

# Cyber Attacks, Spillovers and Contagion in the Cryptocurrency Markets

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

## **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](mailto: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](http://www.SSRN.com)
- from the RePEc website: [www.RePEc.org](http://www.RePEc.org)
- from the CESifo website: <https://www.cesifo.org/en/wp>

# Cyber Attacks, Spillovers and Contagion in the Cryptocurrency Markets

## Abstract

This paper examines mean and volatility spillovers between three major cryptocurrencies (Bitcoin, Litecoin and Ethereum) and the role played by cyber attacks. Specifically, trivariate GARCH-BEKK models are estimated which include suitably defined dummies corresponding to different types, targets and number per day of cyber attacks. Significant dynamic linkages (interdependence) among the three cryptocurrencies under investigation are found in most cases when cyber attacks are taken into account, Bitcoin appearing to be the dominant one. Further, Wald tests for parameter shifts during episodes of turbulence resulting from cyber attacks provide evidence that the latter affect the transmission mechanism between cryptocurrency returns and volatilities (contagion). More precisely, cyber attacks appear to strengthen cross-market linkages, thereby reducing portfolio diversification opportunities for cryptocurrency investors. Finally, the conditional correlation analysis confirms the previous findings.

JEL-Codes: C320, F300, G150.

Keywords: mean and volatility spillovers, contagion, cryptocurrencies, cyber attacks.

*Guglielmo Maria Caporale\**  
*Department of Economics and Finance*  
*Brunel University London / United Kingdom*  
*Guglielmo-Maria.Caporale@brunel.ac.uk*

*Fabio Spagnolo*  
*Department of Economics and Finance*  
*Brunel University London / United Kingdom*  
*fabio.spagnolo@brunel.ac.uk*

*Woo-Young Kang*  
*Department of Economics and Finance*  
*Brunel University London / United Kingdom*  
*woo-young.kang@brunel.ac.uk*

*Nicola Spagnolo*  
*Department of Economics and Finance*  
*Brunel University London / United Kingdom*  
*nicola.spagnolo@brunel.ac.uk*

\*corresponding author

April 2020

## **1. Introduction**

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., 2017). 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, 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., Dyrberg 2016a, 2016b; Baur et al., 2018; Bouri et al., 2017a, 2017b, 2017c), initial coin offerings (Kostovetsky and Benedetti. 2018; Howell et al., 2018; Lee et al., 2018; Li and Mann, 2018; Malinova and Park, 2017), the effects of cyber attacks (Caporale et al., 2019, 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).

Understanding the linkages between cryptocurrencies is crucial for risk management, portfolio diversification, hedging and arbitrage purposes. In particular, investors need to understand the degree of contagion risk they are exposed to when trading cryptocurrencies (Koutmos, 2018) and to choose suitable ones to diversify their portfolios according to their risk preferences (Yi et al., 2018). Long-term investors focus on long-run market connectedness whilst speculators target volatile markets on the basis of short-run linkages and hedgers seek markets with the highest degree of correlation in the medium- to long-term. Some recent studies have investigated these issues. For instance, Fry and Cheah (2016) detect spillovers from Ripple to Bitcoin using an econophysics approach. Ciaian et al. (2018) estimate an ARDL model to examine the relationship between 17 virtual currencies and Altcoin and find stronger linkages between Bitcoin and Altcoin in the short as opposed to the long run. Bacao et al. (2018) find strong contemporaneous correlations between five major cryptocurrencies using unconditional returns; further, their results suggest that Bitcoin is the dominant currency in terms of informational flows. More recently, Borri (2019) analyses co-movement between returns on four cryptocurrencies (Bitcoin, Ether, Ripple and Litecoin) and other global assets such as US

equities or gold, both unconditionally and conditionally. Specifically, he measures the conditional tail-risk using the CoVaR (conditional value-at-risk) method introduced by Adrian and Brunnermeier (2016). His results indicate that cryptocurrency returns are highly correlated among themselves but not with other assets, and that portfolios of cryptocurrencies are less exposed to idiosyncratic risk and can be useful for hedging purposes (though only to a limited extent once their degree of liquidity has been taken into account).

Another important issue is whether or not spillovers change over time. For instance, Boako et al. (2019) apply vine copula methods to analyse both the co-dependence and portfolio value-at-risk (VaR) of six cryptocurrencies and find evidence of strong dependencies and a changing dependency structure. By contrast, the findings in Borro (2019) concerning the conditional correlation between cryptocurrencies and other assets appear to be robust to the introduction of time variation into the empirical model. Ji et al. (2019) examine network connectedness in both the returns and volatility of six major cryptocurrencies (Bitcoin, Ethereum, Ripple, Litecoin, Stellar and Dash) using daily data over the period 7 August 2015 – 22 February 2018 and computing a set of measures developed by Diebold and Yilmaz (2012, 2016). They distinguish between positive- and negative-return spillovers and consider various market characteristics as possible determinants of spillovers. They also test the robustness of their full-sample results by redoing the analysis for two sub-samples, the first being more stable, the second starting at the beginning of 2017 and including the 2017 bull market. Their findings indicate that Bitcoin and Litecoin have the dominant transmitting role; the sub-sample results have both similarities and differences compared to the full-sample ones.<sup>2</sup>

Other studies examine volatility linkages and their changes over time. In particular, Yi et al. (2018) construct a spillover index with some variants for eight cryptocurrencies (i.e., Bitcoin, Ripple, Litecoin, Peercoin, Namecoin, Feathercoin, Novacoin and Terracoin) and conclude that volatility connectedness fluctuates cyclically, and increases when economic conditions are less stable; because this measure does not depend on the market share even cryptocurrencies

---

<sup>2</sup> Using a similar approach, Corbet et al. (2018) find that Bitcoin, Ripple and Litecoin are highly correlated with each other but not with other types of assets, which implies that the former can be used for portfolio diversification purposes.

with smaller trading volumes are found to contribute to the propagation of shocks. By contrast, Koutmos (2018) detects a dominant role for Bitcoin in terms of return and volatility spillovers among the 18 largest cryptocurrencies by market capitalization; he also finds that spillovers have been increasing over time and exhibit spikes corresponding to major news events concerning cryptocurrencies. Katsiampa (2019) estimates a GARCH-BEKK model and finds volatility co-movements between five cryptocurrencies; further, Litecoin and Bitcoin both exhibit a structural break in their conditional variance. Antonakakis et al. (2019) investigate network connectedness between nine cryptocurrencies using an approach which extends the framework of Diebold and Yilmaz (2014), specifically time-varying parameters principal component analysis (TVP-PCA); since connectedness appears to follow a decreasing trend, they then split the sample into pre- and post-August 2017 sub-samples on the basis of an increase in market capitalization at that time, and show that lower volatility is associated with weaker connectedness. Omane-Adjepong and Alagidede (2019) examine market connectedness between seven cryptocurrencies using wavelet methods and also investigate volatility linkages by estimating GARCH specifications; they find various non-homogenous spillovers and possible diversification benefits within intra-week to intra-monthly time horizons for specific pairs.

Most recently, Corbet et al. (2020) analyse the contagion effects between Chinese stock markets resulting from the COVID-2019 pandemic; the evidence based on high-frequency data suggests an increase in the dynamic correlations between Chinese stock indices, gold and Bitcoin, i.e. the latter do not act as hedges, or safe havens, but instead amplify contagion. Similar conclusions are reached by Conlon and McGee (2020) vis-à-vis the S&P500. In general, cryptocurrencies seem to be suitable for diversification purposes but not as a hedge (see Gil-Alana et al., 2020; Liu, 2019; Tiwari et al., 2019, Feng et al., 2018).

The present study investigates both “interdependence”, namely the existence of dynamic linkages, and “contagion”, defined as a shift in the return and volatility spillover parameters (see Forbes and Rigobon, 2002, and Caporale et al., 2005, 2006), among three major cryptocurrencies, namely Bitcoin, Ethereum and Litecoin, where the dates for the shifts are identified using cyber attack data. The framework employed for the empirical analysis is a trivariate GARCH-BEKK model which includes suitably defined dummies associated with

different types, targets and number per day of cyber attacks as explained below. In brief, significant dynamic linkages (interdependence) among the three cryptocurrencies under investigation are found in most cases when cyber attacks are taken into account, Bitcoin appearing to be the dominant one. Further, Wald tests for parameter shifts during episodes of turbulence resulting from cyber attacks provide evidence that the latter affect the transmission mechanism between cryptocurrency returns and volatilities (contagion). More precisely, cyber attacks appear to strengthen cross-market linkages, thereby reducing portfolio diversification opportunities for cryptocurrency investors.

The layout of the paper is as follows. Section 2 outlines the methodology. Section 3 describes the data and Section 4 discusses the empirical results. Section 5 offers some concluding remarks.

## 2. Methodology

### 2.1. Basic Model

We represent the first and second moments of cryptocurrency returns using a trivariate VAR-GARCH(1,1) process. In its most general specification the model takes the following form:

$$x_t = \alpha + \beta x_{t-1} + \phi z_{t-1} + e_t \quad (1)$$

where  $x_t = (\text{Bitcoin}_t, \text{Ethereum}_t, \text{Litecoin}_t)$ ,  $x_{t-1}$  is a corresponding vector of lagged returns, and  $e_t = (e_{1,t}, e_{2,t}, e_{3,t})$  is a residual vector. Furthermore,  $z_{t-1}$  is the Chicago Board Options Exchange index of implied volatility from options on the US S&P 500 (VIX). This is a widely quoted indicator of market sentiment, and is used as a control variable to identify episodes of turbulence in conventional stock markets. The parameters of the mean return equations (1) comprise the constant terms  $\alpha = (\alpha_1, \alpha_2, \alpha_3)$  and the parameters of the autoregressive terms  $\beta = (\beta_{11}, \beta_{12}, \beta_{13} | \beta_{21}, \beta_{22}, \beta_{23} | \beta_{31}, \beta_{32}, \beta_{33})$ , which allow for cross-currency mean return spillovers. The residual vector  $u_t$  is trivariate and normally distributed  $u_t | I_{t-1} \sim (0, H_t)$  with its conditional variance-covariance matrix given by:

$$H_t = \begin{bmatrix} h_{11,t} & h_{12,t} & h_{13,t} \\ h_{21,t} & h_{22,t} & h_{23,t} \\ h_{31,t} & h_{32,t} & h_{33,t} \end{bmatrix} \quad (2)$$

In the multivariate GARCH(1,1)-BEKK representation proposed by Engle and Kroner (1995), which guarantees by construction that the variance-covariance matrices in the system are positive definite,  $H_t$  takes the following form:

$$H_t = C_0' C_0 + \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \begin{bmatrix} e_{1,t-1}^2 & e_{1,t-1}e_{2,t-1} & e_{1,t-1}e_{3,t-1} \\ e_{2,t-1}e_{1,t-1} & e_{2,t-1}^2 & e_{2,t-1}e_{3,t-1} \\ e_{3,t-1}e_{1,t-1} & e_{3,t-1}e_{2,t-1} & e_{3,t-1}^2 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$\begin{bmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{bmatrix}, H_{t-1} \begin{bmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{bmatrix} \quad (3)$$

Equation (3) models the dynamic process of  $H_t$  as a linear function of its own past values  $H_{t-1}$  and past values of the innovations ( $e_{1,t-1}$ ,  $e_{2,t-1}$ ,  $e_{3,t-1}$ ), allowing for own-market and cross-market influences in the conditional variances. The parameters of (3) are given by  $C_0$ , which is restricted to be upper triangular, and two matrices  $A_{11}$  and  $G_{11}$ . The off-diagonal parameters in the latter two matrices capture the volatility spillovers (causality-in-variance) among the three cryptocurrencies under investigation.

Given a sample of  $T$  observations, a vector of unknown parameters<sup>3</sup>  $\theta$ , and a  $3 \times 1$  vector of variables  $x_t$ , the conditional density function for the model (1)-(3) is:

---

<sup>3</sup> Standard errors (SE) are calculated using the quasi-maximum likelihood method of Bollerslev and Wooldridge (1992), which is robust to the distribution of the underlying residuals. A residual vector  $e_t$  following the t-Student  
(continued...)



$$f(x_t | I_{t-1}; \theta) = (2\pi)^{-1} |H_t|^{-1/2} \exp(- [e_t^T (H_t^{-1}) e_t] / 2) \quad (4)$$

The log likelihood function is:

$$\text{Log-Lik} = \sum_{t=1}^T \log f(x_t | I_{t-1}; \theta). \quad (5)$$

## 2.2. Mean and Volatility Contagion

Applying the concept of shift contagion (Forbes and Rigobon, 2002) to the analysis of interdependencies in the first and second moments, we define mean and volatility contagion, respectively, as a shift in the transmission of returns and volatility among crypto currencies during episodes of cyber attacks. In order to test for such shifts, we include in equations (1) and (3) a dummy  $D$  that allows the parameters governing mean and volatility spillovers to change in days associated with these episodes.<sup>4</sup> For instance, the equations for the conditional mean and variance of Bitcoin returns become respectively:

$$\text{Bitcoin}_t = \alpha_1 + \beta_{11}\text{Bitcoin}_{t-1} + (\beta_{12}^* + \beta_{12})\text{Ethereum}_{t-1} + (\beta_{13}^* + \beta_{13})\text{Litecoin}_{t-1} + \phi z_{t-1} + e_{2,t}$$

and

$$\begin{aligned} h_{11,t} = & c_{11}^2 + a_{11}^2 e_{1,t-1}^2 + a_{12}^2 e_{2,t-1}^2 + (a_{13} + a_{13}^* \cdot D)^2 e_{3,t-1}^2 \\ & + 2 a_{11}a_{12}e_{1,t-1}e_{2,t-1} + 2 a_{11}(a_{13} + a_{13}^* \cdot D) e_{1,t-1}e_{3,t-1} + 2 a_{12}(a_{13} + a_{13}^* \cdot D) e_{2,t-1}e_{3,t-1} \\ & + g_{11}^2 h_{11,t-1} + g_{12}^2 h_{22,t-1} + (g_{13} + g_{13}^* \cdot D)^2 h_{33,t-1} \\ & + 2 g_{11}g_{12}h_{12,t-1} + 2 g_{11}(g_{13} + g_{13}^* \cdot D) h_{13,t-1} + 2 g_{12}(g_{13} + g_{13}^* \cdot D) h_{23,t-1} \end{aligned} \quad (6)$$

Mean spillovers from Ethereum and Litcoin to Bitcoin are measured by the parameters  $\beta_{12}$  and  $\beta_{13}$ , whereas  $\beta_{12}^*$  and  $\beta_{13}^*$  capture shifts in these parameters during episodes of cyber attacks. Similarly, volatility spillovers from Ethereum and Litcoin to Bitcoin are measured by the

---

distribution has also been considered. These results are qualitatively similar and therefore are not reported. The complete set of results is available from the authors upon request.

<sup>4</sup> See section 3.3 for details on the construction of the dummies.

parameters  $a_{12}$  and  $g_{12}$ , and  $a_{13}$  and  $g_{13}$  respectively;  $a_{13}^*$  and  $g_{13}^*$ , and  $a_{13}^*$  and  $g_{32d}$  instead capture shifts in these parameters during episodes of cyber attacks.

### **3. Data Set and Identification of Cyber Attacks**

#### **3.1. Cryptocurrencies**

The trivariate GARCH model outlined in the preceding section was estimated for three cryptocurrencies (Bitcoin, Ethereum and Litecoin). The series are daily and have been collected from the website [www.CryptoDataDownload.com](http://www.CryptoDataDownload.com); this provides historical time series 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; the sample period goes from 1 March 2015 to 15 January 2020.<sup>5</sup> We then compute market capital-weighted indices which are based on the five exchanges. The natural log returns are used for the estimation of the models.

**[Insert Figure 1]**

#### **3.2. Cyber Attacks**

The source for the cyber-attack data is the website <http://www.hackmageddon.com> which shows the cyber-attack timeline with target industry, country and cyber-attack type at a daily frequency. Specifically, we collect 4693 daily cyber attacks from 12 August 2015 to 15 January 2020 including daily overlaps. We use the daily number of cyber attacks as an indicator of potential threats to the digital economy. Cyber attacks are classified by target (Government, Industry, Financial and Crypto) or nature (Cyber Crime, Cyber Espionage, Cyber Warfare and Hactivism). We also collected data classified as attacks targeting the US.

---

<sup>5</sup> The [www.CryptoDataDownload.com](http://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.

Following Uma and Padmavathi (2013), Cyber Crime is 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 spyware) 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 1 and 2 show, respectively, the cyber-attack targets and types used for the analysis. It is apparent from Figure 1 that the Industry sector is the most frequent target of cyber attacks, which suggests that it is more vulnerable, compared to other sectors (e.g., Government, Financial and Crypto) that have stronger cyber security protections. In particular, the Crypto currency 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 2 shows that Cyber Crime is the most frequent type of cyber attack, and Cyber Warfare 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.

**[Insert Figure 2 and 3]**

### **3.3. Identification of Cyber Attacks as Potential Turbulent Episodes**

Turbulent periods are identified as those corresponding to cyber attacks. We construct the following four indicators of cyber attacks: i) by target (given by the aggregate number of daily attacks targeting Government, Industry and Finance), named Target; ii) by type (given by the aggregate number of daily Cyber Crime, Cyber Espionage and Cyber Warfare attacks), named Type; (iii) one given by the sum of daily attacks targeting crypto currencies only, named Crypto; finally iv) one given by the sum of daily attacks targeting the US, named US. We do not include all other sectors in Target and Hacktivism in Type in order to avoid the dummy

variable trap. The Chicago Board Options Exchange (CBOE) volatility index (VIX) is also included in the model as a control variable.

For each of the four indicators discussed above, dummy variables are created which aim to capture the impact of the number of daily attacks on the mean and volatility spillovers among cryptocurrencies. More specifically, a dummy is constructed for days where 1-2 cyber attacks were registered, another one for days where 3-4 occurred and finally one for days when more than 5 took place. These are included in the estimated model in turn. The aim is to establish whether there exists a threshold in terms of the number of attacks required for the parameter shifts to occur and be statistically significant. Using this model selection criterion we choose specifications including two dummies in the case of the Crypto indicator and three in all other cases. It should be noted that there is an inverse relationship between the number of attacks per day and the frequency of such an occurrence, namely days with a high number of attacks are less frequent. For example, our sample includes 93 days with a single attack but only 4 with 2 attacks. Further, the number of days with 1-2 attacks represents 40% of the total in the case of the Type indicator and around 50% in the case of the Target or US ones. The corresponding percentages for days with 3-4 attacks are less than half.

Table 1 provides a description of the crypto-attack indicators, whilst Table 2 reports some summary statistics. Most of the series follow a right-skewed distribution, the Industry cyber-attacks target variable being the only exception. In other words, cyber attacks targeting Government, Financial and Crypto currency sectors are not very frequent, in contrast to the Industry sector. Most types of cyber attacks have a low frequency per day while Cyber Crime is highly volatile, with a maximum of 12 attacks per day. As for the three crypto currencies considered, Ethereum is the most volatile (with a standard deviation of 0.068).

**[Insert Table 1 and 2]**

## 4. Empirical Analysis

### 4.1. Hypotheses Tested

We test for volatility spillovers and contagion by placing restrictions on the relevant parameters and computing the following Wald test:

$$W = [R\hat{\theta}]' [R\text{Var}(\hat{\theta})R']^{-1} [R\hat{\theta}] \quad (7)$$

where  $R$  is the  $q \times k$  matrix of restrictions, with  $q$  equal to the number of restrictions and  $k$  equal to the number of regressors;  $\hat{\theta}$  is a  $k \times 1$  vector of the estimated parameters, and  $\text{Var}(\hat{\theta})$  is the heteroscedasticity - robust consistent estimator for the covariance matrix of the parameter estimates. The tests involve joint hypotheses at two and four degrees of freedom ( $k$ ).

Overall we test nine sets of null hypotheses, three for each cryptocurrency. Below we report three sets of null hypotheses where spillover or contagion originates from Bitcoin.

Tests of no volatility spillovers and/or contagion.

$H_{01}$ : No volatility spillovers and no contagion from Bitcoin to Litecoin:  $a_{31} = a_{31}^* = g_{31} = g_{31}^* = 0$ . The null hypothesis assumes that volatility in Litecoin is never influenced by volatility in Bitcoin, neither over the full sample period nor specifically during episodes of turbulence associated to cyber-attacks.

$H_{02}$ : No contagion, that is, no shift in the transmission of volatility from Bitcoin to Litecoin during episodes of turbulence, in the former:  $a_{31}^* = g_{31}^* = 0$ .

$H_{03}$ : No volatility spillovers from Bitcoin to Litecoin over the full sample period:  $a_{31} = g_{31} = 0$ . This hypothesis complements  $H_{02}$ . If we reject  $H_{03}$  and do not reject  $H_{02}$ , there is no volatility contagion, only spillovers; if we do not reject  $H_{03}$  and reject  $H_{02}$ , volatility is transmitted from Bitcoin to Litecoin only during days when attacks occurred, which implies “shift contagion.”

We test the same hypotheses for Litecoin as a conduit for volatility transmission to Bitcoin and Ethereum first and then Ethereum to Bitcoin and Litecoin.

Finally, we compute conditional correlations between Bitcoin and Litecoin as  $\rho_{13,t} = h_{13,t}/(\sqrt{h_{11,t}}\sqrt{h_{33,t}})$ , Ethereum and Bitcoin as  $\rho_{23,t} = h_{23,t}/(\sqrt{h_{22,t}}\sqrt{h_{33,t}})$ , and Ethereum and Litecoin as  $\rho_{12,t} = h_{12,t}/(\sqrt{h_{11,t}}\sqrt{h_{22,t}})$ , respectively, and test for increases during days attacks were registered compared to days when attacks did not occur. The test results are reported in Table 7.

## 4.2. Discussion of the Results

In order to test the adequacy of the models, Ljung–Box portmanteau tests were performed on the standardized and standardized squared residuals. Overall, the results indicate that the selected VAR-GARCH(1,1) specification captures satisfactorily the persistence in the volatility of cryptocurrencies in all estimated models. There is evidence of causality effects in the conditional mean and variance, where the latter are more marked. Note that the sign of the coefficients on cross-market volatilities cannot be determined. Point estimates of the VAR-GARCH(1,1) model parameters, as well as the associated robust p-values and likelihood function values, are presented in Tables 3-6. We select the optimal lag length of the mean equation using the Schwarz information criterion. Mean and volatility spillovers are tested by means of Wald test by placing restrictions on the relevant parameters as discussed in Section 4.1.

The following points are noteworthy. When cyber attacks are not taken into account there is little evidence of causality-in-mean at the standard 5% significance level, whereas causality-in-variance is detected, with volatility spillovers running from Bitcoin to Litecoin ( $a_{31} = -0.401$ ) and Ethereum ( $a_{21} = -0.195$ ), and also from Ethereum to Litecoin ( $a_{32} = 0.145$ ). Overall, the estimated parameters indicate that volatility spillovers run from Bitcoin (but not from Litecoin) to the other two cryptocurrencies.

Further, cyber attacks are found to affect the dynamic linkages between cryptocurrencies, as indicated by the statistical significance in various cases of the dummies discussed in Section 3.2. In particular, on days during which only one cyber attack targeting cryptocurrencies occurred (93 days over the whole sample), there is a downward shift (negative contagion) in the parameter measuring mean spillovers running from Bitcoin to Litecoin ( $\beta_{31}^* = -0.145$ ) and

Ethereum ( $\beta_{21}^* = -0.117$ ), which suggests that cryptocurrency investors react to cyber attacks by diversifying and therefore prefer to hold Bitcoin and short the other two cryptocurrencies. On days when two attacks occurred no shift could be detected, presumably because there are only four such days out of the 1316 included in our sample. When cyber attacks are considered by Type lower mean spillovers are found running from Bitcoin to Litecoin ( $\beta_{31}^* = -0.122$ ) and Ethereum ( $\beta_{21}^* = -0.291$ ) on days when 1-2 attacks were registered. The size of the shift is bigger, in absolute value, on days when 3-4 attacks occurred, and smaller on days with five or more attacks. When cyber attacks are classified instead by Target, again a shift is detected in the parameter measuring the mean spillovers from Bitcoin to the other two cryptocurrencies, its magnitude increasing (in absolute value) with the number of registered attacks per day. A similar pattern emerges when using the previously defined US indicator, though the size of the shift is now inversely related to the number of attacks per day. Finally, the estimated coefficients on the exogenous variable (VIX) are negative and significant, which suggests that a higher level of uncertainty in conventional stock markets has an impact on cryptocurrency returns.

To sum up, our results indicate that there are no significant causality-in-mean effects at the standard 5% significance level. In the case of Bitcoin mean spillovers emerge when cyber attacks are taken into account, although the size of the shift varies depending on the cyber attack indicator which is used. As for linkages between the second moments, there are significant volatility spillovers from Bitcoin to Litecoin and Ethereum, whose size is again magnified by the inclusion of cyber-attack indicators. The largest parameter shifts are detected when the Crypto indicator is included in the model, followed by Target and Type. Specifically, shifts are estimated in the parameters measuring volatility spillovers between Ethereum ( $a_{23}^* = -0.177$ ) and Litecoin ( $a_{32}^* = -0.404$ ); again, the largest shifts in the conditional variance-covariance matrix off-diagonal parameters are found when using the Crypto indicator. The implication of these findings is that cyber attacks play an important role in shaping the dynamic linkages between cryptocurrencies, especially between their volatilities. Bitcoin clearly stands out as the dominant cryptocurrency.

Finally, there is also evidence of co-movement between cryptocurrencies, as shown by the conditional correlations obtained from the VAR-GARCH(1,1) model (Figure 4). In particular, when attacks are not taken into account, the conditional correlations between the three cryptocurrencies are generally positive. On average their mean value is around 0.47, except in the case of Bitcoin-Litecoin, when it is substantially higher (0.66). It is also noteworthy that there has been an upward shift in pairwise correlations since 2018, the year when the cryptocurrency crash occurred (see Fry, 2018). Summary (mean and standard deviations) statistics for the conditional correlations, with and without cyber attacks, along with equal mean tests are reported in Table 7. Subsample conditional correlations including only days when attacks occurred have generally higher mean values compared to those without attacks. The largest shifts occur in the case of cyber attacks targeting cryptocurrencies, though all categories of attacks have an impact on the dynamic correlations.

## **5. Conclusions**

The objective of this study is to shed new light on the dynamic linkages (interdependence) between cryptocurrencies, and on whether shifts in their spillover parameters (contagion) are associated with the occurrence of cyber attacks (contagion), the latter topic not having been previously investigated in the rapidly growing literature on cryptocurrencies. Specifically, trivariate VAR-GARCH (1, 1) models for Bitcoin, Ethereum and Litecoin returns and their volatilities are estimated, and tests are carried out for the presence of spillovers (interdependence), as well as for possible shifts in the spillover parameters during days when cyber attacks occurred; in the latter case, the statistical significance of appropriately defined dummies taking into account their type and target (for which four indicators are constructed) as well as their number per day is tested. Conditional correlations are also calculated for the series of interest.

Our results provide a number of interesting insights. In particular, they suggest that cyber attacks influence the dynamics of conditional returns and variances, with the spillover parameters shifting during days when cyber attacks take place. Various previous studies had already highlighted changes over time in the linkages between cryptocurrencies (see Boako et al., 2019, Ji et al., 2019, Yi et al., 2018, Katsiampa, 2019, Antonakakis et al., 2019 etc.), but



the present one is the first to provide evidence that they are related to the occurrence of cyber attacks. Despite some differences associated with the number of attacks per day, their type and target, in general cyber attacks appear to strengthen cross-market linkages, thereby reducing portfolio diversification opportunities for cryptocurrency investors. Further, Bitcoin seems to play a dominant role (consistently with the evidence reported by Koutmos, 2018, Ji et al., 2019 and others). The conditional correlation analysis confirms these findings.

Future research will aim to establish whether cyber attacks also affect the linkages between cryptocurrency markets and other asset markets, which has important implications for the suitability of cryptocurrencies for diversification purposes and/or as a safe haven or hedge.

## References

- Adrian, T. and M.K. Brunnermeier (2016), “CoVaR”, *American Economic Review*, 106, 7, 1705-1741.
- Alexander, C. and M. Dakos (2020) A critical investigation of cryptocurrency data and analysis, *Quantitative Finance*, 20(2), 173-188.
- Antonakakis, N., Chatzianotniou, I. and D. Gabauer (2019), “Cryptocurrency market contagion: market uncertainty, market complexity, and dynamic portfolios”, *Journal of International Financial Markets, Institutions and Money*, 61, 37-51.
- Bacao, P., Duarte, A.P. Sebastiao, H. and S. Redzepagic (2018), “Information transmission between cryptocurrencies: does Bitcoin rule the cryptocurrency world?”, *Scientific Annals of Economics and Business*, 65, 2, 97-117.
- Balciar, 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.
- 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, 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, 177-189.
- 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.
- Boako, G., Tiwari, A.K. and D. Roubaud (2019), “Vine copula-based dependence and portfolio value-at-risk analysis of the cryptocurrency market”, *International Economics*, 158, 77-90.
- 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), 213–38.
- Bollerslev, T., and J. M.Wooldridge. (1992), “Quasi-maximum Likelihood Estimation and Inference in Dynamic Models with Timevarying Covariances.” *Econometric Reviews* 11: 143–172.

- Borri, N. (2019) “Conditional tail-risk in cryptocurrency markets”, *Journal of Empirical Finance*, 50, 1-19.
- 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, 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), 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, 192–198.
- Caporale, G.M, Cipollini, A., and N. Spagnolo, N. (2005), “Testing for contagion: a conditional correlation analysis”, *Journal of Empirical Finance*, 12, 476-489.
- Caporale, G.M., Pittis, N., and N. Spagnolo (2006), “Volatility transmission and financial crises”, *Journal of Economics and Finance*, 30, 3, 376-390.
- Caporale, G.M. and A. Plastun (2019a), “The day of the week effect in the crypto currency market”, *Finance Research Letters*, 31, 258–269.
- Caporale, G.M. and A. Plastun (2019b), “BitCoin fluctuations and the frequency of price overreactions”, *Financial Markets and Portfolio Management*, 33, 2, 109-131.
- Caporale, G.M. and A. Plastun (2019c), “Price overreactions in the cryptocurrency market”, *Journal of Economic Studies*, 46, 5, 1137-1155.
- Caporale, G.M., Luis-Alana, L. and A. Plastun (2018), “Persistence in the cryptocurrency market”, *Research in International Business and Finance*, 46, 141-148.
- 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.
- Caporale, G.M., Kang, W.-Y., Spagnolo, F. and N. Spagnolo (2019), “Non-linearities, cyber attacks and cryptocurrencies”, *Finance Research Letters*, 7692, 1 - 10.
- Caporale, G.M., Kang, W.-Y., Spagnolo, F. and N. Spagnolo (2020), “Cyber-attacks and cryptocurrencies”, WP no. 20-03, Department of Economics and Finance, Brunel University London, and CESifo WP no.8124.
- Ciaian, P., Rajcaniova, M. and K. d’Artis (2018), “Virtual relationships: short- and long-run evidence from Bitcoin and Altcoin markets”, *Journal of International Financial Markets, Institutions and Money*, 52-173-195.

Conlon, T. and R. McGee (2020), “Safe Haven or Risky Hazard? Bitcoin during the COVID-19 Bear Market”, Available at SSRN: <https://ssrn.com/abstract=3560361>.

Corbet, S., Meegan, A., Larkin, C., Lucey, B. and L. Yarovaya (2018), “Exploring the dynamic relationships between cryptocurrencies and other financial assets”, *Economics Letters*, 165, 28-24.

Corbet, S., Larkin, C. and B. Lucey (2020), “The contagion effects of the COVID-19 pandemic: evidence from gold and cryptocurrencies”, mimeo, Dublin City University Business School.

Diebold, F.X. and K. Yilmaz (2012), “Better to give than to receive: predictive directional measurement of volatility spillovers”, *International Journal of Forecasting*, 28, 1, 57-66.

Diebold, F.X. and K. Yilmaz (2016), “Trans-Atlantic equity volatility connectedness: U.S. and European financial institutions, 2004-2014”, *Journal of Financial Econometrics*, 14, 81-127.

Dwyer, G.P (2015), “The economics of Bitcoin and similar private digital currencies”, *Journal of Financial Stability*, 17, 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.

Feng, W., Y. Wang, and Z. Zhang (2018), “Can cryptocurrencies be a safe haven: a tail risk perspective analysis”, *Applied Economics*, 50, 44, 4745–4762.

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.

Forbes, K.J. and R. Rigobon (2002), “No contagion, only interdependence: measuring stock market comovements”, *Journal of Finance*, 57, 5, 2223-2261.

Fry, J. (2018), “Booms, busts and heavy-tails: The story of Bitcoin and cryptocurrency markets”, *Economics Letters*, 171, 225-229.

Fry, J. and E.-T. Cheah (2016), “Negative bubbles and shocks in cryptocurrency markets”, *International Review of Financial Analysis*, 47, 343-352.

Gil-Alana, L., E. Abakah, and M. Rojo (2020). “Cryptocurrencies and stock market indices. are they related?”, *Research in International Business and Finance*, 51.

Harvey, C. (2016), “Cryptofinance”, Available at SSRN: <https://ssrn.com/abstract=2438299>.

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

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

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*.

Ji, Q., Bouri, E., Lau, C.K.M. and D. Roubaud (2019), “Dynamic connectedness and integration in cryptocurrency markets”, *International Review of Financial Analysis*, 63, 257-272

Katsiampa, P. (2019), “An empirical investigation of volatility dynamics in the cryptocurrency market”, *Research in International Business and Finance*, 50, 322-335.

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

Koutmos, D. (2018), “Return and volatility spillovers among cryptocurrencies”, *Economics Letters*, 173, 122–127.

Lee, D.K.C., Guo, L., Wang, Y., (2018), “Cryptocurrency: a new investment opportunity?”, *Journal of Alternative Investments*, 20 (3), 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, W. (2019), “Portfolio diversification across cryptocurrencies”, *Finance Research Letters*, 29, 200–205.

Liu, Y. and Tsyvinski, A. (2018), “Risks and returns of cryptocurrency. Technical report”, *National Bureau of Economic Research, Working Paper No. 24877*.

Ljung, G. M., and G. E. P. Box. 1978. “On a Measure of Lack of Fit in Time Series Models” *Biometrika*, 65, 297–303.

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

Nadarajah, S. and Chu, J. (2017), “On the inefficiency of Bitcoin”, *Economics Letters*, 150, 6–9.

Omane-Adjepong, M. and I.P. Alagidede (2019), “Multiresolution analysis and spillovers of major cryptocurrency markets”, *Research in International Business and Finance*, 49, 191-206.

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*.

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

Tiwari, A., I. Raheem, and S. Kang (2019), “Time-varying dynamic conditional correlation between stock and cryptocurrency markets using the copula-ADCC-EGARCH model”, *Physica A: Statistical Mechanics and its Applications*, 535.

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.

Yermack, D. (2018), “The potential of digital currency and blockchains”, *NBER Reporter*, 1, 14.17

Yi, S., Xu, Z. and Wang G-J. (2018), “Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?”, *International Review of Financial Analysis*, 60, 98–114

Table 1. Data description

Variable	Description
Government	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.
Industry	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.
Financial	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.
TARGET	The aggregate number of daily attacks targeting Government, Industry and Finance sectors, which may happen multiple times per day. To avoid the dummy variable trap, all other sectors are not included in the count.
Cyber Crime	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.
Cyber Espionage	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.
Cyber Warfare	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.
Hacktivism	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.
TYPE	The aggregate number of daily Cyber Crime, Cyber Espionage and Cyber Warfare attacks, which may happen multiple times per day. To avoid the dummy variable trap, Hacktivism is not included in the count.
USA	Cyber-attack targeting the USA. 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.
Bitcoin	Bitcoin log returns
Ethereum	Ethereum log returns
Litecoin	Litecoin log returns
VIX	Chicago Board Options Exchange (CBOE) volatility index

Notes: Data covers the period from 1 March 2015 to 15 January 2020.

Table 2. Descriptive Statistics

Variables	Mean	Median	S.D.	Min	Max	Obs.	No. of attacks	(% Attacks)
Crypto Currencies and VIX								
Bitcoin	0.002	0.002	0.039	-0.190	0.240	1316		
Ethereum	0.003	-0.001	0.068	-0.285	0.381	1316		
Litecoin	0.002	-0.001	0.059	-0.315	0.595	1316		
VIX	15.02	13.65	4.482	9.140	37.32	1316		
Cyber-attacks to Cryptocurrencies								
Crypto	0.077	0	0.277	0	2	1316	97	(7.4%)
Cyber-attacks by Type								
Cyber Crime	2.808	2	2.011	0	12	1316		
Cyber Espionage	0.411	0	0.681	0	5	1316		
Cyber Warfare	0.116	0	0.370	0	4	1316		
Hactivism	0.233	0	0.515	0	3	1316		
Type	3.334	3	2.246	0	13	1316	1276	(97.0%)
Cyber-attacks by Target								
Government	0.486	0	0.699	0	5	1316		
Industry	0.888	1	1.020	0	6	1316		
Financial	0.202	0	0.471	0	3	1316		
Target	1.575	1	1.332	0	7	1316	1036	(78.8%)
Cyber-attacks to US								
US	1.350	1	1.259	0	9	1316	952	(72.4%)

Notes: S.D. refers to sample standard deviation. No. of attacks (% Attacks) is the number of days (percentage of days) where at least one attack occurred. The total number of attacks occurred over the sample period and % of days where at least one cyber-attack was registered are also reported. The cyber-attack indicator Target is the cumulative index of cyber-attacks targeting Government, Industry and Financial sector, whereas the cyber-attack indicator Type is the cumulative index of cyber-crime, cyber-espionage and cyber-warfare. Cyber-attacks to USA register attacks to companies who are fiscally registered in the USA.



Table 3. Multivariate GARCH(1,1) Parameters Estimates – Crypto Currencies Cyber-Attacks

No cyber-attacks			Number of cyber-attacks per day					
			1		2		1-2	
Conditional Mean Equation								
$\alpha_1$	0.005 ***	(0.012)						
$\alpha_2$	0.002***	(0.050)						
$\alpha_3$	0.011**	(0.062)						
$\beta_{11}$	0.002	(0.965)						
$\beta_{12}$	0.012	(0.443)	$\beta_{12}^*$	0.034	(0.533)	0.011	(0.973)	0.058 (0.133)
$\beta_{13}$	-0.014	(0.571)	$\beta_{13}^*$	-0.041	(0.515)	-0.068	(0.992)	-0.052 (0.345)
$\beta_{22}$	0.023	(0.651)						
$\beta_{21}$	-0.114	(0.162)	$\beta_{21}^*$	-0.145***	(0.009)	-0.099	(0.995)	-0.166*** (0.022)
$\beta_{23}$	0.021	(0.675)	$\beta_{23}^*$	-0.031	(0.356)	0.113	(0.987)	-0.018 (0.558)
$\beta_{33}$	-0.036	(0.465)						
$\beta_{31}$	-0.037	(0.753)	$\beta_{31}^*$	-0.117**	(0.023)	-0.081	(0.634)	-0.118** (0.057)
$\beta_{32}$	0.022	(0.689)	$\beta_{32}^*$	-0.021	(0.551)	0.034	(0.971)	0.063* (0.063)
Vix => Bitcoin	-0.043*	(0.072)						
Vix => Ethereum	-0.061*	(0.083)						
Vix => Litecoin	-0.065*	(0.077)						
Conditional Variance Equation								
$a_{11}$	0.263 ***	(0.000)						
$a_{12}$	-0.001	(0.896)	$a_{12}^*$	-0.043	(0.285)	0.131	(0.669)	-0.061 (0.225)
$a_{13}$	0.026	(0.332)	$a_{13}^*$	-0.039	(0.414)	0.168	(0.561)	-0.041 (0.506)
$a_{22}$	0.327***	(0.000)						
$a_{21}$	-0.195**	(0.055)	$a_{21}^*$	-0.162***	(0.043)	0.256	(0.872)	-0.357*** (0.050)
$a_{23}$	0.061	(0.342)	$a_{23}^*$	-0.177**	(0.027)	0.144	(0.748)	-0.368*** (0.001)
$a_{33}$	0.345***	(0.001)						
$a_{31}$	-0.401**	(0.021)	$a_{31}^*$	-0.333***	(0.001)	0.065	(0.989)	-0.598*** (0.009)
$a_{32}$	0.145***	(0.000)	$a_{32}^*$	-0.404***	(0.000)	0.447	(0.889)	-0.479*** (0.000)
$g_{11}$	0.957***	(0.000)						
$g_{12}$	0.001	(0.852)	$g_{12}^*$	0.011	(0.715)	0.058	(0.299)	-0.018 (0.649)
$g_{13}$	-0.003	(0.749)	$g_{13}^*$	0.063	(0.131)	-0.203	(0.573)	0.091 (0.008)
$g_{22}$	0.952***	(0.000)						
$g_{21}$	0.072**	(0.025)	$g_{21}^*$	0.052	(0.411)	-0.151	(0.953)	0.109 (0.317)
$g_{23}$	-0.034*	(0.079)	$g_{23}^*$	0.071**	(0.039)	0.449	(0.888)	0.249*** (0.007)
$g_{33}$	0.907***	(0.000)						
$g_{31}$	0.144***	(0.002)	$g_{31}^*$	-0.212***	(0.000)	0.096	(0.763)	-0.361** (0.085)
$g_{32}$	-0.036***	(0.006)	$g_{32}^*$	0.138***	(0.000)	0.002	(0.901)	0.244*** (0.000)
Log-Lik	7248.12			7328.73		7262.31		7311.54
LB <sub>10</sub> (Bit)	4.565			4.221		4.324		4.443
LB <sub>2</sub> <sub>10</sub> (Bit)	4.108			4.311		4.287		4.178
LB <sub>10</sub> (Eih)	3.443			3.801		3.901		3.908
LB <sub>2</sub> <sub>10</sub> (Eih)	3.761			3.773		3.744		3.774
LB <sub>10</sub> (Lit)	3.852			3.991		3.664		3.793
LB <sub>2</sub> <sub>10</sub> (Lit)	3.778			4.113		4.101		4.111

Notes: P-values are calculated using the quasi-maximum likelihood method of Bollerslev and Wooldridge (1992), which is robust to the distribution of the underlying residuals. \*\*\* \*\* \* denote rejection at the 1%, 5%, and 10% levels. Point estimates reported in the second column, headed No attacks, refer to the restricted model where attacks were not taken into account and therefore shift dummies are not included. In the other columns only cross currencies shift parameters, with dummies associated to the number of attacks according to the Crypto indicator, are reported. LB<sub>10(c)</sub> and LB<sub>2</sub><sub>10(c)</sub> are the Ljung–Box test (1978) of significance of no autocorrelations of 10 lags in the standardized and standardized squared residuals, respectively. The parameter  $\beta_{21}$  measures the causality effect of Bitcoin returns on Ethereum returns, whereas  $a_{21}$  measures the causality-in-variance effect of Bitcoin returns volatility on Ethereum returns volatility. The effect of cyber-attacks on Ethereum returns is measured by  $(\beta_{21} + \beta_{21}^*)$  whereas  $(a_{21} + a_{21}^*)$  captures the effects on conditional volatility. The covariance stationarity condition is satisfied by all the estimated models, all the eigenvalues of  $A11 \otimes A11 + G11 \otimes G11$  being less than one in modulus. Note that in the conditional variance equation the sign of the parameters cannot be determined.

Table 4. Multivariate GARCH(1,1) Parameters Estimates – Cyber-Attacks by Type

No cyber-attacks			Number of cyber-attacks per day						
			1-2		3-4		> 5		
Conditional Mean Equation									
$\alpha_1$	0.005 ***	(0.012)							
$\alpha_2$	0.002***	(0.050)							
$\alpha_3$	0.011**	(0.062)							
$\beta_{11}$	0.002	(0.965)							
$\beta_{12}$	0.012	(0.443)	$\beta_{12}^*$	-0.037	(0.239)	0.064	(0.332)	-0.052	(0.604)
$\beta_{13}$	-0.014	(0.571)	$\beta_{13}^*$	0.116	(0.546)	0.098	(0.645)	-0.043	(0.444)
$\beta_{22}$	0.023	(0.651)							
$\beta_{21}$	-0.114	(0.162)	$\beta_{21}^*$	-0.122**	(0.017)	-0.031**	(0.021)	0.053	(0.863)
$\beta_{23}$	0.021	(0.675)	$\beta_{23}^*$	0.217	(0.783)	0.061	(0.426)	-0.251	(0.334)
$\beta_{33}$	-0.036	(0.465)							
$\beta_{31}$	-0.037	(0.753)	$\beta_{31}^*$	-0.291***	(0.004)	-0.174**	(0.062)	-0.054	(0.747)
$\beta_{32}$	0.022	(0.689)	$\beta_{32}^*$	-0.115	(0.140)	0.051	(0.319)	-0.071	(0.701)
Vix => Bitcoin	-0.043*	(0.072)							
Vix => Ethereum	-0.061*	(0.083)							
Vix => Litecoin	-0.065*	(0.077)							
Conditional Variance Equation									
$a_{11}$	0.263 ***	(0.000)							
$a_{12}$	-0.001	(0.896)	$a_{12}^*$	-0.011	(0.560)	0.008	(0.775)	0.003	(0.924)
$a_{13}$	0.026	(0.332)	$a_{13}^*$	0.012	(0.591)	-0.061	(0.173)	-0.089	(0.363)
$a_{22}$	0.327***	(0.000)							
$a_{21}$	-0.195**	(0.055)	$a_{21}^*$	-0.184**	(0.017)	-0.151**	(0.032)	-0.143*	(0.092)
$a_{23}$	0.061	(0.342)	$a_{23}^*$	0.014	(0.827)	0.003	(0.917)	0.062	(0.814)
$a_{33}$	0.345***	(0.001)							
$a_{31}$	-0.401**	(0.021)	$a_{31}^*$	-0.231**	(0.048)	-0.304***	(0.005)	-0.358**	(0.069)
$a_{32}$	0.145***	(0.000)	$a_{32}^*$	0.192*	(0.083)	-0.245*	(0.098)	-0.094	(0.091)
$g_{11}$	0.957***	(0.000)							
$g_{12}$	0.001	(0.852)	$g_{12}^*$	-0.002	(0.815)	-0.021	(0.302)	-0.002	(0.991)
$g_{13}$	-0.003	(0.749)	$g_{13}^*$	-0.007	(0.898)	0.029	(0.291)	0.028	(0.519)
$g_{22}$	0.952***	(0.000)							
$g_{21}$	0.072**	(0.025)	$g_{21}^*$	0.058**	(0.050)	0.229**	(0.048)	-0.085	(0.913)
$g_{23}$	-0.034*	(0.079)	$g_{23}^*$	-0.066	(0.244)	-0.227**	(0.038)	0.209	(0.667)
$g_{33}$	0.907***	(0.000)							
$g_{31}$	0.144***	(0.002)	$g_{31}^*$	0.098*	(0.013)	0.231***	(0.004)	0.180**	(0.050)
$g_{32}$	-0.036***	(0.006)	$g_{32}^*$	-0.007**	(0.043)	0.183**	(0.041)	0.114	(0.673)
Log-Lik	7248.12			7306.30		7285.98		7288.72	
LB <sub>10</sub> (Bit)	4.565			4.001		4.377		4.443	
LB <sub>2</sub> <sub>10</sub> (Bit)	4.108			4.231		4.341		4.178	
LB <sub>10</sub> (Eth)	3.443			3.888		4.108		3.908	
LB <sub>2</sub> <sub>10</sub> (Eth)	3.761			3.652		3.994		3.774	
LB <sub>10</sub> (Lit)	3.852			3.898		3.776		3.793	
LB <sub>2</sub> <sub>10</sub> (Lit)	3.778			4.231		4.007		4.111	

Notes: see notes Table 3.

Table 5. Multivariate GARCH(1,1) Parameters Estimates – Cyber-Attacks by Target

No cyber-attacks			Number of cyber-attacks per day						
			1-2		3-4		> 5		
Conditional Mean Equation									
$\alpha_1$	0.005 ***	(0.012)							
$\alpha_2$	0.002***	(0.050)							
$\alpha_3$	0.011**	(0.062)							
$\beta_{11}$	0.002	(0.965)							
$\beta_{12}$	0.012	(0.443)	$\beta_{12}^*$	0.002	(0.884)	0.049	(0.310)	0.063	(0.669)
$\beta_{13}$	-0.014	(0.571)	$\beta_{13}^*$	0.033	(0.347)	0.007	(0.829)	0.054	(0.687)
$\beta_{22}$	0.023	(0.651)							
$\beta_{21}$	-0.114	(0.162)	$\beta_{21}^*$	-0.234***	(0.001)	-0.315**	(0.026)	-0.516**	(0.044)
$\beta_{23}$	0.021	(0.675)	$\beta_{23}^*$	-0.102**	(0.065)	-0.172**	(0.080)	-0.432**	(0.033)
$\beta_{33}$	-0.036	(0.465)							
$\beta_{31}$	-0.037	(0.753)	$\beta_{31}^*$	-0.236***	(0.001)	-0.416**	(0.041)	-0.251**	(0.064)
$\beta_{32}$	0.022	(0.689)	$\beta_{32}^*$	-0.052	(0.214)	0.155***	(0.001)	0.266	(0.157)
Vix => Bitcoin	-0.043*	(0.072)							
Vix => Ethereum	-0.061*	(0.083)							
Vix => Litecoin	-0.065*	(0.077)							
Conditional Variance Equation									
$a_{11}$	0.263 ***	(0.000)							
$a_{12}$	-0.001	(0.896)	$a_{12}^*$	0.046	(0.291)	-0.016	(0.382)	0.097	(0.361)
$a_{13}$	0.026	(0.332)	$a_{13}^*$	-0.031	(0.518)	0.368	(0.583)	-0.302	(0.126)
$a_{22}$	0.327***	(0.000)							
$a_{21}$	-0.195**	(0.055)	$a_{21}^*$	0.112	(0.485)	-0.256**	(0.034)	-0.205**	(0.047)
$a_{23}$	0.061	(0.342)	$a_{23}^*$	-0.148***	(0.023)	0.002	(0.956)	0.101	(0.412)
$a_{33}$	0.345***	(0.001)							
$a_{31}$	-0.401**	(0.021)	$a_{31}^*$	-0.190**	(0.071)	-0.174**	(0.019)	-0.488**	(0.030)
$a_{32}$	0.145***	(0.000)	$a_{32}^*$	-0.050	(0.398)	0.095**	(0.013)	-0.427**	(0.014)
$g_{11}$	0.957***	(0.000)							
$g_{12}$	0.001	(0.852)	$g_{12}^*$	-0.012	(0.541)	-0.066	(0.665)	-0.098	(0.395)
$g_{13}$	-0.003	(0.749)	$g_{13}^*$	-0.044	(0.539)	0.057	(0.502)	0.139	(0.270)
$g_{22}$	0.952***	(0.000)							
$g_{21}$	0.072**	(0.025)	$g_{21}^*$	-0.021***	(0.002)	0.299***	(0.008)	-0.187	(0.428)
$g_{23}$	-0.034*	(0.079)	$g_{23}^*$	-0.085**	(0.036)	-0.056**	(0.097)	0.173	(0.268)
$g_{33}$	0.907***	(0.000)							
$g_{31}$	0.144***	(0.002)	$g_{31}^*$	0.121**	(0.053)	0.129***	(0.001)	0.442	(0.004)
$g_{32}$	-0.036***	(0.006)	$g_{32}^*$	0.049	(0.159)	-0.242***	(0.001)	-0.324**	(0.014)
Log-Lik	7248.12			7310.72		7193.24		7254.10	
LB <sub>10</sub> (Bit)	4.565			4.221		4.285		4.006	
LB <sub>210</sub> (Bit)	4.108			4.311		4.009		4.207	
LB <sub>10</sub> (Eih)	3.443			3.801		3.666		4.111	
LB <sub>210</sub> (Eih)	3.761			3.773		4.234		3.978	
LB <sub>10</sub> (Lit)	3.852			3.991		4.007		3.709	
LB <sub>210</sub> (Lit)	3.778			4.113		4.301		4.229	

Notes: see notes Table 3.

Table 6. Multivariate GARCH(1,1) Parameters Estimates – Cyber-Attacks to the United States

No cyber-attacks			Number of cyber-attacks per day						
			1-2		3-4		> 5		
Conditional Mean Equation									
$\alpha_1$	0.005 ***	(0.012)							
$\alpha_2$	0.002***	(0.050)							
$\alpha_3$	0.011**	(0.062)							
$\beta_{11}$	0.002	(0.965)							
$\beta_{12}$	0.012	(0.443)	$\beta_{12}^*$	0.002	(0.895)	-0.022	(0.613)	-0.036	(0.718)
$\beta_{13}$	-0.014	(0.571)	$\beta_{13}^*$	-0.041	(0.101)	0.044	(0.339)	-0.115	(0.271)
$\beta_{22}$	0.023	(0.651)							
$\beta_{21}$	-0.114	(0.162)	$\beta_{21}^*$	-0.191**	(0.047)	-0.014**	(0.083)	-0.120**	(0.011)
$\beta_{23}$	0.021	(0.675)	$\beta_{23}^*$	-0.170	(0.126)	-0.071	(0.757)	0.013	(0.922)
$\beta_{33}$	-0.036	(0.465)							
$\beta_{31}$	-0.037	(0.753)	$\beta_{31}^*$	-0.122**	(0.092)	-0.107**	(0.029)	-0.104**	(0.034)
$\beta_{32}$	0.022	(0.689)	$\beta_{32}^*$	0.021	(0.592)	-0.073	(0.265)	-0.133	(0.338)
Vix => Bitcoin	-0.043*	(0.072)							
Vix => Ethereum	-0.061*	(0.083)							
Vix => Litecoin	-0.065*	(0.077)							
Conditional Variance Equation									
$a_{11}$	0.263 ***	(0.000)							
$a_{12}$	-0.001	(0.896)	$a_{12}^*$	0.031	(0.542)	0.022	(0.496)	-0.121	(0.105)
$a_{13}$	0.026	(0.332)	$a_{13}^*$	0.017	(0.651)	0.012	(0.709)	-0.316	(0.186)
$a_{22}$	0.327***	(0.000)							
$a_{21}$	-0.195**	(0.055)	$a_{21}^*$	-0.085**	(0.049)	-0.059**	(0.047)	-0.077**	(0.054)
$a_{23}$	0.061	(0.342)	$a_{23}^*$	-0.138**	(0.021)	-0.106**	(0.045)	0.165	(0.564)
$a_{33}$	0.345***	(0.001)							
$a_{31}$	-0.401**	(0.021)	$a_{31}^*$	-0.037**	(0.088)	-0.039**	(0.050)	-0.031**	(0.018)
$a_{32}$	0.145***	(0.000)	$a_{32}^*$	0.218***	(0.001)	0.126*	(0.095)	0.070*	(0.083)
$g_{11}$	0.957***	(0.000)							
$g_{12}$	0.001	(0.852)	$g_{12}^*$	-0.013	(0.444)	-0.015	(0.433)	-0.052	(0.541)
$g_{13}$	-0.003	(0.749)	$g_{13}^*$	-0.023	(0.488)	-0.011	(0.608)	0.066	(0.266)
$g_{22}$	0.952***	(0.000)							
$g_{21}$	0.072**	(0.025)	$g_{21}^*$	0.031*	(0.067)	0.094*	(0.097)	0.004**	(0.062)
$g_{23}$	-0.034*	(0.079)	$g_{23}^*$	-0.001	(0.980)	-0.023**	(0.015)	-0.039	(0.811)
$g_{33}$	0.907***	(0.000)							
$g_{31}$	0.144***	(0.002)	$g_{31}^*$	0.053**	(0.031)	0.124**	(0.014)	0.352**	(0.059)
$g_{32}$	-0.036***	(0.006)	$g_{32}^*$	-0.122***	(0.001)	0.074*	(0.071)	-0.274***	(0.015)
Log-Lik	7248.12			7299.66		7259.67		7253.74	
LB <sub>10</sub> (Bit)	4.565			4.156		4.004		4.612	
LB <sub>210</sub> (Bit)	4.108			4.443		4.307		4.220	
LB <sub>10</sub> (Eih)	3.443			3.976		4.132		3.879	
LB <sub>210</sub> (Eih)	3.761			3.697		3.807		3.664	
LB <sub>10</sub> (Lit)	3.852			3.878		3.776		3.991	
LB <sub>210</sub> (Lit)	3.778			4.009		4.224		3.978	

Notes: see notes Table 3.

Table 7. Tests of Changes in Conditional Correlations

Number of cyber-attacks per day	Total Number of cyber-attacks (% over the total)	Correlations								
		Bitcoin - Litecoin			Bitcoin - Ethereum			Ethereum - Litecoin		
		Mean	Variance	Reject H <sub>0</sub>	Mean	Variance	Reject H <sub>0</sub>	Mean	Variance	Reject H <sub>0</sub>
No Attacks										
None	N/A	0.665	0.225		0.473	0.358		0.489	0.376	
Cyber-Attacks to Crypto Currencies										
1	93 (7.1%)	0.671 (0.479)	0.182 (0.258)	***	0.631 (0.457)	0.183 (0.356)	***	0.662 (0.448)	0.189 (0.389)	***
2	4 (0.3%)	0.662 (0.468)	0.238 (0.225)	***	0.725 (0.473)	0.342 (0.366)	***	0.627 (0.496)	0.337 (0.378)	***
Total (1-2)	97 (7.4%)	0.670 (0.467)	0.186 (0.224)	***	0.633 (0.473)	0.184 (0.356)	***	0.661 (0.496)	0.188 (0.371)	***
Cyber-Attacks by Type										
1-2	544 (41.4%)	0.617 (0.696)	0.336 (0.379)	***	0.387 (0.524)	0.315 (0.384)	***	0.381 (0.547)	0.321 (0.393)	***
3-4	390 (29.6%)	0.625 (0.681)	0.316 (0.359)	***	0.469 (0.511)	0.289 (0.372)	*	0.465 (0.526)	0.281 (0.364)	***
>5	342 (26.0%)	0.721 (0.637)	0.283 (0.317)	***	0.563 (0.441)	0.258 (0.402)	***	0.624 (0.467)	0.278 (0.385)	***
Total	1276 (97.0%)									
Cyber-Attacks by Target										
1-2	762 (57.9%)	0.642 (0.711)	0.369 (0.377)	***	0.464 (0.525)	0.371 (0.354)	***	0.487 (0.555)	0.356 (0.355)	***
3-4	231 (17.5%)	0.701 (0.661)	0.279 (0.321)	***	0.474 (0.472)	0.235 (0.336)		0.489 (0.481)	0.233 (0.384)	
> 5	43 (3.4%)	0.779 (0.654)	0.142 (0.248)	**	0.656 (0.664)	0.125 (0.402)		0.519 (0.689)	0.111 (0.371)	
Total	1036 (78.8%)									
Cyber-Attacks to the US										
1-2	745 (56.7%)	0.666 (0.672)	0.367 (0.361)	*	0.375 (0.491)	0.375 (0.361)	*	0.362 (0.533)	0.366 (0.351)	***
3-4	172 (13.1%)	0.691 (0.662)	0.244 (0.301)		0.485 (0.467)	0.216 (0.411)		0.385 (0.501)	0.209 (0.372)	
>5	35 (2.6%)	0.797 (0.664)	0.131 (0.245)		0.558 (0.481)	0.108 (0.373)		0.539 (0.502)	0.105 (0.348)	
Total	952 (72.4%)									

Notes: Averages and standard deviations of pairwise conditional correlations ( $\rho_{12,t}$ ,  $\rho_{13,t}$ , and  $\rho_{23,t}$ ) for sub-samples including days where cyber-attacks occurred are reported whereas averages and standard deviations of pairwise conditional correlations for sub-samples including days where cyber-attacks were not registered are reported in round brackets. The null hypothesis of equal correlation means among the latters and the former are tested. \*\*\*, \*\*, \* denote rejection of the null hypothesis of an equal conditional correlation ( $H_0$ : Corr. without Cyber Attacks = Corr. with Cyber Attacks) against the alternative ( $H_1$ : Corr. without Cyber Attacks  $\neq$  Corr. with Cyber Attacks) at the 1%, 5%, and 10% levels respectively.

Figure 1. Cryptocurrencies

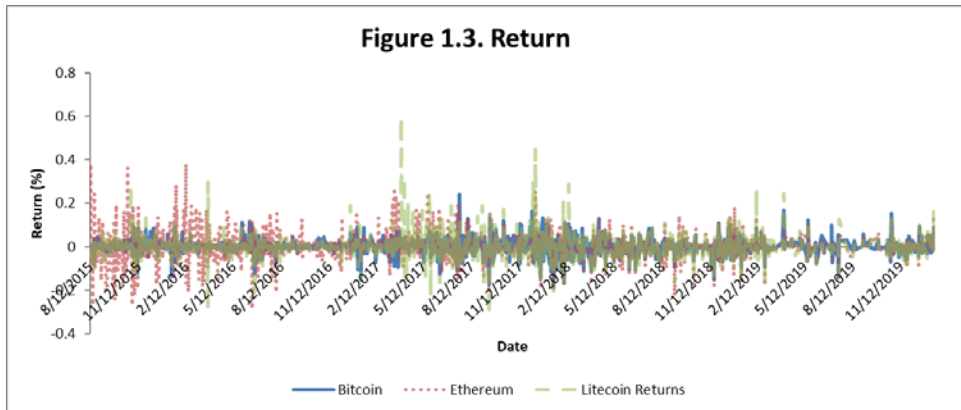
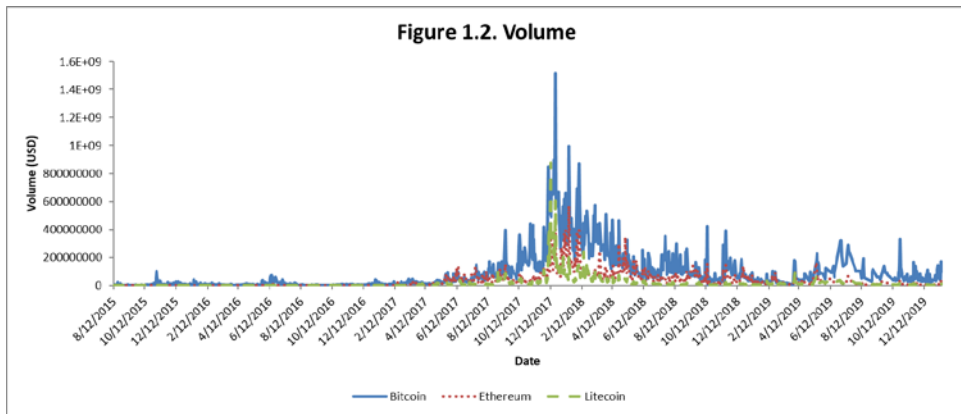
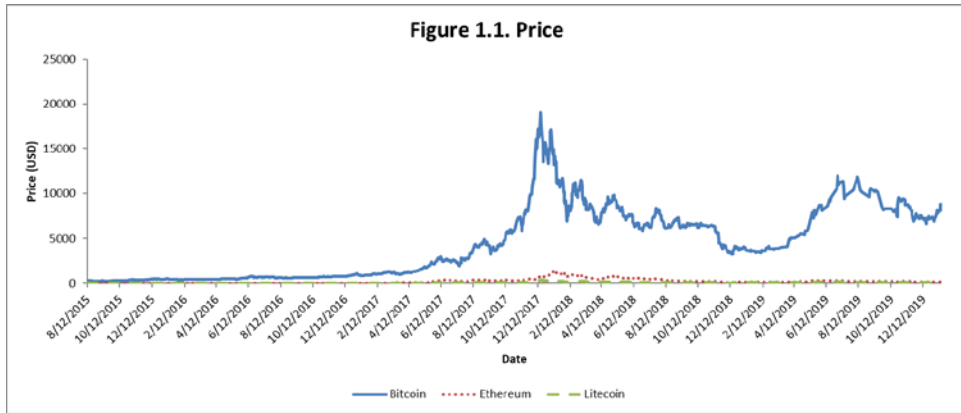


Figure 2. Cyber-Attacks by Target

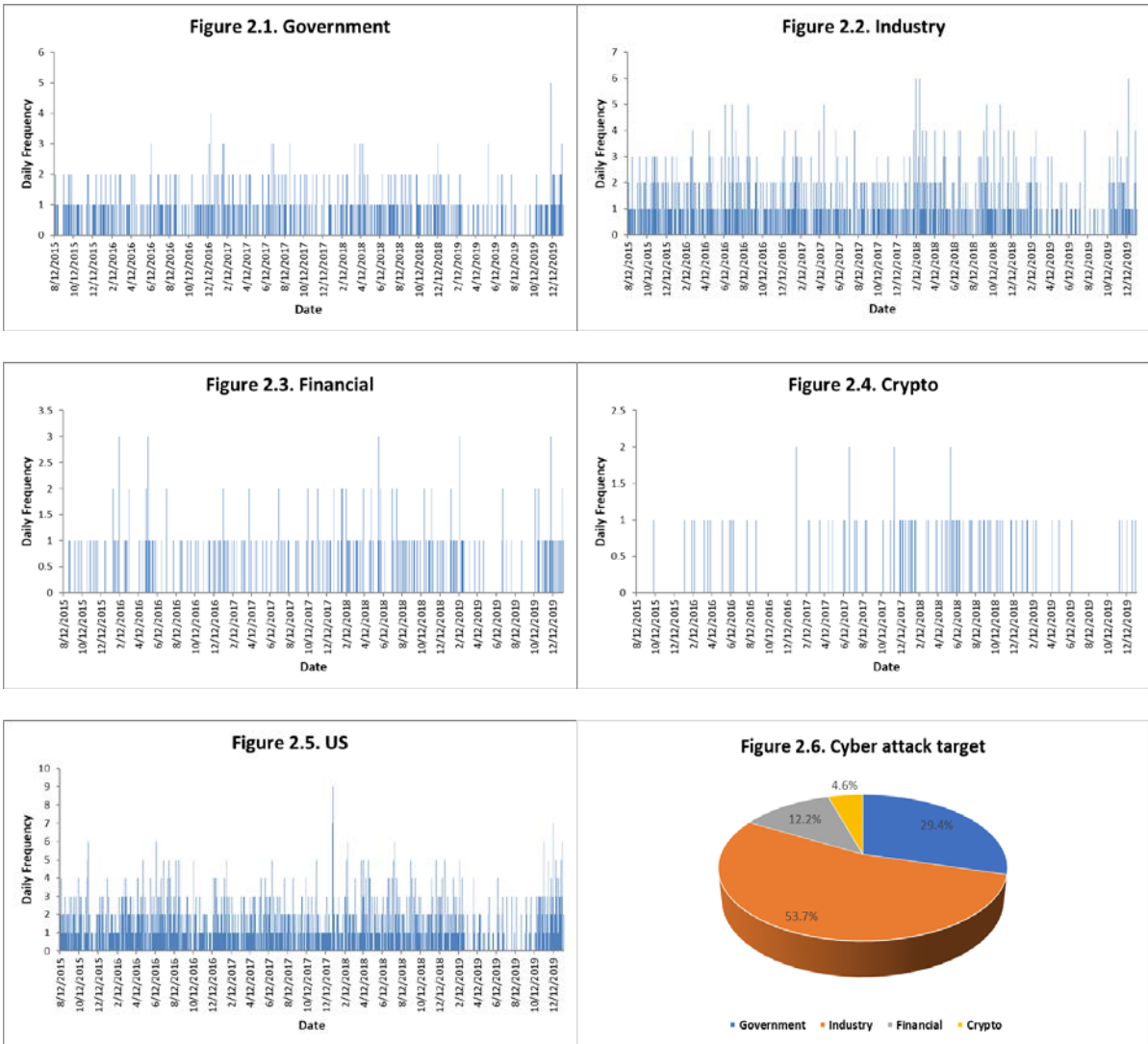


Figure 3. Cyber-Attacks by Type

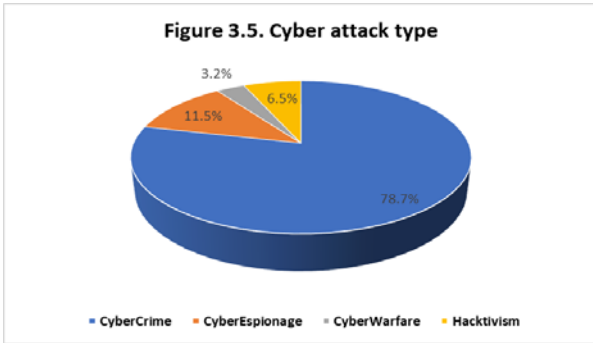
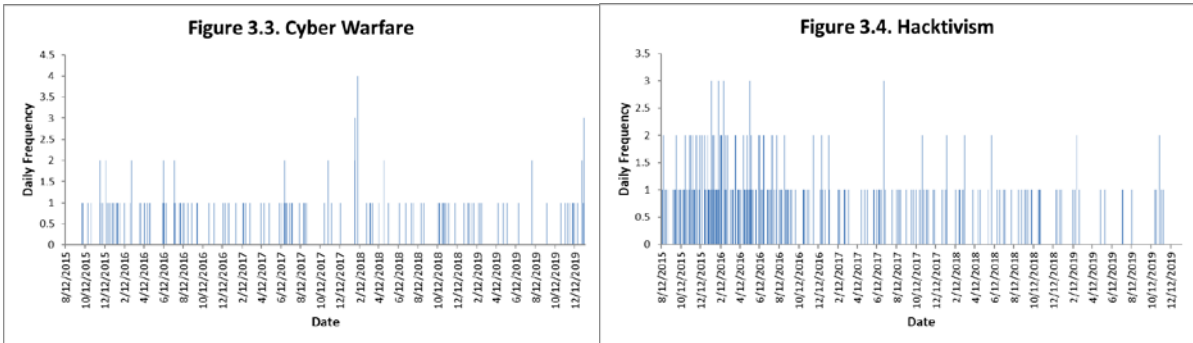
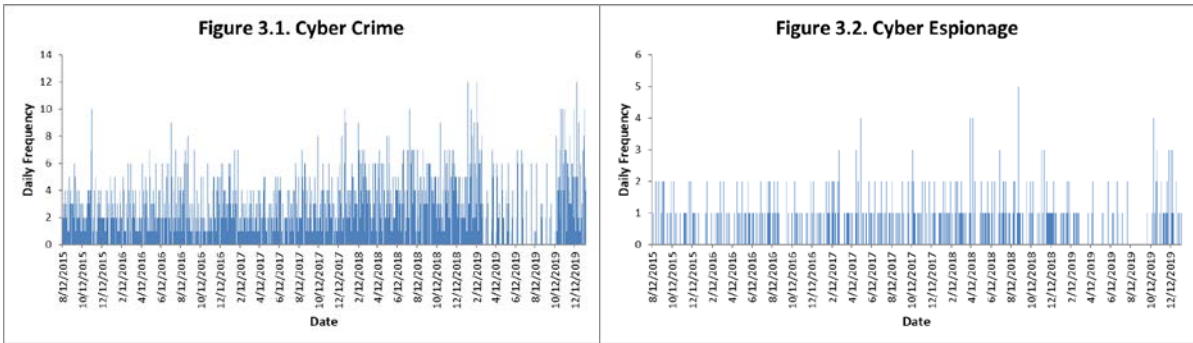




Figure 4. Conditional Correlations

