Journal of Academia Vol. 9, Issue 2 (2021) 121 – 130

HOW INFORMATION ASYMMETRY AND CYBERCRIMINAL RISK AFFECT VOLATILITY AND RETURN OF CRYPTOCURRENCIES

Imran, W. A. W. J.[1], Yahya, M. H.[1], Hafiz Ali, M.[2*], Basir, M. A. Q. A.[3]

[1]School of Business and Economics, Universiti Putra Malaysia (UPM), Jalan Universiti 1 Serdang, 43400 Seri Kembangan, Selangor, Malaysia.
[2]Faculty of Business and Management, Universiti Teknologi MARA (UiTM), Negeri Sembilan Branch, Rembau Campus, Jalan, Kampung Pilin, 71300 Rembau, Negeri Sembilan, Malaysia.
[3]Treasurer's Office, Universiti Kebangsaan Malaysia (UKM), 43600 UKM, Bangi Selangor, Malaysia.

[*]*Corresponding author: hafiz837@uitm.edu.my*

Abstract

This research studies the factors that affect volatility in cryptocurrency markets. The relationship between information asymmetry and cybercriminal risks are studied against the volatility and return of cryptocurrencies, namely, Bitcoin (BTC), Ethereum (ETH), Bitcoin Cash (BCH) dan Ripple (XRP). These cryptocurrencies are selected as they are cryptocurrencies that are being traded by Luno, Sinergy and Tokenzie (the exchange companies regulated by the Securities Commissions of Malaysia). 730 observations were collected for each cryptocurrency via the CoinMarketCap website, from 1 January 2019 to 30 December 2020. The ADF test and the Kolmogorov-Smirnov test have been conducted before the analysis of the data. The results show the stationarity and non-normality of the data collected. The EGARCH-GED model is used to analyse the relationship between information asymmetry and volatility. The findings indicate a significant relationship between information asymmetry and volatility in BTC, ETH ad XRP. The Event Study Method (ESM) is used to analyse the effect of cybercriminal risks on returns. The result shows that all four cryptocurrencies show a significant relationship between cybercriminal risks and returns.

Keywords: Cryptocurrency, cybercriminal, volatility, cumulative abnormal return, EGARCH-GED

Article History:- Received: 30 July 2021; Accepted: 1 August 2021; Published: 31 October 2021

Introduction

Fiat currency is the main medium of exchange used for payment purposes. Unlike commodities, which have intrinsic value, fiat currency is not backed by any assets and depends mostly on the economic situation of the country. Hence, during an economic crisis, a country's currency plunges in value. Whereas, in healthy economic conditions, the value of the currency rises. A country's government is the sole issuer of its fiat currency. Hence, the value of fiat currency derives from the trust of users towards the government's control over its supply.

The invention of cryptocurrency was meant to overcome the shortfalls of fiat currency, particularly in bypassing government control of the currency. The cryptocurrency began in 2009 when Satoshi Nakamoto introduced Bitcoin in an attempt to deal with the 2008 financial crisis, due to the failure of the banking system (Liew et al., 2019). Cryptocurrency is defined as digitalized currency, in which, the transactions are secured by cryptography. The cryptocurrency exchange (payment) can be done with minimum intervention from the government (Katsiampa et al., 2018).

Since their first inception, cryptocurrencies have progressed substantially due to technological development in digitalization, especially for the payment process. Currently, various cryptocurrencies are made available offering different algorithmic designs, which attracted worldwide investors. Based on the estimated combined data of CoinMarketCap and Coinlore, at least 4,928 cryptocurrencies are being traded in the market, such as Bitcoin, Litecoin, Ethereum, Ripple, etc (Wanguba, 2020).

Background of the Study

Firstly, the issue of asynchronous information flow to the market (i.e. information asymmetry) has been a concern for investors, as this issue leads to the access of privileged and unprivileged information (Ante, 2020). Some investors are unable to obtain the necessary information for decision making, yet others are capable of making better financial decisions based on their privileged information. In San Francisco, an exchange company was sued by the US Securities and Exchange Commissions (SEC) for information asymmetry related activities (Lopatto, 2020). The founder and current CEO of Ripple allowed for transactions of XRP to only investors that are very well-informed by both individuals. This subsequently leads to price fluctuation as informed investors are prone to make adjustments accordingly to information obtained.

Secondly, there exists a potential risk in crypto mining. Cryptomining is the process carried out by crypto miners in updating the blockchain with information, whenever transactions occurred (Carlin et al., 2018). Cryptomining allows for income generation, thus it leads to competition among crypto miners in the mining process. Specialized software and a powerful central processing unit (CPU) are used to allow for speedy data processing during mining. Thus, requiring high electricity consumption, which leads to the act of stealing electricity known as cryptojacking. Based on the statistical report by SonicWall, due to the rise of cryptocurrency values, cryptojacking has been increasing rapidly in the first half of 2019 (Cook, 2020).

In the case of Malaysia, there has been a rise in the popularity of the cryptocurrency market. Despite so, there are not many registered exchanges of cryptocurrencies in Malaysia. In 2019, Luno was approved by the Securities Commissions of Malaysia, making it the first and largest cryptocurrency exchange in Malaysia.

In September 2020, two illegal crypto mining operations in Malaysia was caught for stealing electricity worth RM2.5 million (Devi, 2020). Before that, a raid by the Sarawak Energy Berhad (SEB), Electrical Inspectorate Unit (EIU) and the state police discovered an illegal crypto mining operation amounting to approximately RM250,000 (Sarawak Energy, 2020). Illegal activities of crypto mining have become a major concern for countries worldwide.

In addition, cybercriminals are shifting towards hacking crypto wallets and ransomware. These contribute to the riskiness in cryptocurrency investment and leads to the volatility of cryptocurrencies prices. According to the data obtained from the MYCERT website, March and April 2020 have the highest number of cyberattacks amounted to 1,091 and 1,488 respectively, with fraud contributes the most to the total number of attacks. According to Meikeng (2020), after the announcement of the Movement Control Order (MCO) on March 10th, 2020, the number of cyberattacks rose compared to the prior year within the same time frame.

Similar to any type of investment, cryptocurrencies' prices tend to fluctuate due to time. Thus, cryptocurrency investors are concerned with the prediction of future prices. Based on the aforementioned factors, information asymmetry and cybercriminals contribute towards volatility in the cryptocurrency market. Cryptocurrency has been extensively studied on its market dynamics that affect investment behaviour. Nonetheless, it is important to study the volatility of the cryptocurrency market caused by information asymmetry and cybercriminal risks.

Hence, to fill the gap in the literature, this research is set to identify the driving factors that determine the volatility movements of cryptocurrency, whether they can be used to predict future volatility. This research intends to investigate the influence of 1) information asymmetry and 2) cybercriminal risks on volatility movements and return in the cryptocurrency market, respectively. The findings of this research could provide a more accurate prediction for Malaysian cryptocurrency investors in their investment decisions. Moreover, the study is expected to provide an in-depth analysis of the factors that affect cryptocurrencies' volatility.

Literature Review

To understand the relationship between information asymmetry and cybercriminal risk with the movements of cryptocurrencies, the Efficient Market Hypothesis (EMH) is adopted. EMH sets forth the assumptions that the effect of available information is being reflected in the cryptocurrency prices. Therefore, the market adjusts to the changes in information to allow for the trading of cryptocurrencies at fair value. Subsequently, the volatility movements are assumed to be influenced by information asymmetry and cybercriminal risk.

Information Asymmetry

Information asymmetry indicates that users do not acquire information at the same time, leading to public and privileged information (Park and Chai, 2020). As a consequence, market inefficiency occurs as only informed investors can make the best trading decisions out of the information obtained, gaining excess profits. Othman et al. (2019) analysed the effect of asymmetric and symmetric information on the volatility of cryptocurrency by estimating the returns. The study finds, asymmetrical information has no significant relationship against volatility, unlike symmetrical information, which exhibits a significant effect on volatility. The finding is supported by Tissaoui et al. (2020) where they indicated that no immediate interaction between asymmetry information, returns and volatility can be seen in their study. They focused their research on evaluating whether or not intraday information has any effect on Bitcoin price volatility. They concluded that the relationship between arrival of information and lagged trading volume is insignificant.

However, Ante (2020) contradicts the aforementioned studies. Ante (2020) looks into how the nature of information affects the trading volume of informed and uninformed investors[1]. It is found that investors with privileged information tend to adjust their trading volume following the information obtained, where both positive (i.e. enhancement of cybersecurity) and negative (i.e. cyberattacks incidents) news, are found to have different levels of influence on the volatility (McWharter, 2018). Park and Chai (2020) also support the said conclusion, while investigating the relationship between asymmetrical information in the cryptocurrency market. The findings highlight that there exists a significant relationship between the nature of information arrival and volatility through the presence of investment sentiments in decision-making. Fakhfekh and Jeribi (2020) reported the existence of asymmetric volatility effect in cases of uninformed investors driving the prices up in contrast to the falling market. The trading volume contains information that might contribute to the forecasting of future strategies to achieve greater profits (Fousekis and Tzaferi, 2020). Since uninformed investors are relying on the 1) investment sentiment and 2) current trend, their trading volume is affected by the high-risk environment. Therefore, information asymmetry should be mitigated through the disclosure of information[2] to the public and abate privileged information.

Cybercriminal Risks

According to McWharter (2018), at the near-end year 2013, there was a spike in Bitcoin price up to 1,132.36 USD. However, a few months later[3], a Bitcoin exchange company in Japan reported being hacked., which negatively affected the Bitcoin price. Volatility bears a positive relationship with cybercriminal events, as investors perceive the investment as unstable and risky (Corbet et al., 2018). Corbet et al. (2018) observe that whenever news regarding cybercriminals is announced, there are movements in the cryptocurrencies' prices. Cybercriminal proxies in the study include hacking of 1) blockchain technology, 2) cryptocurrencies exchange and 3) users' crypto wallets. These cybercriminal activities led to major losses[4] in the cryptocurrency markets. Lyocsa et al. (2020) supported further analysed the effect of hacking of cryptocurrency exchange on the volatility of the cryptocurrency market.

[1] Informed investors are those who operated or participated in the Bitcoin network, while uninformed investors are common investors in the market who based their trading decisions on their limited knowledge of the cryptocurrency market

[2] Such as Corporate Disclosure and/or Financial Information Disclosure

[3] February 2014

[4] For example, an exchange company in Vietnam committed cryptocurrency theft in 2018, subsequently results in the loss of $650 million for 32,000 investors.

The study notes a significant positive correlation between hacking and the volatility of the cryptocurrency market.

In addition, Al-Hajri et al. (2019) reported that cybercriminals are refining malicious software, which leads to cryptojacking. Cryptojacking can be defined as the techniques used by hackers in the mining operation of cryptocurrencies, albeit, illegally and anonymously. Storsveen and Veliqi (2020) found a positive relationship between cyberattacks and volatility. The study analyses how cyberattack affects cryptocurrencies trading volume, returns and volatility. In the case of volatility, the trend spiked once information of the cyberattacks reached the investors. Moreover, the study concludes that returns and trading volume also influenced volatility. Thus, determining the returns and volume associated with the cyberattacks is sufficient to forecast the volatility of cryptocurrencies.

However, Grobys (2019) finds delayed response in cryptocurrencies' volatility against cyberattacks. The study examines whether Bitcoin and Ethereum price movements can be observed immediately or in a delayed manner after hacking events. The study finds that both cryptocurrencies have a delayed effect on the volatility associated with hacking. EGARCH model is used to identify the estimated time delay, where the increased volatility occurred after 5 days of the hacking incidents. In addition, spill-over effects may occur as companies trade various cryptocurrencies, making them vulnerable to volatility if being hacked.

Methods

Data Sample

The sample data was collected via CoinMarketCap.com. The selection of cryptocurrencies is made based on the exchange companies approved by Bank Negara and regulated by the Securities Commissions of Malaysia (SEC). Three companies have been identified to meet the criteria, namely Luno, Sinergy and Tokenzie. The cryptocurrencies supported by the three companies include Bitcoin (BTC), Ethereum (ETH), Bitcoin Cash (BCH) and Ripple (XRP). The data includes cryptocurrencies' closing price from 1 January 2019 to 30 December 2020. It comprises daily closing prices for BTC, ETH, BCH and XRP, with 730 observations each.

Furthermore, the variables used in this study is based on relevant past literature. Firstly, the asymmetric effect based on the daily returns (Anifowose, 2016) is used as a proxy for information asymmetry. Secondly, the number of cybercriminal attacks obtained from the MYCERT website is used as a proxy for cybercriminal risks, in line with the literature of Storsveen and Veliqi (2020). Thirdly, the persistency of the volatility shocks (Othman et al., 2019) is used as a proxy for volatility. Lastly, cryptocurrencies' daily return (Tweneboah-Koduah and Atsu, 2020) is used as a proxy for return.

Event Study

An event study is used to analyse the reaction of stocks against the occurrence of events (Tweneboah-Koduah and Atsu, 2020). The event study methodology is based on the semi-strong form of the efficient market hypothesis (EMH), in which, the stock prices react immediately and fairly accurate to the available information (Fama, 1998). This method is used to understand the effect of cyberattacks announcements (i.e. cybercriminal risks) on the volatility movements of cryptocurrencies. This study uses the news on the cyberattacks on 13 April 2020 as the event time for this study, as the announcement is made known to the public. By adopting the single-factor market model, the abnormal returns (AR), as well as, the cumulative abnormal returns (CAR) are calculated.

The adoption of the market model assists in the calculation of abnormal return (AR), which described the unusual pattern in stock return that is beyond the expected returns, and it can be in the positive or negative values. AR can be determined using the following formula:

$$AR_{it} = R_{it} - (\alpha_i + \beta_i R_{mt})$$

Where AR_{it} is abnormal return, R_{it} is the return on equity, and R_{mt} is market return.

Next, cumulative abnormal return (*CAR*) is determined from the *AR*. It is used to measure the impact of events, such as the imposition of regulations and cyberattack announcements, on the stocks over the short event window. CAR can be defined as follows:

$$CAR_{T_1,T_2} = \sum_{t=T_1}^{T_2} AR_t$$

In line with Liew et al. (2019), the daily return is calculated using the following formula:

$$R_t = \frac{P_t}{P_{t-1}} - 1$$

Where R_t is the daily return on cryptocurrency index for time t, P_t is the closing price at time t, and P_{t-1} is the corresponding price at the period $t - 1$.

Exponential Generalized Auto-Regressive Conditional Heteroskedasticity (EGARCH) Model

In analysing the volatility of cryptocurrency, prior literature adopts the autoregressive conditional heteroscedasticity (GARCH) model. Bollerslev (1986) first introduced the GARCH model to overcome the scope limitations of the ARCH model. This study uses the EGARCH model to analyse the volatility structure for 2 years. The EGARCH model was introduced by Nelson (1991). Nelson and Cao (1992) state that the EGARCH model is better in comparison to the GARCH model as it poses no restrictions on the non-negative constraints of the parameters (such as variance). The EGARCH-GED model is a better forecast compared to the GARCH model as it is designed to analyse non-normal data. The estimation of volatility movements can be determined using the following EGARCH formula:

$$\ln \sigma_{j,t}^2 = \omega_j + \beta_j \ln\left(\sigma_{j,t-1}^2\right) + \gamma \frac{\varepsilon_{t-1}}{\sqrt{\sigma_{t-1}^2}} + \alpha \left[\frac{|\varepsilon_{t-1}|}{\sqrt{\sigma_{t-1}^2}} - \sqrt{\frac{2}{\pi}} \right]$$

$\sigma_{j,t}$ represents the conditional variance estimated based on past information while α and β represent the symmetric effect and persistence in conditional volatility respectively. The γ parameter is the asymmetric effect used in determining the shocks on volatility. It allows for the estimation of asymmetric information. If γ is equal to 0, the model is considered symmetric. When γ parameter is negative in value, the negative shocks (bad news) have higher volatility than positive shocks (good news); but if the γ parameter is positive in value, positive shocks possess more volatility than negative shocks.

Findings and Analysis

Descriptive Statistics

The mean returns are in the positive range, with BTC and ETH having the same value of 0.0035. BCH has a mean of 0.0027 while XRP 0.0006. The medians for BCH and XRP have negative values in contrast with the positive medians of BTC and ETH. Moreover, the smallest minimum value is reflected by BCH with -0.4296 and the largest maximum value of 0.4086. Apart from that, according to Bentes and Cruz (2011), the volatility index of cryptocurrencies can be determined from the standard deviation. From the results in Table 1, BCH has the highest volatility index with 0.0541, followed by XRP, ETH and BTC, with values of 0.0500, 0.0456 and 0.0367, respectively.

Table 1. Descriptive Statistics

	Mean	Standard deviation	Minimum	Median	Maximum
BTC	0.0035	0.0367	-0.3717	0.0017	0.1819
ETH	0.0035	0.0456	-0.4235	0.0015	0.1894
BCH	0.0027	0.0541	-0.4296	-0.0004	0.4086
XRP	0.0006	0.0500	-0.4233	-0.0009	0.3968

Dickey-Fuller Analysis

The augmented Dickey-Fuller test is carried out in determining the stationarity of the data. Using the

daily returns, the t-stats values are calculated and compared with the critical values of Dickey-Fuller. Results in Table 2 showed that the t-statistic values are significantly smaller than the critical values, hence the cryptocurrencies are assumed to be stationary and no unit root is present in the time series.

Table 2. Results for the ADF test

	t-Statistic	1% Critical Value	5% Critical Value	10% Critical Value
BTC	-29.0005	-3.434	-2.862	-2.567
ETH	-29.7249			
BCH	-29.1338			
XRP	-28.5407			

Note: The critical values are based on MacKinnon (1991) critical values for cointegration tests

Kolmogorov-Smirnov Analysis

The Kolmogorov-Smirnov analysis in Table 3 showed that the variables do not follow a trend of a normal distribution, thus, rejecting the null hypothesis of this test.

Table 3. Result from the Kolmogorov-Smirnov Analysis

	KS-Statistic	1% Critical Value	5% Critical Value	10% Critical Value
BTC	2.963	0.060	0.050	0.045
ETH	2.561			
BCH	2.856			
XRP	4.052			

Note: The critical values are calculated based on N = 730

EGARCH Model Analysis

The Kolmogorov-Smirnov analysis indicates that the data is not normally distributed, this research undertakes the EGARCH model with the Generalized Error Distribution (GED). Ω represents the unconditional variance or the long-run variance in the EGARCH-GED series while α, γ and β represent the coefficients for ARCH, asymmetric and GARCH parameters respectively. The asymmetric effect (γ) is used to determine the shocks on volatility. When the value of γ is equal to 0, it reflects symmetric volatility. As this research is intended to study the relationship of asymmetric effect on volatility movements, the γ must be either in the negative or positive ranges. Based on Table 4, BTC, ETH, BCH and XRP has values of γ of -0.0699, -0.0751, -0.0850, and -0.0213 respectively.

Table 4. EGARCH-GED series parameters for BTC, ETH, BCH and XRP

	Variance Equation			
	BTC	**ETH**	**BCH**	**XRP**
ω (constant)	0.0034	0.0037	0.0033	-0.0003
Ω	-1.0442	-1.2604	-7.0283	-1.5448
α	0.2125	0.1976	0.2434	0.5239
γ	-0.0699	-0.0751	-0.0850	-0.0213
β	0.8643	0.8196	-0.1722	0.8104
α + β	1.0768	1.0172	0.0712	1.3343

Since the values of γ for all four cryptocurrencies are negative, it is deemed that the effect is asymmetric. It indicates that bad news led to higher volatility and good news produce a less volatile market. Generally, it means that given a situation where there is news on cyberattacks (negative shock) and cybersecurity enhancements (positive shock), the former generates higher volatility of cryptocurrencies than the latter. Due to the existence of the asymmetric effect, the cryptocurrency market is considered to be informationally efficient in which all information has been reflected in the cryptocurrency prices. These findings are supported by Fousekis and Tzaferi (2020) in which asymmetric effects influence cryptocurrencies.

The sum of coefficients α and β reflects the volatility persistence. The closer the value to 1, the more persistent is the variance process. However, when the value exceeds the unity value of 1, it is assumed

that the cryptocurrencies' volatility will take a much longer time to peter out. According to Table 4, for BTC, the sum of coefficients α and β is 1.0768, reflecting that the value is more than 1. The same can be observed for ETH as well as XRP with values of 1.0172 and 1.3343 respectively. These values imply that shocks to the conditional variance will be very highly persistent as it is above the unity value of 1. Thus, the volatility of BTC, ETH and XRP will remain longer in the market and may take some time for the cryptocurrencies to stabilize. Although cryptocurrency is generally volatile, having high volatility persistence is extremely risky for investors because the value fluctuates aggressively over the positive and negative ranges for a longer period. Meanwhile, for BCH, since the sum of coefficients α and β are 0.0712, the value is very far from 1, indicating that the shocks have a very low volatility persistence. This explains that BCH will stabilize much quicker in the market as compared to BTC, ETH, and XRP.

The differences in volatility persistence may be due to the market capitalization of cryptocurrencies. As ranked on the CoinMarketCap website, BTC has the largest market capitalization, followed by ETH, XRP and BCH. For BCH, the volatility movements in the market are drastically influenced, either positively or negatively, in the presence of events such as intense competition and economic boom. However, due to its low volatility persistence, the fluctuations are only short term in nature. On the other hand, concerning BTC, ETH and XRP, the effect of information asymmetry that privileged investors possess is less vulnerable to the occurrences of events as these cryptocurrencies are generally more matured and well-established in the cryptocurrency market. Therefore, any changes in the events will not greatly affect the volatility movements of BTC, ETH and XRP, indicating that the fluctuations are long term in nature.

Event Study Method (ESM) Analysis

Based on Table 5, at day +1, the abnormal returns for all four cryptocurrencies show absolute t-stats values lower than the critical values of 1.96, reflecting a slow movement in the cryptocurrency market a day after the cyberattack announcement. But, after day +1, the absolute t-stats values becomes statistically significant. Firstly, at day +2, the values for BTC, ETH, BCH and XRP are 2.211, 2.954, 2.787, and 2.971 respectively. This is slightly more than the critical value of 1.96. Meanwhile, at day +3, the values showed a significant increase from the previous day, in which BTC, ETH, BCH and XRP have t-stats values of 6.946, 12.038, 9.089 and 4.698 respectively. The increase in values, further from 1, implies that the cyberattack announcements have less influence on the returns of cryptocurrencies. This may be due to businesses being the institutional investors are less vulnerable to data breaches; hence, the announcements have little pressure on this group of investors. With fewer large investments by businesses, the prices do not fluctuate much in the markets.

Since cyberattack announcements are perceived as bad news, the cumulative abnormal return (CAR) is expected to decline over the 11-days event windows, reflecting negative shocks to the volatility movements. 5 days before the event date, the CAR values of BTC, ETH, BCH and XRP began to drastically fall between day -2 and day -1, with differences of 6.08%, 7.34%, 9.57% and 5.66% respectively. Next, for the event window after the cyberattack announcements, for day +1, the findings showed that the CAR values of BTC, BCH and XRP decrease to -0.95%, -4.87% and 1.91% respectively. However, it shows a slight increase in returns at day +3 with values of BTC, BCH and XRP being 3.08%, 1.36% and 4.43% respectively, before further decreases to -1.66%, -4.80%, and 0.44% on day +4. On the other hand, only ETH's CAR increases to 8.87% after the announcements. Although it suffered a decline at day +2 with 6.04%, it was increased to 18.26% at day +3, before drastically drops over the remaining event period (day +4 and day +5).

Based on the findings, the effect of the announcements is immediate, and the return movements of BTC, ETH, BCH and XRP persist longer in the market as the values have begun to drop before the occurrences of the event. Therefore, the CAR values are assumed to be affected immediately after the cyberattack announcements. Since the CAR values gradually decrease near the end of the 11-days event window, the effect persists longer in the market for all cryptocurrencies. The results supported the research by Storsveen and Veliqi (2020) where the volatility increases when the information is made public.

Although the data is not normally distributed, the short period of observations contributes to the absence of severe effects on the ESM analysis (Saens and Sandavol, 2005).

Table 5. Abnormal Return (AR), t-statistics and Cumulative Abnormal Return (CAR)

	BTC			**ETH**		
	Intercept	0.0010		Intercept	0.0009	
	Slope (Beta)	-0.0071		Slope (Beta)	0.0027	
	Std. error	0.00101		Std. error	0.0102	
	R-square	0.0005		R-square	0.0001	
Day	**AR**	**t-stat**	**CAR**	**AR**	**t-stat**	**CAR**
-5	6.99%	6.885	6.99%	17.73%	17.470	17.73%
-4	-1.39%	-1.372	5.59%	-2.48%	-2.448	15.25%
-3	2.10%	2.066	7.69%	4.48%	4.411	19.73%
-2	-0.53%	-0.521	7.16%	-1.15%	-1.135	18.57%
-1	-6.08%	-5.993	1.08%	-7.35%	-7.239	11.23%
0	-1.91%	-1.877	-0.82%	-3.11%	-3.060	8.12%
+1	-0.13%	-0.124	-0.95%	0.75%	0.740	8.87%
+2	-3.02%	-2.971	-3.97%	-2.83%	-2.787	6.04%
+3	7.05%	6.946	3.08%	12.22%	12.038	18.26%
+4	-0.38%	-0.370	2.71%	-0.40%	-0.391	17.86%
+5	-4.37%	-4.306	-1.66%	-5.22%	-5.141	12.65%

	BCH			**XRP**		
	Intercept	0.0009		Intercept	0.0009	
	Slope (Beta)	-0.0038		Slope (Beta)	-0.0038	
	Std. error	0.0101		Std. error	0.0101	
	R-square	0.0003		R-square	0.0003	
Day	**AR**	**t-stat**	**CAR**	**AR**	**t-stat**	**CAR**
-5	10.22%	10.070	10.22%	8.89%	8.772	8.9%
-4	-1.59%	-1.569	8.63%	-1.81%	-1.789	7.08%
-3	5.53%	5.449	14.16%	4.48%	4.424	11.56%
-2	-3.38%	-3.330	10.78%	-1.38%	-1.363	10.18%
-1	-9.57%	-9.427	1.21%	-5.55%	-5.474	4.63%
0	-5.16%	-5.080	-3.94%	-1.36%	-1.338	3.27%
+1	0.93%	-0.914	-4.87%	-1.36%	-1.343	1.91%
+2	-3.00%	-2.954	-7.87%	-2.24%	-2.211	-0.33%
+3	9.22%	9.089	1.36%	4.76%	4.698	4.43%
+4	-0.92%	-0.909	0.43%	-0.03%	-0.026	4.41%
+5	-5.24%	-5.159	-4.80%	-3.97%	-3.913	0.44%

Conclusion

Relationship between information asymmetry and cryptocurrencies' volatility movements

The study finds that BTC, ETH, and XRP have high volatility persistence despite having a low volatility index. This explains that the volatility for BTC, ETH and XRP persisted longer in the market. The study also finds the existence of asymmetric information in the market, based on the values of the asymmetric effect of all four cryptocurrencies are less than zero. Hence, it is concluded that information asymmetry has a significant relationship with the volatility movements of the cryptocurrencies, as can be observed from the volatility persistence of BTC, ETH and XRP which have values of more than 1. However, BCH does not share the same result due to its small market size in comparison to the other three cryptocurrencies.

Furthermore, for cryptocurrencies with high volatility persistence, investors may lose confidence as the

financial crisis will also persist in the cryptocurrency market. Since, BTC, ETH and XRP have high volatility persistence due to information asymmetry, regulators should provide adequate policies that enable the efficient and unbiased flow of information in the market. This would mitigate the asymmetric effect on investment decisions as well as maintain the market's stability. In turn, it would restore investors' confidence due to the increase of information transparency in the cryptocurrency market.

Relationship between cybercriminal risks and cryptocurrencies' return movements

In analysing the cryptocurrencies' CAR, due to cybercriminal risks **(**cyberattack announcement), the study finds that ETH has a slightly delayed effect. Whereas, the effect of the announcements occurred immediately for BTC, BCH and XRP, where CAR's negative values declined after the announcements. Although the CAR values for the cryptocurrencies increase at day +3, further drops in values, indicate that there is high volatility persistence against the cyberattack announcements. Therefore, the cybercriminal risk is assumed to have a strong relationship with the return movements in the cryptocurrency market as the CAR fluctuates over the 11 days of the event.

References

Al-Hajri, H. H., Al-Mughairi, B. M., Hossain, M. I., and Karim, A. M. (2019). Crypto Jacking a Technique to Leverage Technology to Mine CryptoCurrency. *International Journal of Academic Research in Business and Social Sciences, 9(3)*, 1210-1221.

Anifowose, M. (2016). Information Asymmetric Effect on the Stock Return Volatility in Nigerian Capital Market. *Accounting Frontier, 14(2)*, 47-64.

Ante, L. (2020). Bitcoin transactions, information asymmetry and trading volume. *Quantitative Finance and Economics, 4(3)*, 365-381.

Bentes, S. R. and Cruz, M. M. D. (2011). Is Stock Market Volatility Persistent? A Fractionally Integrated Approach. *Economics,* 1-22.

Bollerslev, T. (1986). Generalized autoregressive conditional heteroskedasticity. *Journal of Econometrics, 31*, 307-327.

Carlin, D., O'Kane, P., Sezer, S., and Burgess, J. (2018). *Detecting Cryptomining Using Dynamic Analysis.* Paper presented at 2018 16th Annual Conference on Privacy, Security and Trust (PST).

Cook, S. (2020, November 10). *Malware statistics and facts for 2020.* Retrieved November 23, 2020, from https://www.comparitech.com/antivirus/malware-statistics-facts/

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., and Vigne, S. A. (2018). Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in cryptocurrency Markets. *SSRN,* 1-57. Retrieved December 15, 2020, from https://dx.doi.org/10.2139/ssrn.3384707

Devi, V. (2020, September 1). Cryptocurrency premises raided for stealing electricity. *The Star.* Retrieved November 8, 2020, from https://www.thestar.com.my/metro/metro-news/2020/09/01/cryptocurrency-premises-raided-for-stealing-electricity

Fakhfekh, M. and Jeribi, A. (2020). Volatility dynamics of crypto-currencies' returns: Evidence from asymmetric and long memory GARCH models. *Research in International Business and Finance, 51*, 1-10.

Fama, E. F. (1998). Market efficiency, long-term returns, and behavioral finance. *Journal of Financial Economics, 49,* 283-306.

Fousekis, P., and Tzaferi, D. (2020). Returns and volume: Frequency connectedness in cryptocurrency markets. *Economic Modelling, 95*, 13-20. https://doi.org/10.1016/j.econmod.2020.11.013.

Grobys, K. (2019). *When the blockchain does not block: On hackings and uncertainty in the cryptocurrency market.* University of Vaasa, Finland. Retrieved December 17, 2020, https://dx.doi.org/10.2139/ssrn.3555667

Katsiampa, P., Gkillas, K., and Longin, F. (2018). Cryptocurrency Market Activity During Extremely Volatile Periods. *SSRN.* Retrieved November 3, 2020, from http://dx.doi.org/10.2139/ssrn.3220781

Liew, J. K. S., Li, R. Z., Budavari, T., and Sharma, A. (2019). Cryptocurrency Investing Examined. *The Journal of the British Blockchain Association, 2(2)*, 1-12.

Lopatto, E. (2020, December 22). SEC says third-largest cryptocurrency was sold all wrong. *The Verge.* Retrieved December 30, 2020, from https://www.theverge.com/2020/12/22/22196064/ripple-sec-cryptocurrency-security-currency-xrp

Lyocsa, S., Molnar, P., Plihal, T., and Siranova, M. (2020). Impact of macroeconomic news, regulation and hacking exchange markets on the volatility of bitcoin. *Journal of Dynamics and Control, 119*, 103980. Retrieved December 13, 2020, from https://doi.org/10.1016/j.jedc.2020.103980

MacKinnon, J. G. (1991). Critical values for cointegration tests. In *Eds.), Long-Run Economic Relationship: Readings in Cointegration*.

McWharter, N. (2018). Bitcoin and Volatility: Does the Media Play a Role? *Economics Student Theses and Capstone Projects.*

Meikeng, Y. (2020, April 12). Cybersecurity cases rise by 82.5%. *The Star*. Retrieved April 12, 2020 from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

Nelson, D. B. (1991). Conditional Heteroskedasticity in Asset Returns: A New Approach. *Econometrica, 59(2)*, 347-370.

Nelson, D. B. and Cao, C. (1992). Inequality Constraints in the Univariate GARCH Model. *Journal of Business and Economic Statistics, 10(2)*, 229-235.

Othman, A. H. A., Alhabshi, S. M., and Haron, R. (2019). The effect of symmetric and asymmetric information on volatility structure of crypto-currency markets. *Journal of Financial Economic Policy, 11(3)*, 432-450.

Park, M., and Chai, S. (2020). *The Effect of Information Asymmetry on Investment Behaviour in Cryptocurrency Market.* Paper presented at the proceedings of the 53rd Hawaii International Conference on System Sciences.

Saens, R. and Sandoval, E. (2005). Measuring Security Price Performance Using Chilean Daily Stock Returns: The Event Study Method. *Cuadernos de Economia, 42,* 307-328.

Sarawak Energy nabs five cryptocurrency operators stealing state electricity supply. (2020, August 12). *Malay Mail.* Retrieved November 8, 2020, from https://www.malaymail.com/news/malaysia/2020/08/12/sarawak-energy-board-nabs-five-cryptocurrency-operators-stealing-state-elec/1893370

Storsveen, M., and Veliqi, F. (2020). *The Impact of Cryptocurrency-Related Cyberattacks on Cryptocurrencies and Traditional Financial Assets.* Unpublished master's thesis, University of Stavanger, Norway, Europe.

Tissaoui, K., Zaghdoudi, T., and Alfreahat, K. I. (2020). Can intraday public information explain Bitcoin Returns and Volatility? A PGARCH-Based Approach. *Economics Bulletin, 40(3)*, 2085-2092.

Tweneboah-Koduah, S. and Atsu, F. (2020). Reaction of Stock Volatility to Data Breach: An Event Study. *Journal of Cyber Security and Mobility, 9(3),* 1-19.

Wanguba, J. (2020, December 2). How Many Cryptocurrencies Are There In 2020? *E-Crypto News.* Retrieved November 8, 2020, from https://e-cryptonews.com/how-many-cryptocurrencies-are-there-in-2020/