Department of
Economics and Finance

-power variation with the median realized variance estimator .[3] We consider as a jump if it satisfies the following condition:

$$\frac{|\quad|}{\sqrt{\qquad\qquad_{-1}(\ )}} \geq \sqrt{2\log\quad} - \frac{\log\pi + \log(\log\quad)}{2}$$

3.4. *Cyber-attack effects on cryptocurrencies*

We analyze the effects of cyber-attacks returns ( ), realized volatility ( ) and trading volume ( ). In particular, we analyze how cryptocurrencies are affected by cyber-attack types (i.e., cyber-crime ( ), cyber-espionage ( ), cyber-warfare ( ) and hacktivism ( )), targets (i.e., government ( ), industry ( ), finance ( ), cryptocurrency exchange ( ) sectors and US versus non-US countries ( )) while controlling for hash rate ( ), economic uncertainty ( ), stock market liquidity ( ) and real GDP ( ) for cyber-attack incident *i*. Thus, multiple cyber-attacks can occur on a single day. and represent the cryptocurrency and global economy control variables, respectively. and are the country-specific control variables whose average across the relevant countries for each cyber-attack incident *i* is used. The cyber-attack types and targets are binary variables equal to one if the cyber-attack matches a given type or target and zero otherwise.[4] We estimate the following OLS regressions (where the is the error term):

$$= {}_0 + {}_1( ) + {}_2( ) + {}_3( ) + {}_4( ) + {}_5( ) + {}_6( ) + {}_7( ) + {}_8( ) + {}_9( ) + {}_{10}( ) + {}_{11}( ) + {}_{12}(\times) + {}_{13}(\times) + {}_{14}( ) + {}_{15}( ) + \quad (3)$$

$$= {}_0 + {}_1( ) + {}_2( ) + {}_3( ) + {}_4( ) + {}_5( ) + {}_6( ) + {}_7( ) + {}_8( ) + {}_9( ) + {}_{10}( ) + {}_{11}( ) + {}_{12}(\times) + {}_{13}(\times) + {}_{14}( ) + {}_{15}( ) + \quad (4)$$

$$= {}_0 + {}_1( ) + {}_2( ) + {}_3( ) + {}_4( ) + {}_5( ) + {}_6( ) + {}_7( ) + {}_8( ) + {}_9( ) + {}_{10}( ) + {}_{11}( ) + {}_{12}( ) + {}_{13}(\times) + {}_{14}(\times) + {}_{15}( ) + {}_{16}( ) + \quad (5)$$

We then extend the analysis to jumps (see Section 3.2 above). Specifically, average hourly jumps per day ( ) is the dependent variable in the following regression (7):

$$= {}_0 + {}_1(\quad) + {}_2(\quad) + {}_3(\quad) + {}_4(\quad) + {}_5(\quad) + {}_6(\quad)$$
$$+ {}_7(\quad) + {}_8(\quad) + {}_9(\quad) + {}_{10}(\quad) + {}_{11}(\quad) + {}_{12}(\quad \times \quad)$$
$$+ {}_{13}(\quad \times \quad) + {}_{14}(\quad) + {}_{15}(\quad) +$$

[Insert Table 2]

Cyber-attacks targeting the government (Gov) and financial sectors (Fin) have a negative effect on the cryptocurrencies realized volatility (possibly because of overreacting cyber security firms), while Tf1 0 0 1 147.02 589.54 Tm0 g0 G[( )] TJETQq0.00000912 0i

positive relationship between risk and trading volumes could also be explained by a higher percentage of risk-loving investors relative to risk-averse ones; for the same reason greater economic uncertainty increases trading volumes.

However, we do not find any significant impact of cyber-attacks on realized volatility and trading volumes in the case of the US; we conjecture that the presence of more developed cyber security firms in this country could be the

of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare the data source is Hackmageddon) as well as four target sectors (government, industry, finance and cryptocurrency exchange). Moreover, it implements the jump test of Prokopczuk and Wese Simen (2014) and provides additional evidence allowing for jumps in the variables of interest.

Our analysis confirms that in general cryptocurrencies are highly vulnerable to cyber-attacks, owing to the underlying blockchain technology and the possibility to make transactions anonymous (see, e.g., Bouveret 2018, and Benjamin et al., 2019). These appear to be a significant risk factors and to cause severe disruption to markets through their effects on returns, realized volatility and volumes. Other sectors of the economy are also significantly affected. It is therefore essential that appropriate strategies should be designed to enhance cyber security (see, e.g., van Hardeveld et al., 2017).

Interestingly, our findings also reveal some noticeable differences between the US and

profiles. The distinguishing features of the US setup should therefore be taken into account when developing methods to combat cyber-crime aimed, for instance, at cracking blockchain cryptography to trace transactions (e.g., the task force suggested by Konowicz, 2018).

eRenere

Lee, S.S. and Mykland, P.A. (2008) Jumps in Financial Markets: A New Nonparametric Test and Jump Dynamics, *The Review of Financial Studies*, 21(6), pp. 2535 2563.

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

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

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

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

Prokopczuk, M. and Wese Simen, C. (2014) What Makes the Market Jump? Available at SSRN: https://ssrn.com/abstract=2449952 or http://dx.doi.org/10.2139/ssrn.2449952

Stewart, E. (2019) *If bitcoin is so safe, why does it keep getting hacked?* Available at https://www.vox.com/recode/2019/5/8/18537073/binance-hack-bitcoin-stolen-blockchain-security-safu

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

Van Hardeveld, G.J., We

Table 1. Summary statistics

The following table shows summary statistics for cyber-attacks, liquidity and hash rate (Panel A), and five cryptocurrencies including Bitcoin (Panel B), Ethereum (Panel C), Litecoin (Panel D), XRP (Panel E) and Stellar (Panel F). Bit, Eth, Lit, XRP and Stel denote Bitcoin, Ethereum, Litecoin, XRP and Stellar, respectively. _R, _RV, _V, _AHJ following stand for log return, realized volatility, trading volume and average hourly jump per day, respectively, of each of the five cryptocurrencies in turn (e.g., Bit_R indicates log returns in the case of Bitcoin). The data for cyber-

Max	0.173	43.47	304.74	1819.26
N	4390	4462	4462	3271

Panel G. Stellar

Poland	WSE WIG INDEX
Qatar	QE Index
Russian Federation	MICEX INDEX
Saudi Arabia	TADAWUL ALL SHARE INDEX
Sweden	OMX STOCKHOLM 30 INDEX
Singapore	Straits Times Index STI

Th1.42 23nn(54(a)]] TJETQq72.264 707.42 233.78

Table 2. Effects of cyber-

The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency s return (Bit_R, Eth_R, Lit_R, XRP_R, Stel_R) as a dependent variable affected by cyber-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H), countries (US) and block ry specific stock market liquidity (Liq) and real gross domestic product (RGDP). We report the F-statistics, R^2 and number of observations (N). The t-statistics are in the brackets. ***, ** and * denote significance at 1, 5 and 10% levels, respectively.

	Bit_R	Eth_R	Lit_R	XRP_R	Stel_R
	(1)	(2)	(3)	(4)	(5)
Intercept	0.063	0.052	0.11	0.026	0.013
	(1.508)	(0.726)	(1.688)	(0.349)	(0.165)
Gov	0.02	-0.055	0.008		
	(0.509)	(-0.758)	(0.132)		

	(-2.355)	(0.933)	(-0.469)	**(2.716)**	**(2.389)**
RGDP	0.00002	**0.0006***	-0.0001	-0.0003	-0.0003
	(0.092)	**(1.772)**	(-0.51)	(-0.82)	(-0.866)
F-statistics	**3.11*****	**44.58*****	**2.65*****	**3.24*****	**2.53*****
Adjusted R^2	0.02	0.30	0.01	0.02	0.01
N	3260	2873	3260	3260	3260

Table 3. Effects of cyber-

The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency s realized volatility (Bit_RV, Eth_RV, Lit_RV, XRP_RV, Stel_RV) as a dependent variable affected by cyber-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H), countries (US) and

Table 4. Effects of cyber-

The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency s trading volume (Bit_V, Eth_V, Lit_V, XRP_V, Stel_V) as a dependent variable affected by cyber-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H), countries for economic uncertainty (EPU), and country specific stock market liquidity (Liq) and real gross domestic product (RGDP). We report the F-statistics, R^2 and number of observations (N). The t-statistics are in the brackets. ***, ** and * denote significance at 1, 5 and 10% levels, respectively.

	Bit_V (1)	Eth_V (2)	Lit_V (3)	XRP_V (4)	Stel_V (5)
Intercept	**14.647***** **(22.735)**	**16.45***** **(18.079)**	**5.525***** **(5.042)**	**3.305***** **(3.499)**	**5.715***** **(5.265)**
Gov	-0.746 (-1.239)	-0.502 (-0.543)	**-1.719*** **(-1.68)**	-0.81 (-0.873)	-1.311 (-1.208)
Ind	-0.66 (-1.1)	-0.463 (-0.503)	-1.663 (-1.63)	-0.846 (-0.917 25	

	(17.668)	**(5.321)**	**(25.369)**	**(48.502)**	**(40.456)**
EPU	**0.011*****	**0.012*****	**0.014*****	**0.014*****	**0.012*****
	(45.048)	**(33.366)**	**(33.995)**	**(39.769)**	**(26.659)**
RGDP	0.001	0.004	-0.002	0.002	0.0002
	(0.387)	(0.953)	(-0.371)	(0.527)	(0.036)
F-statistics	**1530*****	**1014*****	**646.7*****	**1333*****	**1427*****
Adjusted R^2	0.93	0.91	0.85	0.92	0.93
N	3260	2873	3260	3260	3260

Table 5. Effects of cyber- -US countries

The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency s return (Bit_R, Eth_R, Lit_R, XRP_R, Stel_R) as a dependent variable affected by cyber-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H)
(Hash) while controlling for economic uncertainty (EPU), and country specific stock market liquidity (Liq) and real gross domestic product (RGDP). We show these for US (Panel A) and non-US (Panel B) countries. We report the F-statistics, R^2 and number of observations (N). The t-statistics are in the brackets. ***, ** and * denote significance at 1, 5 and 10% levels, respectively.

	Bit_R	Eth_R	Lit_R	XRP_R	Stel_R
	(1)	(2)	(3)	(4)	(5)
Intercept	-0.064	0.044	0.052	-0.041	0.028
	(-1.048)	(0.624)	(0.554)	(-0.495)	(0.32)

RGDP

Table 6. Effects of cyber-

RGDP	**-0.003*** (-55.724)**	**-0.002*** (-2.695)**	**-0.004*** (-45.765)**	**-0.007*** (-31.81)**	**-0.009*** (-31.252)**
Crypto × Hash	-0.000009 (-0.085)	0.002 (1.504)	0.000002 (0.014)	-0.00007 (-0.177)	-0.00002 (-0.044)
F-statistics	**370.9***	**9.84***	**337.9***	**67.12***	**121***
Adjusted R^2	0.85	0.13	0.84	0.5	0.64
N	1720	1526	1720	1720	1720

			-US		
	Bit_RV (1)	Eth_RV (2)	Lit_RV (3)	XRP_RV (4)	Stel_RV (5)
Intercept	**0.046*** (129.84)**	0.008 (0.622)	**0.069*** (129.933)**	**0.072*** (78.554)**	**0.066*** (52.187)**
Gov					

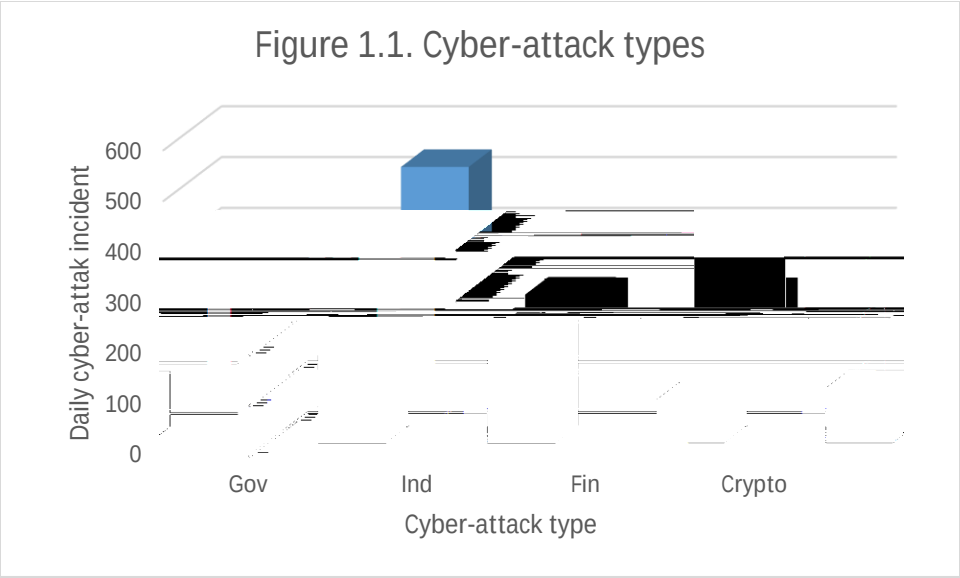
RGDP	0.000005

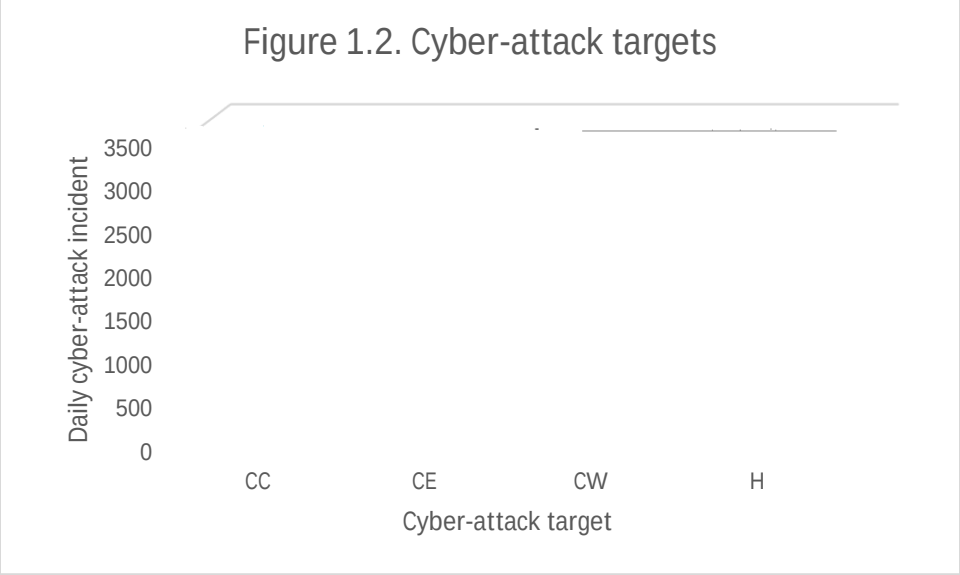
Table 7. Effects of cyber- -US countries

The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency s trading volume (Bit_V, Eth_V, Lit_V, XRP_V, Stel_V) as a dependent variable affected by cyber-

Figure 1. Cyber-attack frequency per day

The figures below show the cyber-attack frequency per day by different cyber-attack types (Figure 1.1) and targets (Figure 1.2).





Appendix

Correlation matrix including daily cryptocurrency data

The following tables show the correlation matrix of our sample including daily data of Bitcoin (Panel A), Ethereum (Panel B), Litecoin (Panel C), XRP (Panel D) and Stellar (Panel E). A Pearson correlation test has been carried out. [a], [b] and [c] denote significance at 1, 5 and 10% levels, respectively.

H (h)	0.25[a]	-0.02	0.05[a]	-0.05[a]	-0.57[a]	-0.11	-0.06[a]	1[a]	
Eth_R (i)	-0.01	-0.02	0	0	-0.01	-0.01	0	0.03[c]	1[a]

Fin (c)	-0.04[a]	0.01	1[a]			
Crypto (d)	-0.04[a]	-0.05[s]	-0.02	1[a]		
CC (e)	-0.27[a]	0.1[a]	0	0.08[a]	1[a]	
CE (f)	0.1[a]	-0.1[a]	-0.04[a]	-0.05[a]	-0.65[a]	1[a]