CESifo WORKING PAPERS

8124
2020

Original Version: February 2020
This Version: January 2021

Cyber-Attacks, Cryptocurrencies, and Cyber Security

Guglielmo Maria Caporale, Woo-Young Kang, Fabio Spagnolo, Nicola Spagnolo

CESifo

Impressum:

CESifo Working Papers
ISSN 2364-1428 (electronic version)
Publisher and distributor: Munich Society for the Promotion of Economic Research - CESifo GmbH
The international platform of Ludwigs-Maximilians University's Center for Economic Studies and the ifo Institute
Poschingerstr. 5, 81679 Munich, Germany
Telephone +49 (0)89 2180-2740, Telefax +49 (0)89 2180-17845, email office@cesifo.de
Editor: Clemens Fuest
https://www.cesifo.org/en/wp
An electronic version of the paper may be downloaded
· from the SSRN website: www.SSRN.com
· from the RePEc website: www.RePEc.org
· from the CESifo website: https://www.cesifo.org/en/wp

CESifo *Working Paper No. 8124*

Cyber-Attacks, Cryptocurrencies, and Cyber Security

Abstract

This paper provides comprehensive evidence on the effects of cyber-attacks (cyber-crime, cyber espionage, cyber warfare and hacktivism) and cyber security on the risk-adjusted returns, realised volatilities and trading volumes of the three main cryptocurrencies (Bitcoin, Ethereum and Litecoin). We find that stronger cyber security is generally effective in increasing the risk-adjusted returns of cryptocurrencies and trading activity even in the presence of cyber-attacks. Hacktivism appears to be the most significant threat to cryptocurrency investors. Further, cyber-attackers hitting the cryptocurrency exchanges are most likely to attack other sectors (government, industry and finance) as well. In addition, in the case of the US they target the government and industry sectors in preference to the cryptocurrency exchanges given the corresponding potential benefits and costs. In all cases appropriate strategies should be designed to enhance cyber security.

JEL-Codes: C220, E400, G100.

Keywords: cyber-attacks, cryptocurrencies, risk-adjusted returns, cyber security.

*Guglielmo Maria Caporale**
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
Guglielmo-Maria.Caporale@brunel.ac.uk

Woo-Young Kang
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
woo-young.kang@brunel.ac.uk

Fabio Spagnolo
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
fabio.spagnolo@brunel.ac.uk

Nicola Spagnolo
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
nicola.spagnolo@brunel.ac.uk

*corresponding author

January 2021

1. Introduction

Despite their rather recent introduction, cryptocurrencies have very rapidly become a widely used type of currency and also a favourite target for cyber criminals, hackers and fraudsters. The main reason is their vulnerability, which is a direct consequence of their anonymity resulting from highly encrypted blockchain technology, where blockchain is essentially "a decentralized network of synchronized online registries that track the ownership and value of each token" (see Matthews, 2017). This implies that the security of cryptocurrencies depends entirely on the blockchain algorithm being used. Since all transactions are recorded, they can be tracked down; however, they can be made anonymous by means of a so-called "tumbler" which exchanges the tokens. Further, there is no central authority responsible for cryptocurrencies.

An important issue in this context is the possible occurrence of a cyber-attack, which can be defined as an attack from one or more computers against other computers or networks aiming at disabling and/or managing the latter and obtaining access to information, thereby compromising its confidentiality, integrity and availability. This breach of security represents a form of cyber risk which has been found to be significant in the case of the financial sector (see Kopp et al., 2017). Such cyber threat can be detrimental to cryptocurrencies which are not regarded as similar to other standard assets and for which empirical evidence is limited (Liu and Tsyvinski, 2018).

The present study provides comprehensive evidence on the effects of cyber-attacks (using data collected from Hackmageddon, http://www.hackmageddon.com) and cyber security on the risk-adjusted returns, realised volatilities and trading volumes of the three main cryptocurrencies (Bitcoin, Ethereum and Litecoin). More specifically, it investigates the effects of four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare) on cryptocurrencies, four target sectors (cryptocurrency exchange, government, industry and finance), and 113 countries. Furthermore, it aims to investigate whether cyber-security attenuates those effects. Risk-adjusted returns (the return-to-risk ratio) are constructed using realised returns and weighted realised covariances as the return and risk components, respectively; this measure considers the systemic risk (correlation) and change in market capitalisations among cryptocurrencies in addition to each currency's own risk, which could all be affected by cyber-attacks. We estimate pooled ordinary least squares (OLS) regressions at the daily frequency over the period from 12 August 2015 to 28 February 2019; the model also includes appropriate control variables, namely stock market liquidity and financial market uncertainty. Further

regressions are run to identify the factors making specific sectors (cryptocurrency exchange, government, industry and finance) more prone to cyber-attacks and how they relate to cryptocurrencies and cyber security.

We find that cyber security is generally helpful for cryptocurrency investors in the presence of cyber-attacks since in most cases it increases their risk-adjusted returns and boosts their confidence and trading activities. Hacktivism represents the main threat for investors, cyber-attacks targeting cryptocurrency exchanges being the most likely to hit other sectors of the economy (i.e., government, industry and finance) as well. In the case of the US, government and industry sectors are less likely to be hit because of the high level of cyber security. This should be enhanced also in other sectors to provide a safer digital trading environment for (cryptocurrency) investors (van Hardeveld et al., 2017).

Our study contributes to the finance literature focusing on Fintech, which is still very limited despite widespread interest across the globe (Chen et al., 2019; Goldstein et al., 2019). Fintech includes seven categories: cybersecurity, mobile transactions, data analytics, blockchain, peer-to-peer (P2P), robo-advising and internet of things (IoT) (Chen et al., 2019).[1] Our analysis adds to the understanding of Fintech in its blockchain and cybersecurity aspects and extends the empirical asset pricing literature on cryptocurrencies.

The remainder of the paper is organised as follows. Section 2 reviews the relevant literature. Section 3 describes the data and the methodology. Section 4 presents the empirical results. Section 5 offers some concluding remarks.

2. Literature Review

Digital currencies, commonly known as cryptocurrencies, have established themselves in recent years both as an alternative to fiat money (see Yermack, 2018) and as a tradable asset used for risk-hedging purposes (see Bouri et al., 2017a, 2017c). Given their increasing importance, a number of studies have been carried out to analyse the main features of these newly created markets, including returns and risk (e.g., Balciar et al., 2017; Liu and Tsyvinski, 2018; Caporale and Zekokh, 2019), market efficiency (e.g., Urquhart, 2016; Bariviera, 2017; Nadarajah and Chu,

[1] Chen et al. (2019) define the peer-to-peer (P2P), robo-advising and Internet of things (IoT) as follows. Peer-to-peer (P2P): Software, systems, or platforms that facilitate consumer-to-consumer financial transactions. Robo-advising: Computer systems or programs that provide automated investment advice to customers or portfolio managers. Internet of things (IoT): Technologies relating to smart devices that gather data in real time and communicate via the internet.

2017) and anomalies (Caporale et al., 2018; Caporale and Plastun, 2019a, 2019b, 2019c), illegal activities (Foley et al., 2018, Li et al., 2018; Gandal et al., 2018; Griffin and Shams, 2018), hedging properties (e.g., Dyhrberg 2016a, 2016b; Baur et al., 2018; Bouri et al., 2017a, 2017b, 2017c), initial coin offerings (ICO) (Kostovetsky and Benedetti. 2018; Howell et al., 2018; Lee et al., 2018; Li and Mann, 2018; Malinova and Park, 2017; An et al., 2020), the effects of cyber-attacks (Caporale et al., 2019; An et al., 2020; Shanaev et al., 2020), and the economic implications of the emergence of this new type of asset (e.g., Böhme et al., 2015; Dwyer, 2015; Harvey, 2016; Raskin and Yermack 2016; Bariviera et al., 2017; Biais et al., 2018; Schilling and Uhlig 2018).

The impact of cyber-crime on cryptocurrency markets and the economy as a whole has been analysed in various recent papers. For instance, Benjamin et al. (2019) estimated that cyber-attacks from criminals operating in underground web communities such as Darknet have resulted in estimated annual losses of $445 billion for the global markets (see Graham, 2017). In another interesting study, Bouveret (2018) used a Value-at-Risk (VaR) framework to measure cyber risk and the resulting losses in a number of countries.

In the case of cryptocurrencies, given their distinctive features (see Corbet et al., 2019a) different methods are required to estimate and manage risk (see Platanakis and Urquhart, 2019). Cyber-attacks are considered a very important risk factor by both small and large "miners", whose task is to group unconfirmed transactions into new blocks and add them to the global ledger known as the "blockchain" (see Hileman and Rauchs, 2017). Benjamin et al. (2019) provided some evidence on the disruptions caused by cyber security breaches in the case of the cryptocurrency markets; these have also been targeted for the purpose of illicit online drug trading (see Martin, 2014), which has given rise to a number of ethical issues (see Martin and Christin, 2016). Shanaev et al. (2020) warned that if any individual or group of coin miners controls over 50% of the network mining, they can take over the chain, especially in the case of cryptocurrencies with small proof-of-work and low hash rates.

Caporale et al. (2019) used a Markov-switching non-linear specification to analyse the effects of cyber-attacks on returns in the case of four cryptocurrencies (Bitcoin, Ethereum, Litecoin and Stellar) over the period between 8 August 2015 and 28 February 2019. They found significant negative effects on the probability of cryptocurrencies staying in the low volatility regime. Corbet et al. (2019b) estimated a DCC-GARCH model and documented that

cryptocurrency hacks increase both the volatility of the currencies hacked and their correlations with other cryptocurrencies; further, they decrease price discovery for the hacked currencies in comparison to others. As for the effects on returns, abnormal ones are observed preceding the hack, which revert to zero when this is publicly announced. However, this research is limited to 17 hacking events on the cryptocurrency exchanges within less than a year.

Developing strategies to deal with and possibly prevent cyber-crime has therefore become very important (see van Hardeveld et al., 2017). In the case of the US, a specific concern has been the use of cryptocurrencies to avoid sanctions. It has been suggested that a task force including agencies from the Departments of the Treasury, State, Justice and Defence should be created to focus in particular on the cracking of blockchain cryptography to trace transactions (see Konowicz, 2018).

None of the above studies considers a wide range of cyber-attacks in different categories and their effects on the risk-adjusted returns and trading volumes of cryptocurrencies and various sectors in the presence of cyber security. The analysis below addresses all these issues using an appropriate empirical framework which yields informative new findings about the effectiveness of cyber security. and differences in the trading behaviour of Bitcoin, Ethereum and Litecoin investors when cyber-attacks occur.

3. Data and Methodology

3.1. Cryptocurrency data

We collect daily data on the closing prices and trading volumes for the three main cryptocurrencies (Bitcoin, Ethereum and Litecoin) over the period between 12 August 2015 and 28 February 2019 from the website www.CryptoDataDownload.com; this provides historical data for traded prices using the Application Programming Interface (API) service and is a reliable cryptocurrency data source as pointed out by Alexander and Dakos (2020). We choose five main exchanges (Bitfinex, Coinbase, Gemini, Kraken and Poloniex) that are common to the three cryptocurrencies under examination.[2] We then compute market capital-weighted indices

[2] The www.CryptoDataDownload.com website does not provide all the cryptocurrency exchanges for each country. Thus, we select from this source data for five major exchanges (the same as in Alexander and Dakos (2020)) in the US and the UK that are common to the three cryptocurrencies being examined (Bitcoin, Ethereum and Litecoin) and were available at the time when they were collected.

which are based on the five exchanges. The natural log returns are used for the estimation of the models. We show these in Figure 1.

[Insert Figure 1]

We use the cryptocurrency return and volume data to compute the return-to-risk ratio; it is essential to use risk-adjusted returns in the case of cryptocurrencies since they are more volatile than standard assets such as stocks and derivatives. As a risk measure, we consider the correlation (i.e., the systemic risk for cryptocurrencies) and change in the trading volumes of cryptocurrencies in addition to each cryptocurrency's own risk (i.e., volatility), which could all be affected by cyber-attacks. Therefore, we compute the risk-adjusted returns of cryptocurrencies as follows:

$$r_{i,t} = \frac{\mu_{i,t}}{\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}} \tag{1}$$

where the components are estimated as below:

$$\mu_{i,t} = \frac{1}{t}\left(ln\frac{P_{i,2}}{P_{i,1}} + ln\frac{P_{i,3}}{P_{i,2}} + \cdots + ln\frac{P_{i,t}}{P_{i,t-1}}\right) \tag{2}$$

$$w_t \times \sigma_t^{Rcov} \times w_t' \tag{3}$$

$$= \begin{pmatrix} w_{1,t} & w_{2,t} & w_{3,t} \end{pmatrix} \begin{pmatrix} \sigma_t^{1,1} & \sigma_t^{1,2} & \sigma_t^{1,3} \\ \sigma_t^{2,1} & \sigma_t^{2,2} & \sigma_t^{2,3} \\ \sigma_t^{3,1} & \sigma_t^{3,2} & \sigma_t^{3,3} \end{pmatrix} \begin{pmatrix} w_{1,t}' \\ w_{2,t}' \\ w_{3,t}' \end{pmatrix}$$

$$= \begin{pmatrix} \frac{P_{1,t} \times V_{1,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} & \frac{P_{2,t} \times V_{2,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} & \frac{P_{3,t} \times V_{3,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \end{pmatrix} \begin{pmatrix} \sigma_t^{1,1} & \sigma_t^{1,2} & \sigma_t^{1,3} \\ \sigma_t^{2,1} & \sigma_t^{2,2} & \sigma_t^{2,3} \\ \sigma_t^{3,1} & \sigma_t^{3,2} & \sigma_t^{3,3} \end{pmatrix} \begin{pmatrix} \frac{P_{1,t} \times V_{1,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \\ \frac{P_{2,t} \times V_{2,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \\ \frac{P_{3,t} \times V_{3,t}}{\sum_{i=1}^{3}(P_{i,t} \times V_{i,t})} \end{pmatrix}$$

$$\sigma_t^{i,j} = \frac{\sum_{t=1}^{t}\left(ln\left(\frac{P_{i,t}}{P_{i,t-1}}\right) \times ln\left(\frac{P_{j,t}}{P_{j,t-1}}\right)\right)}{t} \tag{4}$$

$\mu_{i,t}$ is the realised return, namely the time-varying drift coefficient of the stochastic differential equation we assume cryptocurrency *i* to follow at time *t* – this is the return component. $P_{i,t}$ is the price of cryptocurrency *i* at time *t*, $V_{1,t}$ is its trading volume of cryptocurrency *i* at time *t*, and $w_{i,t}$ $(= \frac{P_{i,t} \times V_{i,t}}{\sum_{i=1}^{N}(P_{i,t} \times V_{i,t})})$ its market capitalization $(P_{i,t} \times V_{i,t})$ weight across *N* different types of cryptocurrencies (where *i=1, ⋯, N*) at time *t*. *N* is equal to three in our case since our sample includes three cryptocurrencies, namely Bitcoin (*i* = 1), Ethereum (*i* = 2) and Litecoin (*i* = 3). w_t is a (*1* × *N*) vector whose elements are the volume weights $w_{i,t}$ of all three cryptocurrencies at time *t*. w_t' is a transpose of the vector w_t. $\sigma_t^{i,j}$ is the realised covariance between cryptocurrencies *i* and *j* at time *t*. σ_t^{Rcov} is the realised covariance at time *t* using all three cryptocurrencies' realised covariance $\sigma_t^{i,j}$ in a (*N* × *N*) matrix form. The resulting $\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}$ is used as the risk component. $r_{i,t}$ is the risk-adjusted return of cryptocurrency *i* at time *t*. We denote $\sqrt{w_t \times \sigma_t^{Rcov} \times w_t'}$ as $\sqrt{Rcov^w}$, and $r_{Bitcoin}$, $r_{Ethereum}$ and $r_{Litecoin}$ as *Bit_RAR*, *Eth_RAR* and *Lit_RAR*, respectively, throughout the paper.

3.2. Cyber-attack data

The recent developments in technology of networking and cyberspace, including cryptocurrencies using blockchain technology, have been highly beneficial. However, the rapid growth in these fields have also promoted unethical practices using these technologies to exploit others, which include cyber-attacks (Uma and Padmavathi, 2013). These are an attempt to damage, destroy or gain illegal access to a computer network or system (Bodford and Kwan, 2018).

The cyber-attack data are taken from the website http://www.hackmageddon.com/ which shows the cyber-attack timeline by target industry, country and cyber-attack type at a daily frequency. The Hackmageddon's cyber-attacks are collected from public sources such as blogs and news sites. Therefore, the sample collection cannot be complete, but it aims to provide a wide overview of the cyber-attack threat landscape across the globe (Passeri, 2020). We have collected data on 4006 daily cyber-attacks (including daily overlaps) from 12 August 2015 to 28 February 2019 for four target sectors, namely the government (*Gov*), industry (*Ind*), finance (*Fin*) and cryptocurrency exchange (*Crypto*) sectors, and created in each case binary variables equal to 1 for the sector affected and 0 for the others. Thus there are four cyber-attack binary variables,

namely cyber-crime (*CC*), cyber espionage (*CE*), hacktivism (*H*) and cyber warfare (*CW*), each being equal to 1 if the corresponding type of attack occurs and 0 otherwise. However, *CW* is dropped from the model to avoid the dummy variable trap. Since multiple cyber attacks may occur within a day, we use the added-up binary figures of these per day which shows the daily intensity in terms of cyber-attack target and type merging into 1157 daily cyber-attacks without daily overlaps in total.

According to Uma and Padmavathi (2013), cyber-crime can be defined as a criminal offence which involves a computer either as an object or a tool to commit a material component of the offence; cyber espionage is the cracking technique and malicious software (e.g., Trojan horses and spy ware) used to obtain information without the permission of the holder from individuals, groups and governments for gaining benefits through illegal abuse methods; cyber warfare is the use of computer technology to penetrate a nation's computer network in order to cause damage or disruption. Hacktivism is instead "the act of gaining access to (and control over) third-party computer systems" (Bodford and Kwan, 2018).

Figure 2 and 3 show, respectively, the cyber-attack targets and types considered in the analysis. It is apparent from Figure 2 that the industry sector (54.5%) is the most frequent target of cyber-attacks, which suggests that it is more vulnerable, compared to other sectors (e.g., government, financial and cryptocurrency exchange) that have stronger cyber security protections. In particular, the cryptocurrency exchanges appear to be the least targeted, presumably because their blockchain technology works effectively against cyber-attacks and this being a new sector hackers need time to learn how to attack it successfully.

Figure 3 shows that cyber-crime (77.6%) is the most frequent type of cyber-attack, and cyber warfare (3.2%) the least frequent; this is not surprising, since the latter is an attack on a nation's computer network and thus on a larger scale relative to other types of cyber-attacks. North America (United States and Canada), the UK and India have been the most frequently targeted by cyber-attacks of the 113 countries considered (Appendix II and III).[3] There were also 930 cyber-attacks targeting more than one country, which is the second most frequent case (see Appendix II); this is plausible since by their nature cyber-attacks are world-wide events without geographical restrictions.

[3] In Appendix II 'More than one country' and 'Unknown' country sources are dropped since they cannot be displayed as countries in Appendix III, where the darker shades indicate more frequent cyber-attacks per day in a given country.

[Insert Figure 2]

[Insert Figure 3]

3.3. Cyber security

As our cyber security measure we use the daily ISE (International Securities Exchange) Cyber Security Index from the Nasdaq Global Indexes available on the Bloomberg platform. The index started on 31 December 2010 with a base value of 100.00 and includes companies actively involved in providing cyber security technology and services. These must be a direct hardware/software developer or a service provider of cyber security with a minimum free float market capitalisation of $100 million and three-month average daily dollar trading volume of $1 million, and also to be listed on an eligible exchange as of the reference dates (i.e., at the end of January, April, July and October each year) with securities seasoned at least three calendar months. Therefore, the index provides a benchmark for companies developing hardware and/or software which protects access to files, websites and networks, both locally and from external origins, or companies that use these tools to provide consulting and/or cyber security services to their clients (Nasdaq Global Indexes, 2020).

3.4. Control variables

We use the daily liquidity (*Liq*) and change in global financial market uncertainty index (ΔVIX) as our financial market control variables. *Liq* is a percent-cost liquidity proxy which is based on daily data measured using the following *FHT* (Fong, Holden, and Trzcinka) method developed by Fong et al. (2017):

$$FHT \equiv S \equiv 2\sigma N^{-1}\left(\frac{1+z}{2}\right) \tag{5}$$

where

$$z \equiv Zeros \equiv \frac{ZRD}{TD + NTD} \tag{6}$$

$$N\left(\frac{S}{2\sigma}\right) - N\left(\frac{-S}{2\sigma}\right) = z \quad (7)$$

ZRD is the number of zero return days, TD is the number of trading days and NTD is the number of no-trade days in a given month. Further, S is the percentage transaction cost, $N^{-1}()$ is the inverse of the cumulative normal distribution function and σ is the standard deviation of the daily stock return over a month. Thus, Liq is the percent transaction cost S which is an increasing function of zero returns and the volatility of the return distribution (equation 5) based on the theoretical probability of a zero return being in the middle region of returns assumed to be normally distributed with zero mean and variance σ^2 (equation 7) (Fong et al., 2017). The stock prices for our sample countries are collected from Bloomberg in daily frequency. *VIX* is the Chicago Board Options Exchange (CBOE) volatility index also collected from Bloomberg. We use the daily percentage change (Δ) of this index as our global financial market uncertainty control variable.

3.5. Summary Statistics

Table 1 shows summary statistics for the series being analysed, namely cyber-attack target and types (Panel A), the financial market control variables (liquidity (*Liq*) and the change in global financial market uncertainty (Δ*VIX*) in Panel B), the cyber security index (*Cyber_Sec* in Panel B), and the logs of returns (*R*), realised return (*Mu*), realized volatility (*RV*), weighted realised covariance ($Rcov^w$), natural logarithm of trading volume (*V*) and risk-adjusted return (*RAR*) of the three cryptocurrencies under investigation (Bitcoin (Panel C), Ethereum (Panel D) and Litecoin (Panel E)) in daily frequencies. In panel F, we show the 96 stock indices used to obtain our country-specific liquidity variables for which we calculate the daily average if they belong to the same cyber-attack incident hitting multiple countries at once. The control variables (*Liq* and Δ*VIX*) are lagged by one year to avoid hindsight bias. We winsorise all variables at the 1st and 99th percentiles.

In most cases the distributions of cyber-attacks target and type data are positively skewed; the exception is cyber-crime (*CC*), which is negatively skewed. In other words, cyber-crime tends to occur very frequently on average relative to other types of cyber-attacks (*CE*, *CW* and *H*) or those targeting certain sectors (*Gov*, *Ind*, *Fin* and *Crypto*) or countries (*US*). We also find that in our sample liquidity, global financial market uncertainty (Δ*VIX*) and cyber security are

positively skewed. *Liq* is a unit-less, non-negative measure (Fong et al., 2017), most of its summary statistics having an absolute value much smaller than 1%, unlike the dependent variables which instead exceed 1% in most cases. Therefore, we use the scaled *Liq* measure multiplied by 100. On the other hand, the *Cyber_Sec* measure is a relatively large, non-negative three-digit global index which we scale by dividing by 100. Finally, ΔVIX is the daily percentage change in the *VIX* index which can be either positive or negative, with many absolute values larger than 1%, and it is not scaled.

We drop from the sample two cyber-attacks that targeted Belarus and Nepal since these two countries do not have an appropriate stock market index to calculate liquidity as above. Thus, we consider 96 countries market indices (Panel F) out of a total of 113 (Appendix II) with overlapping or non-existing stock indices to calculate country-specific liquidity. We find that Bitcoin exhibits the largest trading volume (*Bit_V*) and risk-adjusted returns (*Bit_RAR*) and Litecoin the lowest (*Lit_V* and *Lit_RAR*). The composite risks for the three cryptocurrencies under investigation, measured by the square root of weighted realised covariance ($\sqrt{Rcov^w}$), are generally high, which results in a negatively skewed distribution.

[Insert Table 1]

3.6. Cyber-attack effects associated with cryptocurrencies and cyber security

We analyse the effect of cyber-attacks on the risk-adjusted returns (RAR_t), realised volatility (RV_t) and trading volume (V_t) of cryptocurrencies and their relationship with cyber security ($Cyber\_Sec_t$). In particular, we analyse how cryptocurrencies are affected by cyber-attack targets (i.e., cryptocurrency exchange ($Cyber_{i,t}$), government ($Gov_{i,t}$), industry ($Ind_{i,t}$) and finance ($Fin_{i,t}$) sectors, and US versus non-US countries (US_t)), types (i.e., cyber-crime ($CC_{i,t}$), cyber-espionage ($CE_{i,t}$), cyber-warfare ($CW_{i,t}$) and hacktivism ($H_{i,t}$)) and cyber security ($Cyber\_Sec_t$) while controlling for the change in global financial market uncertainty (ΔVIX_t) and stock market liquidity ($Liq_{i,t}$) in country *i* at day *t* allowing multiple cyber-attacks to occur on a single day. ΔVIX_t represent the global financial uncertainty control variables and $Liq_{i,t}$ is the country-specific financial market control variable which we use the average value if there are multiple countries involved at day *t*. The cyber-attack target and types are binary variables equal to one if the cyber-

attack matches a given type or target and zero otherwise.[4] Our dataset includes multiple cyber-attack incidents within a single day. Therefore, we add up each of these binary variables within each day to obtain daily values which represent cyber-attack intensity measures without date overlaps. We estimate the following pooled OLS regressions, where the $u_{i,t}$ is the error term and *X* denotes in turn each of the three cryptocurrencies, Bitcoin (*Bit*), Ethereum (*Eth*) and Litecoin (*Lit*):

$$\begin{aligned} X\_RAR_t = {} & \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Gov_{i,t}) \\ & + \beta_5(Gov_{i,t} \times Cyber\_Sec_t) + \beta_6(Ind_{i,t}) + \beta_7(Ind_{i,t} \times Cyber\_Sec_t) + \beta_8(Fin_{i,t}) \\ & + \beta_9(Fin_{i,t} \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) \\ & + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \end{aligned} \quad (8)$$

$$\begin{aligned} X\_RV_t = {} & \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Gov_{i,t}) \\ & + \beta_5(Gov_{i,t} \times Cyber\_Sec_t) + \beta_6(Ind_{i,t}) + \beta_7(Ind_{i,t} \times Cyber\_Sec_t) + \beta_8(Fin_{i,t}) \\ & + \beta_9(Fin_{i,t} \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) \\ & + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \end{aligned} \quad (9)$$

$$\begin{aligned} X\_V_t = {} & \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Gov_{i,t}) \\ & + \beta_5(Gov_{i,t} \times Cyber\_Sec_t) + \beta_6(Ind_{i,t}) + \beta_7(Ind_{i,t} \times Cyber\_Sec_t) + \beta_8(Fin_{i,t}) \\ & + \beta_9(Fin_{i,t} \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) \\ & + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \end{aligned} \quad (10)$$

We then estimate the following regressions to analyse the factors making a given sector (i.e., $Crypto_{i,t}$, $Gov_{i,t}$, $Ind_{i,t}$ and $Fin_{i,t}$) a more frequent target for cyber-attacks:

$$\begin{aligned} Crypto_{i,t} = {} & \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Gov_{i,t}) + \beta_3(Gov_{i,t} \times Cyber\_Sec_t) + \beta_4(Ind_{i,t}) \\ & + \beta_5(Ind_{i,t} \times Cyber\_Sec_t) + \beta_6(Fin_{i,t}) + \beta_7(Fin_{i,t} \times Cyber\_Sec_t) + \beta_8(X\_RAR_t) \\ & + \beta_9(X\_RAR_t \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) \\ & + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \end{aligned} \quad (11)$$

[4] CW_t is not included to avoid the dummy variable trap.

$$Gov_{i,t} = \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Ind_{i,t}) + \beta_5(Ind_{i,t} \times Cyber\_Sec_t) + \beta_6(Fin_{i,t}) + \beta_7(Fin_{i,t} \times Cyber\_Sec_t) + \beta_8(X\_RAR_t) + \beta_9(X\_RAR_t \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \quad (12)$$

$$Ind_{i,t} = \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Gov_{i,t}) + \beta_5(Gov_{i,t} \times Cyber\_Sec_t) + \beta_6(Fin_{i,t}) + \beta_7(Fin_{i,t} \times Cyber\_Sec_t) + \beta_8(X\_RAR_t) + \beta_9(X\_RAR_t \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \quad (13)$$

$$Fin_{i,t} = \beta_0 + \beta_1(Cyber\_Sec_t) + \beta_2(Crypto_{i,t}) + \beta_3(Crypto_{i,t} \times Cyber\_Sec_t) + \beta_4(Gov_{i,t}) + \beta_5(Gov_{i,t} \times Cyber\_Sec_t) + \beta_6(Ind_{i,t}) + \beta_7(Ind_{i,t} \times Cyber\_Sec_t) + \beta_8(X\_RAR_t) + \beta_9(X\_RAR_t \times Cyber\_Sec_t) + \beta_{10}(CC_{i,t}) + \beta_{11}(CE_{i,t}) + \beta_{12}(H_{i,t}) + \beta_{13}(US_t) + \beta_{14}(H_{i,t}) + \beta_{15}(Liq_{i,t}) + \beta_{16}(\Delta VIX_t) + u_{i,t} \quad (14)$$

4. Empirical Results

Our aim is to analyse the effects of cyber-attacks on the risk-adjusted returns, realised volatility and trading volumes of three main cryptocurrencies (Bitcoin, Ethereum and Litecoin) accounting for the cyber security level while controlling for the underlying country-specific stock market liquidity and global uncertainty measure. We control for country and month (i.e., seasonality) effects in our analysis - in some countries, for instance, cyber-attacks may be likely to hit certain sectors (e.g., government[5] or financial institution[6]) more than other countries at different times. Furthermore, cyber-attacks may occur more frequently during holidays [7], tax [8] or presidential

[5] See Specops on 13 July 2020 available at https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/ (accessed on 12 January 2021).
[6] Baur-Yazbeck, S. (2018), 4 Cyber Attacks that Threaten Financial Inclusion, *CGAP*, available at https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion (accessed on 12 January 2021).
[7] See Surveillance and Security on 25 November 2014 available at https://www.retailtechnologyreview.com/articles/2014/11/25/lancope-protects-retailers-from-cyber-attacks-during-vulnerable-holiday-season/ (accessed on 12 January 2021).
[8] See TechWerxe on 27 February 2020 available at https://techwerxe.com/5-tips-to-keep-your-companys-data-safe-during-tax-season/ (accessed on 12 January 2021).

election [9] periods when agents are distracted by other events and therefore more vulnerable. There is no multicollinearity among the regressors according to the variance inflation factor (VIF) test whose value is less than 10 in all cases (see Appendix I).

4.1. Cyber-attack effects on the risk-adjusted returns of cryptocurrencies and cyber security

Table 3 suggests that stronger cyber security generally results in higher risk-adjusted returns of the cryptocurrencies under examination when cyber-attacks target different types of sectors. In their presence, the effects of cyber security remain the same except for the cryptocurrency exchanges (*Crypto* × *Cyber_Sec*) and the government sector (*Gov* × *Cyber_Sec*), where they are less pronounced especially in the case of Bitcoin (*Bit_RAR*) and Litecoin (*Lit_RAR*), but are still present since the sum of the relevant significant coefficients (*Cyber_Sec*, *Crypto* and *Gov*) and those on the corresponding interaction terms (*Crypto* × *Cyber_Sec* and *Gov* × *Cyber_Sec*) are still positive. On the other hand, the Ethereum' risk adjusted return (*Eth_RAR*) appears to be relatively immune to cyber-attacks on major sectors of the economy while cyber security still has a positive effect. Hacktivism (*H*) proves to be the most significant type of cyber-attack reducing the risk-adjusted returns, especially for Bitcoins.

Stock market liquidity (*Liq*) also tends to reduce the risk-adjusted returns of the cryptocurrencies under investigation. In a previous study, Wei (2018) showed that in the case of cryptocurrencies more liquidity decreases volatility as market efficiency improves. Our findings suggest that stock investors regard the cryptocurrency markets as a substitute for trading on the basis of their respective liquidities: as active cryptocurrency traders become less likely to arbitrage any signs of return predictabilities in less liquid cryptocurrency markets (Wei, 2018), the liquidity risk increases and so does volatility, leading to a decrease in the risk-adjusted returns of cryptocurrencies.

[Insert Table 3]

4.2. Cyber-attack effects on the realised volatilities of cryptocurrencies and cyber security

[9] Lam, C. (2018), A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election, Boston College Law Review, 59(6), pp. 2261 – 2201.

Table 4 shows that, in most cases, an increase in cyber security reduces the risk of cryptocurrencies (measured by their realised volatilities) in the presence of cyber-attacks. However, this is not the case when the government sector (*Gov* × *Cyber_Sec*) is targeted, the realised volatility of Bitcoin (*Bit_RV*) not being reduced. Hacktivism is the most significant variable increasing risk for all three cryptocurrencies considered. This is plausible as Android Trojans (which run on the Android operating system such as games, system updates or utilities[10]) can make attacks from hackers more effective by identifying crypto wallet owners and giving access to crypto wallets. Therefore, accordingly, cryptocurrencies are likely to be the main target for hackers specialising in web-based attacks (Group-IB, 2017). An increase in stock market liquidity (*Liq*) may lead more investors to trade stocks rather than cryptocurrencies, as argued before. Further, lower liquidity in the cryptocurrency markets can make it more difficult to arbitrage and exit trading positions in a timely manner and therefore which the realised volatility of cryptocurrencies will increase.

[Insert Table 4]

4.3. Cyber-attack effects on the trading volumes of cryptocurrencies and cyber security

In general, cryptocurrency investors become more confident and increase their trading when cyber security protection increases, even in the presence of cyber-attacks (Table 5). Cyber security (*Cyber_Sec*) provides less confidence to cryptocurrency investors when cyber-attacks hit the cryptocurrency exchanges (*Crypto* × *Cyber_Sec*) as opposed to other sectors, and therefore investors become risk-averse. Again hacktivism appears to have the most significant impact on the behaviour of cryptocurrency investors, making them risk-averse and reducing trading, especially in the case of Ethereum. Finally, an increase in *Liq* leads to reduced cryptocurrency trading, which confirms the substitution effect between stock and cryptocurrency markets on the basis of their respective liquidities.

[Insert Table 5]

4.4. Cyber-attack effects on different sectors, cryptocurrencies, and cyber security

[10] https://www.f-secure.com/en (Accessed 6 January 2021)

Tables 6 to 9 show how likely each sector (*Crypto, Gov*, *Ind* and *Fin*) in the economy is to be targeted by cyber-attacks for different levels of cyber security, cyber-attack types (*CC*, *CE*, *H* and *CW*) and targets, country (US versus non-US), cryptocurrency risk-adjusted returns and control variables (*Liq* and ΔVIX).

Overall, we find that cyber-attackers targeting cryptocurrency exchanges are most likely to divert to other sectors (i.e., *Gov*, *Ind* and *Fin*), as indicated by the estimated coefficients for *Crypto*. Cyber security is generally effective in reducing the likelihood of attacks only in the case of the industry sector, the only exception being the US, where it makes attacks to cryptocurrency exchanges less frequent and those to the government and industry sectors more frequent. This suggests that for cyber-attackers the benefits of successfully hitting the US government and industry sectors outweigh the costs and that the opposite holds for cryptocurrency exchanges (Tables 6, 7, 8 and 9).

The cybercriminals targeting cryptocurrency exchanges tend to be those attacking the financial sector (Table 6). This is plausible, as the main motivation for attacking either is likely to be monetary compared to other sectors which could also involve national security (*Gov*), classified information (*Gov*), customers profiles (*Ind*) and so on. Furthermore, as the risk-adjusted returns of cryptocurrencies increase (such as *Bit_RAR* and *Lit_RAR*), cryptocurrency exchanges can become a more attractive target for cyber-attack even in the presence of tighter cyber security (*Bit_RAR* × *Cyber_Sec* and *Lit_RAR* × *Cyber_Sec*). The increase in hacktivism frequency itself does not significantly increase the likelihood of cyber-attacks targeting the cryptocurrency exchanges (Table 6), although its impact on cryptocurrencies is significant once they are hit (as shown in section 4.1 and 4.3).

[Insert Table 6]

[Insert Table 7]

[Insert Table 8]

[Insert Table 9]

5. Conclusions

This paper sheds new light on the effects of cyber-attacks and cyber security on three of the main cryptocurrencies (Bitcoin, Ethereum, and Litecoin). It considers four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare) as well as four target sectors (cryptocurrency exchange, government, industry and finance). The cyber-attacks data are collected from Hackmageddon (http://www.hackmageddon.com), and risk-adjusted returns, realised volatilities and trading volumes of the cryptocurrencies under investigation are used for the analysis. The risk-adjusted returns are calculated using the realised return and weighted realised covariance as measures of return and risk, respectively. The factors making specific sectors (cryptocurrency exchange, government, industry and finance) more prone to cyber-attacks, and their relation to cryptocurrencies and cyber security, are also investigated.

Our findings suggest that stronger cyber security is generally effective in increasing the risk-adjusted returns of cryptocurrencies under examination and trading activities even in the presence of cyber-attacks. Hacktivism appears to be the most significant threat to cryptocurrency investors. Further, cyber-attackers hitting the cryptocurrency exchanges are most likely to attack other sectors (government, industry and finance) as well. In addition, in the case of the US they target the government and industry sectors in preference to the cryptocurrency exchanges given the corresponding potential benefits and costs. In all cases appropriate strategies should be designed to enhance cyber security (see, e.g., van Hardeveld et al., 2017). On the whole, the evidence provided in this paper represents useful information for the cryptocurrency investing community, cyber law enforcement agents, cyber-crime investigation units and other practitioners in addition to the academic community.

References

An, J., Duan, T., Hou, W. and Liu, X. (2020), Cyber Risks and Initial Coin Offerings: Evidence from the World, *Available at SSRN: https://ssrn.com/abstract=3604158*.

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

Bariviera, A., (2017), The inefficiency of bitcoin revisited: A dynamic approach, *Economic Letters*, 161, pp. 1–4.

Bariviera, A., Basgall, M., Hasperue, W. and Naiouf, M. (2017), Some stylized facts of the bitcoin market, *Physica A*, 484, pp. 82–90.

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

Benjamin, V., J.S. Valacich and Chen, H. (2019), DICE-E: a framework for conducting Darknet identification, collection, evaluation with ethics, *MIS Quarterly*, 43(1), pp. 1–22.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. and Menkveld, A.J. (2018), Equilibrium bitcoin pricing, *Toulouse School of Economics Working Papers*, No 18-973, 1–33.

Bodford, J.E. and Kwan, V.S.Y. (2018), A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs? *Cyberpsychology, Behavior and Social Networking*, 21(2), pp. 73–77.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), Bitcoin: Economics, technology, and governance, *Journal of Economic Perspectives*, 29(2), pp. 213–38.

Bouri, E., Gupta, R., Tiwari, A. and Roubaud, D. (2017a), Does bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions, *Finance Research Letters*, 23, pp. 87–95.

Bouri, E., Jalkh, N., Molnr, P. and Roubaud, D. (2017b), Bitcoin for energy commodities before and after the december 2013 crash: Diversifier, hedge or safe haven?, *Applied Economics*, 49(50), pp. 5063–5073.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D. and Hagfors, L.I. (2017c), On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier? *Finance Research Letters*, 20, pp. 192–198.

Bouveret, A. (2018), Cyber risk for the financial sector: a framework for quantitative assessment, *IMF Working Paper no. 18/143*.

Caporale, G.M., Luis-Alana, L. and A. Plastun (2018), Persistence in the cryptocurrency market, *Research in International Business and Finance*, 46, pp. 141–148.

Caporale, G.M., Kang, W-Y., Spagnolo, F. and Spagnolo, N. (2019), Non-linearities, cyber attacks and cryptocurrencies, *Finance Research Letters*, 7692. pp. 1–10.

Caporale, G.M. and A. Plastun (2019a), The day of the week effect in the crypto currency market, *Finance Research Letters*, 31, pp. 258–269.

Caporale, G.M. and A. Plastun (2019b), BitCoin fluctuations and the frequency of price overreactions, *Financial Markets and Portfolio Management*, 33, 2, pp. 109–131.

Caporale, G.M. and A. Plastun (2019c), Price overreactions in the cryptocurrency market, *Journal of Economic Studies*, 46, 5, pp. 1137–1155.

Caporale, G.M. and T. Zekokh (2019), Modelling volatility of cryptocurrencies using Markov-Switching GARCH models, *Research in International Business and Finance*, 48, 143-155.

Chen, M.A., Wu, Q. and Yang, B. (2019), How Valuable Is FinTech Innovation?, *The Review of Financial Studies*, 32(5), pp. 2062–2106.

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

Corbet, S., Cumming, D.J., Lucey, B.M., Peat, M. and Vigne, S.A. (2019b), Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in cryptocurrency Markets, *Available at SSRN: https://ssrn.com/abstract=3384707*.

Dwyer, G.P. (2015), The economics of Bitcoin and similar private digital currencies, *Journal of Financial Stability*, 17, pp. 81–91.

Dyhrberg, A. (2016a), Bitcoin, gold and the dollar - A GARCH volatility analysis, *Finance Research Letters*, 16, pp. 85–92.

Dyhrberg, A. (2016b), Hedging capabilities of bitcoin. Is it the virtual gold? *Finance Research Letters*, 16, pp. 139–144.

Foley, S., Karlsen, J. and Putninš, T.J. (2018), Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?, *Review of Financial Studies*, Forthcoming.

Fong, K.Y.L., Holden, C.W., and Trzcinka, C.A. (2017), What Are the Best Liquidity Proxies for Global Research? *Review of Finance*, 21(4), pp. 1355–1401.

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

Goldstein, I., Jiang, W. and Karolyi, G.A. (2019), To FinTech and Beyond, *The Review of Financial Studies*, 32(5), pp. 1647–1661.

Graham, L. (2017), Cybercrime costs the global economy $450 billion: CEO, *CNBC*, Available at http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global economy-450-billion-ceo.html.

Griffin, J. M. and Shams, A. (2018), Is bitcoin really un-tethered?, *Available at SSRN: https://ssrn.com/abstract=3195066.*

Group-IB. (2017), *Hi-Tech Crime Trends 2017*, Available at: https://www.group-ib.com/resources/threat-research/2017-report.html (Accessed 6 January 2021).

Harvey, C. (2016), "Cryptofinance", *Available at SSRN: https://ssrn.com/abstract=2438299.*

Hileman, G. and Rauchs, M. (2017), *Global Cryptocurrency Benchmarking Study*, Cambridge Centre for Alternative Finance, Judge Business School, University of Cambridge.

Howell, S. T., Niessner, M. and Yermack, D. (2018), Initial coin offerings: Financing growth with cryptocurrency token sales, *National Bureau of Economic Research, Working paper No. 24774.*

Konowicz, D.R. (2018), The New Game: Cryptocurrency Challenges US Economic Sanctions, Faculty of the United States Naval War College Newport, RI, mimeo.

Kopp, E., Kaffenberger, L. and Wilson, C. (2017), Cyber risk, market failures, and financial stability, *IMF Working Paper no. 17/185*.

Kostovetsky, L. and Benedetti, H. (2018), Digital tulips? returns to investors in initial coin offerings, *Available at SSRN: https://ssrn.com/abstract=3182169*.

Lee, D.K.C., Guo, L., Wang, Y., (2018), Cryptocurrency: a new investment opportunity?, *Journal of Alternative Investments*, 20 (3), pp. 16–40.

Li, J. and Mann, W. (2018), Initial coin offering and platform building" *Available at SSRN: https://ssrn.com/abstract=3088726.*

Li, T., Shin, D. and Wang, B. (2018), Cryptocurrency pump-and-dump schemes, *Available at SSRN: https://ssrn.com/abstract=3267041*.

Liu, Y. and Tsyvinski, A. (2018), Risks and returns of cryptocurrency, *NBER Working Paper No. 24877*, pp. 1–25.

Malinova, K. and Park, A. (2017), Market design with blockchain technology, *University College London, Working Paper*.

Martin, J. (2014), Lost on the Silk Road: online drug distribution and the cryptomarket, *Criminology and Criminal Justice*, 14(3), pp. 351–367.

Martin, J. and Christin, N. (2016), Ethics in cryptocurrency research, *International Journal of Drug Policy*, 35, pp. 84–91.

Matthews, O. (2017), Bitcoin and Blockchain: A Russian Money Laundering Bonanza? *Newsweek* (September 18, 2017).

Nadarajah, S. and Chu, J. (2017), On the inefficiency of Bitcoin, *Economics Letters*, 150, 6–9.
Passeri, P. (2020), June 2020 Cyber Attacks Statistics, accessed 16 August 2020, <https://www.hackmageddon.com/2020/08/13/june-2020-cyber-attacks-statistics>

Nasdaq Global Indexes. (2020), *ISE cyber security index (HXR) methodology*. Available at: https://indexes.nasdaqomx.com/docs/Methodology_HXR.pdf (Accessed 5 January 2021)

Platanakis, P. and Urquhart A. (2019), Portfolio Management with Cryptocurrencies: The Role of Estimation Risk, *Economics Letters*, 177, pp. 76–80.

Raskin, M. and Yermack, D. (2016), Digital currencies, decentralized ledgers, and the future of central banking, *National Bureau of Economic Research, Working paper No. 22238.*

Shanaev, S., Shuraeva, A., Vasenin, M. and Kuznetsov, M. (2020), Cryptocurrency value and 51% attacks: evidence from event studies, *Journal of Alternative Investments*, 22(3), pp. 65–77.

Schilling, L. and Uhlig, H. (2018), Some simple bitcoin economics, *Journal of Monetary Economics*, 106, pp. 16–26.

Uma, M. and Padmavathi, G. (2013), A Survey on Various Cyber Attacks and Their Classification, *International Journal of Network Security*, 15(5), pp. 390–396.

Urquhart, A. (2016), The inefficiency of bitcoin, *Economic 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), pp. 1244–1266.

Wei, W.C. (2018), Liquidity and market efficiency in cryptocurrencies, *Economics Letters*, 168, pp. 21–24.

Yermack, D. (2018), The potential of digital currency and blockchains, *NBER Reporter*, 1, pp. 14–17.

Table 1. Data description

Variable	Description
Gov	Cyber-attacks targeting the government sector. It shows 1 if it is a cyber-attack target and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
Ind	Cyber-attacks targeting the industry sector. It shows 1 if it is a cyber-attack target and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
Fin	Cyber-attacks targeting the financial sector. It shows 1 if it is a cyber-attack target and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
Crypto	Cyber-attacks targeting the cryptocurrency exchange sector. It shows 1 if it is a cyber-attack target and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
CC	Cyber-attack type of cyber crime. It shows 1 if the attack type is cyber crime and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
CE	Cyber-attack type of cyber espionage. It shows 1 if the attack type is cyber espionage and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
CW	Cyber-attack type of cyber warfare. It shows 1 if the attack type is cyber warfare and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
H	Cyber-attack type of hacktivism. It shows 1 if the attack type is hacktivism and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
US	Cyber-attack targeting the United States. It shows 1 if the cyber-attack targets US and 0 otherwise, which may happen multiple times per day. We use the added-up figures of these per day which also shows the daily intensity.
Bit_R	Bitcoin's log returns
Eth_R	Ethereum's log returns
Lit_R	Litecoin's log returns
Bit_Mu	Bitcoin's realised return
Eth_Mu	Ethereum's realised return

Lit_Mu	Litecoin's realised return
Bit_RV	Bitcoin's realised volatility
Eth_RV	Ethereum's realised volatility
Lit_RV	Litecoin's realised volatility
Bit_V	Natural logarithm of Bitcoin's volume
Eth_V	Natural logarithm of Ethereum's volume
Lit_V	Natural logarithm of Litecoin's volume
$Rcov^{w}$	Weighted realised covariance computed using Bitcoin, Ethereum and Litecoin.
Bit_RAR	Bitcoin's risk-adjusted return ($= \frac{Bit\_Mu}{\sqrt{Rcov^{w}}}$)
Eth_RAR	Ethereum's risk-adjusted return ($= \frac{Eth\_Mu}{\sqrt{Rcov^{w}}}$)
Lit_RAR	Litecoin's risk-adjusted return ($= \frac{Lit\_Mu}{\sqrt{Rcov^{w}}}$)
Cyber_Sec	The ISE (International Securities Exchange) Cyber Security Index is our cyber security measure collected from Nasdaq Global Indexes through Bloomberg. We use the daily figure of this index which is comprised of companies actively involved in providing cyber security technology and services.
Liq	The liquidity measure computed using the stock index of the country hit by a cyber-attack. We take the average liquidity across the countries hit within the same day.
VIX	Chicago Board Options Exchange (CBOE) volatility index

Notes: Data covers the period from 12 August 2015 to 28 February 2019.

Table 2. Summary statistics

The following table shows summary statistics for cyber-attack target and types (Panel A), the underlying liquidity, block chain's hash rate, global financial market uncertainty and investor protection (Panel B), and three cryptocurrencies including Bitcoin, Ethereum and Litecoin where *Bit*, *Eth* and *Lit* denote Bitcoin (Panel C), Ethereum (Panel D) and Litecoin (Panel E), respectively. *_R*, *_Mu*, *_RV*, *_V* and *_RAR* stand for log return, realised return, realised volatility, natural logarithm of trading volume and risk-adjusted return for the daily cryptocurrency data in turn (e.g., *Bit_R* indicates log returns in the case of Bitcoin). $\sqrt{Rcov^{w}}$ is the square root of weighted realised covariance computed using Bitcoin, Ethereum and Litecoin. The data for cyber-attacks, liquidity, hash rate and the five cryptocurrencies are daily and span the period from 12 August, 2015 to 28 February, 2019; they have been collected from http://www.hackmageddon.com, Bloomberg and www.CryptoDataDownload.com. The *Gov* (government sector), *Ind* (industry sector), *Fin* (financial sector), *Crypto* (cryptocurrency exchange) and *US* (United States) series are binary variables equal to one if the cyber-attack targets these sectors or country, and zero otherwise. The *CC* (cyber-crime), *CE* (cyber-espionage), *H* (hacktivism) and *CW* (cyber-warfare) binary variable are equal to one if they match the cyber-attack type and zero otherwise. For all binary variables, we use the added-up figures per day as cyber-attacks may happen multiple times within a day. *Liq* is a liquidity measure computed using the stock index of the country hit by a cyber-attack. In the case of cyber-attacks targeting multiple countries the average liquidity measure across those countries is used. Δ*VIX* is the Chicago Board Options Exchange (CBOE) volatility index in daily percentage change to proxy the uncertainty in the global financial market. *Cyber_Sec* is the cyber security index collected from Bloomberg. We winsorise all variables at the 1st and 99th percentiles. We report the mean, median, std (standard deviation), Min (minimum), 25th (25th percentile), 75th (75th percentile), Max (maximum) and *N* (number of observations) of each variable, as well as the list of countries with the corresponding market indices included in our sample (Panel F).

Panel A. Cyber-attacks targets and types									
	Gov	*Ind*	*Fin*	*Crypto*	*CC*	*CE*	*CW*	*H*	*US*
Mean	0.47	0.88	0.19	0.08	2.67	0.40	0.10	0.25	1.31
Median	0.68	0.98	0.44	0.27	1.84	0.62	0.30	0.52	1.19
Std.	0.00	1.00	0.00	0.00	2.00	0.00	0.00	0.00	1.00
Min	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
25th	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
75th	1.00	1.00	0.00	0.00	4.00	1.00	0.00	0.00	2.00
Max	3.00	4.00	2.00	1.00	8.00	2.00	1.00	2.00	5.00
N	1157	1157	1157	1157	1157	1157	1157	1157	1157

Panel B. Liquidity, hash rate, global financial market uncertainty and investor protection			
	Liq	Δ*VIX*	*Cyber_Sec*
Mean	0.57	0.03%	2.92
Median	0.25	0.00%	0.55

Std.	0.51	6.42%	2.81
Min	0.20	-16.85%	2.00
25th	0.39	-2.91%	2.50
75th	0.70	1.95%	3.43
Max	1.42	25.47%	4.04
N	1149	1157	1157

Panel C. Bitcoin and $\sqrt{Rcov^{w}}$

	Bit_R	*Bit_Mu*	$\sqrt{Bit\_RV}$	*Bit_V*	*Bit_RAR*	$\sqrt{Rcov^{w}}$
Mean	0.17%	0.19%	4.58%	17.02	5.12%	3.79%
Median	0.23%	0.18%	4.53%	17.12	5.14%	3.81%
Std.	3.67%	0.05%	0.23%	1.74	1.26%	0.39%
Min	-11.30%	0.09%	4.29%	14.04	2.25%	2.54%
25th	-1.09%	0.15%	4.40%	15.45	4.14%	3.55%
75th	1.67%	0.24%	4.65%	18.42	6.07%	4.18%
Max	10.55%	0.32%	5.26%	20.30	8.36%	4.29%
N	1157	1157	1157	1157	1156	1156

Panel D. Ethereum

	Eth_R	*Eth_Mu*	$\sqrt{Eth\_RV}$	*Eth_V*	*Eth_RAR*
Mean	0.34%	0.11%	9.83%	14.69	1.65%
Median	-0.05%	0.41%	8.61%	16.30	10.54%
Std.	6.71%	1.04%	3.12%	3.79	31.99%
Min	-19.34%	-5.80%	7.49%	4.19	-228.23%
25th	-2.87%	0.28%	8.04%	12.63	7.22%
75th	3.36%	0.56%	10.63%	17.73	14.70%
Max	19.92%	0.69%	26.61%	19.53	19.54%
N	1157	1157	1157	1157	1156

Panel E. Litecoin

	Lit_R	*Lit_Mu*	$\sqrt{Lit\_RV}$	*Lit_V*	*Lit_RAR*
Mean	0.14%	0.12%	9.75%	13.43	3.11%
Median	-0.09%	0.13%	9.27%	14.91	3.16%
Std.	5.38%	0.11%	1.13%	3.67	2.72%
Min	-15.93%	-0.04%	8.49%	3.64	-1.11%
25th	-2.13%	0.02%	9.03%	10.52	0.58%
75th	2.14%	0.22%	10.41%	16.32	5.87%
Max	21.68%	0.33%	12.95%	19.21	8.65%
N	1157	1157	1157	1157	1156

Panel F: Countries and market indices

Country	**Market indices**
Australia	S&P/ASX 200 INDEX
Greece	Athex Composite Share Price Index
Barbados	Barbados Exchange Comp

Belgium	BEL 20 INDEX
Romania	BUCHAREST BET INDEX
Bahrain	BB ALL SHARE INDEX
Bosnia and Herzegovina	Bosnia BIRS Index
Lebanon	BLOM STOCK INDEX
Iran	TEHRAN STOCK EXCHANGE
Hungary	BUDAPEST STOCK EXCH INDX
Panama	Bolsa de Panama General
Colombia	COLOMBIA COLCAP INDEX
Costa Rica	BCT Corp Costa Rica Index
Sri Lanka	SRI LANKA COLOMBO ALL SH
Cambodia	Cambodia SE Comp Index
Cyprus	GENERAL MARKET INDEX CSE
Tanzania	Tanzania Share Index
United Arab Emirates	DFM GENERAL INDEX
Bangladesh	DSE Broad Index
Syrian Arab Republic	DSE Weighted Index
Ecuador	ECUINDEX
Egypt	EGX 30 INDEX
Malaysia	FTSE BURSA MAL TOP 100
Kenya	FTSE NSE Kenya 25
Namibia	NAMIBIA OVERALL INDEX
Italy	FTSE MIB INDEX
Spain	IBEX 35 INDEX
Iceland	OMX Iceland All-Share PR
Russian Federation	MOEX Russia Index
Chile	S&P/CLX IPSA (CLP) TR
Iraq	ISX GENERAL INDEX
South Africa	FTSE/JSE AFRICA ALL SHR
Indonesia	JAKARTA COMPOSITE INDEX
Jordan	AMMAN SE GENERAL INDEX
Pakistan	KARACHI 100 INDEX
Kuwait	KWSE All Share
Malta	MALTA STOCK EXCHANGE IND
Maldives	Maldives Stock Exch Indx
Argentina	S&P MERVAL TR ARS
Mongolia	MSE Top 20 Index
Oman	MSM30 Index
Nigeria	NIGERIA STCK EXC ALL SHR
New Zealand	S&P NZX All Index
Philippines	PSEi - PHILIPPINE SE IDX
Palestine	PEX Genral Index
Puerto Rico	GDB PUERTO RICO STOCK IX
Portugal	PSI 20 INDEX
Rwanda	Rwanda St Ex Share Index
Slovakia	SLOVAK SHARE INDEX
Switzerland	SWISS MARKET INDEX
Fiji	SPSE Market Cap Wgt TR
European Union	Euro Stoxx 50 Pr
Estonia	OMX TALLINN OMXT
Trinidad and Tobago	TRINIDAD&TOBAGO CMPOSITE

Tunisia	Tunis SE TUNINDEX
Uganda	USE LSI Index
Virgin Islands	FTSE 100 INDEX
Lithuania	OMX VILNIUS OMXV
Vietnam	HO CHI MINH STOCK INDEX
Zimbabwe	Zimbabwe All Share Index
Austria	AUSTRIAN TRADED ATX INDX
Australia	S&P/ASX 200 INDEX
Brazil	BRAZIL IBOVESPA INDEX
Canada	S&P/TSX COMPOSITE INDEX
China	CSI 300 INDEX
Czech Republic	PRAGUE STOCK EXCH INDEX
Germany	DAX INDEX
Denmark	OMX COPENHAGEN 20 INDEX
Finland	OMX HELSINKI 25 INDEX
France	CAC 40 INDEX
Hong Kong	HANG SENG INDEX
Ireland	IRISH OVERALL INDEX
Israel	TA-125 Index
India	S&P BSE SENSEX INDEX
Italy	FTSE MIB INDEX
Japan	NIKKEI 225
Korea (South)	KOSPI INDEX
Kazakhstan	Kazakhstan KASE Stock Ex
Luxembourg	LUXEMBOURG LuxX INDEX
Montenegro	MONEX INDEX
Mexico	S&P/BMV IPC
Netherlands	AEX-Index
Norway	OBX STOCK INDEX
Poland	WSE WIG INDEX
Qatar	QE Index
Russian Federation	MICEX INDEX
Saudi Arabia	TADAWUL ALL SHARE INDEX
Sweden	OMX STOCKHOLM 30 INDEX
Singapore	Straits Times Index STI
Thailand	STOCK EXCH OF THAI INDEX
Turkey	BIST 100 INDEX
Taiwan	TAIWAN TAIEX INDEX
Ukraine	PFTS Index
United Kingdom	FTSE 100 INDEX
United States of America	DOW JONES INDUS. AVG
Venezuela	VENEZUELA STOCK MKT INDX

Table 3. Effects of cyber-attacks on cryptocurrencies' risk-adjusted returns

The following tables present the pooled OLS regression results using the cryptocurrency's risk-adjusted return (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) as a dependent variable affected by cyber security (*Cyber_Sec*) while having cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CW, H*) and US target (*US*) while controlling for global financial market uncertainty change (ΔVIX) and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Bit_RAR		*Eth_RAR*		*Lit_RAR*	
	(1)		(2)		(3)	
Intercept	0.039***	0.063***	-0.325	0.053	-0.07***	0.04*
	(0.011)	(0.011)	(0.344)	(0.348)	(0.023)	(0.023)
Cyber_Sec	0.006***	0.006***	0.14***	0.121***	0.035***	0.035***
	(0.001)	(0.001)	(0.019)	(0.021)	(0.001)	(0.001)
Crypto		0.003**		0.029		0.008***
		(0.001)		(0.043)		(0.003)
Crypto × *Cyber_Sec*		-0.004**		-0.063		-0.013***
		(0.002)		(0.07)		(0.005)
Gov		0.001		-0.008		-0.0005
		(0.001)		(0.017)		(0.001)
Gov × *Cyber_Sec*		-0.002**		-0.002		-0.002
		(0.001)		(0.028)		(0.002)
Ind		0.0002		-0.014		0.0003
		(0)		(0.013)		(0.001)
Ind × *Cyber_Sec*		0.0001		-0.002		0
		(0.001)		(0.018)		(0.001)
Fin		-0.0003		0.006		0.001
		(0.001)		(0.025)		(0.002)
Fin × *Cyber_Sec*		-0.002		-0.043		-0.004
		(0.001)		(0.039)		(0.003)
CC		-0.0002		0.016		-0.0002
		(0)		(0.009)		(0.001)
CE		0.0001		0.002		0.001
		(0.001)		(0.018)		(0.001)
H		-0.002***		-0.019		-0.003*
		(0.001)		(0.022)		(0.001)

US		-0.001		-0.019		-0.001
		(0)		(0.013)		(0.001)
Liq	-0.026***	-0.025***	-0.59***	-0.589***	-0.027***	-0.026***
	(0.001)	(0.001)	(0.043)	(0.043)	(0.003)	(0.003)
Δ*VIX*	-0.002	-0.004	-0.02	-0.048	0.004	0.001
	(0.005)	(0.005)	(0.157)	(0.159)	(0.011)	(0.011)
Month fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.32	0.33	0.30	0.30	0.48	0.49
F-stats	11.1***	9.55***	10.41***	8.60***	21.35***	17.91***
N	1148	1148	1148	1148	1148	1148

Table 4. Effects of cyber-attacks on cryptocurrency's realised volatility

The following tables present the pooled OLS regression results using the cryptocurrency's realised volatility (*Bit_RV*, *Eth_RV*, *Lit_RV*) as a dependent variable affected by cyber security (*Cyber_Sec*) while having cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CW, H*) and US target (*US*) while controlling for global financial market uncertainty change (ΔVIX) and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Bit_RV (1)		*Eth_RV* (2)		*Lit_RV* (3)	
Intercept	0.051***	0.046***	0.19***	0.098***	0.147***	0.1***
	(0.002)	(0.002)	(0.023)	(0.023)	(0.007)	(0.007)
Cyber_Sec	-0.001***	-0.001***	-0.03***	-0.029***	-0.015***	-0.014***
	(0)	(0)	(0.001)	(0.001)	(0)	(0)
Crypto		0.0001		-0.002		-0.0003
		(0)		(0.003)		(0.001)
Crypto × *Cyber_Sec*		0.001		0.006		0.002
		(0)		(0.005)		(0.001)
Gov		-0.0002**		-0.002		-0.001*
		(0)		(0.001)		(0)
Gov × *Cyber_Sec*		0.0003**		0.002		0.001*
		(0)		(0.002)		(0.001)
Ind		0.0001		0.001		0.0003
		(0)		(0.001)		(0)
Ind × *Cyber_Sec*		-0.0001		-0.0001		-0.0002
		(0)		(0.001)		(0)
Fin		0		-0.001		0
		(0)		(0.002)		(0)
Fin × *Cyber_Sec*		0.0003		0.004		0.001*
		(0)		(0.003)		(0.001)
CC		0		-0.001		0
		(0)		(0.001)		(0)
CE		0		0		0
		(0)		(0.001)		(0)
H		0.001***		0.003**		0.002***
		(0)		(0.001)		(0)

US		0.0001*		0.001		0.0003
		(0)		(0.001)		(0)
Liq	0.005***	0.005***	0.045***	0.045***	0.015***	0.015***
	(0)	(0)	(0.003)	(0.003)	(0.001)	(0.001)
Δ*VIX*	0.0004	0.001	0.007	0.009	0.001	0.002
	(0.001)	(0.001)	(0.01)	(0.011)	(0.003)	(0.003)
Month fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.41	0.43	0.48	0.48	0.66	0.67
F-stats	16.29***	14.28***	21.28***	17.57***	43.63***	36.67***
N	1148	1148	1148	1148	1148	1148

Table 5. Effects of cyber-attacks on cryptocurrency's trading volume

The following tables present the pooled OLS regression results using the cryptocurrency's trading volume (*Bit_V, Eth_V, Lit_V*) as a dependent variable affected by cyber security (*Cyber_Sec*) while having cyber-attack target sectors (*Gov, Ind, Fin, Crypto*), types (*CC, CW, H*) and US target (*US*) while controlling for global financial market uncertainty change (Δ*VIX*) and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Bit_V (1)		*Eth_V* (2)		*Lit_V* (3)	
Intercept	10.952***	17.2***	0.16	14.271***	1.006	14.991***
	(1.248)	(1.257)	(2.445)	(2.45)	(2.551)	(2.569)
Cyber_Sec	2.149***	2.117***	4.579***	4.372***	4.64***	4.557***
	(0.068)	(0.076)	(0.134)	(0.147)	(0.14)	(0.155)
Crypto		0.434***		0.734**		0.716**
		(0.157)		(0.305)		(0.32)
Crypto × Cyber_Sec		-0.553**		-1.184**		-1.389***
		(0.252)		(0.491)		(0.515)
Gov		-0.085		-0.037		-0.134
		(0.062)		(0.121)		(0.127)
Gov × Cyber_Sec		0.037		-0.195		-0.047
		(0.1)		(0.196)		(0.205)
Ind		0.026		-0.106		-0.001
		(0.045)		(0.089)		(0.093)
Ind × Cyber_Sec		-0.013		0.098		0.069
		(0.066)		(0.128)		(0.134)
Fin		0.048		0.011		0.059
		(0.091)		(0.177)		(0.185)
Fin × Cyber_Sec		-0.161		-0.46*		-0.383
		(0.142)		(0.276)		(0.29)
CC		0.011		0.064		0.009
		(0.034)		(0.066)		(0.069)
CE		0.077		0.1		0.085
		(0.066)		(0.129)		(0.135)
H		-0.017		-0.483***		-0.223
		(0.08)		(0.156)		(0.164)

US		-0.023		-0.065		-0.054
		(0.048)		(0.094)		(0.098)
Liq	-0.794***	-0.758***	-3.933***	-3.791***	-1.294***	-1.184***
	(0.155)	(0.157)	(0.303)	(0.306)	(0.316)	(0.321)
Δ*VIX*	0.598	0.569	0.447	0.13	1.578	1.403
	(0.57)	(0.576)	(1.116)	(1.122)	(1.165)	(1.176)
Month fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.51	0.51	0.60	0.61	0.54	0.54
F-stats	23.52***	19.48***	33.76***	28.32***	25.92***	21.47***
N	1148	1148	1148	1148	1148	1148

Table 6. Cryptocurrency exchange sector targeted by cyber-attacks

The following table presents the pooled OLS regression results showing the determinants of cyber-attacks targeting the cryptocurrency exchange (*Crypto*). The independent variables include cyber security (*Cyber_Sec*), other cyber-attack targets (*Gov*, *Ind*, *Fin*), types (*CC*, *CW*, *H*), countries (*US*) and cryptocurrency's risk-adjusted return (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) while controlling for global financial market uncertainty change (Δ*VIX*), and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Crypto (1)	*Crypto* (2)	*Crypto* (3)
Intercept	-0.159	-0.146	-0.154
	(0.266)	(0.267)	(0.266)
Cyber_Sec	0.063***	0.028	0.016
	(0.02)	(0.019)	(0.02)
Gov	-0.033**	-0.035***	-0.033**
	(0.013)	(0.013)	(0.013)
Gov × *Cyber_Sec*	0.002	0.002	0.002
	(0.021)	(0.021)	(0.021)
Ind	-0.05***	-0.049***	-0.049***
	(0.01)	(0.01)	(0.01)
Ind × *Cyber_Sec*	-0.022	-0.02	-0.021
	(0.014)	(0.014)	(0.014)
Fin	-0.067***	-0.065***	-0.066***
	(0.019)	(0.019)	(0.019)
Fin × *Cyber_Sec*	-0.013	-0.018	-0.016
	(0.03)	(0.03)	(0.03)
Bit_RAR	0.684		
	(0.72)		
Bit_RAR × *Cyber_Sec*	5.558***		
	(1.881)		
Eth_RAR		0.038	
		(0.046)	
Eth_RAR × *Cyber_Sec*		0.101	
		(0.131)	
Lit_RAR			0.778**

			(0.358)
Lit_RAR × Cyber_Sec			2.261**
			(1.02)
CC	0.042***	0.041***	0.041***
	(0.007)	(0.007)	(0.007)
CE	0.029***	0.029**	0.029**
	(0.014)	(0.014)	(0.014)
H	0.023	0.026	0.023
	(0.017)	(0.017)	(0.017)
US	-0.029***	-0.028***	-0.028***
	(0.01)	(0.01)	(0.01)
Liq	-0.062	-0.051	-0.059
	(0.04)	(0.036)	(0.036)
Δ*VIX*	0.118	0.118	0.119
	(0.122)	(0.122)	(0.122)
Month fixed effect	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes
Adjusted R^2	0.06	0.05	0.06
F-stats	2.14***	1.97***	2.1***
N	1148	1148	1148

Table 7. Government sector targeted by cyber-attacks

The following table presents the pooled OLS regression results showing the determinants of cyber-attacks targeting the government sector (*Gov*). The independent variables include cyber security (*Cyber_Sec*), other cyber-attack targets (*Crypto*, *Ind*, *Fin*), types (*CC*, *CW*, *H*), countries (*US*) and cryptocurrency's risk-adjusted return (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) while controlling for global financial market uncertainty change (Δ*VIX*), and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Gov (1)	*Gov* (2)	*Gov* (3)
Intercept	-0.89	-0.931	-0.891
	(0.614)	(0.615)	(0.614)
Cyber_Sec	-0.033	-0.019	0.028
	(0.045)	(0.046)	(0.046)
Crypto	-0.224***	-0.23***	-0.221***
	(0.077)	(0.076)	(0.077)
Crypto × *Cyber_Sec*	0.184	0.174	0.178
	(0.123)	(0.123)	(0.124)
Ind	-0.159***	-0.161***	-0.16***
	(0.022)	(0.022)	(0.022)
Ind × *Cyber_Sec*	0.026	0.025	0.026
	(0.032)	(0.032)	(0.032)
Fin	-0.215***	-0.22***	-0.217***
	(0.044)	(0.044)	(0.044)
Fin × *Cyber_Sec*	0.109	0.111	0.109
	(0.069)	(0.069)	(0.069)
Bit_RAR	1.762		
	(1.663)		
Bit_RAR × *Cyber_Sec*	-6.933		
	(4.36)		
Eth_RAR		0.066	
		(0.106)	
Eth_RAR × *Cyber_Sec*		0.298	
		(0.302)	
Lit_RAR			-0.653

			(0.831)
Lit_RAR × *Cyber_Sec*			-3.637 (2.36)
CC	0.063***	0.065***	0.064***
	(0.016)	(0.016)	(0.016)
CE	0.342***	0.342***	0.342***
	(0.031)	(0.031)	(0.031)
H	0.344***	0.338***	0.343***
	(0.038)	(0.038)	(0.038)
US	0.125***	0.122***	0.123***
	(0.023)	(0.023)	(0.023)
Liq	0.049	-0.059	-0.003
	(0.092)	(0.084)	(0.083)
Δ*VIX*	0.073	0.07	0.058
	(0.282)	(0.282)	(0.282)
Month fixed effect	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes
Adjusted R^2	0.06	0.05	0.06
F-stats	0.24***	0.24***	0.24***
N	1148	1148	1148

Table 8. Industry sector targeted by cyber-attacks

The following table presents the pooled OLS regression results showing the determinants of cyber-attacks targeting the industry sector (*Ind*). The independent variables include cyber security (*Cyber_Sec*), other cyber-attack targets (*Crypto*, *Gov*, *Fin*), types (*CC*, *CW*, *H*), countries (*US*) and cryptocurrency's risk-adjusted return (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) while controlling for global financial market uncertainty change (ΔVIX), and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Ind (1)	*Ind* (2)	*Ind* (3)
Intercept	-0.731	-0.728	-0.714
	(0.842)	(0.842)	(0.842)
Cyber_Sec	-0.17***	-0.201***	-0.207***
	(0.062)	(0.061)	(0.063)
Crypto	-0.549***	-0.538***	-0.544***
	(0.104)	(0.104)	(0.104)
Crypto × *Cyber_Sec*	0.159	0.153	0.163
	(0.169)	(0.169)	(0.17)
Gov	-0.296***	-0.298***	-0.297***
	(0.041)	(0.041)	(0.041)
Gov × *Cyber_Sec*	-0.043	-0.043	-0.043
	(0.067)	(0.067)	(0.067)
Fin	-0.317***	-0.315***	-0.315***
	(0.06)	(0.06)	(0.06)
Fin × *Cyber_Sec*	-0.053	-0.062	-0.057
	(0.095)	(0.095)	(0.095)
Bit_RAR	0.757		
	(2.285)		
Bit_RAR × *Cyber_Sec*	4.872		
	(5.979)		
Eth_RAR		-0.006	
		(0.146)	
Eth_RAR × *Cyber_Sec*		0.251	
		(0.413)	
Lit_RAR			0.467

			(1.138)
Lit_RAR × Cyber_Sec			0.248
			(3.237)
CC	0.269***	0.27***	0.268***
	(0.021)	(0.021)	(0.021)
CE	0.223***	0.224***	0.224***
	(0.044)	(0.044)	(0.044)
H	0.198***	0.198***	0.2***
	(0.054)	(0.053)	(0.054)
US	0.137***	0.136***	0.138***
	(0.032)	(0.032)	(0.032)
Liq	-0.211*	-0.265**	-0.196*
	(0.125)	(0.115)	(0.114)
Δ*VIX*	-0.377	-0.38	-0.381
	(0.386)	(0.386)	(0.386)
Month fixed effect	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes
Adjusted R^2	0.31	0.31	0.31
F-stats	9.1***	9.11***	9.07***
N	1148	1148	1148

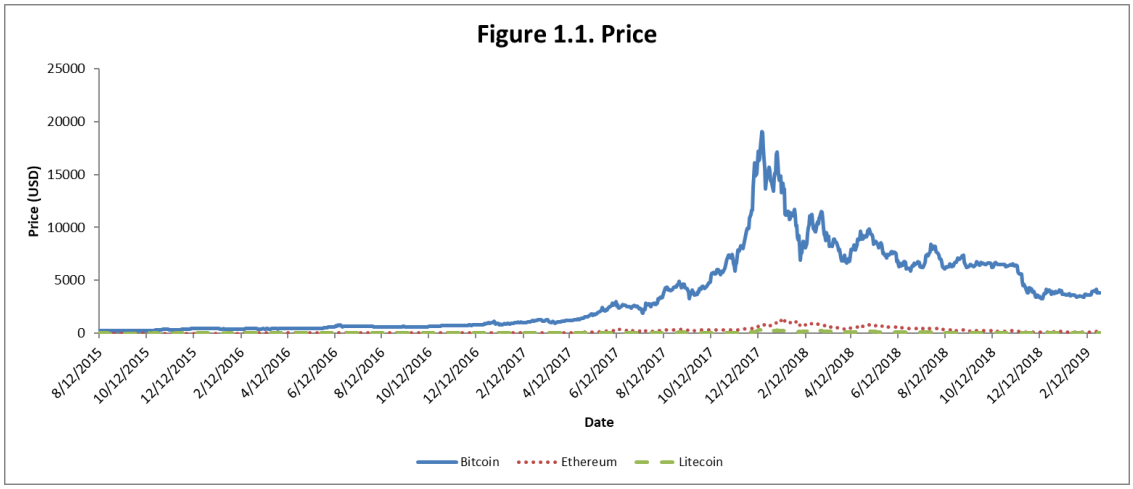
Table 9. Financial sector targeted by cyber-attacks

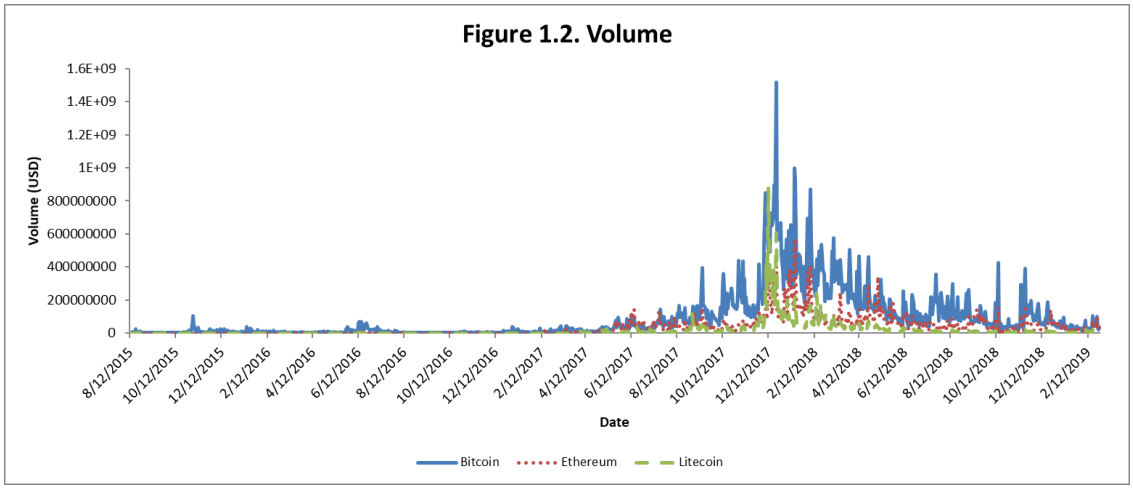
The following table presents the pooled OLS regression results showing the determinants of cyber-attacks targeting the financial sector (*Fin*). The independent variables include cyber security (*Cyber_Sec*), other cyber-attack targets (*Crypto*, *Gov*, *Ind*), types (*CC*, *CW*, *H*), countries (*US*) and cryptocurrency's risk-adjusted return (*Bit_RAR*, *Eth_RAR*, *Lit_RAR*) while controlling for global financial market uncertainty change (ΔVIX), and country specific stock market liquidity (*Liq*). We report the *F*-statistics, adjusted R^2 and number of observations (*N*). The standard errors are in the brackets. ***, ** and * denote significance at 1%, 5% and 10% levels, respectively.

	Fin (1)	*Fin* (2)	*Fin* (3)
Intercept	-0.632	-0.631	-0.628
	(0.426)	(0.426)	(0.426)
Cyber_Sec	0.015	-0.026	-0.015
	(0.032)	(0.031)	(0.032)
Crypto	-0.181***	-0.179***	-0.18***
	(0.053)	(0.053)	(0.053)
Crypto × *Cyber_Sec*	0.026	0.032	0.029
	(0.086)	(0.086)	(0.086)
Gov	-0.099***	-0.101***	-0.1***
	(0.021)	(0.021)	(0.021)
Gov × *Cyber_Sec*	0.026	0.029	0.028
	(0.034)	(0.034)	(0.034)
Ind	-0.081***	-0.081***	-0.081***
	(0.015)	(0.015)	(0.015)
Ind × *Cyber_Sec*	-0.021	-0.021	-0.021
	(0.022)	(0.022)	(0.022)
Bit_RAR	-0.898	-0.631	
	(1.155)	(0.426)	
Bit_RAR × *Cyber_Sec*	4.381	-0.026	
	(3.021)	(0.031)	
Eth_RAR		0.052	
		(0.074)	
Eth_RAR × *Cyber_Sec*		0.163	
		(0.209)	
Lit_RAR			0.166

			(0.576)
Lit_RAR × Cyber_Sec			1.487
			(1.638)
CC	0.113***	0.112***	0.112***
	(0.011)	(0.011)	(0.011)
CE	0.028	0.028	0.028
	(0.022)	(0.022)	(0.022)
H	0.077***	0.083***	0.079***
	(0.027)	(0.027)	(0.027)
US	-0.02	-0.018	-0.019
	(0.016)	(0.016)	(0.016)
Liq	-0.095	-0.056	-0.064
	(0.063)	(0.058)	(0.058)
Δ*VIX*	-0.309	-0.303	-0.303
	(0.195)	(0.195)	(0.195)
Month fixed effect	Yes	Yes	Yes
Country fixed effect	Yes	Yes	Yes
Adjusted R^2	0.14	0.13	0.13
F-stats	3.77***	3.73***	3.74***
N	1148	1148	1148

Figure 1. Cryptocurrencies





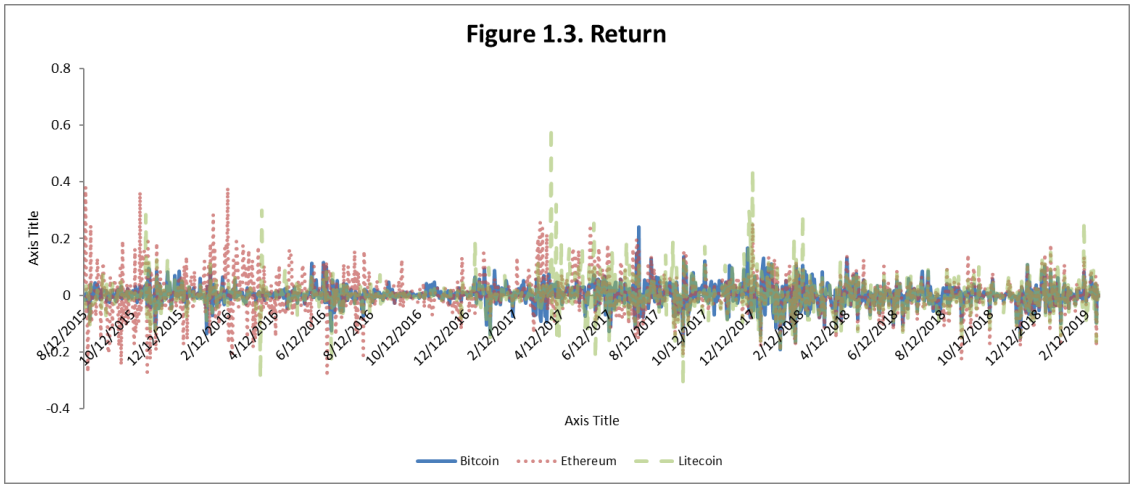
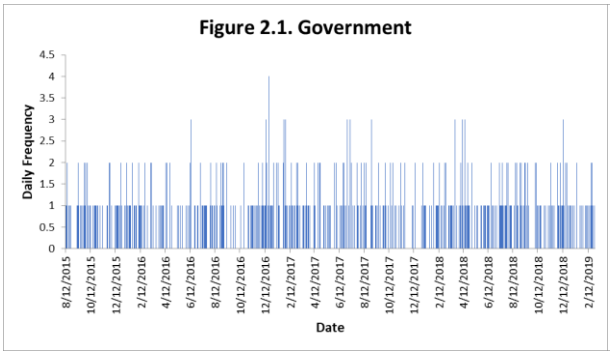
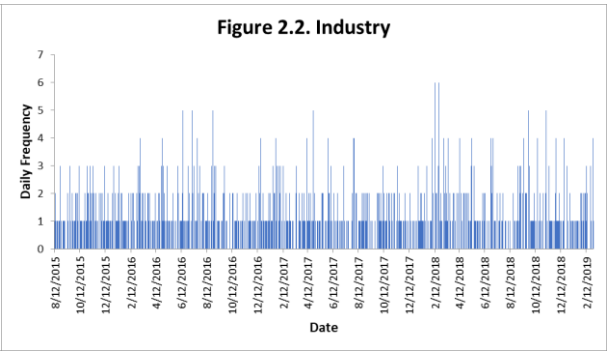
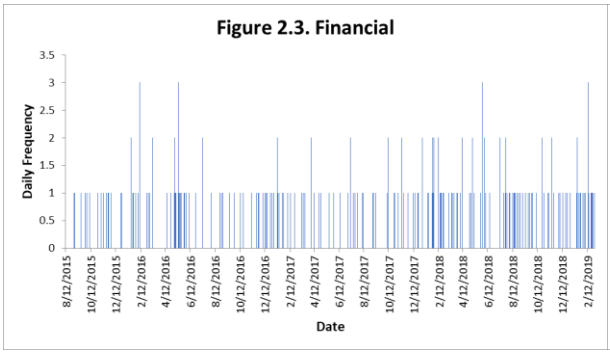
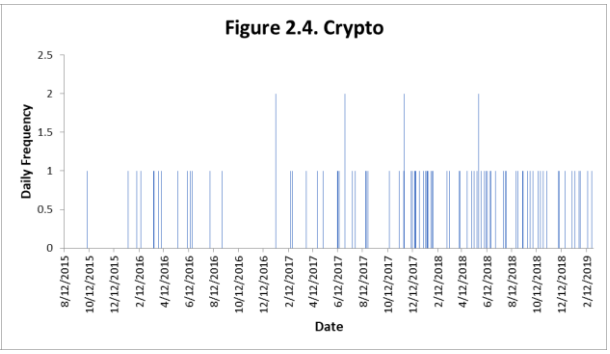


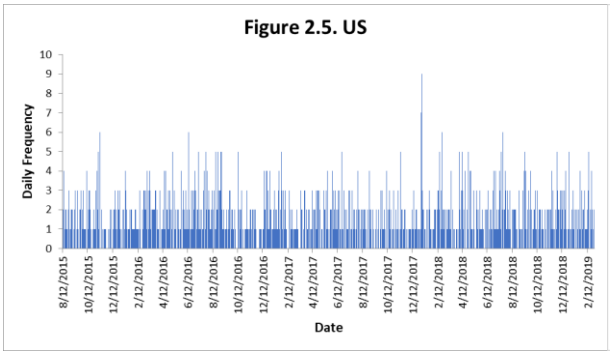
Figure 2. Cyber-Attacks by Target











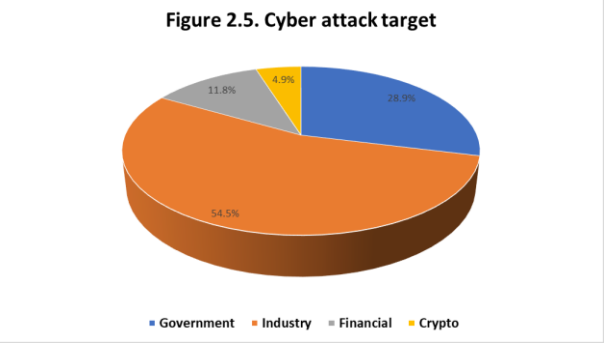
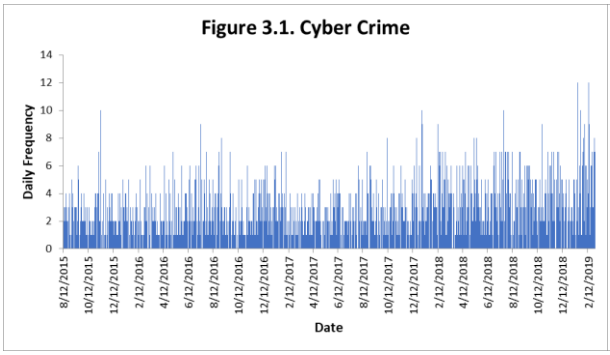
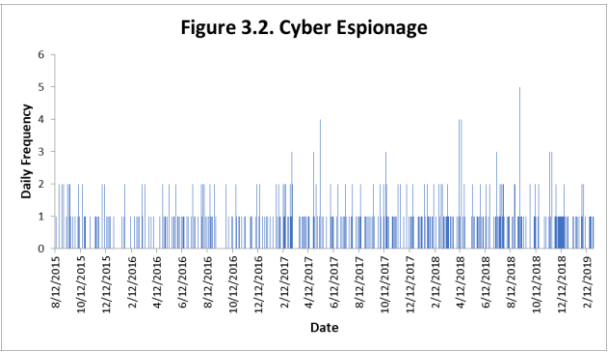
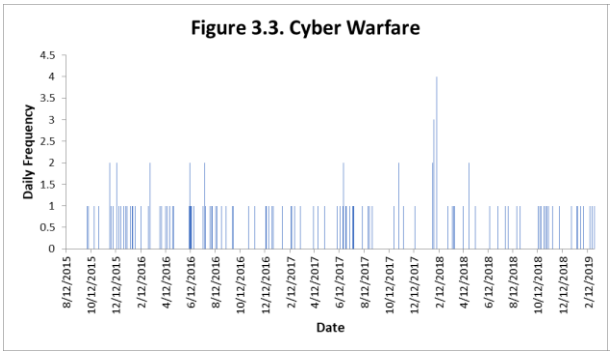
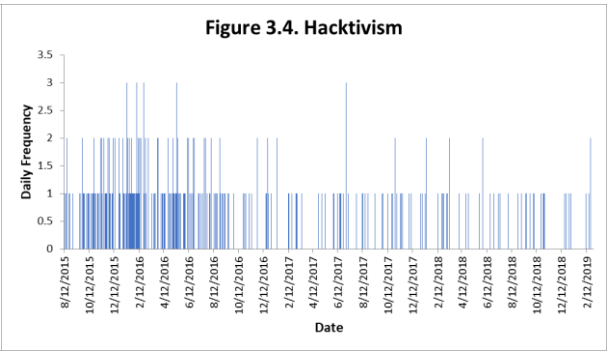


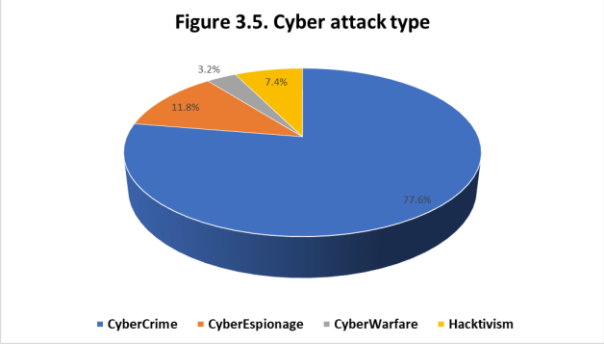
Figure 3. Cyber-Attacks by Type











Appendix I. Variance inflation factor (VIF) test

The following tables show the VIF test results for the regressions from Table 3 to 9.

Panel A. VIF tests including Bitcoin

Cyber_Sec	*Crypto*	*Crypto × Cyber_Sec*	*Gov*	*Gov × Cyber_Sec*	*Ind*	*Ind × Cyber_Sec*	*Fin*	*Fin × Cyber_Sec*	*Bit_RAR*	*Bit_RAR × Cyber_sec*	*CC*	*CE*	*H*	*US*	*Liq*	*VIX*
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	2.54	1.34	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
1.98			1.38	1.07	1.51	1.06	1.24	1.10	1.59	1.87	2.90	1.29	1.35	2.53	1.72	1.06
2.00	1.34	1.26			1.48	1.07	1.23	1.10	1.59	1.88	2.95	1.16	1.25	2.49	1.72	1.06
1.98	1.32	1.26	1.33	1.07			1.22	1.10	1.60	1.88	2.59	1.27	1.33	2.49	1.72	1.06
2.00	1.34	1.26	1.36	1.06	1.51	1.07			1.60	1.87	2.72	1.30	1.34	2.55	1.72	1.06

Panel B. VIF tests including Ethereum

Cyber_Sec	*Crypto*	*Crypto × Cyber_Sec*	*Gov*	*Gov × Cyber_Sec*	*Ind*	*Ind × Cyber_Sec*	*Fin*	*Fin × Cyber_Sec*	*Eth_RAR*	*Eth_RAR × Cyber_sec*	*CC*	*CE*	*H*	*US*	*Liq*	*VIX*
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	2.54	1.34	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
1.90	1.38			1.06	1.52	1.06	1.24	1.10	5.93	6.03	2.90	1.29	1.34	2.53	1.45	1.06
2.01	1.33	1.38			1.48	1.07	1.22	1.10	5.93	6.03	2.95	1.16	1.24	2.48	1.45	1.06
1.89	1.31	1.25	1.33	1.06			1.22	1.10	5.94	6.03	2.58	1.27	1.32	2.49	1.44	1.06
1.91	1.33	1.25	1.36	1.06	1.51	1.07			5.93	6.03	2.73	1.30	1.32	2.54	1.45	1.06

Panel C. VIF tests including Litecoin																
Cyber_Sec	*Crypto*	*Crypto × Cyber_Sec*	*Gov*	*Gov × Cyber_Sec*	*Ind*	*Ind × Cyber_Sec*	*Fin*	*Fin × Cyber_Sec*	*Lit_RAR*	*Lit_RAR × Cyber_sec*	*CC*	*CE*	*H*	*US*	*Liq*	*VIX*
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	2.54	1.34	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
1.32	1.34	1.26	1.39	1.06	1.55	1.07	1.25	1.10			2.99	1.30	1.34	2.54	1.21	1.06
1.07															1.17	1.04
2.07			1.38	1.06	1.51	1.06	1.24	1.10	2.18	1.51	2.89	1.30	1.35	2.53	1.42	1.06
2.08	1.34	1.26			1.48	1.07	1.23	1.10	2.19	1.52	2.94	1.16	1.26	2.48	1.42	1.06
2.06	1.32	1.26	1.33	1.06			1.22	1.10	2.20	1.52	2.58	1.27	1.33	2.49	1.42	1.06
2.08	1.34	1.27	1.36	1.06	1.51	1.07			2.19	1.52	2.72	1.30	1.34	2.54	1.42	1.06

Appendix II. Cyber-attack target country and count

Cyber-attack target country	Cyber-attack count
United States of America	1519
More than one country	930
United Kingdom	231
Unknown	102
India	92
Canada	84
Russian Federation	76
Australia	65
Italy	65
Korea (South)	58
Japan	54
France	44
China	41
Germany	37
Ukraine	36
Brazil	35
Israel	29
Netherlands	28
Thailand	22
Turkey	22
Ireland	21
South Africa	21
Hong Kong	20
Pakistan	20
Sweden	18
Iran	17
Saudi Arabia	17
Switzerland	16
New Zealand	16
United Arab Emirates	15
Singapore	14
Spain	13
Mexico	13
Philippines	12
Taiwan	12
Austria	9
Belgium	9
Norway	9
Azerbaijan	8
Czech Republic	8
Denmark	8
Kenya	8
Poland	8
Venezuela	8
Greece	7
Malaysia	7
Vietnam	7

Armenia	6
Bangladesh	6
European Union	6
Chile	5
Finland	5
Panama	5
Syrian Arab Republic	5
Afghanistan	4
Argentina	4
Cyprus	4
Cambodia	4
Korea (North)	4
Malta	4
Qatar	4
Zimbabwe	4
Egypt	3
Lebanon	3
Sri Lanka	3
Luxembourg	3
Montenegro	3
Nepal	3
Romania	3
Slovakia	3
Albania	2
Barbados	2
Cocos (Keeling) Islands	2
Colombia	2
Costa Rica	2
Ecuador	2
Hungary	2
Indonesia	2
Jordan	2
Kuwait	2
Cayman Islands	2
Kazakhstan	2
Lithuania	2
Nigeria	2
Palestine	2
Uganda	2
Angola	1
Bosnia and Herzegovina	1
Bahrain	1
Bolivia	1
Bahamas	1
Belarus	1
Dominican Republic	1
Algeria	1
Estonia	1
Fiji	1
Gabon	1
Guernsey	1

Guam	1
Iraq	1
Iceland	1
Libya	1
Myanmar	1
Mongolia	1
Maldives	1
Namibia	1
Oman	1
Puerto Rico	1
Paraguay	1
Rwanda	1
Tajikistan	1
Tunisia	1
Trinidad and Tobago	1
Tanzania	1
Virgin Islands	1
Yemen	1

Appendix III. Visualization of cyber-attacks across the globe