Finance Research Letters 32 (2020) 101297

Contents lists available at ScienceDirect

Finance Research Letters

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

Non-linearities, cyber attacks and cryptocurrencies

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, UK
[b] Centre for Applied Macroeconomic Analysis (CAMA), National Australian University, Australia

ARTICLE INFO

Keywords:
Cryptocurrencies
Cyber attacks
Regime switching

JEL classification:
C22
E4
G1

ABSTRACT

This paper uses a Markov-switching non-linear specification to analyse the effects of cyber attacks on returns in the case of four cryptocurrencies (Bitcoin, Ethernam, Litecoin and Stellar) over the period 8/8/2015–2/28/2019. The analysis considers both cyber attacks in general and those targeting cryptocurrencies in particular, and also uses cumulative measures capturing persistence. On the whole, the results suggest the existence of significant negative effects of cyber attacks on the probability for cryptocurrencies to stay in the low volatility regime. This is an interesting finding, that confirms the importance of gaining a deeper understanding of this form of crime and of the tools used by cybercriminals in order to prevent possibly severe disruptions to markets.

1. Introduction

A cyber attack is an attack launched from one or more computers against other computers or networks (either to disable them or to gain access to data and manage them); it compromises information security by affecting its confidentiality, integrity and availability. It is a form of cyber risk, which has now emerged as a type of systemic risk and has had an impact on the financial sector in particular (see Kopp et al., 2017). Bouveret (2018) proposes an empirical model based on the standard Value-at-Risk (VaR) framework for a quantitative assessment of cyber risk and losses and reports evidence for a number of countries.

Benjamin et al. (2019) point out that in the current environment characterised by heavy reliance on information technology increasingly frequent and sophisticated cyber attacks from criminals operating in underground web communities such as Darknet are a very serious issue, and have resulted in estimated annual losses of $445 billion for the global markets (see Graham, 2017). In recent years cryptocurrencies (Bitcoin in particular) have become a favourite target owing to their anonymity. Cyber attacks are in fact mentioned as one of the operational risk factors by both small and large “miners”, whose responsibility in a cryptocurrency system is to group unconfirmed transactions into new blocks and add them to the global ledger known as the “blockchain” (see Hileman and Rauchs, 2017). Benjamin et al. (2019) propose a framework for gaining a better understanding of this form of crime that causes significant disruptions to markets. Analysing the tools employed by cybercriminals has therefore become very important for prevention purposes (see Van Hardeveld et al., 2017).

Cryptocurrencies have distinctive features such that traditional methods to estimate and manage risk might not be appropriate and different portfolio techniques might be required (see Platanakis and Urquhart, 2019; for a thorough review of the empirical literature on cryptocurrencies see Corbet et al., 2019). In particular, they are known to be highly volatile and to exhibit breaks. For instance, Thies and Molnar (2018) identify several structural breaks in the Bitcoin series using a Bayesian change point (BCP) model, whilst Chaim and Laurini (2018) specify two models for Bitcoin incorporating discontinuous jumps to volatility and returns, the

* Corresponding author.
E-mail address: guglielmo-maria.caporale@brunel.ac.uk (G.M. Caporale).

https://doi.org/10.1016/j.frl.2019.09.012
Received 16 July 2019; Received in revised form 10 September 2019; Accepted 21 September 2019
Available online 17 October 2019
1544-6123/

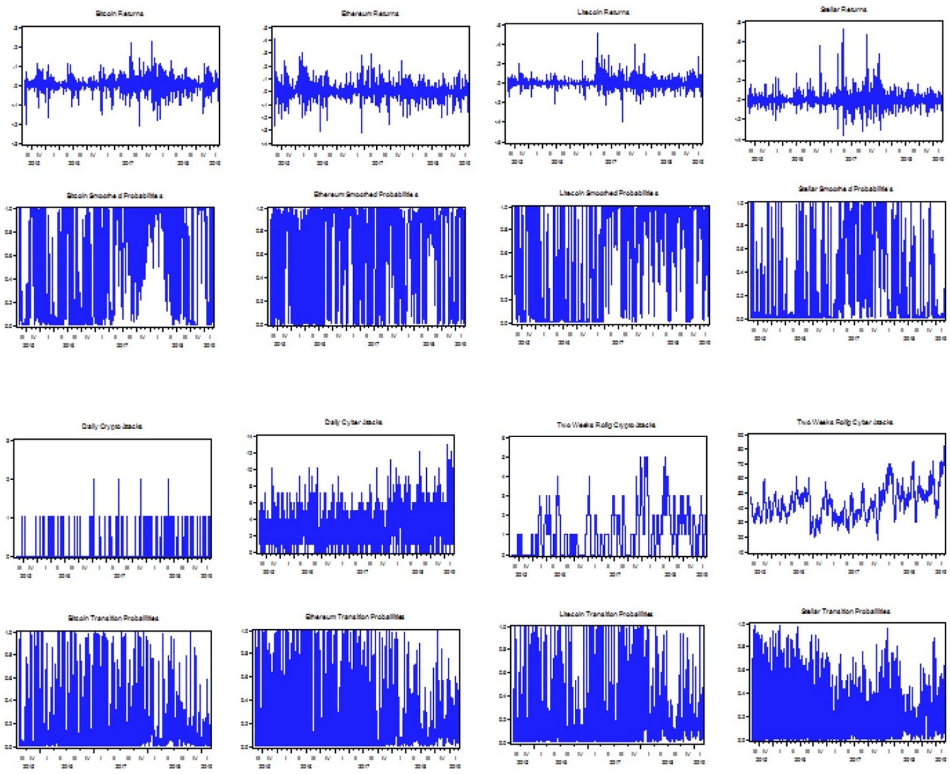

Fig. 1. Cryptocurrency returns and smoothed probabilities Note: The smoothed probability is the probability of being in the high volatility regime.

former being found to have permanent effects, the latter contemporaneous only. Interestingly, Gandal et al. (2018) show that suspicious trading activity is the likely cause of such jumps, specifically in late 2013. In the presence of breaks standard GARCH models can produce biased results (Bauwens et al., 2010; 2014)). In such cases (Ardia et al., 2018a) suggest estimating Markov-Switching GARCH (MS-GARCH) models, whose parameters can change over time according to a discrete latent variable. Caporale and Zekokh (2019) show that indeed standard GARCH models yield relatively inaccurate Value-at-Risk (VaR) and Expected-Shortfall (ES) predictions in the case of the four most popular cryptocurrencies (i.e. Bitcoin, Ethereum, Ripple and Litecoin), and that these can be improved by allowing for asymmetries and regime switching (see also Ardia et al., 2018b, for some evidence on Bitcoin only).

The present paper also adopts a Markov-Switching framework but aims to investigate the additional issue of whether or not cyber attacks affect the time-varying transition probabilities of switching from one regime to another. The remainder of the paper is organised as follows: Section 2 discusses the methodology. Section 3 presents the empirical results. Section 4 concludes.

2. Methodology

The time-varying regime-switching model considered in this paper allows for shifts in the mean and the variance, that is for periods of low and high returns and volatility, and is given by:

$$\Lambda y_t = \mu(s_t) + \sum_{i=1}^{4} \phi_i \Lambda y_{t-i} + \sigma(s_t)\varepsilon_t, \qquad \sigma(s_t) = \sum_{i=1}^{2} \sigma_{(i)} \mathbf{1}\{s_t = i\}, \quad (t \in \mathbb{T}), \tag{1}$$

where Λy_t= percentage change in cryptocurrency prices. Autoregressive terms (up to four lags) are also considered. Therefore, the parameters vector of the mean equation, Eq. (1) is defined by $\mu_{(i)}$ $(i = low, high)$ and $\sigma_{(i)}$ $(i = low, high)$ which are real constants, the autoregressive terms $\sum_{i=1}^{4} \phi_i$, $\{\varepsilon_t\}$ which are i.i.d. errors with $\mathsf{E}(\varepsilon_t) = 0$ and $\mathsf{E}(\varepsilon_t^2) = 1$, and the random variables $\{s_t\}$ in $\mathbb{S} = \{low, high\}$ which indicate the unobserved state of the process at time *t*. Throughout, the regime indicators $\{s_t\}$ are assumed to form a Markov chain on $\mathbb{S}$ with transition probability matrix $\mathbf{P}' = [p_{low,high}]_{2\times 2}$, where $p_{low,high} = \Pr(s_t = high | s_{t-1} = low)$ with $low, high \in \mathbb{S}$. $p_{i,low} = 1 - p_{i,high}$ $(i \in \mathbb{S})$. Each column sums to unity and all elements are non-negative. It is also assumed that $\{\varepsilon_t\}$ and $\{s_t\}$ are independent.

To assess the links between cyber attacks and the cryptocurrencies, we generalise the model in Eq. (1) by allowing the transition probabilities to vary over time. Following Filardo (1994), the transition mechanism governing $\{s_t\}$ is given by:

Table 1
Descriptive statistics and Hansen test.

Panel A	Descriptive statistics[a]							
	Cryptocurrency returns				Cryptocurrency volumes			
	Bitcoin	Ethe.	Lite.	Stellar	Bitcoin	Ethe.	Lite.	Stellar
Mean	0.201	0.299	0.184	0.273	2,680	996	265	44
S. D.	0.039	0.076	0.057	0.082	3,641	1,331	446	94
Skew	− 0.261	− 3.383	1.261	2.055	1.991	1.88	5.026	6.073
Kurt	7.791	68.275	15.204	18.874	8.234	8.172	51.799	64.661
Min	− 0.207	− 1.302	− 0.395	− 0.366	13	0,111	0, 507	0
Max	0.225	0.412	0.511	0.723	23,800	9,210	6,961	1,511
Obs.	1301	1301	1301	1301	1301	1301	1301	1301
	Attacks count by target							
	Crypto attacks		Cyber attacks					
	1 Day	2 weeks	1 Day	2 weeks				
Mean	0.079	1.112	3.085	43.011				
S. D.	0.282	1.132	2.257	10.736				
Skew	3.513	0.914	0.823	0.591				
Kurt	14.991	3.381	3.629	3.326				
Min	0	0	0	18				
Max	2	5	13	82				
Obs.	104		4014					
Panel B	Markov switching state dimension: Hansen test[b]							
	Bitcoin	Ethe.	Lite.	Stellar	Bitcoin	Ethe.	Lite.	Stellar
	Linearity vs two-states				Two-states vs three-states			
LR	4.367	4.512	5.013	4.757	0.232	0.351	0.296	0.302
M = 0	0.001	0.001	0.001	0.001	0.546	0.672	0.643	0.622
M = 1	0.002	0.005	0.004	0.002	0.701	0.748	0.718	0.734
M = 2	0.004	0.007	0.008	0.005	0.788	0.792	0.748	0.768
M = 3	0.010	0.011	0.013	0.009	0.821	0.834	0.809	0.813

[a] Note: Cryptocurrency returns are the percentage change in cryptocurrencies prices. Cryptocurrency volumes are reported in millions of US Dollars. In the empirical analysis the percentage change in volumes is used. Crypto and cyber attacks refer to the number of attacks targeting cryptocurrencies only and other cyber attacks, respectively. Descriptive statistics are reported for the total number of attacks per day (1 day) and the cumulative number of attacks (intensity measure) using a two-weeks rolling window.

[b] The Hansen's standardized Likelihood Ratio test p-values are calculated according to the method described in Hansen (1992), using 1,000 random draws from the relevant limiting Gaussian processes and bandwidth parameter M = 0,1,...,3. Test results for the presence of a third state are also reported.

$$\begin{aligned} p_t^{low} &= \frac{\exp(\gamma_0 + \gamma_1 w_{t-1} + \gamma_2 \Lambda z_{t-1} + \gamma_3 x_{t-1})}{[1 + \exp(\gamma_0 + \gamma_1 w_{t-1} + \gamma_2 \Lambda z_{t-1} + \gamma_3 x_{t-1})]}, \\ p_t^{high} &= \frac{\exp(\eta_0 + \eta_1 w_{t-1} + \eta_2 \Lambda z_{t-1} + \eta_3 x_{t-1})}{[1 + \exp(\eta_0 + \eta_1 w_{t-1} + \eta_2 \Lambda z_{t-1} + \eta_3 x_{t-1})]}. \end{aligned} \tag{2}$$

where w_t= cyber attacks count. For robustness purposes, the following control variables are also included: z_t= VIX for global financial markets uncertainty and Λx_t= change in cryptocurrency volumes.

Note that since p_t^{low}/w_{t-1} has the same sign as γ_1, $\gamma_1 > 0$ implies that an increase in cyber attacks, w_{t-1}, increases the probability of remaining in the low regime. Similarly, $\eta_1 > 0$ implies that an increase in w_{t-1} increases the probability of remaining in the high regime.[1] The same holds for the control variables Λx_{t-1} and z_{t-1}. The density of the data has two components, one for each regime, and the log-likelihood function is constructed as a probability-weighted sum of these two components.

3. Empirical analysis

3.1. Data

Daily data for four cryptocurrencies (Bitcoin, Ethernam, Litecoin and Stellar) and their corresponding volumes over the period 8/8/2015–2/28/2019 (for a total of 1301 observations) are employed for the analysis. The sample size was chosen on the basis of data availability. These series are from coinmarketcap.com.

[1] Note that failure to reject the null hypothesis of H_0: $\gamma_1 = \eta_1 = 0$ suggests a fixed transition probabilities model.

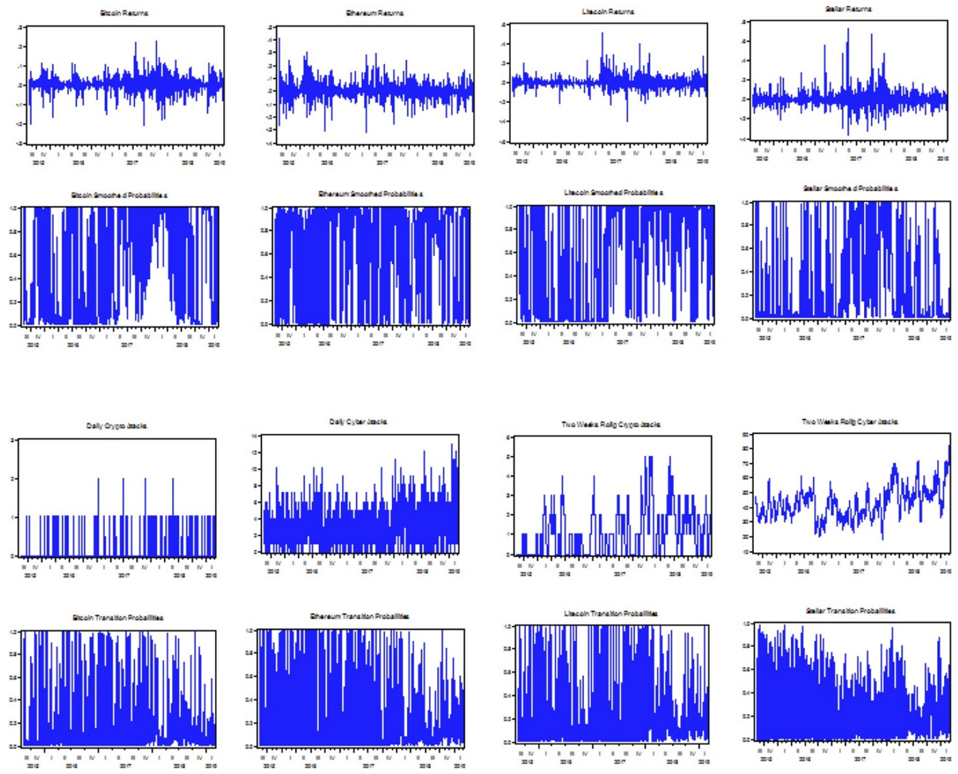

Fig. 2. Cryptocurrency returns, smoothed probabilities, crypto and cyber attacks, and time-varying transition probabilities. Note: Crypto and cyber attacks refer to the number of attacks targeting cryptocurrencies only and other cyber attacks, respectively. The time-varying transition probabilities refer to the probability of switching from a low to a high volatility regime according to parameter estimates (Table 2) for one day crypto attacks.

The data source for cyber attacks is https://www.hackmageddon.com. These include Crime, Espionage, Warfare and Hacktivism cyber attacks. We consider cyber attacks specifically targeting cryptocurrencies (henceforth crypto attacks), as well as other cyber attacks (henceforth cyber attacks). The rational for including the latter is that their extensive media coverage could also affect the perception investors have of cryptocurrencies, since this type of asset relies heavily on cyber security.

Further, we construct an intensity measure based on the cumulative number of crypto attacks, as well as cyber attacks, using a two-week rolling window, which is expected to capture persistence. The two measures for both crypto and cyber attacks are shown in Fig. 1. Visual inspection suggests the presence of an upward trend in the number of crypto as well as cyber attacks over the last two years; this is particularly apparent in the case of the two-week rolling window measures. Finally, VIX data have been obtained from the Federal Reserve of St. Louis.

The descriptive statistics (Panel A, Table 1) indicate that returns are positive for all cryptocurrencies. Higher returns are associated with higher standard deviations, as in the cases of Ethernam and Stellar, their returns being equal to 0.299 and 0.273, respectively. All series exhibit skewness and kurtosis. The average number of cyber attacks exceeds three per day (3.085), whereas the corresponding figure for crypto attacks is much lower (0.079). Over the sample as a whole, the total number of cyber and crypto attacks was equal to 4014 and 104, respectively.

As for volumes, Bitcoin and Ethereum are the largest currencies by market capitalization, with values equal to $8889 and $4535 millions respectively on the last day of our sample (February 28 2019); the corresponding figures for the two smaller cryptocurrencies on the same day were $1119 and $112 millions. Volumes have been highly volatile, especially in the case of the smaller crypto-markets.[2]

3.2. Empirical results

Maximum likelihood (ML) estimates of the model described above are reported in Tables 2 and 3. The null hypothesis of linearity against the alternative of Markov regime switching cannot be tested directly using the standard likelihood ratio (LR) test. We test for the presence of more than one regime against linearity using the Hansen's standardized likelihood ratio test (1992). The value of the standardized likelihood ratio statistics and related p - values (Panel B, Table 1), under the null hypothesis (see Hansen, 1992 for details), provide strong evidence in favour of a two - state Markov regime-switching specification. The presence of a third state has

[2] Please note that in the empirical analysis we use the percentage change in volumes.

Table 2
Markov switching estimation results – crypto attacks.

	One day crypto attacks				Two weeks crypto attacks			
	Bitcoin	Ethe.	Lite.	Stellar	Bitcoin	Ethe.	Lite.	Stellar
	Mean Equation							
μ^l	0.001 (0.421)	−0.002 (0.069)	−0.001 (0.000)	−0.006 (0.000)	0.001 (0.312)	−0.002 (0.089)	−0.001 (0.000)	−0.006 (0.000)
σ^l	0.012 (0.000)	0.031 (0.000)	0.013 (0.000)	0.038 (0.000)	0.012 (0.000)	0.032 (0.000)	0.013 (0.000)	0.038 (0.000)
μ^h	0.002 (0.000)	0.015 (0.031)	0.004 (0.000)	0.026 (0.001)	0.002 (0.000)	0.015 (0.022)	0.004 (0.000)	0.028 (0.001)
σ^h	0.056 (0.000)	0.127 (0.000)	0.078 (0.000)	0.151 (0.000)	0.056 (0.000)	0.133 (0.000)	0.079 (0.000)	0.151 (0.000)
ϕ_1	−0.065 (0.000)	−0.131 (0.000)	−0.138 (0.000)	−0.116 (0.000)	−0.069 (0.000)	−0.123 (0.000)	−0.145 (0.000)	−0.112 (0.000)
				Transition probabilities				
				Low regime				
γ_0	2.326 (0.044)	4.696 (0.000)	5.078 (0.016)	1.321 (0.023)	3.187 (0.016)	6.071 (0.000)	4.969 (0.000)	2.244 (0.007)
γ_1	−1.735 (0.001)	−1.403 (0.002)	−1.951 (0.002)	−1.119 (0.007)	−0.871 (0.000)	−0.851 (0.000)	−0.736 (0.000)	−0.554 (0.012)
γ_2	0.088 (0.199)	−0.073 (0.225)	−0.094 (0.077)	−0.154 (0.174)	0.081 (0.311)	−0.102 (0.051)	−0.071 (0.161)	−0.121 (0.169)
γ_3	−6.845 (0.000)	−5.145 (0.000)	−5.392 (0.000)	−1.072 (0.000)	−7.329 (0.000)	−5.104 (0.000)	−5.471 (0.000)	−1.053 (0.000)
				High regime				
η_0	−2.022 (0.005)	−0.361 (0.694)	−3.285 (0.000)	−3.868 (0.001)	−2.247 (0.002)	−1.215 (0.003)	−3.063 (0.002)	−4.125 (0.001)
η_1	0.705 (0.505)	0.247 (0.211)	0.024 (0.701)	0.387 (0.183)	0.182 (0.211)	0.498 (0.019)	0.074 (0.443)	0.295 (0.159)
η_2	−0.018 (0.613)	−0.044 (0.353)	0.061 (0.042)	0.113 (0.061)	−0.012 (0.725)	−0.025 (0.464)	0.047 (0.111)	0.119 (0.036)
η_3	6.525 (0.000)	4.363 (0.000)	4.798 (0.000)	4.361 (0.000)	6.158 (0.000)	5.106 (0.000)	4.764 (0.000)	4.396 (0.000)
				Diagnostic tests				
LB	0.272	0.451	0.440	2.564	0.272	0.451	0.440	2.564
LB^2	2.665	3.551	4.071	4.887	2.665	3.551	4.071	4.887
LogL	2747.7	1922.5	2357.3	1812.5	2754.8	1929	2359.4	1816.1

Note: Autocorrelation and heteroscedasticity-consistent *p*-values are reported in brackets. LB and LB ^{2}are the Ljung-Box test (1978) of significance of autocorrelations of ten lags in the standardized and standardized squared residuals respectively.

also been tested and rejected. The optimal lag length according to Schwarz information criterion is one. In order to assess the possible role of cyber attacks in determining cryptocurrency returns, we analyse the sign (and significance) of the parameters of the time-varying transition probabilities (which sheds light on whether or not the cyber attack variable affects the probability of staying in the same, or switching to a different regime), and also consider their evolution over time to establish whether changes in regime are triggered by cyber attacks.

In the case of the one-day crypto attacks, the estimated coefficients for the transition probability (Table 2) imply that an increase (decrease) in the number of crypto attacks decreases (increases) the probability of remaining in the lower volatility regime. The effect is particularly pronounced for Bitcoin, Ethereum and Litecoin with γ_1 being equal to − 1.735, − 1.403 and − 1.951, respectively. On the other hand, crypto attacks do not appear to affect cryptocurrency returns during highly volatile periods, with η_1 being positive but insignificant. Maximum likelihood (ML) estimates for one-day cyber attacks (not reported for reasons of space) lead to similar conclusions concerning the signs and significance of the coefficients.

As for the two-weeks rolling crypto attacks measure, a similar pattern emerges, with crypto attacks negatively affecting the probability of staying in the low regime for all four currencies, although the magnitude of the parameter is smaller in absolute value. These findings suggest the presence of memory, measured by the crypto attacks intensity, which also drives the dynamics of the transition probability.

Regarding the results based on the two-week rolling window for cyber attacks (see Table 3), again a similar pattern emerges with γ_1 being equal to − 0.119, −0.092 and − 0.149 and − 0.124 for Bitcoin, Etheuram, Litecoin and Stellar respectively. These results suggest that cyber attacks affect cryptocurrencies but less than crypto attacks. However, a positive and statistically significant effect of cyber attacks on cryptocurrencies is found during highly volatile periods**,** with η_1 being equal to 0.021,0.074,0.042 and 0.143 for Bitcoin, Etheuram, Litecoin and Stellar, respectively.

The evolution of the time-varying transition probabilities and the crypto/cyber attack variables is very informative. The former vary throughout the sample. Changes in the probability of remaining in the less volatile regime appear to be triggered by the crypto/cyber attacks pattern for all four cryptocurrencies (see Fig. 2). The sharp increase in the number of cyber attacks over the last two

Table 3
Markov switching estimation results – cyber attacks.

	One day cyber attacks				Two weeks cyber attacks			
	Bitcoin	Ethe.	Lite.	Stellar	Bitcoin	Ethe.	Lite.	Stellar
	Mean equation							
μ^l	0.001 (0.421)	−0.002 (0.069)	−0.001 (0.000)	−0.006 (0.000)	0.001 (0.387)	−0.002 (0.078)	−0.001 (0.000)	−0.006 (0.000)
σ^l	0.012 (0.000)	0.031 (0.000)	0.013 (0.000)	0.038 (0.000)	0.013 (0.000)	0.031 (0.000)	0.013 (0.000)	0.038 (0.000)
μ^h	0.002 (0.000)	0.015 (0.031)	0.004 (0.000)	0.026 (0.001)	0.002 (0.000)	0.014 (0.036)	0.004 (0.000)	0.028 (0.001)
σ^h	0.056 (0.000)	0.127 (0.000)	0.078 (0.000)	0.151 (0.000)	0.057 (0.000)	0.127 (0.000)	0.079 (0.000)	0.150 (0.000)
ϕ_1	−0.065 (0.000)	−0.131 (0.000)	−0.138 (0.000)	−0.116 (0.000)	−0.069 (0.000)	−0.124 (0.000)	−0.147 (0.000)	−0.112 (0.000)
					Transition probabilities			
					Low regime			
γ_0	2.326 (0.044)	4.696 (0.000)	5.078 (0.016)	1.321 (0.023)	3.974 (0.012)	4.955 (0.000)	6.531 (0.000)	4.055 (0.000)
γ_1	−1.735 (0.001)	−1.403 (0.002)	−1.951 (0.002)	−1.119 (0.007)	−0.119 (0.008)	−0.092 (0.003)	−0.149 (0.003)	−0.124 (0.038)
γ_2	0.088 (0.199)	−0.073 (0.225)	−0.094 (0.077)	−0.154 (0.174)	0.131 (0.061)	−0.017 (0.699)	−0.028 (0.818)	−0.137 (0.038)
γ_3	−6.845 (0.000)	−5.145 (0.000)	−5.392 (0.000)	−1.072 (0.000)	−6.824 (0.000)	−5.439 (0.000)	−4.851 (0.000)	−1.271 (0.000)
					High regime			
η_0	−2.022 (0.005)	−0.361 (0.694)	−3.285 (0.000)	−3.868 (0.001)	−2.401 (0.023)	−1.264 (0.148)	−3.639 (0.000)	−6.683 (0.002)
η_1	0.705 (0.505)	0.247 (0.211)	0.024 (0.701)	0.387 (0.183)	0.021 (0.039)	0.074 (0.028)	0.042 (0.044)	0.143 (0.003)
η_2	−0.018 (0.613)	−0.044 (0.353)	0.061 (0.042)	0.113 (0.061)	−0.025 (0.454)	−0.086 (0.016)	0.033 (0.514)	0.104 (0.046)
η_3	6.525 (0.000)	4.363 (0.000)	4.798 (0.000)	4.361 (0.000)	6.669 (0.000)	4.583 (0.000)	4.701 (0.000)	5.021 (0.000)
					Diagnostic tests			
LB	0.272	0.451	0.440	2.564	0.272	0.451	0.440	2.564
LB^2	2.665	3.551	4.071	4.887	2.665	3.551	4.071	4.887
LogL	2747.7	1922.5	2357.3	1812.5	2750.4	1924.4	2360.1	1817.7

Note: See notes Table 3

years has decreased the probability of remaining in the low volatile regime (p_t^{low}).

Finally, concerning the two control variables, as one would expect, an increase (decrease) in volume changes decreases (increases) the probability of staying in the low regime $\gamma_3 < 0$, whereas it increases (decreases) the probability of remaining in the high regime, $\eta_3 > 0$. The coefficients on the VIX instead are not significant and suggest that crypto currencies are not responsive to global financial markets uncertainty.

Overall, all models appear to be well identified for all four cyber attack measures used. The results indicate the presence of statistically significant low (μ^l) and high (μ^h) returns for all four cryptocurrencies. The low state returns are negative ($\mu^l < 0$) except for Bitcoin. Volatility appears to drive the Markov process, with volatilities in the high regimes (σ^{high}) being at least four times as big as those in the low regimes (σ^{low}). The periods of high and low volatility seem to be accurately identified by the smoothed probabilities, which satisfactorily separate the two regimes for all four cryptocurrencies (Fig. 1). Visual inspection suggests that high-volatility episodes mostly occurred in 2017, whilst the following year exhibited lower volatility. Diagnostic tests on the standardized residuals (Ljung-Box statistics for dependency in the first moment and for heteroskedasticity) do not provide any evidence of linear or non-linear dependence.

4. Conclusions

This paper uses a Markov-switching non-linear specification to analyse the effects of cyber attacks on returns in the case of four cryptocurrencies (Bitcoin, Ethernam, Litecoin and Stellar) over the period 8/8/2015–2/28/2019. More specifically, it examines whether and how they affect the probability of switching between regimes. Previous studies had shown the presence of breaks (see, e.g., Thies and Molnar, 2018 and Chiem and Laurini, 2018) and the importance of allowing for regime switches when analysing the behaviour of cryptocurrencies (see Caporale and Zekokh, 2019); it had also been suggested that suspicious trading activity might be behind jumps in the series (see Gandal et al., 2018); the present study shed lights on the possible determinants of such switches by focusing specifically on the role of cyber attacks given the key importance of cyber security for assets such as cryptocurrencies. The analysis considers both cyber attacks in general and those targeting cryptocurrencies in particular, and also uses cumulative measures capturing persistence. On the whole, the results suggest the existence of significant negative effects of cyber attacks on the probability of cryptocurrencies staying in the low volatility regime. This is an interesting finding, which confirms the importance of gaining a deeper understanding of this form of crime (Benjamin et al., 2019) and of the tools used by cybercriminals (Van Hardeveld et al., 2017) in order to prevent possibly severe disruptions to markets. Further research could explore intra-day data, a wider set of cryptocurrencies as well as cyber attack indicators grouped by targets.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.frl.2019.09.012

References

Ardia, D., Bluteau, K., Boudt, K., Catania, L., 2018a. Forecasting risk with Markov- switching GARCH models: a large-scale performance study. Int. J. Forecast. 34, 733–747.

Ardia, D., Bluteau, K., Rüede, M., 2018b. Regime changes in bitcoin GARCH volatility dynamics. Financ. Res. Lett. https://doi.org/10.1016/j.frl.2018.08.009.

Bauwens, L., Backer, B.D., Dufays, A., 2014. A Bayesian method of change-point estimation with recurrent regimes: application to GARCH models. J. Empir. Financ. 29, 207–229.

Bauwens, L., Preminger, A., Rombouts, J.V.K., 2010. Theory and inference for a Markov switching GARCH model. Econ. J. 13, 218–244.

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

Bouveret, A., 2018. Cyber Risk for the Financial Sector: a Framework for Quantitative Assessment. IMF Working Paper no. 18/143.

Caporale, G.M., Zekokh, T., 2019. Modelling volatility of cryptocurrencies using markov-switching GARCH models. Res. Int. Bus. Financ. 48, 143–155.

Chaim, P., Laurini, M.P., 2018. Volatility and return jumps in bitcoin. Econ. Lett. 173, 158–163.

Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L., 2019. Cryptocurrencies as a financial asset: a systematic analysis. Int. Rev. Financ. Anal. 62 (C), 182–199.

Filardo, A.J., 1994. Business-cycle phases and their transitional dynamics. J. Econ. Bus. Stat. 12 (3), 299–308.

Gandal, N., Hamrick, J.T., Moore, T., Oberman, T., 2018. Price manipulation in the bitcoin ecosystem. J. Monet. Econ. 95, 86–96.

Graham, L., 2017. Cybercrime costs the global economy $450 billion: CEO, CNBC, feb- ruary 7. http://www.cnbc.com/2017/02/07/cybercrime-costs-the-globaleconomy-450-billion-ceo.html.

Hansen, B.E., 1992. The likelihood ratio test under nonstandard conditions: testing the Markov switching model of GNP. J. Appl. Econ. 7, 61–82.

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

Kopp, E., Kaffenberger, L., Wilson, C., 2017. Cyber Risk, Market Failures, and Financial Stability. IMF Working Paper no. 17/185.

Platanakis, P., Urquhart, A., 2019. Portfolio management with cryptocurrencies: the role of estimation risk. Econ. Lett. 177, 76–80.

Thies, S., Molnar, P., 2018. Bayesian change point analysis of bitcoin returns. Financ. Res. Lett. 27, 223–227.

Van Hardeveld, G.J., Webber, C., O'Hara, K., 2017. Deviating from the cybercrimi- nal script: exploring tools of anonymity (mis)used by carders on cryptomarkets. Am. Behav. Sci. 61 (11), 1244–1266.