UIS BUSINESS SCHOOL

MASTER'S THESIS

STUDY PROGRAM:	THESIS IS WRITTEN IN THE FOLLOWING SPECIALIZATION/SUBJECT:
Master of Science in Business Administration	**Applied Finance** IS THE ASSIGNMENT CONFIDENTIAL? **No**

TITLE:

The Impact of Cryptocurrency-Related Cyberattacks on Cryptocurrencies and Traditional Financial Assets

AUTHORS		SUPERVISOR:
Candidate number: 3084 …… 3078 ……	Name: Mattis Storsveen …… Florent Veliqi ……	Peter Molnár

Abstract

This thesis investigates the impact of cryptocurrency-related cyberattacks on the cryptocurrency market as well as on traditional financial markets. We utilize a dataset consisting of historical data on cyberattacks and daily trading data for twenty cryptocurrencies, five payment system stocks, four stock indices and one commodity, over the sample period of December 27, 2013 - December 31, 2019. Regarding the impact on cryptocurrencies, we find that cryptocurrency-related cyberattacks are associated with negative returns, increased volatility and increased trading volume. The size of the impact depends on the magnitude of the cyberattack and this impact is decreasing over time. Furthermore, the results provide evidence that cryptocurrency-related cyberattacks are associated with negative returns and elevated volatility not only for cryptocurrencies, but also for payment companies, the financial and technology sectors, and the general stock market. On the other hand, these attacks are associated with positive returns for gold, and their impact on the commodity index is insignificant.

Keywords: Cryptocurrency market, cryptocurrencies, cybercrime, cyberattacks, return, volatility, trading volume, traditional financial assets

Acknowledgement

This thesis concludes our Master's degree in Business Administration with specialization in Applied Finance, at the University of Stavanger Business School. The chosen topic is motivated by a genuine interest in the cryptocurrency market.

We extend our sincerest gratitude to our supervisor Professor Peter Molnár for his invaluable guidance and helpfulness. His extensive competence and knowledge have been an immense contribution to our work.

Contents

List of Figures

List of Tables

1 Introduction

In 2008, the paper *Bitcoin: A Peer-to-Peer Electronic Cash System* was published by the pseudonym Satoshi Nakamoto, through which the cryptocurrency market emerged, with the creation of Bitcoin and the activation of the blockchain in 2009. Roughly a decade later, thousands of cryptocurrencies have entered the market. As of December 2019, there are about 5000 cryptocurrencies with an accumulated market capitalization of approximately $200 billion (CoinMarketCap). Despite the fact that trading in cryptocurrencies is, by many, considered raw speculation because of their highly volatile nature (Trimborn and Härdle, 2018; Liu and Serletis, 2019), the rapidly growing market has attracted investors looking to take part in the rise of cryptocurrencies. Individuals can trade cryptocurrencies for traditional currencies and assets through cryptocurrency exchanges, which are often regulated, where users need accounts with valid identities to trade. Alternatively, individuals can trade cryptocurrencies through unregulated peer-to-peer transactions, allowing individuals to trade anonymously and without having to rely on an intermediary.

Unlike traditional financial markets, the cryptocurrency market is not dependent on higher authorities, any physical assets, nor any political or governmental regulation. Instead, cryptocurrencies are founded on an algorithm that traces all transactions. The lack of a centralized system and the inherently low levels of regulation for this digital asset, combined with its users' ability to trade anonymously, are thought to facilitate the growth of illegal activity. Foley et al. (2019) discover that about one-fourth of all Bitcoin users are participating in illegal activity and claim that the cryptocurrency market might be one of the largest unregulated markets in the world. Additionally, they estimate that approximately $76 billion of the annual illegal activity can be linked to Bitcoin, which makes up roughly 46% of all Bitcoin transactions. This nearly constitutes all illegal drugs traded on a yearly basis in the U.S. and European markets combined (Foley et al., 2019).

The substantial amount of illegal activity that can be linked to Bitcoin (and other cryptocurrencies) can possibly be explained by the fact that the cryptocurrency technology is, in large, based on the ideas of decentralization, anonymity and irreversible transactions. Further, because these characteristics make it impossible to track and revert transactions, appealing opportunities emerge for cybercriminals. Most prominently, once private financial information is stolen from individual cryptocurrency users and abused, or weaknesses in a cryptocurrency exchange's code are exploited, there is no way to recover the funds.

As cryptocurrencies are becoming more incorporated into global finance and payment systems, we see an increasing interest in understanding the underlying mechanics of the market and how cryptocurrencies are related to the world economy. Numerous studies examine how the cryptocurrency market affects traditional financial markets, in which the main topics comprise risk and diversification. There is, however, a gap in the literature when it comes to understanding the impact of cyberattacks linked to cryptocurrencies (Corbet et al., 2019a). The purpose of this thesis is to fill this void by investigating the impact of cryptocurrency-related cyberattacks on the return, volatility and trading volume of cryptocurrencies and traditional financial assets.

This thesis expand the literature on cybercrime in the cryptocurrency market in several ways, contributing to a broader understanding of how cryptocurrencies and other, more traditional, financial assets are affected by cryptocurrency-related cyberattacks. A more accurate estimate of the impact of cyberattacks is achieved by incorporating a loss magnitude that captures the size of the estimated loss while controlling for the continuously growing market capitalization. Further, compared to previous research, a large sample is utilized, consisting of trading history for twenty cryptocurrencies from December 27, 2013, through December 31, 2019. This mitigates any small-sample issues. Finally, this thesis expands previous research on cryptocurrency-related cyberattacks by additionally investigating their impact on traditional financial assets.

We find that cryptocurrency-related cyberattacks have a statistically significant impact on the return, volatility and trading volume of cryptocurrencies, translating into a negative impact on cryptocurrencies overall. More specifically, cryptocurrency-related cyberattacks are associated with negative returns, increased volatility and increased trading volume. With respect to traditional financial assets, we find that, for payment system stocks, these cyberattacks are associated with negative returns and elevated volatility. Further, evident from the results, cryptocurrency-related cyberattacks, overall, have a negative impact on stock indices and a positive effect on gold.

The remainder of this thesis is organized as follows. Section 2 briefly explains the cryptocurrency technology and the most common cyberattacks. Section 3 provides an overview of the literature background. Section 4 introduces the data collection and data processing, while a detailed explanation of the methodology and research approach is provided in Section 5. Section 6 presents and discusses the results and Section 7 concludes.

2 The cryptocurrency technology and cyberattacks

Cryptocurrency transactions are considered virtually impossible to manipulate because of the highly advanced technology underlying the cryptocurrencies. This section aims to describe how people with the right tools and competence are able to exploit weaknesses in the system by providing the reader with information about the technology and the system's weaknesses.

2.1 Technology: Cryptography and blockchain

A cryptocurrency is a system that allows for secure online payments by using cryptography and blockchain technology to protect information and communications. Cryptography refers to the use of encryption algorithms to ensure that only the intended receiver is able to access the information (Rouse, 2020), whereas a blockchain is a means of keeping record of transactions. This is a decentralized system, meaning that no third parties, such as financial institutions and political or governmental regulatory systems, are required. It is, arguably, the advantages brought by this decentralized technology that draw people to the cryptocurrency market. Most notably, the blockchain technology seems to solve the double-spending problem and makes it nearly impossible to counterfeit. This results in a system that can be trusted, which makes it possible for people to trade directly with each other without having to rely on an intermediary, subsequently reducing transaction costs and increasing the efficiency.

The prevalence of a cryptocurrency relies on its advanced security and is most certainly derived from its revolutionary, innovative technology. The technology behind cryptography refers to a system that protects and secures information and communication – through utilization of encryption algorithms – to ensure that only intended receivers can read and process the data (Katz and Lindell, 2014). Essentially, cryptography transforms data into a format that is illegible for operators without permission. Moreover, the information can only be viewed with a key that encrypts it. Thus, data can be transferred without allowing unwarranted authorities to tamper with it. The information continues to have integrity seeing as it cannot be changed while it is being stored or transferred. Finally, cryptography also assists in non-repudiation, which means that the sender or creator cannot deny the validity of a message. The blockchain technology, which underlies most cryptocurrencies, is fundamentally a public database (the chain) where digital information (the block) is stored. In essence, the blockchain technology enables

digital information to be recorded and distributed, but not changed. The blockchain is a distributed, decentralized public ledger, meaning that no central authority (the government, financial institutions or any other third party) is required. Instead, transactions are verified by a network of computers, effectively distributing authority between the users to allow for peer-to-peer trading.

Every block on the blockchain is added at the end of the chain, and each of these blocks contain a cryptographic hash (a mathematical algorithm that converts any data into a distinct format), which makes it extremely difficult to go back and change the digital information. Assuming that a potential cybercriminal attempts to change one single block, the cybercriminal would then have to change every single block after the changed block on the blockchain. This would require a recalculation of all the hashes and, necessarily, a tremendous quantity of computing power. Further, to control for any uncertainty, blockchain networks have initiated a system commonly referred to as the "proof of work", which is based on solving advanced computational math problems to verify transactions and add them to the blockchain. The process of adding blocks to the blockchain is referred to as mining.

2.2 Cyberattacks

Some of the blockchain's characteristics have, arguably, had the repercussion of making cryptocurrencies attractive targets for cybercriminals. In particular, we would like to highlight two factors; irreversible transactions and anonymity. The former is based on transactions not being reversible if there already is consensus in the blockchain network that the new information is valid, i.e. once illegal transactions reach the blockchain, the funds are lost for good. The latter makes it impossible to find out who is responsible and to recover stolen funds by accessing their computer.

Although a blockchain is considered to be incredibly difficult, if not impossible, to hack because of the advanced technology on which it is developed, it is still prone to several types of cybersecurity threats (Xu, 2016; Sayeed and Marco-Gisbert, 2019; Li et al., 2020). The most prominent threat is the possibility of a 51% attack (Swan, 2015), which refers to cybercriminals that gain control over more than half of the network's computing or mining hash power. Cybercriminals that gain possession of the majority of the network's processing power can exploit several vulnerabilities in the blockchain technology by manipulating the recording protocol for new transactions (blocks) which, in turn, interferes with or prevents other miners from

adding blocks to the blockchain (Li et al., 2020). They can also complete transactions and then fraudulently construct it so that it seems like they still have the coins that were just spent. This type of manipulation, referred to as double-spending, allows cybercriminals to spend their cryptocurrencies twice. However, seeing as a 51% attack would potentially require cybercriminals to acquire control of millions of computers (depending on the size of the cryptocurrency and its blockchain), a successful attack is particularly unlikely.

Cryptocurrency exchanges and individual cryptocurrency users, whose systems are not as secure as the blockchain, are considerably more vulnerable to cyberattacks. Cryptocurrency exchanges manage large volumes of money and are, therefore, attractive targets for cybercriminals. One can argue that cryptocurrency exchanges are particularly vulnerable to cyberattacks due to their centralized systems (Moore and Christin, 2013), making them prone to the same security limitations as "the rest of the internet". This means that cryptocurrency exchanges are only as secure and protected against a cyberattack as the implementation of their security. In fact, as of 2015, at least three of the five largest cryptocurrency exchanges – Bitfinex, Bitstamp, BTC-e, BTC China and Mt.Gox – had been subject to cyberattacks (Brandvold et al., 2015). Cybercriminals can also exploit loopholes in a cryptocurrency exchange's code to steal funds by manipulating the system. Cyberattacks targeting cryptocurrency exchanges are better explained by reviewing how the largest Bitcoin and Ethereum hacks took place.

In 2014, the world's largest Bitcoin exchange, Mt. Gox, ceased all Bitcoin withdrawals in an attempt to find out why they were encountering transaction delays. They discovered that they had been exposed to a transaction malleability attack, involving that someone was able to manipulate the transaction data before it reached the blockchain by exploiting shortcomings in their system. The cybercriminals were capable of overwriting the transactions, effectively making the transactions look like they were not confirmed when, in reality, they were confirmed. As a consequence, they were able to get away with around 470 million dollars' worth of Bitcoins before the Mt. Gox exchange finally caught up to what they were doing. Because the blockchain is immutable, and the transactions had already reached the blockchain, nothing could be done to retrieve the funds (Trautman, 2014; Garnier and Solna, 2019).

The largest Ethereum attack took place in 2016, when a cybercriminal exploited a 28-day exit loophole in the Decentralized Autonomous Organization (DAO)

exchange that allowed the attacker to get away with around 50 million dollars. The cybercriminal was capable of making DAO's contract withdraw Ether several times before the contract could refresh its balance. There were primarily two issues that allowed this hack to occur. First of all, the contract was designed to send the Ether before refreshing the token balance and, second of all, the DAO coders overlooked the likelihood of a recursive call. As a consequence, the cybercriminal made the contract malfunction as a result of its recursive function, which would reset the code and allow the cybercriminal to exchange DAO tokens multiple times. This loop continued until 50 million dollars' worth of Ether was stolen and, subsequently, lead to the creation of two cryptocurrencies; Ethereum and Ethereum classic (Mehar et al., 2019; de Graaf, 2019; Zachariadis et al., 2019).

Regarding individual cryptocurrency users, there are many different ways for cybercriminals to target individuals in an effort to gain access to sensitive information. Cybercriminals are constantly developing new methods to target individuals and, with the intention of providing a general understanding of how cyberattacks occur, this thesis only explains a few. One of the most established methods is the so-called phishing method – a type of social engineering attack that is based on stealing sensitive user data such as login documentations, credit card numbers and other account information, i.e. passwords (Goel and Jain, 2018). Phishing occurs when a cybercriminal pretends to be a reliable source and tricks individuals into opening emails (or other communication platforms), and further misleads the victims into clicking on harmful internet links that are designed to give the cybercriminal full access of the victims' sensitive user data. Phishing may also be used to direct individuals to a website that installs a mining application on the victim's personal computer (Higbee, 2018). This type of hack is much more subtle as it, instead of transferring funds from the victim's bank account or cryptocurrency wallet, drains the victim's computing power, thereby imposing higher electricity expenses on the victim.

A clipboard hijacking attack is another common way for cybercriminals to target individuals. This type of attack is based on a damaging software utilized to make illegal, swindling cryptocurrency transactions. Cybercriminals can easily accomplish this by changing the cryptocurrency wallet addresses from the victims' saved clipboards to similar ones that are possessed by the cybercriminals. Individuals may also be attacked through keyloggers – computer software that the cybercriminal secretly programs into the victim's device (i.e. phone or computer). This software transmits sensitive data from the victim's device to the cybercriminal's device.

Conclusively, the cryptocurrency market is affected by flaws in the cryptocurrency exchanges' infrastructure and human errors, ultimately making it possible to hack what seems to be a nearly impossible target.

3 Literature review

The rapid rate at which the cryptocurrency market has been developing over the last decade has attracted a multitude of investors looking to take part in the tremendous, yet unknown, growth potential. The interest in understanding how cryptocurrencies behave has increased accordingly. In the early stages, studies on the cryptocurrency market, in large, based their analysis solely on Bitcoin while alternative cryptocurrencies were being overlooked. The issue with limiting the analysis to only one cryptocurrency is that digital assets do not react in an identical manner (Corbet et al., 2020). Cryptocurrencies have been recognized as a likely improvement of, and possibly a successor for, currency as we know it, while also exhibiting the characteristics of a financial asset. "This dual nature has proved crucial to its success" (Polasik et al., 2015).

Bitcoin is characterized as what Selgin (2015) calls a "synthetic commodity money" because it is a hybrid between fiat currency (having no intrinsic value) and commodity currency (being unregulated). One of the main drivers of Bitcoin prices is its popularity (Polasik et al., 2015), and Bitcoin's performance is correlated with the perception of the underlying technology (Cahill et al., 2020). Baur et al. (2018) investigate Bitcoin's current and future usage by analyzing its statistical properties. They find that the majority of Bitcoin users hold Bitcoin for investment, and that Bitcoin offers diversification benefits because it is uncorrelated with traditional assets and currencies. As for its future as a transactional medium, Easley et al. (2019) argue that the Bitcoin blockchain does not have the necessary processing capabilities to replace fiat currencies, having a capacity to process only seven transactions per second (in comparison, Visa can theoretically process up to 50 thousand transactions per second).

Urquhart (2016) recognized that, despite the claims of Bitcoin being an asset rather than a currency, the efficiency of Bitcoin had not yet been investigated. The author employs a series of tests to see if Bitcoin is robust to weak form market efficiency and finds the Bitcoin market to be inefficient in the full period studied (October 1, 2010 - July 31, 2016). However, results from dividing the sample into two

sub-samples indicate that Bitcoin is becoming more efficient over time, perhaps because the number of people that are analyzing and trading Bitcoin is constantly increasing.

Balcilar et al. (2017) analyze the impact of trading volumes on Bitcoin returns and volatility and find that volume can predict returns, but not volatility. Aalborg et al. (2019) find that neither the volatility nor the volume is able to predict or explain the return. On the contrary, both the return and the trading volume improve volatility predictions, and the volume also have explanatory power on the volatility. Returns and volatility of Bitcoin are studied further in Thies and Molnár (2018), who find that higher volatility is associated with higher average returns. Enoksen et al. (2020) study cryptocurrency bubbles and find that higher volatility, trading volume and transactions are positively associated with the presence of bubbles across cryptocurrencies.

3.1 Cybercrime and cryptocurrencies

While countless of studies have been conducted on the cryptocurrency market, there is a gap in the literature when it comes to understanding the impact cyberattacks related to cryptocurrencies have on the cryptocurrency market (Corbet et al., 2019a). It is at least intuitively obvious that cryptocurrencies, whose existence depends entirely on the internet, are highly exposed to cybercrime. In recent years, the research on the cryptocurrency market have directed more attention towards investigating the market's exposure to cybercrime.

One of the criminal domains in cybercrime is online trading with stolen credit card information, often referred to as "carding". van Hardeveld et al. (2017) recognize the persistent challenges with cybercrime in the crypto market and study some of the tools that are employed by cybercriminals, with a special focus on carding. The authors' objective is to contribute to a better understanding of criminal operations in the cryptocurrency market, identify pitfalls in the tools that are used, reveal potential weaknesses related to the security of individual cryptocurrency users, and help law enforcement make more informed decisions with regards to how they approach investigations.

In recent years, there has been an increased interest in understanding how cryptocurrencies are affected by illegal online activity. Gandal et al. (2018) investigate the impact of suspicious trading activity that occurred on the Mt. Gox

Bitcoin exchange in 2013 and discover that both the price growth and the trading volume were significantly higher on days with suspicious trading activity. More specifically, they find that prices increased on around 80% of the days with suspicious trading activity, while prices increased only on around 55% of the days without suspicious trading activity. One would expect that the continuously growing market capitalization of the crypto market would eliminate the possibilities to manipulate the price. However, Gandal et al. argue that price manipulation remains feasible because the number of small-cap cryptocurrencies keep increasing.

Corbet et al. (2019c) study issues related to the cryptocurrency market and find that it lacks major regulatory policies and, thus, leaves room for criminality to evolve. The authors also find cryptocurrencies to be characterized by significantly higher volatility than more traditional assets, and suggest that a contributing factor might be the fact that cryptocurrencies have no earnings and no consensus valuation framework. Corbet et al. (2019a) and Corbet et al. (2019b) investigate the financial market implications of cryptocurrency-related cybercriminality, as well as the dynamics between price volatility, price discovery and cyberattacks, for eight of the major cryptocurrencies. They find cryptocurrency hacking events to elevate both the volatility of the attacked cryptocurrency and the wide cross-cryptocurrency correlation. They also discover that cryptocurrency hacks significantly minimize price discovery derived within the hacked cryptocurrency compared to other cryptocurrencies. Finally, they find that abnormal returns tend to revert to zero in the time periods leading up to cybercrime occurrences when news of the hack are made public. The authors use either a continuous variable for the combined number of cyberattacks or a continuous variable that measures the natural logarithm of the estimated loss, depending on which research question they are investigating.

Caporale et al. (2020) investigate how the returns, realized volatility and trading volume of Bitcoin, Ethereum, Litecoin, XRP and Stellar are affected by cyberattacks. They control for four different cyberattacks (cybercrime, cyber espionage, hacktivism and cyberwarfare), four different target sectors (government, industry, finance and cryptocurrency exchanges), geographic target and the block chain's hash rates. They also control for economic uncertainty, country-specific stock market liquidity and real GDP. The authors use binary variables for the cyberattack types, cyberattack targets and the geographic target (1 if U.S.). They find that only cyber-warfare has a significant effect on returns. Economic uncertainty is found to have either a positive or negative influence on the return, depending on the cryptocurrency. Further, cyberattacks targeting the financial sector have a negative

impact on the cryptocurrencies' realized volatility and trading volume. Moreover, they find a negative relationship between returns and realized volatility, and that the trading volume is positively affected by returns and realized volatility.

The purpose of this thesis is to contribute to a broader understanding of the cryptocurrency market by investigating the impact of cyberattacks on returns, volatility and trading volume. This thesis build upon the aforementioned studies on cryptocurrency cybercrime in a couple of ways. Previous research on cryptocurrencies capture the effect of cyberattacks by incorporating some kind of dummy variable to denote the number of attacks or to reflect the estimated loss. Instead, in an effort to more accurately capture the impact of cyberattacks, this thesis incorporates a loss magnitude – effectively capturing the size of the estimated loss while accounting for the cryptocurrency market's continuously growing market capitalization. Further, our dataset consists of trading history for twenty cryptocurrencies from December 27, 2013, to December 31, 2019. Compared to previous research, this increases the number of observations and reduces any small-sample problems.

Finally, a comparative analysis is conducted, applying the same investigation on various financial assets. Corbet et al. (2019a) and Corbet et al. (2019b) investigate the interactions between several traditional financial assets (S&P500, gold, oil and the GBP/USD exchange rate) and cryptocurrencies. Our thesis expand the research by investigating how traditional assets are influenced by cryptocurrency-related cyberattacks. This thesis analyzes payment system stocks because we suspect that their performance are likely to be more affected by cyberattacks in the cryptocurrency market – compared to other stocks. Additionally, more attention is directed to different sectors in the stock market by including commodity, financial and technology indices.

3.2 Cybercrime and traditional financial assets

Several papers investigate the impact of cybercrime on traditional financial assets. Garg et al. (2003), Campbell et al. (2003) and Cavusoglu et al. (2004) find that cyberattacks have a negative impact on firms' market value. There is also evidence of delayed market reaction (Garg et al., 2003), and it has been shown that smaller firms are more affected by cyberattacks than larger firms (Cavusoglu et al., 2004). According to Andoh-Baidoo (2013), the degree to which investors link announcements of cyberattacks to market value is positively correlated with their knowledge about

security breaches. Further, Andoh-Baidoo finds that investors are more likely to react negatively to cyberattacks targeting internet firms compared to cyberattacks on other firms.

Arcuri et al. (2017) investigate the effect of information security breaches on stock returns and find that market returns are expected to decrease following cyberattack announcements, and that financial companies are often more affected than other companies. Kamiya et al. (2020) find that firms that deal with a large amount of customers are more likely to be targeted by cybercriminals. Moreover, attacked firms suffer a substantial loss in equity value whenever customers' personal financial information is stolen. Kamiya et al. additionally find an increasing trend in the number of cyberattacks. Bianchi and Tosun (2019) find that excess returns are expected to drop following cyberattack announcements, whereas the trading volume and the bid-ask spread are expected to increase on the announcement date.

4 Data

This section describes the data collection and data processing, and provides descriptive statistics for the main variables. This paper uses daily trading data to analyze how hacking attacks related to cryptocurrencies influence the daily return, volatility and trading volume for twenty major cryptocurrencies. To analyze this relationship, historical trading data (open, high, low, and close prices, trading volume and market capitalization) and historical data on cyberattacks (date of the attack, estimated loss and the target) are downloaded.

Daily trading data for cryptocurrencies are retrieved from CoinMarketCap. CoinMarketCap lists cryptocurrencies by market capitalization, from which twenty cryptocurrencies are chosen. Selected cryptocurrencies are required to have trading history prior to 2018 and stablecoins – coins that are designed to have a constant price – are excluded. With respect to these criteria, the twenty largest cryptocurrencies are selected. Table 1 lists the chosen cryptocurrencies. Data is collected as far back as possible, up to and including December 31, 2019. The trading volume is not reported prior to December 27, 2013 and, thus, the sample period utilized is December 27, 2013 - December 31, 2019, amounting to 2196 unique calendar days. Bitcoin (BTC), Litecoin (LTC), XRP (XRP) and Dogecoin (DOGE) are the cryptocurrencies with the longest trading history, while Cardano (ADA) has the shortest history. With respect to market capitalization, DCR is the

cryptocurrency with the smallest market capitalization in the sample, being the 39th largest cryptocurrency at the time of writing (CoinMarketCap, 2020).

Historical data on cybercrime are available on hackmageddon and includes the date of the attack, the target and the estimated loss. The website is developed and maintained by Paolo Passeri, who has more than 15 years of experience from the computer security industry. Access to the full database, with statistics from 2012 to 2019, was obtained upon request. As can be seen in Table 2, a total of 77 cryptocurrency-related cyberattacks are observed during the sample period.

Although the main focus lies on the cryptocurrency market, to investigate whether the effect of cyberattacks is unique for cryptocurrencies, this thesis also studies the impact of cryptocurrency-related cyberattacks in the context of traditional financial assets, over the sample period. Five payment system stocks, four indices, and one commodity are selected, for which daily trading data are retrieved from Yahoo Finance. 1513 unique trading days are observed in this period. The chosen payment systems are Visa (V), Mastercard (MA), PayPal (PYPL), American Express (AXP), and Western Union (WU). The chosen indices are S&P500 (SPY), iShares

Table 1: Overview of the chosen cryptocurrencies.

Name	Ticker	From	To
Bitcoin	BTC	12/27/13	12/31/19
Litecoin	LTC	12/27/13	12/31/19
XRP	XRP	12/27/13	12/31/19
Dogecoin	DOGE	12/27/13	12/31/19
Dash	DASH	2/14/14	12/31/19
Monero	XMR	5/22/14	12/31/19
Stellar	XLM	8/5/14	12/31/19
NEM	XEM	4/1/15	12/31/19
Ethereum	ETH	8/7/15	12/31/19
Decred	DCR	2/10/16	12/31/19
Ethereum Classic	ETC	7/24/16	12/31/19
Neo	NEO	9/9/16	12/31/19
Zcash	ZEC	10/29/16	12/31/19
IOTA	MIOTA	6/13/17	12/31/19
EOS	EOS	7/1/17	12/31/19
Bitcoin Cash	BCH	7/23/17	12/31/19
Binance Coin	BNB	7/25/17	12/31/19
TRON	TRX	9/13/17	12/31/19
Chainlink	LINK	9/20/17	12/31/19
Cardano	ADA	10/1/17	12/31/19

Table 2: Overview of all cryptocurrency-related cyberattacks observed between February 25, 2013, and December 31, 2019.

Date	Target	Loss (USD)	Date	Target	Loss (USD)
03/03/2014	Flexcoin	620 000	18/05/2018	Bitcoin Gold 51% attack	18 000 000
06/03/2014	Poloniex	50 000	22/05/2018	Verge	1 650 000
19/03/2014	CoinEx	NA	28/05/2018	Taylor	1 350 000
11/05/2014	Dogecoin	74 000	05/06/2018	Japanese Syndicate Wallet	10 000 000
05/01/2015	Bitstamp	5 200 000	06/06/2018	Litecoin Cash 51% attack	NA
14/02/2015	Bter	1 750 000	11/06/2018	Coinrail	37 200 000
15/03/2015	AllCrypt	NA	20/06/2018	Bithumb	31 500 000
26/03/2015	Cryptoine	NA	09/07/2018	Bankor	13 500 000
22/06/2015	Scrypt.cc	NA	12/07/2018	40 individuals	5 000 000
15/01/2016	Cryptsy	6 000 000	26/07/2018	KICKICO	7 700 000
06/02/2016	Loanbase	8 000	30/07/2018	Altex Exchange	NA
19/03/2016	naira4dollar.com	15 000	04/08/2018	Livecoin	1 800 000
15/05/2016	Gatecoin	2 000 000	07/09/2018	Bancour	13 500 000
17/06/2016	The DAO	50 000 000	09/09/2018	C-CEX	NA
14/07/2016	Steemit	85 000	14/09/2018	EOSBet	200 000
02/08/2016	Bitfinex	65 000 000	20/09/2018	Zaif	60 000 000
17/02/2017	Zcoin	400 000	26/09/2018	Pigeoincoin	15 000
22/04/2017	Yapizon	5 000 000	06/10/2018	SpankChain	38 000
29/06/2017	ClassicEtherWallet	308 700	15/10/2018	EOSBet	338 000
17/07/2017	CoinDash	7 000 000	21/10/2018	Trade.io	7 500 000
19/07/2017	Perity	30 000 000	28/10/2018	MapleChange	6 000 000
24/07/2017	Veritaseum	8 400 000	05/12/2018	Vertcoin 51% attack	10 000
21/08/2017	Enigma	500 000	21/12/2018	Electrum Bitcoin Wallets	750 000
01/10/2017	OKEx	3 000 000	07/01/2019	Ethereum Classic	1 100 000
20/11/2017	Tether	31 000 000	14/01/2019	Cryptopia	3 600 000
22/11/2017	Bitcoin Gold	3 955 000	23/02/2019	EOS Cryptocurrency	7 700 000
06/12/2017	NiceHash	68 000 000	25/03/2019	DragonEx	1 000 000
19/12/2017	Youbit	NA	27/03/2019	CoinBene	45 000 000
20/12/2017	EtherDelta	266 789	30/03/2019	Bithumb	21 000 000
13/01/2018	BlackWallet	400 000	16/04/2019	Electrum Bitcoin wallet	4 000 000
19/01/2018	IOTA	4 000 000	29/04/2019	Electrum Bitcoin wallet	600 000
26/01/2018	Coincheck	524 000 000	07/05/2019	Binance	41 000 000
28/01/2018	Experity	150 000	06/06/2019	GateHub	10 000 000
31/01/2018	Bee Token	1 000 000	27/06/2019	Bitrue	4 000 000
10/02/2018	BitGrail	170 000 000	12/07/2019	Bitpoint	32 000 000
04/04/2018	Verge	780 000	05/08/2019	Banks and exchanges	2 000 000 000
12/04/2018	Coinsecure	3 300 000	14/09/2019	EOSPlay	110 000
18/04/2018	Ian Balina	200 000	27/11/2019	Upbit	48 800 000
24/04/2018	MyEtherWallet	152 000			

S&P Commodity-Indexed Trust (GSG), iShares U.S. Financials ETF (IYF), and Technology Select Sector SPDR Fund (XLK). SPDR Gold Shares (GLD) is the chosen commodity.

Regarding the selection of stocks, the focus is restricted to payment system stocks because, intuitively, they are likely to be more affected by news in the cryptocurrency market than other stocks – seeing as the cryptocurrencies also have the ability to serve as a payment vehicle. Moreover, Polasik et al. (2015) find that PayPal, among other transaction vehicles, is a substitute for Bitcoin. The indices were chosen because they are well suited to represent the stock market overall, as well as the financial and technology sectors – which are closely linked to cryptocurrencies. Gold, which is poorly correlated with cryptocurrencies (Borri, 2019), is selected because it is viewed by investors as a safe haven. Therefore, if cyberattacks cause increased uncertainty in the stock market, it could lead to a decrease in the stocks' market value, while the impact on gold price could be the opposite. For consistency, exchange traded funds (ETFs) are utilized to represent indices and gold.

The following subsections explain how the dependent and independent variables are defined. In general, the variables are log-transformed to reduce the impact of potential outliers in the sample. From this point forward, let the opening price, the closing price, the highest traded price and the lowest traded price on day t be denoted by O_t, C_t, H_t and L_t, respectively.

4.1 Return

The daily closing price of Bitcoin is graphed in Figure 1 (a), which shows that the closing price is non-stationary. To make the prices stationary, natural logarithmic returns on day t, r_t, are calculated from daily closing prices as shown in Equation (1).

$$r_t = \ln \frac{C_t}{C_{t-1}} \tag{1}$$

As can be seen in Figure 1 (b), the natural logarithm of return is clearly a stationary process and much more suited for a regression analysis than the closing price. Descriptive statistics for the return are presented in Table 3. All return distributions exhibit high kurtosis and, with the exception of Bitcoin, they are all are positively skewed. During the sample period, most of the cryptocurrencies had positive returns. Further, Bitcoin returns are by far the least volatile, with a

standard deviation of 3.9%. In comparison, returns on the other cryptocurrencies have a standard deviations between 5.7% and 8.8%.

Figure 1: Daily closing prices (a) and daily log returns (b) of Bitcoin.

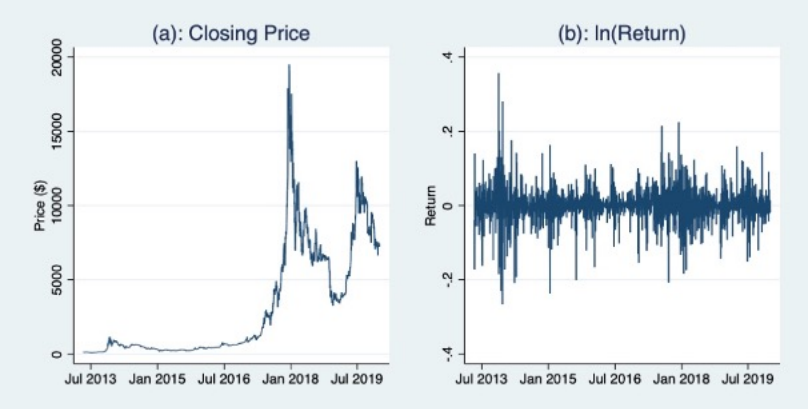

Table 3: Descriptive statistics for the log return.

Ticker	N	Mean	SD	Min	Median	Max	Skew	Kurt
BTC	2136	0.0012	0.039	-0.238	0.0015	0.225	-0.29	8.64
LTC	2136	0.0005	0.057	-0.514	-0.0004	0.510	0.61	15.97
XRP	2136	0.0012	0.067	-0.616	-0.0030	1.027	2.42	42.95
DOGE	2136	0.0003	0.063	-0.493	-0.0022	0.518	0.89	14.27
DASH	2087	0.0020	0.068	-0.427	-0.0023	0.768	1.40	17.23
XMR	1990	0.0014	0.066	-0.325	-0.0010	0.585	0.79	9.94
XLM	1915	0.0015	0.075	-0.366	-0.0034	0.723	2.13	20.48
XEM	1676	0.0031	0.081	-0.362	-0.0002	0.996	2.04	22.47
ETH	1548	0.0034	0.061	-0.316	-0.0006	0.303	0.27	7.05
DCR	1361	0.0017	0.074	-0.342	-0.0020	0.441	1.07	8.13
ETC	1196	0.0011	0.065	-0.435	-0.0013	0.458	0.21	10.21
NEO	1149	0.0034	0.086	-0.461	-0.0022	0.801	1.63	17.44
ZEC	1099	-0.0004	0.062	-0.236	-0.0039	0.528	0.76	9.58
MIOTA	872	-0.0016	0.070	-0.377	-0.0024	0.384	0.30	7.65
EOS	854	0.0008	0.074	-0.385	0.0000	0.347	0.42	7.62
BCH	832	-0.0010	0.072	-0.410	-0.0034	0.432	0.62	10.05
BNB	830	0.0036	0.065	-0.342	0.0000	0.482	0.99	11.40
TRX	780	0.0024	0.088	-0.358	-0.0020	0.787	2.64	24.49
LINK	773	0.0030	0.077	-0.318	-0.0041	0.484	0.76	7.53
ADA	762	-0.0013	0.070	-0.217	-0.0030	0.640	2.15	20.14

4.2 Volatility

Volatility estimators based on high and low prices are more precise than a volatility estimator that is only based on closing prices (Molnár, 2012, 2016; Fiszeder et al., 2019). Therefore, the Garman and Klass (1980) volatility estimator is utilized. Equations (2), (3) and (4) define the daily open-to-high, open-to-low and open-to-close returns, respectively.

$$h_t = \ln H_t - \ln O_t \tag{2}$$

$$l_t = \ln L_t - \ln O_t \tag{3}$$

$$c_t = \ln C_t - \ln O_t \tag{4}$$

Garman and Klass (1980) argue that an estimator that utilizes c, h and l, rather than one that is solely based on the quantity $h - l$, must be more precise. Equation (5) presents the Garman-Klass estimator.

$$\widehat{\sigma}^2_{GK} = 0.5(h_t - l_t)^2 - (2\ln 2 - 1)c_t^2 \tag{5}$$

Moreover, it is common to use logarithmic transformation of the variance when studying cryptocurrencies. The reason is that cryptocurrencies are highly volatile, with extremely high variance on some days, and these days would have too large of an impact on the overall results. Log-transformation of the variance mitigates the impact of these extreme values. Figure 2 compares the Garman-Klass variance (a) with the log-transformed Garman-Klass variance (b). In short, the log-transformed variance is not only less affected by outliers but also more symmetrically

Figure 2: Daily Garman-klass variance (a) and daily log-transformed Garman-Klass variance (b) of Bitcoin.

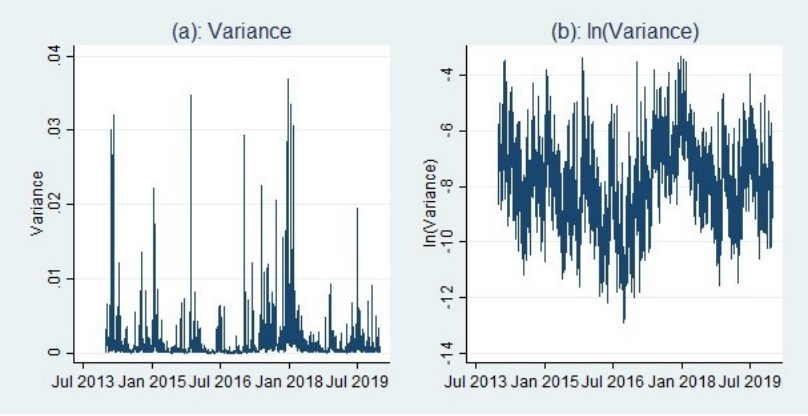

Table 4: Descriptive statistics for the volatility, measured as a logarithm of variance of daily returns estimated from Garman-Klass estimator.

Ticker	N	Mean	SD	Min	Median	Max	Skew	Kurt
BTC	2136	-7.946	1.631	-12.903	-7.884	-3.298	-0.05	2.73
LTC	2136	-7.298	1.658	-13.881	-7.278	-1.662	-0.05	2.85
XRP	2136	-7.468	1.738	-12.147	-7.571	0.000	0.33	3.21
DOGE	2136	-6.658	1.361	-10.608	-6.788	-2.133	0.38	3.04
DASH	2087	-6.498	1.356	-10.630	-6.630	0.224	0.53	3.74
XMR	1990	-6.184	1.233	-10.214	-6.201	1.464	0.16	3.55
XLM	1915	-6.225	1.343	-9.559	-6.331	-0.638	0.46	3.31
XEM	1676	-6.014	1.356	-9.666	-6.066	-1.536	0.22	2.86
ETH	1548	-6.744	1.437	-11.083	-6.773	-2.616	0.15	2.83
DCR	1361	-5.923	1.357	-9.603	-5.913	-1.279	0.13	2.80
ETC	1196	-6.586	1.386	-10.295	-6.618	-2.016	0.18	2.84
NEO	1149	-6.021	1.331	-9.497	-6.091	-1.911	0.21	2.89
ZEC	1099	-6.318	1.226	-9.609	-6.394	-1.403	0.37	3.24
MIOTA	872	-6.213	1.357	-9.751	-6.198	-1.873	0.12	2.81
EOS	854	-6.391	1.402	-10.546	-6.378	-2.299	0.02	2.84
BCH	832	-6.452	1.327	-10.146	-6.489	-1.374	0.24	3.15
BNB	830	-6.509	1.357	-10.053	-6.526	-1.877	0.25	3.10
TRX	780	-6.222	1.459	-9.770	-6.297	-1.393	0.50	3.36
LINK	773	-5.733	1.214	-8.715	-5.813	-2.075	0.18	2.90
ADA	762	-6.365	1.259	-10.312	-6.370	-1.912	0.31	3.40

distributed, and therefore more suitable for regression analysis. The log-transformed Garman-Klass variance is, thus, utilized as a representation for volatility. Descriptive statistics for the volatility are presented in Table 4.

4.3 Trading volume

Figure 3 (a) graphs Bitcoin's reported trading volume. It is evident that the volume has a clear upward trend and must be standardized to make it stationary. The trading volume is standardized by subtracting the natural logarithm of the 30-day median from the natural logarithm of the trading volume on day t. This is shown in Equation (6), where $Volume$ is the reported trading volume and V represents the standardized trading volume. V_t is graphed in Figure 3 (b), illustrating that the reported trading volume has successfully been standardized in a way that makes it stationary. Descriptive statistics for the standardized trading volume are presented in Table 5. The mean is positive for all cryptocurrencies, indicating that the trading

volume has been increasing during the sample period.

$$V_t = \ln Volume_t - \ln median(Volume_{t-30,t-1}) \tag{6}$$

Figure 3: Daily reported trading volume (a) and daily standardized trading volume (b) for Bitcoin.

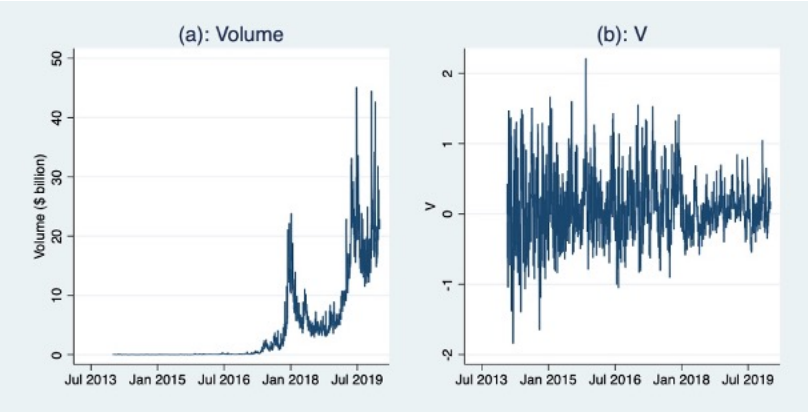

Table 5: Descriptive statistics for the standardized trading volume.

Ticker	N	Mean	SD	Min	Median	Max	Skew	Kurt
BTC	2136	0.079	0.442	-1.842	0.020	2.215	0.54	4.36
LTC	2136	0.089	0.621	-1.834	0.016	3.569	1.13	6.22
XRP	2136	0.091	0.775	-3.048	0.013	4.222	0.71	5.36
DOGE	2136	0.072	0.741	-1.767	-0.024	3.795	1.16	5.47
DASH	2087	0.105	0.620	-1.793	0.026	3.752	1.20	6.55
XMR	1990	0.093	0.710	-1.966	0.001	5.074	1.63	9.73
XLM	1915	0.117	0.902	-2.268	-0.007	5.140	1.28	6.66
XEM	1676	0.090	0.865	-2.953	0.015	4.656	0.84	5.63
ETH	1548	0.130	0.586	-1.561	0.050	2.980	0.98	5.39
DCR	1361	0.131	0.785	-1.652	-0.011	3.816	1.56	6.68
ETC	1196	0.109	0.663	-1.854	0.020	3.161	0.84	5.02
NEO	1149	0.139	0.757	-3.205	0.042	3.703	0.61	6.70
ZEC	1099	0.110	0.471	-1.037	0.026	3.009	1.30	6.43
MIOTA	872	0.029	0.630	-1.493	-0.096	3.299	1.32	5.97
EOS	854	0.104	0.542	-1.378	0.013	2.540	0.98	5.07
BCH	832	0.079	0.605	-1.930	-0.025	2.839	1.05	6.00
BNB	830	0.075	0.617	-9.340	0.015	2.359	-3.85	67.87
TRX	780	0.178	0.667	-1.346	0.068	3.970	2.29	11.64
LINK	773	0.096	0.721	-2.294	0.032	3.257	0.46	4.60
ADA	762	0.058	0.663	-1.281	-0.056	3.085	1.00	4.58

When analyzing traditional assets, who are only traded five days a week, the median

in Equation (6) is calculated over the past 22 trading days instead of the past 30 calendar days to properly account for the number of trading days.

4.4 Loss magnitude

To capture the effect cybercrime has on the dependent variables, a continuous variable for the estimated loss is included as an explanatory variable. A reported estimated loss of NA is counted as 1. It is natural to assume that, due to the cryptocurrency market's rapidly growing market capitalization, a loss of $1 million today would have a smaller impact than a loss of $1 million in, say, 2014. Therefore, the estimated loss is transformed into a loss magnitude LM_t, with the market capitalization of Bitcoin on the day of the attack as a reference point. The loss magnitude is expressed in Equation (7). $LM_t = 0$ on days where no cyberattacks are observed. Descriptive statistics for the loss magnitude are presented in Table 6.

$$LM_t = \frac{EstimatedLoss_t}{MarketCapitalization_t^{BTC}} \tag{7}$$

Table 6: Descriptive statistics for the loss magnitude. The statistics are multiplied by 1000 to reduce the number of decimal points.

	N	Mean	SD	Min	Median	Max	Skew	Kurt
LM	77	0.450	1.468	0.000	0.025	9.485	4.84	26.97

4.5 Lagged dependent variable

Lagged values of the dependent variables are included as regressors to account for the presence of autocorrelation. Let Y_t denote the dependent variables (r, σ^2 and V). For each of these variables, weekly and monthly averages of lagged observations are calculated according to Equation (8) and (9), respectively.

$$Y_w = \frac{\sum_{k=1}^{7}(Y_{t-k})}{7} \tag{8}$$

$$Y_m = \frac{\sum_{k=1}^{30}(Y_{t-k})}{30} \tag{9}$$

Throughout this paper the weekly averages are denoted by r_w, σ_w^2 and V_w, while the monthly averages are denoted by r_m, σ_m^2 and V_m. Because V_m uses the past 30 values of the standardized trading volume (which is calculated using the median of the past 30 values of the reported trading volume) the first observation that can be used in the

regressions occurs 60 calendar days after the first observation in the trading history. When analyzing traditional financial assets, the denominators in Equation (8) and (9) should be 5 and 22, respectively, to properly account for the number of trading days. The first data point thus occurs 44 trading days after the first observation.

Table 7 presents an overview of the correlation between the main variables, namely returns, volatility, standardized trading volume (volume) and the loss magnitude (attacks). The correlation matrix is calculated as the average of the cryptocurrencies' correlation matrices. The correlation coefficients between LM and the dependent variables show that the return is negatively correlated with the loss magnitude, while the variance and the trading volume are positively correlated with the loss magnitude.

Table 7: Correlation matrix, calculated as the average of the cryptocurrencies' correlation matrices.

	Return	**Volatility**	**Volume**	**Attacks**
Return	1	0.082	0.246	-0.006
Volatility	0.082	1	0.483	0.016
Volume	0.246	0.483	1	0.004
Attacks	-0.006	0.016	0.004	1

5 Methodology

This section describes the statistical procedures utilized to answer our research questions. Challenges – and appropriate adjustments – related to the data characteristics are also explained. Depending on the asset in question, this thesis utilizes either panel data regressions or time series regressions to study how cyberattacks linked to the cryptocurrency market influence the returns, volatility and trading volume. Two model specifications are estimated for each dependent variable. Our primary objective is to study the impact of cyberattacks, and so the loss magnitude is included in both specifications.

In the first specification, lags of the dependent variable are included as explanatory variables to account for autocorrelation. Instead of including many lags, we follow the HAR structure (Corsi, 2009) and include the one-day lag, as well as weekly and monthly averages of the one-day lag. The HAR-RV model is able to successfully model the long-memory behavior of volatility by including simple averages of daily

observations. In fact, the model outperforms the short-memory models (one day, one week, and two weeks) and is comparable to the much more complicated long-memory ARIFMA model (Corsi, 2009). Additionally, other control variables are included because we suspect that the returns, volatility and trading volume might be influencing each other. Equation (10), (11) and (12) express this specification for the return, the variance and the trading volume, respectively, where ϵ_t is the error term at time t.

$$\begin{aligned} r_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_w + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \epsilon_t \end{aligned} \tag{10}$$

$$\begin{aligned} \sigma^2_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_w + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \epsilon_t \end{aligned} \tag{11}$$

$$\begin{aligned} V_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_{,w} + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \epsilon_t \end{aligned} \tag{12}$$

The second specification introduces an interaction term between LM_t and a time variable *time* to account for a potential time trend in the impact of the loss magnitude on the dependent variables. *time* is a linear time index that takes the value of 1 for observations made on December 27, 2013, and 2196 for observations made on December 31, 2019. Equation (13), (14) and (15) express this specification for the return, the variance and the trading volume, respectively.

$$\begin{aligned} r_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_w + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \beta_{11} LM_t \cdot time_t + \epsilon_t \end{aligned} \tag{13}$$

$$\begin{aligned} \sigma^2_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_w + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \beta_{11} LM_t \cdot time_t + \epsilon_t \end{aligned} \tag{14}$$

$$\begin{aligned} V_t =& \beta_0 + \beta_1 r_{t-1} + \beta_2 r_w + \beta_3 r_m + \beta_4 \sigma^2_{t-1} + \beta_5 \sigma^2_w + \beta_6 \sigma^2_m \\ &+ \beta_7 V_{t-1} + \beta_8 V_w + \beta_9 V_m + \beta_{10} LM_t + \beta_{11} LM_t \cdot time_t + \epsilon_t \end{aligned} \tag{15}$$

5.1 Investigation of cryptocurrencies

To investigate the impact cyberattacks have on cryptocurrencies, the six models presented above are employed in unbalanced panel data regressions. A robustness check reveals the presence of heteroskedasticity in the panels. Although the OLS estimator remains unbiased, heteroskedasticity may cause the standard errors to be inaccurately estimated. Thus, hypothesis tests and confidence intervals are not

reliable, seeing as the standard errors are used to derive the t-statistics and the upper and lower bounds of a confidence interval. The issues related to the presence of heteroskedasticity are solved by implementing Driscoll-Kraay (Driscoll and Kraay, 1998) standard errors.

We also test for the presence of cross-sectional dependence by applying the Pesaran CD test (Pesaran, 2006), which allows us to test the null hypothesis of cross-sectional independence. The null hypothesis is strongly rejected in all models and, conclusively, the panel exhibits cross-sectional dependence. Hoechle (2007), who states that "erroneously ignoring cross-sectional correlation in the estimation of panel models can lead to severely biased statistical results", finds Driscoll-Kraay standard errors to be well calibrated and robust to very general forms of cross-sectional dependence. This means that there is no need for further adjustments to the model as these standard errors are already used to account for heteroskedasticity. A possible drawback with this test is that, in cases where positive and negative correlations are added together, the null hypothesis may not be rejected even though there is indeed CD in the errors. In our case, however, the average absolute correlation is very high which further strengthens the validity of the test (De Hoyos and Sarafidis, 2006).

When it comes to deciding between fixed or random effects, the fixed effects specification is more suitable because it assumes that the variation across entities is correlated with the predictors and allows us to analyze how variables that vary across time affect the dependent variables (Torres-Reyna, 2007).

5.2 Investigation of traditional financial assets

To investigate how the returns, volatility, and trading volume of payment system stocks are affected by cryptocurrency-related cyberattacks, unbalanced panel data regressions are employed on the six models in Equation (10) - (15). The robustness check and panel data testing that was explained in the previous sub-section is also performed on the payment system panel data, revealing the presence of heteroskedasticity, autocorrelation and cross-sectional dependence. This is identical to what we found for the cryptocurrency sample and, therefore, the same adjustments are implemented. This involves running a fixed effects model that uses Driscoll-Kraay standard errors and includes lags of the dependent variable as explanatory variables (again, following the HAR-RV model).

When studying how the indices are affected by cryptocurrency-related cyberattacks, panel data regression is not applicable because we wish to investigate the impact on each sector individually, rather than the average impact on the market. This is also the case for gold. For these assets, time series regressions are employed on the six models in Equation (10) - (15). The time series regressions are estimated with robust standard errors to account for heteroskedasticity.

6 Results

This section presents our findings on how cyberattacks related to the cryptocurrency market influence the return, volatility and trading volume of cryptocurrencies and traditional financial assets. As described in section 5, we run two model specifications on each of the dependent variables, both of which include the loss magnitude (LM_t) to capture the effect of cyberattacks. The first specification includes control variables that account for autocorrelation and correlation between the dependent variables, while the second specification introduces an interaction term between LM_t and a linear time index to account for a potential time trend in the impact of LM_t.

We first perform panel data regressions on the cryptocurrency data to estimate the average effect of cyberattacks. Then, to investigate whether the impact of LM_t is unique for cryptocurrencies, we run panel data regressions on payment system stocks and time series regressions on stock indices and gold. Finally, we conduct a closer investigation of each individual cryptocurrency and payment system stock to shed light on entity-specific relationships.

Note that the number of observations in the regressions are not equivalent to the number of days in the sample period (December 27, 2013 - December 31, 2019). Recalling from Section 4, the first data point utilized in the regressions, for the cryptocurrencies, occurs on February 25, 2014 because 60 lagged values of the trading volume are needed to calculate the monthly average of the standardized trading volume (V_m). For the traditional financial assets, after adjusting the variables to the number of trading days in a month, the first data point utilized in the regressions occurs on March 4, 2014 because 44 lagged values of the trading volume are needed to calculate V_m.

6.1 Return

6.1.1 Investigation of cryptocurrencies

Evident from Table 8, the first specification finds no evidence of a significant relationship between LM_t and the return. In the second specification, which decomposes LM_t into a constant component and a time-varying component, both LM_t and $LM_t \cdot time$ are statistically significant at the 0.01 level. The standardized coefficient of LM_t is negative, suggesting that the loss magnitude and, thus, cyberattacks related to the cryptocurrency market have a negative impact on daily returns. The interaction term is estimated to be a very small number of the opposite sign from the coefficient of LM_t, indicating that the impact of LM_t is decreasing over time. More specifically, an average cyberattack (see descriptive statistics for the loss magnitude in Table 6) is estimated to decrease the return by $0.00045 \cdot (-29.286 + 0.016 \cdot time) = -1.32\% + 0.0007\% \cdot time$.

The decreasing time trend may indicate that some of the younger cryptocurrencies are less affected by cybercrime in the cryptocurrency market, or simply that a cyberattack today has a smaller impact because the faith in the cryptocurrency market has grown stronger and, subsequently, made the market more robust to cyberattack events. The former is investigated in Section 6.4.

We do not find evidence of autocorrelation, meaning that cryptocurrency returns are independent of previous returns. As for the other control variables, both specifications estimate V_{t-1} and V_m to be statistically significant, providing evidence that the trading volume has predictive abilities on the return. The volatility, on the other hand, does not exhibit statistically significant predictive abilities on the return.

6.1.2 Investigation of traditional financial assets

Table 8 shows that cyberattacks related to the cryptocurrency market have a negative effect on daily returns on payment system stocks. This relationship was also found for cryptocurrencies. However, when decomposing LM_t into a constant component and a time-varying component, we find that the impact of LM_t becomes more negative over time. A possible explanation for this observation could be that cryptocurrencies are becoming more and more incorporated in the world economy over time, and that cyberattacks on cryptocurrencies therefore have a stronger impact on traditional financial markets today than they had in the past.

For the indices, we find that the relationship between cryptocurrency-related

Table 8: The impact of cyberattacks on the return of cryptocurrencies and traditional financial assets.

	Cryptocurrencies		**Payment systems**		**S&P500**		**Commodities**		**Financials**		**Technology**		**Gold**	
r_{t-1}	-0.025	-0.025	-0.010	-0.011	0.004	0.004	-0.078**	-0.077**	0.003	0.002	-0.027	-0.028	-0.064**	-0.064**
	(0.018)	(0.018)	(0.025)	(0.025)	(0.042)	(0.042)	(0.035)	(0.035)	(0.041)	(0.041)	(0.042)	(0.042)	(0.032)	(0.032)
r_w	0.074	0.073	-0.149**	-0.149**	-0.163	-0.163	0.055	0.056	-0.176*	-0.176	-0.239*	-0.240*	0.119	0.118
	(0.053)	(0.053)	(0.062)	(0.062)	(0.133)	(0.133)	(0.092)	(0.092)	(0.107)	(0.107)	(0.132)	(0.132)	(0.082)	(0.083)
r_m	-0.012	-0.010	-0.117	-0.116	-0.120	-0.126	0.080	0.083	0.123	0.121	0.055	0.058	-0.197	-0.197
	(0.130)	(0.130)	(0.116)	(0.116)	(0.311)	(0.311)	(0.151)	(0.151)	(0.207)	(0.207)	(0.270)	(0.270)	(0.159)	(0.159)
σ_{t-1}	0.001	0.001	-0.001**	-0.001**	-0.001	-0.001	-0.001	-0.001	-0.000	-0.000	-0.001**	-0.001**	0.001**	0.001**
	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
σ_w	0.000	0.000	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.002	0.002	-0.001	-0.001
	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
σ_m	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	0.000
	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
V_{t-1}	0.005***	0.005***	0.001	0.001	0.000	0.000	-0.000	-0.000	-0.000	-0.000	-0.001	-0.001	-0.001	-0.001
	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)	(0.001)	(0.001)
V_w	-0.003	-0.003	-0.001	-0.001	-0.001	-0.001	0.000	0.000	-0.001	-0.001	-0.002	-0.002	0.001	0.001
	(0.003)	(0.003)	(0.002)	(0.002)	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)	(0.001)	(0.001)
V_m	0.007***	0.007***	0.001	0.001	-0.000	-0.000	-0.004**	-0.004***	0.001	0.001	0.001	0.001	0.001	0.001
	(0.003)	(0.003)	(0.002)	(0.002)	(0.003)	(0.003)	(0.001)	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)
LM_t	-1.634	-29.286***	-2.518**	0.608	-2.137***	-0.406	-0.128	2.101	-2.255***	-0.418	-2.861**	0.431	1.425***	1.978*
	(4.545)	(3.946)	(1.050)	(1.309)	(0.805)	(1.467)	(0.973)	(3.325)	(0.732)	(1.342)	(1.196)	(1.668)	(0.222)	(1.059)
$LM_t \cdot time$		0.016***		-0.003**		-0.002		-0.002		-0.002		-0.003**		-0.001
		(0.002)		(0.001)		(0.001)		(0.003)		(0.001)		(0.001)		(0.001)
Constant	0.011	0.011	0.003	0.003	0.002	0.002	-0.001	-0.001	0.006	0.006	0.002	0.002	0.000	0.000
	(0.009)	(0.009)	(0.006)	(0.006)	(0.004)	(0.004)	(0.005)	(0.005)	(0.005)	(0.005)	(0.006)	(0.006)	(0.005)	(0.005)
N	28,268	28,268	6,964	6,964	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469
Groups	20	20	5	5										
Within R^2	0.008	0.009	0.011	0.012										
Adj. R^2					0.007	0.007	0.006	0.006	0.007	0.007	0.014	0.015	0.005	0.005
Method	Panel data regression with fixed effects and Driscoll-Kraay standard errors				Time series regression with robust standard errors									

The table presents panel data regression results (for cryptocurrencies and payment systems) and time series regression results (for the stock indices and gold) over the period February 25, 2014 - December 31, 2019. We analyze how log returns are affected by the loss magnitude (LM_t), while controlling for autocorrelation (r_{t-1}, r_w, r_m) and other control variables (σ_{t-1}, σ_w, σ_m, V_{t-1}, V_w, V_m). We also decompose the impact of LM_t into a constant component and a time-varying component by including the interaction term $LM_t \cdot time$, where $time$ is a linear time index. Standard errors are in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

cyberattacks and returns on the technology index is in accordance with the results from the panel regressions on payment system stocks. The returns on S&P500 and the financial index are also estimated to decrease on the day of an attack. However, decomposing LM_t into a constant and a time-varying component does not improve the model, suggesting that the impact of LM_t does not exhibit a time trend for these indices. Moreover, the results reveal a significantly positive relationship between cyberattacks and daily returns on gold, which is in line with the contemplation that gold is a safe haven. The impact of LM_t on daily returns on gold does not appear to change over time.

6.2 Volatility

6.2.1 Investigation of cryptocurrencies

As can be seen in Table 9, we experience more consistent results across the two specifications for the volatility, both of which estimating the coefficient of LM_t to be positive and statistically significant at the 0.01 level. In other words, both specifications provide evidence that the volatility of cryptocurrencies increases on the day of a cyberattack. In the second specification, the interaction term is significant at the 0.01 level and is estimated to be a very small, negative number (i.e. it has the opposite sign from the coefficient of LM_t). Hence, when decomposing LM_t into a constant component and a time-varying component, we find that cyberattacks increase the volatility of cryptocurrencies, but this effect is weaker now than it was in the past. An average cyberattack (see descriptive statistics for the loss magnitude in Table 6) is estimated to increase the volatility by $0.00045 \cdot (535.972 - 0.231 \cdot time) = 24.12\% - 0.0104\% \cdot time$.

The results indicate that including the interaction term only slightly improves the model's ability to account for variance between the panel entities. Moreover, both specifications provide evidence of positive autocorrelation in cryptocurrency volatility as the coefficients of σ^2, σ_w^2 and σ_m^2 are all positive and statistically significant at the 0.01 level. For the other control variables, the coefficients and their standard errors are almost identical across the two specifications. All control variables, except for r_{t-1}, have a statistically significant impact on volatility, suggesting that previous returns and trading volume are able to predict volatility.

Table 9: The impact of cyberattacks on the volatility of cryptocurrencies and traditional financial assets.

	Cryptocurrencies		**Payment systems**		**S&P500**		**Commodities**		**Financials**		**Technology**		**Gold**	
r_{t-1}	-0.110	-0.109	-2.318**	-2.299**	-12.769***	-12.746***	-4.081*	-4.158**	-9.515***	-9.510***	-11.062***	-11.106***	1.777	1.753
	(0.244)	(0.244)	(1.131)	(1.132)	(3.060)	(3.061)	(2.097)	(2.101)	(2.534)	(2.534)	(2.306)	(2.309)	(2.857)	(2.859)
r_w	-1.611**	-1.589**	-9.778***	-9.817***	-47.025***	-47.066***	-4.903	-4.929	-33.458***	-33.517***	-29.545***	-29.578***	1.170	1.275
	(0.669)	(0.670)	(3.095)	(3.099)	(7.918)	(7.923)	(4.991)	(4.991)	(6.652)	(6.651)	(6.414)	(6.416)	(7.711)	(7.715)
r_m	4.223***	4.197***	-15.061**	-15.106**	-69.011***	-68.675***	-29.485***	-29.712***	-35.497**	-35.202**	-32.951**	-32.848**	26.796*	26.814*
	(1.318)	(1.320)	(6.444)	(6.459)	(23.407)	(23.424)	(9.176)	(9.169)	(16.382)	(16.389)	(16.499)	(16.504)	(15.456)	(15.462)
σ_{t-1}	0.288***	0.288***	0.116***	0.116***	0.169***	0.170***	0.025	0.026	0.167***	0.167***	0.105***	0.105***	0.062	0.063*
	(0.017)	(0.017)	(0.020)	(0.020)	(0.041)	(0.041)	(0.031)	(0.031)	(0.034)	(0.034)	(0.035)	(0.035)	(0.038)	(0.038)
σ_w	0.350***	0.349***	0.236***	0.236***	0.368***	0.368***	0.311***	0.309***	0.210***	0.210***	0.259***	0.261***	0.049	0.049
	(0.034)	(0.034)	(0.044)	(0.044)	(0.082)	(0.082)	(0.071)	(0.071)	(0.062)	(0.062)	(0.071)	(0.071)	(0.089)	(0.089)
σ_m	0.249***	0.250***	0.450***	0.451***	0.267***	0.266***	0.528***	0.531***	0.411***	0.412***	0.440***	0.439***	0.720***	0.720***
	(0.039)	(0.039)	(0.050)	(0.051)	(0.079)	(0.079)	(0.069)	(0.069)	(0.064)	(0.064)	(0.074)	(0.074)	(0.092)	(0.092)
V_{t-1}	0.345***	0.343***	0.420***	0.419***	0.093	0.091	0.030	0.031	0.072*	0.072*	0.222***	0.224***	0.014	0.013
	(0.027)	(0.027)	(0.045)	(0.045)	(0.120)	(0.120)	(0.029)	(0.029)	(0.038)	(0.038)	(0.075)	(0.075)	(0.081)	(0.081)
V_w	-0.185***	-0.183***	-0.101	-0.102	-0.161	-0.163	0.029	0.028	0.073	0.071	0.122	0.121	0.315**	0.312**
	(0.037)	(0.037)	(0.075)	(0.075)	(0.196)	(0.197)	(0.053)	(0.053)	(0.069)	(0.069)	(0.137)	(0.137)	(0.152)	(0.152)
V_m	-0.091**	-0.091**	-0.286**	-0.288**	-0.330	-0.327	-0.024	-0.021	-0.070	-0.071	-0.261	-0.261	-0.206	-0.207
	(0.042)	(0.042)	(0.121)	(0.122)	(0.219)	(0.219)	(0.089)	(0.089)	(0.099)	(0.099)	(0.170)	(0.170)	(0.192)	(0.192)
LM_t	144.735**	535.972***	49.774	-104.453***	95.887***	-1.191	78.280**	-92.180	141.885***	-94.599	96.991***	196.434***	-4.833	-148.256
	(69.661)	(41.406)	(36.602)	(32.663)	(34.727)	(122.404)	(38.517)	(150.438)	(53.715)	(116.119)	(30.345)	(58.135)	(53.693)	(109.478)
$LM_t \cdot time$		-0.231***		0.147***		0.093		0.162		0.225***		-0.095**		0.137
		(0.023)		(0.028)		(0.089)		(0.112)		(0.084)		(0.044)		(0.085)
Constant	-0.764***	-0.765***	-1.839***	-1.839***	-2.057***	-2.054***	-1.373***	-1.363***	-2.210***	-2.197***	-1.959***	-1.955***	-1.860***	-1.855***
	(0.134)	(0.135)	(0.283)	(0.283)	(0.345)	(0.345)	(0.322)	(0.322)	(0.414)	(0.414)	(0.366)	(0.366)	(0.533)	(0.533)
N	28,268	28,268	6,964	6,964	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469
Groups	20	20	5	5										
Within R^2	0.480	0.481	0.295	0.296										
Adj. R^2					0.496	0.495	0.366	0.366	0.39	0.39	0.437	0.437	0.191	0.191
Method	Panel data regression with fixed effects and Driscoll-Kraay standard errors				Time series regression with robust standard errors									

The table presents panel data regression results (for cryptocurrencies and payment systems) and time series regression results (for the stock indices and gold) over the period February 25, 2014 - December 31, 2019. We analyze how the volatility (log-transformed Garman-Klass variance) is affected by the loss magnitude (LM_t), while controlling for autocorrelation (σ_{t-1}, σ_w, σ_m) and other control variables (r_{t-1}, r_w, r_m, V_{t-1}, V_w, V_m). We also decompose the impact of LM_t into a constant component and a time-varying component by including the interaction term $LM_t \cdot time$, where t is a linear time index. Standard errors are in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

6.2.2 Investigation of traditional financial assets

The results reported in Table 9 indicate that cyberattacks decrease the volatility of the payment systems. This effect is only statistically significant when decomposing LM_t into a constant component and a time-varying component. Further, the coefficient of $LM_t \cdot time$ has the opposite sign from the coefficient of LM_t. This is consistent with the decreasing time trend that was observed in the cryptocurrency data, although the impact is becoming less negative rather than less positive. Conclusively, the negative impact of cryptocurrency-related cyberattacks on payment system stocks have decreased over time. The results indicate that the impact of cyberattacks on the volatility of payment system stocks is positive in the second half of the sample.

The indices, on the other hand, are estimated to become more volatile on the day of a cyberattack. We find that the impact of cyberattacks on the volatility of technology stocks is decreasing over time. The positive impact of a cyberattack on the volatility of the financial index, however, is increasing over time. For S&P500 and the commodity index, decomposing LM_t into a constant component and a time-varying component does not improve the model. The volatility of gold is unaffected by cyberattacks.

6.3 Trading volume

6.3.1 Investigation of cryptocurrencies

The estimated impact of cyberattacks on the trading volume is presented in Table 10. The first specification provides evidence of a positive relationship between cyberattacks and the trading volume of cryptocurrencies. When decomposing LM_t into a constant component and a time-varying component in the second specification, the coefficients of LM_t and $LM_t \cdot time$ are both statistically significant at the 0.01 level. Thus, we find that the positive impact of LM_t on the trading volume is decreasing over time, seeing as the constant component of LM_t is positive while the time-varying component of LM_t is negative. More specifically, an average cyberattack (see descriptive statistics for the loss magnitude in Table 6) is estimated to increase the trading volume by $0.00045 \cdot (190.796 - 0.083 \cdot time) = 8.59\% - 0.0037\% \cdot time$.

Both specifications estimate the volume variables to be (highly) statistically significant and, thus, provide evidence of serial correlation in the trading volume. Moreover, the results provide evidence that both returns and volatility are able to

Table 10: The impact of cyberattacks on the trading volume of cryptocurrencies and traditional financial assets.

	Cryptocurrencies		Payment systems		S&P500		Commodities		Financials		Technology		Gold	
r_{t-1}	0.676***	0.677***	-0.424	-0.421	-3.586***	-3.565***	0.435	0.441	-2.753	-2.752	-3.389***	-3.372***	1.998	1.985
	(0.100)	(0.100)	(0.430)	(0.430)	(1.049)	(1.050)	(1.903)	(1.905)	(2.002)	(2.003)	(0.975)	(0.976)	(1.294)	(1.295)
r_w	1.660***	1.668***	-2.037*	-2.043*	-9.137***	-9.173***	-4.085	-4.083	-4.400	-4.414	-7.899***	-7.885***	2.043	2.103
	(0.223)	(0.223)	(1.198)	(1.198)	(2.987)	(2.990)	(5.381)	(5.383)	(5.517)	(5.519)	(2.930)	(2.932)	(3.585)	(3.587)
r_m	1.909***	1.900***	-6.428**	-6.436**	-19.607**	-19.313**	-14.058	-14.039	-20.786*	-20.713*	0.053	0.011	22.280***	22.290***
	(0.469)	(0.469)	(2.627)	(2.629)	(8.261)	(8.267)	(9.718)	(9.725)	(12.362)	(12.368)	(7.309)	(7.311)	(6.863)	(6.866)
σ_{t-1}	-0.023***	-0.022***	0.017*	0.017*	0.054***	0.055***	-0.005	-0.005	0.016	0.016	0.045***	0.046***	0.001	0.001
	(0.007)	(0.007)	(0.009)	(0.009)	(0.015)	(0.015)	(0.029)	(0.029)	(0.029)	(0.029)	(0.016)	(0.016)	(0.017)	(0.018)
σ_w	-0.025**	-0.026**	-0.021	-0.021	-0.008	-0.008	-0.076	-0.076	0.084	0.084	0.056*	0.056*	-0.060	-0.060
	(0.010)	(0.010)	(0.016)	(0.016)	(0.029)	(0.029)	(0.073)	(0.073)	(0.055)	(0.055)	(0.033)	(0.033)	(0.040)	(0.040)
σ_m	0.019*	0.020*	-0.043**	-0.043**	-0.107***	-0.108***	0.001	0.001	-0.191***	-0.191***	-0.163***	-0.163***	-0.007	-0.008
	(0.010)	(0.010)	(0.017)	(0.017)	(0.028)	(0.028)	(0.076)	(0.076)	(0.052)	(0.052)	(0.034)	(0.034)	(0.045)	(0.045)
V_{t-1}	0.577***	0.576***	0.425***	0.424***	0.221***	0.219***	0.232***	0.232***	0.192***	0.192***	0.235***	0.235***	0.214***	0.214***
	(0.021)	(0.021)	(0.023)	(0.023)	(0.041)	(0.041)	(0.037)	(0.037)	(0.033)	(0.033)	(0.037)	(0.037)	(0.038)	(0.038)
V_w	0.265***	0.266***	0.185***	0.185***	0.275***	0.274***	0.270***	0.270***	0.258***	0.257***	0.224***	0.225***	0.309***	0.308***
	(0.021)	(0.021)	(0.030)	(0.030)	(0.071)	(0.071)	(0.059)	(0.059)	(0.062)	(0.062)	(0.063)	(0.063)	(0.069)	(0.069)
V_m	-0.126***	-0.126***	-0.304***	-0.305***	-0.277***	-0.275***	-0.197**	-0.197**	-0.163*	-0.164*	-0.253***	-0.253***	-0.221**	-0.221**
	(0.016)	(0.016)	(0.044)	(0.044)	(0.076)	(0.076)	(0.089)	(0.089)	(0.084)	(0.084)	(0.073)	(0.073)	(0.089)	(0.089)
LM_t	50.157**	190.796***	35.134*	10.918	50.480**	-34.067	-33.376*	-19.410	17.872	-40.527	35.707***	-4.099	0.061	-81.710*
	(21.877)	(25.653)	(18.475)	(59.842)	(22.424)	(35.055)	(17.251)	(71.146)	(34.563)	(122.464)	(13.759)	(27.453)	(29.157)	(41.825)
$LM_t \cdot time$		-0.083***		0.023		0.081***		-0.013		0.056		0.038*		0.078**
		(0.012)		(0.044)		(0.028)		(0.055)		(0.089)		(0.022)		(0.037)
Constant	-0.167***	-0.167***	-0.421***	-0.421***	-0.635***	-0.632***	-0.715*	-0.716*	-0.894**	-0.890**	-0.612***	-0.614***	-0.725***	-0.722***
	(0.037)	(0.037)	(0.100)	(0.100)	(0.124)	(0.124)	(0.370)	(0.370)	(0.347)	(0.347)	(0.161)	(0.161)	(0.247)	(0.247)
N	28,268	28,268	6,964	6,964	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469	1,469
Groups	20	20	5	5										
Within R^2	0.591	0.591	0.286	0.287										
Adj. R^2					0.353	0.353	0.114	0.114	0.138	0.137	0.307	0.307	0.124	0.124
Method	Panel data regression with fixed effects and Driscoll-Kraay standard errors				Time series regression with robust standard errors									

The table presents panel data regression results (for cryptocurrencies and payment systems) and time series regression results (for the stock indices and gold) over the period February 25, 2014 - December 31, 2019. We analyze how the standardized trading volume is affected by the loss magnitude (LM_t), while controlling for autocorrelation (V_{t-1}, V_w, V_m) and other control variables (r_{t-1}, r_w, r_m, σ_{t-1}, σ_w, σ_m). We also decompose the impact of LM_t into a constant component and a time-varying component by including the interaction term $LM_t \cdot time$, where t is a linear time index. Standard errors are in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

predict the trading volume. The return evidently has a positive effect on the trading volume, while the volatility, on average, is estimated to have a negative impact on the trading volume.

6.3.2 Investigation of traditional financial assets

Table 10 shows that cyberattacks are estimated to have a statistically significant impact on the trading volume for the payment systems only when the interaction term is omitted. Hence, decomposing the impact of LM_t into a constant component and a time-varying component does not improve the model. This suggests that LM_t does not exhibit a time trend in the payment system dataset. Conclusively, we find that cyberattacks have a positive impact on the trading volume and that the impact does not seem to change over time.

As for the indices, our findings indicate that the impact of cyberattacks on the volume of S&P500 and the technology index is positive and increasing over time. For the commodity index, we find that the impact of LM_t is negative and constant over time, while the financial index is not estimated to be affected by cyberattacks on cryptocurrencies. For gold, the results show that the trading volume decreases on the day of a cyberattack, and that the impact of LM_t is becoming less negative over time. In fact, the impact on gold's trading volume is estimated to be positive in the second half of the sample.

6.4 Closer investigation of cryptocurrencies

A closer investigation of the cryptocurrencies is conducted by employing time series regressions on each cryptocurrency to determine whether the average effect of the cyberattacks is caused by a strong effect in only one (or a few) of the cryptocurrencies, or whether cyberattacks have similar impact on most cryptocurrencies. The results are presented in Appendix A.

6.4.1 Return

The overall results from the time series regressions, provided in Table A.1 to A.4, coincide with the panel regression results. Moreover, the results report that both LM_t and $LM_t \cdot time$ are predominantly statistically significant among the ten cryptocurrencies with the longest trading history (Table A.1 and A.2) after decomposing LM_t into a constant and a time-varying part. However, for the ten cryptocurrencies with the shortest trading history (Table A.3 and A.4),

decomposing the impact of the loss magnitude into a constant component and a time-varying component generally does not improve the model. Additionally, among the ten youngest cryptocurrencies (with the exception of LINK) we can see that their returns are either positively affected or not affected by cyberattacks. This can explain why the negative impact that was found in the panel data analysis is decreasing over time. Conclusively, these observations indicate that the impact of cyberattacks on a given cryptocurrency depends on its maturity, and that there is evidence of a time trend.

Time series regressions show no evidence of autocorrelation, except for in the case of DCR and ETC. The relationship between volatility and returns also remains insignificant in the time series regressions. However, the time series regressions generally do not provide evidence that the trading volume is able to predict the return.

6.4.2 Volatility

Time series regressions on the cryptocurrencies, presented in Table A.5 to A.8, reveal that the findings from the panel data regressions are mostly present only among the ten cryptocurrencies with the longest trading history (Table A.5 and A.6). For the ten cryptocurrencies with the shortest trading history (Table A.7 and A.8), however, decomposing the impact of LM_t into a constant and a time-varying part does not seem to improve the model. Only the regression on TRX provides evidence of the same relationship that we found in the panel data regression. With that, the results provide evidence of a time trend and variability across panel entities.

The variables that control for autocorrelation remain unchanged in terms of significance in the time series regressions. The impact of the returns on the volatility is not very consistent across the cryptocurrencies. Most of the cryptocurrencies are only affected by either one of r_{t-1}, r_w or r_m, and we do not see a clear pattern in relation to the cryptocurrencies' maturity. Moreover, the significant impact that V_w and V_m evidently have on volatility in the panel regression seems to be caused by a strong relationship in only a few of the cryptocurrencies.

6.4.3 Trading volume

The time series regressions, presented in Table A.9 to A.12, reveal that the findings from the panel data regressions are generally only present among the ten oldest cryptocurrencies (Table A.9 and A.10). This is probably a contributing factor to the

decreasing time trend in the impact of cyberattacks.

The time series regressions coincide with the panel data regressions in that evidence of autocorrelation is present in most of the cryptocurrencies. The impact of the control variables on the trading volume is, on average, also present, although there are some differences across cryptocurrencies. More specifically, the coefficients of r_m, σ_w^2, σ_m^2 and V_m are generally only statistically significant among the ten oldest cryptocurrencies.

6.5 Closer investigation of payment system stocks

Seeing as the initial analyses of payment system stocks brought very interesting findings, a closer investigation of the payment system stocks is conducted by employing time series regressions on each stock. The objective is to study how individual effects in each of the stocks compare to the pooled effects that was estimated in the panel data analyses. The results are presented in Appendix B.

6.5.1 Return

Results from employing time series regressions on the return specifications for each payment system stock individually are presented in Table B.1. These findings mostly coincide with the panel regression results, i.e. cyberattacks influence returns on payment systems negatively and the impact is becoming more negative over time. We do, however, not find evidence of a time trend in the case of American Express and Western Union.

6.5.2 Volatility

Results from employing time series regressions on the volatility specifications for each payment system stock individually are presented in Table B.2. We find the same relationship for Visa and Mastercard as was found in the panel regression on the payment systems. The volatility of American Express and Western Union, however, is estimated to increase on the day of a cyberattack. This relationship seems to be increasing over time in the case of Western Union, whereas for American Express, decomposing the impact of LM_t into a constant and a time-varying component does not seem to improve the model. For PayPal we find that the effect of LM_t on the volatility is changing over time.

6.5.3 Trading volume

Results from employing time series regressions on the trading volume specifications for each payment system stock individually are presented in Table B.3. These findings show that only Visa and Mastercard report the same relationship that was found in the panel regression on the payment systems, seeing as the trading volume of both of these stocks are positively affected by cyberattacks, while we find no evidence that the impact of LM_t is changing over time. The impact of cyberattacks on the trading volume of American Express is found to be increasing over time. In the case of PayPal and Western Union, we do not find evidence that cyberattacks on cryptocurrencies influence their trading volume.

7 Conclusion

The literature on the cryptocurrency market has been growing rapidly since the inception of Bitcoin in 2009. We investigate whether cyberattacks related to crytocurrencies affect the returns, volatility, and trading volume of cryptocurrencies. The analyses are based on trading history and historical data on cyberattacks from December 27, 2013, to December 31, 2019. Further, to investigate whether cyberattacks on cryptocurrencies is a cryptocurrency-specific risk, we also analyze the impact of these cyberattacks on payment system stocks, the general stock market, the technology sector, the financial sector, and gold.

Investigation of twenty large cryptocurrencies reveals that cyberattacks in the cryptocurrency market have a statistically significant impact on their daily returns, volatility and trading volume. Our findings provide evidence that cryptocurrency-related cyberattacks have a negative impact on daily returns but that the impact is becoming less negative over time. As for the volatility and the trading volume, we find that cryptocurrency-related cyberattacks elevate both the volatility and the trading volume. The results suggest that the impact on the volatility and the trading volume is decreasing over time. Moreover, time series regressions on each of the cryptocurrencies reveal that these relationships are predominantly present among the ten cryptocurrencies with the longest trading history, suggesting that there is variability across cryptocurrencies. This might be a contributing factor to the decreasing time trend in the impact of cyberattacks on our dependent variables.

Investigation of five payment system stocks provides evidence that cryptocurrency-related cyberattacks do indeed have an impact on the payment systems. Both daily returns and volatility are expected to decrease on the day of a cyberattack. As for the trading volume, we find that cryptocurrency-related cyberattacks elevate the trading volume on the day of the attack. Cryptocurrency-related cyberattacks also have a negative impact on the general stock market and the technology and financial sectors, where they are associated with negative returns and increased volatility. On the other hand, gold acts as safe heaven with respect to these attacks. On the day of a cyberattack, gold exhibits positive returns and decreased volatility.

References

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

Andoh-Baidoo, F. K. (2013). Explaining investors' reaction to internet security breach using deterrence theory. *International Journal of Electronic Finance*, 7(1):1–14.

Arcuri, M. C., Brogi, M., and Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. In *ITASEC*, pages 175–193.

Balcilar, M., Bouri, E., Gupta, R., and Roubaud, D. (2017). Can volume predict Bitcoin returns and volatility? A quantiles-based approach. *Economic Modelling*, 64:74–81.

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

Bianchi, D. and Tosun, O. K. (2019). Cyber Attacks and Stock Market Activity. *Available at SSRN 3190454*.

Borri, N. (2019). Conditional tail-risk in cryptocurrency markets. *Journal of Empirical Finance*, 50:1–19.

Brandvold, M., Molnár, P., Vagstad, K., and Valstad, O. C. A. (2015). Price discovery on Bitcoin exchanges. *Journal of International Financial Markets, Institutions and Money*, 36:18–35.

Cahill, D., Baur, D. G., Liu, Z. F., and Yang, J. W. (2020). I am a blockchain too: How does the market respond to companies' interest in blockchain? *Journal of Banking & Finance*, 113.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448.

Caporale, G. M., Kang, W.-Y., Spagnolo, F., and Spagnolo, N. (2020). Cyber-Attacks and Cryptocurrencies. *CESifo Working Paper No. 8124*.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1):70–104.

CoinMarketCap (2020). Top 100 Coins by Market Capitalization. https://coinmarketcap.com. Accessed: January 20, 2020.

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., and Vigne, S. (2019a). Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in Cryptocurrency Markets. *Available at SSRN 3384707*.

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

Corbet, S., Larkin, C., Lucey, B., Meegan, A., and Yarovaya, L. (2020). Cryptocurrency reaction to FOMC Announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability*, 46.

Corbet, S., Lucey, B., Urquhart, A., and Yarovaya, L. (2019c). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, 62:182–199.

Corsi, F. (2009). A Simple Approximate Long-Memory Model of Realized Volatility. *Journal of Financial Econometrics*, 7(2):174–196.

de Graaf, T. (2019). From old to new: From internet to smart contracts and from people to smart contracts. *Computer Law & Security Review*, 35(5):105322.

De Hoyos, R. E. and Sarafidis, V. (2006). Testing for cross-sectional dependence in panel-data models. *The Stata Journal*, 6(4):482–496.

Driscoll, J. C. and Kraay, A. C. (1998). Consistent Covariance Matrix Estimation with Spatially Dependent Panel Data. *Review of Economics and Statistics*, 80(4):549–560.

Easley, D., O'Hara, M., and Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109.

Enoksen, F., Landsnes, C. J., Lučivjanská, K., and Molnár, P. (2020). Understanding risk of bubbles in cryptocurrencies. *Journal of Economic Behavior & Organization*, 176:129–144.

Fiszeder, P., Fałdziński, M., and Molnár, P. (2019). Range-based DCC models for covariance and value-at-risk forecasting. *Journal of Empirical Finance*, 54:58–76.

Foley, S., Karlsen, J. R., and Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies*, 32(5):1798–1853.

Gandal, N., Hamrick, J., Moore, T., and Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, 95:86–96.

Garg, A., Curtis, J., and Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2):74–83.

Garman, M. B. and Klass, M. J. (1980). On the Estimation of Security Price Volatilities from Historical Data. *Journal of Business*, 53(1):67–78.

Garnier, J. and Solna, K. (2019). Chaos and order in the bitcoin market. *Physica A: Statistical Mechanics and its Applications*, 524:708–721.

Goel, D. and Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, 73:519–544.

hackmageddon (2020). Information Security Timelines and Statistics. https://www.hackmageddon.com. Accessed: January 20, 2020.

Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security*, 2018(7):13–15.

Hoechle, D. (2007). Robust standard errors for panel regressions with cross-sectional dependence. *The Stata Journal*, 7(3):281–312.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*.

Katz, J. and Lindell, Y. (2014). *Introduction to Modern Cryptography*. CRC press.

Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107:841–853.

Liu, J. and Serletis, A. (2019). Volatility in the Cryptocurrency Market. *Open Economies Review*, 30(4):779–811.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., and Laskowski, M. (2019). Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: the DAO Attack. *Journal of Cases on Information Technology (JCIT)*, 21(1):19–32.

Molnár, P. (2012). Properties of range-based volatility estimators. *International Review of Financial Analysis*, 23:20–29.

Molnár, P. (2016). High-low range in GARCH models of stock return volatility. *Applied Economics*, 48(51):4977–4991.

Moore, T. and Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In *International Conference on Financial Cryptography and Data Security*, pages 25–33. Springer.

Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System.

Pesaran, M. H. (2006). Estimation and Inference in Large Heterogeneous Panels with a Multifactor Error Structure. *Econometrica*, 74(4):967–1012.

Polasik, M., Piotrowska, A. I., Wisniewski, T. P., Kotkowski, R., and Lightfoot, G. (2015). Price fluctuations and the Use of Bitcoin: An Empirical Inquiry. *International Journal of Electronic Commerce*, 20(1):9–49.

Rouse, M. (2020). What is cryptography? https://searchsecurity.techtarget.com/definition/cryptography. Accessed: March 5, 2020.

Sayeed, S. and Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, 9(9):1788.

Selgin, G. (2015). Synthetic commodity money. *Journal of Financial Stability*, 17:92–99.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. " O'Reilly Media, Inc.".

Thies, S. and Molnár, P. (2018). Bayesian change point analysis of Bitcoin returns. *Finance Research Letters*, 27:223–227.

Torres-Reyna, O. (2007). Panel Data Analysis Fixed and Random Effects using Stata (v. 4.2). *Data & Statistical Services, Princeton University*, 112.

Trautman, L. J. (2014). Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology*, 20(4).

Trimborn, S. and Härdle, W. K. (2018). CRIX an Index for cryptocurrencies. *Journal of Empirical Finance*, 49:107–122.

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

van Hardeveld, G. J., Webber, C., and O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, 61(11):1244–1266.

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):1–9.

Yahoo Finance (2020). Stock Market Live, Quotes, Business & Finance News. https://finance.yahoo.com. Accessed: January 20, 2020.

Zachariadis, M., Hileman, G., and Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, 29(2):105–117.

A Appendix: Closer investigation of cryptocurrencies

Table A.1: The impact of cyberattacks on cryptocurrency returns (1/4).

	Dependent variable: Return									
	BTC		**LTC**		**XRP**		**DOGE**		**DASH**	
r_{t-1}	-0.011	-0.010	-0.020	-0.020	-0.019	-0.019	0.011	0.011	-0.014	-0.014
	(0.036)	(0.036)	(0.038)	(0.038)	(0.075)	(0.075)	(0.040)	(0.040)	(0.047)	(0.047)
r_w	0.022	0.016	0.087	0.085	0.176	0.175	-0.075	-0.075	-0.109	-0.111
	(0.093)	(0.092)	(0.096)	(0.096)	(0.141)	(0.141)	(0.106)	(0.106)	(0.159)	(0.160)
r_m	0.002	0.000	-0.094	-0.092	-0.053	-0.052	0.133	0.134	0.001	0.006
	(0.181)	(0.181)	(0.204)	(0.204)	(0.201)	(0.201)	(0.217)	(0.217)	(0.204)	(0.204)
σ_{t-1}	-0.001	-0.001	0.001	0.001	0.001	0.001	0.003	0.003	0.000	0.000
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)
σ_w	0.002	0.002	-0.003	-0.003	0.004	0.004	-0.002	-0.002	-0.001	-0.001
	(0.002)	(0.002)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.004)	(0.004)
σ_m	-0.001	-0.001	0.003	0.002	-0.004*	-0.004*	0.001	0.001	0.003	0.003
	(0.002)	(0.002)	(0.003)	(0.003)	(0.002)	(0.002)	(0.003)	(0.003)	(0.004)	(0.004)
V_{t-1}	0.007	0.007*	0.006	0.006	0.003	0.003	0.009**	0.009**	0.010	0.010
	(0.004)	(0.004)	(0.005)	(0.005)	(0.003)	(0.003)	(0.004)	(0.004)	(0.007)	(0.007)
V_w	-0.005	-0.005	-0.007	-0.007	-0.003	-0.003	-0.006	-0.006	0.005	0.004
	(0.006)	(0.006)	(0.007)	(0.007)	(0.006)	(0.006)	(0.006)	(0.006)	(0.008)	(0.008)
V_m	0.000	0.001	0.013**	0.013**	0.008	0.008	0.003	0.003	0.006	0.006
	(0.006)	(0.006)	(0.005)	(0.005)	(0.007)	(0.007)	(0.005)	(0.005)	(0.007)	(0.007)
LM_t	-1.043	-31.061***	-1.216	-17.017**	0.060	-6.838	-2.963	-28.449***	-1.852	-24.466***
	(6.061)	(7.963)	(3.491)	(6.760)	(2.391)	(6.323)	(4.980)	(5.912)	(4.590)	(5.112)
$LM_t \cdot time$		0.017***		0.009***		0.004		0.014***		0.013***
		(0.004)		(0.003)		(0.003)		(0.003)		(0.002)
Constant	0.001	0.001	-0.002	-0.003	0.001	0.001	0.010	0.010	0.015	0.015
	(0.007)	(0.007)	(0.009)	(0.009)	(0.011)	(0.011)	(0.013)	(0.013)	(0.017)	(0.017)
N	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,087	2,087
R^2	0.003	0.008	0.007	0.008	0.014	0.014	0.013	0.015	0.014	0.015
Adj. R^2	-0.002	0.003	0.003	0.003	0.009	0.009	0.009	0.010	0.010	0.010

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.2: The impact of cyberattacks on cryptocurrency returns (2/4).

	Dependent variable: Return									
	XMR		**XLM**		**XEM**		**ETH**		**DCR**	
r_{t-1}	-0.047	-0.047	0.059	0.059	-0.092*	-0.093*	-0.001	-0.000	-0.125***	-0.124***
	(0.035)	(0.035)	(0.059)	(0.059)	(0.049)	(0.049)	(0.047)	(0.046)	(0.042)	(0.042)
r_w	0.138	0.135	-0.110	-0.111	-0.052	-0.051	-0.005	-0.015	0.049	0.045
	(0.096)	(0.096)	(0.141)	(0.141)	(0.116)	(0.116)	(0.125)	(0.124)	(0.131)	(0.131)
r_m	-0.095	-0.090	0.180	0.179	0.117	0.125	0.001	0.012	-0.256	-0.281
	(0.217)	(0.217)	(0.214)	(0.215)	(0.224)	(0.224)	(0.204)	(0.203)	(0.293)	(0.293)
σ_{t-1}	0.002	0.002	0.002	0.002	0.002	0.002	-0.000	-0.000	-0.001	-0.001
	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.003)	(0.003)
σ_w	-0.000	-0.000	0.001	0.001	0.001	0.002	-0.001	-0.002	0.004	0.004
	(0.004)	(0.004)	(0.005)	(0.005)	(0.005)	(0.005)	(0.004)	(0.004)	(0.004)	(0.004)
σ_m	-0.002	-0.002	-0.001	-0.001	-0.001	-0.001	0.004	0.004	0.004	0.004
	(0.004)	(0.004)	(0.005)	(0.005)	(0.005)	(0.005)	(0.004)	(0.004)	(0.004)	(0.004)
V_{t-1}	-0.001	-0.001	0.003	0.003	0.006	0.006	0.014*	0.014*	-0.001	-0.001
	(0.004)	(0.004)	(0.004)	(0.004)	(0.005)	(0.005)	(0.008)	(0.008)	(0.005)	(0.005)
V_w	0.007	0.007	0.000	0.000	-0.005	-0.005	-0.004	-0.003	0.005	0.004
	(0.007)	(0.007)	(0.007)	(0.007)	(0.006)	(0.006)	(0.011)	(0.011)	(0.006)	(0.006)
V_m	0.001	0.001	0.000	0.000	0.010	0.010	0.009	0.008	0.012	0.013
	(0.006)	(0.006)	(0.006)	(0.006)	(0.007)	(0.007)	(0.010)	(0.010)	(0.008)	(0.008)
LM_t	0.155	-22.812	-1.056	-13.588	-11.893	-60.958***	-14.432	-87.620***	-4.363	-57.380***
	(6.881)	(20.584)	(3.439)	(10.406)	(9.751)	(10.389)	(12.742)	(20.247)	(9.413)	(5.664)
$LM_t \cdot time$		0.013		0.007		0.028***		0.041***		0.030***
		(0.009)		(0.005)		(0.005)		(0.009)		(0.003)
Constant	-0.004	-0.004	0.016	0.016	0.018	0.019	0.018	0.019	0.037**	0.039**
	(0.012)	(0.012)	(0.016)	(0.016)	(0.018)	(0.018)	(0.016)	(0.016)	(0.015)	(0.015)
N	1,990	1,990	1,915	1,915	1,676	1,676	1,548	1,548	1,361	1,361
R^2	0.008	0.009	0.012	0.012	0.020	0.024	0.023	0.038	0.025	0.031
Adj. R^2	0.003	0.004	0.006	0.006	0.014	0.017	0.017	0.031	0.018	0.023

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.3: The impact of cyberattacks on cryptocurrency returns (3/4).

	Dependent variable: Return									
	ETC		**NEO**		**ZEC**		**MIOTA**		**EOS**	
r_{t-1}	-0.094**	-0.093**	-0.019	-0.019	-0.043	-0.042	-0.054	-0.054	-0.020	-0.020
	(0.044)	(0.044)	(0.070)	(0.070)	(0.041)	(0.042)	(0.057)	(0.057)	(0.043)	(0.043)
r_w	0.155	0.156	0.040	0.039	0.168	0.170	0.306*	0.306*	0.090	0.094
	(0.147)	(0.147)	(0.179)	(0.179)	(0.122)	(0.122)	(0.160)	(0.160)	(0.140)	(0.141)
r_m	0.134	0.131	-0.155	-0.155	-0.036	-0.040	-0.402	-0.403	-0.080	-0.090
	(0.265)	(0.265)	(0.234)	(0.235)	(0.246)	(0.245)	(0.313)	(0.313)	(0.383)	(0.384)
σ_{t-1}	0.001	0.001	0.003	0.003	0.004	0.003	0.003	0.003	-0.000	-0.000
	(0.002)	(0.002)	(0.003)	(0.003)	(0.003)	(0.003)	(0.004)	(0.004)	(0.004)	(0.004)
σ_w	0.003	0.003	-0.002	-0.002	0.004	0.004	0.001	0.001	0.001	0.001
	(0.005)	(0.005)	(0.006)	(0.006)	(0.005)	(0.005)	(0.006)	(0.006)	(0.007)	(0.007)
σ_m	-0.004	-0.004	0.006	0.006	-0.009*	-0.009*	-0.002	-0.002	0.001	0.001
	(0.005)	(0.005)	(0.006)	(0.006)	(0.005)	(0.005)	(0.006)	(0.006)	(0.007)	(0.007)
V_{t-1}	0.001	0.001	0.003	0.003	0.003	0.003	0.007	0.007	0.005	0.005
	(0.007)	(0.007)	(0.008)	(0.008)	(0.008)	(0.008)	(0.010)	(0.010)	(0.015)	(0.015)
V_w	-0.008	-0.008	0.001	0.001	-0.021*	-0.021*	-0.006	-0.006	-0.006	-0.005
	(0.010)	(0.010)	(0.010)	(0.010)	(0.011)	(0.012)	(0.012)	(0.012)	(0.021)	(0.021)
V_m	0.006	0.006	0.004	0.004	0.022**	0.022**	0.020	0.020	0.019	0.020
	(0.008)	(0.008)	(0.007)	(0.007)	(0.011)	(0.011)	(0.013)	(0.013)	(0.013)	(0.013)
LM_t	0.585	-64.632	0.140	-65.864	1.507	-49.782	4.523***	20.796	6.303***	-47.703
	(1.623)	(48.953)	(1.620)	(48.212)	(1.638)	(43.940)	(1.268)	(37.203)	(1.772)	(38.765)
$LM_t \cdot time$		0.029		0.030		0.023		-0.007		0.024
		(0.021)		(0.021)		(0.019)		(0.016)		(0.017)
Constant	-0.000	0.001	0.047**	0.048**	-0.009	-0.008	0.011	0.011	0.013	0.013
	(0.020)	(0.021)	(0.020)	(0.020)	(0.020)	(0.020)	(0.017)	(0.017)	(0.022)	(0.022)
N	1,196	1,196	1,149	1,149	1,099	1,099	872	872	854	854
R^2	0.009	0.010	0.010	0.010	0.011	0.012	0.027	0.027	0.013	0.013
Adj. R^2	0.001	0.001	0.001	0.000	0.002	0.002	0.016	0.015	0.001	0.000

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.4: The impact of cyberattacks on cryptocurrency returns (4/4).

	Dependent variable: Return									
	BCH		**BNB**		**TRX**		**LINK**		**ADA**	
r_{t-1}	0.036	0.035	0.078	0.079	0.016	0.016	-0.084	-0.084	-0.050	-0.050
	(0.061)	(0.061)	(0.074)	(0.074)	(0.073)	(0.073)	(0.055)	(0.055)	(0.075)	(0.075)
r_w	-0.149	-0.148	-0.136	-0.132	0.379*	0.379*	0.202	0.202	0.201	0.201
	(0.158)	(0.159)	(0.161)	(0.161)	(0.229)	(0.229)	(0.164)	(0.164)	(0.146)	(0.146)
r_m	-0.065	-0.067	-0.574	-0.583	-0.257	-0.257	-0.322	-0.319	0.046	0.044
	(0.389)	(0.389)	(0.403)	(0.405)	(0.521)	(0.521)	(0.345)	(0.345)	(0.309)	(0.310)
σ_{t-1}	-0.002	-0.002	-0.001	-0.001	0.004	0.004	0.005	0.005	0.007	0.007
	(0.005)	(0.005)	(0.003)	(0.003)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)
σ_w	-0.003	-0.003	0.001	0.000	0.002	0.002	-0.003	-0.002	-0.003	-0.003
	(0.006)	(0.006)	(0.005)	(0.005)	(0.008)	(0.008)	(0.008)	(0.008)	(0.008)	(0.008)
σ_m	0.006	0.006	0.011*	0.011*	-0.004	-0.004	-0.000	-0.000	-0.003	-0.003
	(0.006)	(0.006)	(0.006)	(0.006)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
V_{t-1}	0.024	0.024	0.010	0.009	0.005	0.005	0.005	0.005	0.003	0.003
	(0.018)	(0.018)	(0.006)	(0.006)	(0.019)	(0.019)	(0.008)	(0.008)	(0.013)	(0.013)
V_w	-0.000	-0.000	-0.010	-0.009	-0.017	-0.017	-0.011	-0.010	-0.009	-0.009
	(0.018)	(0.018)	(0.010)	(0.010)	(0.030)	(0.030)	(0.011)	(0.011)	(0.017)	(0.018)
V_m	-0.007	-0.007	0.026**	0.026**	0.026	0.026	0.019	0.019	0.017	0.017
	(0.015)	(0.015)	(0.012)	(0.012)	(0.018)	(0.018)	(0.012)	(0.012)	(0.013)	(0.013)
LM_t	3.711***	-31.188	1.994	-39.461	4.098*	7.011	-2.350	-83.519***	3.043*	-7.201
	(1.186)	(32.144)	(1.582)	(38.528)	(2.279)	(86.096)	(2.415)	(31.530)	(1.779)	(46.451)
$LM_t \cdot time$		0.016		0.018		-0.001		0.036***		0.005
		(0.014)		(0.017)		(0.038)		(0.014)		(0.020)
Constant	-0.001	-0.001	0.066***	0.067***	0.010	0.010	0.016	0.018	0.000	0.001
	(0.028)	(0.028)	(0.023)	(0.023)	(0.026)	(0.026)	(0.028)	(0.029)	(0.026)	(0.026)
N	832	832	830	830	780	780	773	773	762	762
R^2	0.023	0.023	0.033	0.033	0.043	0.043	0.015	0.016	0.029	0.029
Adj. R^2	0.011	0.010	0.021	0.020	0.030	0.029	0.002	0.001	0.016	0.015

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.5: The impact of cyberattacks on cryptocurrency volatility (1/4).

	Dependent variable: Volatility									
	BTC		LTC		XRP		DOGE		DASH	
r_{t-1}	-1.753***	-1.767***	-0.556	-0.558	0.494	0.500	0.341	0.342	-0.473	-0.474
	(0.652)	(0.653)	(0.460)	(0.461)	(0.420)	(0.420)	(0.419)	(0.419)	(0.362)	(0.362)
r_w	-3.315*	-3.207*	-4.101***	-4.065***	-0.715	-0.698	-1.421	-1.420	-2.765**	-2.759**
	(1.846)	(1.845)	(1.380)	(1.380)	(1.219)	(1.220)	(1.223)	(1.223)	(1.277)	(1.278)
r_m	5.323	5.347	2.537	2.467	2.440	2.425	-1.137	-1.146	3.433	3.415
	(3.631)	(3.632)	(3.051)	(3.052)	(2.726)	(2.728)	(2.932)	(2.932)	(2.763)	(2.765)
σ_{t-1}	0.222***	0.222***	0.187***	0.186***	0.374***	0.374***	0.277***	0.277***	0.262***	0.262***
	(0.035)	(0.035)	(0.036)	(0.036)	(0.031)	(0.031)	(0.032)	(0.032)	(0.032)	(0.032)
σ_w	0.427***	0.430***	0.354***	0.354***	0.165***	0.165***	0.290***	0.289***	0.328***	0.328***
	(0.059)	(0.059)	(0.062)	(0.062)	(0.055)	(0.055)	(0.058)	(0.058)	(0.056)	(0.056)
σ_m	0.264***	0.263***	0.369***	0.370***	0.369***	0.369***	0.343***	0.345***	0.276***	0.276***
	(0.054)	(0.054)	(0.056)	(0.056)	(0.054)	(0.054)	(0.058)	(0.058)	(0.058)	(0.058)
V_{t-1}	0.603***	0.598***	0.692***	0.690***	0.288***	0.286***	0.378***	0.378***	0.417***	0.416***
	(0.109)	(0.110)	(0.093)	(0.093)	(0.064)	(0.064)	(0.064)	(0.064)	(0.076)	(0.076)
V_w	-0.003	-0.005	-0.212*	-0.211*	0.073	0.073	-0.140	-0.139	-0.095	-0.095
	(0.161)	(0.161)	(0.121)	(0.121)	(0.093)	(0.093)	(0.088)	(0.088)	(0.110)	(0.110)
V_m	-0.215	-0.217	0.010	0.010	-0.203*	-0.203*	-0.047	-0.047	-0.116	-0.115
	(0.141)	(0.141)	(0.103)	(0.103)	(0.111)	(0.111)	(0.080)	(0.080)	(0.120)	(0.120)
LM_t	288.279**	831.306***	341.260***	739.204***	139.220*	326.593	185.008***	455.395***	125.349***	208.458*
	(120.759)	(177.107)	(61.372)	(149.315)	(81.714)	(211.470)	(54.528)	(36.338)	(37.108)	(120.267)
$LM_t \cdot time$		-0.307***		-0.225***		-0.106		-0.153***		-0.047
		(0.084)		(0.068)		(0.103)		(0.016)		(0.060)
Constant	-0.727***	-0.719***	-0.715***	-0.708***	-0.713***	-0.708***	-0.620***	-0.618***	-0.900***	-0.900***
	(0.165)	(0.165)	(0.173)	(0.173)	(0.186)	(0.186)	(0.168)	(0.168)	(0.201)	(0.201)
N	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,087	2,087
R^2	0.558	0.559	0.530	0.530	0.539	0.539	0.493	0.493	0.433	0.433
Adj. R^2	0.556	0.557	0.528	0.528	0.537	0.536	0.491	0.491	0.430	0.430

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.6: The impact of cyberattacks on cryptocurrency volatility (2/4).

	Dependent variable: Volatility									
	XMR		XLM		XEM		ETH		DCR	
r_{t-1}	-0.846**	-0.842**	0.483	0.483	0.622*	0.626*	-0.600	-0.606	-0.302	-0.305
	(0.344)	(0.345)	(0.372)	(0.372)	(0.319)	(0.319)	(0.463)	(0.462)	(0.409)	(0.409)
r_w	1.133	1.168	0.519	0.546	-0.898	-0.904	-3.333**	-3.228**	-1.616	-1.603
	(1.095)	(1.096)	(1.029)	(1.030)	(1.246)	(1.247)	(1.513)	(1.511)	(1.429)	(1.430)
r_m	3.677	3.600	5.739**	5.777**	6.231**	6.161**	5.473	5.359	4.613	4.704
	(2.670)	(2.671)	(2.346)	(2.346)	(2.685)	(2.686)	(3.483)	(3.480)	(3.863)	(3.868)
σ_{t-1}	0.271***	0.271***	0.364***	0.364***	0.255***	0.257***	0.206***	0.205***	0.263***	0.264***
	(0.033)	(0.033)	(0.033)	(0.033)	(0.033)	(0.033)	(0.044)	(0.044)	(0.037)	(0.037)
σ_w	0.365***	0.363***	0.138**	0.135**	0.308***	0.305***	0.399***	0.400***	0.297***	0.296***
	(0.057)	(0.057)	(0.060)	(0.060)	(0.061)	(0.061)	(0.073)	(0.073)	(0.077)	(0.077)
σ_m	0.234***	0.235***	0.361***	0.363***	0.307***	0.308***	0.247***	0.244***	0.349***	0.349***
	(0.056)	(0.056)	(0.062)	(0.062)	(0.061)	(0.061)	(0.072)	(0.072)	(0.074)	(0.074)
V_{t-1}	0.276***	0.276***	0.158***	0.156***	0.288***	0.284***	0.641***	0.641***	0.111	0.110
	(0.062)	(0.062)	(0.054)	(0.054)	(0.057)	(0.057)	(0.116)	(0.116)	(0.076)	(0.077)
V_w	-0.155*	-0.154*	-0.021	-0.018	-0.178**	-0.171**	-0.186	-0.193	-0.019	-0.018
	(0.083)	(0.083)	(0.078)	(0.078)	(0.076)	(0.076)	(0.158)	(0.157)	(0.106)	(0.106)
V_m	-0.124	-0.123	-0.205***	-0.209***	-0.197**	-0.197**	-0.206	-0.200	-0.085	-0.088
	(0.088)	(0.088)	(0.079)	(0.079)	(0.093)	(0.093)	(0.145)	(0.145)	(0.123)	(0.123)
LM_t	141.602*	508.319***	110.641*	456.259***	187.326*	653.230***	255.582*	1,014.090***	230.318***	423.206***
	(73.054)	(24.671)	(61.549)	(104.240)	(98.442)	(58.416)	(132.951)	(247.951)	(39.056)	(21.208)
$LM_t \cdot time$		-0.208***		-0.196***		-0.262***		-0.426***		-0.108***
		(0.015)		(0.047)		(0.031)		(0.110)		(0.011)
Constant	-0.820***	-0.826***	-0.863***	-0.865***	-0.792***	-0.800***	-1.052***	-1.065***	-0.551***	-0.557***
	(0.189)	(0.189)	(0.200)	(0.200)	(0.223)	(0.223)	(0.241)	(0.242)	(0.211)	(0.212)
N	1,990	1,990	1,915	1,915	1,676	1,676	1,548	1,548	1,361	1,361
R^2	0.425	0.425	0.452	0.453	0.437	0.438	0.470	0.473	0.469	0.470
Adj. R^2	0.422	0.422	0.449	0.450	0.433	0.434	0.466	0.469	0.466	0.465

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.7: The impact of cyberattacks on cryptocurrency volatility (3/4).

	Dependent variable: Volatility									
	ETC		NEO		ZEC		MIOTA		EOS	
r_{t-1}	-0.269	-0.269	-0.256	-0.256	-0.231	-0.241	0.313	0.311	-0.437	-0.438
	(0.512)	(0.512)	(0.354)	(0.354)	(0.542)	(0.543)	(0.483)	(0.483)	(0.503)	(0.503)
r_w	-1.839	-1.840	-0.492	-0.498	-3.979**	-4.021**	-4.584***	-4.592***	-1.051	-1.054
	(1.784)	(1.785)	(1.086)	(1.087)	(1.775)	(1.778)	(1.465)	(1.466)	(1.676)	(1.681)
r_m	1.796	1.799	6.337**	6.335**	10.345***	10.438***	2.906	2.880	-3.189	-3.178
	(4.064)	(4.066)	(2.501)	(2.502)	(3.729)	(3.729)	(3.937)	(3.943)	(4.295)	(4.315)
σ_{t-1}	0.202***	0.202***	0.238***	0.237***	0.243***	0.246***	0.159***	0.159***	0.226***	0.226***
	(0.045)	(0.045)	(0.042)	(0.042)	(0.040)	(0.040)	(0.051)	(0.051)	(0.056)	(0.056)
σ_w	0.402***	0.402***	0.456***	0.457***	0.363***	0.357***	0.385***	0.384***	0.417***	0.417***
	(0.077)	(0.077)	(0.070)	(0.070)	(0.074)	(0.075)	(0.094)	(0.094)	(0.097)	(0.097)
σ_m	0.234***	0.234***	0.174**	0.175**	0.221***	0.221***	0.372***	0.373***	0.233***	0.233***
	(0.076)	(0.076)	(0.068)	(0.068)	(0.080)	(0.080)	(0.087)	(0.087)	(0.089)	(0.089)
V_{t-1}	0.615***	0.615***	0.389***	0.390***	0.615***	0.612***	0.541***	0.542***	0.623***	0.623***
	(0.114)	(0.114)	(0.095)	(0.095)	(0.129)	(0.128)	(0.116)	(0.116)	(0.169)	(0.169)
V_w	-0.473***	-0.473***	-0.422***	-0.423***	-0.543***	-0.531***	-0.345**	-0.345**	-0.436*	-0.436*
	(0.140)	(0.140)	(0.114)	(0.114)	(0.171)	(0.171)	(0.150)	(0.150)	(0.228)	(0.228)
V_m	0.188	0.188	-0.056	-0.056	-0.052	-0.055	0.023	0.025	0.201	0.201
	(0.135)	(0.135)	(0.094)	(0.094)	(0.169)	(0.169)	(0.155)	(0.156)	(0.165)	(0.166)
LM_t	33.581	90.483	57.878***	-281.305	-18.685	1,159.411	56.773***	420.195	127.778***	182.383
	(26.526)	(850.023)	(15.208)	(439.496)	(52.459)	(862.002)	(16.089)	(402.277)	(29.106)	(673.553)
$LM_t \cdot time$		-0.025		0.152		-0.528		-0.162		-0.024
		(0.372)		(0.193)		(0.377)		(0.175)		(0.294)
Constant	-1.098***	-1.099***	-0.812***	-0.807***	-1.098***	-1.126***	-0.550**	-0.556**	-0.837***	-0.838***
	(0.282)	(0.285)	(0.234)	(0.235)	(0.304)	(0.306)	(0.235)	(0.237)	(0.298)	(0.299)
N	1,196	1,196	1,149	1,149	1,099	1,099	872	872	854	854
R^2	0.414	0.414	0.501	0.501	0.373	0.374	0.521	0.521	0.479	0.479
Adj. R^2	0.409	0.408	0.497	0.496	0.367	0.367	0.516	0.515	0.473	0.472

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.8: The impact of cyberattacks on cryptocurrency volatility (4/4).

	Dependent variable: Volatility									
	BCH		BNB		TRX		LINK		ADA	
r_{t-1}	-0.306	-0.302	-1.034*	-1.050*	-0.043	-0.051	0.085	0.083	-0.502	-0.523
	(0.641)	(0.642)	(0.556)	(0.554)	(0.439)	(0.439)	(0.450)	(0.450)	(0.543)	(0.544)
r_w	-2.397	-2.430	-0.450	-0.525	-0.478	-0.493	-2.763*	-2.761*	-4.835***	-4.803***
	(1.738)	(1.743)	(1.698)	(1.689)	(1.477)	(1.477)	(1.418)	(1.420)	(1.446)	(1.445)
r_m	11.099**	11.150**	7.026*	7.212*	-0.899	-0.881	6.804**	6.785**	4.177	4.400
	(4.676)	(4.683)	(4.212)	(4.227)	(3.099)	(3.098)	(2.911)	(2.912)	(3.575)	(3.573)
σ_{t-1}	0.274***	0.275***	0.364***	0.362***	0.303***	0.304***	0.262***	0.263***	0.233***	0.234***
	(0.064)	(0.064)	(0.041)	(0.041)	(0.051)	(0.051)	(0.049)	(0.049)	(0.055)	(0.055)
σ_w	0.414***	0.411***	0.362***	0.363***	0.285***	0.281***	0.308***	0.308***	0.322***	0.325***
	(0.085)	(0.085)	(0.076)	(0.076)	(0.084)	(0.084)	(0.090)	(0.090)	(0.094)	(0.094)
σ_m	0.167**	0.167**	0.170**	0.167**	0.291***	0.289***	0.333***	0.332***	0.286***	0.279***
	(0.085)	(0.085)	(0.075)	(0.075)	(0.080)	(0.080)	(0.087)	(0.087)	(0.086)	(0.087)
V_{t-1}	0.433**	0.432**	0.112	0.126	0.439**	0.440**	0.324***	0.325***	0.509***	0.510***
	(0.193)	(0.193)	(0.103)	(0.098)	(0.173)	(0.173)	(0.098)	(0.098)	(0.122)	(0.122)
V_w	-0.400*	-0.395*	-0.205	-0.212	-0.277	-0.267	-0.220*	-0.221*	-0.333**	-0.341**
	(0.205)	(0.205)	(0.132)	(0.130)	(0.179)	(0.179)	(0.126)	(0.126)	(0.162)	(0.162)
V_m	-0.360*	-0.362*	-0.043	-0.051	0.142	0.135	-0.132	-0.129	0.066	0.061
	(0.207)	(0.207)	(0.153)	(0.154)	(0.152)	(0.152)	(0.122)	(0.122)	(0.154)	(0.154)
LM_t	51.410	827.504*	10.441	888.004	60.956	1,390.646*	-17.634	463.486	40.947	1,193.694
	(35.706)	(487.995)	(28.632)	(848.976)	(37.692)	(726.918)	(27.272)	(743.418)	(46.771)	(766.279)
$LM_t \cdot time$		-0.347		-0.391		-0.594*		-0.215		-0.515
		(0.214)		(0.371)		(0.317)		(0.325)		(0.336)
Constant	-0.911***	-0.926***	-0.702***	-0.722***	-0.833***	-0.859***	-0.583**	-0.594**	-1.055***	-1.075***
	(0.310)	(0.312)	(0.267)	(0.270)	(0.287)	(0.289)	(0.246)	(0.249)	(0.332)	(0.333)
N	832	832	830	830	780	780	773	773	762	762
R^2	0.402	0.402	0.535	0.535	0.544	0.544	0.474	0.474	0.473	0.473
Adj. R^2	0.395	0.394	0.529	0.529	0.538	0.538	0.467	0.467	0.466	0.466

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.9: The impact of cyberattacks on cryptocurrency trading volume (1/4).

	Dependent variable: Trading Volume									
	BTC		LTC		XRP		DOGE		DASH	
r_{t-1}	-0.154	-0.159	0.338*	0.338*	0.602***	0.603***	1.091***	1.091***	0.534***	0.534***
	(0.213)	(0.213)	(0.193)	(0.193)	(0.207)	(0.207)	(0.225)	(0.225)	(0.192)	(0.192)
r_w	0.846	0.886	1.183**	1.200**	1.761***	1.763***	2.100***	2.100***	0.833	0.842
	(0.580)	(0.579)	(0.525)	(0.525)	(0.582)	(0.583)	(0.591)	(0.591)	(0.634)	(0.635)
r_m	3.254***	3.263***	2.119*	2.086*	3.157**	3.155**	1.724	1.722	3.611***	3.586***
	(1.244)	(1.244)	(1.210)	(1.210)	(1.247)	(1.247)	(1.329)	(1.329)	(1.133)	(1.134)
σ_{t-1}	-0.030***	-0.031***	-0.024**	-0.025**	-0.017	-0.016	-0.006	-0.006	-0.010	-0.010
	(0.010)	(0.010)	(0.011)	(0.011)	(0.014)	(0.014)	(0.018)	(0.018)	(0.013)	(0.013)
σ_w	0.001	0.002	-0.045**	-0.046**	-0.003	-0.003	-0.056**	-0.056**	-0.014	-0.015
	(0.017)	(0.017)	(0.020)	(0.020)	(0.024)	(0.024)	(0.027)	(0.027)	(0.024)	(0.024)
σ_m	0.010	0.009	0.040**	0.041**	0.004	0.004	0.032	0.032	-0.010	-0.010
	(0.015)	(0.015)	(0.019)	(0.019)	(0.025)	(0.025)	(0.027)	(0.028)	(0.024)	(0.024)
V_{t-1}	0.564***	0.562***	0.647***	0.647***	0.603***	0.603***	0.547***	0.547***	0.513***	0.512***
	(0.042)	(0.042)	(0.035)	(0.035)	(0.035)	(0.035)	(0.054)	(0.054)	(0.041)	(0.041)
V_w	0.302***	0.301***	0.250***	0.250***	0.203***	0.203***	0.306***	0.306***	0.331***	0.331***
	(0.059)	(0.058)	(0.049)	(0.049)	(0.045)	(0.045)	(0.054)	(0.054)	(0.056)	(0.056)
V_m	-0.161***	-0.161***	-0.109**	-0.109**	-0.189***	-0.189***	-0.132***	-0.133***	-0.185***	-0.185***
	(0.049)	(0.049)	(0.044)	(0.044)	(0.051)	(0.051)	(0.040)	(0.040)	(0.048)	(0.048)
LM_t	92.557***	293.207***	82.881***	267.907***	41.228***	65.984*	58.122***	136.357***	28.713	143.748***
	(31.483)	(43.436)	(25.363)	(86.851)	(15.771)	(37.297)	(11.910)	(34.517)	(21.188)	(42.136)
$LM_t \cdot time$		-0.114***		-0.105**		-0.014		-0.044**		-0.065***
		(0.021)		(0.044)		(0.020)		(0.019)		(0.020)
Constant	-0.141***	-0.138***	-0.199***	-0.195***	-0.092	-0.091	-0.180**	-0.180**	-0.196**	-0.196**
	(0.047)	(0.047)	(0.060)	(0.060)	(0.086)	(0.086)	(0.083)	(0.083)	(0.090)	(0.090)
N	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,136	2,087	2,087
R^2	0.481	0.482	0.595	0.596	0.561	0.561	0.614	0.614	0.562	0.562
Adj. R^2	0.478	0.480	0.593	0.594	0.559	0.558	0.612	0.612	0.560	0.560

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.10: The impact of cyberattacks on cryptocurrency trading volume (2/4).

	Dependent variable: Trading Volume									
	XMR		XLM		XEM		ETH		DCR	
r_{t-1}	0.485**	0.487**	1.456***	1.456***	0.921***	0.923***	0.484**	0.481**	0.400*	0.401*
	(0.193)	(0.193)	(0.224)	(0.225)	(0.217)	(0.217)	(0.192)	(0.191)	(0.216)	(0.216)
r_w	3.722***	3.737***	1.862***	1.872***	2.282***	2.279***	1.351**	1.400**	2.477***	2.476***
	(0.563)	(0.563)	(0.618)	(0.618)	(0.728)	(0.729)	(0.595)	(0.594)	(0.803)	(0.804)
r_m	1.403	1.372	2.020	2.035	2.432	2.398	2.088*	2.036	2.303	2.296
	(1.195)	(1.196)	(1.320)	(1.320)	(1.490)	(1.491)	(1.267)	(1.265)	(2.034)	(2.037)
σ_{t-1}	-0.035***	-0.035***	0.007	0.008	-0.069***	-0.069***	-0.026*	-0.027*	-0.104***	-0.104***
	(0.013)	(0.013)	(0.021)	(0.021)	(0.018)	(0.018)	(0.015)	(0.015)	(0.021)	(0.021)
σ_w	-0.035	-0.036	-0.069**	-0.070**	-0.041	-0.043	-0.017	-0.016	0.005	0.005
	(0.024)	(0.024)	(0.033)	(0.033)	(0.033)	(0.033)	(0.025)	(0.025)	(0.039)	(0.039)
σ_m	0.034	0.034	0.009	0.010	0.078**	0.079**	0.005	0.004	0.056	0.056
	(0.023)	(0.023)	(0.034)	(0.035)	(0.034)	(0.034)	(0.024)	(0.024)	(0.036)	(0.036)
V_{t-1}	0.486***	0.486***	0.515***	0.515***	0.572***	0.570***	0.587***	0.587***	0.573***	0.573***
	(0.033)	(0.033)	(0.041)	(0.041)	(0.039)	(0.039)	(0.048)	(0.048)	(0.045)	(0.045)
V_w	0.370***	0.370***	0.309***	0.310***	0.251***	0.255***	0.293***	0.289***	0.249***	0.249***
	(0.045)	(0.045)	(0.051)	(0.051)	(0.051)	(0.051)	(0.067)	(0.066)	(0.057)	(0.057)
V_m	-0.193***	-0.193***	-0.140***	-0.142***	-0.143**	-0.143**	-0.145**	-0.142**	-0.176**	-0.176**
	(0.042)	(0.042)	(0.052)	(0.052)	(0.060)	(0.060)	(0.061)	(0.060)	(0.072)	(0.072)
LM_t	47.179*	197.147***	50.881**	181.863***	86.163*	312.722***	120.308**	469.635***	44.642***	29.231
	(24.299)	(24.593)	(24.848)	(34.481)	(48.582)	(38.913)	(56.911)	(129.764)	(7.839)	(22.600)
$LM_t \cdot time$		-0.085***		-0.074***		-0.127***		-0.196***		0.009
		(0.012)		(0.016)		(0.020)		(0.058)		(0.011)
Constant	-0.206***	-0.208***	-0.296***	-0.297***	-0.184	-0.187	-0.239***	-0.245***	-0.215**	-0.214**
	(0.075)	(0.075)	(0.110)	(0.110)	(0.141)	(0.141)	(0.091)	(0.091)	(0.108)	(0.108)
N	1,990	1,990	1,915	1,915	1,676	1,676	1,548	1,548	1,361	1,361
R^2	0.618	0.618	0.578	0.578	0.541	0.542	0.599	0.603	0.521	0.521
Adj. R^2	0.616	0.616	0.575	0.575	0.539	0.539	0.596	0.600	0.518	0.518

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.11: The impact of cyberattacks on cryptocurrency trading volume (3/4).

	Dependent variable: Trading Volume									
	ETC		NEO		ZEC		MIOTA		EOS	
r_{t-1}	0.626***	0.629***	0.635***	0.635***	0.404**	0.406**	0.691***	0.692***	0.414**	0.417**
	(0.224)	(0.223)	(0.162)	(0.162)	(0.199)	(0.200)	(0.236)	(0.236)	(0.173)	(0.173)
r_w	1.441**	1.454**	0.995*	0.994*	1.264**	1.271**	1.098*	1.100*	1.183**	1.205**
	(0.705)	(0.704)	(0.599)	(0.600)	(0.584)	(0.585)	(0.655)	(0.656)	(0.555)	(0.556)
r_m	3.241**	3.217**	1.352	1.352	1.869	1.853	1.326	1.331	0.763	0.693
	(1.613)	(1.610)	(1.365)	(1.365)	(1.238)	(1.239)	(1.589)	(1.590)	(1.460)	(1.464)
σ_{t-1}	-0.037**	-0.037**	-0.054***	-0.054***	-0.030**	-0.030**	-0.087***	-0.087***	-0.008	-0.008
	(0.016)	(0.016)	(0.019)	(0.019)	(0.014)	(0.014)	(0.021)	(0.021)	(0.016)	(0.016)
σ_w	-0.011	-0.009	-0.001	-0.001	0.016	0.017	0.024	0.025	-0.036	-0.037
	(0.028)	(0.028)	(0.029)	(0.029)	(0.023)	(0.023)	(0.036)	(0.037)	(0.031)	(0.031)
σ_m	-0.007	-0.007	0.029	0.029	-0.023	-0.023	0.034	0.034	0.021	0.022
	(0.028)	(0.028)	(0.026)	(0.026)	(0.025)	(0.025)	(0.035)	(0.035)	(0.029)	(0.029)
V_{t-1}	0.672***	0.671***	0.700***	0.700***	0.578***	0.579***	0.700***	0.700***	0.639***	0.638***
	(0.050)	(0.050)	(0.052)	(0.052)	(0.056)	(0.056)	(0.053)	(0.053)	(0.058)	(0.058)
V_w	0.163***	0.163***	0.194***	0.194***	0.181***	0.179***	0.139**	0.139**	0.224***	0.225***
	(0.061)	(0.061)	(0.061)	(0.062)	(0.064)	(0.065)	(0.062)	(0.062)	(0.085)	(0.086)
V_m	-0.104*	-0.105*	-0.106*	-0.105*	-0.016	-0.016	-0.016	-0.016	-0.015	-0.013
	(0.054)	(0.055)	(0.057)	(0.057)	(0.054)	(0.054)	(0.062)	(0.062)	(0.051)	(0.051)
LM_t	-3.773	-599.145	28.981***	-21.107	33.835***	-165.449	12.460*	-49.495	28.347**	-327.629**
	(14.863)	(406.573)	(7.042)	(219.513)	(9.869)	(234.256)	(6.734)	(221.570)	(11.146)	(156.849)
$LM_t \cdot time$		0.267		0.022		0.089		0.028		0.159**
		(0.178)		(0.096)		(0.102)		(0.097)		(0.068)
Constant	-0.336***	-0.324***	-0.139	-0.138	-0.208**	-0.203**	-0.173*	-0.172*	-0.133	-0.129
	(0.098)	(0.098)	(0.093)	(0.093)	(0.090)	(0.091)	(0.093)	(0.094)	(0.087)	(0.088)
N	1,196	1,196	1,149	1,149	1,099	1,099	872	872	854	854
R^2	0.638	0.639	0.718	0.718	0.541	0.541	0.662	0.662	0.696	0.696
Adj. R^2	0.635	0.635	0.716	0.715	0.537	0.537	0.658	0.657	0.692	0.692

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table A.12: The impact of cyberattacks on cryptocurrency trading volume (4/4).

	Dependent variable: Trading Volume									
	BCH		BNB		TRX		LINK		ADA	
r_{t-1}	0.373	0.372	0.889**	0.860**	0.468***	0.465***	0.837***	0.837***	0.243	0.232
	(0.241)	(0.241)	(0.430)	(0.407)	(0.167)	(0.165)	(0.215)	(0.215)	(0.245)	(0.244)
r_w	0.702	0.713	3.349**	3.203**	1.956***	1.950***	0.646	0.646	-0.240	-0.224
	(0.660)	(0.661)	(1.352)	(1.245)	(0.500)	(0.499)	(0.719)	(0.720)	(0.609)	(0.608)
r_m	2.232	2.215	-0.255	0.111	-1.414	-1.408	0.225	0.226	2.023	2.140
	(1.727)	(1.727)	(3.904)	(3.869)	(1.176)	(1.175)	(1.413)	(1.413)	(1.561)	(1.551)
σ_{t-1}	-0.042**	-0.042**	0.069	0.066	-0.016	-0.015	-0.029	-0.029	-0.049**	-0.048**
	(0.018)	(0.018)	(0.055)	(0.053)	(0.014)	(0.014)	(0.024)	(0.024)	(0.023)	(0.023)
σ_w	-0.005	-0.004	-0.109	-0.107	-0.041*	-0.043*	-0.042	-0.042	-0.034	-0.032
	(0.029)	(0.029)	(0.080)	(0.079)	(0.023)	(0.023)	(0.040)	(0.040)	(0.041)	(0.041)
σ_m	0.016	0.016	0.042	0.037	0.037	0.037	0.059	0.059	0.055	0.051
	(0.028)	(0.028)	(0.027)	(0.027)	(0.023)	(0.023)	(0.040)	(0.040)	(0.037)	(0.037)
V_{t-1}	0.744***	0.744***	0.260	0.287	0.673***	0.673***	0.709***	0.709***	0.749***	0.749***
	(0.064)	(0.064)	(0.206)	(0.184)	(0.057)	(0.057)	(0.052)	(0.052)	(0.058)	(0.058)
V_w	0.142**	0.141**	0.485***	0.470***	0.196***	0.199***	0.160**	0.160**	0.122*	0.118
	(0.070)	(0.071)	(0.166)	(0.154)	(0.068)	(0.068)	(0.063)	(0.064)	(0.074)	(0.074)
V_m	-0.213***	-0.212***	-0.099	-0.115	0.058	0.056	-0.080	-0.080	-0.038	-0.041
	(0.068)	(0.068)	(0.113)	(0.114)	(0.047)	(0.047)	(0.061)	(0.061)	(0.066)	(0.066)
LM_t	9.945	-248.298	36.419	1,752.401	14.730	480.875	-6.359	-38.324	32.481*	635.064
	(7.354)	(253.129)	(38.418)	(1,580.637)	(16.486)	(653.629)	(12.176)	(321.263)	(18.583)	(474.045)
$LM_t \cdot time$		0.115		-0.765		-0.208		0.014		-0.269
		(0.111)		(0.691)		(0.286)		(0.139)		(0.207)
Constant	-0.174	-0.169	0.021	-0.018	-0.117	-0.126	-0.061	-0.060	-0.174	-0.184
	(0.115)	(0.116)	(0.280)	(0.278)	(0.093)	(0.092)	(0.113)	(0.115)	(0.151)	(0.151)
N	832	832	830	830	780	780	773	773	762	762
R^2	0.716	0.717	0.461	0.466	0.814	0.815	0.653	0.653	0.666	0.666
Adj. R^2	0.713	0.713	0.455	0.459	0.812	0.812	0.649	0.648	0.661	0.662

The table presents time series regression results for the cryptocurrencies over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

B Appendix: Closer investigation of payment system stocks

Table B.1: The impact of cyberattacks on payment system stock returns.

	Dependent variable: Return									
	Visa		Mastercard		PayPal		American Express		Western Union	
r_{t-1}	-0.049	-0.050	-0.041	-0.043	0.008	0.008	0.037	0.037	-0.010	-0.010
	(0.037)	(0.037)	(0.035)	(0.035)	(0.040)	(0.040)	(0.035)	(0.035)	(0.033)	(0.034)
r_w	-0.282***	-0.280***	-0.257**	-0.259**	-0.118	-0.118	-0.111	-0.110	-0.078	-0.076
	(0.105)	(0.105)	(0.110)	(0.110)	(0.104)	(0.104)	(0.087)	(0.087)	(0.085)	(0.085)
r_m	0.013	0.015	0.045	0.055	-0.518*	-0.520*	0.056	0.054	-0.183	-0.183
	(0.197)	(0.197)	(0.218)	(0.218)	(0.266)	(0.266)	(0.188)	(0.188)	(0.158)	(0.158)
σ_{t-1}	-0.001	-0.001	-0.001*	-0.001*	-0.001	-0.001	-0.001*	-0.001*	-0.001	-0.000
	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
σ_w	0.002	0.002	0.002	0.002	-0.001	-0.001	0.001	0.001	0.000	0.000
	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)
σ_m	-0.001	-0.001	0.000	-0.000	0.000	0.000	0.001	0.001	0.002*	0.002*
	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)
V_{t-1}	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.002	0.002
	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.002)	(0.001)	(0.001)
V_w	-0.002	-0.002	-0.001	-0.001	-0.001	-0.001	0.000	0.000	-0.000	-0.000
	(0.002)	(0.002)	(0.003)	(0.003)	(0.003)	(0.003)	(0.002)	(0.002)	(0.002)	(0.002)
V_m	0.004	0.004	0.000	0.000	0.002	0.002	-0.003	-0.002	0.002	0.002
	(0.003)	(0.003)	(0.003)	(0.003)	(0.004)	(0.004)	(0.003)	(0.003)	(0.003)	(0.003)
LM_t	-3.362**	0.901	-2.933*	2.209	-2.502***	-0.966	-2.031***	-0.509	-1.908*	1.022
	(1.544)	(2.781)	(1.707)	(2.562)	(0.844)	(0.888)	(0.650)	(1.423)	(1.064)	(2.473)
$LM_t \cdot time$		-0.004*		-0.005**		-0.002**		-0.001		-0.003
		(0.002)		(0.002)		(0.001)		(0.001)		(0.002)
Constant	0.002	0.002	0.005	0.005	-0.012	-0.012	0.004	0.004	0.020**	0.020**
	(0.007)	(0.007)	(0.008)	(0.009)	(0.010)	(0.010)	(0.008)	(0.008)	(0.010)	(0.010)
N	1,469	1,469	1,469	1,469	1,088	1,088	1,469	1,469	1,469	1,469
R^2	0.027	0.029	0.021	0.023	0.016	0.016	0.008	0.009	0.013	0.014
Adj. R^2	0.021	0.022	0.014	0.016	0.007	0.006	0.002	0.001	0.006	0.006

The table presents time series regression results for the payment system stocks over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table B.2: The impact of cyberattacks on payment system stock volatility.

	Dependent variable: Volatility									
	Visa		Mastercard		PayPal		American Express		Western Union	
r_{t-1}	-5.492***	-5.400***	-2.899*	-2.840*	-1.835	-1.815	-1.661	-1.660	-0.105	-0.137
	(1.747)	(1.747)	(1.631)	(1.633)	(1.385)	(1.388)	(1.666)	(1.666)	(1.858)	(1.861)
r_w	-12.564***	-12.676***	-14.804***	-14.728***	-1.358	-1.360	-14.106***	-14.147***	-10.786**	-10.868**
	(4.852)	(4.855)	(4.654)	(4.656)	(3.501)	(3.503)	(4.363)	(4.365)	(4.365)	(4.369)
r_m	-24.000**	-24.202**	-20.374*	-20.771**	1.887	1.923	-13.706	-13.635	-16.925*	-16.944*
	(11.513)	(11.518)	(10.520)	(10.533)	(8.520)	(8.526)	(9.507)	(9.515)	(8.903)	(8.906)
σ_{t-1}	0.161***	0.161***	0.111***	0.113***	0.035	0.035	0.098***	0.099***	0.121***	0.119***
	(0.034)	(0.034)	(0.037)	(0.037)	(0.041)	(0.041)	(0.037)	(0.037)	(0.036)	(0.036)
σ_w	0.202***	0.200***	0.122	0.116	0.294***	0.294***	0.314***	0.314***	0.171**	0.173**
	(0.070)	(0.070)	(0.080)	(0.081)	(0.092)	(0.092)	(0.074)	(0.074)	(0.073)	(0.074)
σ_m	0.446***	0.449***	0.576***	0.578***	0.531***	0.531***	0.350***	0.350***	0.478***	0.478***
	(0.069)	(0.069)	(0.081)	(0.081)	(0.092)	(0.092)	(0.078)	(0.078)	(0.085)	(0.085)
V_{t-1}	0.289***	0.288***	0.474***	0.473***	0.464***	0.463***	0.415***	0.415***	0.446***	0.448***
	(0.084)	(0.084)	(0.096)	(0.096)	(0.084)	(0.085)	(0.077)	(0.077)	(0.071)	(0.071)
V_w	0.132	0.132	0.060	0.061	-0.111	-0.112	-0.309**	-0.308**	-0.110	-0.113
	(0.135)	(0.135)	(0.146)	(0.146)	(0.142)	(0.142)	(0.126)	(0.127)	(0.126)	(0.126)
V_m	-0.332*	-0.338*	-0.119	-0.117	-0.269	-0.269	-0.199	-0.200	-0.632***	-0.635***
	(0.186)	(0.186)	(0.160)	(0.160)	(0.163)	(0.163)	(0.187)	(0.187)	(0.182)	(0.182)
LM_t	63.241	-271.265***	30.248	-184.294***	22.719	-22.641	77.109***	20.442	54.621*	-59.113
	(77.326)	(59.760)	(54.286)	(55.575)	(21.230)	(32.322)	(25.646)	(83.841)	(32.261)	(73.155)
$LM_t \cdot time$		0.319***		0.205***		0.067*		0.054		0.109*
		(0.044)		(0.046)		(0.037)		(0.066)		(0.057)
Constant	-1.799***	-1.789***	-1.781***	-1.791***	-1.237***	-1.238***	-2.272***	-2.268***	-2.121***	-2.122***
	(0.371)	(0.371)	(0.377)	(0.377)	(0.398)	(0.398)	(0.432)	(0.432)	(0.524)	(0.524)
N	1,469	1,469	1,469	1,469	1,088	1,088	1,469	1,469	1,469	1,469
R^2	0.354	0.356	0.339	0.340	0.310	0.310	0.279	0.279	0.216	0.216
Adj. R^2	0.350	0.351	0.334	0.335	0.304	0.303	0.274	0.274	0.210	0.210

The table presents time series regression results for the payment system stocks over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table B.3: The impact of cyberattacks on payment system stock trading volume.

	Dependent variable: Trading Volume									
	Visa		**Mastercard**		**PayPal**		**American Express**		**Western Union**	
r_{t-1}	-0.819	-0.800	-0.500	-0.495	-0.485	-0.474	-0.046	-0.044	-0.165	-0.141
	(0.701)	(0.702)	(0.620)	(0.621)	(0.604)	(0.605)	(0.739)	(0.739)	(0.806)	(0.807)
r_w	-2.997	-3.020	-2.185	-2.178	-0.692	-0.694	-2.616	-2.677	-2.314	-2.249
	(1.957)	(1.958)	(1.731)	(1.732)	(1.658)	(1.658)	(1.782)	(1.785)	(2.064)	(2.064)
r_m	-8.441*	-8.483*	-12.193***	-12.227***	-0.042	-0.022	-15.768***	-15.663***	0.814	0.829
	(4.622)	(4.624)	(4.154)	(4.156)	(4.370)	(4.373)	(4.214)	(4.215)	(4.066)	(4.066)
σ_{t-1}	0.025	0.025	0.033**	0.033**	0.015	0.015	-0.005	-0.004	0.017	0.018
	(0.016)	(0.016)	(0.014)	(0.014)	(0.019)	(0.019)	(0.017)	(0.017)	(0.018)	(0.018)
σ_w	-0.015	-0.016	-0.050*	-0.050*	-0.051	-0.051	-0.006	-0.006	-0.000	-0.001
	(0.029)	(0.029)	(0.030)	(0.030)	(0.040)	(0.040)	(0.032)	(0.032)	(0.034)	(0.035)
σ_m	-0.046	-0.045	-0.040	-0.040	-0.018	-0.018	-0.044	-0.043	-0.065*	-0.065*
	(0.029)	(0.029)	(0.029)	(0.029)	(0.042)	(0.042)	(0.032)	(0.032)	(0.038)	(0.038)
V_{t-1}	0.364***	0.364***	0.395***	0.395***	0.490***	0.490***	0.419***	0.418***	0.439***	0.438***
	(0.036)	(0.036)	(0.037)	(0.037)	(0.042)	(0.042)	(0.042)	(0.042)	(0.038)	(0.038)
V_w	0.213***	0.213***	0.264***	0.264***	0.203***	0.202***	0.154***	0.155***	0.106*	0.108*
	(0.057)	(0.057)	(0.056)	(0.056)	(0.061)	(0.061)	(0.059)	(0.059)	(0.060)	(0.060)
V_m	-0.377***	-0.378***	-0.286***	-0.286***	-0.288***	-0.288***	-0.371***	-0.372***	-0.330***	-0.328***
	(0.076)	(0.076)	(0.066)	(0.066)	(0.073)	(0.073)	(0.083)	(0.083)	(0.087)	(0.087)
LM_t	51.724*	-17.828	38.769**	20.300	22.197	-2.162	36.315	-47.960	24.059	114.074
	(28.955)	(70.821)	(18.761)	(60.206)	(14.136)	(21.643)	(26.760)	(55.031)	(19.551)	(86.035)
$LM_t \cdot time$		0.066		0.018		0.036		0.080**		-0.086
		(0.052)		(0.046)		(0.023)		(0.039)		(0.064)
Constant	-0.319**	-0.317**	-0.514***	-0.515***	-0.453**	-0.453**	-0.493***	-0.486**	-0.425*	-0.423*
	(0.155)	(0.155)	(0.147)	(0.147)	(0.192)	(0.192)	(0.190)	(0.190)	(0.229)	(0.229)
N	1,469	1,469	1,469	1,469	1,088	1,088	1,469	1,469	1,469	1,469
R^2	0.272	0.272	0.330	0.330	0.349	0.349	0.264	0.265	0.258	0.259
Adj. R^2	0.267	0.267	0.325	0.324	0.343	0.342	0.259	0.259	0.253	0.253

The table presents time series regression results for the payment system stocks over the period February 25, 2014 - December 31, 2019. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.