J. Int. Financ. Markets Inst. Money 74 (2021) 101298

Contents lists available at ScienceDirect

Journal of International Financial Markets, Institutions & Money

journal homepage: www.elsevier.com/locate/intfin

Cyber-attacks, spillovers and contagion in the cryptocurrency markets

Guglielmo Maria Caporale [a,*], Woo-Young Kang [a], Fabio Spagnolo [a], Nicola Spagnolo [a,b]

[a] Department of Economics and Finance, Brunel University London, Uxbridge, Middlesex UB8 3PH, United Kingdom
[b] Centre for Applied Macroeconomic Analysis (CAMA), Canberra, Australia

ARTICLE INFO

Article history:
Received 12 May 2020
Accepted 14 January 2021
Available online 18 January 2021

JEL Classification:
C32
F30
G15

Keywords:
Crypto currencies
Cyber-attacks
Mean and volatility spillovers
Contagion

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) between the three cryptocurrencies under investigation are found in most cases when cyber-attacks are taken into account, Bitcoin appearing to be the dominant cryptocurrency. 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.

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., 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, 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., 2019), 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

* Corresponding author.
E-mail address: Guglielmo-Maria.Caporale@brunel.ac.uk (G.M. Caporale).

https://doi.org/10.1016/j.intfin.2021.101298
1042-4431/

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.

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 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 collected from Hackmageddon (http://www.hackmageddon.com). These are classified by target sectors (government, industry, financial institution and cryptocurrency), attack nature (cyber-crime, cyber espionage, cyber warfare and hacktivism) and target country (US versus non-US).

We find that cyber-attacks targeting cryptocurrencies have a major impact on the dynamic linkages between the three cryptocurrencies under examination, especially in the case of their second moments, and that Bitcoin plays a dominant role

[1] 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.

vis-à-vis Litecoin and Ethereum. Furthermore, the conditional correlations between these three cryptocurrencies are generally positive, and they are higher in the subsample including only days with cyber-attacks, the largest shifts in the correlation parameters occurring when cyber-attacks target cryptocurrencies. Therefore, cyber-attacks strengthen cross-market linkages and consequently reduce portfolio diversification opportunities for cryptocurrency investors.

It is noteworthy that the capital raised for FinTech development has been rising exponentially. Global investment in Fintech companies reached $57 billion in the first half of 2018, up from $38.1 billion over the whole of 2017 (KPMG, 2018), and major financial institutions and technology firms have been increasing their investment in Fintech innovation (Nash, 2016; Russo, 2017; Chen et al., 2019). However, despite widespread interest across the globe the finance literature focusing on Fintech is still very limited (Chen et al., 2019; Goldstein et al., 2019). Fintech can be classified in seven categories (Chen et al., 2019): cybersecurity, mobile transactions, data analytics, blockchain, peer-to-peer (P2P), robo-advising and internet of things (IoT).[2] Our paper adds to the understanding of Fintech in its blockchain and cybersecurity aspects and contributes to the literature on asset diversification.

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:

$$x_t = \alpha + \beta x_{t-1} + f z_{t-1} + e_t \tag{1}$$

where x_t = (Bitcoin$_t$, Ethereum$_t$, 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 Eq. (1) comprise the constant terms $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ and the parameters of the autoregressive terms $\beta = (\beta_{11}, \beta_{12}, \beta_{13} \mid \beta_{21}, \beta_{22}, \beta_{23} \mid \beta_{31}, \beta_{32}, \beta_{33})$, which allow for cross-currency mean return spillovers. The residual vector e_t is trivariate and normally distributed $e_t \mid I_{t-1} \sim (0, H_t)$ with its conditional variance–covariance matrix given by:

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

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:

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

Eq. (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 and G whose elements are the a and g coefficients respectively. 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[3] θ, and a 3×1 vector of variables x_t, the conditional density function for the model (1)–(3) is:

$$f(x_t | I_{t-1}; \theta) = (2\pi)^{-1} |H_t|^{-1/2} \exp\left(-\left[e_t' \left(H_t^{-1} \right) e_t \right] / 2 \right) \tag{4}$$

[2] 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.

[3] 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 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.

The log likelihood function is:

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

In recent years, sever types of models have been used to investigate cross-country co-movements. Among those, copula models have become increasingly popular. A comprehensive discussion of the pros and cons of using them rather than DCC and GARCH models can be found in Al Rahahleh and Bhatti (2017), Nguyen et al. (2017) and Bhatti and Do (2019). Given the nature of our research question, we have chosen to estimate reduced-form VAR models including a GARCH component because of their suitability to analyse both co-movement and spillover effects within the same econometric framework. Furthermore, the adopted BEKK representation guarantees by construction the positive-definiteness of the variance–covariance matrix.

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.[4] For instance, the equations for the conditional mean and variance of Bitcoin returns become respectively:

$$Bitcoin_t = \alpha_1 + \beta_{11} Bitcoin_{t-1} + (\beta_{12} + \beta^*_{12}) Ethereum_{t-1} + (\beta_{13} + \beta^*_{13}) Litecoin_{t-1} + fz_{t-1} + e_{2,t}$$

and

$$\begin{aligned} h_{11,t} &= c_{11}^2 + a_{11}^2 e_{1,t-1}^2 + a_{12}^2 e_{2,t-1}^2 + \left(a_{13} + a^*_{13} \hat{\mathrm{A}} \cdot D\right)^2 e_{3,t-1}^2 \\ &+ 2a_{11}a_{12}e_{1,t-1}e_{2,t-1} + 2a_{11}\left(a_{13} + a^*_{13}\hat{\mathrm{A}} \cdot D\right)e_{1,t-1}e_{3,t-1} + 2a_{12}\left(a_{13} + a^*_{13}\hat{\mathrm{A}} \cdot D\right)e_{2,t-1}e_{3,t-1} \\ &+ {g_{11}}^2 h_{11,t-1} + {g_{12}}^2 h_{22,t-1} + \left(g_{13} + {g_{13}}^* \hat{\mathrm{A}} \cdot D\right)^2 h_{33,t-1} \\ &+ 2g_{11}g_{12}h_{12,t-1} + 2g_{11}\left(g_{13} + {g_{13}}^* \hat{\mathrm{A}} \cdot D\right)h_{13,t-1} + 2g_{12\left(g_{13}+{g_{13}}^* \hat{\mathrm{A}} \cdot D\right)h_{23,t-1}} \end{aligned} \tag{6}$$

Mean spillovers from Ethereum and Litcoin to Bitcoin are measured by the parameters β_{12} and β_{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 parameters a_{12} and g_{12}, and a_{13} and g_{13} respectively; $a_{12}{}^*$ and $g_{12}{}^*$, and $a_{13}{}^*$ and $g_{13}{}^*$ instead capture shifts in these parameters during episodes of cyber-attacks.

3. Data set and identification of cyber-attacks

3.1. Crypto currencies

The trivariate GARCH model outlined in the preceding section was estimated for three crypto currencies (Bitcoin, Ethereum and Litecoin). The series are daily and have been collected from the website 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 12 August 2015 to 15 January 2020.[5] We then compute market capital-weighted indices which are based on the five exchanges. Natural log returns are used for the estimation of the models; these series are displayed in Fig. 1.

3.2. Cyber-attacks

The recent developments in networking and cyberspace technology, including cryptocurrencies and blockchain technology, have yielded significant benefits. However, the rapid growth in these fields has also been associated with the rise of

[4] See section 3.3 for details on the construction of the dummies.

[5] 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.

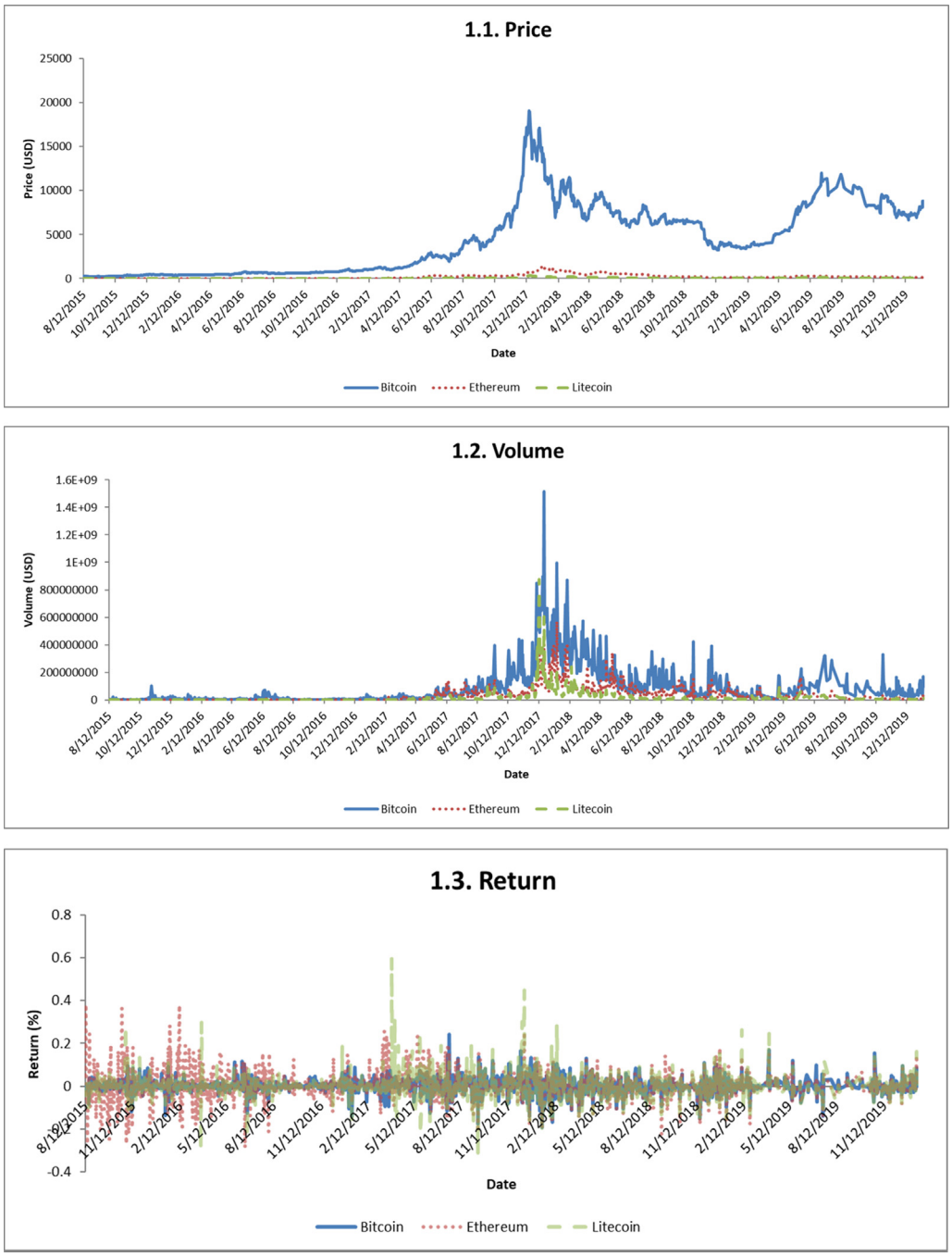


Fig. 1. Cryptocurrencies.

unethical practices to use these technologies to exploit others, such as cyber-attacks (Uma and Padmavathi, 2013), these being an attempt to damage, destroy or gain illegal access to a computer network or system (Bodford and Kwan, 2018).

The most common type of cyber-attack is "double-spending", when the attacker manipulates the blockchain consensus to secure a financial gain (Shanaev et al., 2019). This could be quite limited as the miner needs a substantial initial investment to purchase specialised hardware and the cryptocurrency price may drop significantly as a result of investors losing confidence in the market, especially if the attacker controls over 50% of the mining capacity in the blockchain (Kroll et al., 2013; Shanaev et al., 2019). However, the number of attempted and successful cyber-attacks on blockchains and cryptocurrencies has significantly increased over time for the following reasons. Firstly, cryptocurrency prices have risen sharply, which has made double-spending more attractive and profitable. Secondly, many altcoins (i.e., cryptocurrency coins other than Bitcoin)

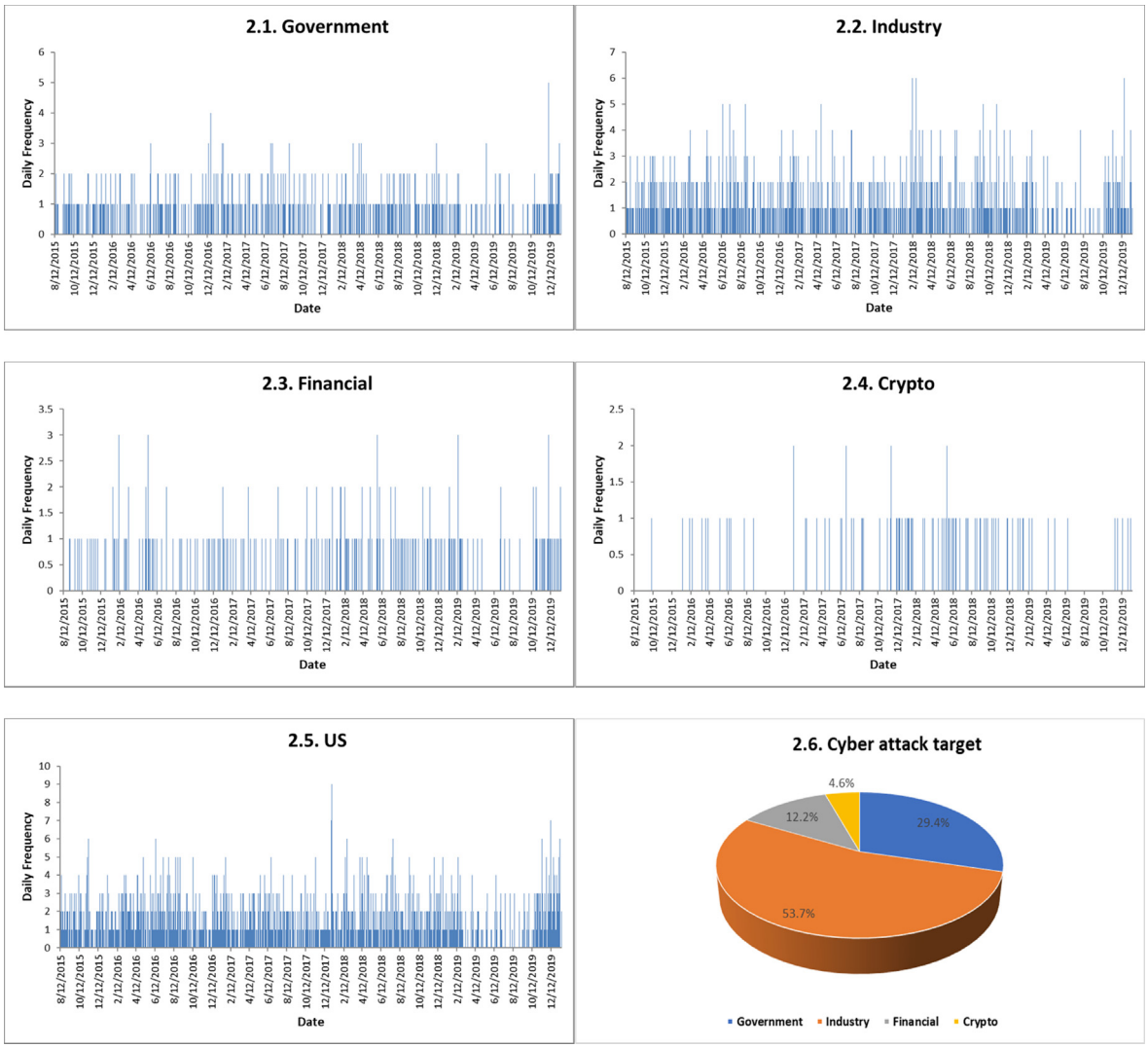


Fig. 2. Cyber-Attacks by Target.

have been introduced, including some which are much more vulnerable to cyber-attacks given their low hash rates and the very small involvement of communities. Thirdly, the mining industry has started to offer computational power for rent, which significantly lowers the initial investment required (Shanaev et al., 2019). An et al. (2020) argue that the negative impacts of cyber-attacks can be mitigated if the institutions protect investor better in anti-director rights (La Porta et al 2002), the degree of control on managers' self-dealing activities (Djankov et al. 2008), the extent to which lenders can collect a commercial debt at ease, and the level of protection on private foreign investment (Acemoglu and Johnson 2005), which institutions believe to be the most important for firm access to external finance.

For our analysis, we use cyber-attack data collected from Hackmageddon (http://www.hackmageddon.com) which are classified by target (Government, Industry, Financial and Crypto) and type (Cyber Crime, Cyber Espionage, Cyber Warfare and Hacktivism). These are updated regularly through public sources such as blogs and news sites, and therefore the sample collection cannot be complete, but it aims to provide a high level of overview of the cyber-attack threat landscape across the globe (Passeri, 2020). Specifically, our sample includes 4693 daily cyber-attacks observations between 12 August 2015 and 15 January 2020 including daily overlaps. We use the daily number of cyber-attacks as an indicator of potential threats to the digital economy. The data are also classified as attacks targeting either the US or non-US countries.

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 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 technol-

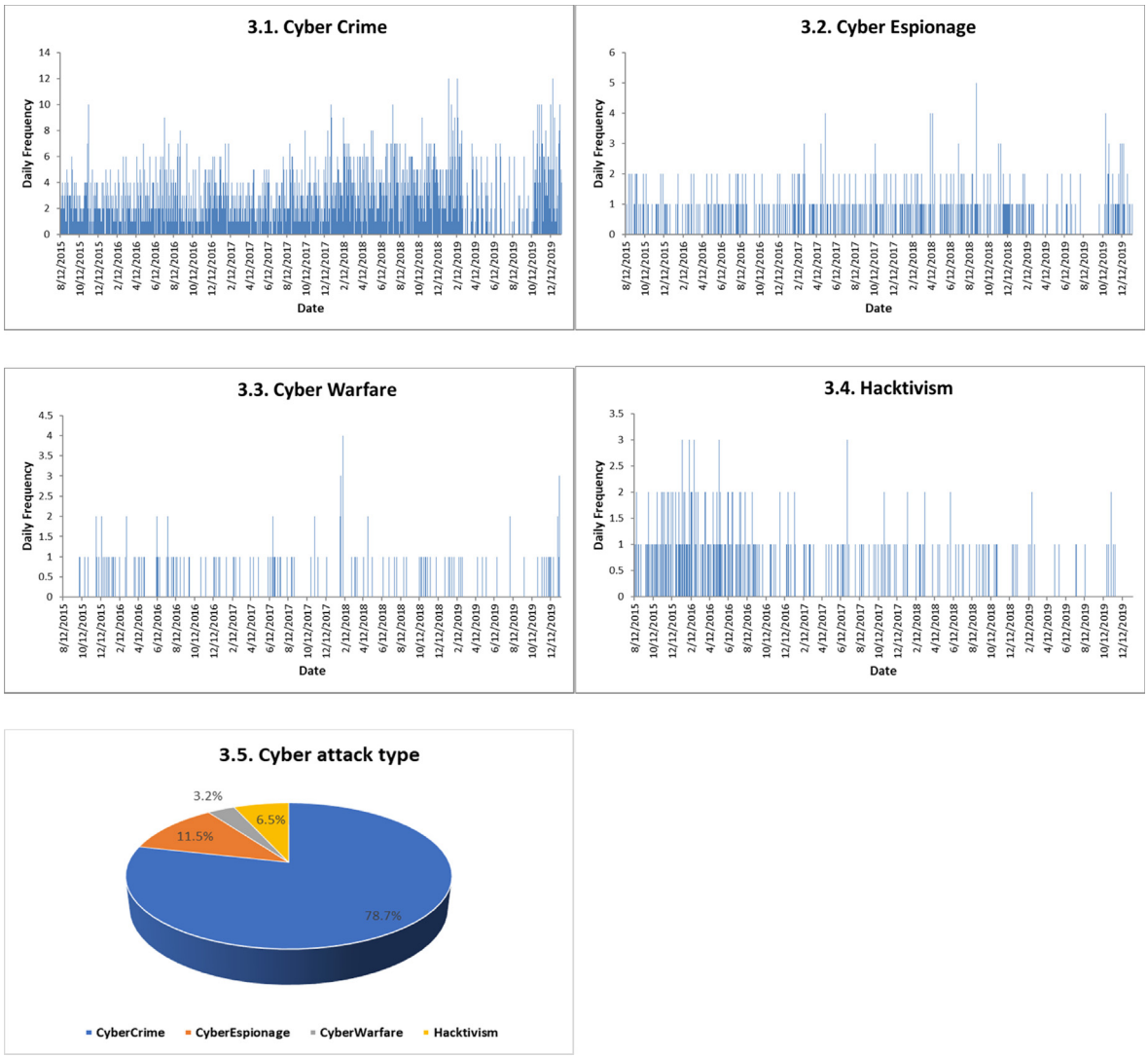


Fig. 3. Cyber-Attacks by Type.

ogy 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).

Figs. 2 and 3 show, respectively, the cyber-attack targets and types used for the analysis. It is apparent from Fig. 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.

Fig. 3 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. Within our sample, on any given day cyber-attacks can target one or more of the 122 countries considered (including 'unknown' countries). The US, Canada, the UK and India are the most frequently targeted across the globe (Appendix A and B).[6] There are 1173 occurrences of cyber-attacks targeting more than one country, which is the second most frequent case according to Appendix A – a plausible finding given the fact that by nature cyber-attacks are world-wide events without geographical restrictions.

[6] Appendix II visualises the number of cyber-attacks per day by country; a darker shade indicates more frequent attacks. The 'More than one country' and 'Unknown country' data from Appendix I are not included because they cannot be associated to specific countries.

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 12 August 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		
Hacktivism	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.

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

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

No cyber-attacks			Number of cyber-attacks per day					
			1–2		3–4		> 5	
Conditional Mean Equation								
α_1	0.005***	(0.012)						
α_2	0.002***	(0.050)						
α_3	0.011**	(0.062)						
β_{11}	0.002	(0.965)						
β_{12}	0.012	(0.443)	β_{12}^*	0.034	(0.533)	0.011	(0.973)	0.058	(0.133)
β_{13}	−0.014	(0.571)	β_{13}^*	−0.041	(0.515)	−0.068	(0.992)	−0.052	(0.345)
β_{22}	0.023	(0.651)						
β_{21}	−0.114	(0.162)	β_{21}^*	−0.145***	(0.009)	−0.099	(0.995)	−0.166***	(0.022)
β_{23}	0.021	(0.675)	β_{23}^*	−0.031	(0.356)	0.113	(0.987)	−0.018	(0.558)
β_{33}	−0.036	(0.465)						
β_{31}	−0.037	(0.753)	β_{31}^*	−0.117**	(0.023)	−0.081	(0.634)	−0.118**	(0.057)
β_{32}	0.022	(0.689)	β_{32}^*	−0.021	(0.551)	0.034	(0.971)	0.063*	(0.063)
VIX => Bitcoin	−0.043*	(0.072)						
VIX => Etherum	−0.061*	(0.083)						
VIX => Litcoin	−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	
$LB_{10\ (Bit)}$	4.565			4.221		4.324		4.443	
$LB2_{10\ (Bit)}$	4.108			4.311		4.287		4.178	
$LB_{10\ (Eth)}$	3.443			3.801		3.901		3.908	
$LB2_{10\ (Eth)}$	3.761			3.773		3.744		3.774	
$LB_{10\ (Lit)}$	3.852			3.991		3.664		3.793	
$LB2_{10\ (Lit)}$	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. $LB_{10(.)}$ and $LB2_{10(.)}$ are the Ljung and Box (1978) of significance of no autocorrelations of 10 lags in the standardized and standardized squared residuals, respectively. The parameter β_{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.

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

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								
α_1	0.005***	(0.012)						
α_2	0.002***	(0.050)						
α_3	0.011**	(0.062)						
β_{11}	0.002	(0.965)						
β_{12}	0.012	(0.443)	β_{12}*	−0.037	(0.239)	0.064	(0.332)	−0.052	(0.604)
β_{13}	−0.014	(0.571)	β_{13}*	0.116	(0.546)	0.098	(0.645)	−0.043	(0.444)
β_{22}	0.023	(0.651)						
β_{21}	−0.114	(0.162)	β_{21}*	−0.122**	(0.017)	−0.031**	(0.021)	0.053	(0.863)
β_{23}	0.021	(0.675)	β_{23}*	0.217	(0.783)	0.061	(0.426)	−0.251	(0.334)
β_{33}	−0.036	(0.465)						
β_{31}	−0.037	(0.753)	β_{31}*	−0.291***	(0.004)	−0.174**	(0.062)	−0.054	(0.747)
β_{32}	0.022	(0.689)	β_{32}*	−0.115	(0.140)	0.051	(0.319)	−0.071	(0.701)
VIX => Bitcoin	−0.043*	(0.072)						
VIX => Etherum	−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	
$LB_{10\ (Bit)}$	4.565			4.001		4.377		4.443	
$LB2_{10\ (Bit)}$	4.108			4.231		4.341		4.178	
$LB_{10\ (Eth)}$	3.443			3.888		4.108		3.908	
$LB2_{10\ (Eth)}$	3.761			3.652		3.994		3.774	
$LB_{10\ (Lit)}$	3.852			3.898		3.776		3.793	
$LB2_{10\ (Lit)}$	3.778			4.231		4.007		4.111	

Notes: see notes Table 3.

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).

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:

$$W = \left[R\widehat{\theta}\right]' \left[RVar\left(\widehat{\theta}\right)R'\right]^{-1} \left[R\widehat{\theta}\right] \tag{7}$$

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								
α_1	0.005***	(0.012)						
α_2	0.002***	(0.050)						
α_3	0.011**	(0.062)						
β_{11}	0.002	(0.965)						
β_{12}	0.012	(0.443)	β_{12}^*	0.002	(0.884)	0.049	(0.310)	0.063	(0.669)
β_{13}	−0.014	(0.571)	β_{13}^*	0.033	(0.347)	0.007	(0.829)	0.054	(0.687)
β_{22}	0.023	(0.651)						
β_{21}	−0.114	(0.162)	β_{21}^*	−0.234***	(0.001)	−0.315**	(0.026)	−0.516**	(0.044)
β_{23}	0.021	(0.675)	β_{23}^*	−0.102**	(0.065)	−0.172**	(0.080)	−0.432**	(0.033)
β_{33}	−0.036	(0.465)						
β_{31}	−0.037	(0.753)	β_{31}^*	−0.236***	(0.001)	−0.416**	(0.041)	−0.251**	(0.064)
β_{32}	0.022	(0.689)	β_{32}^*	−0.052	(0.214)	0.155***	(0.001)	0.266	(0.157)
VIX => Bitcoin	−0.043*	(0.072)						
VIX => Etherum	−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	
$LB_{10\ (Bit)}$	4.565			4.221		4.285		4.006	
$LB2_{10\ (Bit)}$	4.108			4.311		4.009		4.207	
$LB_{10\ (Eth)}$	3.443			3.801		3.666		4.111	
$LB2_{10\ (Eth)}$	3.761			3.773		4.234		3.978	
$LB_{10\ (Lit)}$	3.852			3.991		4.007		3.709	
$LB2_{10\ (Lit)}$	3.778			4.113		4.301		4.229	

Notes: see notes Table 3.

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; θ is a $k \times 1$ vector of the estimated parameters, and $Var\left(\widehat{\theta}\right)$ 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."

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								
α_1	0.005***	(0.012)						
α_2	0.002***	(0.050)						
α_3	0.011**	(0.062)						
β_{11}	0.002	(0.965)						
β_{12}	0.012	(0.443)	β_{12}*	0.002	(0.895)	−0.022	(0.613)	−0.036	(0.718)
β_{13}	−0.014	(0.571)	β_{13}*	−0.041	(0.101)	0.044	(0.339)	−0.115	(0.271)
β_{22}	0.023	(0.651)						
β_{21}	−0.114	(0.162)	β_{21}*	−0.191**	(0.047)	−0.014**	(0.083)	−0.120**	(0.011)
β_{23}	0.021	(0.675)	β_{23}*	−0.170	(0.126)	−0.071	(0.757)	0.013	(0.922)
β_{33}	−0.036	(0.465)						
β_{31}	−0.037	(0.753)	β_{31}*	−0.122**	(0.092)	−0.107**	(0.029)	−0.104**	(0.034)
β_{32}	0.022	(0.689)	β_{32}*	0.021	(0.592)	−0.073	(0.265)	−0.133	(0.338)
VIX => Bitcoin	−0.043*	(0.072)						
VIX => Etherum	−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	
$LB_{10\ (Bit)}$	4.565			4.156		4.004		4.612	
$LB2_{10\ (Bit)}$	4.108			4.443		4.307		4.220	
$LB_{10\ (Eth)}$	3.443			3.976		4.132		3.879	
$LB2_{10\ (Eth)}$	3.761			3.697		3.807		3.664	
$LB_{10\ (Lit)}$	3.852			3.878		3.776		3.991	
$LB2_{10\ (Lit)}$	3.778			4.009		4.224		3.978	

Notes: see notes Table 3.

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 $\rho_{13,t} = h_{13,t}/\left(\sqrt{h_{11,t}}\sqrt{h_{33,t}}\right)$, Ethereum and Bitcoin as $\rho_{23,t} = h_{23,t}/\left(\sqrt{h_{22,t}}\sqrt{h_{33,t}}\right)$, and Ethereum and Litecoin as $\rho_{12,t} = h_{12,t}/\left(\sqrt{h_{11,t}}\sqrt{h_{22,t}}\right.$, 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.

Table 7
Tests of Changes in Conditional Correlations.

Number of cyber-attacks per day	Total Number of cyber-attacks (% over the total)	Correlations								
		Bitcoin - Litcoin			Bitcoin - Ethereum			Ethereum - Litcoin		
		Mean	Variance	Reject H_0	Mean	Variance	RejectH_0	Mean	Variance	RejectH_0
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	0.182	***	0.631	0.183	***	0.662	0.189	***
		(0.479)	(0.258)		(0.457)	(0.356)		(0.448)	(0.389)	
2	4 (0.3%)	0.662	0.238	***	0.725	0.342	***	0.627	0.337	***
		(0.468)	(0.225)		(0.473)	(0.366)		(0.496)	(0.378)	
Total (1–2)	97 (7.4%)	0.670	0.186	***	0.633	0.184	***	0.661	0.188	***
		(0.467)	(0.224)		(0.473)	(0.356)		(0.496)	(0.371)	
Cyber-Attacks by Type										
1–2	544 (41.4%)	0.617	0.336	***	0.387	0.315	***	0.381	0.321	***
		(0.696)	(0.379)		(0.524)	(0.384)		(0.547)	(0.393)	
3–4	390 (29.6%)	0.625	0.316	***	0.469	0.289	*	0.465	0.281	***
		(0.681)	(0.359)		(0.511)	(0.372)		(0.526)	(0.364)	
>5	342 (26.0%)	0.721	0.283	***	0.563	0.258	***	0.624	0.278	***
		(0.637)	(0.317)		(0.441)	(0.402)		(0.467)	(0.385)	
Total	1276 (97.0%)									
Cyber-Attacks by Target										
1–2	762 (57.9%)	0.642	0.369	***	0.464	0.371	***	0.487	0.356	***
		(0.711)	(0.377)		(0.525)	(0.354)		(0.555)	(0.355)	
3–4	231 (17.5%)	0.701	0.279	***	0.474	0.235		0.489	0.233	
		(0.661)	(0.321)		(0.472)	(0.336)		(0.481)	(0.384)	
> 5	43 (3.4%)	0.779	0.142	**	0.656	0.125		0.519	0.111	
		(0.654)	(0.248)		(0.664)	(0.402)		(0.689)	(0.371)	
Total	1036 (78.8%)									
Cyber-Attacks to the US										
1–2	745 (56.7%)	0.666	0.367	*	0.375	0.375	*	0.362	0.366	***
		(0.672)	(0.361)		(0.491)	(0.361)		(0.533)	(0.351)	
3–4	172 (13.1%)	0.691	0.244		0.485	0.216		0.385	0.209	
		(0.662)	(0.301)		(0.467)	(0.411)		(0.501)	(0.372)	
>5	35 (2.6%)	0.797	0.131		0.558	0.108		0.539	0.105	
		(0.664)	(0.245)		(0.481)	(0.373)		(0.502)	(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 latter 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 ≠ Corr. with Cyber-attacks) at the 1%, 5%, and 10% levels respectively.

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.

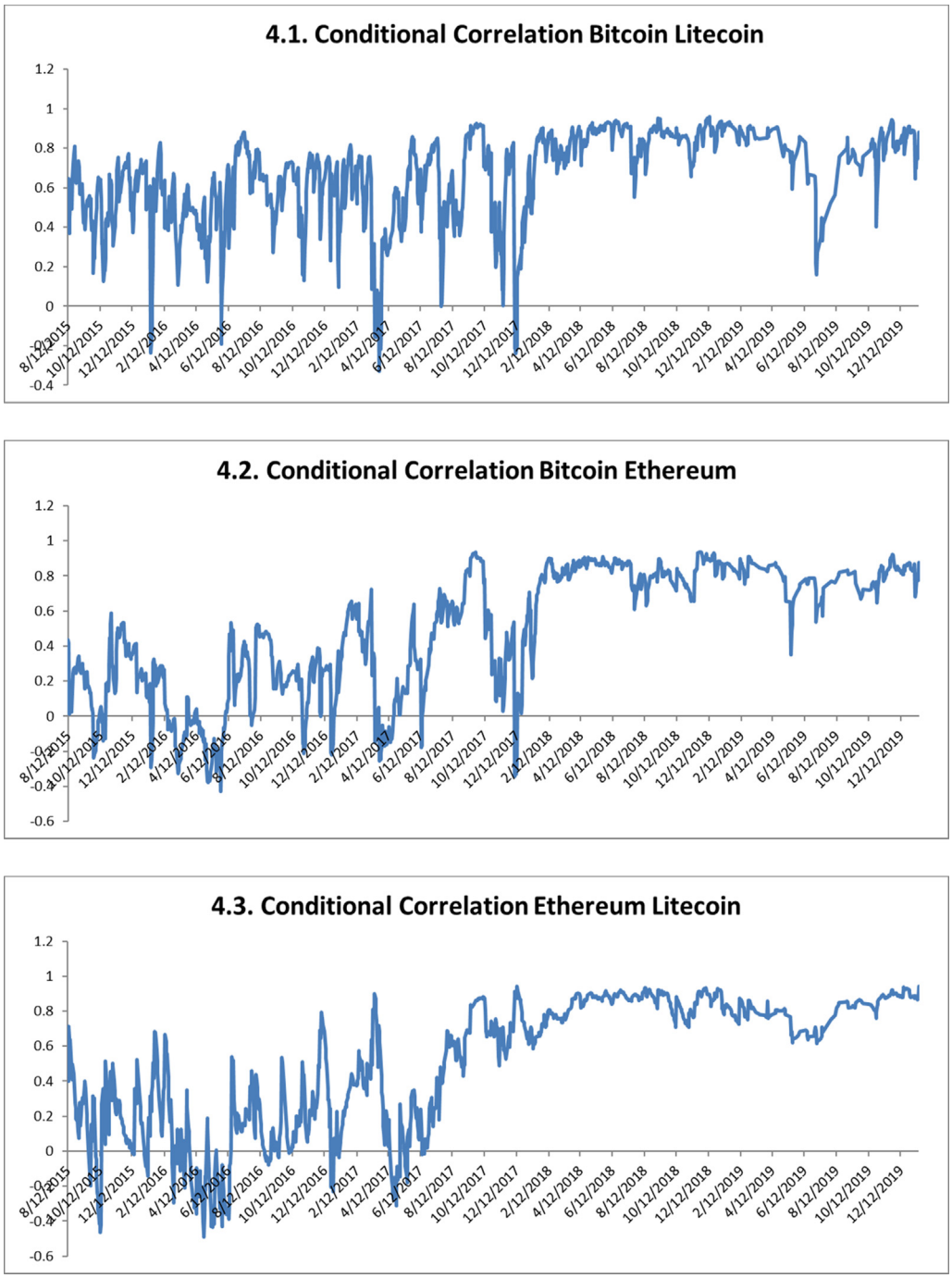


Fig. 4. Conditional Correlations.

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 (Fig. 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.

Appendix A. Cyber-attack target country and count

Cyber-attack target country	Cyber-attack count
United States of America	1775
More than one country	1173
United Kingdom	247
Unknown	120
India	100
Canada	96
Russian Federation	81
Italy	80
Australia	73
Republic of Korea	64
Japan	60
France	52
Germany	51
China	44
Ukraine	39
Brazil	37
Israel	33
Netherlands	31

(*continued on next page*)

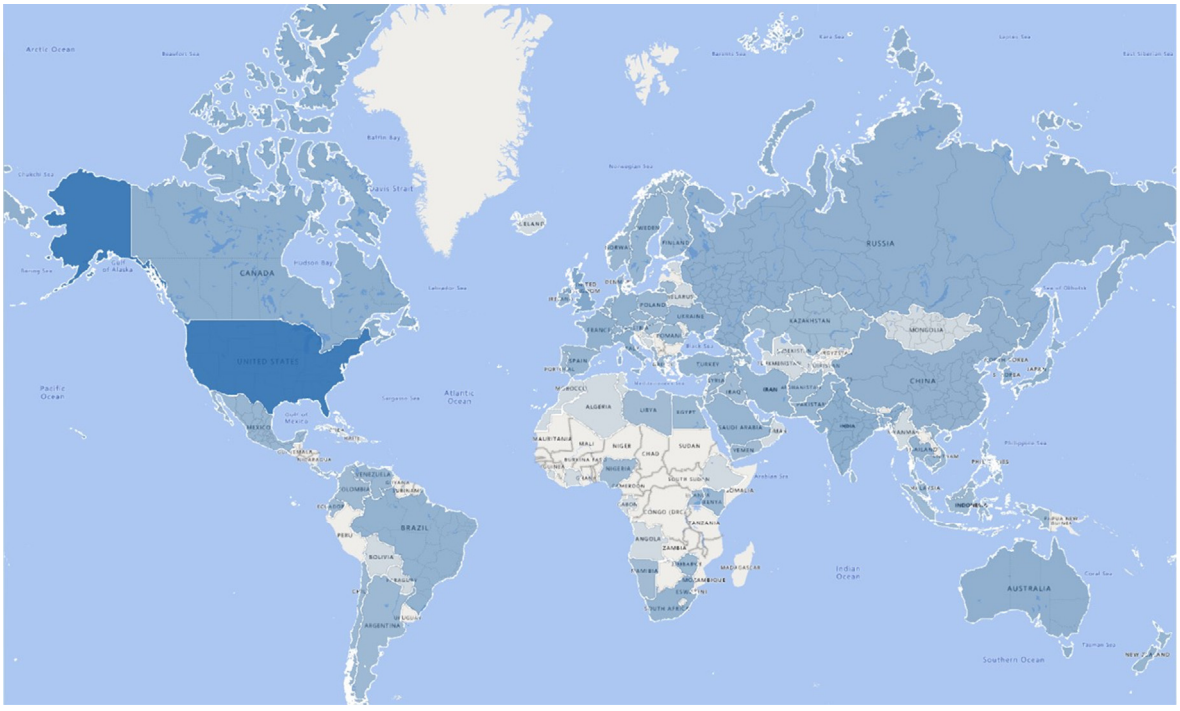
Appendix A (*continued*)

Cyber-attack target country	Cyber-attack count
Iran	25
Turkey	25
Hong Kong	24
South Africa	23
Thailand	23
Ireland	22
Pakistan	21
Singapore	19
Saudi Arabia	18
Spain	18
Sweden	18
New Zealand	17
Switzerland	16
United Arab Emirates	16
Mexico	14
Philippines (the)	14
Belgium	12
Taiwan	12
Austria	11
Czechia	11
Denmark	9
Norway	9
Poland	9
Azerbaijan	8
Kenya	8
Malaysia	8
Venezuela	8
Chile	7
Greece	7
Viet Nam	7
Armenia	6
Bangladesh	6
Europe	6
Panama	6
Argentina	5
Cambodia	5
Finland	5
Syrian Arab Republic	5
Afghanistan	4
Cyprus	4
Democratic People's Republic of Korea	4
Egypt	4
Malta	4
Qatar	4
Zimbabwe	4
Kazakhstan	3
Lebanon	3
Luxembourg	3
Montenegro	3
Nepal	3
Romania	3
Slovakia	3
Sri Lanka	3
Albania	2
Bahrain	2
Barbados	2

Appendix A (*continued*)

Cyber-attack target country	Cyber-attack count
Cayman Islands	2
Cocos (Keeling) Islands	2
Colombia	2
Costa Rica	2
Ecuador	2
Hungary	2
Indonesia	2
Iraq	2
Jordan	2
Kuwait	2
Libya	2
Lithuania	2
Nigeria	2
Palestine, State of	2
Puerto Rico	2
Uganda	2
Algeria	1
Angola	1
Bahamas	1
Belarus	1
Bolivia	1
Bosnia and Herzegovina	1
Croatia	1
Dominican Republic	1
Estonia	1
Ethiopia	1
Fiji	1
Gabon	1
Georgia	1
Guam	1
Guernsey	1
Iceland	1
Isle of Man	1
Maldives	1
Mongolia	1
Myanmar	1
Namibia	1
Oman	1
Paraguay	1
Portugal	1
Rwanda	1
Sierra Leone	1
Tajikistan	1
Tanzania	1
Trinidad and Tobago	1
Tunisia	1
Virgin Islands	1
Yemen	1

Appendix B. Visualization of cyber-attacks across the globe



References

Acemoglu, D., Johnson, S., 2005. Unbundling institutions. J. Polit. Econ. 113 (5), 949–995.

Adrian, T., Brunnermeier, M.K., 2016. CoVaR. Am. Econ. Rev. 106 (7), 1705–1741.

Alexander, C., Dakos, M., 2020. A critical investigation of cryptocurrency data and analysis. Quantit. Finan. 20 (2), 173–188.

Al Rahahleh, N., Bhatti, M.I., 2017. Co-movement measure of information transmission on international equity markets. Physica A 470, 119–131.

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

Antonakakis, N., Chatzianotniou, I., Gabauer, D., 2019. Cryptocurrency market contagion: market uncertainty, market complexity, and dynamic portfolios. J. Int. Finan. Markets, Inst. Money 61, 37–51.

Bacao, P., Duarte, A.P., Sebastiao, H., Redzepagic, S., 2018. Information transmission between cryptocurrencies: does Bitcoin rule the cryptocurrency world?. Sci. Ann. Econom. Busin. 65 (2), 97–117.

Balciar, M., Bouri, E., Gupta, R., Roubaud, D., 2017. "Can volume predict bitcoin returns and volatility?", A quantiles-based approach. Econ. Model. 64, 74–81.

Bariviera, A., 2017. The inefficiency of bitcoin revisited: A dynamic approach. Econ. Lett. 161, 1–4.

Bariviera, A., Basgall, M., Hasperue, W., Naiouf, M., 2017. Some stylized facts of the bitcoin market. Phys. A 484, 82–90.

Baur, D.G., Hong, K., Lee, A.D., 2018. Bitcoin: medium of exchange or speculative assets?. J. Int. Finan. Markets, Inst. Money 54, 177–189.

Bhatti, M.I., Do, H.Q., 2019. Recent development in copula and its applications to the energy, forestry and environmental sciences. Int. J. Hydrogen Energy 44 (36), 19453–19473.

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., Roubaud, D., 2019. Vine copula-based dependence and portfolio value-at-risk analysis of the cryptocurrency market. Int. Econ. 158, 77–90.

Bodford, J.E., Kwan, V.S.Y., 2018. A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs?. Cyberpsychol., Behav. Soc. Netw. 21 (2), 73–77.

Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: Economics, technology, and governance. J. Econ. Perspect. 29 (2), 213–238.

Bollerslev, T., Wooldridge, J.M., 1992. Quasi-maximum Likelihood Estimation and Inference in DynamicModels with Timevarying Covariances. Econometr. Rev. 11, 143–172.

Borri, N., 2019. Conditional tail-risk in cryptocurrency markets. J. Empiric. Finan. 50, 1–19.

Bouri, E., Gupta, R., Tiwari, A., Roubaud, D., 2017a. Does bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. Finan. Res. Lett. 23, 87–95.

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

Bouri, E., Molnár, P., Azzi, G., Roubaud, D., Hagfors, L.I., 2017c. On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier?. Finan. Res. Lett. 20, 192–198.

Caporale, G.M., Cipollini, A., Spagnolo, N., 2005. Testing for contagion: a conditional correlation analysis. J. Empiric. Finan. 12, 476–489.

Caporale, G.M., Pittis, N., Spagnolo, N., 2006. Volatility transmission and financial crises. J. Econom. Finan. 30 (3), 376–390.
Caporale, G.M., Plastun, A., 2019a. The day of the week effect in the crypto currency market. Finan. Res. Lett. 31, 258–269.
Caporale, G.M., Plastun, A., 2019b. BitCoin fluctuations and the frequency of price overreactions. Fin. Markets. Portfolio Mgmt. 33 (2), 109–131.
Caporale, G.M., Plastun, A., 2019c. Price overreactions in the cryptocurrency market. J. Econ. Stud. 46 (5), 1137–1155.
Caporale, G.M., Luis-Alana, L., Plastun, A., 2018. Persistence in the cryptocurrency market. Res. Int. Busin. Finan. 46, 141–148.
Caporale, G.M., Zekokh, T., 2019. Modelling volatility of cryptocurrencies using Markov-Switching GARCH models. Res. Int. Busin. Finan. 48, 143–155.
Caporale, G.M., Kang, W.-Y., Spagnolo, F., Spagnolo, N., 2019. Non-linearities, cyber attacks and cryptocurrencies. Finan. Res. Lett. 7692, 1–10.
Chen, M.A., Wu, Q., Yang, B., 2019. How Valuable Is FinTech Innovation?. Rev. Finan. Stud. 32 (5), 2062–2106.
Ciaian, P., Rajcaniova, M., d'Artis, K., 2018. Virtual relationships: short- and long-run evidence from Bitcoin and Altcoin markets. J. Int. Finan. Markets, Inst. Money 52, 173–195.
Conlon, T., McGee, R., 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., Yarovaya, L., 2018. Exploring the dynamic relationships between cryptocurrencies and other financial assets. Econ. Lett. 165, 28–124.
Corbet, S., Larkin, C., Lucey, B., 2020. "The contagion effects of the COVID-19 pandemic: evidence from gold and cryptocurrencies", mimeo. Dublin City University Business School.
Diebold, F.X., Yilmaz, K., 2012. Better to give than to receive: predictive directional measurement of volatility spillovers. Int. J. Forecast. 28 (1), 57–66.
Diebold, F.X., Yilmaz, K., 2016. Trans-Atlantic equity volatility connectedness: U.S. and European financial institutions, 2004–2014. J. Finan. Econometr. 14, 81–127.
Djankov, S., La Porta, R., Lopez-de-Silanes, F., Shleifer, A., 2008. The law and economics of self-dealing. J. Financ. Econ. 88 (3), 430–465.
Dwyer, G.P., 2015. The economics of Bitcoin and similar private digital currencies. J. Finan. Stab. 17, 81–91.
Dyhrberg, A., 2016a. Bitcoin, gold and the dollar - A GARCH volatility analysis. Finan. Res. Lett. 16, 85–92.
Dyhrberg, A., 2016b. Hedging capabilities of bitcoin. Is it the virtual gold?. Finan. Res. Lett. 16, 139–144.
Feng, W., Wang, Y., Zhang, Z., 2018. Can cryptocurrencies be a safe haven: a tail risk perspective analysis. Appl. Econ. 50 (44), 4745–4762.
Foley, S., Karlsen, J., Putniņš, T.J., 2018. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev. Finan. Stud., Forthcoming.
Forbes, K.J., Rigobon, R., 2002. No contagion, only interdependence: measuring stock market comovements. J. Finan. 57 (5), 2223–2261.
Fry, J., 2018. Booms, busts and heavy-tails: The story of Bitcoin and cryptocurrency markets. Econ. Lett. 171, 225–229.
Fry, J., Cheah, E.-T., 2016. Negative bubbles and shocks in cryptocurrency markets. Int. Rev. Finan. Anal. 47, 343–352.
Gil-Alana, L., Abakah, E., Rojo, M., 2020. Cryptocurrencies and stock market indices. are they related?. Res. Int. Busin. Finan. 51, 101063.
Harvey, C., 2016. "Cryptofinance", Available at SSRN: https://ssrn.com/abstract=2438299.
Gandal, N., Hamrick, J., Moore, T., Oberman, T., 2018. Price manipulation in the bitcoin ecosystem. J. Monetary Econ. 95, 86–96.
Goldstein, I., Jiang, W., Karolyi, G.A., 2019. To FinTech and Beyond. Rev. Finan. Stud. 32 (5), 1647–1661.
Griffin, J.M., Shams, A., 2018. Is bitcoin really un-tethered? Available at SSRN: https://ssrn.com/abstract=3195066.
Howell, S.T., Niessner, M., 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., Roubaud, D., 2019. Dynamic connectedness and integration in cryptocurrency markets. Int. Rev. Finan. Anal. 63, 257–272.
Katsiampa, P., 2019. An empirical investigation of volatility dynamics in the cryptocurrency market. Res. Int. Busin. Finan. 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. Econ. Lett. 173, 122–127.
KPMG. (2018), Global Fintech investment soars to record US$57B in first half of 2018. The Pulse of Fintech 2018, July 30.
Kroll, J., Davey, I., Felten, E., 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Proc. WEIS, 1–21.
La Porta, R., Lopez-de-Silanes, F., Shleifer, A., Vishny, R., 2002. Investor protection and corporate valuation. J. Finan. 57 (3), 1147–1170.
Lee, D.K.C., Guo, L., Wang, Y., 2018. Cryptocurrency: a new investment opportunity?. J. Alternat. Invest. 20 (3), 16–40.
Li, J., Mann W., 2018. Initial coin offering and platform building. Available at SSRN: https://ssrn.com/abstract=3088726.
Li, T., Shin, D., Wang, B., 2018. Cryptocurrency pump-and-dump schemes. Available at SSRN: https://ssrn.com/abstract=3267041.
Liu, W., 2019. Portfolio diversification across cryptocurrencies. Finan. Res. Lett. 29, 200–205.
Liu, Y., Tsyvinski, A., 2018. Risks and returns of cryptocurrency. Technical report, National Bureau of Economic Research, Working Paper No. 24877.
Ljung, G.M., Box, G.E.P., 1978. On a Measure of Lack of Fit in Time Series Models. Biometrika 65, 297–303.
Malinova, K., Park, A., 2017. Market design with blockchain technology. University College London, Working Paper.
Nadarajah, S., Chu, J., 2017. On the inefficiency of Bitcoin. Econ. Lett. 150, 6–9.
Nash, K.S., 2016. Big banks stake fintech claims with patent application surge. Wall Street J., May 10.
Nguyen, C., Bhatti, M.I., Henry, D., 2017. Are Vietnam and Chinese stock markets out of the US contagion effect in extreme events?. Physica A 480, 10–21.
Omane-Adjepong, M., Alagidede, I.P., 2019. Multiresolution analysis and spillovers of major cryptocurrency markets. Res. Int. Busin. Finan. 49, 191–206.
Passeri, P., 2020. June 2020 Cyber Attacks Statistics, accessed 16 August 2020, <https://www.hackmageddon.com/2020/08/13/june-2020-cyber-attacks-statistics>.
Raskin, M., Yermack, D., 2016. Digital currencies, decentralized ledgers, and the future of central banking. National Bureau of Economic Research, Working paper No. 22238.
Russo, C., 2017. Goldman and Google are among the most active blockchain investors. Bloomberg, October 17.
Schilling, L., Uhlig, H., 2018. Some simple bitcoin economics. Journal of Monetary Economics 106, 16–26.
Shanaev, S., Shuraeva, A., Vasenin, M., Kuznetsov, M., 2019. Cryptocurrency value and 51% attacks: evidence from event studies. J. Alternat. Invest. 22 (3), 65–77.
Tiwari, A., Raheem, I., Kang, S., 2019. Time-varying dynamic conditional correlation between stock and cryptocurrency markets using the copula-ADCC-EGARCH model. Physica A: Statist. Mech. Appl., 535.
Uma, M., Padmavathi, G., 2013. A Survey on Various Cyber Attacks and Their Classification. Int. J. Netw. Secur. 15 (5), 390–396.
Urquhart, A., 2016. The inefficiency of bitcoin. Econ. Lett. 148, 80–82.
Yermack, D., 2018. The potential of digital currency and blockchains. NBER Reporter 1 (14), 17.
Yi, S., Xu, Z., Wang, G.-J., 2018. Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?. Int. Rev. Finan. Anal. 60, 98–114.