Investigating the Dynamics Between Price Volatility, Price Discovery, and Criminality in cryptocurrency Markets

Shaen Corbet[a], Douglas J. Cumming[b], Brian M. Lucey[c,d,e], Maurice Peat[e], Samuel A. Vigne[f]

[a] *DCU Business School, Dublin City University, Dublin 9, Ireland*

[b] *FAU College of Business, Florida Atlantic University, Boca Raton, FL 33431, United States*

[c] *Trinity Business School, Trinity College Dublin, Dublin 2, Ireland*

[d] *Institute of Business Research, University of Economics Ho Chi Minh City, Ho Chi Minh City, Vietnam*

[e] *University of Sydney Business School, Sydney, New South Wales, Australia*

[f] *Queen's Management School, Queen's University Belfast, BT9 5EE, Northern Ireland*

[*] *Corresponding Author: shaen.corbet@dcu.ie*

Abstract

This paper identifies several stylised facts relating to the volatility and price discovery process from eight cryptocurrencies utilising an empirical analysis of intra-day trading data to uncover four main results. First, cryptocurrencies exhibit weekend-volatility effects while intra-day volatility is found to be influenced by international trading times, periods of substantial volatility in the markets for oil, and GBP/USD and cybercrime events. Secondly, a thorough investigation of recent cybercriminality identifies that cryptocurrency hacks are found to increase both the volatility of the currency hacked and the correlations across the hacked currency and other cryptocurrencies. Thirdly, hacks significantly reduce price discovery sourced within the hacked currency relative to other cryptocurrencies. Finally, there are abnormal returns associated with the hacks observed in the hours prior to the actual hacking event, which reverts to zero at the time of the public announcement of the hack.

Keywords: Market Manipulation; Price Volatility; Cryptocurrency; Hacking; Cybercrime; Cryptocurrencies; Bitcoin; GARCH; Currencies.

"... hacks in the cryptocurrency space are problematic since transactions are irreversible. Since the network is decentralised and trustless, it doesn't have a mechanism to discriminate between transactions that are made with stolen coins or legitimate ones. Without the ability to reverse a transaction, the protections around preventing illegitimate transactions become incredibly important."

Forbes[1], September 27, 2018

[1] https://www.forbes.com/sites/forbesagencycouncil/2018/09/27/cryptocurrency-how-to-avoid-getting-hacked/

Preprint submitted to SSRN *May 3, 2019*

Conflict-of-interest disclosure statement

Shaen Corbet
I have nothing to disclose

Douglas J. Cumming
I have nothing to disclose

Brian M. Lucey
I have nothing to disclose

Maurice Peat
I have nothing to disclose

Samuel A. Vigne
I have nothing to disclose

The above authors have no conflict-of-interests with regards to the following submission.

No funding has been received in exchange for the following work. This research is not under consideration in any other publication.

This is the first submission of this research.

We sincerely thank the editorial team for their time and efforts when considering our work.

1. Introduction

Cryptocurrencies involve blockchain, or 'distributed ledger', technology. Cryptocurrencies have become popular because they enable efficient payment systems through a decentralised distributed ledger, which does not depend on a political process or governmental regulatory system. Blockchain technology is immutable (that is, the history can be added to but not changed). Blockchain technology transactions minimise search, legal, and transactions costs, as well as counterfeiting risks [Harvey, 2017]. Cryptocurrency and blockchain research in its entirety is in its relative youth. Our research attempts to establish key stylised facts surrounding the source of price volatility in eight of the largest international cryptocurrencies determined by market capitalisation, while utilising a number of methodological approaches to analyse the core of the investment product's price discovery. One such topic that has widely damaged both the confidence and integrity associated with both these products and exchanges one such topic includes cybercriminality, such as fraud and hacking, whose risks come in a variety of forms. For example, with access to the public's credentials, hackers can steal electronic identities and move funds from legitimate accounts. Hackers may engage in phishing attacks in which the hacker steals credentials by faking the appearance of trustworthy sources. Hackers may further steal information through direct security breaches. Concluding our analysis, we set out to examine the frequency of hacks of the major cryptocurrencies from a recent 12-month period and determine the financial market consequences of these hacking events with regards to price volatility and price discovery. We regard these hacking events as exogenous and unexpected to the currency hacked. That is, there is attempted hacking of all cryptocurrencies at all times, but the success of a hack is rather random and unexpected and subject to inadvertent security breaches and is no more common for major or minor cryptocurrencies.

We obtained all intra-day trading data from September 2017 to August 2018 for eight major cryptocurrencies: Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Monero, Cardano, and Bitcoin cash. Our empirical analysis of intra-day trading data shows the following stylised facts. First, we have identified that there are substantial differences in cryptocurrency volatility between weekdays and weekends robust across a number of measures. This is simply denoted as a 'weekend effect'. Secondly, we identify that there are substantially elevated levels of cryptocurrency volatility while United States and European markets are open; however, this volatility is substantially reduced while Chinese and Japanese markets are operational. Finally, there is evidence of substantially elevated cryptocurrency volatility during episodes of stress in GBP/USD and oil markets. However, we must also note that there is no evidence identified to accept the hypotheses that cryptocurrency volatility varies based on the times that traditional markets open and indeed; there is no evidence identified to support the presence of hour-of-the-day effects.

Developing from this evidence, we discover that cryptocurrency hacks not only increase volatility of the currency hacked but also increase the correlations with the hacked currency and other currencies. Hence, cryptocurrency hacks are systematically damaging to cryptocurrency markets generally. The observed changes are very much hack-specific, however, and do not affect all currencies equally. Further, we observe changes in the information and component shares of price discovery generated within the hacked currency, whereby there is a reduction in price discovery found to be approximately 10-20%. Finally, we find abnormal returns associated with the hacks of between -2% to -24%, depending on the specific event. The abnormal returns are observed 4 hours prior to the actual hacking event and revert back to zero at the time and announcement of the hack.

What might uninformed investors assume in the world of cryptocurrencies? They might expect that the exchange mechanism would be secure, units of currency deposited at an exchange could be recovered, or, if sold, the payment would be transferred as directed. Furthermore, uninformed investors would expect prices on the exchange to be the product of transactions between individuals with no information advantage. These investors would most likely exhibit major behavioural biases, such as representativeness, which would lead to a concentration of trading in the largest and best publicised currencies; or, indeed, a trend-chasing bias that would lead to markets exhibiting bubble-like behaviour, which would then manifest in positive return correlations. If the majority of market participants are primarily uninformed when news of a hacking event is published, we would expect a consistent reaction from these investors after the announcement of the hack. In the event of an exchange hack, uninformed investors would be expected to: 1) trade out of the effected market and into other currencies and exchanges, leading to an increase in volatility and correlation in the markets; 2) observe changes in trading behaviour, which would, therefore, also lead to changes in the information leadership, where the affected market should have reduced leadership relative to other assets; 3) observed reactions will concentrate major assets; and 4) shift trending behavior between assets.

In the event of a scam type event, such as an ICO fraud, uninformed investors would be expected to: 1) lose confidence in all assets, leading to a general negative co-movement across the markets; 2) become uncertain about the value of all assets, leading to a general increase in volatility; and 3) observe that information leadership should be largely unaffected, if the hack is not related to a single exchange asset combination. When there is a majority of informed traders, it would be expected in advance of the event to observe persistence in post-event abnormal returns, that both volatility and information leadership changes in the minor assets. In short, these markets present evidence of manipulation when exhibiting such behaviour. If these markets are open to such manipulation, then the argument that they should be used by institutional investors for diversification purposes is questionable. There are operational risks in these markets that are not captured by the standard statistical approach to portfolio formation. Prior research, however, has not investigated the financial market impacts of cryptocurrency hacks. In this paper, we contribute to this new area of study by examining the effects of cryptocurrency hacks on volatility, asset correlations, price discovery, and the magnitude and timing of abnormal returns.

This paper is organised as follows. In Section 2, we provide a description of the methodology used to address these issues. Section 3 introduces the data. Section 4 introduces the selected methodologies as separated in three directions of analyses: i) to analyse stylised facts relating to intra-day cryptocurrency volatility; ii) to analyse the relationship between cryptocurrency volatility and traditional financial markets; and iii) to analyse the influence of cybercriminality on cryptocurrency volatility and price discovery. The results are described in Section 5, with an associated discussion and suggestions for future work in Section 6. Concluding remarks are offered in Section 7.

2. Previous Research

The continued evolution of cryptocurrencies and the underlying exchanges on which they trade has generated tremendous urgency to develop our understanding of a product that has been identified as a potential enhancement of and replacement for traditional cash as we know it. As our understanding of FinTech evolves (Goldstein et al. [2019]) and the growing value of blockchain (Chen et al. [2019]), one key area of research focuses on the interactions between cryptocurrencies and other more traditional financial markets. Urquhart and Zhang [2018] assessed the relationship between Bitcoin and currencies at the hourly frequency and found that Bitcoin could be an intraday hedge for the CHF, EUR, and GBP, though it acts as a diversifier for the AUD, CAD, and JPY. The authors also found that Bitcoin acts as a safe haven during periods of extreme market turmoil for the CAD, CHF, and GBP. This supports the results of Sensoy [2018], who found that both markets have become more informationally efficient over time, which is echoed by the work of Vidal-Tomás and Ibañez [2018], who examine the semi-strong efficiency of Bitcoin in the Bitstamp and Mt.Gox. Guesmi et al. [2018] analysed the conditional cross effects and volatility spillovers between Bitcoin and other financial assets providing evidence that Bitcoin can offer diversification benefits and hedging opportunities for investors, while Ciaian et al. [2018] employed an Autoregressive Distributed Lag model to examine interlinkages within the cryptocurrency market. Using a dynamic conditional correlation model, Bouri et al. [2017] examined as to whether Bitcoin could act as a hedge and safe haven for major world stock indices, bond, oil, gold, the general commodity index and the US dollar index using data between July 2011 and December 2015. They found that Bitcoin is a poor hedge and is suitable for diversification purposes only. Corbet et al. [2018] and Corbet et al. [2018] found evidence of the relative isolation of these assets from the financial and economic assets and that cryptocurrencies may offer diversification benefits for investors with short investment horizons. Time variation in the linkages reflects external economic and financial shocks. With regards to the introduction and relationship between cryptocurrencies and cryptocurrency derivatives, Corbet et al. [2018] claim that the introduction of Bitcoin futures and the ability to trade these would have resulted in a reduction in the variance of Bitcoin prices, or facilitated hedging strategies that could have mitigated pricing risk in the spot market. The authors find that it is possible that the Bitcoin could have acted as a unit of account, moving it closer to being a currency.

Market efficiency can be determined by a number of specific factors; however, cryptocurrencies' market efficiency can be measured through a host of progressive factors, including the existence of a new futures exchange, liquid cross-currency indices, and the relative reduction of intra-day volatility, although daily volatility remains high. In this section, we separate market inefficiency into product efficiency, as well as price efficiency. Bouoiyour and Selmi [2015] use ARDL bounds testing to reveal extremely speculative behaviour of Bitcoin, its partial usefulness in trade transactions without overlooking its dependence on the Shanghai Stock Market and the hash-rate. The authors find no evidence of Bitcoin providing a safe haven, while Roth [2015] investigated the architectural structure of Bitcoin using a functional analysis by employing the Systems Modelling Language (SysML). Urquhart [2016] was the first to examine the market efficiency of Bitcoin and found through a battery of tests that Bitcoin was inefficient, although it was becoming less inefficient over time. With regards to structural efficiency, Biais et al. [2019] identified that forks could lead to orphaned blocks and persistent divergence, generated by a range of factors including information delays and software upgrades. The result of the inefficiency of Bitcoin has been supported in follow-up studies that have used a range of different testing procedures and different data sets, where examples are Bariviera et al. [2017], Brauneis and Mestel [2018], Sensoy [2018], Tiwari et al. [2018], and Vidal-Tomás and Ibañez [2018]. Through the use of a significant database spanning 2010 through 2017, Urquhart [2018] found that both realised volatility and the volume of Bitcoin traded, controlled for Bitcoin fundamentals, are both significant drivers of the next day's attention for Bitcoin. Balcilar et al. [2017] show that volume cannot help to predict the volatility of Bitcoin returns at any point on the conditional distribution, but volume can predict returns, with the exception of Bitcoin, bull, and bear market regimes. Further, Corbet et al. [2017] while utilising the bubble identification methodology of Phillips et al. [2011], found clear evidence of periods in which Bitcoin and Ethereum experienced bubble phases.

Hu et al. [2018] analysed intra-day price behaviour of Bitcoin, Litecoin, and Ripple by examining the price clustering of non-fiat cryptocurrency exchange rate pairs. The findings report a significant price clustering at the round numbers 00, 000, and 0000, providing support for a negotiation hypothesis that predicts higher clustering for higher prices and price volatility. Furthermore, Koutmos [2018] found that a one standard deviation shock to transaction activity leads to just over a 0.30% gain in returns on the third day following the shock. However, the results report a reversal in this pattern by the sixth day after the investigated shocks. Fry and Cheah [2016] tested for contagion during bubbles and found a spillover from Ripple to Bitcoin. However, the latter study only considered Bitcoin and Ripple. The existence of structural breaks in Bitcoin volatilities has also been confirmed by Ardia et al. [2018], who did so through the use of a two-regime MSGARCH model that utilised in-sample forecasting performance with an inverted leverage effect in low- and high-volatility regimes. With regards to liquidity, Wei [2018] presented evidence that return predictability diminishes in cryptocurrencies with high market liquidity, contributing to cryptocurrency efficiency and liquidity debates. While there is little research that focuses specifically on issues relating to the interconnections between traditional financial market opening hours or trading times and the volatility of cryptocurrency markets, there is also a gap in the literature with regards to day-of-the-week effects in these new digital assets. Such traditional financial market literature such as Berument and Kiymaz [2001], Keim and Stambaugh [1984], Yamori and Kurihara [2004], and Lakonishok and Maberly [1990] supports our selected methodologies of investigation.

However, cryptocurrencies as a new asset class is not without its substantial issues, particularly that of the provision of a platform for criminality and, indeed, major cybercriminality events. While much debate surrounds the process in which this product can be regulated, there exists a wide variety of channels in which criminality can develop and thrive. We have experienced multiple, exceptionally sophisticated, high-value hacking events, both at the level of the exchange and individual cryptocurrencies alike. Each event further depreciates trust and confidence in this asset class. Furthermore, the very nature of cryptocurrencies has provided a unique and efficient channel through which both illicit funds and, indeed, illicit cross-border transactions can easily take place, although traditional assets are not without their shortcomings. Regulatory bodies and policy-makers alike have observed the growth of cryptocurrencies with a certain amount of scepticism, based on this growing potential for illegality and malpractice. Foley et al. [2019] estimate that around $76 billion of illegal activity per year involve bitcoin (46% of bitcoin transactions). This is estimated to be in the same region of the U.S. and European markets for illegal drugs, and is identified as ‘black e-commerce’. While the volatility of cryptocurrency price returns has been studied, for example, by Chu et al. [2017] and Phillip et al. [2018], the potential for market manipulation appears to have been broadly identified in cryptocurrency cross-correlations and market interdependencies. Griffins and Shams [2018] investigated as to whether Tether influenced Bitcoin and other cryptocurrency prices to find that purchases with Tether were timed following market downturns and resulted in significant increases in the price of Bitcoin. Further, less than 1% of the hours in which Tether experienced significant transactions is associated with 50% of the increase in Bitcoin prices and 64% of other top cryptocurrencies, drawing the damning conclusion that Tether was used to provide price support and manipulate cryptocurrency prices. Furthermore, Gandal et al. [2018] identified the impact of suspicious trading activity on the Mt.Gox Bitcoin exchange theft, when approximately 600,000 Bitcoins were attained. The authors demonstrated that the suspicious trading likely caused the spike in price in late 2013 from $150 to $1,000, most likely driven by one single actor. These two significant pieces of research have fine-tuned the focus of regulators, policy-makers, and academics alike, as the future growth of cryptocurrencies cannot be sustained at pace with such significant questions of abnormality remaining unanswered.

While such damaging research continues to evolve and identify substantial issues within the markets for cryptocurrencies, we also consider the results of many analyses of detrimental manipulation techniques based on traditional financial markets. While focusing on cybercriminality and the questionable market interlinkages that exist, two of the most problematic issues have been identified as ‘pump-and-dumps’ and ‘spoofing’, both identified within the definition of illegal price manipulation as defined by Kyle and Viswanathan [2008]. Putniņš [2012] states that there are three specific avenues on which we must build in order to minimise risks from market manipulations, namely 1) collecting more comprehensive data, 2) using detection controlled estimation methods, and 3) conducting controlled experiments. Sabherwal et al. [2011] analysed the information content of stock message boards to find evidence of the most common use for small firms with weak financials, with strong evidence provided of a two-day pump followed by a two-day dump manipulation pattern. Message board sentiment is found to be an important predictor of trading-related activities. Jiang et al. [2005] examine abnormal turnover and returns and the relationship between them, as well as the long-term performance of the selected stocks, to conclude that the evidence suggests informed trading rather than manipulation, based on an investigation of stock pools in the US since the 1920s. Comerton-Forde and Putniņš [2011] constructed an index of the probability and intensity of closing price manipulation while quantifying the effects of closing price manipulation on trading characteristics and stock price accuracy using a unique sample of prosecuted manipulation cases.

Clarkson et al. [2006] use an intra-day analysis to examine the market reaction to takeover rumour postings in the Hotcopper Internet Discussion Site (IDS), presenting evidence of abnormal returns and trading volumes during the ten-minute posting intervals and abnormal trading in the ten minutes immediately preceding the announcement, indicating that the market has anticipated and responded to the announcement. This is an example of a 'pump-and-dump', which is broadly defined as a scheme that attempts to boost the price of a stock through recommendations based on false or misleading statements. The perpetrators most likely possess an established position in the company's stock and sell their positions after the hype has led to a higher share price. They have been shown to be extremely detrimental to the functionality of the financial market. It is important to identify that Chiu and Koeppl [2019] estimate net gains of 1-4 bps for US corporate debt market yields when mining. Diaz et al. [2011] addresses challenges relating to applying data mining techniques to detect stock price manipulations and extends previous results by incorporating the analysis of intra-day trade prices, in addition to closing prices for the investigation of trade-based manipulations, extending previous results on the topic by analysing empirical evidence in normal and manipulated hourly data and the particular characteristics of intra-day trades within suspicious hours. Zaki et al. [2011] describes a case study on fraud detection using data mining techniques that help analysts to identify possible instances of touting based on spam emails. Their results strongly suggest the cumulative effect of 'stock touting' spam emails is key to understanding the patterns of manipulations associated with touting email campaigns and that data mining techniques can be used to facilitate fraud investigations of spam emails. 'Spoofing' is best defined as a type of scam where an intruder attempts to gain unauthorised access to a user's system or information by pretending to be the user. The main purpose is to trick the user into releasing sensitive information in order to gain access to one's bank account, computer system, or to steal personal information, such as passwords. This process can occur across multiple platforms and products, however; to date, little investigation has been based on cryptocurrency markets. Lee et al. [2013] examine how investors strategically spoof the stock market by placing orders with little chance of being executed but which mislead other traders into thinking there is an imbalance in the order book.

The authors use intra-day order and trade data from the Korea Exchange (KRX) in a custom data set identifying individual accounts. We found that investors strategically place spoofing orders, which, given the KRX's order-disclosure rule at the time, creates the impression of a substantial order book imbalance, with the intent to manipulate subsequent prices. Further research that considers the effects of issues such as spoofing includes Cumming et al. [2011], who investigated exchange trading rules based on market manipulation, insider trading, and broker-agency conflicts, and O'Hara [2015] who analysed high-frequency market microstructure.

3. Data

We first set out to investigate the interactions between a number of traditional assets for some of the largest cryptocurrencies traded around the world. While considering an exceptionally broad number of products, our final selection of traditional financial market assets was predicated on providing a broad representation of stocks, commodities, currencies, and options. Therefore, we have selected GBP/USD to represent interatctions between cryptocurrencies and broad currency markets, the S&P500 as a representation of stock market performance, both gold and oil (as measured by West Texas Intermediate, WTI oil markets) as a representation of commodity markets, and finally the VIX (CBOE volatility index) to represent options markets and implied volatility respectively. Our selected traditional financial markets, sampled at 60-minute intervals, was collected from Thomson Reuters Tick History for the period from midnight on 1 September 2017 through midnight on 10 August 2018. This time period was selected as it maximised the number of observations available across all of our selected markets. From the 60-minute transaction prices our selected financial products, the log return for each period, $r_t = ln(P_t/P_{t-1})$ is then estimated. We utilise data from the Bitfinex exchange at an 60-minute frequency for the eight most liquid cryptocurrencies throughout the period. We therefore use data for Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Monero, Cardano and Bitcoin Cash. We considered the use of higher frequency data and even tick level data, however, the use of hourly data was found to be most effective from a methodological standpoint. One distinct issue surrounds the opening times of our selected financial products. Cryptocurrency markets are open 24 hours a day, seven days a week, providing 8,297 hourly observations in our sample (with the exception of Cardano with 7,376 observations due to data being unavailable prior to 09:00 on 9 October 2007). Our selected traditional financial markets have varying opening times All times are matched using Greenwich Mean Time (GMT). However, gold which represents the most infrequently trading product has 1,229 observations, whereas GBP/USD presents 5,891 observations. Commodity markets as represented by gold and oil markets are the traditional markets most frequently open.

Table 1 presents the descriptive statistics of the selected traditional assets and cryptocurrencies. The VIX represents the most volatile of the selected traditional financial markets as denoted with mean hourly returns of +0.015%. All cryptocurrencies present evidence of mean hourly returns above the next most volatile traditional asset which is the market for oil. Stellar is the most volatile cryptocurrency with a variance of 0.00045 and standard deviation of 0.02111. The largest one hour loss occurred in the market for Bitcoin Cash (-23.91%), while the largest gain occurred in the market for Stellar (+40.325%). Table 2 presents the correlation matrix for all of our selected variables for the entire period of time under investigation. We observe that there are three distinct areas of interest, namely the correlations between both traditional financial assets and cryptocurrencies in isolation and indeed the correlations between these two asset classes. There are a number of stark observations, namely quite elevated correlations between intra-asset classes, however, little inter-asset correlations further indicative of the relative isolation of cryptocurrencies as an asset class as previously identified (Corbet et al. [2018]). Intra-cryptocurrency return correlations also present evidence of strong comovement of cryptocurrencies and Bitcoin with the exception of Stellar (+0.052) and Cardano (+0.088). Observing traditional financial market correlations, the VIX presents a theoretically expected negative relationship with the S&P500 (-0.768), while Oil as identified by the price movements of West Texas Intermediate presents a positive correlation with equity markets (+0.363).

Insert Tables 1 and 2 about here

In order to investigate the effects of cybercriminality on cryptocurrency markets, we utilise data from the Bitfinex exchange at a 60-minute frequency for the eight most liquid cryptocurrencies throughout the period[2]. We use data for Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Monero, Cardano and Bitcoin Cash. We considered the use of higher frequency data and even tick level data, however, the use of hourly data was found to be most effective from a methodological standpoint. One distinct issue surrounds the opening times of our selected financial products. The log return for each period are calculated $r_t = ln(P_t/P_{t-1})$. Cryptocurrency markets are open 24 hours a day, seven days a week, providing 8,297 hourly observations in our sample (with the exception of Cardano with 7,376 observations due to data being unavailable prior to 09:00 on 9 October 2007).

Insert Table 3 about here

[2] While considering an exceptionally broad number of products, we have incorporated a number of traditional financial markets in our descriptive statistics to act as a benchmark through which we can compare our selected cryptocurrency returns. These traditional financial assets are also utilised as control variables within the mean equations of the multivariate GARCH methodology used in Sections 4 and 5. We have selected GBP/USD to represent interactions between cryptocurrencies and broad currency markets, the S&P500 as a representation of stock market performance, both gold and oil (as measured by West Texas Intermediate, WTI oil markets) as a representation of commodity markets, and finally the VIX (CBOE volatility index) to represent options markets and implied volatility respectively. Our selected financial markets variables, sampled at 60-minute intervals, were collected from Thomson Reuters Tick History for the period from midnight on September 1st 2017 through midnight, the 10th of August 2018.

In Table 3 we have established a list of the seventeen largest cryptocurrency hacking events between September 2017 and August 2018. The list of hacking events includes a broad number of unique situations that targeted either the exchange on which cryptocurrencies trade, the blockchain supporting a specific cryptocurrency, or indeed the wallets of cryptocurrency investors. We have only included events that were determined as newsworthy if covered by any one of a number of mainstream international broadsheet newspapers as determined by a thorough search using the LexisNexis database. The largest estimated loss from such cryptocurrency theft occurred on the 9th of April 2018 when an alleged online scam, reportedly sourced in Vietnam, let to the generation of a false ICO led by the companies Ifan and Pincoin. The two firms are alleged to have misled approximately 32,000 investors and to have stolen in the region of $650 million. The scale of this theft dwarfed the estimated amounts lost throughout the majority of other included hacking events with the exception of the Coincheck hacking on the 26th of January 2018, when the exchange suspended all deposits in the cryptocurrency NEM due to a hack on their exchange which led to the theft of approximately $532.6 million. While these two particular events are particularly prevalent due to the scale of losses that were generated, a substantial number of cybercrime events have generated losses above $50 million. When compared to events of such scale, there are two particular hacking events that did not generate such substantial monetary losses, but were particularly disturbing due to the nature and ability of the criminals that had masterminded such thefts. In particular the $400,000 lost in Stellar on the 13th of January 2018 and the $900,000 lost on the 31st of January 2018 through the ICO of BeeToken. During the Stellar Lumen (XLM) hack, wallets hosted by Blackwallet.co were accessed without permission, where the hosting server had its settings changed remotely to allow code to run that would then send balances to wallets belonging to the hackers, leading to the decision to close the server in an attempt to mitigate the attack. In the latter event, the attackers targeted the BeeToken ICO with phishing attacks, leading to the theft of assets in Ethereum directly from investors who had been misled by false emails that appeared to have been sent by official sources.

4. Methodology

The development of the theoretical understanding of a relatively new financial product can often be associated with substantial conflicting evidence. The cryptocurrency asset class is no exception. However, much research continues to identify this asset class to contain exceptionally high levels of volatility when compared to more established counterparts (Corbet et al. [2018]). The source of this cryptocurrency market volatility is exceptionally important to identify, particularly as regulators, policy-markers and experts try to both value, regulate and decide on the future viability of the product. We therefore set out the three following stages of analysis. We first analyse the intraday volatility of our selected cryptocurrencies through a range of traditional methodologies. Next, we focus on stylised facts associated with cryptocurrencies in comparison to traditional financial markets, namely the existence of time-of-the-day effects and the transition of volatility behaviour during the opening hours of the exchanges on which traditional financial markets trade. It has been broadly identified (Corbet et al. [2018]; Gandal et al. [2018]; Griffins and Shams [2018]) that cybercriminality remains one of the key concerns[3] undermining the viability of digital currency at large as ‘the future of finance’. There are identified weaknesses both at the exchange-level, within the underlying technology and most disturbingly through the trading structures of these assets in the form of ‘spoofing’ and ‘pump-and-dumps’. Considering the identification of both volatility and non-volatility effects, we finally set out to establish as to whether cybercriminiality is indeed one of the main driving forces behind the volatility of cryptocurrencies. Further, we set out to establish as to whether cryptocurrency investors value varying types of cybercriminality in a differing manner.

4.1. Does the intra-day volatility of cryptocurrency markets change based on the time-of-the-day and when traditional financial markets close?

While we analyse the informational share that is transferred between traditional markets, cryptocurrency markets and indeed, within these sub-categories of financial market products, we further develop this analysis by investigating intra-day volatility. One of the key questions relating to cryptocurrencies as a financial product is based on their behaviour in correlation with the opening hours of traditional financial markets, and their behaviour when the same markets are closed. We have selected five markets as representative of our selected traditional financial markets: 1) GBP/USD; 2) VIX; 3) Gold; 4) the S&P500; and 5) Oil as measured by West Texas Intermediate. The first stage of our analysis therefore focuses on three distinct areas:

- H_1: Does the intra-day volatility of cryptocurrencies change significantly when traditional markets are closed?
- H_2: Does the intra-day volatility of cryptocurrencies change significantly at the weekend when compared to weekdays?
- H_3: Is there a difference in intra-day cryptocurrency volatility based on the opening hours of major international financial markets?

To analyse these specific hypotheses and to provide robustness within our selected framework, we utilise the work of Parkinson [1980], Garman and Klass [1980], Rogers and Satchell [1991] and Yang and Zhang [2000]. It is important to note that traditional financial markets have pre-determined

[3] The International Monetary Fund (IMF) have previously expressed their satisfaction with the development of the cryptocurrency industry and the benefits that are contained within its continued growth (An Even-handed Approach to Cryptocurrencies, IMF blogpost written by Christine Lagarde, Head of the International Monetary Fund, available at: https://blogs.imf.org/2018/04/16/an-even-handed-approach-to-crypto-assets/), the Securities and Exchange Commission (SEC) in 2018 have backtracked on earlier positivity to warn of the inherent potential for spoofing and other market manipulation techniques (US Securities and Exchange Commission, Public Statement, Statement on Potentially Unlawful Online Platforms for Trading Digital Assets, Available at: https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading)

opening and closing times, however, cryptocurrency markets do not. To create a comparative series that can be used for comparison, we define the opening and closing times of traditional markets as defined by the exchange. To test H_1, we analyse the volatility of cryptocurrency markets within the opening and closing times of our selected traditional financial markets. However, we identify midnight as the opening and closing time of each individual day for the purposes of calculation for cryptocurrencies when testing H_2 and H_3.

Parkinson [1980] utilised estimates of high and low prices to provide a concise volatility estimator. The diffusion constant characterising the random walk which is the same as the variance of the rate of return, is found to become an important quantity to calculate and was at this time traditionally estimated using closing prices only. However, one issue of this estimator was based on the assumption of continuous trading, which is effective for cryptocurrencies but not for traditional assets, which underestimates the volatility for potential movements in prices when markets are closed. The estimate is calculated as:

$$\text{Volatility}_{Park} = \sigma_p = \sqrt{\frac{F}{N}}\sqrt{\frac{1}{4\ln(2)}\sum_{i=1}^{N}\left(\ln(\frac{h_i}{l_i})\right)^2} \tag{1}$$

where F represents the number of trading days in year, N is the number of observations in the sample, h and l represent the high and low prices respectively and o and c represent the opening and closing prices respectively. Garman and Klass [1980] developed on the work of Parkinson [1980] through the use of opening and closing prices, with their estimate calculated as:

$$\text{Volatility}_{G-Klass} = \sigma_{GK} = \sqrt{\frac{F}{N}}\sqrt{\sum_{i=1}^{N}\frac{1}{2}\left(\ln(\frac{h_i}{l_i})\right)^2 - (2\ln(2)-1)\left(\ln(\frac{c_i}{o_i})\right)^2} \tag{2}$$

Rogers and Satchell [1991] developed on this work assuming that the average return is zero. Therefore, financial products that possess drift which denotes a non-zero mean, require a measure that incorporates such movement. However, this measure somewhat understated volatility due to its inability to incorporate jumps in volatility. Their research builds on a simple correction to overcome the error where this approximation of the true high and low values of the drifting Brownian motion by the high and low values of a random walk introduces an error that can be considered quite often to be serious enough to render the calculation as useless. It is calculated as:

$$\text{Volatility}_{Rogers} = \sigma_{RS} = \sqrt{\frac{F}{N}}\sqrt{\sum_{i=1}^{N}\ln(\frac{h_i}{c_i})\ln(\frac{h_i}{o_i}) + \ln(\frac{l_i}{c_i})\ln(\frac{l_i}{o_i})} \tag{3}$$

Yang-Zhang modified the Garman-Klass volatility measure to support jumps in the price of the series. The measure does assume a zero drift, hence it will overestimate the volatility if a security has a non-zero mean return. It is estimated as:

$$\text{Vol}_{GKY} = \sigma_{GKY} = \sqrt{\frac{F}{N}}\sqrt{\sum_{i=1}^{N}\left(\ln(\frac{o_i}{c_{i-1}})\right)^2 + \frac{1}{2}\left(\ln(\frac{h_i}{l_i})\right)^2 - (2\ln(2)-1)\left(\ln(\frac{c_i}{o_i})\right)^2} \tag{4}$$

Yang and Zhang [2000] developed further on this measure through the creation of a a volatility measure that handles both opening jumps and drift. It is the sum of the overnight volatility (close-to-open volatility) and a weighted average of the Rogers and Satchell [1991] volatility and the open-to-close volatility. They present a new volatility estimator that is unbiased in the continuous limit, independent of the drift and consistent in dealing with opening price jumps. Further, it has the smallest variance among all estimators with similar properties. The assumption of continuous prices does mean the measure tends to slightly underestimate the volatility[4].

$$\text{Volatility}_{Yang-Z} = \sigma_{YZ} = \sqrt{F}\sqrt{\sigma^2_{\text{o/n Vol}} + k\sigma^2_{\text{op-cl Vol}} + (1-k)\sigma^2_{RS}} \tag{5}$$

Overall, Parkinson [1980] generated a measure utilising high and low prices that cannot handle drift or overnight jumps in prices. Garman and Klass [1980] were the first to utilise both high and low, and opening and closing prices but could not provide a methodology that could effectively account for drift in prices and overnight jumps. Rogers and Satchell [1991] provided a measure that used both high and low, and opening and closing prices to provide a measure that can hand drift but not overnight jumps, while Yang and Zhang [2000] generated a measure that can handle both drift and overnight jumps. We develop on the work of Parkinson [1980], Garman and Klass [1980], Rogers and Satchell [1991] and Yang and Zhang [2000] to test the listed hypotheses. To test H_{NUM}, we present the results of our analysis sub-divided between the opening and closing times of our selected traditional markets. To test H_{NUM}, we sub-divide the analysis and compare results for cryptocurrency markets between week-days and the weekend. Finally, to test H_{NUM}, we sub-divide our analysis based on the opening hours (as based on GMT) of Japanese stock markets as represented by the Tokyo Stock Exchange (00:00 to 06:00 GMT), Chinese financial markets as represented by the Shanghai and Shenzen Stock Exchanges (open between 01:30 and 07:00), European and United Kingdom financial markets as represented by the Euronext Paris, Frankfurt Stock Exchange and London Stock Exchange respectively (all open between 08:00 to 16:30 GMT) and United States financial markets as represented by the New York Stock Exchange (14:30 to 21:00 GMT). Adjustments are made throughout for the international implementation of daylight savings time.

[4] In the calculation of the estimate provided by Yang and Zhang [2000], we must note that $k = \frac{0.34}{1.34+(\frac{N+1}{N-1})}$. Further, we calcuate overnight volatility and open to close volatility as $\sigma^2_{\text{o/n Vol}} = \frac{1}{N-1}\sum_{i=1}^{N}\left[\ln(\frac{o_i}{c_{i-1}} - \overline{\ln(\frac{o_i}{c_{i-1}})}\right]^2$ and $\sigma^2_{\text{op-cl Vol}} = \frac{1}{N-1}\sum_{i=1}^{N}\left[\ln(\frac{c_i}{o_i} - \overline{\ln(\frac{c_i}{o_i})}\right]^2$ respectively.

4.2. Cryptocurrency market volatility due to opening hours and traditional market volatility

The second stage of our analysis builds upon a multivariate GARCH(1,1) methodology to identify as to whether there exists volatility in the largest cryptocurrency markets due to the hour-of-the-day in which trading takes place. Further, we investigate as to whether cryptocurrency volatility has been influenced by periods of substantial volatility in traditional financial markets. We therefore identify two further hypotheses:

- H_4: Does cryptocurrency market volatility change substantially based on the hour-of-the-day in which trading takes place?
- H_5: Has cryptocurrency volatility varied substantially during periods of traditional market volatility?

The GARCH specification was developed byBollerslev [1986] and was designed to include lagged conditional variance terms as autoregressive terms. The general GARCH (p,q) model has the following form:

$$R_t = a + b\prime X_t + \varepsilon_t, \text{ where } \varepsilon_t|\Omega_t \sim iidN(0, h_t) \tag{6}$$

$$h_t = \omega + \Sigma_{i=1}^{p} \alpha_i h_{t-i} + +\Sigma_{j=1}^{q} \beta_j \varepsilon_{t-j}^2 \tag{7}$$

which states that the value of the variance scaling parameter h_t now depends both on the past value of the shocks, which are captured by the lagged square residual terms, and on past values of itself, which are captured by the lagged h_t terms. Specification tests found that the GARCH(1,1) model served as the best fitting to estimate volatility effects through the use of dummy variables that are used to denote both the time-of-the-day and also periods of substantial traditional market volatility. It is also necessary to mitigate international effects which can be completed through the inclusion of the returns of traditional financial products in the mean equation of the GARCH(1,1) methodology. The volatility sourced in shocks that are incorporated in the returns of traditional financial markets are therefore considered in the volatility estimation of the selected structure. The GARCH(1,1) methodology used to investigate H_4 has the following form:

$$R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 \pounds/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + \varepsilon_t \tag{8}$$

$$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{24} D_{ToD_i} \tag{9}$$

R_{t-j} represents the lagged value of cryptocurrency returns, n hours before R_t is observed. $b_2\pounds/\$_t$ represents the interaction between the selected cryptocurrency returns and $\pounds/\$$, while b_3VIX_t

represents the value of the VIX in the hour that the estimate R_t was observed. Finally, $b_5S\&P_t$ and b_6Oil represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through West Texas Intermediate (WTI) respectively. $\sum_{i=1}^{24} D_{ToD}$ is included in the variance equation to provide a coefficient relating to specific hour in which trading has taken place for each of our investigated cryptocurrencies. Bollerslev [1986] showed that restrictions on the parameters for positivity, $\omega > 0$, $\alpha \geq 0$ and $\beta \geq 0$, and the wide-sense stationarity condition, $\alpha+\beta < 1$. Nelson [1990] proved that the GARCH (1,1) process is uniquely stationary if $E[log(\beta+\alpha\epsilon_t^2)] < 0$, where Bougerol and Picard [1992] generalise this for any GARCH (p,q) order model. Bollerslev [1986] also proved that if the fourth order moment exists, then the model can handle leptokurtosis.

H_5 investigates as to whether cryptocurrency volatility varied substantially during periods of traditional market volatility? While a number of other recent works focus on the presence of dynamic relationships between traditional financial markets and cryptocurrencies (Corbet et al. [2018]; Tiwari et al. [2018]; Urquhart [2017]), we set out to analyse as to whether the structure of cryptocurrency volatility presents evidence of substantial change as traditional financial market volatility conditions change. We therefore build on the above GARCH(1,1) methodology through the use of the adapted variance equation:

$$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{4} D_{vol_i} \tag{10}$$

where $\sum_{i=1}^{4} D_{vol_i}$ develops on a dummy variable that is established based on the quartile of volatility that has been experienced in the markets for GBP/USD, VIX, S&P500, gold and oil separately. Quartile 1 represents the denoted lowest estimates of volatility in each of the analysed markets, while quartile 4 denotes the highest estimates of volatility.

4.3. Cryptocurrency market volatility due to hacking events: A multivariate GARCH analysis

We have selected three areas of investigation on which to focus our analysis of the effects of cybercriminality on cryptocurrency markets. First, we focus on the direct volatility changes through the use of a multivariate GARCH analysis to investigate and identify the presence of differing pricing behaviour in the period immediately after cybercrime events. Secondly, due to the large amount of research focusing on the comovement of asset prices during periods of great stress and crises (Forbes and Rigobon [2002]), we use a DCC-GARCH analysis to analyse changing correlations between cryptocurrencies, while incorporating methodological ‘learning’ through the inclusion of variables representing traditional financial market products and dummy variables relating to cybercriminality in cryptocurrency markets. Finally, we investigate changes in the flow of information between cryptocurrencies in the period before and after major cybercriminality events. To do so we build on the work of Hasbrouck [1995] and Gonzalo and Granger [1995] to analyse the information share, the component share and the information leadership share of price discovery between cryptocurrencies. We therefore set out to analyse our final three hypotheses which investigate:

- H_6: Does cryptocurrency market volatility change substantially in the aftermath of cybercriminality?
- H_7: Does such cryptocurrency volatility vary by severity of cybercriminality event?
- H_8: Do the conditional correlations between cryptocurrency markets change substantially in the aftermath of cybercriminality events?
- H_9: Does the information share and component share of price discovery change between the periods before and after cybercrime events in cryptocurrency markets?

4.3.1. Cryptocurrency market volatility due to hacking events: A multivariate GARCH analysis

We utilise a multivariate GARCH(1,1) methodology to obtain volatility changes in the immediate aftermath of a major cybercrime incident relating to cryptocurrency markets. The GARCH specification was developed by Bollerslev [1986]. Specification tests found that the GARCH (1,1) model served as the best fitting to estimate volatility effects after industrial incidents for publicly traded companies. It is also necessary to mitigate international effects which can be completed through the inclusion of the returns of traditional financial products in the mean equation of the GARCH(1,1) methodology. The volatility sourced in shocks that are incorporated in the returns of traditional financial markets are therefore considered in the volatility estimation of the selected structure. Dummy variables are used in the variance equation denoted as unity in the first one hundred and twenty hours (five days) after the cybercrime incident and zero otherwise. The lagged cryptocurrency returns for the five preceding hours were found to provide explanatory significance and are therefore included in the mean equation. The GARCH (1,1) methodology used in this study has the following form:

$$R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 \pounds/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + b_7 Bit_t + \varepsilon_t \tag{11}$$

$$\varepsilon_t | \Omega_t \sim iidN(0, h_t) \tag{12}$$

$$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{17} D_i \tag{13}$$

R_{t-j} represents the lagged value of cryptocurrency returns, n hours before R_t is observed. $b_2 \pounds/\$_t$ represents the interaction between the selected cryptocurrency returns and £/\$, while $b_3 VIX_t$ represents the value of the VIX in the hour that the estimate R_t was observed. Finally, $b_5 S\&P_t$ and $b_6 Oil$ represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through the West Texas Intermediate (WTI). $b_7 Bit_t$ represents the returns of

Bitcoin to incorporate cryptocurrency market dynamics, however, in the methodology investigating Bitcoin specifically, b_7 is set to zero. $\sum_{i=1}^{17} D_i$ is included in the variance equation to provide a coefficient relating to the included seventeen dummy variables listed in Table 6. Bollerslev [1986] argue for restrictions on the parameters for positivity, $\omega > 0$, $\alpha \geq 0$ and $\beta \geq 0$, and the wide-sense stationarity condition, $\alpha + \beta < 1$. Nelson [1990] proved that the GARCH (1,1) process is uniquely stationary if $E[log(\beta + \alpha\epsilon_t^2)] < 0$, where Bougerol and Picard [1992] generalise this for any GARCH (p,q) order model. Bollerslev [1986] also proved that if the fourth order moment exists, then the model can handle leptokurtosis.

4.3.2. Cryptocurrency market behaviour during hacking events: A DCC-GARCH analysis

Using a multivariate GARCH analysis to analyse the changes in cryptocurrency volatility due to cybercriminality is a very useful starting point. We then investigate as to whether there has been a significant increase in the comovement of high frequency cryptocurrency returns. Significant increases in the comovement and correlation of returns in traditional financial markets have been widely observed in periods of sharp financial crises. Forbes and Rigobon [2002] found that correlation coefficients are conditional on market volatility as they investigated stock market comovements during the 1997 Asian crisis, the 1994 Mexican devaluation, and the 1987 U.S. market crash. Further evidence was provided by Baig and Goldfajn [1999] through the use of dummy variables that controlled for domestic news to find cross-border contagion in currency and stock markets. A number of explanations for such comovements have been provided, such as trade between countries (Glick and Rose [1999]) and interconnectedness of the banking sector (Kaminsky and Reinhart [2000]); neither of which present an adequate explanation to any identified behaviour in cryptocurrency markets. We first test for the presence of such comovements in cryptocurrency markets and then specifically investigate their responses during cybercrime events using a DCC-GARCH methodology[5].

When specifying the form of the conditional correlation matrix R_t, two requirements have to be considered. The first is that the covariance matrix H_t has to be positive and the second is that all the elements in the conditional correlation matrix R_t have to be equal or less than unity. The DCC model is estimated by using a two-step approach to maximise the log-likelihood function. If we let θ denote the parameters in D_t and ϑ, the parameters in R_t, then the log-likelihood is:

$$l_t(\theta, \vartheta) = \left[-\frac{1}{2}\Sigma_{t=1}^{T} nlog(2\pi) + log\left|D_t\right|^2 + \varepsilon_t^{'} D_t^{-2} \varepsilon t\right] + \left[\Sigma_{t=1}^{T} log\left|R_t\right| z_t^{'} R_t^{-1} z_t - z_t^{'} z_t\right] \tag{14}$$

[5] As proposed by Engle (2002), the DCC-GARCH model is designed to allow for a two-stage estimation of the conditional variance matrix h_t. In the first stage, univariate GARCH (1,1) volatility models are fitted for each of the stock return residuals and estimates of $\sqrt{h_{it}}$ are obtained. In the second stage, stock return residuals are transformed by their estimated standard deviations from the first stage as $z_{it} = \frac{\epsilon_{it}}{\sqrt{h_{it}}}$. Finally, the standardised residual z_{it} is used to estimate the correlation parameters.

The first part of the log likelihood function is volatility, which is the sum of the individual GARCH likelihoods. The log-likelihood function can be maximised in the first stage over the parameters D_t. Given the estimated parameters in the first stage, the correlation component of the likelihood function in the second stage is maximised to estimate the correlation coefficients. Finally, we examine the DCC-GARCH model's change in behaviour before and after cybercriminality in cryptocurrency markets occur. In a first stage analysis, we estimate the impact of external shocks on the dynamic conditional correlation features. We regress the time-varying correlation model as follows:

$$\rho_{ij,t} = \omega_{ij} + \Sigma_{p=1}^{p} \varphi_p \rho_{ij,t-p} + \Sigma_{k=1}^{2} \alpha_k DM_{k,t} + \varepsilon_{ij,t} \tag{15}$$

where $\rho_{ij,t}$ is the pair-wise conditional correlation coefficient between the cryptocurrency i and cryptocurrency j. DM_1 is a dummy variable denoting the date of the cybercrime incident. The value of the dummy variables are set equal to unity for the period after the cybercrime incident and zero otherwise. The conditional variance equation is assumed to follow a GARCH(1,1) specification including a dummy variable identifying the exact hour of the incident, $DM_k(k = 1)$:

$$h_{i,t} = A_0 + A_1 \varepsilon_{t-1}^2 + B_1 h_{i,t-1} + \Sigma_{k=1}^{2} d_k DM_{k,t} \tag{16}$$

where $A_0 > 0$, $A_1 \geq 0$, $B_1 \geq 0$ and $A_1 + B_1 < 1$. In the mean equation, the coefficient d_1 is statistically significant in all the incidents investigated. We use both the Akaike Information Criterion (AIC) and the Schwarz Bayesian Information Criterion (SBIC) to determine the appropriate lag length.

4.3.3. Information share and component share of price discovery before and after hacking events

There are two standard measures of price discovery commonly employed in the literature: the Hasbrouck [1995] Information Share (IS) and the Gonzalo and Granger [1995] Component Share (CS) approach. Hasbrouck [1995] demonstrates that the contribution of a price series to price discovery (the 'Information Share') can be measured by the proportion of the variance in the common efficient price innovations that is explained by innovations in that price series. Gonzalo and Granger [1995] decompose a cointegrated price series into a permanent component and a temporary component using error correction coefficients. The permanent component is interpreted as the common efficient price, the temporary component reflects deviations from the efficient price caused by trading fractions. We estimate IS and CS, as developed by Hauptfleisch et al. [2016] using the error correction parameters and variance-covariance of the error terms from the Vector Error Correction Model (VECM):

$$\Delta_{p1,t} = \alpha_1 (p_{1,t-1} - p_{2,t-1}) + \sum_{i=1}^{200} \gamma_i \Delta p_{1,t-i} + \sum_{j=1}^{200} \delta_j \Delta p_{2,t-j} + \varepsilon_{1,t} \tag{17}$$

$$\Delta_{p2,t} = \alpha_2(p_{1,t-1} - p_{2,t-1}) + \sum_{k=1}^{200} \varphi_k \Delta p_{1,t-k} + \sum_{m=1}^{200} \phi_m \Delta p_{2,t-m} + \varepsilon_{2,t} \tag{18}$$

where $\Delta p_{i,t}$ is the change in the log price $(p_{i,t})$ of the asset traded in market i at time t. The next stage is to obtain the component shares from the normalised orthogonal vector of error correction coefficients, therefore:

$$CS_1 = \gamma_1 = \frac{\alpha_2}{\alpha_2 - \alpha_1}; CS_2 = \gamma_2 = \frac{\alpha_1}{\alpha_1 - \alpha_2} \tag{19}$$

Given the covariance matrix of the reduced form VECM error terms [6] where:

$$M = \begin{pmatrix} m_{11} & 0 \\ m_{12} & m_{22} \end{pmatrix} = \begin{pmatrix} \sigma_1 & 0 \\ \rho\sigma_2 & \sigma_2(1-\rho^2)^{\frac{1}{2}} \end{pmatrix} \tag{20}$$

we calculate the IS using:

$$IS_1 = \frac{(\gamma_1 m_{11} + \gamma_2 m_{12})^2}{(\gamma_1 m_{11} + \gamma_2 m_{12})^2 + (\gamma_2 m_{22})^2} \tag{21}$$

$$IS_2 = \frac{(\gamma_2 m_{22})^2}{(\gamma_1 m_{11} + \gamma_2 m_{12})^2 + (\gamma_2 m_{22})^2} \tag{22}$$

Recent studies show that IS and CS are sensitive to the relative level of noise in each market, they measure a combination of leadership in impounding new information and the relative level of noise in the price series from each market. The measures tend to overstate the price discovery contribution of the less noisy market. An appropriate combination of IS and CS cancels out dependence on noise, Yan and Zivot [2010]; Putniņš [2013]. The combined measure is known as the Information Leadership Share (ILS) which is calculated as:

$$ILS_1 = \frac{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right|}{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right| + \left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|} \text{ and } ILS_2 = \frac{\left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|}{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right| + \left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|} \tag{23}$$

5. Results

During the short amount of time in which cryptocurrencies have existed, we have witnessed many astonishing price variations have been observed, along with broad structural changes and substantial illegality. We continue to develop our understanding of these young products throughout their development. We first focus on the key hypotheses that analyse the stylised facts surrounding the pricing of cryptocurrencies in comparison to other traditional financial markets. We then

[6] $\Omega = \begin{pmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix}$ and its Cholesky factorisation, $\Omega = MM'$.

investigate the effects of broad cybercriminality, both within the products and the exchanges on which cryptocurrencies trade. The issues continue to damage both the reputation and credentials of the market at large, and have continued to evolve in both scale and sophistication.

5.1. Does cryptocurrency volatility change due to the opening times of traditional financial markets?

In the following sections we first consider Hypotheses H_1 through H_3 which investigate the stylised facts relating to intra-day volatility based on when traditional markets are open or closed, whether it is a weekday or the weekend, or indeed, based on the opening hours of the main traditional exchanges. Hypothesis H_1 is analysed in Table 4, while observing the results of the four selected intra-day volatility measures, we can identify that there are a wide range of outcomes. While calculating the averages of the volatility measures, cryptocurrency markets appear to be most volatile while the VIX and gold markets are open (an average rank of 1.6 and 1.8 respectively). The market for GBP/USD, while open, presents the next most volatile time period for cryptocurrency markets with the S&P500 and Oil market opening times reflecting the least volatile in comparison. As previously identified, the Garman-Klass indicator presents the broadest range of outcomes in comparison to the other comparable measures. These results are quite pronounced in the market for Bitcoin, where average intra-day volatility while the gold market is open is 0.47%. However, these is little intra-day volatility difference during the opening hours of the S&P500 and Oil markets. Bitcoin Cash, while representing a product with a shorter life span, present evidence of a intra-day volatility reduction while both Gold and the S&P500 is trading. These findings are robust across measures. The largest average result is identified in the market for Stellar (1.51%) while gold markets are open. It is important to observe that while there are clear differences identified between the investigated cryptocurrency markets, there are also substantial and significant differences in intra-day volatility depending on the operational trading hours investigated. However, despite this, the variation between the individual markets do not correlate across all eight of the investigated markets, therefore, although we can state that on average there are substantial differences based on differing opening times, we cannot definitively state that this is the same for all cryptocurrencies. On this occasion, we can therefore reject H_1.

Insert Table 4 about here

In Table 5 we present the results of the analysis of hypothesis H_2 which investigates the difference between the intra-day volatility of cryptocurrency markets dependent on whether it is a weekday or the weekend. Across all measures analysed, we find clear evidence that accepts H_2, that first of all, that there is a clear difference weekend effect in cryptocurrency markets, but also there is evidence of elevated intra-day volatility during the week and a substantial reduction at the weekend. This is found to significantly support of hypothesis H_2. We must note again that cryptocurrency markets are open twenty-four hours a day, seven days per week, whereas traditional markets have structured opening and closing times.

Insert Table 5 about here

The final analysis of intra-day volatility investigates as to whether cryptocurrency markets present evidence of differing volatility depending on the international exchange that is open. Table 6 presents the results based on hypothesis H_3. This analysis presents some very interesting results. intra-day volatility is found to be substantially elevated while both European and United States financial markets are trading with the exception of Cardano during European opening and Ripple, Bitcoin Cash and Cardano during United States opening. However, cryptocurrency volatility is broadly below average during both Japanese and Chinese trading times with the exception of results for Stellar, and again, Bitcoin Cash and Cardano. This presents evidence supporting the hypothesis that cryptocurrency intra-day volatility behaves in a different manner depending on the exchange that is open.

Insert Table 6 about here

While we observe this evidence of contrasting intra-day volatility during Asian, American and European market opening times, it is also important to investigate hour-of-the-day effects as we do throughout the investigation of H_4 with results presented in Table 7. In this analysis, we investigate the hourly trading volatility of each of our eight investigated cryptocurrencies using a multivariate GARCH analysis. There is evidence of a significant increase in volatility in the markets for Bitcoin, Ethereum, Ripple and Cardano at 11:00am GMT. In the largest market by market capitalisation, Bitcoin, there are only two hours of elevated volatility at 06:00am and 11:00am GMT, with only the latter observation being significant. In the markets for Bitcoin Cash and Stellar, there are no significant periods of elevated volatility throughout the day indicating no abnormalities. The markets for Ripple and Cardano present evidence of elevated and significant volatility after 08:00am until midday GMT. Despite a number of alternative specifications and differing frequencies of investigation, there are a number of differing times where individual cryptocurrencies exhibit elevated levels of GARCH-calculated volatility, but there is no evidence to support hypothesis H_4 across the cryptocurrency markets investigated.

Insert Table 7 about here

5.2. How has cryptocurrency volatility been affected by traditional financial market volatility?

While we have observed that there do exist clear differences in intra-day volatility between weekdays and the weekend in cryptocurrency markets with further support that differing volatility based on the exchange that is open (with American and European opening times exhibiting substantially more volatility than Chinese and Japanese opening hours). In this section, we need to investigate as to whether cryptocurrency volatility exhibits differing volatility behaviour during episodes of substantial volatility in traditional financial markets? We therefore investigate H_5 in Table 8, which is supported further by the following DCC-GARCH analysis investigating volatility transfers.

Insert Table 8 about here

We observe several interesting results through this analysis of volatility. With the exception of Cardano, there are few significant relationships identified between individual cryptocurrency markets and differing periods of low throughout high volatility in the markets for VIX, the S&P500 and gold. It must be noted that with the exception of the relationship between Cardano and the VIX, all differential between high and low differential GARCH-calculated volatility and positive despite this lack of confidence. However, we clearly observe some very strong interactions and behavioural differentials between our selected cryptocurrency markets and both the market for oil and GBP/USD. High volatility periods are associated with a significant increase in volatility in the markets for Bitcoin, Ethereum, Litecoin, Monero and Cardano, whereas there are few interactions between the selected variables and periods of low and below-average volatility periods. The scale of such volatility differentials are largest in the markets for Bitcoin, Litecoin and Cardano. The relationship between the volatility differentials in the market for GBP/USD and cryptocurrencies are far more pronounced. The largest significant differentials are identified in the markets for Bitcoin and Bitcoin Cash, with further significant positive volatility differentials identified in the markets for Ethereum and Monero.

Therefore, we can accept H_5 through the presentation of such evidence indicating that periods denoted to contain substantial volatility in the markets oil and GBP/USD are also associated with sharp, significant increases in the volatility of cryptocurrency markets. This would indicate that the transfer of news and sentiment that would effect GBP/USD and oil markets are capable of generating significant volatility in cryptocurrency markets, providing further evidence of the continued evolution of these young products and exchanges.

5.3. Has the style and scale of cybercriminality directly influenced the volatility of cryptocurrencies?

After identifying a number of stylised facts surrounding the intra-day volatility of cryptocurrency markets and the interactions with volatility in traditional financial markets, we next set out to establish the source of this volatility. During the relatively short time in which cryptocurrencies have existed, there have been numerous episodes of significant cybercriminality that have damaged both the reputation and credibility of both individual cryptocurrencies and the broader exchanges on which they trade. It is important that we investigate the differing behaviour of cryptocurrency investors in the periods both before and after such incidents. Our analysis first sets out to investigate broad volatility changes and the transfer of volatility in the aftermath of cybercriminality. While the second stage investigates changes in the information content of such pricing has changed due to such an event.

5.3.1. What price volatility dynamics exist in the aftermath of cryptocurrency cybercriminality?

The first stage of our analysis investigates the changes in the volatility dynamics of our selected cryptocurrencies in the periods before and after cybercrime events. We investigate H_6 which analyses as to whether there is a substantial change in cryptocurrency volatility in the period after cybercriminality. We focus on the direct volatility change using a multivariate-GARCH analysis, but also focus on the change in dynamic correlations though the use of a DCC-GARCH methodology. The multivariate-GARCH methodology, of which our results are presented in Table 9, is predicated on three sources of information, the incorporation of past information as incorporated through lagged cryptocurrency returns. Further,Table 10 provides robustness through the estimation of GARCH caluclated volatility throughout the entire period in which we can denote episodes of cybercriminality. We observe that lagged returns are significant in all of our investigated cryptocurrencies with the exception of Ethereum. International effects are incorporated in the multivariate-GARCH methodology through the inclusion of the traditional assets: GBP/USD, VIX, gold, S&P500 and oil. As the most widely renowned and market leading cryptocurrency in terms of market valuation, Bitcoin is used as a control variable in the analysis of our selected cryptocurrencies with the exception of the methodology relating to Bitcoin itself. We observe that there is a strong significant and positive relationship between Bitcoin and our investigated cryptocurrencies, with the exception of Bitcoin and both Stellar (+0.1717) and Cardano (+0.0424). While Bitcoin presents positive relationships with the returns of the traditional assets with the exception of oil, it is very much similar to the market relationships found in Ripple. However, in comparison to the other large capitalisation cryptocurrencies, both Ethereum and Litecoin presents mostly negative relationships with traditional assets. The relationships of those cryptocurrencies with both medium and low market capitalisation is broadly non-standard, with uniformly positive relationships identified with the VIX and Bitcoin. The cumulative ARCH and GARCH coefficients are found to be below unity and are significant at the 1% level throughout all individual methodologies.

Insert Tables 9 and 10 about here

While there are multiple differing responses, there appears to be no significantly uniform responses across all markets investigated which indicates that all markets have differing volatility responses to the investigated cybercrime events. However, there are broad responses for hack 4, 7, 8, 10, 14 and 15. Hack 4 and 15 are related to a cybercrime event within an exchange (Coincheck and Coinrail respectively), which traded a broad number of cryptocurrencies therefore presenting a theoretically plausible influence across a broad number of products. Hack 7, 8, 10 and 14 are associated to scam and cybercriminality that has taken place at the time of an ICO. Such results indicate that there are broad differences in the volatility responses of cryptocurrencies with evidence supporting significant instability generated within attacks on exchanges and ICO-fraud, both of which can be observed to be heavily dependent on perceptions of stability and financial safety. Any threat to such stability is found to lead widespread responses across a large number of cryptocurrencies rather than at the individual level. There is also evidence of cryptocurrency-specific volatility based on the market that has been directly targeted by such cybercrime. Such evidence is identified in the market for Bitcoin in hack 3 (+0.0033), hack 4 (-0.0031) and hack 11 (-0.0027) and for Ethereum during hack 8 (0.0033). The remaining hacks are found to be quite geographically-specific and product-specific, relating to cryptocurrencies that are not included in our selection due to a number of factors including data availability and illiquidity.

Insert Table 11 about here

To analyse H_7, which investigates as to whether the severity of each incident is related to the level of volatility that is incurred, use dummy variables that represent the time period at which the stated hack in Table 6 occurs. Within this methodology, we incorporate the estimated dollar value lost during the cybercrime event. Results are presented using a continuous dummy variable denoting the scale of the loss in each market investigated. In Table 11, we observe that four markets present significant evidence denoting that volatility is correlated with the size of the cybercriminality event (Bitcoin, Litecoin, Ripple and Monero). It must be noted that although the results of four markets remain insignificant, all results are positive throughout this analysis, with Cardano presenting evidence of a substantial positive relationship between the dollar-valued scale of cybercriminality and GARCH-calculated volatility measure.

5.3.2. Do the conditional correlations between cryptocurrency markets change substantially in the aftermath of cybercriminality events?

We next analyse the dynamic correlations between our selected cryptocurrencies using a DCC-GARCH methodology to investigate H_8, investigating as to whether such dynamic correlations change after cybercrime events. Our results are denoted in Table 12 and are further presented graphically in Figure 1. In Table 12, we observe the average dynamic correlation between each cryptocurrency pair included in our sample. The highest cross-cryptocurrency correlations identified are based on the relationships between Litecoin and Bitcoin, Litecoin and Ethereum, Ripple and Ethereum, Monero and Ethereum, Ripple and Ethereum, Monero and Litecoin, Bitcoin Cash and Litecoin, Monero and Ripple, and finally, Bitcoin Cash and Monero (all estimates are calculated as +0.0002). We then provide the estimates of the same dynamic corrlation relationship in the period surrounding each hacking event. There are a number of very interesting results presented in this analysis. First, we observe that there are lower estimates identified for smaller capitalisation cryptocurrencies when compared to the cross-correlations between their larger counterparts. This holds true not only for the dynamic correlations between smaller cyrptocurrencies themselves, but also for the relationships between smaller and larger cryptocurrencies. Secondly, we can identify two specific periods where there is a sustained increase in cross-cryptocurrency correlations as controlled for each hacking event. We identify the largest sustained increase in cross-cryptocurrency correlations at the time of hack 3 through hack 5 (6th of December 2017 through 13th of January 2018). Peak cross-correlations occur during hack 4 (18th of December 2017). These events coincide with the service breach and hacking of Nicehash, the bankrupcy of Youbit due to an external hack, and the DNS hijacking of Blackwallet.co resulting in the remote theft of $400,000 in Stellar Lumer (XLM). The combined losses from these three events is approximately $103.4 million, which is less than some individual hacking events. Further, in some relationships, the elevated cross-correlations last beyond the time of hack 6 which represents the second largest loss of investor's capital ($532.6 million in NEM) which represents the largest specific hacking event in our sample. However, it would appear that the sustained internationally relayed coverage of the four events led to a substantial loss of confidence in cryptocurrency market during this time, which is reflected in the broad cross-correlations of both the largest and smallest cryptocurrencies alike. Overall, we can accept hypotheses H_8.

Insert Table 12 about here

The second distinct phase of elevated cross-correlations occurs during hack 12 through 13, representing the period between the 4th of March 2018 and the 9th of April 2018 linked with the theft of approximately $300 million during the multi-level-marketing scheme created by GainBitcoin and the ICO scam inspired by Ifan and Pincoin that resulted in the loss of $650 million. Figure 1 further supports these results, with evidence of the spikes in cross-cryptocurrency correlations clearly coinciding with the timing of our selected hacking events as denoted by the grey-shaded time periods. Interestingly, there are two specific periods throughout the majority of the cross-cryptocurrency relationships that also results in elevated correlations. The first at approximately 13:00 on the 5th of September 2017, while during a period of elevated correlations strongly linked to hack 11, there is a further sharp increase in correlations throughout the night of the 18th of March 2018 and the days thereafter. The former event appears to occur at the same time as the first time that Bitcoin fell below $4,400 in a significant sell-off which generated substantial fear throughout the entire cryptocurrency sector, while the latter event occurs in the midst of two significant announcements. The first was the decision by Google to ban cryptocurrency advertisement, indicating that even legitimate companies would not be able to advertise their services in a similar manner to a decision already made by Facebook. The second significant news event which generated such broad cryptocurrency comovement surrounded the thwarted theft on the Binance exchange, where hackers had manipulated the market before attempting to cash out. The attack was not successful, therefore, it is not included as one of our cybercrime events. Further, the exchange offered $250,000 for information that could lead to the arrest of the hackers and put aside $10 million in a pool for future bounty rewards to mitigate such attacks.

While considering the results of the above DCC-GARCH analysis, we must briefly take the relationships between our selected cryptocurrencies into account. Bitcoin and Litecoin are identical in structure as peer-to-peer networks, therefore it would not be unreasonable to expect some similarities in the volatility responses in these cryptocurrencies as investor's observe their structure, dynamics and response mechanism to shocks in a similar manner. Cardano runs on smart contracts in the same manner as Ethereum[7]. Stellar is an open-source, decentralised protocol for digital currency to fiat currency transfers which allows cross-border transactions between any pair of currencies. It shares similar characteristics with Ripple, and in fact was created by the same person who founded the Mt. Gox exchange and co-founded Ripple (Jed McCaleb). Monero is found to be in relative isolation when compared to the other seven of our selected cryptocurrencies as it uses a Proof of Work mechanism to issue new coins and incentivise miners to secure the network and validate transactions through an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount or destination. These contrasting characteristics and interlinkages in design add further supportive to differing results that are identified.

Insert Figure 1 about here

The combination of the above multivariate GARCH and DCC-GARCH analysis presents a number of interesting observations. Primarily, we can identify that there are sharp volatility responses in cryptocurrency markets during cybercrime events, which appear to be rationally targeted at cryptocurrencies directly involved and the broader sector of cryptocurrencies should the cybercrime event be systemically damaging. This is particularly evident during cybercrime events relating to theft directly based on wallets which proponents state is one of the key safety features of virtual currencies, and attacks on cryptocurrency exchanges that trade multiple cryptocurrencies. Further, we find evidence of broad comovement in cryptocurrency markets during periods of extreme stress and severe reputational damage which supports the hypotheses that these relatively youthful markets have developed to act somewhat similarly to traditional financial assets in time of crises.

5.3.3. Does the information share and component share of price discover change between the periods before and after cybercrime events in cryptocurrency markets?

Developing from the volatility which can be attributed to our selected hacking events and the dynamic conditional correlations between the cryptocurrency cross-pairs, we calculate the compo-

[7] Smart contracts have been found to mitigate informational asymmetry and improve welfare and consumer surplus through enhanced entry and competition, yet distributing information during consensus generation may encourage greater collusion (Cong and He [2019])

nent share, information share and information leadership to uncover the key components of price discovery. This final stage of our analysis specifically investigates as to whether this information share and component share of information changes substantially after cybercriminality, denoted as hypothesis H_9. These measures provide information based on the contribution of each asset to price discovery which can be explained by the proportion of variance in the common efficient price innovations. We then proceed to map the changes in the individual components of price discovery as set out through heat-maps presented in Figures 2, 3 and 4, which portray heat-maps representing the information share, the information leadership share and the component share of price discovery respectively.

Insert Figures 2, 3 and 4 about here

While focusing on the largest changes in information share in Figure 2, we can clearly identify that there are a number of individual changes in relationships during the cyrbercrime event analysed. For example, hack 1 relating to the $280 million theft of Ethereum generates a response in the relationship between Ethereum and that of Stellar (+0.17), Bitcoin Cash (+0.13) and Monero (+0.16). Similar relationships are identified for hack 15, 16 and 17 with differing responses observed in the change of information share between high market capitalisation cryptocurrencies such as Bitcoin, Ethereum, Litecoin and Ripple, which present evidence of increased values. Whereas low market capitalisation cryptocurrencies such as Stellar, Cardano, Bitcoin Cash and Monero present evidence of much sharper changes in informational flows during these cybercrime events. However, sharper responses are identified for the same cybercrime events when analysing the information leadership share (Figure 3) and component share (Figure 4) of price discovery, where further distinct differences can be observed based on the market capitalisation of our selected cryptocurrencies. Evidence is presented of Bitcoin's prominent position in the cyrptocurrency asset class throughout these hacks as identified in the substantial shifts in information flows in the periods before and after these cybercrime events. These distinct differences in our information measures are of particular interest; information share demonstrates the contribution of a price series to price discovery which can be measured by the proportion of the variance in the common efficient price innovations while the component share presents the permanent and temporary components of price discovery, therefore the common efficient price and the efficient price caused by trading fractions. There is evidence to suggest that cybercriminality can distort these pricing relationships and can also influence large and small cryptocurrencies in a different manner.

There is further evidence of differing responses based on the size of the cryptocurrencies analysed during hacks relating to cybercrime fraud. Such evidence is provided for hack 10 and 13 which represent the release of news in February 2018 relating to a Ukrainian phishing network responsible for the theft of a reported $50 million and the theft of approximately $650 million in an ICO scam in Vietnam. Both events led to broad decreases in information share between Bitcoin and other high capitalisation cryptocurrencies, but decreases between Bitcoin and low capitalisation cryptocurrencies. However, the same information share relationship increases between smaller cryptocurrencies. During hack 13, there is evidence of very significant responses in the information leadership share and component share from Stellar to other smaller cryptocurrencies.

One of the most interesting results surrounds that of hack 2, relating to the theft of almost $431 million in the cryptocurrency Tether on the 21st of November 2017 where an attacker had stolen the funds directly from the Treasury wallet and subsequently moved them to an unauthorised account. While analyzing this event, we must consider the work of Gandal et al. [2018] who identified the impact of suspicious trading activity on the Mt.Gox Bitcoin exchange theft when approximately 600,000 Bitcoins were attained. The authors demonstrated that the suspicious trading likely caused the spike in price in late 2013 from $150 to $1,000, most likely driven by one single actor. These two new and significant pieces of research have fine-tuned the focus of regulators, policy-makers and academics alike, broad trust in both cryptocurrencies and the exchanges on which they trade cannot be sustained with such significant questions of abnormality remaining unanswered. The relationship between these cryptocurrencies is further established through the fact that Tether is pegged to Bitcoin. Analyzing the changes in information share during this time, we observe that Bitcoin influences Ethereum more in the period after the hacking event (+0.20), but obtains larger information flows from all of the other cryptocurrencies analyzed. Interestingly, Ethereum and Litecoin lose information share against the other cryptocurrencies while Ripple and Stellar gain informational authority. Similar, but far more pronounced estimates are identified in the analysis based on the information leadership share and component share of information.

With regards to cybercriminality based on the hacking of the exchanges on which cryptocurrencies trade, hack 3 and 4 related to the breaches at NiceHash and Youbit respectively. Hack 6 relates to the 26th of January hack of the Coincheck exchange in NEM. While hacks 3 and 4 relate directly to Bitcoin, there is evidence of increased information share responses to Bitcoin during hack 3 and from Bitcoin during hack 4 to other large cryptocurrencies with the exception of Ethereum. Interestingly, Ethereum increases it's information share during these events, which might indicate an improvement in it's perception as a central cryptocurrency during such a damaging time for Bitcoin. While the same relationships are identified in tests based on information leadership share and component share, the results are far more pronounced. During event 6, $536 million of NEM was lost during the hacking of Coincheck, which were stolen during several unauthorised transactions from a hot wallet. NEM is a blockchain platform that was designed and coded from the ground up for scale and speed that has a fixed supply of 8,999,999,999 units in it's genesis block. During this hacking event, over 523 million of these NEM units were stolen. While presenting no evidence of a significant volatility response during the multivariate GARCH analysis, with further evidence of it occurrence signalling the end of a pronounced period of comovement during this time. The scale of this cybercrime event resulted in widespread news coverage and despite little evidence of direct pricing volatility, there is substantial evidence of net transfer of information from smaller to larger cryptocurrencies through all three measures analysed, with particularly pronounced results evident in the the component share of information. The scale of this event appears to have provided somewhat of an informational equilibrium between large and small cryptocurrencies alike, as the shock echoed through the entire cryptocurrency sector.

Hacks 5, 7 and 8 warrant particular attention. As observed during the volatility and comovement analyses outlined above, these three cybercrime events represent the smallest estimated monetary losses. However, there are distinct characteristics related to each that appear to have generated substantial reverberations within cryptocurrency markets due to the nature of the cybercrime event. Hack 5 was based on the unprecedented direct theft of Stellar from a wallet, resulting in widespread discourse in the cryptocurrency community as to how such a theft could occur as the very nature of blockchain was to mitigate such risk of occurrence. As a partial robustness check to support the use of our selected methodology, in Figure 2 we observe a clear and sharp increase in the information flow between Stellar and Cardano (+0.44), while the sharpest declines with all other cryptocurrencies are related to relationships specifically with Stellar, such as that with Bitcoin (-0.47), Ethereum (-0.42) and Litecoin (-0.42). These responses are mirrored in the results relating to information leadership share, but are found to be quite broad when observing the component share response. Hack 7 and 8 refer to the BeeToken phishing attack and the Seele ICO scam, which although relate to quite minuscule losses when compared to other listed events, occurred in rapid succession during a period of broad reputation damage to the credibility of cryptocurrency markets. While proponents of the new financial asset class continued to identify the safety of it's use as key feature of cryptocurrencies, these particular events exposed deep flaws within their structure and supported the argument against their credibility due to the ease in which assets could be stolen. These events all generate substantial flows of information through all measures from smaller cryptocurrencies to largest cryptocurrencies.

Insert Figure 5 about here

In Figure 5, we analyse the abnormal returns associated with each of the investigated hacking events. While evidence of varying responses can be observed throughout each of the presented hacking events, there are particularly pronounced results provided in hacks 5 and 13. For brevity, we have only included the stated hacks[8] In the hour before event 5 relating to the theft of Stellar, we observe substantial abnormal returns in the markets Ripple (-24%), along with Ethereum (-11%), Litecoin (-7%), Bitcoin Cash (-4%) and the cryptocurrency at the centre of the hack, Stellar (-2%). This result is not only interesting due to the scale of the abnormal returns identified, but largely due to the fact that such negative abnormal returns can be identified in advance of what

[8] All other results related to the abnormal returns of cryptocurrencies due to hacking events are available from the authors on request.

can be considered to be official announcements. Abnormal returns appear largely pronounced of up to 4 hours after the time of the hacking event. Similarly, hack 13 which relates to the official announcement of the $650 million estimated loss through the Vietnamese ICO-theft initiated by the companies Ifan and Pincoin. This is found to be associated with significant abnormal returns in the four hours prior to the official announcement, initially leading to sharp losses in Ethereum markets four hours beforehand and then generating substantial abnormal one-hour gains (of over $4 in some cases) in all markets in both two and three hour periods before the announcement. At the time of the announcement, abnormal returns had fallen to levels close to 0%. While the role of automated trading programs warrants particular investigation in these scenarios, we cannot eliminate the role of illicit behaviour as cryptocurrency markets absorb the broadly damaging news of such significant cybercrime events.

Insert Table 13 about here

Table 13 presents an overview of the results contained within this analysis. Overall, with regards to intra-day volatility, we find evidence that there exist ‘weekend effects’ in cryptocurrency markets and that volatility is found to vary based on the opening hours of traditional financial markets. However, we could not find evidence of hour-of-the-day effects or indeed, any differential in volatility overnight as traditional financial markets closed. Most importantly, we identify a broad range of significant findings relating to the existence of sharp differences in volatility and information flow within these young markets in the aftermath of cybercriminality and broad hacking events. Should cryptocurrency markets aspire to become reputationally-comparable to that of key traditional financial markets, it is of paramount importance that such broad criminality be eliminated within the products and exchanges on which they trade. Should this not transpire, investors will continue to be broadly exposed to the exceptional moral hazard and asymmetric information issues that exist. Such changes in volatility and information content merit the protection of investors, or at the very least, further more substantial warnings that there exist abnormal risks of theft through both product and exchange manipulation. As research on cryptocurrency markets continues to evolve, while focusing and reflecting on the future benefits of both cryptocurrencies and blockchain at large, we must also consider the product’s evolution to coincide with the development of a reasonable level of investor confidence, that must be absent irrational exuberance, yet inclusive of a risk premium that reflects appropriate investor exposure in an efficient, sensible and legitimate manner.

6. Conclusion

This research provides a number of novel findings related to our selected cryptocurrency markets. The first stage of our analysis identifies a number of stylised facts relating to the intra-day price volatility and source of volatility within these markets. While investigating a number of hypotheses relating to intra-day cryptocurrency volatility, we have identified a number of stylised facts.

First, we have identified that there are substantial differences in cryptocurrency volatility between weekdays and weekends robust across a number of measures. Secondly, we identify that there are substantially elevated levels of cryptocurrency volatility while United States and European markets are open, however, this volatility is substantially reduced while Chinese and Japanese markets are operational. Finally, there is evidence of substantially elevated cryptocurrency volatility during episodes of substantial stress in GBP/USD and oil markets. However, we must also note that there is no evidence identified to accept the hypotheses that cryptocurrency volatility varies based on the times that traditional markets open and indeed, there is no evidence identified to support the presence of hour-of-the-day effects.

There are broad volatility responses for cybercrime events within an exchange which traded a broad number of cryptocurrencies indicating that such cybercrime generates sector-wide volatility effects. Further, there are significant differences in the volatility responses of cryptocurrencies with further evidence identifying significant instability generated within attacks on exchanges and ICO-fraud, both of which can be heavily dependent on perceptions of stability and financial safety. In a DCC-GARCH analysis, we observe that there are lower volatility estimates identified for smaller capitalisation cryptocurrencies when compared to the cross-correlations between their larger counterparts. This holds true not only for the dynamic correlations between smaller cyrptocurrencies themselves, but also for the relationships between smaller and larger cryptocurrencies. We also identify two specific periods where there is a sustained increase in cross-cryptocurrency correlations as controlled for each hacking event. We identify the largest sustained increase in cross-cryptocurrency correlations between the 6th of December 2017 and the 13th of January 2018, incorporating a number of significant hacks in our sample. Peak cross-correlations occur on the 18th of December 2017. These events coincide with the service breach and hacking of Nicehash, the bankrupcy of Youbit due to an external hack, and the DNS hijacking of Blackwallet.co resulting in the remote theft $400,000 in Stellar Lumer (XLM). It would appear that the sustained internationally relayed coverage of the four events led to a substantial loss of confidence in the cryptocurrency market during this time, which is reflected in the broad cross-correlations of both the largest and smallest cryptocurrencies alike. The second distinct phase of elevated cross-correlations occurs during the period between the 4th of March 2018 and the 9th of April 2018 which represent the theft of approximately $300 million during the multi-level-marketing scheme created by GainBitcoin and the ICO scam inspired by Ifan and Pincoin that resulted in the loss of $650 million. We also find significant differences in the price discovery dynamics in the pairwise relationships between our selected cryptocurrencies.

Three distinct novel results are presented. There exist substantial and sustained differences in the volatility of broad cryptocurrency markets dependent on a weekend effects, whether Asian, American and European markets are open, and indeed, dependent on episodes of extreme volatility in GBP/USD and oil markets. Further, we find evidence of broad comovement in cryptocurrency markets during periods of extreme stress and severe reputational damage which supports the hypotheses that these relatively youthful markets have developed to act somewhat similarly to traditional financial assets in time of crises. Further, there is substantial evidence to suggest that these same relationships change substantially in the period after cryptocurrency cybercriminality, indicating that not only is the price volatility of these financial products directly influenced, but also the manner in which the information share, information leadership share and the component share of the price discovery is processed. This result broadly indicates the presence of market manipulation within this young industry, a finding that institutional investors and regulators should find concerning.

Bibliography

Ardia, D., K. Bluteau, and M. Ruede (2018). Regime changes in bitcoin garch volatility dynamics. *Finance Research Letters (Forthcoming).*

Baig, T. and I. Goldfajn (1999). Financial market contagion in the asian crisis. *IMF staff papers 46*(2), 167–195.

Balcilar, M., E. Bouri, R. Gupta, and D. Roubaud (2017). Can volume predict bitcoin returns and volatility? a quantiles-based approach. *Economic Modelling 64*, 74–81.

Bariviera, A. F., M. J. Basgall, W. Hasperué, and M. Naiouf (2017). Some stylized facts of the bitcoin market. *Physica A: Statistical Mechanics and its Applications 484*, 82–90.

Berument, H. and H. Kiymaz (2001). The day of the week effect on stock market volatility. *Journal of Economics and Finance 25*(2), 181–193.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019). The blockchain folk theorem. *The Review of Financial Studies 32*(5), 1662–1715.

Bollerslev, T. (1986). Generalized autoregressive conditional heteroskedasticity. *Journal of Econometrics 31*(3), 307–327.

Bougerol, P. and N. Picard (1992). Stationarity of Garch processes and of some nonnegative time series. *Journal of Econometrics 52*(1-2), 115–127.

Bouoiyour, J. and R. Selmi (2015). What does bitcoin look like? *Annals of Economics & Finance 16*(2).

Bouri, E., P. Molnár, G. Azzi, D. Roubaud, and L. I. Hagfors (2017). On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier? *Finance Research Letters 20*, 192–198.

Brauneis, A. and R. Mestel (2018). Price discovery of cryptocurrencies: Bitcoin and beyond. *Economics Letters*.

Chen, M., Q. Wu, and B. Yang (2019). How valuable is fintech innovation? *The Review of Financial Studies 32*(5), 2062–2106.

Chiu, J. and T. V. Koeppl (2019). Blockchain-based settlement for asset trading. *The Review of Financial Studies 32*(5), 1716–1753.

Chu, J., S. Chan, S. Nadarajah, and J. Osterrieder (2017). Garch modelling of cryptocurrencies. *Journal of Risk and Financial Management 10*(4), 17.

Ciaian, P., M. Rajcaniova, et al. (2018). Virtual relationships: Short-and long-run evidence from bitcoin and altcoin markets. *Journal of International Financial Markets, Institutions and Money 52*, 173–195.

Clarkson, P. M., D. Joyce, and I. Tutticci (2006). Market reaction to takeover rumour in internet discussion sites. *Accounting & Finance 46*(1), 31–52.

Comerton-Forde, C. and T. J. Putniņš (2011). Measuring closing price manipulation. *Journal of Financial Intermediation 20*(2), 135–158.

Cong, L. W. and Z. He (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies 32*(5), 1754–1797.

Corbet, S., C. Larkin, B. Lucey, A. Meegan, and L. Yarovaya (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters 165*(1), 28–34.

Corbet, S., B. Lucey, M. Peat, and S. Vigne (2018). Bitcoin futures - what use are they? *Economics Letters (Forthcoming).*

Corbet, S., B. Lucey, and L. Yarovya (2017). Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters, forthcoming*.

Corbet, S., B. M. Lucey, A. Urquhart, and L. Yarovaya (2018). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis In press, corrected proof available online at: https://www.sciencedirect.com/science/article/pii/S1057521918305271.*

Corbet, S., A. Meegan, C. Larkin, B. Lucey, and L. Yarovaya (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters 165*, 28–34.

Cumming, D., S. Johan, and D. Li (2011). Exchange trading rules and stock market liquidity. *Journal of Financial Economics 99*(3), 651–671.

Diaz, D., B. Theodoulidis, and P. Sampaio (2011). Analysis of stock market manipulations using knowledge discovery techniques applied to intraday trade prices. *Expert Systems with Applications 38*(10), 12757–12771.

Foley, S., J. R. Karlsen, and T. J. Putnins (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies 32*(5), 1789–1853.

Forbes, K. J. and R. Rigobon (2002). No contagion, only interdependence: measuring stock market comovements. *The Journal of Finance 57*(5), 2223–2261.

Fry, J. and E.-T. Cheah (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis 47*, 343–352.

Gandal, N., J. Hamrick, T. Moore, and T. Oberman (2018). Price manipulation in the bitcoin ecosystem. *Journal of Monetary Economics 95*, 86–96.

Garman, M. B. and M. J. Klass (1980). On the estimation of security price volatilities from historical data. *Journal of Business*, 67–78.

Glick, R. and A. K. Rose (1999). Contagion and trade: Why are currency crises regional? *Journal of international Money and Finance 18*(4), 603–617.

Goldstein, I., W. Jiang, and A. Karolyi (2019). To fintech and beyond. *The Review of Financial Studies 32*(5), 1647–1661.

Gonzalo, J. and C. Granger (1995). Estimation of common long-memory components in cointegrated systems. *Journal of Business & Economic Statistics 13*(1), 27–35.

Griffins, J. and A. Shams (2018). Is bitcoin really un-tethered? *Available at SSRN: https://ssrn.com/abstract=3195066 13 June 2018.*

Guesmi, K., S. Saadi, I. Abid, and Z. Ftiti (2018). Portfolio diversification with virtual currency: Evidence from bitcoin. *International Review of Financial Analysis (Forthcoming).*

Harvey, C. R. (2017). Blockchain 2.0.

Hasbrouck, J. (1995). One security, many markets: Determining the contributions to price discovery. *The Journal of Finance 50*(4), 1175–1199.

Hauptfleisch, M., T. J. Putniņš, and B. Lucey (2016). Who sets the price of gold? london or new york. *Journal of Futures Markets 36*(6), 564–586.

Hu, B., T. McInish, J. Miller, and L. Zeng (2018). Intraday price behavior of cryptocurrencies. *Finance Research Letters (Forthcoming).*

Jiang, G., P. G. Mahoney, and J. Mei (2005). Market manipulation: A comprehensive study of stock pools. *Journal of Financial Economics 77*(1), 147–170.

Kaminsky, G. L. and C. M. Reinhart (2000). On crises, contagion, and confusion. *Journal of international Economics 51*(1), 145–168.

Keim, D. B. and R. F. Stambaugh (1984). A further investigation of the weekend effect in stock returns. *The Journal of Finance 39*(3), 819–835.

Koutmos, D. (2018). Bitcoin returns and transaction activity. *Economics Letters 167*, 81–85.

Kyle, A. S. and S. Viswanathan (2008). How to define illegal price manipulation. *American Economic Review 98*(2), 274–79.

Lakonishok, J. and E. Maberly (1990). The weekend effect: Trading patterns of individual and institutional investors. *The Journal of Finance 45*(1), 231–243.

Lee, E. J., K. S. Eom, and K. S. Park (2013). Microstructure-based manipulation: Strategic behavior and performance of spoofing traders. *Journal of Financial Markets 16*(2), 227–252.

Nelson, D. B. (1990). Stationarity and persistence in the garch(1,1) model. *Econometric Theory 6*(3), 318–334.

O'Hara, M. (2015). High frequency market microstructure. *Journal of Financial Economics 116*(2), 257–270.

Parkinson, M. (1980). The extreme value method for estimating the variance of the rate of return. *Journal of Business*, 61–65.

Phillip, A., J. Chan, and S. Peiris (2018). A new look at cryptocurrencies. *Economics Letters 163*, 6–9.

Phillips, P. C., Y. Wu, and J. Yu (2011). Explosive behavior in the 1990's nasdaq: When did exuberance escalate asset values? *International Economic Review 52*(1), 201–226.

Putniņš, T. J. (2012). Market manipulation: A survey. *Journal of Economic Surveys 26*(5), 952–967.

Putniņš, T. J. (2013). What do price discovery metrics really measure? *Journal of Empirical Finance 23*, 68–83.

Rogers, L. C. G. and S. E. Satchell (1991). Estimating variance from high, low and closing prices. *The Annals of Applied Probability*, 504–512.

Roth, N. (2015). An architectural assessment of bitcoin: using the systems modeling language. *Procedia Computer Science 44*, 527–536.

Sabherwal, S., S. K. Sarkar, and Y. Zhang (2011). Do internet stock message boards influence trading? evidence from heavily discussed stocks with no fundamental news. *Journal of Business Finance & Accounting 38*(9-10), 1209–1237.

Sensoy, A. (2018). The inefficiency of bitcoin revisited: A high-frequency analysis with alternative currencies. *Finance Research Letters*.

Tiwari, A. K., R. Jana, D. Das, and D. Roubaud (2018). Informational efficiency of bitcoinâĂŤan extension. *Economics Letters 163*, 106–109.

Urquhart, A. (2016). The inefficiency of bitcoin. *Economics Letters 148*, 80–82.

Urquhart, A. (2017). Price clustering in bitcoin. *Economics letters 159*, 145–148.

Urquhart, A. (2018). What causes the attention of bitcoin? *Economics Letters 166*, 40–44.

Urquhart, A. and H. Zhang (2018). Is bitcoin a hedge or safe-haven for currencies? An intraday analysis. *Available at SSRN: https://ssrn.com/abstract=3114108*.

Vidal-Tomás, D. and A. Ibañez (2018). Semi-strong efficiency of bitcoin. *Finance Research Letters*.

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

Yamori, N. and Y. Kurihara (2004). The day-of-the-week effect in foreign exchange markets: multi-currency evidence. *Research in International Business and Finance 18*(1), 51–57.

Yan, B. and E. Zivot (2010). A structural analysis of price discovery measures. *Journal of Financial Markets 13*(1), 1–19.

Yang, D. and Q. Zhang (2000). Drift-independent volatility estimation based on high, low, open, and close prices. *The Journal of Business 73*(3), 477–492.

Zaki, M., B. Theodoulidis, and D. Díaz Solís (2011). 'Stock-touting' through spam e-mails: A data mining case study. *Journal of Manufacturing Technology Management 22*(6), 770–787.

Table 1: Descriptive statistics of the traditional financial assets and cryptocurrencies

	Count	Mean	Variance	Std Dev	Skew	Kurt	Min	Max
Traditional Financial Assets								
GBP/USD	5,891	0.00000	0.00000	0.00076	0.24383	10.24634	-0.00664	0.00965
VIX	3,070	0.00015	0.00067	0.02596	-0.19906	57.44486	-0.46779	0.34793
Gold	1,229	-0.00007	0.00000	0.00157	0.35547	5.13538	-0.00721	0.01013
S&P500	1,671	-0.00001	0.00001	0.00227	-1.11241	10.32006	-0.01715	0.01479
Oil (WTI)	5,040	0.00006	0.00001	0.00316	-0.23558	7.57966	-0.02506	0.02188
Cryptocurrencies								
Bitcoin	8,297	0.00011	0.00014	0.01195	0.48299	10.40750	-0.10547	0.11889
Ethereum	8,297	0.00007	0.00018	0.01352	0.85312	15.16250	-0.10905	0.15243
Litecoin	8,297	0.00011	0.00027	0.01657	1.48860	20.91631	-0.12945	0.23656
Ripple	8,297	0.00020	0.00038	0.01954	2.37126	34.32370	-0.16514	0.30347
Stellar	8,297	0.00046	0.00045	0.02111	2.99377	47.85589	-0.14332	0.40325
Monero	8,297	0.00010	0.00029	0.01713	0.34831	8.26498	-0.12667	0.18751
Bitcoin Cash	8,297	0.00019	0.00039	0.01981	0.69729	16.24494	-0.23913	0.27164
Cardano	7,376	0.00035	0.00035	0.01859	2.44642	30.14793	-0.17087	0.31692

Note: We have selected GBP/USD to represent interatctions between cryptocurrencies and broad currency markets, the S&P500 as a representation of stock market performance, both gold and oil (as measured by West Texas Intermediate, WTI oil markets) as a representation of commodity markets, and finally the VIX (CBOE volatility index) to represent options markets and implied volatility respectively. Our selected cryptocurrencies represent the eight largest by market capitalisation during the period in which data was collected. Our selected financial markets, sampled at 60-minute intervals, was collected from Thomson Reuters Tick History for the period from midnight on 1 September 2017 through midnight on 10 August 2018.

Table 2: Correlation matrix between traditional financial assets and cryptocurrencies

	GBP/USD	VIX	Gold	S&P500	Oil	BTC	ETC	LTC	RIP	STE	MON	BTCa	CAR
GBP/USD	1.000												
VIX	0.014	1.000											
Gold	-0.548	0.085	1.000										
S&P500	-0.035	-0.768	-0.131	1.000									
Oil (WTI)	-0.244	-0.271	0.116	0.363	1.000								
Bitcoin	0.025	-0.010	0.016	0.051	-0.016	1.000							
Ethereum	0.014	0.014	0.040	0.045	0.008	0.710	1.000						
Litecoin	0.010	-0.011	0.005	0.028	-0.007	0.618	0.690	1.000					
Ripple	0.025	0.028	0.061	0.025	0.016	0.484	0.557	0.416	1.000				
Stellar	-0.002	0.045	0.014	-0.007	-0.033	0.052	0.218	0.165	0.248	1.000			
Monero	-0.002	-0.018	0.033	0.060	0.012	0.642	0.676	0.552	0.406	0.217	1.000		
Bitcoin Cash	0.021	-0.014	-0.050	0.058	0.023	0.593	0.613	0.522	0.342	0.157	0.560	1.000	
Cardano	-0.043	0.013	0.027	0.004	0.062	0.088	0.239	0.094	0.246	0.443	0.206	0.256	1.000

Note: We have selected GBP/USD to represent interatctions between cryptocurrencies and broad currency markets, the S&P500 as a representation of stock market performance, both gold and oil (as measured by West Texas Intermediate, WTI oil markets) as a representation of commodity markets, and finally the VIX (CBOE volatility index) to represent options markets and implied volatility respectively. Our selected cryptocurrencies represent the eight largest by market capitalisation during the period in which data was collected. Our selected financial markets, sampled at 60-minute intervals, was collected from Thomson Reuters Tick History for the period from midnight on 1 September 2017 through midnight on 10 August 2018.

Table 3: Cryptocurrency hacking events used to investigate the differences in price volatility and discover

Hack	**Date**	Est. Time	Amount	Market	Description
1	07-Nov-17	11:51	$280.0m	Ethereum	On November 6th, a user playing with the Parity multisig wallet library contract triggered its kill function, effectively freezing the funds on all Parity multisig wallets linked to the library's code. The vulnerability was deployed after July 20th 2017 and was found by an anonymous user. The user decided to exploit this vulnerability and made himself the 'owner' of the library contract.
2	21-Nov-17	04:15	$30.0m	Tether	Tether blamed a 'malicious action by an external attacker' stating that $30,950,010 USDT was removed from the Tether Treasury wallet on Nov. 19, 2017 and sent to an unauthorized bitcoin address. As Tether is the issuer of the USDT managed asset, we will not redeem any of the stolen tokens, and we are in the process of attempting token recovery to prevent them from entering the broader ecosystem.'
3	06-Dec-17	10:45	$64.0m	Bitcoin	Service breach and hack at NiceHash, a marketplace for miners to rent out their hash rate to others. The situation escalated after hours of website outage and reports from a multitude of users that their NiceHash-associated wallets had been emptied.
4	18-Dec-17	21:35	$37.0m	Bitcoin	The South Korean bitcoin exchange named Youbit moved to declare bankruptcy following what it said was a debilitating hack and theft. A message on Youbit's official website stated that, at around 4:34 a.m. local time, an external hack resulted in the loss of 'about 17 % of total assets.'
5	13-Jan-18	12:00	$0.4m	Stellar	A DNS hijack has led to hackers withdrawing $400,000 worth of Stellar Lumen (XLM) coins from wallets hosted by Blackwallet.co without user permission. On January 13, attackers took control of BlackWallet's hosting server, changing settings to allow code to run which automatically sent customer balances over 20XLM to an address under the hackers' control.
6	26-Jan-18	15:00	$532.6m	NEM	On Jan. 26, Coincheck suspended all deposits in NEM on their exchange. NEM Foundation president Lon Wong confirmed Coincheck was hacked, calling the stolen funds 'the biggest theft in the history of the world.' Once the hack was confirmed by the exchange, reported to have happened 3:00 AM local time on Jan. 26, it was then revealed that the hack resulted in a loss of 523 mln NEM coins, worth approximately $532.6 mln around Jan. 26. The coins were stolen via several unauthorized transactions from a hot wallet.

(continued on next page)

Table 3: Cryptocurrency hacking events used to investigate the differences in price volatility and discover

Hack	**Date**	Est. Time	Amount	Market	Description
7	31-Jan-18	20:22	$0.9m	BeeToken	Cryptocurrency startup BeeToken was hacked while the attackers targeted its initial coin offering (ICO) with phishing attacks and duped investors for over $1 million worth of Ethereum.
8	05-Feb-18	17:00	$1.8m	Ethereum	Potential Seele ICO investors were scammed out of nearly $2 million by impersonators posing as administrators, who used the company's Telegram channel to get them to send their money over before the token sale began. Seele, a blockchain project that describes itself as 'blockchain 4.0,' with potential applications in IoT, game assets, fintech, among others areas.
9	08-Feb-18	12:00	$195.0m	Nano	The hack is estimated to have occurred on 8 February 2018, however, Nano's developers allege that the exchange was insolvent long before February, stating 'we now have sufficient reason to believe that Firano has been misleading the Nano Core Team and the community regarding the solvency of the BitGrail exchange for a significant period of time.'
10	15-Feb-18	09:00	$50.0m	Bitcoin	Cisco had already been investigating potential cybercriminality in partnership with the Ukrainian Cyberpolice stating that those behind a large scam had netted $50 million in cryptocurrency over a three-year period. 'The campaign was very simple and after initial setup the attackers needed only to continue purchasing Google AdWords to ensure a steady stream of victims,' they wrote.
11	04-Mar-18	17:41	$50.0m	Bitcoin	BTC Global was launched in Sep. 25, 2017 by 'famous' trader Steven Twain. His success in binary options trading led people to believe that the platform was trustworthy. However, the set-up was criticized and called out for being a scam ever since it was released.
12	05-Apr-18	12:00	$300.0m	Bitcoin	GainBitcoin began as a multi-level marketing (MLM) scheme in 2015 and amassed over 100,000 investors, all of whom were promised monthly returns of 10% on their investment. When authorities caught on, Amit Bhardwaj, who had established the scheme had moved his base of operations to Dubai while continuing operations in India.

(continued on next page)

Table 3: Cryptocurrency hacking events used to investigate the differences in price volatility and discover

Hack	**Date**	Est. Time	Amount	Market	Description
13	09-Apr-18	12:00	$650.0m	ICO	Occurring in Vietnam, the largest alleged scam connected to an ICO has been pulled off by two blockchain firms, Ifan and Pincoin. The two firms have allegedly duped 32,000 investors for around VND 15 trillion ($660 million). Ifan is registered in Singapore while Pincoin is registered in Dubai, however, both firms had approached the same company in Vietnam (Modern Tech) to advertise their projects to potential local investors.
14	19-Apr-18	09:00	$20.0m	Bitcoin	Two men started the scheme in 2015 and subsequently built a multi-level company by promising investors high returns through investing in bitcoin. ‘The multi-level transaction is a risk to the socioeconomic order with mass production of many victims,’ the prosecuting judge was quoted as saying in the report.
15	10-Jun-18	17:00	$40.0m	NPXS	Coinrail stated that it had suspended services after it suffered what it calls a ‘cyber intrusion,’ which resulted in a range of ERC-20 based tokens stolen from the platform. However, Coinrail only provided the names of some of the tokens that were taken in the alleged breach without disclosing the exact amounts at stake.
16	16-Jun-18	07:33	$31.5m	Ethereum	Bithumb moved a large amount of Ethereum to its cold wallet when they recently noticed abnormal access. On June 16, Bithumb announced an abrupt server check ‘in order to maximize security settings.’ The maintenance was planned from 5:20 am KST to 9:00 am KST, but exceeded the scheduled time.
17	09-Jul-18	21:35	$23.5m	Ethereum	In a statement revealed July 9, Bancor experienced a security breach to the hot wallet used to update smart contracts on its exchange, resulting in a loss of approximately $23.5 million worth of Ethereum. In a more detailed statement released at a later stage, Bancor outlined the extent of the theft, indicating that 24,984 ETH ($12.5M), 229M NPXS ($1M) and 3.2M BNT ($10M) were stolen in total.

In the above table we have established a list of seventeen of the largest cryptocurrency hacking events between September 2017 and August 2018. The list of hacking events include a broad number of unique situations that targeted either the exchange on which cryptocurrencies trade, the blockchain supporting a specific cryptocurrency or indeed the wallets of cryptocurrency investors. We have only included events that were determined as newsworthy if covered by any one of a number of mainstream international broadsheet newspapers as determined by a thorough search using the LexusNexis database.

Table 4: intra-day volatility of cryptocurrency markets during traditional financial market opening hours

	BTC	ETH	LTC	RIP	STL	MON	BTCa	CAR	Ave Rank
GBP/USD open									
Park	0.11%	0.27%	0.19%	0.38%	0.44%	0.27%	0.10%	0.25%	
G-Klass	0.24%	0.72%	0.50%	1.19%	1.17%	0.77%	0.40%	0.57%	
Rogers	0.13%	0.28%	0.20%	0.36%	0.42%	0.25%	0.11%	0.25%	
Yang-Z	0.17%	0.37%	0.26%	0.54%	0.56%	0.35%	0.17%	0.31%	
	0.16%	0.41%	0.29%	0.61%	0.65%	0.41%	0.20%	0.34%	
	3	3	4	2	4	4	2	3	3.1
VIX open									
Park	0.18%	0.39%	0.54%	0.56%	0.61%	0.47%	0.17%	0.24%	
G-Klass	0.46%	1.03%	1.36%	1.87%	1.99%	1.32%	0.31%	0.95%	
Rogers	0.20%	0.41%	0.56%	0.50%	0.53%	0.47%	0.26%	0.14%	
Yang-Z	0.28%	0.52%	0.77%	0.86%	0.86%	0.59%	0.27%	0.23%	
	0.28%	0.59%	0.81%	0.95%	1.00%	0.71%	0.26%	0.39%	
	2	1	2	1	2	2	1	2	1.6
Gold open									
Park	0.30%	0.42%	0.82%	0.40%	1.05%	0.58%	-0.07%	0.56%	
G-Klass	0.82%	0.70%	1.48%	0.82%	2.55%	1.72%	-0.11%	1.56%	
Rogers	0.32%	0.49%	0.96%	0.43%	0.99%	0.52%	-0.07%	0.55%	
Yang-Z	0.46%	0.65%	1.14%	0.74%	1.45%	0.87%	0.14%	0.82%	
	0.47%	0.57%	1.10%	0.60%	1.51%	0.92%	-0.03%	0.87%	
	1	2	1	3	1	1	4	1	1.8
S&P500 open									
Park	0.07%	0.27%	0.39%	0.39%	0.46%	0.33%	-0.24%	0.20%	
G-Klass	-0.07%	0.01%	0.27%	0.90%	1.51%	1.05%	-1.25%	0.59%	
Rogers	0.13%	0.41%	0.56%	0.44%	0.43%	0.27%	-0.02%	0.13%	
Yang-Z	0.13%	0.33%	0.52%	0.63%	0.69%	0.40%	-0.29%	0.15%	
	0.06%	0.25%	0.44%	0.59%	0.77%	0.51%	-0.45%	0.27%	
	4	5	3	4	3	3	5	4	3.9
Oil open									
Park	0.05%	0.22%	0.18%	0.35%	0.40%	0.23%	0.07%	0.16%	
G-Klass	0.04%	0.57%	0.43%	1.07%	1.08%	0.68%	0.25%	0.42%	
Rogers	0.07%	0.24%	0.20%	0.33%	0.37%	0.22%	0.08%	0.14%	
Yang-Z	0.08%	0.31%	0.25%	0.52%	0.53%	0.28%	0.15%	0.22%	
	0.06%	0.34%	0.27%	0.57%	0.59%	0.35%	0.14%	0.23%	
	5	4	5	5	5	5	3	5	4.6

Note: The above volatility estimates represent the distance from the average intra-day value as calculated by the multiple estimation techniques presented in Section 4.1. Each of the individual market opening times are then compared and ranked in order of 1 through 5, indicative of most volatile (1) and least volatile (5). The average rank indicates the average rank across all analysed cryptocurrencies.

Table 5: intra-day volatility of cryptocurrency markets separated by weekday and weekend trading times

	BTC	ETH	LTC	RIP	STL	MON	BTCa	CAR
Park								
Weekdays	0.12%	0.28%	0.20%	0.39%	0.46%	0.26%	0.09%	0.22%
Weekends	-0.31%	-0.71%	-0.51%	-0.99%	-1.15%	-0.67%	-0.23%	-0.57%
G-Klass								
Weekdays	0.27%	0.75%	0.55%	1.22%	1.24%	0.77%	0.34%	0.53%
Weekends	-0.70%	-1.90%	-1.41%	-3.08%	-3.10%	-1.95%	-0.88%	-1.37%
Rogers								
Weekdays	0.14%	0.29%	0.21%	0.37%	0.43%	0.25%	0.11%	0.21%
Weekends	-0.35%	-0.73%	-0.53%	-0.93%	-1.09%	-0.63%	-0.28%	-0.55%
Yang-Z								
Weekdays	0.18%	0.38%	0.27%	0.56%	0.58%	0.35%	0.16%	0.28%
Weekends	-0.46%	-0.97%	-0.69%	-1.41%	-1.47%	-0.89%	-0.42%	-0.73%

Note: The above volatility estimates represent the distance from the average intra-day value as calculated by the multiple estimation techniques presented in Section 4.1.

Table 6: intra-day volatility of cryptocurrency markets during differing geographic financial market opening hours

		BTC	ETH	LTC	RIP	STL	MON	BTCa	CAR	Average Rank
Tokyo markets open	Park	-0.17%	-0.22%	-0.29%	-0.18%	0.20%	-0.18%	-0.04%	0.34%	
	G-Klass	-0.34%	-0.49%	-0.72%	-0.84%	0.08%	-0.18%	0.55%	0.96%	
	Rogers	-0.19%	-0.20%	-0.25%	-0.09%	0.25%	-0.25%	-0.15%	0.36%	
	Yang-Z	-0.27%	-0.30%	-0.47%	-0.30%	0.26%	-0.15%	0.03%	0.49%	
	Average	-0.24%	-0.30%	-0.43%	-0.35%	0.20%	-0.19%	0.10%	0.53%	
	Rank	3	3	3	3	2	3	2	1	2.5
Beijing markets open	Park	-0.23%	-0.33%	-0.35%	-0.29%	-0.14%	-0.33%	-0.03%	-0.09%	
	G-Klass	-0.71%	-0.89%	-1.10%	-1.15%	-0.91%	-1.01%	0.05%	-0.45%	
	Rogers	-0.22%	-0.31%	-0.32%	-0.22%	-0.10%	-0.30%	-0.11%	-0.02%	
	Yang-Z	-0.29%	-0.38%	-0.47%	-0.37%	-0.13%	-0.31%	0.07%	0.11%	
	Average	-0.36%	-0.48%	-0.56%	-0.51%	-0.32%	-0.49%	0.00%	-0.11%	
	Rank	4	4	4	4	4	4	3	3	3.8
Europe markets open	Park	0.22%	0.28%	0.33%	0.37%	0.14%	0.33%	0.50%	-0.09%	
	G-Klass	0.74%	0.96%	1.26%	1.41%	0.54%	0.99%	1.34%	0.13%	
	Rogers	0.20%	0.25%	0.24%	0.28%	0.09%	0.34%	0.48%	-0.16%	
	Yang-Z	0.27%	0.38%	0.46%	0.56%	0.16%	0.36%	0.68%	-0.16%	
	Average	0.36%	0.47%	0.57%	0.65%	0.23%	0.50%	0.75%	-0.07%	
	Rank	1	1	1	1	1	1	1	2	1.1
US markets open	Park	0.05%	0.18%	0.18%	-0.10%	-0.11%	0.11%	-0.34%	-0.26%	
	G-Klass	0.04%	-0.16%	-0.08%	-0.69%	0.43%	0.01%	-1.61%	-0.59%	
	Rogers	0.07%	0.27%	0.27%	-0.06%	-0.17%	0.14%	-0.18%	-0.29%	
	Yang-Z	0.15%	0.26%	0.37%	0.06%	0.03%	0.16%	-0.31%	-0.35%	
	Average	0.08%	0.14%	0.19%	-0.20%	0.04%	0.10%	-0.61%	-0.37%	
	Rank	2	2	2	2	3	2	4	4	2.6

Note: The above volatility estimates represent the distance from the average intra-day value as calculated by the multiple estimation techniques presented in Section 4.1. Each of the individual national market opening times are then compared and ranked in order of 1 through 5, indicative of most volatile (1) and least volatile (5). The average rank indicates the average rank across all analysed cryptocurrencies. When comparing differing time zones of investigation, all opening times have been converted to Greenwich Mean Time (GMT), with daylight savings times across jurisdictions taken into account and alternated accordingly.

Table 7: GARCH-calculated volatility based on the hour-of-the-day in which trades are completed

	Bitcoin	Bitcoin Cash	Ethereum	Litecoin	Ripple	Stellar	Monero	Cardano
12:00AM	-0.00134**	-0.00236**	-0.00095	-0.00164**	-0.00250***	-0.00168**	-0.00159*	-0.00065
01:00AM	-0.00111*	-0.00115	-0.00062	-0.00080	-0.00160*	-0.00343***	-0.00257***	-0.00008
02:00AM	-0.00142**	-0.00175*	-0.00005	-0.00085	-0.00177*	-0.00172**	-0.00173*	-0.00008
03:00AM	-0.00116*	-0.00232**	-0.00058	-0.00217**	-0.00162*	-0.00227***	-0.00179*	-0.00003
04:00AM	-0.00060	-0.00120	-0.00027	-0.00036	-0.00054	-0.00156*	-0.00149	+0.00128
05:00AM	-0.00080	-0.00095	-0.00004	-0.00121	-0.00166*	-0.00313***	-0.00070	-0.00015
06:00AM	+0.00058	-0.00111	-0.00039	+0.00013	-0.00196**	-0.00080	-0.00221**	+0.00133*
07:00AM	-0.00104*	-0.00226**	-0.00003	-0.00167**	-0.00068	-0.00242***	-0.00113	+0.00049
08:00AM	-0.00120*	-0.00152	-0.00011	-0.00066	+0.00100	-0.00132	-0.00199**	+0.00175**
09:00AM	-0.00133**	-0.00236**	-0.00131*	-0.00110	+0.00187**	-0.00180**	-0.00109	+0.00032
10:00AM	-0.00133**	-0.00076	-0.00110	+0.00001	-0.01285***	-0.00334***	-0.00193**	+0.00195**
11:00AM	+0.00094*	-0.00165	+0.00154**	+0.00065	+0.00406***	-0.00017	-0.00100	+0.00157**
12:00PM	-0.00053	-0.00134	-0.00057	-0.00071	-0.00569***	-0.00102	-0.00101	+0.00225***
13:00PM	-0.00087	-0.00141	-0.00077	-0.00039	-0.00002	-0.00226***	-0.00158*	-0.00007
14:00PM	-0.00158**	-0.00252**	-0.00064	-0.00102	-0.00148*	-0.00247***	-0.00113	+0.00150*
15:00PM	-	-	-	-	-	-	-	+0.00298***
16:00PM	-0.00024	-0.00094	-0.00047	-0.00002	-0.00089	-0.00103	+0.00062	+0.00255***
17:00PM	-0.00096*	-0.00230**	-0.00079	-0.00101	-0.00184**	-0.00271***	-0.00137*	+0.00198**
18:00PM	-0.00053	-0.00207*	-0.00074	-0.00068	-0.00133	-0.00193**	-0.00152	+0.00348***
19:00PM	-0.00068	-0.00074	-0.00091	-0.00042	-0.00225**	-0.00090	-0.00062	+0.00234***
20:00PM	-0.00127*	-0.00209*	-0.00134*	-0.00204***	-0.00153*	-0.00200**	-0.00224**	+0.00264***
21:00PM	-0.00165**	-0.00319***	+0.00009	-0.00095	-0.00097	-0.00044	-0.00197**	+0.00137*
22:00PM	-0.00051	-0.00024	-0.00005	-0.00104	-0.00139*	-0.00171**	-0.00078	+0.00092
23:00PM	-0.00064	-0.00079	+0.00051	+0.00005	-0.00086	-0.00196**	-0.00025	-
Constant	0.00102**	0.00159**	0.00052	0.00069	0.00127**	0.00151**	0.00136**	-0.00142**
ARCH	0.07615***	0.09578***	0.11583***	0.11171***	0.48590***	0.11666***	0.08821***	0.17359***
	(35.55)	(27.70)	(26.74)	(31.10)	(36.40)	(41.91)	(25.98)	(31.82)
GARCH	0.90819***	0.88126***	0.84654***	0.87015***	0.59315***	0.89265***	0.90290***	0.81949***
	(350.57)	(204.89)	(163.15)	(233.56)	(90.37)	(362.69)	(264.84)	(182.74)
N	8,297	8,297	8,297	8,297	8,297	8,297	8,297	7,376
Wald Chi2	72.88	30.30	34.02	38.47	4623.58	71.16	34.97	150.74
Prob >Chi2	0.00000	0.14110	0.06490	0.02270	0.00000	0.00000	0.05240	0.00000
Log-Likelihood	26,541.23	22,591.69	25,575.23	24,331.72	23,147.71	23,445.54	23,375.97	21,921.16

Note: The results are based on GARCH methodologies utilising data at hourly intervals over the period 1 September 2017 through 12 August 2018. The selected GARCH methodology utilises the following mean equation: $R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 £/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + \varepsilon_t$ with a variance equation represented by $h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{24} D_{ToD}$. For brevity, only the results relative to the time of day volatility estimates are presented. Further results are available from the authors on request. T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Table 8: Cryptocurrency price volatility during differing traditional financial market volatility regimes

	Bitcoin	Bitcoin Cash	Ethereum	Litecoin	Ripple	Stellar	Monero	Cardano
GBP/USD Volatility								
Low Vol.	-0.00140***	-0.00251***	-0.00109**	-0.00114**	-0.00084	-0.00067	-0.00183***	-0.00105**
Below Average Vol.	-0.00119***	-0.00120**	-0.00080*	-0.00083	-0.00065	-0.00114***	-0.00120**	-0.00119***
Above Average Vol.	-0.00107***	-0.00133**	-0.00074	-0.00054	-0.00187***	-0.00156***	-0.00145***	-0.00085**
High Vol.	-0.00067***	-0.00126*	-0.00091**	-0.00063	-0.00043	-0.00135***	-0.00138**	-0.00135***
High-Low Difference	+0.00072	+0.00125	+0.00018	+0.00051	+0.00042	-0.00068	+0.00045	-0.00031
VIX Volatility								
Low Vol.	-0.00056	-0.00065	-0.00071	-0.00010	-0.00136*	+0.00041	-0.00050	+0.00194***
Below Average Vol.	+0.00035	+0.00097*	+0.00012	+0.00082*	+0.00036	+0.00062	+0.00058	+0.00112**
Above Average Vol.	+0.00051	+0.00061	+0.00026	+0.00080	-0.00223***	+0.00103**	+0.00147**	+0.00295***
High Vol.	-0.00015	+0.00066	+0.00004	+0.00067	-0.00001	0.00195***	+0.00051	+0.00016
High-Low Difference	+0.00042	+0.00132	+0.00075	+0.00077	+0.00135	+0.00154	+0.00101	-0.00178
S&P500 Volatility								
Low Vol.	-0.00073	-0.00117	-0.00129**	-0.00107	-0.00008	-0.00188***	+0.00004	-0.00115*
Below Average Vol.	+0.00018	+0.00068	-0.00003	+0.00011	+0.00120*	+0.00071	-0.00002	+0.00011
Above Average Vol.	+0.00044	-0.00048	+0.00002	+0.00037	+0.00008	+0.00045	-0.00014	-0.00030
High Vol.	-0.00035	-0.00094	-0.00021	-0.00059	+0.00053	+0.00057	+0.00068	-0.00046
High-Low Difference	+0.00038	+0.00023	+0.00108	+0.00048	+0.00061	+0.00246	+0.00063	+0.00069
Gold Volatility								
Low Vol.	+0.00001	-0.00050	+0.00005	-0.00054	-0.00021	-0.00075	-0.00023	+0.00196***
Below Average Vol.	-0.00018	-0.00060	-0.00004	-0.00107*	-0.00084	+0.00018	-0.00103	-0.00045
Above Average Vol.	-0.00026	-0.00003	-0.00009	-0.00041	+0.00046	-0.00055	+0.00009	-0.00073
High Vol.	+0.00073*	-0.00044	+0.00102*	+0.00083	+0.00003	-0.00041	+0.00043	+0.00093
High-Low Difference	+0.00072	+0.00006	+0.00098	+0.00137	+0.00024	+0.00034	+0.00067	-0.00104
Oil Volatility								
Low Vol.	+0.00013	+0.00078	-0.00001	-0.00029	+0.00166**	+0.00085*	+0.00071	-0.00018
Below Average Vol.	+0.00093**	+0.00065	+0.00054	+0.00051	+0.00097	+0.00143***	+0.00089	+0.00025
Above Average Vol.	+0.00069	+0.00110	+0.00056*	+0.00023	-0.00065	+0.00043	+0.00114**	-0.00007
High Vol.	+0.00116***	+0.00149	+0.00071**	+0.00089**	+0.00097	-0.00011	+0.00153**	+0.00139***
High-Low Difference	+0.00103	+0.00071	+0.00071	+0.00119	-0.00069	+0.00095	+0.00082	+0.00157

Note: Dummy variables are generated based on the quartile of volatility that each of the above individual traditional financial markets fall. The first quartile represents the lowest periods of volatility while the fourth quartile represents the highest level of volatility. The resulting dummy variables are then used in a GARCH methodology to investigate potential behavioural differences in cryptocurrency volatility during these periods. The stated high-low difference is defined as the difference between the periods denoted as the highest and the lowest levels of volatilities. The methodologies utilise data at hourly intervals over the period 1 September 2017 through 12 August 2018. Full regression results are available from the authors on request. For presentation purposes, only the coefficients associated with the determined dummy variables are presented. T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Table 9: Multivariate GARCH methodology analysing cryptocurrency response to hacking events

Variable	Bitcoin	Ethereum	Litecoin	Ripple	Stellar	Monero	Bit. Cash	Cardano
R_1	-0.1896***	-0.0447	-0.0558**	-0.1736***	-0.2628***	-0.1499***	-0.0060	-0.2760***
	(-4.21)	(-1.74)	-2.39	-8.44	-6.48	-5.06	-0.27	-8.84
R_2	-0.0488	-0.0131	-0.0727***	-0.2037***	0.0345	-0.0137	-0.0504**	-0.0709*
	(-1.57)	(-0.62)	-3.67	-10.14	1.17	-0.44	-2.11	-1.72
R_3	0.0460	-0.0059	-0.0472*	0.0579**	-0.1813***	0.0774***	-0.0216	0.0761**
	(1.52)	(-0.24)	-1.91	2.44	-11.08	2.86	-0.88	2.11
R_4	-0.0930***	-0.0168	-0.0656***	-0.0092	-0.0393*	-0.0192	-0.0063	-0.0828***
	(-3.34)	(-0.86)	-4.02	-0.40	-1.78	-0.74	-0.25	-3.03
R_5	-0.0103	-0.0192	-0.0283	-0.0217	-0.1823***	-0.0653**	-0.0341	-0.0078
	(-0.42)	(-0.95)	-1.43	-0.98	-9.04	-2.40	-1.62	-0.25
GBP/USD	0.2395	-0.4719	0.2629	0.7008	-0.2349***	0.0365	-0.7563	-0.1159
	(0.38)	(-1.23)	0.52	0.75	-3.89	0.05	-1.00	-0.09
VIX	0.0152	-0.0122	-0.0177	0.0141	0.0191	0.0153	0.0109	0.0237
	(0.88)	(-0.75)	-1.00	0.61	0.88	0.92	0.48	0.96
Gold	0.2286	-0.1741	-0.0458	0.3451	-0.5614*	-0.0373	-0.6397*	0.0896
	(0.67)	(-0.68)	-0.20	0.83	-1.78	-0.11	-1.91	0.16
S&P500	0.1595	0.0130	0.2417	0.4752	0.1625	0.1028	-0.0808	0.1235
	(0.56)	(0.06)	1.01	1.24	0.56	0.36	-0.23	0.39
Oil	-0.1174	-0.0506	-0.0124	-0.1537	-0.2540*	0.1124	0.1365	0.3203*
	(-1.04)	(-0.60)	-0.16	-1.08	-1.71	0.90	0.96	1.73
Bitcoin	-	0.8062***	0.8968***	0.5907***	0.1717***	0.7511***	0.8665***	0.0424
	(-)	(31.98)	29.78	17.35	4.72	19.66	25.62	1.03
D_1	-0.0011	0.0010	0.0016	0.0007	0.0011	0.0030*	0.0023	0.0019
	(-1.60)	(0.92)	1.22	0.42	0.38	1.90	1.53	1.54
D_2	-0.0005	-0.0015***	-0.0006	-0.0012	0.0016	-0.0003	0.0002	-0.0004
	(-0.67)	(-4.19)	-0.63	-1.20	0.43	-0.27	0.12	-0.43
D_3	0.0033***	-0.0021***	-0.0013	0.0008	0.0002	-0.0003	-0.0010	0.0003
	(2.89)	(-2.54)	-1.32	1.02	0.04	-0.18	-0.70	0.13
D_4	-0.0031***	-0.0016	-0.0010	0.0023	0.0053***	-0.0068***	-0.0051**	-0.0002
	(-2.62)	(-1.59)	-0.49	1.43	2.59	-6.52	-2.38	-0.16
D_5	-0.0020*	-0.0013	-0.0019	-0.0033*	-0.0016	-0.0009	-0.0030*	-0.0009
	(-1.69)	(-1.02)	-1.33	-1.68	-0.83	-0.50	-1.90	-0.60
D_6	-0.0010	0.0005	-0.0001	-0.0002	-0.0011	-0.0008	-0.0003	-0.0006
	(-0.98)	(0.50)	-0.13	-0.17	-1.13	-0.68	-0.23	-0.65
D_7	-0.0008	-0.0003	0.0032***	0.0106***	0.0056***	-0.0011	-0.0016	0.0019**
	(-0.83)	(-0.27)	2.47	17.34	9.23	-0.76	-1.17	2.41
D_8	0.0025	0.0033*	0.0029	0.0042***	0.0010	0.0053**	0.0054**	0.0011
	(1.37)	(1.91)	1.38	2.49	0.87	2.31	2.39	0.90
D_9	-0.0004	-0.0008	-0.0002	0.0008	0.0000	-0.0013	-0.0009	-0.0006
	(-0.26)	(-0.71)	-0.11	0.39	0.05	-0.69	-0.44	-0.50
D_{10}	0.0008	0.0003	-0.0003	0.0020***	-0.0004	0.0021	0.0028***	-0.0002
	(0.87)	(0.29)	-0.19	2.77	-0.44	1.61	2.75	-0.44
D_{11}	-0.0027***	-0.0018**	-0.0012	-0.0041***	0.0017**	-0.0028***	-0.0020**	-0.0010
	(-6.74)	(-2.33)	-1.41	-4.72	2.50	-3.18	-2.09	-0.98
D_{12}	-0.0005	0.0010	0.0000	0.0001	0.0002	-0.0005	-0.0002	0.0009
	(-0.86)	(0.99)	0.00	0.05	0.31	-0.62	-0.19	1.08
D_{13}	0.0091***	0.0017*	0.0009	0.0013	0.0011	0.0010	0.0016	0.0008
	(4.52)	(1.65)	0.95	0.67	1.19	0.81	1.27	1.50
D_{14}	0.0008	0.0020*	0.0011	0.0018	0.0000	0.0027**	0.0065***	0.0000
	(1.13)	(1.91)	1.08	1.22	-0.03	2.12	5.19	-0.01
D_{15}	-0.0023***	-0.0021**	-0.0023**	-0.0008	0.0001	-0.0053***	-0.0015	0.0016***
	(-4.68)	(-2.36)	-2.63	-0.50	0.10	-8.39	-1.04	2.68
D_{16}	0.0002	0.0004	0.0002	-0.0001	0.0000	0.0000	0.0001	-0.0003
	(0.25)	(0.50)	0.25	-0.09	-0.07	0.03	0.08	-0.50
D_{17}	-0.0009	-0.0007	-0.0003	-0.0008	0.0099***	-0.0013	-0.0007	0.0101***
	(-1.17)	(-0.67)	-0.28	-0.39	50.18	-1.08	-0.42	52.61
ARCH	0.0600***	0.1160***	0.1122***	0.1922***	0.1039***	0.0882***	0.0960***	0.1693***
	(38.31)	(27.26)	33.59	44.28	50.27	26.06	28.32	36.53
GARCH	0.9287***	0.8457***	0.8682***	0.7401***	0.8927***	0.9025***	0.8803***	0.8273***
	(547.03)	(166.53)	244.46	126.58	447.46	265.69	211.51	207.79

The GARCH (1,1) methodology used in this study has the following form: $R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 £/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t$ $+ b_6 Oil_t + b_7 Bit_t + \varepsilon_t$ where $h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + \sum_{i=1}^{17} D_i$. R_{t-j} represents the lagged value of cryptocurrency returns, n hours before R_t is observed. $b_2 £/\$_t$ represents the interaction between the selected cryptocurrency returns and £/\$, while $b_3 VIX_t$ represents the value of the VIX in the hour that the estimate R_t was observed. Finally, $b_5 S\&P_t$ and $b_6 Oil$ represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through West Texas Intermediate (WTI) respectively. $\sum_{i=1}^{17} D_i$ is included in the variance equation to provide a coefficient relating to the included seventeen dummy variables listed in Table 3. T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Table 10: Multivariate GARCH methodology using a continuous variable representing cryptocurrency cybercriminality

Variable	Bitcoin	Ethereum	Litecoin	Ripple	Stellar	Monero	Bit. Cash	Cardano
GBP/USD	0.2603	-0.4136	0.1857	0.7232	-0.3563***	-0.0840	-0.6414	-0.1867
	(0.48)	(-1.08)	(0.38)	(0.80)	(-6.40)	(-0.11)	(-0.86)	(-0.14)
VIX	0.0243	-0.0121	-0.0087	0.0406	0.0246	0.0019	0.0196	0.0224
	(1.36)	(-0.74)	(-0.45)	(1.45)	(1.03)	(0.09)	(0.89)	(0.68)
Gold	0.3161	-0.1161	-0.1151	0.1236	-1.6722***	-0.0055	-0.6468**	-0.1227
	(1.17)	(-0.50)	(-0.64)	(0.30)	(-4.82)	(-0.02)	(-2.01)	(-0.19)
S&P500	0.1495	0.0204	0.2712	0.3528	0.1936	0.1635	0.0368	0.3369
	(0.52)	(0.10)	(1.02)	(0.94)	(0.64)	(0.47)	(0.10)	(0.94)
Oil	-0.0817	-0.0510	0.0233	0.1251	-0.3224***	0.0667	0.1202	0.0385
	(-0.79)	(-0.63)	(0.31)	(0.73)	(-1.89)	(0.45)	(0.86)	(0.28)
Bitcoin	-	0.7866***	0.9286***	0.7733***	0.1332***	0.8394***	0.8162***	-
	(-)	(33.39)	(28.83)	(26.12)	(3.62)	(25.87)	(23.12)	(-)
Volatility Change	1.3916***	0.4297	1.2624***	3.2872**	1.2265*	1.4947***	0.8512	0.7668
	(5.22)	(0.66)	(3.40)	(2.29)	(1.87)	(8.82)	(1.52)	(0.15)
ARCH	0.2924***	0.1879***	0.2309***	0.4030***	0.2846***	0.2607***	0.3532***	0.4629***
	(4.35)	(8.15)	(7.32)	(18.43)	(8.55)	(2.64)	(7.79)	(6.13)
GARCH	0.5062***	0.7866***	0.7598***	0.5845***	0.9218***	0.4477***	0.6280***	0.5750***
	(7.50)	(9.84)	(10.92)	(13.91)	(13.75)	(4.42)	(7.54)	(10.45)

The GARCH (1,1) methodology used in this study has the following form: $R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 £/\$_t + b_3 VIX_t$ $+ b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + b_7 Bit_t + \varepsilon_t$ where $h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u^2_{t-1} + D_i$. R_{t-j} represents the lagged value of cryptocurrency returns, n hours before R_t is observed. $b_2 £/\$_t$ represents the interaction between the selected cryptocurrency returns and $£/\$$, while $b_3 VIX_t$ represents the value of the VIX in the hour that the estimate R_t was observed. Finally, $b_5 S\&P_t$ and $b_6 Oil$ represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through West Texas Intermediate (WTI) respectively. A continuous variable representing the combined number of cybercriminality events is included in the variance equation to provide a coefficient relating to the included seventeen dummy variables listed in Table 3. T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Table 11: Multivariate GARCH methodology analysing the effects of cryptocurrency cybercriminality based on the estimated dollar value stolen

Variable	Bitcoin	Ethereum	Litecoin	Ripple	Stellar	Monero	Bit. Cash	Cardano
GBP/USD	0.2547	-0.4272	0.1704	0.6072	-0.3523***	-0.0297	-0.6585	-0.1965
	(0.46)	(-1.12)	(0.34)	(0.70)	(-5.25)	(-0.04)	(-0.89)	(-0.14)
VIX	0.0231	-0.0113	-0.0098	0.0326	0.0262	0.0083	0.0168	0.0237
	(1.31)	(-0.68)	(-0.52)	(1.19)	(1.11)	(0.45)	(0.79)	(0.71)
Gold	0.3161	-0.1311	-0.1053	-0.0039	-1.6372***	0.0011	-0.6576**	-0.0862
	(1.09)	(-0.56)	(-0.55)	(-0.01)	(-4.58)	(0.00)	(-2.05)	(-0.13)
S&P500	0.1698	0.0380	0.2759	0.2700	0.2316	0.2174	0.0163	0.3542
	(0.58)	(0.18)	(1.05)	(0.71)	(0.75)	(0.65)	(0.05)	(0.92)
Oil	-0.0963	-0.0549	0.0204	0.1685	-0.3233*	0.0402	0.1244	0.0422
	(-0.95)	(-0.68)	(0.27)	(1.07)	(-1.90)	(0.28)	(0.88)	(0.30)
Bitcoin	-	0.7856***	0.9311***	0.7792***	0.1329***	0.8471***	0.8191***	-
	(-)	(32.94)	(28.63)	(23.62)	(3.57)	(25.52)	(23.00)	(-)
Volatility Change	0.0705***	0.0289	0.0640***	0.1460***	0.0609	0.0866***	0.0434	0.1190
	(4.41)	(0.82)	(2.87)	(2.77)	(1.60)	(7.24)	(1.29)	(0.13)
ARCH	0.2860***	0.1810***	0.2226***	0.4549***	0.2821***	0.2804***	0.3767***	0.4521***
	(4.15)	(7.97)	(7.14)	(14.73)	(8.50)	(2.79)	(7.83)	(6.08)
GARCH	0.5221***	0.7946***	0.7621***	0.5813***	0.9239***	0.4649***	0.6292***	0.5834***
	(7.58)	(9.74)	(10.72)	(15.33)	(13.72)	(4.39)	(7.50)	(10.72)

The GARCH (1,1) methodology used in this study has the following form:
$R_t = a_0 + \sum_{j=1}^{5} b_j R_{t-j} + b_2 £/\$_t + b_3 VIX_t + b_4 Gold_t + b_5 S\&P_t + b_6 Oil_t + b_7 Bit_t + \varepsilon_t$ where
$h_t = \omega + \alpha_1 h_{t-1} + \beta_1 u_{t-1}^2 + D_{USD\$_i}$. R_{t-j} represents the lagged value of cryptocurrency returns, n hours before R_t is observed. $b_2 £/\$_t$ represents the interaction between the selected cryptocurrency returns and £/\$, while $b_3 VIX_t$ represents the value of the VIX in the hour that the estimate R_t was observed. Finally, $b_5 S\&P_t$ and $b_6 Oil$ represent the relationship between cryptocurrency returns and the returns of the S&P500 and oil as measured through West Texas Intermediate (WTI) respectively. A continuous variable representing the natural logarithm of the estimated dollar value stolen due to cybercriminality is included in the variance equation to provide a coefficient relating to the included seventeen dummy variables listed in Table 3. T-statistics are in parentheses. *, ** and *** indicate significance at the 10%, 5% and 1% levels, respectively.

Table 12: Dynamic correlations between selected cryptocurrency markets during hacking events

	ET-BT	LT-BT	RI-BT	ST-BT	MO-BT	Bc-BT	LT-ET	RI-ET	ST-ET	MO-ET	Bc-ET	RI-LT	ST-LT
Total	0.01	0.02	0.01	0.00	0.01	0.01	0.02	0.02	0.01	0.02	0.01	0.02	0.01
D_1	0.01	0.02	0.01	0.01	0.01	0.01	0.02	0.01	0.00	0.01	0.02	0.02	0.00
D_2	0.00	0.01	0.00	0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.01	0.00
D_3	0.01	0.02	0.01	0.01	0.04	0.01	0.02	0.01	0.02	0.04	0.02	0.01	0.03
D_4	0.16	0.25	0.19	0.05	0.17	0.12	0.24	0.20	0.07	0.16	0.13	0.33	0.13
D_5	0.10	0.13	0.13	0.07	0.10	0.11	0.14	0.17	0.07	0.10	0.12	0.19	0.11
D_6	0.02	0.02	0.02	0.00	0.02	0.02	0.01	0.02	0.00	0.02	0.02	0.02	0.00
D_7	0.04	0.06	0.04	0.02	0.04	0.03	0.06	0.05	0.02	0.04	0.03	0.07	0.04
D_8	0.02	0.02	0.03	0.00	0.02	0.02	0.02	0.03	0.00	0.02	0.02	0.03	0.00
D_9	0.02	0.02	0.03	0.01	0.02	0.02	0.02	0.03	0.01	0.02	0.02	0.03	0.01
D_{10}	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.00
D_{11}	0.03	0.03	0.02	0.00	0.03	0.03	0.02	0.02	0.00	0.03	0.02	0.02	0.00
D_{12}	0.02	0.02	0.02	0.00	0.02	0.02	0.02	0.02	0.01	0.02	0.02	0.02	0.00
D_{13}	0.02	0.02	0.02	0.00	0.02	0.02	0.02	0.03	0.00	0.02	0.02	0.03	0.00
D_{14}	0.01	0.00	0.00	0.00	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.00
D_{15}	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.01	0.02	0.01	0.01	0.01
D_{16}	0.01	0.00	0.01	0.00	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.00
D_{17}	0.00	0.00	0.01	0.00	0.01	0.00	0.01	0.01	0.00	0.01	0.01	0.01	0.00

	MO-LT	Bc-LT	CA-LT	ST-RI	MO-RI	Bc-RI	CA-RI	MO-ST	Bc-ST	CA-ST	Bc-MO	CA-MO	CA-Bc
Total	0.02	0.02	0.00	0.01	0.02	0.01	0.01	0.01	0.00	0.01	0.02	0.01	0.00
D_1	0.01	0.03	0.00	0.00	0.00	0.01	0.00	0.01	-0.02	0.01	0.00	0.00	0.02
D_2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.01	0.00	0.00
D_3	0.05	0.04	0.02	0.01	0.02	0.01	0.01	0.05	0.04	0.06	0.05	0.02	0.02
D_4	0.25	0.18	0.05	0.17	0.19	0.12	0.06	0.08	0.04	0.06	0.17	0.02	0.02
D_5	0.14	0.16	0.03	0.11	0.10	0.13	0.04	0.09	0.10	0.04	0.15	0.03	0.03
D_6	0.02	0.02	0.00	0.00	0.02	0.02	0.00	0.00	0.00	0.00	0.02	0.00	0.00
D_7	0.06	0.05	0.04	0.03	0.04	0.03	0.03	0.02	0.02	0.02	0.03	0.02	0.02
D_8	0.02	0.02	0.00	0.01	0.03	0.02	0.01	0.00	0.00	0.01	0.02	0.00	0.00
D_9	0.02	0.02	0.00	0.01	0.03	0.02	0.01	0.01	0.00	0.00	0.02	0.00	0.00
D_{10}	0.01	0.01	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.00
D_{11}	0.02	0.02	0.00	0.00	0.02	0.02	0.00	0.00	0.00	0.00	0.03	0.00	0.00
D_{12}	0.01	0.02	0.00	0.01	0.02	0.02	0.00	0.00	0.01	0.00	0.02	0.00	0.00
D_{13}	0.02	0.02	0.00	0.01	0.03	0.03	0.01	0.00	0.00	0.01	0.02	0.00	0.00
D_{14}	0.01	0.01	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.01
D_{15}	0.02	0.01	0.01	0.01	0.02	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.01
D_{16}	0.01	0.01	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.00
D_{17}	0.01	0.01	0.00	0.00	0.01	0.01	0.01	0.01	0.00	0.12	0.00	0.01	0.01

Note: For presentation purposes, the names of the selected cryptocurrencies have been shortened. They are now presented as BT (Bitcoin), ET (Ethereum), LT (Litecoin), RI (Ripple), ST (Stellar), MO (Monero), Bc (Bitcoin Cash), and CA (Cardano). Results are scaled for presentation purposes by multiplying original coefficients by 10^2. For brevity we have only included selected abnormal return results. All other results related to the abnormal returns of cryptocurrencies due to hacking events are available from the authors on request. The results indicate the dynamic correlations between the stated products at the time of each hacking event. We estimate the impact of external shocks on the dynamic conditional correlation features. We regress the time-varying correlation model as follows: $\rho_{ij,t} = \omega_{ij} + \Sigma_{p=1}^{p} \varphi_p \rho_{ij,t-p} + \Sigma_{k=1}^{2} \alpha_k DM_{k,t} + \varepsilon_{ij,t}$ where $\rho_{ij,t}$ is the pair-wise conditional correlation coefficient between the cryptocurrency i and cryptocurrency j. DM_1 is a dummy variable denoting the date of the cybercrime incident.The shaded areas represent the periods that incorporate major cryptocurrency hacking events that are denoted in Table 6.

Table 13: Overview of the acceptance and rejection of the selected research hypotheses

Hypothesis	Description	Result	Note
H_1	Does the intra-day volatility of cryptocurrencies change significantly when traditional markets are closed?	Reject	We identified clear differences between the investigated cryptocurrency markets with both substantial and significant differences in intra-day volatility depending on the operational trading hours investigated. However, despite this, the variation between the individual markets do not correlate across all eight of the investigated markets, therefore, although we can state that on average there are substantial differences based on differing opening times, we cannot definitively state that this is the same for all cryptocurrencies.
H_2	Does the intra-day volatility of cryptocurrencies change significantly at the weekend when compared to weekdays?	Accept	There is a clear difference weekend effect in cryptocurrency markets, but also there is evidence of elevated intra-day volatility during the week and a substantial reduction at the weekend.
H_3	Is there a difference in intra-day cryptocurrency volatility based on the opening hours of major international financial markets?	Accept	intra-day volatility is found to be substantially elevated while both European and United States financial markets are trading with the exception of Cardano during European opening and Ripple, Bitcoin Cash and Cardano during United States opening. However, cryptocurrency volatility is broadly below average during both Japanese and Chinese trading times with the exception of results for Stellar, and again, Bitcoin Cash and Cardano. This presents evidence supporting the hypothesis that cryptocurrency intra-day volatility behaves in a different manner depending on the exchange that is open.
H_4	Does cryptocurrency market volatility change substantially based on the hour-of-the-day in which trading takes place?	Reject	Despite a number of alternative specifications and differing frequencies of investigation, there are a number of differing times where individual cryptocurrencies exhibit elevated levels of GARCH-calculated volatility, but there is no evidence to support hypothesis H_4 across the cryptocurrency markets investigated.
H_5	Has cryptocurrency volatility varied substantially during periods of traditional market volatility?	Accept	We identify evidence indicating that periods denoted to contain substantial volatility in the markets for both oil and GBP/USD are also associated with sharp, significant increases in the volatility of cryptocurrency markets.
H_6	Does cryptocurrency market volatility change substantially in the aftermath of cybercriminality?	Accept	We can identify that there are sharp volatility responses in cryptocurrency markets during cybercrime events, which appear to be rationally targeted at cryptocurrencies directly involved and the broader sector of cryptocurrencies should the cybercrime event be systemically damaging.
H_7	Does such cryptocurrency volatility vary by severity of cybercriminality event?	Accept	It must be noted that although the results of four markets remain insignificant, all results are positive throughout this analysis, with Cardano presenting evidence of a substantial positive relationship between the dollar-valued scale of cybercriminality and GARCH-calculated volatility measure.
H_8	Do the conditional correlations between cryptocurrency markets change substantially in the aftermath of cybercriminality events?	Accept	There are two broad results: we observe that there are lower estimates identified for smaller capitalisation cryptocurrencies when compared to the cross-correlations between their larger counterparts. Secondly, we can identify two specific periods where there is a sustained increase in cross-cryptocurrency correlations as controlled for each hacking event.
H_9	Does the information share and component share of price discovery change between the periods before and after cybercrime events in cryptocurrency markets?	Accept	There is significant evidence provided to suggest that cybercriminality can distort these information share with the investigated pricing relationships and can also influence large and small cryptocurrencies in a different manner.

Note: The development of the above hypotheses are explained throughout Section 2, with the selected methodology presented in Section 4.

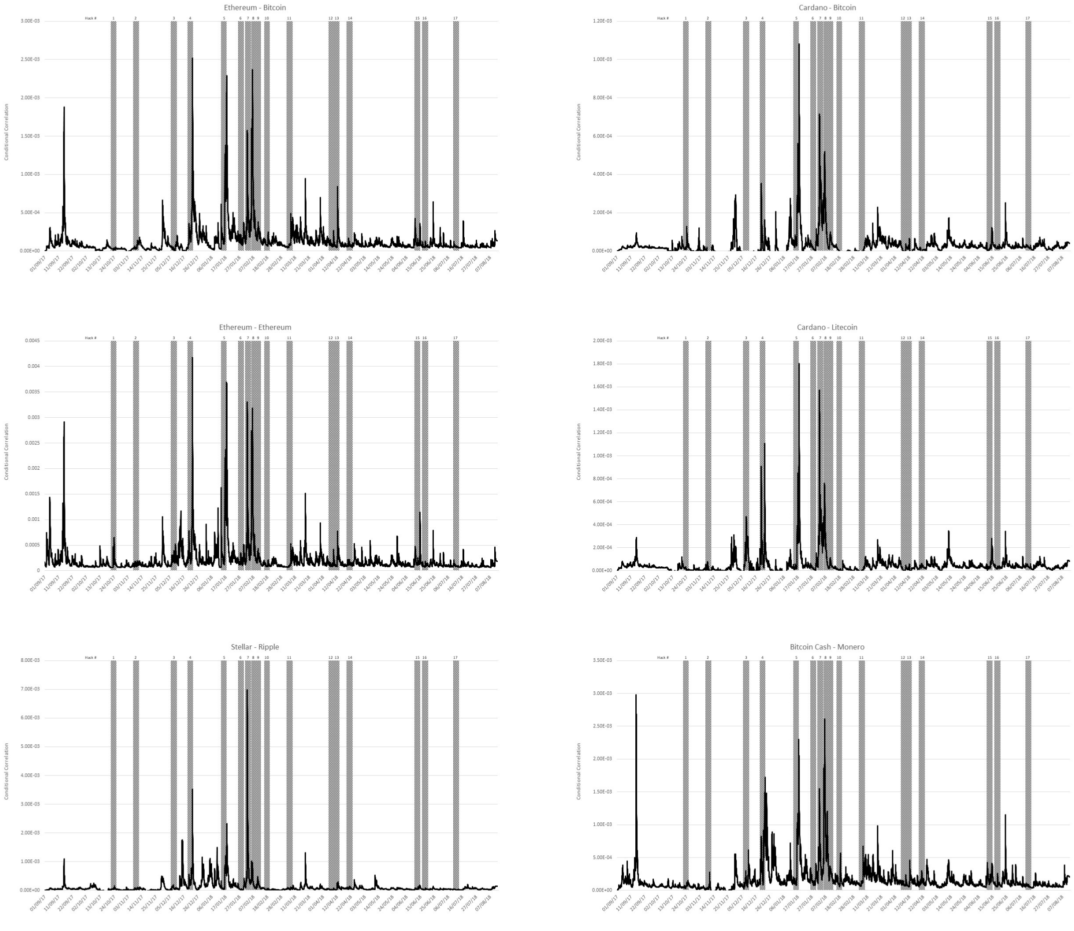
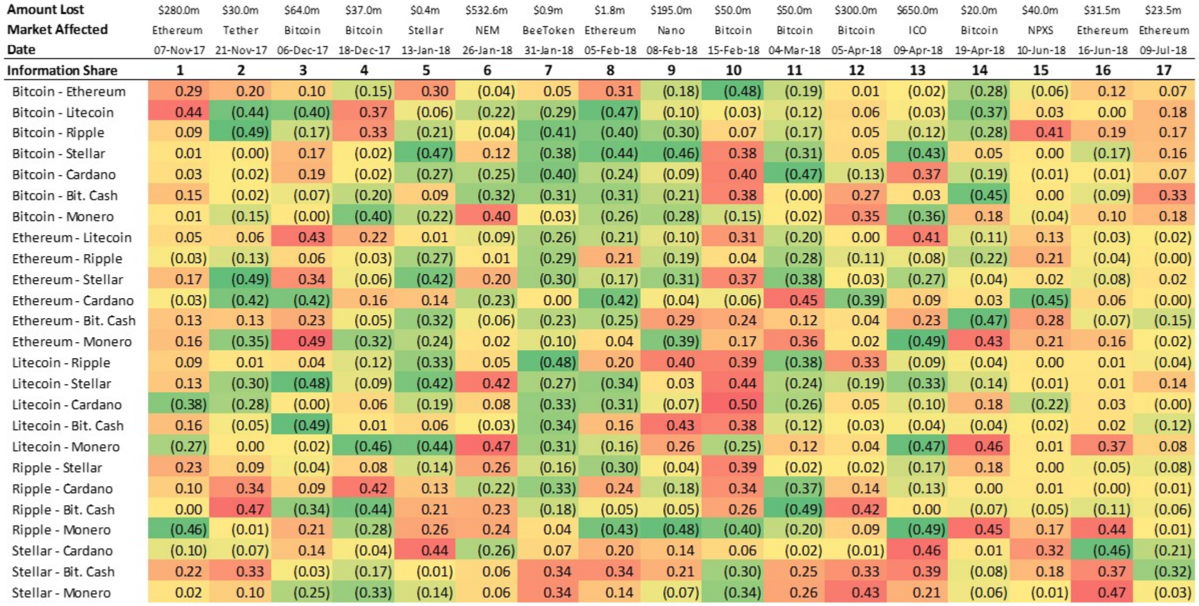
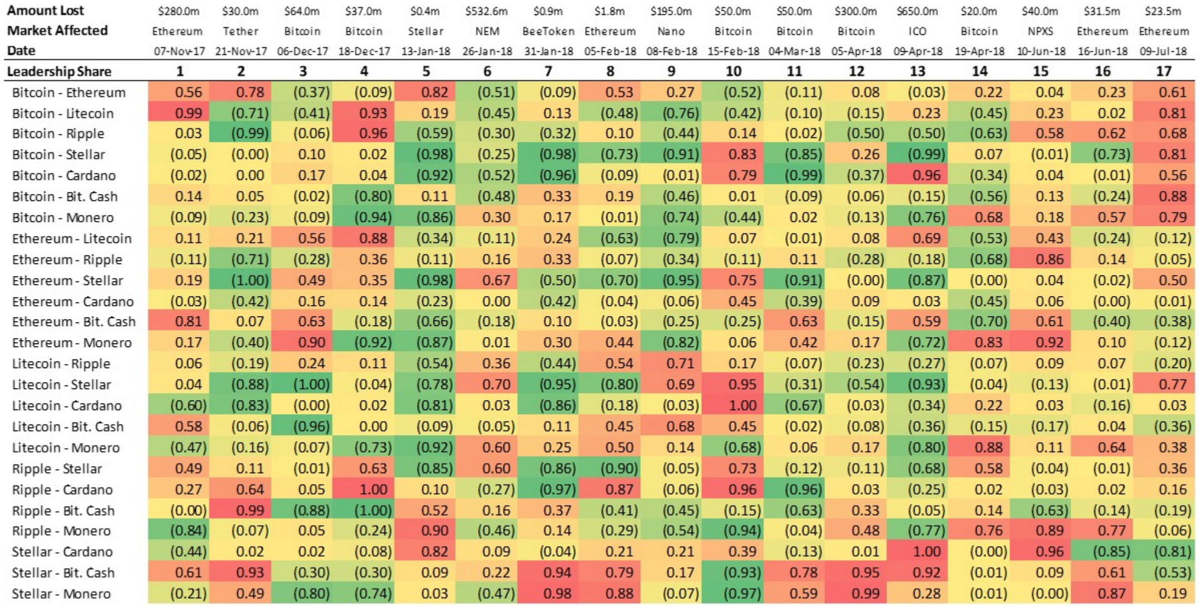


Figure 1: **Selected dynamic correlations between cryptocurrencies during cybercrime events**
We examine the DCC-GARCH model's change in behaviour before and after cybercriminility in cryptocurrency markets occur. In a first stage analysis, we estimate the impact of external shocks on the dynamic conditional correlation features. We regress the time-varying correlation model as follows: $\rho_{ij,t} = \omega_{ij} + \Sigma_{p=1}^{p} \varphi_p \rho_{ij,t-p} + \Sigma_{k=1}^{2} \alpha_k DM_{k,t} + \varepsilon_{ij,t}$ where $\rho_{ij,t}$ is the pair-wise conditional correlation coefficient between the cryptocurrency i and cryptocurrency j. DM_1 is a dummy variable denoting the date of the cybercrime incident.The shaded areas represent the periods that incorporate major cryptocurrency hacking events that are denoted in Table 3. For brevity we have only included selected dynamic correlation results. All other results related to the abnormal returns of cryptocurrencies due to hacking events are available from the authors on request.



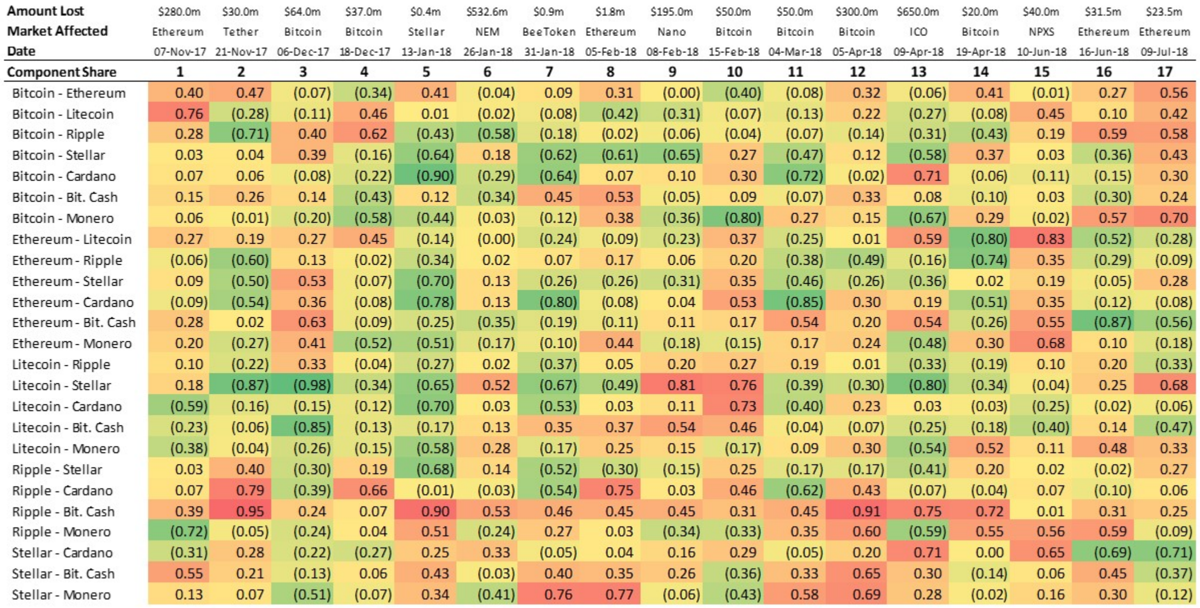
Amount Lost	$280.0m	$30.0m	$64.0m	$37.0m	$0.4m	$532.6m	$0.9m	$1.8m	$195.0m	$50.0m	$50.0m	$300.0m	$650.0m	$20.0m	$40.0m	$31.5m	$23.5m
Market Affected	Ethereum	Tether	Bitcoin	Bitcoin	Stellar	NEM	BeeToken	Ethereum	Nano	Bitcoin	Bitcoin	Bitcoin	ICO	Bitcoin	NPXS	Ethereum	Ethereum
Date	07-Nov-17	21-Nov-17	06-Dec-17	18-Dec-17	13-Jan-18	26-Jan-18	31-Jan-18	05-Feb-18	08-Feb-18	15-Feb-18	04-Mar-18	05-Apr-18	09-Apr-18	19-Apr-18	10-Jun-18	16-Jun-18	09-Jul-18
Information Share	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Bitcoin - Ethereum	0.29	0.20	0.10	(0.15)	0.30	(0.04)	0.05	0.31	(0.18)	(0.48)	(0.19)	0.01	(0.02)	(0.28)	(0.06)	0.12	0.07
Bitcoin - Litecoin	0.44	(0.44)	(0.40)	0.37	(0.06)	(0.22)	(0.29)	(0.47)	(0.10)	(0.03)	(0.12)	0.06	(0.03)	(0.37)	0.03	0.00	0.18
Bitcoin - Ripple	0.09	(0.49)	(0.17)	0.33	(0.21)	(0.04)	(0.41)	(0.40)	(0.30)	0.07	(0.17)	0.05	(0.12)	(0.28)	0.41	0.19	0.17
Bitcoin - Stellar	0.01	(0.00)	0.17	(0.02)	(0.47)	0.12	(0.38)	(0.44)	(0.46)	0.38	(0.31)	0.05	(0.43)	0.05	0.00	(0.17)	0.16
Bitcoin - Cardano	0.03	(0.02)	0.19	(0.02)	(0.27)	(0.25)	(0.40)	(0.24)	(0.09)	0.40	(0.47)	(0.13)	0.37	(0.19)	(0.01)	(0.01)	0.07
Bitcoin - Bit. Cash	0.15	(0.02)	(0.07)	(0.20)	0.09	(0.32)	(0.31)	(0.31)	(0.21)	0.38	(0.00)	0.27	0.03	(0.45)	0.00	(0.09)	0.33
Bitcoin - Monero	0.01	(0.15)	(0.00)	(0.40)	(0.22)	0.40	(0.03)	(0.26)	(0.28)	(0.15)	(0.02)	0.35	(0.36)	0.18	(0.04)	0.10	0.18
Ethereum - Litecoin	0.05	0.06	0.43	0.22	0.01	(0.09)	(0.26)	(0.21)	(0.10)	0.31	(0.20)	0.00	0.41	(0.11)	0.13	(0.03)	(0.02)
Ethereum - Ripple	(0.03)	(0.13)	0.06	(0.03)	(0.27)	0.01	(0.29)	0.21	(0.19)	0.04	(0.28)	(0.11)	(0.08)	(0.22)	0.21	(0.04)	(0.00)
Ethereum - Stellar	0.17	(0.49)	0.34	(0.06)	(0.42)	0.20	(0.30)	(0.17)	(0.31)	0.37	(0.38)	(0.03)	(0.27)	(0.04)	0.02	(0.08)	0.02
Ethereum - Cardano	(0.03)	(0.42)	(0.42)	0.16	0.14	(0.23)	0.00	(0.42)	(0.04)	(0.06)	0.45	(0.39)	0.09	0.03	(0.45)	0.06	(0.00)
Ethereum - Bit. Cash	0.13	0.13	0.23	(0.05)	(0.32)	(0.06)	(0.23)	(0.25)	0.29	0.24	0.12	0.04	0.23	(0.47)	0.28	(0.07)	(0.15)
Ethereum - Monero	0.16	(0.35)	0.49	(0.32)	(0.24)	0.02	(0.10)	0.04	(0.39)	0.17	0.36	0.02	(0.49)	0.43	0.21	0.16	(0.02)
Litecoin - Ripple	0.09	0.01	0.04	(0.12)	(0.33)	0.05	(0.48)	0.20	0.40	0.39	(0.38)	0.33	(0.09)	(0.04)	0.00	0.01	(0.04)
Litecoin - Stellar	0.13	(0.30)	(0.48)	(0.09)	(0.42)	0.42	(0.27)	(0.34)	0.03	0.44	(0.24)	(0.19)	(0.33)	(0.14)	(0.01)	0.01	0.14
Litecoin - Cardano	(0.38)	(0.28)	(0.00)	0.06	(0.19)	0.08	(0.33)	(0.31)	(0.07)	0.50	(0.26)	0.05	(0.10)	0.18	(0.22)	0.03	(0.00)
Litecoin - Bit. Cash	0.16	(0.05)	(0.49)	0.01	0.06	(0.03)	(0.34)	0.16	0.43	0.38	(0.12)	(0.03)	(0.04)	(0.04)	(0.02)	0.02	(0.12)
Litecoin - Monero	(0.27)	0.00	(0.02)	(0.46)	(0.44)	0.47	(0.31)	(0.16)	0.26	(0.25)	0.12	0.04	(0.47)	0.46	0.01	0.37	0.08
Ripple - Stellar	0.23	0.09	(0.04)	0.08	(0.14)	0.26	(0.16)	(0.30)	(0.04)	0.39	(0.02)	(0.02)	(0.17)	0.18	0.00	(0.05)	(0.08)
Ripple - Cardano	0.10	0.34	0.09	0.42	0.13	(0.22)	(0.33)	0.24	(0.18)	0.34	(0.37)	0.14	(0.13)	0.00	0.01	(0.00)	(0.01)
Ripple - Bit. Cash	0.00	0.47	(0.34)	(0.44)	0.21	0.23	(0.18)	(0.05)	(0.05)	0.26	(0.49)	0.42	0.00	(0.07)	(0.05)	(0.11)	(0.06)
Ripple - Monero	(0.46)	(0.01)	0.21	(0.28)	0.26	0.24	0.04	(0.43)	(0.48)	(0.40)	(0.20)	0.09	(0.49)	0.45	0.17	0.44	(0.01)
Stellar - Cardano	(0.10)	(0.07)	0.14	(0.04)	0.44	(0.26)	0.07	0.20	0.14	0.06	(0.02)	(0.01)	0.46	0.01	0.32	(0.46)	(0.21)
Stellar - Bit. Cash	0.22	0.33	(0.03)	(0.17)	(0.01)	0.06	0.34	0.34	0.21	(0.30)	0.25	0.33	0.39	(0.08)	0.18	0.37	(0.32)
Stellar - Monero	0.02	0.10	(0.25)	(0.33)	(0.14)	0.06	0.34	0.14	(0.07)	(0.34)	0.26	0.43	0.21	(0.06)	(0.01)	0.47	(0.03)

Figure 2: **Change in Information Share (IS) between cryptocurrencies in the period after a hacking event**
The above figure represents the change in the information share of price discovery in the period before each of the hacking events that are denoted in Table 3. We estimate IS using the error correction parameters and variance-covariance of the error terms from the Vector Error Correction Model (VECM): $\Delta_{p1,t} = \alpha_1(p_{1,t-1} - p_{2,t-1}) + \sum_{i=1}^{200} \gamma_i \Delta p_{1,t-i} + \sum_{j=1}^{200} \delta_j \Delta p_{2,t-j} + \varepsilon_{1,t}$ and $\Delta_{p2,t} = \alpha_2(p_{1,t-1} - p_{2,t-1}) + \sum_{k=1}^{200} \varphi_k \Delta p_{1,t-k} + \sum_{m=1}^{200} \phi_m \Delta p_{2,t-m} + \varepsilon_{2,t}$ where $\Delta p_{i,t}$ is the change in the log price $(p_{i,t})$ of the asset traded in market i at time t. Given the covariance matrix of the reduced form VECM error terms where: $M = \begin{pmatrix} m_{11} & 0 \\ m_{12} & m_{22} \end{pmatrix} = \begin{pmatrix} \sigma_1 & 0 \\ \rho\sigma_2 & \sigma_2(1-\rho^2)^{\frac{1}{2}} \end{pmatrix}$ we calculate the IS using: $IS_1 = \frac{(\gamma_1 m_{11} + \gamma_2 m_{12})^2}{(\gamma_1 m_{11} + \gamma_2 m_{12})^2 + (\gamma_2 m_{22})^2}$ and $IS_2 = \frac{(\gamma_2 m_{22})^2}{(\gamma_1 m_{11} + \gamma_2 m_{12})^2 + (\gamma_2 m_{22})^2}$. The heatmap is colour-coded so that green cells denoted large increases in the share of price discovery from cryptocurrency A to B, while red cells denoted large increases in the share of price discovery from cryptocurrency B to A.



Amount Lost	$280.0m	$30.0m	$64.0m	$37.0m	$0.4m	$532.6m	$0.9m	$1.8m	$195.0m	$50.0m	$50.0m	$300.0m	$650.0m	$20.0m	$40.0m	$31.5m	$23.5m
Market Affected	Ethereum	Tether	Bitcoin	Bitcoin	Stellar	NEM	BeeToken	Ethereum	Nano	Bitcoin	Bitcoin	Bitcoin	ICO	Bitcoin	NPXS	Ethereum	Ethereum
Date	07-Nov-17	21-Nov-17	06-Dec-17	18-Dec-17	13-Jan-18	26-Jan-18	31-Jan-18	05-Feb-18	08-Feb-18	15-Feb-18	04-Mar-18	05-Apr-18	09-Apr-18	19-Apr-18	10-Jun-18	16-Jun-18	09-Jul-18
Leadership Share	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Bitcoin - Ethereum	0.56	0.78	(0.37)	(0.09)	0.82	(0.51)	(0.09)	0.53	0.27	(0.52)	(0.11)	0.08	(0.03)	0.22	0.04	0.23	0.61
Bitcoin - Litecoin	0.99	(0.71)	(0.41)	0.93	0.19	(0.45)	0.13	(0.48)	(0.76)	(0.42)	(0.10)	(0.15)	0.23	(0.45)	0.23	0.02	0.81
Bitcoin - Ripple	0.03	(0.99)	(0.06)	0.96	(0.59)	(0.30)	(0.32)	0.10	(0.44)	0.14	(0.02)	(0.50)	(0.50)	(0.63)	0.58	0.62	0.68
Bitcoin - Stellar	(0.05)	(0.00)	0.10	0.02	(0.98)	(0.25)	(0.98)	(0.73)	(0.91)	0.83	(0.85)	0.26	(0.99)	0.07	(0.01)	(0.73)	0.81
Bitcoin - Cardano	(0.02)	0.00	0.17	0.04	(0.92)	(0.52)	(0.96)	(0.09)	(0.01)	0.79	(0.99)	(0.37)	0.96	(0.34)	0.04	(0.01)	0.56
Bitcoin - Bit. Cash	0.14	0.05	(0.02)	(0.80)	0.11	(0.48)	0.33	0.19	(0.46)	0.01	(0.09)	(0.06)	(0.15)	(0.56)	0.13	(0.24)	0.88
Bitcoin - Monero	(0.09)	(0.23)	(0.09)	(0.94)	(0.86)	0.30	0.17	(0.01)	(0.74)	(0.44)	0.02	(0.13)	(0.76)	0.68	0.18	0.57	0.79
Ethereum - Litecoin	0.11	0.21	0.56	0.88	(0.34)	(0.11)	0.24	(0.63)	(0.79)	0.07	(0.01)	0.08	0.69	(0.53)	0.43	(0.24)	(0.12)
Ethereum - Ripple	(0.11)	(0.71)	(0.28)	0.36	(0.11)	0.16	0.33	(0.07)	(0.34)	(0.11)	0.11	(0.28)	(0.18)	(0.68)	0.86	0.14	(0.05)
Ethereum - Stellar	0.19	(1.00)	0.49	0.35	(0.98)	0.67	(0.50)	(0.70)	(0.95)	0.75	(0.91)	(0.00)	(0.87)	(0.00)	0.04	(0.02)	0.50
Ethereum - Cardano	(0.03)	(0.42)	0.16	0.14	(0.23)	0.00	(0.42)	(0.04)	(0.06)	0.45	(0.39)	0.09	0.03	(0.45)	0.06	(0.00)	(0.01)
Ethereum - Bit. Cash	0.81	0.07	0.63	(0.18)	(0.66)	(0.18)	0.10	(0.03)	(0.25)	(0.25)	0.63	(0.15)	0.59	(0.70)	0.61	(0.40)	(0.38)
Ethereum - Monero	0.17	(0.40)	0.90	(0.92)	(0.87)	0.01	0.30	0.44	(0.82)	0.06	0.42	0.17	(0.72)	0.83	0.92	0.10	(0.12)
Litecoin - Ripple	0.06	(0.19)	0.24	0.11	(0.54)	0.36	(0.44)	0.54	0.71	0.17	(0.07)	(0.23)	(0.27)	(0.07)	0.09	0.07	(0.20)
Litecoin - Stellar	0.04	(0.88)	(1.00)	(0.04)	(0.78)	0.70	(0.95)	(0.80)	0.69	0.95	(0.31)	(0.54)	(0.93)	(0.04)	(0.13)	(0.01)	0.77
Litecoin - Cardano	(0.60)	(0.83)	(0.00)	0.02	(0.81)	0.03	(0.86)	(0.18)	(0.03)	1.00	(0.67)	(0.03)	(0.34)	0.22	0.03	(0.16)	0.03
Litecoin - Bit. Cash	0.58	(0.06)	(0.96)	0.00	(0.09)	(0.05)	0.11	0.45	0.68	0.45	(0.02)	(0.08)	(0.36)	(0.15)	(0.17)	0.04	(0.36)
Litecoin - Monero	(0.47)	(0.16)	(0.07)	(0.73)	(0.92)	0.60	0.25	0.50	0.14	(0.68)	0.06	0.17	(0.80)	0.88	0.11	0.64	0.38
Ripple - Stellar	0.49	0.11	(0.01)	0.63	(0.85)	0.60	(0.86)	(0.90)	(0.05)	0.73	(0.12)	(0.11)	(0.68)	0.58	(0.04)	(0.01)	0.36
Ripple - Cardano	0.27	0.64	0.05	1.00	0.10	(0.27)	(0.97)	0.87	(0.06)	0.96	(0.96)	0.03	(0.25)	0.02	(0.03)	0.02	0.16
Ripple - Bit. Cash	(0.00)	0.99	(0.88)	(1.00)	0.52	0.16	0.37	(0.41)	(0.45)	(0.15)	(0.63)	0.33	(0.05)	0.14	(0.63)	(0.14)	(0.19)
Ripple - Monero	(0.84)	(0.07)	0.05	(0.24)	0.90	(0.46)	0.14	(0.29)	(0.54)	(0.94)	(0.04)	0.48	(0.77)	0.76	0.89	0.77	(0.06)
Stellar - Cardano	(0.44)	0.02	0.02	(0.08)	0.82	0.09	(0.04)	0.21	0.21	0.39	(0.13)	0.01	1.00	(0.00)	0.96	(0.85)	(0.81)
Stellar - Bit. Cash	0.61	0.93	(0.30)	(0.30)	0.09	0.22	0.94	0.79	0.17	(0.93)	0.78	0.95	0.92	(0.01)	0.09	0.61	(0.53)
Stellar - Monero	(0.21)	0.49	(0.80)	(0.74)	0.03	(0.47)	0.98	0.88	(0.07)	(0.97)	0.59	0.99	0.28	(0.01)	(0.00)	0.87	0.19

Figure 3: **Change in Information Leadership Share (ILS) between cryptocurrencies in the period after a hacking event**
The above figure represents the change in the information leadership share of price discovery in the period before each of the hacking events that are denoted in Table 3. We estimate ILS using the error correction parameters and variance-covariance of the error terms from the Vector Error Correction Model (VECM): $\Delta_{p1,t} = \alpha_1(p_{1,t-1} - p_{2,t-1}) + \sum_{i=1}^{200} \gamma_i \Delta p_{1,t-i} + \sum_{j=1}^{200} \delta_j \Delta p_{2,t-j} + \varepsilon_{1,t}$ and $\Delta_{p2,t} = \alpha_2(p_{1,t-1} - p_{2,t-1}) + \sum_{k=1}^{200} \varphi_k \Delta p_{1,t-k} + \sum_{m=1}^{200} \phi_m \Delta p_{2,t-m} + \varepsilon_{2,t}$ where $\Delta p_{i,t}$ is the change in the log price $(p_{i,t})$ of the asset traded in market i at time t. Recent studies show that IS and CS are sensitive to the relative level of noise in each market, they measure a combination of leadership in impounding new information and the relative level of noise in the price series from each market. The measures tend to overstate the price discovery contribution of the less noisy market. An appropriate combination of IS and CS cancels out dependence on noise. The combined measure is known as the Information Leadership Share (ILS) which is calculated as: $ILS_1 = \frac{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right|}{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right| + \left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|}$ and $ILS_2 = \frac{\left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|}{\left|\frac{IS_1}{IS_2}\frac{CS_2}{CS_1}\right| + \left|\frac{IS_2}{IS_1}\frac{CS_1}{CS_2}\right|}$



Amount Lost	$280.0m	$30.0m	$64.0m	$37.0m	$0.4m	$532.6m	$0.9m	$1.8m	$195.0m	$50.0m	$50.0m	$300.0m	$650.0m	$20.0m	$40.0m	$31.5m	$23.5m
Market Affected	Ethereum	Tether	Bitcoin	Bitcoin	Stellar	NEM	BeeToken	Ethereum	Nano	Bitcoin	Bitcoin	Bitcoin	ICO	Bitcoin	NPXS	Ethereum	Ethereum
Date	07-Nov-17	21-Nov-17	06-Dec-17	18-Dec-17	13-Jan-18	26-Jan-18	31-Jan-18	05-Feb-18	08-Feb-18	15-Feb-18	04-Mar-18	05-Apr-18	09-Apr-18	19-Apr-18	10-Jun-18	16-Jun-18	09-Jul-18
Component Share	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Bitcoin - Ethereum	0.40	0.47	(0.07)	(0.34)	0.41	(0.04)	0.09	0.31	(0.00)	(0.40)	(0.08)	0.32	(0.06)	0.41	(0.01)	0.27	0.56
Bitcoin - Litecoin	0.76	(0.28)	(0.11)	0.46	0.01	(0.02)	(0.08)	(0.42)	(0.31)	(0.07)	(0.13)	0.22	(0.27)	(0.08)	0.45	0.10	0.42
Bitcoin - Ripple	0.28	(0.71)	0.40	0.62	(0.43)	(0.58)	(0.18)	(0.02)	(0.06)	(0.04)	(0.07)	(0.14)	(0.31)	(0.43)	0.19	0.59	0.58
Bitcoin - Stellar	0.03	0.04	0.39	(0.16)	(0.64)	0.18	(0.62)	(0.61)	(0.65)	0.27	(0.47)	0.12	(0.58)	0.37	0.03	(0.36)	0.43
Bitcoin - Cardano	0.07	0.06	(0.08)	(0.22)	(0.90)	(0.29)	(0.64)	0.07	0.10	0.30	(0.72)	(0.02)	0.71	(0.06)	(0.11)	(0.15)	0.30
Bitcoin - Bit. Cash	0.15	0.26	0.14	(0.43)	0.12	(0.34)	0.45	0.53	(0.05)	0.09	(0.07)	0.33	0.08	(0.10)	0.03	(0.30)	0.24
Bitcoin - Monero	0.06	(0.01)	(0.20)	(0.58)	(0.44)	(0.03)	(0.12)	0.38	(0.36)	(0.80)	0.27	0.15	(0.67)	0.29	(0.02)	0.57	0.70
Ethereum - Litecoin	0.27	0.19	0.27	0.45	(0.14)	(0.00)	(0.24)	(0.09)	(0.23)	0.37	(0.25)	0.01	0.59	(0.80)	0.83	(0.52)	(0.28)
Ethereum - Ripple	(0.06)	(0.60)	0.13	(0.02)	(0.34)	0.02	0.07	0.17	0.06	0.20	(0.38)	(0.49)	(0.16)	(0.74)	0.35	(0.29)	(0.09)
Ethereum - Stellar	0.09	(0.50)	0.53	(0.07)	(0.70)	0.13	(0.26)	(0.26)	(0.31)	0.35	(0.46)	(0.26)	(0.36)	0.02	0.19	(0.05)	0.28
Ethereum - Cardano	(0.09)	(0.54)	0.36	(0.08)	(0.78)	0.13	(0.80)	(0.08)	0.04	0.53	(0.85)	0.30	0.19	(0.51)	0.35	(0.12)	(0.08)
Ethereum - Bit. Cash	0.28	0.02	0.63	(0.09)	(0.25)	(0.35)	(0.19)	(0.11)	0.11	0.17	0.54	0.20	0.54	(0.26)	0.55	(0.87)	(0.56)
Ethereum - Monero	0.20	(0.27)	0.41	(0.52)	(0.51)	(0.17)	(0.10)	0.44	(0.18)	(0.15)	0.17	0.24	(0.48)	0.30	0.68	0.10	(0.18)
Litecoin - Ripple	0.10	(0.22)	0.33	(0.04)	(0.27)	0.02	(0.37)	0.05	0.20	0.27	0.19	0.01	(0.33)	(0.19)	0.10	0.20	(0.33)
Litecoin - Stellar	0.18	(0.87)	(0.98)	(0.34)	(0.65)	0.52	(0.67)	(0.49)	0.81	0.76	(0.39)	(0.30)	(0.80)	(0.34)	(0.04)	0.25	0.68
Litecoin - Cardano	(0.59)	(0.16)	(0.15)	(0.12)	(0.70)	0.03	(0.53)	0.03	0.11	0.73	(0.40)	0.23	0.03	(0.03)	(0.25)	(0.02)	(0.06)
Litecoin - Bit. Cash	(0.23)	(0.06)	(0.85)	(0.13)	(0.17)	0.13	0.35	0.37	0.54	0.46	(0.04)	(0.07)	(0.25)	(0.18)	(0.40)	0.14	(0.47)
Litecoin - Monero	(0.38)	(0.04)	(0.26)	(0.15)	(0.58)	0.28	(0.17)	0.25	0.15	(0.17)	0.09	0.30	(0.54)	0.52	0.11	0.48	0.33
Ripple - Stellar	0.03	0.40	(0.30)	0.19	(0.68)	0.14	(0.52)	(0.30)	(0.15)	0.25	(0.17)	(0.17)	(0.41)	0.20	0.02	(0.02)	0.27
Ripple - Cardano	0.07	0.79	(0.39)	0.66	(0.01)	(0.03)	(0.54)	0.75	0.03	0.46	(0.62)	0.43	(0.07)	(0.04)	0.07	(0.10)	0.06
Ripple - Bit. Cash	0.39	0.95	0.24	0.07	0.90	0.53	0.46	0.45	0.45	0.31	0.45	0.91	0.75	0.72	0.01	0.31	0.25
Ripple - Monero	(0.72)	(0.05)	(0.24)	0.04	0.51	(0.24)	0.27	0.03	(0.34)	(0.33)	0.35	0.60	(0.59)	0.55	0.56	0.59	(0.09)
Stellar - Cardano	(0.31)	0.28	(0.22)	(0.27)	0.25	0.33	(0.05)	0.04	0.16	0.29	(0.05)	0.20	0.71	0.00	0.65	(0.69)	(0.71)
Stellar - Bit. Cash	0.55	0.21	(0.13)	0.06	0.43	(0.03)	0.40	0.35	0.26	(0.36)	0.33	0.65	0.30	(0.14)	0.06	0.45	(0.37)
Stellar - Monero	0.13	0.07	(0.51)	(0.07)	0.34	(0.41)	0.76	0.77	(0.06)	(0.43)	0.58	0.69	0.28	(0.02)	0.16	0.30	(0.12)

Figure 4: **Change in Component Share (CS) between cryptocurrencies in the period after a hacking event**
The above figure represents the change in the component share of price discovery in the period before each of the hacking events that are denoted in Table 3. We estimate CS using the error correction parameters and variance-covariance of the error terms from the Vector Error Correction Model (VECM): $\Delta_{p1,t} = \alpha_1(p_{1,t-1} - p_{2,t-1}) + \sum_{i=1}^{200} \gamma_i \Delta p_{1,t-i} + \sum_{j=1}^{200} \delta_j \Delta p_{2,t-j} + \varepsilon_{1,t}$ and $\Delta_{p2,t} = \alpha_2(p_{1,t-1} - p_{2,t-1}) + \sum_{k=1}^{200} \varphi_k \Delta p_{1,t-k} + \sum_{m=1}^{200} \phi_m \Delta p_{2,t-m} + \varepsilon_{2,t}$ where $\Delta p_{i,t}$ is the change in the log price $(p_{i,t})$ of the asset traded in market i at time t. The next stage is to obtain the component shares from the normalised orthogonal to the vector of error correction coefficients, therefore: $CS_1 = \gamma_1 = \frac{\alpha_2}{\alpha_2 - \alpha_1}$ and $CS_2 = \gamma_2 = \frac{\alpha_1}{\alpha_1 - \alpha_2}$. The heatmap is colour-coded so that green cells denoted large increases in the share of price discovery from cryptocurrency A to B, while red cells denoted large increases in the share of price discovery from cryptocurrency B to A.

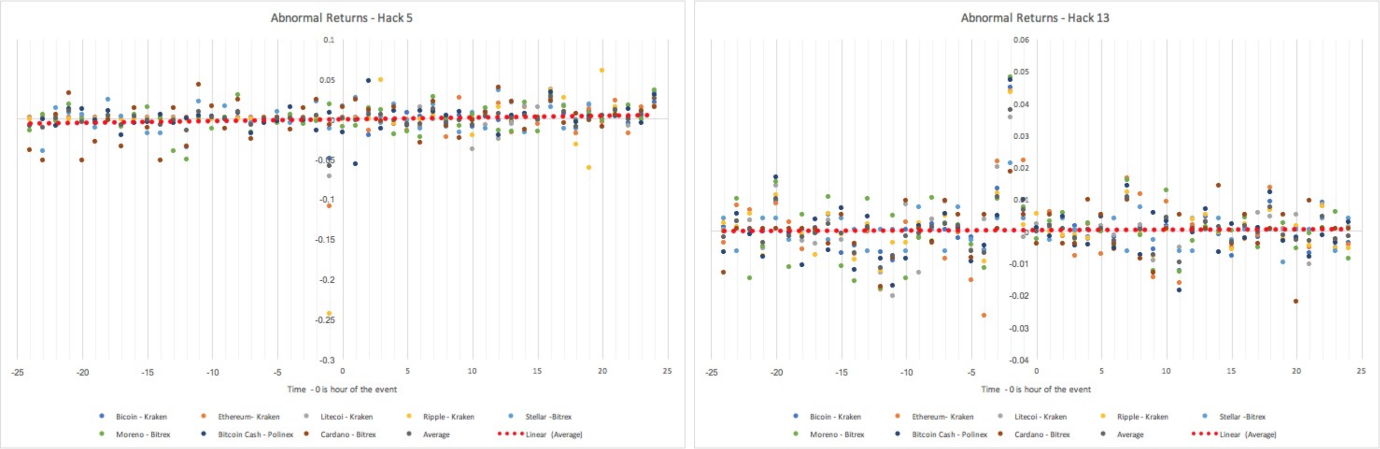


Figure 5: **Abnormal cryptocurrency returns in the period after each denoted hacking event**
The above figure represents the abnormal returns of our selected cryptocurrencies during the 24 hours periods both before and after major cryptocurrency hacking events that are denoted in Table 3. For brevity we have only included selected abnormal return results. All other results related to the abnormal returns of cryptocurrencies due to hacking events are available from the authors on request.