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

Working Paper

Cyber-Attacks and Cryptocurrencies

CESifo Working Paper, No. 8124

Provided in Cooperation with:
Ifo Institute – Leibniz Institute for Economic Research at the University of Munich

Suggested Citation: Caporale, Guglielmo Maria; Kang, Woo-Young; Spagnolo, Fabio; Spagnolo, Nicola (2020) : Cyber-Attacks and Cryptocurrencies, CESifo Working Paper, No. 8124, Center for Economic Studies and ifo Institute (CESifo), Munich

This Version is available at:
https://hdl.handle.net/10419/216520

CESifo WORKING PAPERS

8124
2020

February 2020

Cyber-Attacks and Cryptocurrencies

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

CESifo

Impressum:

CESifo Working Papers
ISSN 2364-1428 (electronic version)
Publisher and distributor: Munich Society for the Promotion of Economic Research - CESifo GmbH
The international platform of Ludwigs-Maximilians University's Center for Economic Studies and the ifo Institute
Poschingerstr. 5, 81679 Munich, Germany
Telephone +49 (0)89 2180-2740, Telefax +49 (0)89 2180-17845, email office@cesifo.de
Editor: Clemens Fuest
https://www.cesifo.org/en/wp
An electronic version of the paper may be downloaded
· from the SSRN website: www.SSRN.com
· from the RePEc website: www.RePEc.org
· from the CESifo website: https://www.cesifo.org/en/wp

CESifo *Working Paper No. 8124*

Cyber-Attacks and Cryptocurrencies

Abstract

This paper provides some comprehensive evidence on the effects of cyber-attacks on the returns, realized volatility and trading volume of five of the main cryptocurrencies (Bitcoin, Ethereum, Litecoin, XRP and Stellar) in 99 developed and developing countries. More specifically, it investigates the effects of four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare) on four target sectors (government, industry, finance and cryptocurrency exchange). We find that in the US cyber security firms tend to overreact to cyberattacks affecting cryptocurrencies and more wealth is spent on cyber security compared to other countries. Both hacktivism and cyber-warfare have a significant impact on cryptocurrencies. Cryptocurrency exchanges are more vulnerable to cyber-attacks in non-US countries and in the presence of high economic uncertainty and less so if the industry sector is already being targeted. Finally, cryptocurrency investors exhibit risk-loving behaviour when the hash rate and cryptocurrency returns increase and risk-averse one when cyber-attacks target the financial and industry sectors and economic uncertainty is high.

JEL-Codes: C220, E400, G100.

Keywords: cyber security, cyber-attacks, cryptocurrencies, return and volatility jumps.

*Guglielmo Maria Caporale**
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
Guglielmo-Maria.Caporale@brunel.ac.uk

Woo-Young Kang
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
woo-young.kang@brunel.ac.uk

Fabio Spagnolo
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
fabio.spagnolo@brunel.ac.uk

Nicola Spagnolo
Department of Economics and Finance
Brunel University London, Uxbridge,
Middlesex UB8 3PH, United Kingdom
nicola.spagnolo@brunel.ac.uk

*corresponding author

February 2020

1. Introduction

Despite their rather recent introduction, cryptocurrencies have very rapidly become a widely used type of currency and also a favorite target for cyber criminals, hacksters and fraudsters. The main reason is their vulnerability, which is a direct consequence of their anonymity resulting from highly encrypted blockchain technology, where blockchain is essentially "a decentralized network of synchronized online registries that track the ownership and value of each token" (see Matthews, 2017). This implies that the security of cryptocurrencies depends entirely on the blockchain algorithm being used. Since all transactions are recorded, they can be tracked down; however, they can be made anonymous by means of a so-called "tumbler" which exchanges the tokens. Further, there is no central authority responsible for cryptocurrencies.

An important issue in this context is the possible occurrence of a cyber-attack, which can be defined as an attack from one or more computers against other computers or networks aiming at disabling and/or managing the latter and obtaining access to information, thereby compromising its confidentiality, integrity and availability. Such a breach of security represents a form of cyber risk which has been found to be significant in the case of the financial sector (see Kopp et al., 2017). The present study examines its impact on a wider range of sectors and provides some comprehensive evidence on the effects of cyber-attacks on the returns, realized volatility and trading volume of five of the main cryptocurrencies (Bitcoin, Ethereum, Litecoin, XRP and Stellar – the data sources are CoinMarketCap and Bitfinex) in 99 developed and developing countries. More specifically, it investigates the effects of four different types of cyber-attacks (cyber-crime, cyber-espionage, hacktivism and cyber-warfare – the data source is Hackmageddon) on four target sectors (government, industry, finance and cryptocurrency exchange) by estimating ordinary least squares (OLS) regressions using daily data over the period from March 1, 2015 to February 28, 2019; the model also includes appropriate control variables, namely stock market liquidity, the hash rate, real GDP and economic uncertainty. Further, logistic regressions are run to identify the factors making cryptocurrency exchanges more susceptible to cyber-attacks.

The analysis is then extended to allow for the possibility of jumps in the variables of interest. Specifically, as a first step the jump test proposed by Prokopczuk and Wese Simen (2014) is carried out, and then the OLS regressions are re-estimated for average hourly jumps as well as their realized volatility and trading volume whenever statistically significant jumps are detected by the test. Finally, the entire analysis is repeated separately for the US and the other

countries respectively to shed some light on the differences observed between the former and the latter, possibly reflecting the presence of more developed cyber security firms in the US.

We find that cyber security firms in the US respond more actively to cyber attacks, which leads to a safer cryptocurrency trading environment and higher returns. Further, realized volatility falls in the government and financial sectors, possibly as a result of overreacting cyber security firms. Cryptocurrency exchanges in non-US countries appear to be more vulnerable to cyber-attacks with faster mining speed compared to those hitting the US, which invests more heavily in cyber security. Consequently, positive wealth effects on returns and volatility are found in the case of the US but not of the other countries, whose cryptocurrency exchanges appear to be more prone to cyber-attacks given the lower level of cyber security; the effects on the trading volume of risk and hash rate are instead comparable and suggest that investors are risk-lovers. However, when economic uncertainty is high and cyber-attacks target the financial and industry sectors, investors exhibit risk-averse behaviosr.

Regarding cyber-attacks on cryptocurrency exchanges, non-US countries appear to be more likely to be targeted given their lower degree of cyber security, and the lower percentage of risk-loving investors in these countries also means that economic uncertainty tends to reduce volatility. As for the cases when jumps occur, our analysis shows that cyber-attacks targeting cryptocurrency exchanges have a significant downside risk impact, particularly on Bitcoin and Stellar, in both the US and the other countries. The hash rate and economic uncertainty have a consistently positive and negative effect, respectively, on purchases and sales of cryptocurrencies.

The remainder of the paper is organized as follows. Section 2 reviews the relevant literature. Section 3 describes the data and the methodology. Section 4 presents the empirical results. Section 5 offers some concluding remarks.

2. Literature Review

The impact of cyber-crime on cryptocurrency markets and the economy as a whole has been analyzed in various recent papers. For instance, Benjamin et al. (2019) estimated that cyber-attacks from criminals operating in underground web communities such as Darknet have resulted in estimated annual losses of $445 billion for the global markets (see Graham, 2017). In another interesting study, Bouveret (2018) used a Value-at-Risk (VaR) framework to measure cyber risk and the resulting losses in a number of countries.

In the case of cryptocurrencies, given their distinctive features (see Corbet et al., 2019a) different methods are required to estimate and manage risk (see Platanakis and Urquhart, 2019). Cyber-attacks are considered a very important risk factor by both small and large "miners", whose task 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) provided some evidence on the disruptions caused by cyber security breaches in the case of the cryptocurrency markets; these have also been targeted for the purpose of illicit online drug trading (see Martin, 2014), which has given rise to a number of ethical issues (see Martin and Christin, 2016).

Caporale et al. (2019) used a Markov-switching non-linear specification to analyse the effects of cyber-attacks on returns in the case of four cryptocurrencies (Bitcoin, Ethereum, Litecoin and Stellar) over the period 8/8/2015–2/28/2019. They found significant negative effects on the probability of cryptocurrencies staying in the low volatility regime. Corbet et al. (2019b) estimated a DCC-GARCH model and documented that cryptocurrency hacks increase both the volatility of the currencies hacked and their correlations with other cryptocurrencies; further, they decrease price discovery for the hacked currencies in comparison to others. As for the effects on returns, abnormal ones are observed in the hours preceding the hack, which revert to zero when this is publicly announced. However, this research is limited to 17 hacking events on the cryptocurrency exchanges within less than a year.

Developing strategies to deal with and possibly prevent cyber crime has therefore become very important (see van Hardeveld et al., 2017). In the case of the US, a specific concern has been the use of cryptocurrencies to avoid sanctions. It has been suggested that a task force including agencies from the Departments of the Treasury, State, Justice and Defense should be created to focus in particular on the cracking of blockchain cryptography to trace transactions (see Konowicz, 2018).

None of the above studies consider different categories of cyber-attacks and their effects on returns, realized volatility as well as volume in various sectors, neither do they allow for possible jumps in the variables. The analysis below addresses all these issues using an appropriate empirical framework which yields informative new findings about the effectiveness of cyber security in the US and elsewhere.

3. Data and Methodology

3.1. *Cyber-attack data*

The cyber-attack data are taken from the website http://www.hackmageddon.com/ which shows the cyber-attack timeline with target industry, country and cyber-attack type at a daily frequency. Specifically, we have collected data on 4463 daily cyber-attacks (including daily overlaps) from March 1, 2015 to February 28, 2019 for four target sectors, namely the government (Gov), industry (Ind), finance (Fin) and cryptocurrency exchange sectors, and created in each case binary variables equal to 1 for the sector affected and 0 for the others. Thus there are four cyber-attack binary variables, namely cyber-crime (CC), cyber-espionage (CE), hacktivism (H) and cyber-warfare (CW), each being equal to 1 if the corresponding type of attack occurs and 0 otherwise. However, CW is dropped from the model to avoid the dummy variable trap.

3.2. *Cryptocurrency data*

We collect daily data on the closing prices and trading volumes for five cryptocurrencies (Bitcoin, Ethereum, Litecoin, XRP and Stellar) over the period March 1, 2015 to February 28, 2019 from CoinMarketCap (http://www.coinmarketcap.com). We take logs of returns, realized volatility and trading volumes for the analysis.

Since cryptocurrencies typically exhibit high volatility with speedy transactions compared to other currencies, we extend our analysis to examine jump data based on their hourly frequencies. Given the fact that CoinMarketCap does not provide cryptocurrency data at a higher frequency than daily, we also use Bitfinex (https://www.bitfinex.com/) as a data source since it includes data denoted in USD at the millisecond frequency. We collect these data from March 1, 2015 to February 28, 2019 and select only the last cryptocurrency transactions within each hour to have the closing cryptocurrency prices within that hour.[1] We also take the logs of returns, realized volatility and trading volumes[2] for these hourly data. Then we select those passing the jump test proposed by Prokopczuk and Wese Simen (2014), who extend the Lee and Mykland

[1] CoinMarketCap and Bitfinex are different trading platform whilst cryptocurrency prices are global indices; in particular, CoinMarketCap has been in existence for longer than Bitfinex and therefore spans a longer time period. Thus, the daily closing prices of cryptocurrencies on these two platforms could be slightly different. For this reason, we use CoinMarketCap and Bitfinex data separately in our analysis.

[2] The hourly trading volumes in Bitfinex can be either positive or negative as they are recorded as spot buy or sell transactions in each millisecond. We take their absolute value before applying the log transformation.

(2008)'s model by replacing its bi-power variation with the median realized variance estimator $MedRV$.[3] We consider r_j as a jump if it satisfies the following condition:

$$\frac{|r_t|}{\sqrt{MedRV_{i-1}(r)}} \geq \sqrt{2\log n} - \frac{\log\pi + \log(\log n)}{2\sqrt{2\log n}} - \frac{\log(-\log x)}{\sqrt{2\log n}} \quad (1)$$

where $MedRV_{i-1}(r)$ is calculated as:

$$MedRV_{i-1}(r) = \frac{\pi}{(6-4\sqrt{3}+\pi)(\mathrm{K}-3)} \times \frac{1}{K-3} \times \sum_{j=i-K+3}^{i-1} \mathrm{median}(|r_j|, |r_{j-1}|, |r_{j-2}|)^2 \quad (2)$$

According to the above jump test, if the ratio ($\frac{|r_t|}{\sqrt{MedRV_{i-1}(r)}}$) is at least equal to the critical value ($\sqrt{2\log n} - \frac{\log\pi+\log(\log n)}{2\sqrt{2\log n}} - \frac{\log(-\log x)}{\sqrt{2\log n}}$), the null hypothesis that r_t is a normal return (not a jump) is rejected. r_t is the log return of cryptocurrency prices at time *t*. *K* refers to the rolling window width, and is an integer between $\sqrt{252 \times nobs}$ and $252 \times nobs$ where $nobs$ is the number of returns observed each trading day. We use hourly data with 24 returns per trading day, i.e. $nobs = 24$. Following Lee and Mykland (2008), we choose the optimal window size *K* for hourly data as 78, the smallest integer of *K* ($= \sqrt{252 \times nobs}$). x is a 95% confidence interval as in Lee and Mykland (2008) and Prokopczuk and Wese Simen (2014). We do not consider seasonality since cryptocurrency returns have been shown not to exhibit it (Kaiser, 2019), unlike stock returns (see Prokopczuk and Wese Simen, 2014).

3.3. *Liquidity*

We measure liquidity using the following FHT method due to Fong et al. (2017):

$$\mathrm{FHT} \equiv \mathrm{S} \equiv 2\sigma N^{-1}\left(\frac{1+z}{2}\right) \quad (1)$$

where

$$\mathrm{z} \equiv \mathrm{Zeros} \equiv \frac{ZRD}{TD+NTD} \quad (2)$$

ZRD is the number of zero return days, TD is the number of trading days and NTD is the number of no-trade days in a given month. Further, S is the percentage transaction cost, $N^{-1}()$ is the

[3] According to Andersen et al. (2012), the median realized variance estimator, a truncation-based estimator, supersedes the bi-power variation method (Prokopczuk and Wese Simen, 2014).

inverse of the cumulative normal distribution function and σ is the standard deviation of the daily stock return over a month.

Table 1 shows summary statistics for the series being analyzed, namely cyber-attack target and types (Panel A), economic and blockchain control variables (Liquidity, hash rate, economic uncertainty index and real GDP in Panel B), and the logs of returns, realized volatility and trading volume of the five cryptocurrencies under investigation (Bitcoin (Panel C), Ethereum (Panel D), Litecoin (Panel E), XRP (Panel F) and Stellar (Panel G)). Summary statistics for all five cryptocurrencies, for both the daily (_R, _RV and _V) and average hourly jumps per day (_AHJ), are reported in Table 1. The sample size for average hourly jumps per day is smaller since we only include the data passing the jump test (Section 3.2). The economic control variables, economic uncertainty index (EPU) and real GDP (RGDP) are all lagged one year to avoid hindsight bias.

In most cases the distributions of cyber-attacks, liquidity, hash rate and economic control variables (EPU and real GDP) are right-skewed, the exception being the cyber-crime variable, which has a larger median than its mean. We drop from the sample two cyber-attacks that targeted Belarus and Nepal since these two countries do not have an appropriate stock market index to calculate liquidity as above. Thus, we consider 99 countries and their corresponding market indices (Panel H) and find that Bitcoin exhibits the largest trading volume (Panel C: Bit_V) among all five cryptocurrencies. XRP appears to be the riskiest of the five cryptocurrencies in our sample (Panel F: XRP_RV and XRP_AHJ).

In our sample cyber-crime (CC: 3397 daily incidents) and industry sector (Ind: 541 daily incidents) are the most frequent cyber-attack type and target, respectively (see Figure 1). However, there are also other types of both.

[Insert Table 1]

[Insert Figure 1]

3.4. *Cyber-attack effects on cryptocurrencies*

We analyze the effects of cyber-attacks on cryptocurrencies' returns (R_i), realized volatility (RV_i) and trading volume (V_i). In particular, we analyze how cryptocurrencies are affected by cyber-attack types (i.e., cyber-crime (CC_i), cyber-espionage (CE_i), cyber-warfare (CW_i) and hacktivism (H_i)), targets (i.e., government (Gov_i), industry (Ind_i), finance (Fin_i), cryptocurrency exchange ($Cyber_i$) sectors and US versus non-US countries (US_i)) while controlling for the blockchain's hash rate ($Hash_i$), economic uncertainty (EPU_i), stock market liquidity (Liq_i) and real GDP ($RGDP_i$) for cyber-attack incident i. Thus, multiple cyber-attacks can occur on a single day. $Hash_i$ and EPU_i represent the cryptocurrency and global economy control variables, respectively. Liq_i and $RGDP_i$ 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 u_i is the error term):

$$\begin{aligned} R_i = {} & \beta_0+\beta_1(Gov_i) + \beta_2(Ind_i) + \beta_3(Fin_i) + \beta_4(Crypto_i) + \beta_5(CC_i) + \beta_6(CE_i) \\ & + \beta_7(H_i) + \beta_8(Liq_i) + \beta_9(US_i) + \beta_{10}(RV_i) + \beta_{11}(Hash_i) + \beta_{12}(Crypto_i \times US_i) \\ & + \beta_{13}(Crypto_i \times Hash_i) + \beta_{14}(EPU_i) + \beta_{15}(RGDP_i) + u_i \end{aligned} \quad (3)$$

$$\begin{aligned} RV_i = {} & \beta_0+\beta_1(Gov_i) + \beta_2(Ind_i) + \beta_3(Fin_i) + \beta_4(Crypto_i) + \beta_5(CC_i) + \beta_6(CE_i) \\ & + \beta_7(H_i) + \beta_8(Liq_i) + \beta_9(US_i) + \beta_{10}(R_i) + \beta_{11}(Hash_i) + \beta_{12}(Crypto_i \times US_i) \\ & + \beta_{13}(Crypto_i \times Hash_i) + \beta_{14}(EPU_i) + \beta_{15}(RGDP_i) + u_i \end{aligned} \quad (4)$$

$$\begin{aligned} V_i = {} & \beta_0+\beta_1(Gov_i) + \beta_2(Ind_i) + \beta_3(Fin_i) + \beta_4(Crypto_i) + \beta_5(CC_i) + \beta_6(CE_i) \\ & + \beta_7(H_i) + \beta_8(Liq_i) + \beta_9(US_i) + \beta_{10}(R_i) + \beta_{11}(RV_i) + \beta_{12}(Hash_i) \\ & + \beta_{13}(Crypto_i \times US_i) + \beta_{14}(Crypto_i \times Hash_i) + \beta_{15}(EPU_i) + \beta_{16}(RGDP_i) + u_i \end{aligned} \quad (5)$$

We also estimate the following logistic regression to analyze the factors making a given cryptocurrency exchange a cyber-attack target:

$$\begin{aligned} Crypto_i = {} & \beta_0+\beta_1(Gov_i) + \beta_2(Ind_i) + \beta_3(Fin_i) + \beta_4(CC_i) + \beta_5(CE_i) + \beta_6(H_i) \\ & + \beta_7(Liq_i) + \beta_8(US_i) + \beta_9(R_i) + \beta_9(RV_i) + \beta_{10}(Hash_i) + \beta_{11}(Crypto_i \times US_i) \\ & + \beta_{12}(Crypto_i \times Hash_i) + \beta_{13}(EPU_i) + \beta_{14}(RGDP_i) + u_i \end{aligned} \quad (6)$$

[4] CW_i is not included to avoid the dummy variable trap.

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

$$AHJ_i = \beta_0+\beta_1(Gov_i) + \beta_2(Ind_i) + \beta_3(Fin_i) + \beta_4(Crypto_i) + \beta_5(CC_i) + \beta_6(CE_i) + \beta_7(H_i) + \beta_8(Liq_i) + \beta_9(US_i) + \beta_{10}(JRV_i) + \beta_{11}(Hash_i) + \beta_{12}(Crypto_i \times US_i) + \beta_{13}(Crypto_i \times Hash_i) + \beta_{14}(EPU_i) + \beta_{15}(RGDP_i) + u_i \quad (7)$$

We estimate equation (7) to analyze the cyber-attack effects on the cryptocurrencies' jumps.

4. Empirical Results

As already mentioned, our aim is to analyze the effects of cyber-attack target sector, type and country on the returns, realized volatility and trading volume of five cryptocurrencies (Bitcoin, Ethereum, Litecoin, XRP and Stellar) controlling for the underlying block chain's hash rate and country-specific liquidity computed using the stock indices. There is no multicollinearity between these regressors as shown in the Appendix.

4.1. *Cyber-attack effects on cryptocurrencies*

Table 2 suggests that US cyber security firms tend to overreact to cyber-attacks. Their response makes the cryptocurrency trading environment safer, which enables investors to obtain higher investment returns. However, the higher hash rates (Hash) may make a cryptocurrency cheaper as it becomes easier to mine given the bigger total outstanding volume. In addition, there is more downside than upside risk, which eventually reduces cryptocurrency returns. Further, economic uncertainty (EPU) significantly affects cryptocurrency returns. However, its effects can be either positive or negative. Specifically, the downside risk for Bitcoin (which has the largest share in the cryptocurrency market) increases. On the other hand, the effects on XRP and Stellar returns are positive. Thus, investors appear to be risk-averse if trading Bitcoin and risk-loving in the case of XRP and Stellar. However, when cyber-attacks target cryptocurrency exchanges in the US (Crypto × US), Stellar investors exhibit risk-averse behaviour and are inclined to sell rather than buy, as indicated by the negative effect of uncertainty on returns. As for cyber-attack targets or types, only cyber warfare is found to affect returns significantly.

[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 those targeting the industry sector (Ind) can have either a positive or a negative impact (see Table 3). By contrast, no effects are detected in the case of cryptocurrency exchanges, presumably because these are relatively immune to cyber-attacks compared to other sectors as a result of their block chain property and related cyber security firms.

Concerning cyber-attack types, we find that hacktivism and cyber warfare have a significant impact on realized volatility. Hacktivism (H), which is "the act of gaining access to (and control over) third-party computer systems" (Bodford and Kwan, 2018), significantly increases cryptocurrency risk in most cases. Cyber-warfare (CW) is the use of computer technology to penetrate a nation's computer network in order to cause damage or disruption (Uma and Padmavathi, 2013),[5] and is also found to increase risk. However, no impact is detected when cyber-attacks target the US, a possible explanation being the presence of more developed cyber security firms and blockchain security in this country's cryptocurrency exchanges compared to the others.

Stock market liquidity (Liq) also tends to increase the realized volatility of the cryptocurrencies under investigation. In a previous study, Wei (2018) showed that in the case of cryptocurrencies more liquidity decreases volatility as market efficiency improves. Our findings suggest that investors regard cryptocurrencies as a substitute for stocks: as stock market liquidity and efficiency increase, they shift their trading activities from the cryptocurrency to the stock market. Consequently, it becomes more difficult to find counterparties to trade within the cryptocurrency market, its liquidity risk increases and so does volatility.

An increase in the block chain's hash rate (Hash) has a significant impact on the cryptocurrencies' realized volatility (see Table 3). This can be either positive (if cryptocurrencies

[5] More specifically, Uma and Padmavathi (2013) define cyber-crime (CC) as a criminal office which involves a computer either as an object or a tool to commit a material component of the offence. They also define cyber espionage (CE) as the cracking techniques and malicious software (e.g., Trojan horses and spy ware) to obtain secret information of individuals, groups and governments for gaining benefits of their own through illegal abuse methods and obtain information without the permission of the holder.

are generated at a faster speed, which increases their outstanding total, trading volumes and realized volatilities) or negative (if liquidity increases and the market becomes more efficient, which reduces volatilities).

Economic uncertainty (EPU) can also have either a positive or a negative effect on volatility. The former occurs if wealth is reduced by uncertainty and investors become more willing to take risks by investing in cryptocurrencies in order to earn higher returns; their behaviour then increases trading volumes and volatility as in the case of XRP and Stellar. On the other hand, realized volatility can fall if cyber security firms overreact by adopting excessive protection, as in the case of Bitcoin and Litecoin.

As for real GDP (RGDP), this variable has a negative and significant impact on realized volatility through its effects on investors' wealth; specifically, investors in wealthier countries with higher real GDP appear to be less willing to take risks when trading cryptocurrencies than those in other countries in order to earn higher returns.

[Insert Table 3]

As shown in Table 4, cyber-attacks targeting the government, financial and industry sectors have a negative impact on the trading volume. This suggests that investors tend to freeze their cryptocurrency trading activities to reduce possible losses. However, cyber-attacks targeting cryptocurrency exchanges can have either a positive or no effect on the trading volume. This is because, despite this type of threat to cryptocurrency exchanges, investors could have a strong belief that the blockchain system and some related insurance scheme (e.g., the emergency insurance fund introduced in July 2018, see Stewart, 2019) can protect them more effectively than in the case of other sectors. Stock market liquidity has a negative impact on the trading volume. A plausible interpretation is that investors regard the stock market as an alternative trading platform to the cryptocurrency market. Therefore, as liquidity in the former increases, they shift their trading activities to the latter, as already argued before.

We also find that the hash rate positively affects the trading volume: as it becomes easier to mine cryptocurrencies with a faster hash rate, trading increases, especially if investors are risk-lovers. Cryptocurrencies' return and realized volatility also have a positive effect on trading: when investors experience higher returns, they are more inclined to trade to make profits. A

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 explanation. Therefore, next we analyze the effects of cyber-attacks separately for the US and the other countries.

[Insert Table 4]

4.2. *Cyber-attacks effects on cryptocurrencies in the US and the other countries*

Table 5 shows that in the US, as wealth increases, investors tend to make profits from cryptocurrency trading. This could be due to the better technology used in terms of computers, Internet speed, information, etc. By contrast, real GDP does not have a significant impact on cryptocurrency investors in non-US countries; in other words, the additional wealth appears to be invested in other markets. Realized volatility has a significantly negative impact on returns in non-US countries, but either an insignificant or a positive one in the US, namely higher risk is seen as a positive signal in the US but a negative one elsewhere.

[Insert Table 5]

US wealth has a negative impact on risk, possibly because higher wealth is spent on reducing risk through cyber security; this does not happen in the other countries, where risk instead increases (see Table 6), this effect being magnified by an increase in the hash rate (the ease of mining cryptocurrencies). Thus, cryptocurrency exchanges in non-US countries appear to be more susceptible to cyber-attacks given the faster speed of mining cryptocurrencies owing to weaker cyber security compared to the US (Table 6). This is consistent with the findings in Kamiya et al. (2019) showing that in the case of firms cyber-attacks have an insignificant impact on their target if the board pays more attention to risk management before the attack; otherwise there is a significant shareholder wealth loss much larger than the attack's out-of-pocket costs (e.g., investigation and remediation costs, legal penalties, and regulatory penalties).

[Insert Table 6]

Higher wealth induces cryptocurrency investors to trade more in the US but not elsewhere, which suggests that the additional wealth might be spent on cyber security and cryptocurrency trading platforms in the US but not in the other countries (see Table 7), a result which is consistent with the previous findings reported in Table 5. Similarly, the evidence presented in Table 4 and 8 concerning the relationship between returns as well as realized volatility and the trading volume is consistent: both in the US and elsewhere higher risk leads investors to engage more in speculative activities to make up for their trading losses; further, they tend to be risk-lovers as indicated by the fact that both economic uncertainty and the hash rate have a positive impact on trading volumes.

[Insert Table 7]

4.3. *Cyber-attack effects on cryptocurrency exchanges*

Table 8 presents the evidence regarding cyber-attacks effects on cryptocurrency exchanges based on the estimation of logistic regressions for the five cryptocurrencies in our sample. We find that cryptocurrency exchanges are less likely to be targeted if the industry sector (Ind) is already being targeted; thus, these sectors appear to be substitute targets for cyber-attacks. Non-US countries are more likely to be targeted given their less effective cyber security and lower investment on cryptocurrency platforms compared to the US. Economic uncertainty increases the likelihood that cryptocurrency exchanges will be subject to cyber-attacks by making them more vulnerable. Then realized volatility either increases or decreases (see Table 3) depending on the percentage of risk-loving investors and the effectiveness of cyber security, both of which are typically higher in more developed countries such as the US.

[Insert Table 8]

4.4. *Cyber-attacks effect on cryptocurrency jumps*

Table 9 reports the results concerning the cyber-attacks effects on cryptocurrency jumps. The analysis is carried out only for the cases when the jump test given by equation (1) and (2) is passed. The calculated jumps for daily average frequencies are then used as the dependent variable.

Cyber-attacks targeting cryptocurrency exchanges appear to have a significant impact (either positive or negative) on average hourly jumps in some cases (e.g., Bitcoin and Stellar – see Table 9) in both the US and the other countries. As can be seen from Table 9, in the case of Bitcoin and Stellar there are downside risks affecting jumps when cyber-attacks target cryptocurrency exchanges. This is consistent with our finding in Table 2 of a more sizeable downside risk in cryptocurrency trading: especially Bitcoin and Stellar investors engage in a massive selloff of cryptocurrencies because of their worries resulting from cyber-attacks. This suggests that the Bitcoin and Stellar traders perceive a higher risk in hourly jumps when cyber-attacks occur, despite the highly developed cyber security. Litecoin shows some overreaction to cyber-attacks but this is only weakly significant. We also find that the hash rate and economic uncertainty consistently affect the cryptocurrency jumps except in the case of XRP. The increase in hash rates (Hash) makes mining easier and investors more eager to purchase cryptocurrencies. This drives up demand and leads to a positive jump. On the other hand, the negative sentiment resulting from economic uncertainty (EPU) makes investors sell cryptocurrencies because of the fear of further drops in their prices. This suggests that they might be risk-averse and trade less in the presence of greater uncertainty. However, the hash rate effect on cryptocurrency jumps indicates that they may exhibit risk-loving behaviour in the absence of cyber-attacks and economic uncertainty.

[Insert Table 9]

5. Conclusions

This paper sheds new light on the effects of cyber-attacks in a large set of developed and developing countries by estimating OLS regressions for five of the main cryptocurrencies (Bitcoin, Ethereum, Litecoin, XRP and Stellar), and distinguishing between four different types

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 the other countries, possibly reflecting different degrees of cyber security and investors' risk 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).

References

Andersen, T., Dobrev, D., and Schaumburg, E. (2012). Jump-robust volatility estimation using nearest neighbor truncation. *Journal of Econometrics*, 169(1), pp. 75–93.

Benjamin, V., J.S. Valacich and Chen, H. (2019), "DICE-E: a framework for conducting Darknet identification, collection, evaluation with ethics", *MIS Quarterly*, 43(1), pp. 1–22.

Bodford, J.E. and Kwan, V.S.Y. (2018) A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs? *Cyberpsychology, Behavior and Social Networking*, 21(2), pp. 73–77.

Bouveret, A. (2018), Cyber risk for the financial sector: a framework for quantitative assessment, *IMF Working Paper no. 18/143*.

Caporale, G.M., Kang, W-Y., Spagnolo, F. and Spagnolo, N. (2019), Non-linearities, cyber attacks and cryptocurrencies, *forthcoming in Finance Research Letters*.

Corbet, S., Lucey, B., Urquhart, A. and Yarovaya, L. (2019a), Cryptocurrencies as a financial asset: A systematic analysis, *International Review of Financial Analysis*, 62(C), pp. 182–199.

Corbet, S., Cumming, D.J., Lucey, B.M., Peat, M. and Vigne, S.A. (2019b), Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in cryptocurrency Markets, Available at SSRN: https://ssrn.com/abstract=3384707 or http://dx.doi.org/10.2139/ssrn.3384707.

Fong, K.Y.L., Holden, C.W., and Trzcinka, C.A. (2017) What Are the Best Liquidity Proxies for Global Research? *Review of Finance*, 21(4), pp. 1355–1401.

Graham, L. (2017), Cybercrime costs the global economy $450 billion: CEO, *CNBC*, Available at http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global economy-450-billion-ceo.html.

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

Kaiser, L. (2019) Seasonality in cryptocurrencies, *Finance Research Letters*, 31, pp. 232–238.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. and Stulz, R. (2019) Risk management, firm reputation, and the impact of successful cyberattacks on target firms, *forthcoming in Journal of Financial Economics*.

Konowicz, D.R. (2018), The New Game: Cryptocurrency Challenges US Economic Sanctions, Faculty of the United States Naval War College Newport, RI, mimeo.

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

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., Webber, C. and O'Hara, K. (2017) Deviating from the cybercriminal script: exploring tools of anonymity (mis)used by carders on cryptomarkets, *American Behavioral Scientist*, 61(11), pp. 1244–1266.

Wei, W.C. (2018) Liquidity and market efficiency in cryptocurrencies, *Economics Letters*, 168, pp. 21–24.

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-attacks, liquidity, hash rate and the five cryptocurrencies are daily and span the period from March 1, 2015 to February 28, 2019; they have been collected from http://www.hackmageddon.com, Bloomberg, https://data.bitcoinity.org and http://www.coinmarketcap.com, respectively. The Gov (government sector), Ind (industry sector), Fin (financial sector) and Crypto (cryptocurrency exchange) series are binary variables equal to one if the cyber-attack targets these sectors and zero otherwise. The CC (cyber-crime), CE (cyber-espionage), H (hacktivism) and CW (cyber-warfare) binary variable are equal to one if they match the cyber-attack type and zero otherwise. US is a binary variable equal to one if the cyber-attack targets the US and zero otherwise. Liq is a liquidity measure computed using the stock index of the country hit by a cyber-attack. In the case of cyber-attacks targeting multiple countries the average liquidity measure across those countries is used. Hash measures the average hashes per second across the mining pools on the blockchain level which we impose natural logarithm on it for scaling purpose. We report the mean, median, std (standard deviation), Min (minimum), 25^{th} (25^{th} percentile), 75^{th} (75^{th} percentile), Max (maximum) and N (number of observations) of each variable, as well as the list of countries with the corresponding market indices included in our sample (Panel G).

Panel A. Cyber-attacks targets and types									
	Gov	Ind	Fin	Crypto	CC	CE	CW	H	US
Mean	0.06	0.12	0.02	0.02	0.76	0.12	0.03	0.09	0.39
Median	0	0	0	0	1	0	0	0	0
Std.	0.25	0.33	0.14	0.15	0.43	0.32	0.17	0.29	0.49
Min	0	0	0	0	0	0	0	0	0
25^{th}	0	0	0	0	1	0	0	0	0
75^{th}	0	0	0	0	1	0	0	0	1
Max	1	1	1	1	1	1	1	1	1
N	4462	4462	4462	4462	4462	4462	4462	4462	4462

Panel B. Liquidity, hash rate, economic uncertainty index and real GDP				
	Liq	Hash	EPU	RGDP
Mean	0.006	40.76	154.04	4.70
Median	0.005	40.55	142.51	2.40
Std.	0.005	1.80	54.27	63.24
Min	0.000	37.67	81.69	-9.80
25^{th}	0.004	39.50	111.75	1.60
75^{th}	0.007	42.56	168.70	2.90

Max	0.173	43.47	304.74	1819.26
N	4390	4462	4462	3271

Panel C. Bitcoin				
	Bit_R	Bit_RV	Bit_V	Bit_AHJ
Mean	0.000	0.045	20.100	-0.003
Median	0.002	0.045	20.410	-0.002
Std.	0.039	0.003	2.269	0.044
Min	-0.208	0.042	16.180	-0.183
25^{th}	-0.012	0.044	17.960	-0.025
75^{th}	0.015	0.046	22.330	0.019
Max	0.215	0.053	23.890	0.113
N	4462	4462	4462	419

Panel D. Ethereum				
	Eth_R	Eth_RV	Eth_V	Eth_AHJ
Mean	0.000	0.006	18.880	0.000
Median	-0.003	0.001	20.350	-0.007
Std.	0.079	0.054	2.953	0.067
Min	-1.302	0.000	11.530	-0.139
25^{th}	-0.029	0.000	16.440	-0.045
75^{th}	0.029	0.004	21.410	0.056
Max	0.412	1.696	22.940	0.141
N	4017	4017	4017	193

Panel E. Litecoin				
	Lit_R	Lit_RV	Lit_V	Lit_AHJ
Mean	0.000	0.070	17.410	0.018
Median	0.000	0.069	18.320	0.000
Std.	0.061	0.004	2.614	0.438
Min	-0.514	0.064	13.090	-1.553
25^{th}	-0.020	0.067	14.700	-0.030
75^{th}	0.018	0.072	19.770	0.017
Max	0.510	0.080	22.660	5.446
N	4462	4462	4462	371

Panel F. XRP				
	XRP_R	XRP_RV	XRP_V	XRP_AHJ
Mean	0.003	0.076	16.750	0.025
Median	-0.004	0.077	17.610	0.044
Std.	0.073	0.005	3.278	0.074
Min	-0.616	0.065	10.910	-0.139
25^{th}	-0.024	0.074	13.460	-0.022
75^{th}	0.016	0.079	19.810	0.079
Max	1.027	0.088	22.930	0.220
N	4462	4462	4462	206

Panel G. Stellar				
	Stel_R	Stel_RV	Stel_V	Stel_AHJ
Mean	0.003	0.074	14.133	0.001
Median	-0.004	0.077	14.762	0.000
Std.	0.080	0.009	3.964	0.036
Min	-0.366	0.060	6.196	-0.112
25^{th}	-0.032	0.064	10.246	-0.021
75^{th}	0.028	0.083	17.946	0.027
Max	0.674	0.087	21.138	0.092
N	4462	4462	4462	337

Panel H: Countries and market indices	
Country	**Market indices**
Australia	S&P/ASX 200 INDEX
Greece	Athex Composite Share Pr
Barbados	Barbados Exchange Comp
Belgium	BEL 20 INDEX
Romania	BUCHAREST BET INDEX
Bahrain	BB ALL SHARE INDEX
Bosnia and Herzegovina	Bosnia BIRS Index
Lebanon	BLOM STOCK INDEX
Iran, Islamic Republic of	TEHRAN STOCK EXCHANGE
Hungary	BUDAPEST STOCK EXCH INDX
Panama	Bolsa de Panama General
Colombia	COLOMBIA COLCAP INDEX
Costa Rica	BCT Corp Costa Rica Index
Sri Lanka	SRI LANKA COLOMBO ALL SH
Cambodia	Cambodia SE Comp Index
Cuba	CUBOPP Index
Cyprus	GENERAL MARKET INDEX CSE
Tanzania, United Republic of	Tanzania Share Index
United Arab Emirates	DFM GENERAL INDEX
Bangladesh	DSE Broad Index
Syrian Arab Republic (Syria)	DSE Weighted Index
Ecuador	ECUINDEX
Egypt	EGX 30 INDEX
Malaysia	FTSE BURSA MAL TOP 100
Kenya	FTSE NSE Kenya 25
Namibia	NAMIBIA OVERALL INDEX
Italy	FTSE MIB INDEX
Spain	IBEX 35 INDEX
Iceland	OMX Iceland All-Share PR
Russian Federation	MOEX Russia Index
Chile	S&P/CLX IPSA (CLP) TR
Iraq	ISX GENERAL INDEX
South Africa	FTSE/JSE AFRICA ALL SHR
Indonesia	JAKARTA COMPOSITE INDEX
Jordan	AMMAN SE GENERAL INDEX

Pakistan	KARACHI 100 INDEX
Kuwait	KWSE All Share
Malta	MALTA STOCK EXCHANGE IND
Maldives	Maldives Stock Exch Indx
Macedonia	MBI 10 Index
Argentina	S&P MERVAL TR ARS
Morocco	MASI Free Float Index
Mongolia	MSE Top 20 Index
Oman	MSM30 Index
Nigeria	NIGERIA STCK EXC ALL SHR
New Zealand	S&P NZX All Index
Philippines	PSEi - PHILIPPINE SE IDX
Palestinian Territory	PEX Genral Index
Puerto Rico	GDB PUERTO RICO STOCK IX
Portugal	PSI 20 INDEX
Rwanda	Rwanda St Ex Share Index
Slovakia	SLOVAK SHARE INDEX
Switzerland	SWISS MARKET INDEX
Fiji	SPSE Market Cap Wgt TR
European Union	Euro Stoxx 50 Pr
Estonia	OMX TALLINN OMXT
Trinidad and Tobago	TRINIDAD&TOBAGO CMPOSITE
Tunisia	Tunis SE TUNINDEX
Uganda	USE LSI Index
British Virgin Islands	FTSE 100 INDEX
Lithuania	OMX VILNIUS OMXV
Vietnam	HO CHI MINH STOCK INDEX
Zimbabwe	Zimbabwe All Share Index
Austria	AUSTRIAN TRADED ATX INDX
Australia	S&P/ASX 200 INDEX
Brazil	BRAZIL IBOVESPA INDEX
Canada	S&P/TSX COMPOSITE INDEX
China	CSI 300 INDEX
Czech Republic	PRAGUE STOCK EXCH INDEX
Germany	DAX INDEX
Denmark	OMX COPENHAGEN 20 INDEX
Finland	OMX HELSINKI 25 INDEX
France	CAC 40 INDEX
Hong Kong, SAR China	HANG SENG INDEX
Ireland	IRISH OVERALL INDEX
Israel	TA-125 Index
India	S&P BSE SENSEX INDEX
Italy	FTSE MIB INDEX
Japan	NIKKEI 225
Korea (South)	KOSPI INDEX
Kazakhstan	Kazakhstan KASE Stock Ex
Luxembourg	LUXEMBOURG LuxX INDEX
Montenegro	MONEX INDEX
Mexico	S&P/BMV IPC
Netherlands	AEX-Index
Norway	OBX STOCK INDEX

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
Thailand	STOCK EXCH OF THAI INDEX
Turkey	BIST 100 INDEX
Taiwan, Republic of China	TAIWAN TAIEX INDEX
Ukraine	PFTS Index
United Kingdom	FTSE 100 INDEX
United States of America	DOW JONES INDUS. AVG
Venezuela (Bolivarian Republic)	VENEZUELA STOCK MKT INDX

Table 2. Effects of cyber-attacks on cryptocurrency's return

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 chain's hash rates (Hash) while controlling 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.

	Cryptocurrency's return				
	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	0.013	0.012
	(0.509)	(-0.758)	(0.132)	(0.172)	(0.145)
Ind	0.02	-0.053	0.009	0.012	0.001
	(0.514)	(-0.731)	(0.151)	(0.162)	(0.007)
Fin	-0.01	-0.0005	-0.016	-0.01	-0.011
	(-0.895)	(-0.022)	(-0.927)	(-0.496)	(-0.462)
Crypto	0.01	-0.044	0.015	0.017	0.024
	(0.267)	(-0.618)	(0.241)	(0.228)	(0.298)
CC	0.001	0.005	0.005	0.009	-0.0003
	(0.323)	(0.622)	(0.822)	(1.2)	(-0.041)
CE	0.003	0.003	0.005	0.012	0.003
	(0.568)	(0.322)	(0.653)	(1.477)	(0.271)
H	0.001	**0.015***	0.009	0.009	-0.006
	(0.251)	**(1.681)**	(1.24)	(1.137)	(-0.64)
Liq	0.087	**0.591***	0.239	-0.216	-0.117
	(0.65)	**(1.932)**	(1.131)	(-0.864)	(-0.421)
US	0.002	**0.007****	**0.004****	0.0004	**0.0049***
	(1.609)	**(2.546)**	**(1.966)**	(0.156)	**(1.687)**
Hash	**-0.002*****	**-0.003*****	**-0.004*****	-0.001	-0.001
	(-3.421)	**(-3.116)**	**(-3.689)**	(-1.271)	(-1.088)
RV	**-1.783*****	**-0.704*****	**-1.842*****	**-0.89*****	-0.26
	(-5.131)	**(-33.865)**	**(-5.034)**	**(-3.537)**	(-1.294)
EPU	**-0.00004****	0.00003	-0.00001	**0.00008*****	**0.00008****

	(-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-attacks on cryptocurrency's realized volatility

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 block chain's hash rates (Hash) while controlling 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.

	Cryptocurrency's realized volatility				
	Bit_RV	Eth_RV	Lit_RV	XRP_RV	Stel_RV
	(1)	(2)	(3)	(4)	(5)
Intercept	**0.047*****	0.025	**0.07*****	**0.076*****	**0.072*****
	(24.28)	(0.462)	**(24.357)**	**(15.188)**	**(10.253)**
Gov	-0.001	-0.023	-0.001	-0.005	-0.008
	(-0.612)	(-0.423)	(-0.298)	(-1.061)	(-1.057)
Ind	-0.001	-0.021	-0.0003	-0.005	-0.008
	(-0.503)	(-0.386)	(-0.116)	(-0.987)	(-1.063)
Fin	-0.001	-0.006	-0.001	-0.002	-0.003
	(-1.319)	(-0.347)	(-0.882)	(-1.458)	(-1.56)
Crypto	-0.001	-0.024	-0.001	-0.005	-0.006
	(-0.703)	(-0.43)	(-0.219)	(-0.901)	(-0.898)
CC	0.0001	0.0027	-0.00003	0.0001	0.0006
	(0.583)	(0.471)	(-0.084)	(0.26)	(0.803)
CE	0.00007	-0.00068	-0.00007	0.00012	0.00055
	(0.29)	(-0.105)	(-0.207)	(0.212)	(0.666)
H	**0.001*****	0.007	**0.001****	**0.001****	**0.002****
	(2.714)	(1.085)	**(2.483)**	**(2.281)**	**(2.416)**
Liq	**0.066*****	0.36	**0.12*****	**0.141*****	**0.126*****
	(9.888)	(1.544)	**(12.047)**	**(8.172)**	**(5.191)**
US	0.00001	-0.0005	0.00005	-0.00002	-0.00016
	(0.189)	(-0.237)	(0.464)	(-0.113)	(-0.611)
Hash	**-0.001*****	**-0.003*****	**-0.002*****	0.00009	**0.00263*****
	(-31.646)	**(-4.124)**	**(-41.914)**	(1.356)	**(29.353)**
R	**-0.005*****	**-0.408*****	**-0.004*****	**-0.004*****	-0.002
	(-5.131)	**(-33.865)**	**(-5.034)**	**(-3.537)**	(-1.294)
EPU	**-0.00001*****	0.00002	**-0.000005*****	**0.00001*****	**0.00003*****

	(-11.559)	(0.941)	**(-4.05)**	**(5.718)**	**(11.704)**
RGDP	**-0.00003***** **(-2.758)**	0.00015 (0.563)	**-0.00003*** **(-1.948)**	**-0.00005**** **(-1.992)**	**-0.00009***** **(-2.663)**
F-statistics	**125.7*****	**44.36*****	**147.9*****	**16.05*****	**82.08*****
Adjusted R^2	0.52	0.30	0.56	0.11	0.41
N	3260	2873	3260	3260	3260

Table 4. Effects of cyber-attacks on cryptocurrency's trading volume

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 (US) and block chain's hash rates (Hash) while controlling 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.

	Cryptocurrency's trading volume				
	Bit_V	Eth_V	Lit_V	XRP_V	Stel_V
	(1)	(2)	(3)	(4)	(5)
Intercept	**14.647*****	**16.45*****	**5.525*****	**3.305*****	**5.715*****
	(22.735)	**(18.079)**	**(5.042)**	**(3.499)**	**(5.265)**
Gov	-0.746	-0.502	**-1.719***	-0.81	-1.311
	(-1.239)	(-0.543)	**(-1.68)**	(-0.873)	(-1.208)
Ind	-0.66	-0.463	-1.663	-0.846	-1.42
	(-1.1)	(-0.503)	(-1.63)	(-0.915)	(-1.312)
Fin	-0.272	-0.135	-0.421	0.244	-0.067
	(-1.581)	(-0.491)	(-1.438)	(0.92)	(-0.215)
Crypto	-0.441	0.006	-1.159	-0.614	-1.225
	(-0.738)	(0.007)	(-1.142)	(-0.667)	(-1.138)
CC	-0.024	-0.061	0.094	-0.056	0.063
	(-0.384)	(-0.628)	(0.895)	(-0.587)	(0.563)
CE	-0.037	-0.069	0.089	-0.103	0.052
	(-0.528)	(-0.638)	(0.761)	(-0.966)	(0.413)
H	-0.032	-0.105	0.06	**-0.184***	-0.033
	(-0.465)	(-0.945)	(0.51)	**(-1.739)**	(-0.269)
Liq	**-5.39*****	**-12.34*****	**-17.28*****	**-13.5*****	**-10.21****
	(-2.599)	**(-3.18)**	**(-4.867)**	**(-4.245)**	**(-2.76)**
US	0.001	-0.002	-0.023	0.04	0.017
	(0.032)	(-0.052)	(-0.629)	(1.201)	(0.44)
Hash	**1.097*****	**1.519*****	**1.273*****	**1.377*****	**1.508*****
	(126.552)	**(119.039)**	**(79.589)**	**(118.044)**	**(98.135)**
R	0.177	**1.758*****	**1.628*****	**3.331*****	**3.585*****
	(0.653)	**(7.397)**	**(5.515)**	**(14.904)**	**(15.261)**
RV	**95.139*****	**1.661*****	**156.3*****	**155.4*****	**108.4*****

	(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-attacks on cryptocurrency's return between US and non-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) and block chain's hash rates (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.

Panel A. Cryptocurrency's return in US					
	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)
Gov	0.013	-0.068	-0.017	-0.008	-0.001
	(0.336)	(-0.989)	(-0.275)	(-0.112)	(-0.013)
Ind	0.017	-0.071	-0.002	-0.004	-0.004
	(0.439)	(-1.039)	(-0.032)	(-0.062)	(-0.048)
Fin	-0.003	0.01	-0.011	-0.012	-0.002
	(-0.248)	(0.507)	(-0.579)	(-0.551)	(-0.096)
Crypto	0.005	-0.054	-0.009	-0.013	-0.009
	(0.119)	(-0.822)	(-0.146)	(-0.19)	(-0.113)
CC	0.004	-0.005	0.002	0.01	**-0.026***
	(0.481)	(-0.339)	(0.154)	(0.72)	**(-1.734)**
CE	0.006	-0.002	0.005	**0.026***	-0.006
	(0.772)	(-0.101)	(0.405)	**(1.743)**	(-0.341)
H	0.003	0.013	0.003	0.005	**-0.038****
	(0.401)	(0.819)	(0.257)	(0.324)	**(-2.256)**
Liq	-0.016	-0.535	0.445	-0.205	**-2.344*****
	(-0.041)	(-0.75)	(0.67)	(-0.283)	**(-2.847)**
Hash	0.001	0.002	-0.003	0.001	**-0.003***
	(0.442)	(1.417)	(-1.44)	(0.865)	**(-1.853)**
RV	0.631	**1.891*****	-1.03	-0.053	0.354
	(0.724)	**(13.5)**	(-1.176)	(-0.119)	(1.007)
EPU	0.000001	0.00005	0.00002	0.00005	**0.0001****
	(0.066)	(1.218)	(0.553)	(1.248)	**(2.227)**

RGDP	**0.008****	**0.013*****	0.005	**0.016*****	0.002
	(2.241)	**(3.169)**	(1.02)	**(3.286)**	(0.323)
Crypto × Hash	-0.002	-0.013	-0.007	-0.005	-0.002
	(-0.392)	(-1.586)	(-1.185)	(-0.736)	(-0.309)
F-statistics	**2.04*****	**9.45*****	**2.09*****	**2.64*****	**2.99*****
Adjusted R^2	0.02	0.13	0.02	0.02	0.03
N	1720	1526	1720	1720	1720

Panel B. Cryptocurrency's return in non-US

	Bit_R	Eth_R	Lit_R	XRP_R	Stel_R
	(1)	(2)	(3)	(4)	(5)
Intercept	**0.12*****	0.009	**0.129*****	0.02	0.022
	(4.989)	(0.723)	**(3.522)**	(0.659)	(0.887)
Gov	0.003	-0.004	**0.012****	-0.006	**0.013***
	(0.928)	(-0.542)	**(2.216)**	(-0.904)	**(1.701)**
Ind	0.001	-0.001	0.005	**-0.01***	-0.005
	(0.263)	(-0.231)	(1.008)	**(-1.702)**	(-0.694)
Fin	**-0.07***	-0.014	-0.065	-0.041	-0.069
	(-1.828)	(-1.289)	(-1.121)	(-0.561)	(-0.857)
Crypto	-0.009	0.001	0.012	-0.002	**0.037****
	(-1.364)	(0.045)	(1.165)	(-0.178)	**(2.539)**
CC	-0.0004	0.006	0.007	0.009	0.009
	(-0.08)	(0.632)	(0.902)	(0.996)	(0.852)
CE	0.00005	0.003	0.004	0.007	0.003
	(0.01)	(0.324)	(0.493)	(0.681)	(0.252)
H	-0.001	0.013	0.01	0.012	0.004
	(-0.269)	(1.328)	(1.197)	(1.175)	(0.38)
Liq	0.081	**0.955*****	0.183	-0.137	0.161
	(0.562)	**(2.82)**	(0.837)	(-0.49)	(0.535)
Hash	**-0.002*****	**-0.003***	**-0.003***	-0.002	0.001
	(-2.851)	**(-1.899)**	**(-1.904)**	(-1.489)	(0.364)
RV	**-2.557*****	**-0.752*****	**-1.992*****	**-0.685***	**-0.57***
	(-5.065)	**(-36.857)**	**(-3.941)**	**(-1.805)**	**(-1.92)**
EPU	**-0.00007*****	-0.00004	-0.00004	**0.00008***	0.00001
	(-3.276)	(-1.009)	(-1.315)	**(1.868)**	(0.246)

RGDP	-0.000007 (-0.039)	0.001 (1.566)	-0.0002 (-0.719)	-0.0003 (-0.933)	-0.0004 (-1.017)
Crypto × Hash	0.007 (1.556)	**0.019**** **(2.172)**	0.008 (1.202)	**0.018**** **(2.108)**	0.003 (0.297)
F-statistics	**2.80*****	**61.11*****	**2.10*****	**2.51*****	**2.01*****
Adjusted R^2	0.03	0.52	0.02	0.02	0.02
N	1540	1347	1540	1540	1540

Table 6. Effects of cyber-attacks on cryptocurrency's realized volatility between US and non-US countries

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) and block chain's hash rates (Hash) while controlling 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). We show these for US (Panel A) and non-US (Panel B) countries. The t-statistics are in the brackets***, ** and * denote significance at 1, 5 and 10% levels, respectively.

Panel A. Cryptocurrency's realized volatility in US					
	Bit_RV	Eth_RV	Lit_RV	XRP_RV	Stel_RV
	(1)	(2)	(3)	(4)	(5)
Intercept	**0.053*****	0.0003	**0.078*****	**0.088*****	**0.09*****
	(47.844)	(0.024)	**(43.483)**	**(22.532)**	**(15.805)**
Gov	-0.001	0.001	-0.0001	-0.004	-0.006
	(-0.599)	(0.11)	(-0.08)	(-1.126)	(-1.014)
Ind	-0.001	0.004	0.0004	-0.004	-0.006
	(-0.528)	(0.308)	(0.228)	(-1.051)	(-1.058)
Fin	-0.001	-0.004	-0.0004	**-0.002***	**-0.003***
	(-1.549)	(-1.218)	(-0.747)	**(-1.807)**	**(-1.932)**
Crypto	-0.0001	0.002	0.001	-0.002	-0.003
	(-0.092)	(0.14)	(0.507)	(-0.535)	(-0.466)
CC	0.00008	0.002	-0.0001	-0.0001	0.0005
	(0.415)	(0.695)	(-0.317)	(-0.199)	(0.432)
CE	0.00005	0.001	0.00006	0.0005	0.001
	(0.217)	(0.346)	(0.175)	(0.582)	(0.953)
H	**0.001****	-0.0001	**0.0007****	0.0012	0.002
	(2.207)	(-0.054)	**(1.975)**	(1.46)	(1.513)
Liq	**0.046*****	**0.27****	**0.191*****	**0.149*****	-0.078
	(4.131)	**(2.182)**	**(10.717)**	**(3.818)**	(-1.37)
Hash	**-0.001*****	**-0.001*****	**-0.002*****	**-0.001*****	**0.002*****
	(-55.019)	**(-5.538)**	**(-62.255)**	**(-7.439)**	**(18.648)**
R	0.0005	**0.057*****	-0.001	-0.0002	0.002
	(0.724)	**(13.5)**	(-1.176)	(-0.119)	(1.007)
EPU	**-0.000005*****	0.00001	**0.000002****	**0.00002*****	**0.00004*****
	(-7.642)	(1.642)	**(2.474)**	**(10.37)**	**(14.504)**

RGDP	**-0.003*****	**-0.002*****	**-0.004*****	**-0.007*****	**-0.009*****
	(-55.724)	**(-2.695)**	**(-45.765)**	**(-31.81)**	**(-31.252)**
Crypto × Hash	-0.000009	0.002	0.000002	-0.00007	-0.00002
	(-0.085)	(1.504)	(0.014)	(-0.177)	(-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

Panel B. Cryptocurrency's realized volatility in non-US					
	Bit_RV	Eth_RV	Lit_RV	XRP_RV	Stel_RV
	(1)	(2)	(3)	(4)	(5)
Intercept	**0.046*****	0.008	**0.069*****	**0.072*****	**0.066*****
	(129.84)	(0.622)	**(129.933)**	**(78.554)**	**(52.187)**
Gov	0.0002	-0.001	0.0001	-0.001	-0.001
	(1.067)	(-0.121)	(0.377)	(-1.067)	(-1.203)
Ind	**0.0003***	0.005	0.0003	-0.001	**-0.001****
	(1.835)	(0.843)	(1.055)	(-1.258)	**(-2.197)**
Fin	0.003	-0.014	0.003	**0.01****	**0.016****
	(1.544)	(-1.307)	(1.102)	**(1.998)**	**(2.258)**
Crypto	-0.0005	-0.002	-0.0002	-0.001	-0.001
	(-1.29)	(-0.124)	(-0.356)	(-0.718)	(-0.615)
CC	0.0001	0.004	0.00004	0.0002	0.001
	(0.382)	(0.535)	(0.109)	(0.335)	(0.621)
CE	-0.0003	0.001	-0.001	-0.001	-0.001
	(-1.054)	(0.151)	(-1.5)	(-1.159)	(-0.698)
H	0.0004	0.01	0.001	0.001	0.001
	(1.393)	(1.053)	(1.346)	(1.202)	(1.352)
Liq	**0.026*****	**0.574***	**0.05*****	**0.051*****	0.03
	(3.597)	**(1.786)**	**(4.562)**	**(2.686)**	(1.155)
Hash	**-0.001*****	**-0.004*****	**-0.002*****	-0.00002	**0.002*****
	(-22.729)	**(-2.99)**	**(-29.39)**	(-0.181)	**(19.162)**
R	**-0.007*****	**-0.674*****	**-0.005*****	**-0.003***	**-0.004***
	(-5.065)	**(-36.857)**	**(-3.941)**	**(-1.805)**	**(-1.92)**
EPU	**-0.000008*****	-0.00002	**-0.000004****	**0.00001*****	**0.00003*****
	(-7.198)	(-0.568)	**(-2.124)**	**(4.171)**	**(8.483)**

RGDP	0.000005	0.0003	0.00001	0.00001	-0.000003
	(0.485)	(0.852)	(0.947)	(0.596)	(-0.086)
Crypto × Hash	**0.001*****	**0.015***	**0.0008****	**0.001****	**0.002*****
	(3.192)	**(1.819)**	**(2.387)**	**(2.542)**	**(2.652)**
F-statistics	**71.22*****	**61.44*****	**80.46*****	**9.50*****	**45.74*****
Adjusted R^2	0.53	0.52	0.56	0.12	0.42
N	1540	1347	1540	1540	1540

Table 7. Effects of cyber-attacks on cryptocurrency's trading volume between US and non-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-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H) and block chain's hash rates (Hash) while controlling 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). We show these for US (Panel A) and non-US (Panel B) countries. The t-statistics are in the brackets. ***, ** and * denote significance at 1, 5 and 10% levels, respectively.

Panel A. Cryptocurrency's trading volume in US					
	Bit_V	Eth_V	Lit_V	XRP_V	Stel_V
	(1)	(2)	(3)	(4)	(5)
Intercept	**10.28*****	**14.088*****	**-8.674*****	**-2.46****	0.122
	(11.005)	**(16.55)**	**(-6.137)**	**(-2.423)**	(0.11)
Gov	-0.636	-0.168	**-1.62***	-0.394	-1.069
	(-1.06)	(-0.201)	**(-1.691)**	(-0.449)	(-1.048)
Ind	-0.568	-0.258	**-1.73***	-0.496	-1.16
	(-0.953)	(-0.312)	**(-1.82)**	(-0.569)	(-1.146)
Fin	-0.295	-0.05	**-0.504***	0.292	-0.108
	(-1.643)	(-0.201)	**(-1.759)**	(1.111)	(-0.354)
Crypto	-0.458	0.049	-1.449	-0.726	-1.463
	(-0.782)	(0.061)	(-1.549)	(-0.846)	(-1.468)
CC	0.071	-0.257	0.103	-0.019	0.138
	(0.632)	(-1.591)	(0.575)	(-0.119)	(0.726)
CE	0.084	-0.291	0.217	-0.025	0.259
	(0.666)	(-1.597)	(1.083)	(-0.138)	(1.214)
H	0.082	-0.193	0.023	-0.158	0.064
	(0.647)	(-1.031)	(0.113)	(-0.855)	(0.3)
Liq	-8.731	**23.737*****	**-60.38*****	**-21.33****	5.194
	(-1.429)	**(2.748)**	**(-6.021)**	**(-2.387)**	(0.501)
Hash	**1.194*****	**1.665*****	**1.655*****	**1.442*****	**1.497*****
	(66.74)	**(94.905)**	**(53.357)**	**(90.507)**	**(74.852)**
R	0.475	-0.124	**1.922*****	**3.147*****	**3.289*****
	(1.282)	(-0.397)	**(5.233)**	**(10.512)**	**(10.783)**
RV	**166.7*****	**24.217*****	**327*****	**206.1*****	**149.691*****
	(12.561)	**(13.468)**	**(24.693)**	**(37.207)**	**(33.915)**

EPU	**0.011*****	**0.012*****	**0.013*****	**0.013*****	**0.009*****
	(33.861)	**(26.627)**	**(25.688)**	**(27.119)**	**(16.164)**
RGDP	**0.351*****	**0.819*****	**1.124*****	**0.773*****	**1.04*****
	(6.55)	**(16.16)**	**(14.798)**	**(13.105)**	**(15.366)**
Crypto × Hash	0.042	-0.111	0.033	0.092	0.041
	(0.713)	(-1.087)	(0.349)	(1.079)	(0.416)
F-statistics	**881.3*****	**711.9*****	**438.5*****	**852.5*****	**937.5*****
Adjusted R^2	0.93	0.93	0.87	0.93	0.94
N	1720	1526	1720	1720	1720

Panel B. Cryptocurrency's trading volume in non-US					
	Bit_V	Eth_V	Lit_V	XRP_V	Stel_V
	(1)	(2)	(3)	(4)	(5)
Intercept	**14.195*****	**16.209*****	**4.83*****	**2.77*****	**4.514*****
	(37.765)	**(96.094)**	**(7.507)**	**(7.28)**	**13.819)**
Gov	**-0.271*****	**-0.267*****	**-0.606*****	**-0.21****	-0.115
	(-4.742)	**(-2.67)**	**(-6.182)**	**(-2.345)**	(-1.112)
Ind	**-0.144*****	-0.1	**-0.449*****	**-0.155****	**-0.145***
	(-2.994)	(-1.181)	**(-5.471)**	**(-2.068)**	**1.665)**
Fin	0.366	-0.106	0.857	0.088	0.765
	(0.62)	(-0.727)	(0.85)	(0.096)	0.717)
Crypto	0.141	**0.356****	0.158	**0.304***	0.244
	(1.323)	**(2.072)**	(0.862)	**(1.82)**	(1.257)
CC	-0.081	-0.025	0.063	-0.077	0.038
	(-1.088)	(-0.218)	(0.493)	(-0.661)	(0.28)
CE	-0.073	0.057	0.055	-0.087	0.032
	(-0.88)	(0.444)	(0.388)	(-0.672)	(0.212)
H	-0.098	-0.068	0.023	-0.196	-0.06
	(-1.197)	(-0.515)	(0.162)	(-1.532)	(-0.403)
Liq	**-4.698****	-6.529	**-11.58*****	**-8.273****	-4.748
	(-2.11)	(-1.458)	**(-3.034)**	**(-2.382)**	(-1.183)
Hash	**1.092*****	**1.529*****	**1.266*****	**1.388*****	**1.498*****
	(85.007)	**(81.321)**	**(53.263)**	**(80.033)**	**(66.986)**
R	-0.239	**1.639*****	**1.188*****	**3.156*****	**3.717*****
	(-0.603)	**(4.52)**	**(2.647)**	**(9.855)**	**(10.839)**

RV	**97.762*****	**1.182*****	**152.6*****	**156.3*****	**112.4*****
	(12.429)	**(3.086)**	**(17.196)**	**(33.036)**	**(28.351)**
EPU	**0.01*****	**0.012*****	**0.013*****	**0.014*****	**0.011*****
	(29.881)	**(22.453)**	**(21.407)**	**(25.486)**	**(16.775)**
RGDP	0.0001	-0.001	-0.006	-0.002	-0.006
	(0.048)	(-0.149)	(-1.196)	(-0.369)	(-1.143)
Crypto × Hash	-0.043	**-0.216***	-0.118	**-0.178***	-0.181
	(-0.626)	**(-1.888)**	(-1.004)	**(-1.651)**	(-1.452)
F-statistics	**820.9*****	**582.4*****	**337.5*****	**697.6*****	**756.4*****
Adjusted R^2	0.93	0.92	0.85	0.92	0.93
N	1540	1347	1540	1540	1540

Table 8. Cryptocurrency exchange targeted by cyber-attacks

The following table presents the logistic regression results to show the determinants affecting cyber-attacks targeting cryptocurrency exchange (Crypto) which we use as our binary dependent variable. We use the independent variables including other cyber-attack targets (Gov, Ind, Fin), types (CC, CW, H), countries (US) and block chain's hash rates (Hash) while controlling for economic uncertainty (EPU), and country specific stock market liquidity (Liq) and real gross domestic product (RGDP). We report the χ^2, Pseudo R^2 and number of observations (N). The t-statistics are in the brackets. ***, ** and * denote significance at 1, 5 and 10% levels, respectively.

Cyber-attack targeting cryptocurrency exchange					
	Crypto(Bit)	Crypto (Eth)	Crypto (Lit)	Crypto (XRP)	Crypto (Stel)
	(1)	(2)	(3)	(4)	(5)
Intercept	-5.903	-6.344	-8.062	-5.967	-4.567
	(-1.011)	(-1.618)	(-1.214)	(-1.582)	(-1.249)
Gov	-15.97	-16.29	-15.98	-15.98	-16
	(-0.016)	(-0.014)	(-0.016)	(-0.016)	(-0.016)
Ind	**-2.626****	**-2.287****	**-2.651*****	**-2.638****	**-2.628****
	(-2.558)	**(-2.21)**	**(-2.582)**	**(-2.572)**	**(-2.562)**
Fin	-16.51	-16.41	-16.51	-16.49	-16.52
	(-0.008)	(-0.008)	(-0.008)	(-0.008)	(-0.009)
CC	1.292	1.254	1.306	1.312	1.295
	(1.263)	(1.226)	(1.278)	(1.283)	(1.267)
CE	-15.72	-15.82	-15.69	-15.69	-15.7
	(-0.016)	(-0.015)	(-0.016)	(-0.016)	(-0.016)
H	-15.36	-15.62	-15.37	-15.35	-15.36
	(-0.017)	(-0.015)	(-0.017)	(-0.017)	(-0.017)
Liq	4.357	28.71	3.991	3.563	3.845
	(0.215)	(0.836)	(0.192)	(0.174)	(0.198)
US	**-0.408***	**-0.516****	**-0.422***	**-0.416***	**-0.43***
	(-1.657)	**(-2.007)**	**(-1.712)**	**(-1.692)**	**(-1.747)**
R	-4.066	2.641	0.99	-0.043	1.63
	(-1.482)	(1.166)	(0.52)	(-0.032)	(1.429)
RV	12.82	-6.124	23.81	16.24	13.89
	(0.188)	(-0.402)	(0.51)	(0.568)	(0.683)
Hash	0.01	0.027	0.036	-0.003	-0.031
	(0.106)	(0.288)	(0.356)	(-0.038)	(-0.296)
EPU	**0.004***	**0.005****	**0.004***	**0.004***	0.003

	(1.783)	**(2.132)**	**(1.889)**	**(1.719)**	(1.371)
RGDP	-0.007	0.007	-0.004	-0.006	-0.003
	(-0.121)	(0.149)	(-0.075)	(-0.096)	(-0.052)
χ^2	**81.36*****	**70.99*****	**79.61*****	**79.45*****	**81.44*****
Pseudo R^2	0.12	0.11	0.12	0.12	0.12
N	1720	1526	1720	1720	1720

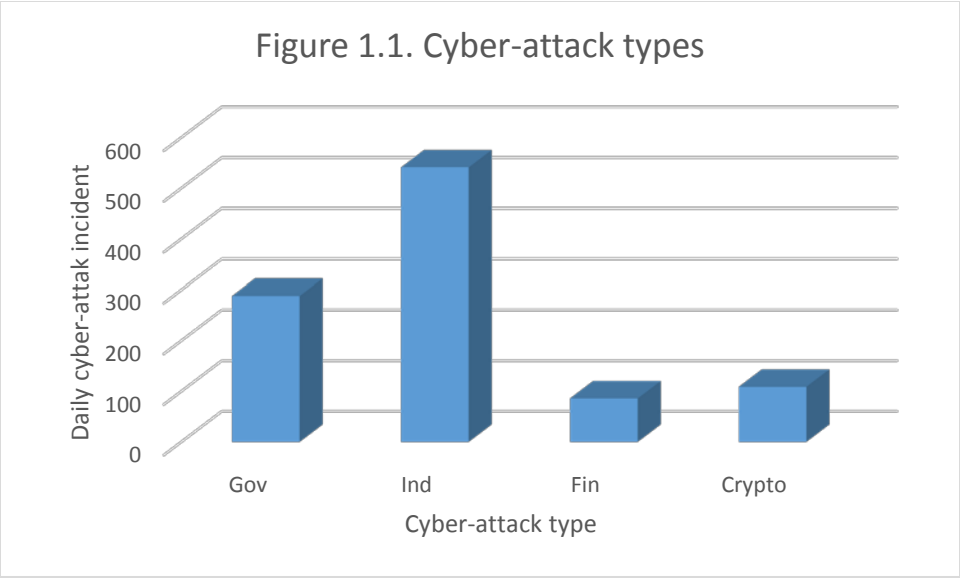
Table 9. Effects of cyber-attacks on cryptocurrency's average hourly jumps

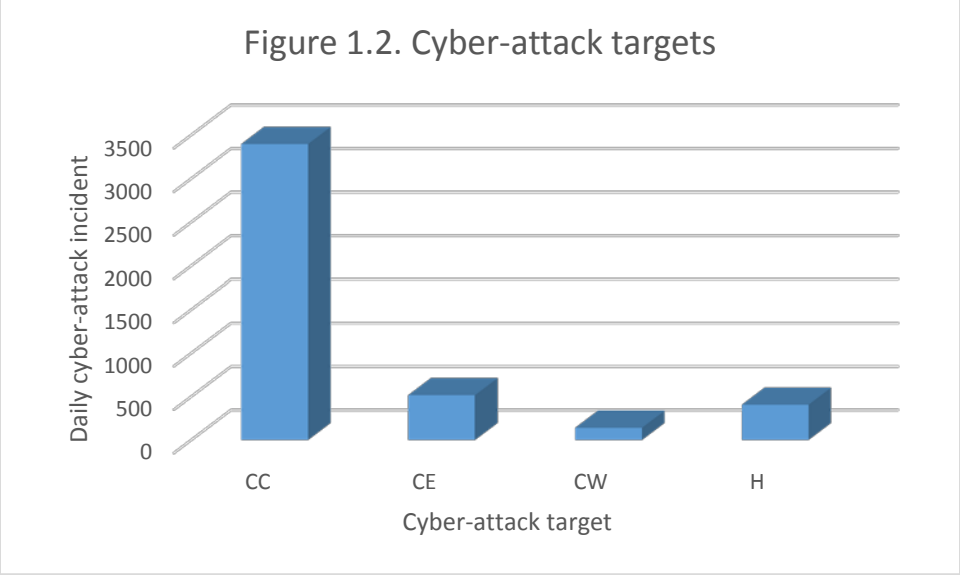
The following tables present the ordinary least squares (OLS) regression results using the cryptocurrency's average hourly jumps. We use cryptocurrency's average hourly jumps per day (Bit_AHJ, Eth_AHJ, Lit_AHJ, XRP_AHJ, Stel_AHJ) as for our dependent variable. We analyze how these are affected by cyber-attack targets (Gov, Ind, Fin, Crypto), types (CC, CW, H), countries (US) and block chain's hash rates (Hash) while controlling 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.

	Cryptocurrency's average hourly jump				
	Bit_AHJ	Eth_AHJ	Lit_AHJ	XRP_AHJ	Stel_AHJ
	(1)	(2)	(3)	(4)	(5)
Intercept	**0.05****	**0.327****	**1.621****	**-3.043**	**-0.477*****
	(2.248)	**(5.189)**	**(5.374)**	**(-0.734)**	**(-4.743)**
Crypto	**-0.034****	-0.007	**0.583***	-0.033	**-0.183****
	(-2.007)	(-0.192)	**(1.835)**	(-0.876)	**(-2.306)**
Liq	0.047	-3.179	1.273	-0.632	1.875
	(0.222)	(-1.443)	(0.55)	(-0.43)	(1.64)
US	0.001	-0.001	0.03	0.012	**-0.009***
	(0.286)	(-0.117)	(0.589)	(0.818)	**(-1.874)**
Hash	**0.01****	**0.063****	**0.335****	0.082	-0.014
	(2.545)	**(4.697)**	**(6.193)**	(1.166)	(-0.601)
EPU	**-0.0002****	**-0.001****	**-0.01****	0.01	**0.003*****
	(-2.27)	**(-6.807)**	**(-7.341)**	(0.721)	**(6.985)**
RGDP	-0.002	-0.002	-0.003	-0.002	-0.001
	(-1.135)	(-0.591)	(-0.183)	(-0.638)	(-0.898)
Crypto × US	0.037	-0.022	-0.052	0.021	-0.005
	(1.247)	(-0.503)	(-0.132)	(0.29)	(-0.228)
Crypto × Hash	-0.003	-0.018	0.22	-0.094	**0.082****
	(-0.369)	(-0.518)	(1.486)	(-1.213)	**(2.163)**
F-statistics	**3.419*****	**6.03*****	**4.15*****	**1.63***	**5.17*****
Adjusted R^2	0.15	0.43	0.19	0.09	0.25
N	347	160	315	135	213

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.

Panel A. Correlation matrix (with Bitcoin)

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)
Gov (a)	1[a]															
Ind (b)	-0.1[a]	1[a]														
Fin (c)	-0.04[a]	0.01	1[a]													
Crypto (d)	-0.04	-0.05[a]	-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[b]	-0.05[a]	-0.65[a]	1[a]										
CW (g)	0.08a	-0.04[b]	-0.02	-0.02	-0.32[a]	-0.07[a]	1[a]									
H (h)	0.25[a]	-0.02	0.05[a]	-0.05[a]	-0.57[a]	-0.11[a]	-0.06[a]	1[a]								
Bit_R (i)	0.02	0.02	-0.01	-0.03[b]	-0.01	0.01	-0.01	0	1[a]							
Bit_RV (j)	0.2[a]	0.29[a]	0.06[a]	-0.04[b]	-0.12[a]	-0.04[b]	-0.01	0.22[a]	-0.03[b]	1[a]						
Bit_V (k)	-0.28[a]	-0.38[a]	-0.14[a]	0.06[a]	0.14[a]	0.02	-0.02	-0.23[a]	-0.06[a]	-0.58[a]	1[a]					
Bit_AHJ (l)	0.05	0.02	0	-0.04	-0.07	0.08[c]	0.1[b]	-0.01	0.67[a]	0.13[a]	-0.03	1[a]				
Liq (m)	0.08[a]	0.02	0.01	-0.04[b]	-0.03[b]	0.01	-0.03[c]	0.05[a]	-0.01	0.17[a]	-0.05[a]	0.03	1[a]			
Hash (n)	-0.27[a]	-0.38[a]	-0.12[a]	0.05[a]	0.15[a]	0.02	-0.02	-0.23[a]	-0.05[a]	-0.63[a]	0.94[a]	0.02	-0.03[b]	1[a]		
EPU (o)	-0.19[a]	-0.27[a]	-0.1[a]	0.06[a]	0.06[a]	0.03[c]	0.02	-0.14[a]	-0.06[a]	-0.45[a]	0.62[a]	-0.07	-0.09[a]	0.46[a]	1[a]	
RGDP (p)	0.02	0.01	0	-0.01	-0.04[b]	0.02	0.04[b]	0.02	0	-0.01	-0.02	-0.07	-0.04[b]	0	0.02	1[a]

Panel B. Correlation matrix (with Ethereum)

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)
Gov (a)	1[a]															
Ind (b)	-0.1[a]	1[a]														
Fin (c)	-0.04[a]	0.01	1[a]													
Crypto (d)	-0.04[a]	-0.05[a]	-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]										
CW (g)	0.08[a]	-0.04[b]	-0.02	-0.02	-0.32[a]	-0.07[a]	1[a]									

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]							
Eth_RV (j)	0.03[b]	0.06[a]	-0.01	-0.01	-0.01	-0.01	0	0.03	-0.48[a]	1[a]						
Eth_V (k)	-0.28[a]	-0.39[a]	-0.15[a]	0.05[a]	0.11[a]	0.02[c]	-0.03[c]	-0.19[a]	0.02	-0.06[a]	1[a]					
Eth _AHJ (l)	0.04	-0.03	-0.03	-0.05	-0.01	0.1	0.03	-0.08	0.35[a]	-0.03	0.09	1[a]				
Liq (m)	0.08[a]	0.02	0.01	-0.04[b]	-0.03[b]	0.01[c]	-0.03[a]	0.05[a]	0.02	0.01	-0.09[a]	0.08	1[a]			
Hash (n)	-0.27[a]	-0.38[a]	-0.12[a]	0.05[a]	0.15[a]	0.02	-0.02[a]	-0.23[a]	-0.02	-0.08[a]	0.91[a]	0.25[a]	-0.03[b]	1[a]		
EPU (o)	-0.19[a]	-0.27[a]	-0.1[a]	0.06[a]	0.06[a]	0.03	0.02[a]	-0.14[a]	0.02	-0.03[c]	0.52[a]	-0.04	-0.09[a]	0.46[a]	1[a]	
RGDP (p)	0.02	0.01	0	-0.01	-0.04[b]	0.02[b]	0.04	0.02	0	0	-0.02	-0.04	-0.04[b]	0	0.02	1[a]

Panel C. Correlation matrix (with Litecoin)

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)
Gov (a)	1[a]															
Ind (b)	-0.1[a]	1[a]														
Fin (c)	-0.04[b]	0.01	1[a]													
Crypto (d)	-0.04[a]	-0.05[a]	-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[b]	-0.05[a]	-0.65[a]	1[a]										
CW (g)	0.08[a]	-0.04[b]	-0.02	-0.02	-0.32[a]	-0.07[a]	1[a]									
H (h)	0.25[a]	-0.02	0.05[a]	-0.05[a]	-0.57[a]	-0.11[a]	-0.06[a]	1[a]								
Lit_R (i)	0.01	0.01	-0.01	0	-0.01	0	-0.01	0.02	1[a]							
Lit_RV (j)	0.21[a]	0.3[a]	0.08[a]	-0.04[b]	-0.13[a]	-0.03[b]	0	0.23[a]	-0.03[b]	1[a]						
Lit_V (k)	-0.28[a]	-0.38[a]	-0.14[a]	0.05[a]	0.13[a]	0.02	-0.02	-0.21[a]	0.01	-0.54[a]	1[a]					
Lit_AHJ (l)	-0.02	0.05	-0.01	-0.01	0.03	0	-0.01	-0.02	0.06	-0.01	0.02	1[a]				
Liq (m)	0.08[a]	0.02	0.01	-0.04[b]	-0.03[b]	0.01	-0.03[c]	0.05[a]	0	0.17[a]	-0.05[a]	0.02	1[a]			
Hash (n)	-0.27[a]	-0.38[a]	-0.12[a]	0.05[a]	0.15[a]	0.02	-0.02	-0.23[a]	-0.03[b]	-0.71[a]	0.88[a]	0.01	-0.03[b]	1[a]		
EPU (o)	-0.19[a]	-0.27[a]	-0.1[a]	0.06[a]	0.06[a]	0.03[c]	0.02	-0.14[a]	-0.02	-0.39[a]	0.61[a]	-0.13[b]	-0.09[a]	0.46[a]	1[a]	
RGDP (p)	0.02	0.01	0	-0.01	-0.04[b]	0.02	0.04[b]	0.02	0	-0.02	-0.02	0	-0.04[b]	0[b]	0.02	1[a]

Panel D. Correlation matrix (with XRP)

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)
Gov (a)	1[a]															
Ind (b)	-0.1[a]	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]										
CW (g)	0.08[a]	-0.04[b]	-0.02	-0.02	-0.32[a]	-0.07[a]	1[a]									
H (h)	0.25[a]	-0.02	0.05[a]	-0.05[a]	-0.57[a]	-0.11[a]	-0.06[a]	1[a]								
XRP_R (i)	-0.01	-0.01	-0.02	0	0.01	-0.01	-0.01	0	1[a]							
XRP_RV (j)	-0.03[b]	-0.05[a]	-0.07[a]	0.01	-0.02	-0.01	-0.02	0.05[a]	-0.05[a]	1[a]						
XRP_V (k)	-0.27[a]	-0.37[a]	-0.14[a]	0.05[a]	0.14[a]	0.02	-0.02	-0.22[a]	0.07[a]	0.32[a]	1[a]					
XRP_AHJ (l)				-0.06	-0.08	0	0.06	0.1	0.49[a]	-0.04	0.01	1[a]				
Liq (m)	0.08[a]	0.02	0.01	-0.04[b]	-0.03[b]	0.01	-0.03[c]	0.05[a]	-0.03[b]	0.12[a]	-0.05[a]	0.02	1[a]			
Hash (n)	-0.27[a]	-0.38[a]	-0.12[a]	0.05[a]	0.15[a]	0.02	-0.02	-0.23[a]	0	0.09[a]	0.9[a]	0.13[c]	-0.03[b]	1[a]		
EPU (o)	-0.19[a]	-0.27[a]	-0.1[a]	0.06[a]	0.06[a]	0.03[c]	0.02	-0.14[a]	0.03[b]	0.1[a]	0.62[a]	-0.12[c]	-0.09[a]	0.46[a]	1[a]	
RGDP (p)	0.02	0.01	0	-0.01[b]	-0.04[b]	0.02	0.04[b]	0.02	0	-0.03[c]	-0.02	-0.05	-0.04[b]	0	0.02	1[a]

Panel E. Correlation matrix (with Stellar)

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)
Gov (a)	1[a]															
Ind (b)	-0.1[a]	1[a]														
Fin (c)	-0.04[b]	0.01	1[a]													
Crypto (d)	-0.04[a]	-0.05[a]	-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[b]	-0.05[a]	-0.65[a]	1[a]										
CW (g)	0.08[a]	-0.04[b]	-0.02	-0.02	-0.32[a]	-0.07[a]	1[a]									
H (h)	0.25[a]	-0.02	0.05[a]	-0.05[a]	-0.57[a]	-0.11[a]	-0.06[a]	1[a]								
Stel_R (i)	0.02	-0.01	0.01	0.01	-0.01	0.02	0	-0.01	1[a]							
Stel_RV (j)	-0.18[a]	-0.27[a]	-0.14[a]	0.04[b]	0.07[a]	0.02	-0.03[b]	-0.11[a]	-0.03[c]	1[a]						
Stel_V (k)	-0.26[a]	-0.38[a]	-0.15[a]	0.05[a]	0.14[a]	0.03[b]	-0.02	-0.22[a]	0.05[a]	0.75[a]	1[a]					
Stel_AHJ (l)				0.03	-0.01	0.02	0.01	-0.02	0.66[a]	-0.08	-0.05	1[a]				
Liq (m)	0.08[a]	0.02	0.01	-0.04[b]	-0.03[b]	0.01	-0.03[c]	0.05[a]	-0.02	0.03[c]	-0.04[a]	0.06	1[a]			
Hash (n)	-0.27[a]	-0.38[a]	-0.12[a]	0.05[a]	0.15[a]	0.02	-0.02	-0.23[a]	-0.02	0.63[a]	0.92[a]	0.07	-0.03[b]	1[a]		
EPU (o)	-0.19[a]	-0.27[a]	-0.1[a]	0.06[a]	0.06[a]	0.03[c]	0.02	-0.14[a]	0.02	0.43[a]	0.59[a]	-0.06	-0.09[a]	0.46[a]	1[a]	
RGDP (p)	0.02	0.01	0	-0.01	-0.04[b]	0.02	0.04[b]	0.02	-0.01	-0.03[c]	-0.02	0.01	-0.04[b]	0	0.02	1[a]