Non-Linearities, Cyber Attacks and Cryptocurrencies

Guglielmo Maria Caporale [dW]

cryptocurrency volumes.

Note that since $s_w^{o\ r\ z}$@ z_{v31} has the same sign as $_1$, $_1$ A 0 implies that an increase in cyber attacks, z_{v31} >increases the probability of remaining in the low regime. Similarly, $_1$ A 0 implies that an increase in z_{v31} increases the probability of remaining in the high regime.[1] The same holds for the control variables $\{_{v31}$ and $\}_{v31}$ =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 on the closing prices and the corresponding volumes for four cryptocurrencies (Bitcoin, Ethernam, Litecoin and Stellar) over the period 8/8/2015 - 28/2/2019 (for a total of 1301 observations) are employed for the analysis. The sample size was chosen on the basis of data availability. The series are taken from coinmarketcap.com. Cryptocurrencies are not o!cially denominated in any specific national currency; in our study they are expressed in terms of USD.

The data source for cyber attacks is https://www.hackmageddon.com, which is regularly updated with media and personal reports submitted from all over the world with daily timeliness. These include Crime, Espionage, Warfare and Hacktivism (or hacking) cyber attacks. We consider cyber attacks specifically targeting cryptocurrencies (henceforth crypto attacks), 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 $8 >889 and $4 >535 millions respectively on the last day of our sample (28 February 2019); the corresponding figures for the two smaller cryptocurrencies on the same day were $1 >119 and $112 millions. Volumes have been highly volatile, especially in the case of the smaller cryptomarkets.[2]

3.2 Empirical Results

Maximum likelihood (ML) estimates of the model described above are reported in Tables 2-3. 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

1 403 and 1 951

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 8/8/2015–28/2/2019. 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 Zekhok, 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.

References

[1] Ardia, D., Bluteau, K., Boudt, K., Catania, L. (2018a). "Forecasting risk with Markov-switching GARCH models: A large-scale performance study", International Journal of Fore- casting, 34, 733-747.

[2] Ardia, D., Bluteau, K., Rüede, M. (2018b). "Regime changes in Bitcoin GARCH volatility dynamics", Finance Research Letters. https://doi.org/10.1016/j.frl.2018.08.009

[3] Bauwens, L., Backer, B.D., Dufays, A. (2014). "A Bayesian method of change-point estimation with recurrent regimes: Application to GARCH models", Journal of Empirical Finance, 29, 207-229.

[4] Bauwens, L., Preminger, A., Rombouts, J.V.K. (2010). "Theory and inference for a Markov switching GARCH model", Econometrics Journal, 13, 218-244.

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

[6] Bouveret, A. (2018). “Cyber risk for the financial sector: a framework for quantitative assess- ment”, IMF Working Paper no. 18/143.

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

[8] Chaim, P. and M.P. Laurini (2018), “Volatility and return jumps in Bitcoin”, Economics Letters, 173, 158-163.

[9] Corbet, S., Lucey, B., Urquhart, A. and L. Yarovaya (2019). "Cryptocurrencies as a financial asset: A systematic analysis", International Review of Financial Analysis, 62(C), 182-199.

[10] Filardo AJ (1994). "Business-cycle phases and their transitional dynamics", Journal of Economics and Business Statistics 12, 3, 299-308.

[11] Gandal, N., Hamrick, J.T., Moore, T. and T. Oberman (2018) “Price manipulation in the Bitcoin ecosystem”, Journal of Monetary Economics, 95, 86-96.

[12] 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-global economy-450-billion- ceo.html).

[13] Hamilton, J.D. (1990). "Analysis of Time Series Subject to Changes in Regime", Journal of Econometrics, 45, 39-70.

[14] Hansen, B.E. (1992). "The Likelihood Ratio Test Under Nonstandard Conditions: Testing the Markov Switching Model of GNP", Journal of Applied Econometrics, 7, 61-82.

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

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

[17] Platanakis, P. and A. Urquhart (2019). “Portfolio Management with Cryp- tocurrencies: The Role of Estimation Risk”, Economics Letters, 177, 76-80.

[18] Thies, S. and P. Molnar (2018), “Bayesian change point analysis of Bitcoin returns”, Finance Research Letters, 27, 223-227.

[19] Van Hardeveld, G.J., Webber, C. and K. O’Hara (2017). “Deviating from the cybercriminal script: exploring tools of anonymity (mis)used by carders on cryptomarkets”, American Behavioral Scientist, 61, 11, 1244-1266.

Table 1: Descriptive Statistics and Hansen Test

Panel A	Descriptive Statistics[d]							
	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	30 261							

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				
o	0 θ01 (0 ⫬421)	30 θ02 (0 θ69)	30 θ01 (0 θ00)	30 θ06 (0 θ00)	0 θ01 (0 ∃12)	30 θ02 (0 θ89)	30 θ01 (0 θ00)	30 θ06 (0 θ00)
o	0 θ12 (0 θ00)	0 θ31 (0 θ00)	00013) (0 θ00)	0 θ38 (0 θ00)	0 θ12 (0 θ00)	00(2 000)		

Table 3: Markov switching Estimation Results - Cyber Attacks

	Two weeks cyber attacks			
	Bitcoin	Ethe.	Lite.	Stellar
	Mean Equation			
o	0 001 (0 387)	30 002 (0 078)	30 001 (0 000)	30 006 (0 000)
o	0 013 (0 000)	0 031 (0 000)	0 013 (0 000)	0 038 (0 000)
k	0 002 (0 000)	0 014 (0 036)	0 004 (0 000)	0 028 (0 001)
k	0 057 (0 000)	0 127 (0 000)	0 079 (0 000)	0 150 (0 000)
$!_1$	30 069 (0 000)	30 124 (0 000)	30 147 (0 000)	30 112 (0 000)
	Transition Probabilities			
	Low Regime			
0	3 974 (0 012)	4 955 (0 000)	6 531 (0 000)	4 055 (0 000)
1	30 119 (0 008)	30 092 (0 003)	30 149 (0 003)	30 124 (0 038)
2	0 131 (0 061)	30 017 (0 699)	30 028 (0 818)	30 137 (0 038)
3	36 824 (0 000)	35 439 (0 000)	34 851 (0 000)	31 271 (0 000)
	High Regime			
0	32 401 (0 023)	31 264 (0 148)	33 639 (0 000)	36 683 (0 002)
1	0 021 (0 039)	0 074 (0 028)	0 042 (0 044)	0 143 (0 003)
2	30 025 (0 454)	30 086 (0 016)	0 033 (0 514)	0 104 (0 046)
3	6 669 (0 000)	4 583 (0 000)	4 701 (0 000)	5 021 (0 000)
	Diagnostic Tests			
LB	0 272	0 451	0 =	

Figure 1: