of novelty, capitalization, liquidity, reputation and other factors, the results of the study are also not similar. According to Table 12, the largest sustained increases in multiple markets were identified at the time of criminal incident 17 through incident 19 (8th of October 2018 through 27th of March 2019). Peak cross-correlations occurred during criminal incident 18 (14th of January 2019) – which represents increases in the dynamic correlations of Litecoin and Ether, Ripple and Bitcoin, Cardano and Bitcoin, Zcash and Bitcoin. These events coincide with the ICO exit scam of the Pincoin cryptocurrency, an exchange named Cryptopia which had been pulled offline due to certain hacking forms, and Coinbene hack resulting in the theft of $45 in Coinbene Coin and Maximine Coin. The combined losses from these three events are approx. $721 million. In addition, the Coinbene hack appears to coincide with the first time Bitcoin dropped below $4,400 in a significant sell-off, which has provoked growing concerns throughout the cryptocurrency sector. The mentioned fall of Bitcoin occurred during two major announcements. The first announcement was Google's decision to prohibit cryptocurrency advertising, implying that even legitimate corporates will not be able to market their services in the same way as Facebook has already decided. The failed theft on the Binance exchange, where hackers had manipulated the market before attempting to cash out, was the second significant news event that caused such widespread cryptocurrency co-movement. As the attack was unsuccessful, it is not included in the list of criminal incidents. In addition, the exchange offered $250,000 for information that could lead to hackers being arrested and set aside $10 million in a reserve for future rewards to prevent future attacks.

Further, the period during criminal incident 27 through 29 (30th of July 2019 through 9th of November 2019) presents the second largest sustained increases in cross-correlations of Litecoin and Ether, Monero and Bitcoin, Ripple and Ether, Cardano and Bitcoin. In terms of losses, criminal incident 27 related to the PlusToken exit scam resulted in $6 billion in losses, indicating the largest specific criminal incident in this analysis. It is important to note that in some other relationships such as Cardano and Ether, Monero and Tether, Monero and Cardano, Litecoin and Bitcoin, elevated cross-correlations were identified at the time of the criminal incident 28 through 30 (28th of October 2019 through 27th of November 2019). The mentioned events are related to approx. $5,9 million hacking of Bitcoin, a PureBit exit scam that resulted in the loss of Ether (approx. $3 million), and a hacking incident in the Upbit exchange when approx. $48,5 millions of Ether were stolen. The extensive international coverage of the three incidents appears to have resulted in a significant loss of confidence in the cryptocurrency market during this period, as evidenced by the extensive cross-correlations between the largest and smallest cryptocurrencies.

The third distinct phase of elevated cross-correlations occurred during criminal incident 34 through 36, representing the period between the 18th of April 2020 and 24th of June 2020. The mentioned increase is associated with the theft of approx. $25 million through the hack into the Lendf.me lending platform, money laundering event of BTC-e exchange that laundered over $4 billion and hacking event in CryptoCore platform that resulted in the loss of $200 million.

Moreover, the pairs of criminal incidents 1 through 3 (26th of January 2018 through 8th of February 2018), 23 through 25 (1st of June 2019 through 27th of June 2019), 32 through 33 (5th of February 2020 through 14th of February 2020) and 31 through 33 (12th of December 2019 through 14th of February 2020) influenced changes of dynamic correlations in the same cryptocurrency markets, i.e., Monero and Bitcoin. The changes in dynamic correlations between Ether and Bitcoin were caused by criminal incidents 1 through 3 and 32 through 33. Considering the mentioned cryptocurrency pairs, Monero and Bitcoin presented the highest peak of cryptocurrency correlations during criminal incident 31 through 33. Based on the Table 12, the peak of increase in cross-correlations was 0,3323. The highest estimate of dynamic correlations between Ether and Bitcoin was identified at the time of criminal incident 32 through 33, with the peak of 0,3176. Criminal incident 31 is related to an ICO, a project named Shopin, that offered a blockchain-based shopper profile solution. On the 12th of December 2019, the founder of Shopin was charged for operating a $42 million ICO without registering with the U.S. Securities and Exchange Commission. Given the research results that the two main counterparties that presented the highest increase in dynamic cryptocurrency correlations during criminal incident 32 were Bitcoin and Ether. Criminal incident 32 is related to a cyber-attack in Altsbit, an Italian cryptocurrency

exchange. At the time of 5th of February 2020, the exchange was shut down after a suspected cyber-attack when most customers' funds were stolen. The stolen amount of Bitcoin and Ether was estimated at approx. $72,5 million at press time. Altsbit has only been operating in the last few months, therefore it could not afford to cover the losses caused by the hack. On the 6th of February 2020, the exchange informed users about the cyber-attack, but most articles in the media were released on the 10th of February 2020. Criminal incident 33 is associated with money laundering activities. On the 13th of February 2020, a man has been arrested in Ohio for operating the Helix, a Darknet-based cryptocurrency laundering service (Bitcoin mixer). The estimated losses due to money laundering through the mixer were approx. $300 million.

The following distinct periods of sustained increase in cross-cryptocurrency correlations were identified during criminal incidents 23 through 25 (1st of June 2019 through 27th of June 2019) between Cardano and Ether with the peak of 0,2173. Criminal incident 23 represents the cyber-attack of ledger wallets of 18,473 customers. The exact number of stolen Ripple coins is still unknown yet estimates suggest that at least 9,5 million dollars were taken. Criminal incident 24 is associated with $29 million scam in Bitcoin. However, criminal incident 25 could support the results of the investigation, as Cardano was one of the cryptocurrencies lost as a result of this criminal incident. In general, Bitrue, a Singaporean exchange, lost 9,3 million in Ripple and 2,5 million in Cardano from its hot wallet, $4 millions in total. This cyber-attack occurred when a hacker exploited a vulnerability in the review process systems that enabled to steal clients' funds.

Another distinct period was identified during criminal incident 37 through 39 (10t of September 2020 through 26th of September 2020) between Zcash and Ether with the peak cross-correlations of 0,4912. Criminal incident 37 represents a security breach at Eterbase, a Slovakian cryptocurrency exchange, during which malicious hackers accessed its network and stole funds worth $5,4 million. The majority of the stolen funds from the hot wallets were in Ether, making up almost $3,9 million of the approx. $5,4 million stolen. Criminal incident 38 is associated with cryptocurrency-themed phishing campaigns, in which two Russians have been charged for stealing approx. $17 million. The losses occurred in 3 separate cryptocurrency exchanges: $10 million from 142 Binance customers, $5,24 million from 158 Poloniex users, and $1.17 million from 42 Gemini customers. Further, as a result of criminal incident 9, few major withdrawals were detected in KuCoin, a crypto-currency exchange in Singapore. The team of KuCoin suspected that the hot wallets had been drained of Bitcoin, Ether, ERC-20 tokens and other cryptocurrencies. The estimated loss due to this criminal incident is $150 million. As Ether was one of the main cryptocurrencies stolen due to criminal incidents 37, 38 and 39, this could support the result of the investigation that the cross-correlation between Zcash and Ether increased the most at the time of the particular criminal incidents.

Further, sustained increases between Zcash and Bitcoin as well as Dash and Bitcoin were identified at the time of criminal incident 39 through 41 (26th of September 2020 through 3rd of November 2020), with the peak cross-correlations 0,3655 and 0,5410 respectively. Criminal incident 40 is related to a hack that resulted in theft of approx. $24 million worth of cryptocurrency from Harvest Finance, a web portal that allows users to invest cryptocurrencies and then manipulate price fluctuations to achieve small profits. The hacker managed to steal $13 million worth of USD Coin (USDC) and $11 million worth of Tether. However, the hacker returned $2,5 millions to the platform two minutes after the attack, but the reason for such action remains unclear. Criminal incident 41 is associated with the significant losses due to drug sales on the Silk Web marketplace. Thousands of Bitcoins that worth $1 billion at the time were seized by law enforcement. This action was reported as the largest seizure of cryptocurrency in the agency's history. The Justice Department seized 70,000 bitcoins generated in revenue from the sale of drugs on the Silk Web marketplace from a hacker, named "Individual X," who transferred the cryptocurrency from Silk Road to a hacker-controlled wallet. It is important to highlight that the cryptocurrencies that experienced the highest sustained increases as a result of the aforementioned criminal incidents were Zcash and Dash. Both of these cryptocurrencies are often used in illicit activities because of privacy-enhancing and protecting features.

The relationships between the selected cryptocurrencies must be taken into account while considering the findings of the DCC-GARCH analysis presented above. As Bitcoin and Litecoin have identical structures as peer-to-peer networks, it is reasonable to expect some similarities in their volatility responses as investors examine their structure, dynamics, and response mechanism to shocks in the same way. Cardano is based on smart contracts in the same manner as Ether. Compared to the other eight cryptocurrencies, Monero is found to be in relatively isolated because it uses a Proof of Work mechanism to issue new coins and encourage miners to secure the network and validate transactions through an obfuscated public ledger. This means that anyone is able to make transactions, but no outside observer can tell the source, amount, or destination. The above-mentioned contrasting characteristics and interlinkages in the design contribute to the different results of the analysis.

A number of interesting findings emerge from the combination of the multivariate GARCH and DCC-GARCH analyses which were presented in third part. In order to summarize the results of the third analysis, two broad results must be mentioned. First, comparing the cross-correlations between larger and smaller capitalization cryptocurrencies, it was discovered that smaller capitalization cryptocurrencies estimates were lower. Secondly, the analysis revealed twelve specific periods where a sustained increase in cross-cryptocurrency correlations as controlled for each criminal incident was identified. In particular, cryptocurrency markets have been found to be

abruptly volatile in response to criminal incidents that appear to be rationally targeted at directly related cryptocurrencies and the wider cryptocurrency sector should the criminal events be systemically damaging. This is especially noticeable during criminal incidents involving wallet theft, which is considered one of the most important safety features of virtual assets, and cyber-attacks on cryptocurrency exchanges that trade various cryptocurrencies. Furthermore, broad co-movement in cryptocurrency markets has been observed during periods of crisis and major reputational damage. This supports the presumption that these relatively young markets have evolved to behave similarly to traditional financial assets during the crisis. Therefore, the third hypothesis is also accepted meaning that criminal incidents provoke changes in the conditional correlations between cryptocurrency markets.

CONCLUSIONS AND RECOMMENDATIONS

An extensive literature analysis regarding the impact of criminal activity in cryptocurrency markets on cryptocurrency prices revealed that although cryptocurrencies have a tremendous potential to challenge traditional payment networks due to advances in their technological architecture, the cryptocurrency ecosystem has become a common target of attacks by cybercriminals. The nature of cryptocurrencies provides an effective channel through which illegal funds, as well as illegal cross-border transactions, can be conducted. Anonymity, flexibility, speed of transactions and the lower fees together with easy access to the online markets and lack of regulation are the main factors behind increasing cryptocurrency-related crime worldwide. Moreover, even the COVID-19 pandemic provided new opportunities to conduct illicit activities that resulted in significant price fluctuations. For this reason, an amount of empirical research towards criminal activity associated with the cryptocurrency market, in particular money laundering through cryptocurrencies, is rapidly evolving. Although there is still little evidence of a direct impact of money laundering on cryptocurrency prices, cybercrime is known to causes the largest losses. In addition, there is some evidence that illegal trading in Darknet markets caused fluctuations in cryptocurrencies and hacking attacks have a direct impact on volatility and cross-correlations of cryptocurrencies. Cryptocurrencies are also frequently used in fraud, pump-and-dump or Ponzi schemes. Given the lack of regulation and literature on the analysis of Pump-and-Dump schemes, the cryptocurrency ecosystem is extremely vulnerable to such manipulations.

Moreover, the literature analysis revealed that the consequences of any criminal activity are directly connected to the level of its development. As attractiveness is one of the key factors of cryptocurrency prices, increasing value is causing a growing appetite to engage in criminal activity as the potential benefits increase. In addition, criminal activity involving cryptocurrencies undermines investor confidence, which can directly affect the value of cryptocurrency. Despite the significant rise in prices in recent years, cryptocurrencies have been subjected to accusations of pricing bubbles. This is mostly related to the paradox that exists between regulatory oversight, the potential for illicit use because of the anonymity within a young exchange system and infrastructure breaches influenced by the rise of cybercrime. Each of them affects the perception of the role of cryptocurrencies as a reliable and legitimate investment option.

The existing literature identifies three main factors that determine the supply and demand for pricing, attractiveness, and global macroeconomic indicators. Moreover, the risk and uncertainty can also affect the cryptocurrency price. Trust and expectations are crucial for cryptocurrencies as they are currently developing their market. As the attractiveness of a cryptocurrency has an impact on its price, the decisions of investors can be influenced by media

coverage. Consequently, attention-driven investments might have a positive or negative effect on the other cryptocurrency markets. Macro-financial indicators affect the price of a cryptocurrency through stock market indices, inflation, price indices and exchange rates. Recent literature emphasized that economic and financial variables can explain around 70% of price fluctuations.

Based on the analysis of diverse researches' findings, methods and variables used in the recent academic literature, it was discovered that GARCH models are the most suitable models for investigations of cryptocurrency price volatility and its factors. As a result of this, three specific GARCH models were constructed for the investigation of cryptocurrency price dynamics in terms of criminal activity. Multivariate GARCH model was chosen to examine both individual cryptocurrency markets volatility due to criminal incidents and the impact of criminal incidents on the cryptocurrency market based on estimated losses in US dollars. This model was selected for the investigation as it is the most suitable to investigate volatility effects through the use of dummy variables which denote periods of significant volatility in traditional markets. Dynamic conditional correlation (DCC) GARCH model was used for cryptocurrency market behavior during criminal incidents as it helps to analyze whether the co-movement of cryptocurrency returns has increased significantly.

In order to achieve the aim of the work, empirical research was carried out by establishing three separate methodologies that showed that criminal activity affects the prices of cryptocurrencies. Firstly, multivariate GARCH analysis uncovered that there are broad volatility responses for criminal incidents within individual cryptocurrency markets indicating that criminal activity generates sector-wide volatility effects. Furthermore, there are significant differences in the volatility responses of cryptocurrencies providing further evidence of significant instability resulting from criminal incidents on exchanges and ICO- fraud, both of which may be highly dependent on perceptions of stability and financial safety. Furthermore, any threat to such stability has been found to provoke a broad response in many cryptocurrencies rather than at the individual level. The analysis also disclosed evidence of market-based cryptocurrency volatility that was directly targeted by a particular criminal incident. Further, the results of the investigation of price volatility changes due to criminal incidents in the cryptocurrency market based on the stolen value in US dollars suggest that volatility of cryptocurrencies varies by the severity of criminal incident even though the estimated of five cryptocurrency markets remain insignificant, all results were positive throughout the analysis. Additionally, Cardano and Tether demonstrated a significant positive relationship between the dollar-valued scale of criminal incidents and estimated volatility.

Comparing the cross-correlations between larger and smaller capitalization cryptocurrencies, DCC-GARCH analysis found that smaller capitalization cryptocurrencies had lower volatility estimates. This applies not only to dynamic correlations between the smaller

cryptocurrencies themselves but also to the relationships between the smaller and larger cryptocurrencies. Furthermore, DCC-GARCH analysis identified twelve specific time periods of the sustained increase in cross-cryptocurrency correlations controlled for each criminal incident. The mentioned specific periods were linked with particular hacks, ICO exit scams, thefts and money laundering events. Widespread international coverage of the four criminal incidents appears to lead to a substantial loss of confidence in the cryptocurrency market, as evidenced by the broad cross-correlations between the largest and smallest cryptocurrencies.

To conclude, this investigation discovered evidence of widespread co-movement in cryptocurrency markets during times of extreme stress and severe reputational damage, supporting the hypothesis that these relatively young markets have evolved to behave similarly to traditional financial assets during the crisis. Moreover, there is strong evidence that the same relationships are changing significantly in the period after the criminal incidents in the cryptocurrency market. The investigation of recent illicit activity identified that criminal incidents in the cryptocurrency market increase both the volatility of the involved cryptocurrency and the correlations across the involved cryptocurrency and other cryptocurrency markets. This result essentially indicates that market manipulation exits the cryptocurrency ecosystem and that it should be a concern for institutional investors and regulators.

Recommendations. The analyzed topic lends itself to more detailed development and therefore remains a topic for future research. This study is limited by the lack of consolidated and verifiable data on all types of criminal incidents in cryptocurrency markets. According to this analysis, market participants are interested in the privacy and safety of their funds which is not always ensured within the available exchanges and existing regulations. Therefore, this study might help to recognize how criminal activity and its severity affects cryptocurrency volatility and which markets are the most vulnerable due to their specific characteristics. This research also revealed considerable information for investors and cryptocurrency users to help them to sort out the cryptocurrency markets with higher potentials and identify what aspects should be more considered before investing in cryptocurrencies. In addition, the study provides traders with relevant insights regarding the relation between the altcoin market and Bitcoin. The results of this research might be of interest to traders and investors seeking to understand the drivers of prices and help to inform vendors of the favorable conditions for the use of virtual currency. Furthermore, the results of this investigation might also help regulators and policy-making bodies to understand the impact of a lack of regulation in the cryptocurrency market. Due to the vulnerability to various factors that cause high volatility, cryptocurrencies do not appear to be a safe haven investment. In any case, traders, long-term investors and cryptocurrency users must be aware of the risks associated with digital assets.

As the results of the research suggest that there is a significant negative impact of criminal incidents on the likelihood that cryptocurrencies will remain in a low volatility regime, it highlights the necessity of gaining a deeper understanding of criminal activity in cryptocurrency markets and the tools used by criminals to prevent potentially significant market disruptions. Given the critical relevance of cyber security for assets such as cryptocurrencies, this study provided insight that the most common type of criminal incident is cyber-attacks. Following recent cyber-attacks on financial institutions, cyber risk has emerged as a significant threat to financial stability. Further research could investigate intra-day data, consider the date when the criminal incident occurred and announced publicly separately and include a wider set of cryptocurrencies and incorporate other types of criminal incidents such as ransomware attacks and theft of digital wallets to identify vulnerabilities of virtual currencies and cyber-attack indicators grouped by targets.

LIST OF REFERENCES

Akaike, H. (1974). A new look at the statistical model identification. *IEEE Transactions on Automatic Control* 19, 716–23.

Albrecht, C., Duffin, K., Albrecht, C., & Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*. 22.

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

Alkhazali, O., Bouri, E., & Roubaud, D. (2018). The impact of positive and negative macroeconomic news surprises: Gold versus Bitcoin. *Economics Bulletin*. 38. 373-382.

Anika, E. I. (2019). New technology for old crimes? the role of cryptocurrencies in circumventing the global anti-money laundering regime and facilitating transnational crime. Master of Laws. *University of British Columbia*, 180.

Ardia, D., Bluteau, K., Boudt, K., & Catania, L. (2018). Forecasting risk with Markov-switching GARCH models: A large-scale performance study. *International Journal of Forecasting*. 34. 733-747.

Azqueta-Gavaldon, A. (2020). Causal inference between cryptocurrency narratives and prices: Evidence from a complex dynamic ecosystem. *Physica A: Statistical Mechanics and its Applications,* vol. 537.

Bauwens, L., Backer, B. D., & Dufays, A. (2014). A Bayesian method of change-point estimation with recurrent regimes: Application to GARCH models. *Journal of Empirical Finance*, 29, 207-229.

Bejaoui, A., Ben Sassi, S., & Majdoub, J. (2019). Market dynamics, cyclical patterns and market states: Is there a difference between digital currencies markets. *Studies in Economics and Finance*, Vol. 37 No. 4, pp. 585-604.

Benjamin, V., Valacich, J., & Chen, H. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Q*, 43.

Bollerslev, T. (1986). Generalized autoregressive conditional heteroskedasticity. *Journal of Econometrics*, 31 (3), 307–327.

Bougerol, P., & Picard, N. (1992). Stationarity of Garch processes and of some nonnegative time series. *Journal of Econometrics*, 52 (1-2), 115–127.

Engle, R. F. (2002). Dynamic conditional correlation: A simple class of multivariate generalized autoregressive conditional heteroskedasticity models. *Journal of Business and Economic Statistics,* 20, 339–350.

Bouoiyour, J., & Selmi, R. (2015). What does Bitcoin look like? *Annals of Economics and Finance*, vol. 16, issue 2, 449-492.

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

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. *Financial Crises eJournal*.

Brada, J., & Sedlaček, J. (2017). Comparison and Analysis of Major Cryptocurrencies. *Information Technology for Practice*. 140-147.

Buchholz, M., Delaney, J., Warren, J., & Parker, J. (2012). Bits and bets, information, price volatility, and demand for Bitcoin. *Economics* 312.

Caporale, G. M., & Zekokh, T. (2019). Modelling volatility of cryptocurrencies using Markov-Switching GARCH models. *Research in International Business and Finance*. 48.

Caporale, G. M., Kang, W. Y, Spagnolo, F., & Spagnolo N. (2020). Non-linearities, cyber-attacks and cryptocurrencies. *Finance Research Letters*, Volume 32, 2020, 101297, ISSN 1544-6123.

Caporale, G. M., Kang, W. Y, Spagnolo, F., & Spagnolo N. (2021). Cyber-attacks, cryptocurrencies, and cyber security. *Journal of International Financial Markets, Institutions and Money*, volume 74.

Chu, J., Chan, S., Nadarajah, S., & Osterrieder, J. (2017). GARCH Modelling of Cryptocurrencies. *Journal of Risk and Financial Management*. 10. 17.

Ciaian, P., Rajcaniova, M., & Kancs, A. (2016). The digital agenda of virtual currencies: Can BitCoin become a global currency? *Inf Syst E-Bus Manage* 14, 883–919.

Ciupa, K. (2019). Cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems. *OECD Global Anti-Corruption & Inegrity forum conference materials*.

Conrad, C., Custovic, A., Ghysels, E., & Lv, K. (2018). Long-and Short-Term Cryptocurrency Volatility Components: A GARCH-MIDAS Analysis. *Journal of Risk and Financial Management*, 11(2).

Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a Financial Asset: A Systematic Analysis. *International Review of Financial Analysis*, 62, 182-199.

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2019). The destabilising effects of cryptocurrency cybercriminality. *Economics Letters,* Volume 191.

Corbet, S., Larkin, C., & Lucey, B. (2020). The contagion effects of the COVID-19 pandemic: Evidence from Gold and Cryptocurrencies. *Finance Research Letters*. 35.

De Giovanni, D., Leccadito, A., & Pirra, M. (2020). On the determinants of data breaches: A cointegration analysis. *Decisions in Economics and Finance*, 1-20.

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control,* Vol. 22 No. 3, pp. 480-497.

Fanusie, Y. J., & Robinson, T. (2018). Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. *Center on Sanctions and Illicit Finance & Elliptic*.

Foley, S., Karlsen, J. R., & Putniš, T. J. (2019). Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853.

Forgang, G. (2019). Money Laundering Through Cryptocurrencies. *Economic Crime Forensics Capstones*, 40.

Gandal, N., Hamrick, J.T., Moore, T., & Oberman, T. (2018). Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics*, 95.

Goczek, L., & Skliarov, I. (2019). What drives the Bitcoin price? A factor augmented error correction mechanism investigation. *Applied Economics*, 51:59, 6393-6410.

Goldsmith, D., Grauer, K., & Shmalo, Y. (2020). Analyzing hack subnetworks in the bitcoin transaction graph. *Applied Network Science*, 5, 22.

Guindy, M. (2021). Cryptocurrency price volatility and investor attention. *International Review of Economics & Finance*, Volume 76, p. 556-570.

Gurrib, I., Kweh, Q. L., Nourani, M., & Ting, I. (2019). Are Cryptocurrencies Affected by Their Asset Class Movements or News Announcements? *Malaysian Journal of Economic Studies*. 56. 201-225.

Hakim das Neves, R. (2020). Bitcoin pricing: impact of attractiveness variables. *Financial Innovation*, 6, 1-18.

Icellioglu, C., & Oner, S. (2019). An Investigation on the Volatility of Cryptocurrencies by means of Heterogeneous Panel Data Analysis. *Procedia Computer Science*, 158, 913-920.

Jeribi, A., Jena, S.K., & Lahiani, A. (2021) Are Cryptocurrencies a Backstop for the Stock Market in a COVID-19-Led Financial Crisis? Evidence from the NARDL Approach. *Int. J. Financial Stud*, 9, 33.

Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*. 7. 10.1186/s40163-018-0093-5.

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, 43, 141-157.

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325–344.

Koerhuis, W., Kechadi, T., & Le-Khac, N. (2019). Forensic Analysis of Privacy-Oriented Cryptocurrencies. *Forensic Science International: Digital Investigation,* 33.

Kristoufek, L. (2013). Bitcoin meets google trends and Wikipedia: quantifying the relationship between phenomena of the internet era. *Sci Rep,* 3(3415):1–7.

Kristoufek, L. (2015). What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. *PLoS ONE,* 10(4): e0123923.

Lee, H., & Choi, K.S. (2021). Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *An International Journal of Evidence-based Research, Policy, and Practice*, volume 16.

Li, X., & Whinston, A. (2020). Analyzing Cryptocurrencies. *Information Systems Frontiers*. 22.

Liu, J., & Serletis, A. (2019). Volatility in the Cryptocurrency Market. *Open Economies Review,* 30, 779–811.

Liu, Y., Tsyvinski, A., & Wu, X. (2019). Common Risk Factors in Cryptocurrency. *International Political Economy: Monetary Relations eJournal.*

Moore, T., Han, J., & Clayton, R. (2012). The postmodern ponzi scheme: empirical analysis of high yield investment programs. *Financial Cryptography and Data Security*, 41-56.

Moore, T., & Christin, N. (2013). Beware the middleman: empirical analysis of BitCoin-exchange risk. *Financial Cryptography and Data Security*, 7859:25–33.

Nelson, D. B. (1990). Stationarity and persistence in the garch (1,1) model. *Econometric Theory* 6 (3), 318–334.

Park, S., & Park, H. W. (2020). Diffusion of cryptocurrencies: web traffic and social network attributes as indicators of cryptocurrency performance. *Quality & Quantity*, 54, 297–314.

Phillips, R. C., & Gorse, D. (2018). Cryptocurrency price drivers: Wavelet coherence analysis revisited. *PLoS ONE*, 13.

Polasik, M., Piotrowska, A., Wisniewski, T., Kotkowski, R., & Lightfoot, G. (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. *International Journal of Electronic Commerce*. 20, 9-49.

Saiedi, E., Brostrom, A., & Ruiz, F. (2020). Global drivers of cryptocurrency infrastructure adoption. *Small Business Economics*, 1-54.

Scheau, M., & Pop, S. (2018). Cybercrime Evolution. *International conference KNOWLEDGE-BASED ORGANIZATION*, 24. 225-229.

Scheau, M. C., Craciunescu, S. L., Brici, I., & Achim, M. V. (2020). A Cryptocurrency Spectrum Short Analysis. *Risk and Financial Management*, 13, 184.

Schwarz, G. E. (1978). Estimating the dimension of a model. *Annals of Statistics 6*, 461–64.

Seele, P. (2018). Let Us Not Forget: Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation. *Humanistic Management Journal*, 3, 133–139.

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). Exploring the use of Zcash cryptocurrency for illicit or criminal purposes. *RAND Corporation*.

Sovbetov, Y. (2018). Factors influencing cryptocurrency prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. *Journal of Economics and Financial Analysis*, 2 (2): 1-27.

Tiwari, A. K., & Satish, P. R. (2019). Modelling the dynamics of Bitcoin and Litecoin: GARCH versus stochastic volatility models. *Applied Economics*, 51. 1-10.

Trump, B. D., Wells, E., Trump, J., & Linkov, I. (2018). Cryptocurrency: governance for what was meant to be ungovernable. *Environment Systems and Decisions*, 38, 426–430.

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

Zhu, Y., Dickinson, D., & Li, J. (2017). Analysis on the influence factors of Bitcoin's price based on VEC model. *Financial Innovation*, 3, 3.

Wei, W. C. (2018). The impact of Tether grants on Bitcoin. *Economics Letters*. 171.

White, L. (2015). The Market for Cryptocurrencies. *Cato Journal*. 35. 383-402.

INVESTIGATING DYNAMICS BETWEEN PRICE VOLATILITY AND CRIMINALITY IN CRYPTOCURRENCY MARKETS

Karolina MACIULEVIČIŪTĖ

Master Thesis

Finance and Banking Master Programme

Faculty of Economics and Business Administration, Vilnius University
Supervisor Assoc. prof. PhD Alfreda Šapkauskienė, Vilnius, 2022

SUMMARY IN LITHUANIAN

60 psl., 12 lentelių, 8 pav., 70 šaltinių.

Pagrindinis baigiamojo darbo tikslas yra išanalizuoti nusikaltamos veiklos kriptovaliutų rinkose įtaką kriptovaliutų kainų svyravimams. Baigiamasis darbas susideda iš trijų pagrindinių dalių. Literatūros analizėje nagrinėjami teoriniai kriptovaliutų panaudojimo nusikalstamose veiklose aspektai, kriptovaliutų rinkoje pasitaikančios nusikalstamos veiklos rūšys ir jų įtaka kriptovaliutų kainoms, apžvelgiami pagrindiniai veiksniai lemiantys kriptovaliutos kainą bei pagrindiniai skirtumai ir ypatybės skirtingose kriptovaliutų rinkose analizuojant mokslinių darbų tyrimų metodus bei gautus rezultatus. Metodologijos dalis apima trijų skirtingų kiekybinių tyrimo modelių formavimą. Praktinėje dalyje analizuojami pirmojo, antrojo ir trečiojo empirinių tyrimų rezultatai.

Atlikus literatūros analizę, buvo pasirinkti du statistiniai modeliai trims baigiamojo darbo tyrimo dalims įgyvendinti. Pirmuoju modeliu (daugiamačiu apibendrintu autoregresinio sąlyginio heteroskedatiškumo modeliu) išanalizuoti tiesioginiai kriptovaliutų kainų pokyčiai iš karto po nusikalstamos veiklos incidentų kriptovaliutų rinkoje. Šiame modelyje devynių skirtingų kriptovaliutų kaina buvo pasirinkta kaip priklausomas tyrimo kintamasis, nepriklausomi kintamieji buvo tradiciniai finansiniai instrumentai ir datos, žyminčios keturiasdešimt keturis nusikalstamos veiklos incidentus. Antruoju modeliu išnagrinėtas nusikalstamos veiklos incidentų poveikis kriptovaliutų rinkai priklausomai nuo nuostolių dydžio. Šį modelį sudaro kokie patys kintamieji kaip ir pirmąjį, tačiau šiuo atveju įtraukiami nusikalstamos veiklos incidentų metu patirti nuostoliai išreikšti JAV doleriais. Trečiuoju tyrimo modeliu (dinaminiu sąlyginės koreliacijos apibendrintu autoregresinio sąlyginio heteroskedastiškumo modeliu) išanalizuota kokius koreliacijų tarp kriptovaliutų rinkų pokyčius sukelia kinta nusikalstamos veiklos incidentai. Analizė parengta naudojant „Matlab“, „Eviews“ ir „OxMetrics“ programines įrangas.

Pirmasis tyrimo modelis atskleidė, jog kriptovaliutų rinkos nepastovumas padidėja dėl nusikalstamo veiklos incidentų kriptovaliutų rinkose. Remiantis antrojo tyrimo modelio rezultatais nustatyta, kad kriptovaliutų kainų kintamumas priklauso nuo nusikalstamos veiklos sukeltų nuostolių dydžio. Trečiasis tyrimo modelis nustatė, kad nusikalstamos veiklos incidentai turi įtakos sąlyginės koreliacijos tarp kriptovaliutų rinkų pokyčiams. Išvadose ir pasiūlymuose apibendrinta literatūros analizė ir trijų tyrimų rezultatai.

ANNEXES

Annex 1. Cryptocurrency criminal incidents used in price volatility investigation (compiled by an author using public sources)

No.	Date	Amount	Market	Description
1	2018-01-26	$530m	NEM	26 January 2018, all deposits were suspended in NEM on the Coincheck exchange. Once the hack was confirmed by the exchange, it was then revealed that the hack resulted in a loss of 523 mln. NEM coins, worth approx. $532.6 mln 26 January. The coins were stolen via several unauthorized transactions from a hot wallet.
2	2018-02-05	$1.8m	Ether	Potential Seele ICO investors have been scammed out of approx. $2 million by administrators who have used the Telegram channel to transfer their money back before the token sale started. Seele, a blockchain project with potential applications in IoT, game assets, fintech, etc.
3	2018-02-08	$195m	Nano	The hack is assumed to have taken place on 8 February 2018, but Nano's developers argue it was insolvent long before February and claim that now they have a reason to believe that Firano misled Nano Core team and the community for a significant period of time in respect of solvency of the BitGrail exchange.
4	2018-02-15	$50m	Bitcoin	Together with the Ukrainian cyberpolice, Cisco investigated potential cyber criminality and stating that $50 million of cryptocurrency had been netted by the people behind a large scam over a three-year period. According to Cisco, the campaign was straightforward as the attackers just had to continue buying Google AdWords after initial configuration in order to ensure a constant stream of victims.
5	2018-03-04	$50m	Bitcoin	BTC Global was launched 25 September 2017 by ‘famous’ trader Steven Twain. Using fake Twitter accounts claiming to send free Ether and Bitcoin to imposters or sending fake emails to ICO investors, cryptocurrency scams are increasing at an astounding level. BTC Global was the latest company joined the growing list of scammers. It was reported that more than 500,000 Bitcoins have been pocketed from people in South Africa, the United States, Australia and other countries.
6	2018-04-05	$300m	Bitcoin	GainBitcoin started in 2015 as a multi-level marketing system (MLM) which brought together over 100,000 investors, all of whom promised 10 percent monthly returns. Amit Bhardwaj, who had set up the scheme, moved his base of operations to Dubai while continuing operations in India when the authorities caught up.
7	2018-04-09	$650m	ICO	Two blockchain companies, Ifan and Pincoin, have pulled of the largest alleged ICO scam in Vietnam. Both companies have reportedly duplicated 32,000 investors with some 15 trillion VND ($660 million) in investment. Even though Ifan is registered in Singapore and Pincoin is registered in Dubai, both companies in Vietnam have approached the same company (Modern Tech) in order to announce their projects to potential investors.
8	2018-04-13	$3.3m	Bitcoin	The Chief Strategy Officer (CSO) of the cryptocurrency exchange Coinsecure has been charged with a suspected case of fraud in which 438 Bitcoins were lost or misrepresented for approx. $3.3 million.
9	2018-04-19	$20m	Bitcoin	In 2015, two men started and subsequently built a multi-level company, which promised high returns for investors through Bitcoin investment.
10	2018-05-14	$48m	ICO	The Shenzhen Puyin Blockchain Group has run a tea-based Blockchain project and allegedly raised about 48 million dollars from investors. Overall, the scam was defrauded by a total of 3,000 people who claimed that its token value was linked - in a so-called stable fashion - with the value of particularly rare Chinese tea combinations.
11	2018-06-07	$3m	ICO	Block Broker have disappeared in an exit scam when it claimed to offer investors protection from fraudulent ICOs. Block Broker stole $3 million from investors and eliminated its online presence after the photo of the CEO of an unaffiliated photographer was found to be stolen.
12	2018-06-10	$40m	NPXS	After suffering what it called a 'cyber intruding' that resulted in a range of ERC-20 bases stolen from the platform, Coinrail suspended the service. However, only certain tokens taken in the alleged breach were given by Coinrail without the exact amount being disclosed.
13	2018-06-16	$31.5m	Ether	When Bithumb noticed an abnormal access recently, they moved a large number of Ether to its cold wallet. On June 16 Bithumb reported that it would abruptly check the server to maximize security settings.
14	2018-07-09	$23.5m	Ether	The hot wallet used to update smart contracts on the exchange of Bancor has been affected by a safety violation resulting in a loss of around $23.5 million in Ether. The detailed scale of theft was discussed by Bancor in the later stages, which indicated that a total of 24.984 ETH ($12.5 million), 229M NPXS ($1 million) and 3.2 million BNT ($10 million) were stolen.

15	2018-08-19	$87m	Bitcoin, Ether and other coins	Three Chinese nationals were arrested over the alleged theft of theft of $87 million in cryptocurrencies by targeting both individual and corporate wallets. The three suspects from China's capital Beijing and its Changchun and Hunan provinces were taken into police custody on August 15th, after a 30-day investigation by local authorities. The investigation started in March, the year when the local police were informed by one of the hacking attach victims. The victim reported that almost $15 million in Bitcoin and Ether taken from unknown attackers.
16	2018-09-14	$60m	Bitcoin, Bitcoin Cash, and MonaCoin	Zaif, an Osaka-based cryptocurrency exchange, has lost $60 million to the company and user finances in a cyber-attack that hackers have siphoned away from Zaif hot wallet's Bitcoin, Bitcoin Cash, and MonaCoin. On Monday 17 September, the company discovered the hack and confirmed that one day after it reached the authorities and reported the occurrence.
17	2018-10-08	$660m	ICO	After pulling an ICO exit scam, the Pincoin operators came out with a $660 million trader fund, which was unsurprising given the 48 percent return the company promised to investors. The cryptocurrency known as Pincoin (PIN) was released back on 12 January. That was the beginning of a scam.
18	2019-01-14	$16m	Cryptopia	The Cryptopia, an exchange in New Zealand, had been pulled offline due to certain hacking forms, but there was lack of details about the incidents. The business was suspended, and the company went into liquidation. It has since emerged, that individual wallets have not been held by users.
19	2019-03-27	$45m	Coinbene Coin and Maximine Coin	CoinBebe is estimated to lose over $45 million in losses due to hacking. The hacker has stolen Coinbene Coin approx. $6 million and Maxime Coin approx. $39 million, which was subsequently placed on the market.
20	2019-03-29	$20m	EOS and Ripple	29 March 2019 Bithumb disclosed another security incident, which was the third in two years. It is estimated that cyber attackers may have stolen approx. $20 million in EOS tokens and Ripple.
21	2019-05-07	$41m	Bitcoin	Cyber attackers have disrupted cryptocurrency exchange platform Binance and stolen Bitcoin worth $41 million.
22	2019-05-22	$200m	Bestmixer	Bestmixer.io started operating in May 2018. Just a month later, police started to investigate the mixing service, which found that the so-called leading world crypto mixing service managed to launder on behalf of its customers for at least $200 million in cryptocurrency over the course of the year. On May 22, Bestmixer.io was seized by European police.
23	2019-06-01	$9.5m	Ripple	Ledger wallets of 18,473 customers were compromised. Suspicious API calls were identified, and an investigation revealed that the attackers managed to access a database containing valid access tokens. The exact number of coins stolen is still unknown, yet estimates suggest that at least 9.5 million dollars were taken.
24	2019-06-25	$29m	Bitcoin	Europol and Eurojust conducted six arrests in the UK and the Netherlands. The suspects were reported to have been involved in a $29 million scam in Bitcoin. A possible suspect living in the Netherlands was identified in February 2018, by the South West Regional Cyber Crime Unit (SW RCCU) and referred the case to the Joint cybercrime operating force (J-CAT) hosted by Europol's European Cyber Crime Centre (EC3).
25	2019-06-27	$4m	Ripple and Cardano	Bitrue, a Singaporean exchange, lost 9.3 million in XRP and 2.5 million in Cardano from its hot wallet, worth millions of dollars. A hacker exploited a vulnerability in review process systems which enabled to steal clients' funds.
26	2019-07-11	$32m	Bitcoin, Bitcoin Cash, Ether Litecoin, and Ripple	Bitpoint, a Japan-based cryptocurrency exchange, was the subject of $32 million in cryptocurrency theft, of which $23 million belonged to the customers of the organization.
27	2019-07-30	$6b	Bitcoin, Ether, EOS	PlusToken allegedly carried out an exit scam, with deposits estimating to $2.9 billion. More than 100 people suspected of engaging in the PlusToken investment scam were arrested by Chinese police. Investors were based mainly in China and in South Korea, who stored Bitcoin, Ether and EOS on the platform.
28	2019-10-28	$5.9m	Bitcoin	MapleChange, a Canadian crypto trading post, reported that over 900 BTC had been stolen, but clients would not be refunded, and the company's website and social media presence disappeared very quickly.
29	2019-11-09	$3m	Ether	Although the South Korean cryptocurrency exchange PureBit operated only a few months, it allegedly managed to pull an exit scam and stole $3 million in Ethere with it.
30	2019-11-27	$48.5m	Ether	Upbit, a South Korean cryptocurrency exchange, reported 342,000 in Ether had been stolen from the company's hot wallet, worth approx. $48.5 million at that time. However, the has exchange promised to ensure that the customers are not affected and that Upbit assets are covered by funds.

31	2019-12-12	$42m	ICO	The founder of Shopin, a project that offered a blockchain-based shopper profile solution, was charged for operating a $42 million ICO without registering with SEC.
32	2020-02-05	$72.5m	Bitcoin, Ether	Altsbit, an Italian cryptocurrency exchange, shut down after a suspected cyber-attack in which the majority of customer's funds were stolen. The stolen amount of Bitcoin and Ether was estimated at approx. $72.5 million at press time.
33	2020-02-13	$300m	Bitcoin	An Ohio man has been arrested for operating the Helix Bitcoin mixing service. It is estimated that the mixer laundered approx. $300 million.
34	2020-04-18 and 2020-04-19	$25m	Lendf.me	Hackers have stolen over $25 million in cryptocurrency from the Lendf.me lending platform. The attacks occurred during the weekend, on Saturday and Sunday, respectively. Investigators reported that hackers seem to have used bugs and legitimate features from various blockchain technologies to orchestrate a sophisticated "reentrancy attack". Such attacks enable hackers to withdraw funds multiple times, in a loop, before the initial payment is approved or declined.
35	2020-06-22	$4b	NZD	New Zealand law enforcement has seized $140 million NZD ($90 million USD) as part of a case against the alleged founder of BTC-e - Alexander Vinnik who has been sought by law enforcement in the US, France, and Russia on charges of money laundering. Prosecutors state that over the course BTC-e operation, the exchange was used to launder over $4 billion.
36	2020-06-24	$200m	CryptoCore	Researchers reported that over $200 million cryptocurrency has been stolen from online exchanges by the CryptoCore hacking group.
37	2020-09-10	$5.4m	Ether	Eterbase, a Slovakian cryptocurrency exchange reported a security breach during which malicious hackers accessed its network and stole funds worth $5.4 million. The majority of the stolen funds from the hot wallets were in Ether, making up almost $3.9 million of the almost $5.4 million stolen.
38	2020-09-16	$17m	Binance, Poloniex and Gemini users	Two Russians were charged for stealing approx. $17 million in cryptocurrency-themed phishing campaigns. The losses occurred in 3 separate cryptocurrency exchanges: $10 million from 142 Binance customers, $5.24 million from 158 Poloniex users, and $1.17 million from 42 Gemini customers.
39	2020-09-26	$150m	Bitcoin, Ether, ERC-20 tokens	KuCoin, a crypto-currency exchange in Singapore, has stored several assets in hot wallets instead of cold wallets where crypto-currency is safely stored away from the web. After few major withdrawals were detected, KuCoin's team suspected that the hot wallets were being drained of Bitcoin, Ether, ERC-20 tokens and other cryptocurrencies.
40	2020-10-26	$21.5m	USD Coin and Tether	A hacker has stolen approx. $24 million worth of cryptocurrency from Harvest Finance, a web portal that allows users to invest cryptocurrencies, then manipulate variations in price to achieve small profits. Overall, the hacker managed to steal $13 million worth of USD Coin (USDC) and $11 million worth of Tether (USDT). The hacker returned 2,5 million dollars to the platform two minutes after the attack, however, the reason of such action remains unclear.
41	2020-11-03	$1b	Bitcoin	Thousands of Bitcoins that worth $1 billion at the time were seized by law enforcement which was reported as the biggest seizure of cryptocurrency in the history of agency. Justice Department seized the 70,000 bitcoins generated in revenue from drug sales on the Silk Web marketplace from a hacker, named as “Individual X,” who moved the cryptocurrency from Silk Road into a wallet the hacker controlled.
42	2020-11-04	$24m	ICO	U.S. and Brazilian law enforcement have confiscated $ 24 million in cryptocurrency from individuals suspected of being involved in an online investment fraud scam. The crimes have occurred between August 2017 and May 2019. During this time, Fagundes and other defendants demanded funds from prospective investors online by promising innovative investment opportunities for cryptocurrencies. Criminals held the funds in a way that would have mandated regulation under Brazilian law, which Fagundes and the others allegedly did not comply with. They reportedly held the funds in a way that would have obliged them to regulate under Brazilian law, which Fagundes and others allegedly did not comply with.
43	2021-03-04	$31m	Binance USD, Binance tokens	The Meerkat Financial, a decentralized financing project, reported that cryptocurrency assets, e.g., 13.96 million of Binance USD and the 73,653 of Binance tokens were stolen by $31 million only one day after Binance Smart Chain was launched.
44	2021-03-16	$5.7m	Roll	A security breach at Roll cryptocurrency platform enabled hacker to obtain a private key to Roll’s hot wallet and embezzle its contents which worth approx. $5.7 million.

Annex 2. Dynamic correlations between cryptocurrency markets during criminal incidents (prepared by an author using OxMetrics software output). For presentation purposes, the names of the selected cryptocurrencies have been shortened. They are now presented as BT (Bitcoin), ET (Ether), LT (Litecoin), RI (Ripple), CA (Cardano), TH (Tether), MO (Monero), ZC (ZCash) and DA (Dash).

Variable	ET-BT	LT-BT	RI-BT	CA-BT	TE-BT	MO-BT	ZC-BT	DA-BT	LT-ET	RI-ET	CA-ET	TE-ET
Total	0,0176	0,1821	0,0270	0,1328	0,0293	0,0050	0,1515	0,0600	0,2130	0,1961	0,1682	0,0816
D_1	0,0101	0,1873	0,0415	0,4193	0,0240	0,0001	0,0076	0,0410	0,1065	0,0178	0,1441	0,0040
D_2	0,3001	0,1797	0,0258	0,0000	0,0201	0,1747	0,0073	0,0034	0,0538	0,0096	0,0440	0,0004
D_3	0,1040	0,1831	0,0182	0,0169	0,0294	0,0133	0,0050	0,0410	0,0575	0,0121	0,0786	0,0314
D_4	0,0049	0,0002	0,0158	0,0039	0,0294	0,0004	0,0002	0,0027	0,0215	0,0087	0,0724	0,1712
D_5	0,1288	0,0353	0,0555	0,0002	0,0280	0,0122	0,0075	0,0012	0,0002	0,0354	0,0146	0,0360
D_6	0,0089	0,0353	0,0115	0,0106	0,0441	0,0135	0,0046	0,0002	0,0379	0,0028	0,2734	0,0089
D_7	0,0003	0,0012	0,0202	0,0104	0,0220	0,0134	0,0031	0,0056	0,0428	0,0087	0,0191	0,0122
D_8	0,0017	0,1811	0,0014	0,0163	0,0418	0,0201	0,0004	0,0069	0,0380	0,0158	0,0100	0,0437
D_9	0,0106	0,0353	0,0207	0,0028	0,0427	0,1754	0,0020	0,0018	0,0345	0,0127	0,0080	0,0444
D_{10}	0,1310	0,0353	0,0217	0,0852	0,0274	0,0133	0,0040	0,0033	0,0421	0,0037	0,2725	0,0338
D_{11}	0,1383	0,1771	0,0007	0,0161	0,0113	0,0163	0,0001	0,0022	0,0374	0,0006	0,2342	0,0058
D_{12}	0,0016	0,1708	0,0003	0,0038	0,0406	0,0131	0,0174	0,0410	0,0369	0,0020	0,1441	0,2629
D_{13}	0,0002	0,1816	0,0231	0,0076	0,0397	0,0133	0,0157	0,0009	0,0362	0,0027	0,1098	0,0090
D_{14}	0,0046	0,1728	0,0134	0,0026	0,0376	0,0156	0,1268	0,2471	0,1077	0,0002	0,0043	0,0361
D_{15}	0,0126	0,0353	0,0184	0,0113	0,0076	0,0134	0,0121	0,0089	0,0372	0,0300	0,1441	0,0164
D_{16}	0,0087	0,0016	0,0129	0,0098	0,0055	0,0004	0,0051	0,1092	0,0471	0,0066	0,1429	0,0024
D_{17}	0,0175	0,1973	0,0056	0,0202	0,0319	0,0123	0,0126	0,0067	0,0158	0,0030	0,0013	0,0069
D_{18}	0,0044	0,1096	0,2797	0,2361	0,0171	0,0135	0,2527	0,0577	0,5213	0,0010	0,0470	0,0026
D_{19}	0,1239	0,0128	0,1101	0,0187	0,0180	0,1429	0,0242	0,0410	0,0007	0,0131	0,0058	0,0013
D_{20}	0,1225	0,0150	0,0219	0,0206	0,0190	0,0217	0,0137	0,0203	0,0045	0,0016	0,0103	0,0013
D_{21}	0,0008	0,0090	0,0477	0,0079	0,0594	0,0005	0,0101	0,0060	0,0324	0,0287	0,0241	0,0607
D_{22}	0,1728	0,1680	0,0035	0,0027	0,0211	0,0133	0,0119	0,0026	0,0336	0,0033	0,0096	0,0504
D_{23}	0,0089	0,0031	0,0002	0,0002	0,0551	0,0005	0,0016	0,0006	0,0356	0,0014	0,0044	0,0026
D_{24}	0,0011	0,0400	0,0138	0,0037	0,0177	0,2173	0,0089	0,0011	0,0418	0,0052	0,2522	0,0000
D_{25}	0,0015	0,0353	0,0198	0,0033	0,0180	0,0013	0,0016	0,0015	0,0372	0,0041	0,0008	0,0107
D_{26}	0,1360	0,0354	0,0198	0,0028	0,0198	0,1429	0,0008	0,0009	0,0338	0,0169	0,0128	0,0004
D_{27}	0,0021	0,0025	0,0029	0,4137	0,0203	0,0001	0,0123	0,0011	0,0577	0,0003	0,0042	0,0088
D_{28}	0,0746	0,3881	0,2442	0,3377	0,0228	0,3132	0,2209	0,0010	0,4512	0,2447	0,1266	0,0005
D_{29}	0,1423	0,3455	0,2740	0,3122	0,1382	0,0014	0,1965	0,0309	0,0435	0,0282	0,3262	0,0163
D_{30}	0,1292	0,0344	0,0129	0,0125	0,0360	0,0146	0,0070	0,0004	0,2523	0,3002	0,0619	0,0038
D_{31}	0,0003	0,3644	0,0001	0,0012	0,0228	0,0001	0,0131	0,0010	0,0361	0,0018	0,0069	0,0056
D_{32}	0,3020	0,1083	0,1076	0,0997	0,0220	0,3323	0,0771	0,0563	0,0029	0,0079	0,0042	0,0188
D_{33}	0,3176	0,1159	0,1040	0,0984	0,0292	0,3249	0,0684	0,0278	0,0034	0,0923	0,0993	0,0080
D_{34}	0,0230	0,0158	0,0212	0,0245	0,1479	0,0057	0,0003	0,0078	0,0001	0,0017	0,0915	0,0012
D_{35}	0,3454	0,1323	0,1184	0,0062	0,0192	0,0119	0,0137	0,0449	0,0715	0,3106	0,0015	-0,0017
D_{36}	0,1274	0,2044	0,0487	0,0117	0,0196	0,1708	0,0147	0,0608	0,3516	0,0018	0,0037	0,0174

D_{37}	0,0086	0,0194	0,0001	0,0022	0,0230	0,0004	0,0009	0,1983	0,0492	0,0029	0,0225	0,1556
D_{38}	0,0125	0,1761	0,0038	0,0118	0,0162	0,0004	0,0022	0,0004	0,0524	0,0064	0,0051	0,0422
D_{39}	0,0024	0,0523	0,1497	0,0188	0,0192	0,1753	0,0358	0,0004	0,0450	0,0020	0,3334	0,0103
D_{40}	0,0028	0,1777	0,1134	0,0486	0,0261	0,1904	0,3655	0,5410	0,0194	0,0010	0,1441	0,0317
D_{41}	0,1728	0,1076	0,0121	0,0154	0,0004	0,0129	0,0127	0,0024	0,0580	0,0009	0,2716	0,0082
D_{42}	0,0067	0,1850	0,0103	0,0149	0,0227	0,0129	0,0129	0,0028	0,0579	0,0137	0,0002	0,0073
D_{43}	0,1186	0,0022	0,0140	0,0119	0,0139	0,0849	0,0122	0,0007	0,0281	0,0022	0,1441	0,0030
D_{44}	0,0049	0,0422	0,0097	0,0057	0,0162	0,0004	0,0117	0,0033	0,0121	0,0327	0,2780	0,0002
Variable	**MO-ET**	**ZC-ET**	**DA-ET**	**RI-LT**	**CA-LT**	**TE-LT**	**MO-LT**	**ZC-LT**	**DA-LT**	**CA-RI**	**TE-RI**	**MO-RI**
Total	0,0762	0,2876	0,0534	0,0645	0,0853	0,0348	0,1253	0,0120	0,0186	0,1525	0,0590	0,2348
D_1	0,1249	0,2865	0,0059	0,1930	0,0576	0,0128	0,1277	0,0001	0,0271	0,0646	0,0335	0,2194
D_2	0,1650	0,2306	0,0060	0,0380	0,0184	0,0021	0,0553	0,0027	0,0854	0,0144	0,0316	0,0199
D_3	0,1658	0,0107	0,0059	0,0398	0,0289	0,0073	0,0466	0,0042	0,0854	0,0048	0,0163	0,0046
D_4	0,0016	0,0050	0,0085	0,0550	0,0003	0,0231	0,0255	0,0887	0,0005	0,0136	0,0412	0,2005
D_5	0,0008	0,0004	0,0731	0,0118	0,0148	0,0316	0,0129	0,0000	0,0184	0,0622	0,0956	0,1927
D_6	0,0044	0,2870	0,0007	0,0030	0,0191	0,0096	0,0100	0,0012	0,0176	0,0267	0,0350	0,1927
D_7	0,0059	0,0005	0,0029	0,0008	0,0025	0,0421	0,0165	0,0007	0,0181	0,0102	0,0362	0,0112
D_8	0,0072	0,0007	0,0062	0,0010	0,0133	0,0116	0,0151	0,0051	0,0180	0,0213	0,0632	0,2068
D_9	0,0002	0,0018	0,0011	0,0005	0,0007	0,0011	0,0063	0,0000	0,0854	0,0191	0,0387	0,2052
D_{10}	0,1662	0,0009	0,0010	0,0033	0,0189	0,0025	0,0099	0,0019	0,0180	0,0231	0,0280	0,0010
D_{11}	0,1652	0,0009	0,0004	0,0474	0,0096	0,0026	0,0071	0,0001	0,0178	0,0231	0,0297	0,1945
D_{12}	0,0383	0,2865	0,0001	0,0037	0,0048	0,0002	0,0052	0,0001	0,0854	0,0223	0,0611	0,1964
D_{13}	0,0022	0,2673	0,0004	0,0003	0,0100	0,0056	0,0076	0,0006	0,0854	0,0205	0,0318	0,2040
D_{14}	0,1249	0,3390	0,0027	0,0124	0,0124	0,0207	0,1277	0,0887	0,0184	0,0199	0,0600	0,1884
D_{15}	0,2134	0,0027	0,0003	0,0013	0,0055	0,0190	0,0077	0,0001	0,0206	0,0274	0,0428	0,0022
D_{16}	0,1149	0,1755	0,0473	0,0239	0,0203	0,0254	0,0109	0,0004	0,0171	0,0047	0,0550	0,0096
D_{17}	0,1229	0,0032	0,0019	0,0056	0,0252	0,1937	0,0091	0,0002	0,0195	0,0390	0,0556	0,2026
D_{18}	0,1679	0,1755	0,0029	0,0028	0,0169	0,0488	0,0125	0,0011	0,0216	0,0187	0,0394	0,0057
D_{19}	0,1640	0,0022	0,0030	0,0086	0,0009	0,0019	0,0318	0,0003	0,0433	0,0449	0,0326	0,0535
D_{20}	0,1642	0,2866	0,0030	0,0281	0,0001	0,0018	0,0131	0,0005	0,0253	0,0480	0,0317	0,1891
D_{21}	0,1664	0,1892	0,0004	0,0403	0,0024	0,0015	0,0106	0,0005	0,0194	0,0287	0,0301	0,1928
D_{22}	0,1665	0,0040	0,0010	0,0017	0,0090	0,0043	0,0061	0,0502	0,0854	0,0230	0,0671	0,2034
D_{23}	0,1249	0,0213	0,0007	0,0006	0,0001	0,0514	0,0014	0,0001	0,1104	0,0247	0,0652	0,2045
D_{24}	0,2257	0,0005	0,0000	0,0016	0,0100	0,1714	0,0122	0,0010	0,0206	0,0314	0,0385	0,0046
D_{25}	0,1682	0,2868	0,0001	0,0015	0,0006	0,0004	0,0021	0,0002	0,0197	0,0324	0,0376	0,0040
D_{26}	0,1650	0,2758	0,0004	0,0443	0,0024	0,0044	0,0565	0,0000	0,0854	0,0118	0,0274	0,2062
D_{27}	0,0009	0,1424	0,0000	0,0734	0,2608	0,0747	0,0125	0,0003	0,0082	0,2842	0,0633	0,0002
D_{28}	0,0184	0,2646	0,0137	0,0557	0,1491	0,0263	0,2435	0,0338	0,0854	0,0309	0,0942	0,1861
D_{29}	0,0184	0,2852	0,0731	0,0526	0,0490	0,0503	0,0780	0,0887	0,0363	0,2220	0,0709	0,0139
D_{30}	0,0057	0,0054	0,0040	0,0609	0,0061	0,0515	0,0187	0,0009	0,0092	0,0057	0,0482	0,1862
D_{31}	0,1660	0,2817	0,0002	0,0015	0,0106	0,0073	0,0111	0,0001	0,0173	0,0234	0,0356	0,2063
D_{32}	0,2389	0,0128	0,0001	0,0344	0,0559	0,0458	0,0053	0,0004	0,0854	0,0160	0,0202	0,0051
D_{33}	0,2456	0,0084	0,0005	0,0011	0,0245	0,0417	0,0627	0,0010	0,0182	0,0396	0,0188	0,0119
D_{34}	0,0006	0,3088	0,0012	0,0885	0,0536	0,0368	0,0363	0,0005	0,0178	0,0308	0,0630	0,0036
D_{35}	0,0020	0,0012	0,0008	0,0865	0,0119	0,0081	0,1900	0,0002	0,0110	0,2887	0,0687	0,0036

D_{36}	0,1249	0,0041	0,0462	0,1459	0,2342	0,0098	0,0409	0,0957	0,0255	0,0030	0,0328	0,0018
D_{37}	0,0053	0,0011	0,0731	0,0020	0,0551	0,0210	0,0133	0,0006	0,0854	0,0153	0,0955	0,2162
D_{38}	0,1659	0,4912	0,0008	0,0070	0,0044	0,0038	0,0185	0,0008	0,0854	0,0240	0,0591	0,2006
D_{39}	0,1249	0,0005	0,0738	0,0787	0,0254	0,0491	0,0177	0,0010	0,1464	0,2964	0,0731	0,0056
D_{40}	0,0000	0,0071	0,0731	0,0374	0,0004	0,0251	0,0025	0,0061	0,0184	0,0049	0,0044	0,2034
D_{41}	0,0024	0,0001	0,0012	0,0651	0,0400	0,0033	0,0261	0,0009	0,0166	0,0245	0,1951	0,0005
D_{42}	0,0016	0,0000	0,0017	0,0004	0,0171	0,0259	0,0278	0,0008	0,0167	0,0240	0,0148	0,0005
D_{43}	0,1249	0,0009	0,0002	0,0003	0,0260	0,0051	0,0044	0,0353	0,0171	0,0213	0,0319	0,1889
D_{44}	0,0157	0,0063	0,0023	0,0421	0,0069	0,0033	0,0697	0,0123	0,0000	0,1142	0,0305	0,2117
Variable	**ZC-RI**	**DA-RI**	**TE-CA**	**MO-CA**	**ZC-CA**	**DA-CA**	**MO-TE**	**ZC-TE**	**DA-TE**	**ZC-MO**	**DA-MO**	**ZC-DA**
Total	0,2589	0,2075	0,0383	0,1884	0,0894	0,0162	0,1021	0,0981	0,0619	0,0019	0,0004	0,0155
D_1	0,0147	0,0235	0,0028	0,0222	0,0045	0,0003	0,0073	0,0016	0,0023	0,0003	0,0003	0,0013
D_2	0,0073	0,0045	0,0014	0,0378	0,0129	0,0092	0,0028	0,0021	0,0057	0,0049	0,0011	0,1413
D_3	0,0048	0,0010	0,0228	0,0148	0,0002	0,0085	0,0109	0,0055	0,0003	0,0417	0,1276	0,0008
D_4	0,0104	0,0057	0,0169	0,0174	0,0018	0,0076	0,0059	0,0299	0,0697	0,0001	0,0000	0,0005
D_5	0,0063	0,0257	0,0148	0,0191	0,0114	0,0015	0,0024	0,0282	0,0233	0,0001	0,0004	0,0005
D_6	0,0007	0,0062	0,0274	0,0104	0,0004	0,0032	0,0011	0,0068	0,0017	0,0897	0,1276	0,0784
D_7	0,0065	0,0117	0,0304	0,0176	0,0034	0,0068	0,0067	0,0201	0,0309	0,0003	0,0004	0,0006
D_8	0,0001	0,0079	0,0931	0,0074	0,0050	0,0064	0,0114	0,0032	0,0051	0,0897	0,1276	0,0004
D_9	0,0006	0,0009	0,0069	0,0026	0,0043	0,0003	0,0312	0,0396	0,0035	0,0426	0,1726	0,0003
D_{10}	0,0092	0,0002	0,0251	0,0052	0,0049	0,0036	0,0030	0,0014	0,0005	0,0026	0,1696	0,0000
D_{11}	0,0001	0,0060	0,0413	0,0063	0,0002	0,0006	0,0028	0,0090	0,0060	0,0001	0,1276	0,0002
D_{12}	0,0001	0,0005	0,0311	0,0065	0,0009	0,0000	0,0259	0,0251	0,0119	0,1933	0,1276	0,0001
D_{13}	0,0031	0,0049	0,2115	0,0018	0,0052	0,0020	0,0040	0,0096	0,0020	0,0897	0,0002	0,0043
D_{14}	0,0048	0,0003	0,0607	0,0043	0,0001	0,0020	0,0004	0,0008	0,0070	0,0003	0,0056	0,0010
D_{15}	0,0015	0,0214	0,2606	0,0113	0,0081	0,0349	0,0126	0,0112	0,0038	0,0003	0,0004	0,0061
D_{16}	0,0081	0,0119	0,0229	0,0048	0,0018	0,0029	0,0130	0,0134	0,0032	0,0434	0,0055	0,0001
D_{17}	0,0047	0,0011	0,0256	0,0065	0,0022	0,0029	0,0226	0,0015	0,0276	0,0003	0,0079	0,1445
D_{18}	0,0018	0,0015	0,0260	0,0343	0,0010	0,0053	0,0060	0,0207	0,0096	0,0020	0,0004	0,0012
D_{19}	0,0077	0,2064	0,0025	-0,0048	0,0069	0,0040	0,0012	0,0001	0,0048	0,0053	0,1276	0,0020
D_{20}	0,0021	0,0091	0,0016	0,0034	0,0067	0,1301	0,0015	0,0006	0,0048	0,0897	0,0059	0,1394
D_{21}	0,0256	0,0041	0,0553	0,0019	0,0007	0,0021	0,0071	0,0453	0,0074	0,0897	0,1741	0,0009
D_{22}	0,0008	0,0018	0,0260	0,0034	0,0033	0,0058	0,0759	0,0122	0,0033	0,0004	0,1276	0,0010
D_{23}	0,0012	0,0010	0,0023	0,0030	0,0036	0,0012	0,0028	0,0004	0,0036	0,0045	0,0059	0,0005
D_{24}	0,0043	0,0041	0,0025	0,0052	0,0007	0,0001	0,0026	0,0000	0,0010	0,0031	0,1276	0,0013
D_{25}	0,0032	0,0103	0,0017	0,0044	0,0003	0,0001	0,0000	0,0007	0,0028	0,0003	0,1276	0,0000
D_{26}	0,0044	0,0077	0,0014	0,0024	0,0038	0,0030	0,0017	0,0036	0,0078	0,0512	0,0059	0,0019
D_{27}	0,0019	0,0252	0,0519	0,0088	0,3532	0,0027	0,0018	0,0000	0,0045	0,0078	0,0004	0,0018
D_{28}	0,0529	0,0526	0,0139	0,0041	0,0413	0,0576	0,0525	0,0282	0,0501	0,0044	0,0955	0,0104
D_{29}	0,0429	0,0884	0,0202	0,1915	0,0846	0,0410	0,4893	0,0254	0,0328	0,0038	0,0082	0,0010
D_{30}	0,0014	0,0220	0,0181	0,0054	0,0073	0,0025	0,0213	0,0166	0,0055	0,0015	0,0000	0,0126
D_{31}	0,0003	0,0005	0,0037	0,0024	0,0047	0,0042	0,0075	0,0144	0,0003	0,0004	0,0001	0,0008
D_{32}	0,0081	0,0050	0,0654	0,0014	0,0042	0,0067	0,0386	0,0469	0,0185	0,0897	0,0004	0,0002
D_{33}	0,0283	0,0096	0,0329	0,0006	0,0013	0,0102	0,0331	0,0489	0,0417	0,0837	0,4775	0,0008
D_{34}	0,0042	0,0011	0,0413	0,0253	0,0163	0,0111	0,0028	0,0002	0,0008	0,0052	0,0001	0,0018

D_{35}	0,0131	0,0127	0,0009	0,0099	0,0040	0,0869	0,0030	0,0010	0,0117	0,0002	0,0083	0,1495
D_{36}	0,0032	0,0014	0,0020	0,0000	0,0031	0,0042	0,0027	0,0013	0,0048	0,0055	0,1276	0,0139
D_{37}	0,0005	0,0007	0,1091	0,0187	0,0006	0,0076	0,0183	0,0014	0,0077	0,0000	0,0007	0,0052
D_{38}	0,0002	0,0042	0,0006	0,0040	0,0020	0,0046	0,0042	0,0125	0,0102	0,1914	0,0001	0,0003
D_{39}	0,2201	0,0107	0,0156	0,0022	0,0134	0,0027	0,0149	0,0094	0,0134	0,0897	0,0040	0,0058
D_{40}	0,0011	0,0030	0,0207	0,0085	0,0072	0,0049	0,0115	0,0005	0,0134	0,0354	0,0061	0,0004
D_{41}	0,0001	0,0044	0,0085	0,0057	0,0228	0,0016	0,0255	0,0024	0,0088	0,0002	0,0017	0,1431
D_{42}	0,0001	0,0001	0,0217	0,0019	0,0001	0,0024	0,0123	0,0010	0,0985	0,0001	0,0019	0,0006
D_{43}	0,0027	0,0009	0,0076	0,0062	0,0045	0,0014	0,0024	0,0126	0,0200	0,0002	0,0001	0,0040
D_{44}	0,0362	0,0063	0,0021	0,0032	0,0030	0,0025	0,0035	0,0046	0,0022	0,0020	0,0004	0,0006