UNIVERSITY OF SOUTHAMPTON
FACULTY OF SOCIAL SCIENCES
SOUTHAMPTON BUSINESS SCHOOL

Bitcoin Markets and Cyberattacks

By

Musab Al Malahmeh

A thesis submitted for the degree of

Doctor of Philosophy in Finance

June 2021

UNIVERSITY OF SOUTHAMPTON
FACULTY OF SOCIAL SCIENCES
SOUTHAMPTON BUSINESS SCHOOL

Bitcoin Markets and Cyberattacks

By

Musab Al Malahmeh

Main Supervisor: Professor Tapas Mishra
Supervisor: Dr . D Luo

A thesis submitted for the degree of
Doctor of Philosophy in Finance

June 2021

UNIVERSITY OF SOUTHAMPTON

Abstract

FACULTY OF SOCIAL SCIENCES

SOUTHAMPTON BUSINESS SCHOOL

Doctor of Philosophy in Finance

by Musab Al Malahmeh

This thesis investigates the impact of the security breach on the Bitcoin cross-market prices by shedding new light on the influences of cyberattacks from several angles. Therefore, the thesis was divided into three separate but interconnected studies that explore the effect of cybercrime by using several empirical strategies to understand the complex behaviour of Bitcoin cross-market prices after breach events. Chapter two investigates the impact of security breaches on the relationship between Bitcoin cross-market prices. Continuous security breach often triggers a collapse of investors' sentiment resulting in an expected diversification of investment across platforms or exchange currencies. Moreover, being able to identify a pattern in such security breaches helps in the formation of an adaptive prediction of Bitcoin prices. Thus, the researcher studied the relationships among 14 Bitcoin market prices. Further, he employed network theory to study the impact of breach events on the Bitcoin price network. The findings of the undirected network reveal that cybercrime influenced the topological structure of the Bitcoin prices network. Also, the impact pattern depended on the size of economic loss generated after breach events. Moreover, security breaches can change the crucial players in the Bitcoin prices network.

Chapter three examines the causal relationships between cross-market Bitcoin prices after experiencing a security breach. The researcher employed rolling estimations of a time-varying network to reveal the changes that occurred in the topological structure of the Bitcoin cross-market prices network pre and post each cybercrime. He also classified the changes to most senders and receivers of information among Bitcoin pairs pre and post each breach event. The study sheds light on the temporal dimension of the network and the magnitude of the information spillover between Bitcoin cross-market prices through time. The contagion effects of cyber-attacks are mainly highlighted by showing evidence of the change in the flow of information between the Bitcoin prices network post each security breach. Moreover, the most interesting pattern was that the Bitcoin pair that represents the location of the Bitcoin platform became more active in sending information or Effective Transfer Entropy (ETE) in the network.

Chapter Four provides comprehensive evidence by classifying security breaches that targeted the Bitcoin platform into several categories. Also, the influences of each category are traced to show the impact of the three main classifications on the Bitcoin markets network. The Effective Transfer Entropy (ETE) models was used to evaluate the interdependency among Bitcoin pairs and to shed light on the network adjustment during episodes of turbulence. Further, network analysis is adopted to reveal the change in the causality relationships. The findings suggest that each category of cyberattack has a unique impact on the Bitcoin cross-market prices. More precisely, the cyberattack that influences the availability of cryptocurrencies' platforms and generates money loss appears to increase the information transition among Bitcoin markets which may increase the contagion risk in the Bitcoin prices network. Meanwhile, the cybercrime under the confidentiality category reduces the causality linkages in the network.

Contents

List of Figures

List of Tables

Declaration of Authorship

I, Musab Al Malahmeh, declare that this thesis titled, 'Bitcoin Markets and Cyberattacks' and the work presented in it are my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University.

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.

3. Where I have consulted the published work of others, this is always clearly attributed.

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.

5. I have acknowledged all main sources of help.

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

7. None of this work has been published before submission

Signed:

Date: 7- June - 2021

Acknowledgements

I am grateful to those who guided and encouraged me all along my PhD journey that led to this thesis. I express my gratitude to every one of them and say from my deepest heart “Thank you". I would like to begin by expressing my sincere appreciation and greatest thanks to my supervisor Professor Tapas Mishra. My appreciation to him is beyond any language can ever express as he was always present and offered the greatest support. I will never forget your compassionate heart especially during my illness, and I have been honoured to work with you. I extend my respect and gratitude to my second supervisor Dr. D Luo and my previous supervisors Dr. Jeremy Cheah and Dr. Raju Chinthalapati for their great help which enormously contributed to the success of this work.

To those who planted the seed of loving education since childhood: I owe to my father and mother the deepest debt. I will always be indebted to you. Your unconditional love and prayers were my guardian angel throughout the difficult times. I owe a deep debt of gratitude to my family who supported me. To my wife Tamadour and my son Mohamad, I can never forget the overwhelming love and support I had from you throughout my doctoral study. And I also express my great gratitude for your endured hardship throughout my absence. I can never forget the support and love I had from my sister Hadeel, and my brothers Mohamad, Ahmad, and Ismael. My thanks also go to my sponsor, Mutah University, for their financial support during my Master’s and PhD journey.

Chapter 1

Introduction

1.1 Research Context

In the history of money development and to replace the barter system, humans developed the idea to switch to an entity that can serve as a medium of exchange Schweikart (1991). The entity could be anything available regardless of the value of that object. Over time, the goldsmith's note became more convenient as a store of value, where ancestors deposited their precious items with goldsmiths and used that note in their trading activities (Wray, 2012). However, during the 17th century and by the government order, central banks replaced the goldsmith's note with fiat money (Wray, 2012). This, in turn, meant that money was managed by governmental authority and replaced the old form of money from individual assets to paper notes to play a dominant role as we witness nowadays. However, with the new Internet technologies and the evolution of e-commerce, the need for a new cash payment system has emerged, with different online payment systems being introduced, such as PayPal (Chuen, 2015). Meanwhile, the concept of digital currency has also begun to emerge and evolve (Khairuddin, 2019) where digital currency developed into several forms starting from electronic cash as credit or debit card, to virtual currency that opened the door to borderless technologies that helped to send and receive money and exchanges quickly in the case of the conventional currencies (Bureau, 2016). Virtual currency can be categorised into two classes. The concept of virtual currency first emerged in 1996; the first non-cryptocurrency was called E-gold. Later another digital currency was introduced in 2006 called Liberty Reserve but since this digital currency was used for money laundering the US government decided to stop its use (Resnick et al., 2006).

The second form of virtual currency was in the form of cryptocurrency. Bitcoin was the first cryptocurrency founded by an anonymous entity , but can be called Satoshi Nakamoto in 2009 (Nakamoto, 2008b). Notably, the emergence of Bitcoin coincided with the financial crisis in 2008 where people's trust in the traditional financial systems was at its lowest level (Marella et al., 2020). On 3 January, 2009, the first Bitcoin was founded, and the first notable deal that used Bitcoin occurred on 22 May 2010, where 10,000 Bitcoins were paid for two slices of pizza.Over time, and a decade since its inception, Bitcoin has become a central component in the present global economy. Indeed, market capitalisation for Bitcoin exceeded one trillion dollars in 2021 since the early uses of Bitcoin in 2009 (coinmarketcap, 2021). Further, during 2021, Bitcoin has experienced a new price level exceeded $60,000 US dollar[1]. Therefore, the rapid demand for cryptocurrencies – particularly

[1] https://coinmarketcap.com/

Bitcoin – raised the necessity for more studies to understand the nature of the growing t digital cash system during the last decade.

Cryptocurrencies such as Bitcoin suffer from serious drawbacks. Because authorities or any legal entities cannot intervene in Bitcoin, this may make Bitcoin vulnerable to price manipulation, which may generate more risk (Gandal et al., 2018). Also, The cryptocurrencies markets are unregulated and, because of the lawless nature and an uncontrollable environment, they can be vulnerable to abuse by hackers and thieves (Feder et al., 2018b).In general, users, platforms or wallets, merchants, and Bitcoin miners are the main four main parties of interest in the Bitcoin market (Shcherbak, 2014). However, each Bitcoin stakeholder is exposed to certain kinds of risk that arise from cyberattacks. For instance, Bitcoin *miners* are exposed to several types of security breaches, such as Dropping Transactions (Sigurdsson et al., 2018) and 51% Attacks (Shanaev et al., 2019). On the other hand, *merchants* that accept Bitcoin as a medium of exchange also suffer from double-spending attacks and malleability attacks (Hassan et al., 2020, Pinzón and Rocha, 2016). Meanwhile, Bitcoin *users* deal with several cybercrime techniques; for example, DNS hijacking, account hijacking, SIM swapping, and site defacing (Sigurdsson et al., 2018). In the same vein, the Bitcoin *market and wallets* facing the same risk of security breach events. The security system vulnerability of the Bitcoin platform is exploited by malicious entities when they plan to steal money from the platform (Conti et al., 2018). And Bitcoin market price manipulation (Gandal et al., 2018).

In 2019 there was approximately more than US $4 billion of theft in the cryptocurrencies market, compared to $1.7 and $1.2 billion of crypto crimes in 2018 and 2017, respectively (Forbes, 2019). There are several reasons behind cybercrimes. Rauchs and Hileman (2017) reported that 75% of cryptocurrencies' platforms consider Two-factor authentication (2FA) as an option compared with 25% of platforms that provide this authentication process as obligatory. In the same vein, Anise and Lady (2017) stated that only 28% of investors used 2FA compared with 56% who had never heard about this method. Cryptocurrencies' platforms not only suffer from the loss of cryptocurrencies because of security breaches but incur costs after dealing with security breaches as the platform needs labour and time to repair the damaged system. Moreover, the reputation of the platform may be negatively impacted after the announcement of the cybercrime incident. Therefore, cryptocurrencies' platforms may lose the opportunity to expand their client base in the future (Shanaev et al., 2019).

1.2 Research Aims

The overall aim of this thesis was to shed light on the impact of cyberattacks on the Bitcoin cross-market prices network from different angles. The thesis highlights a promising investment such as Bitcoin by adopting reliable analytical methods to empower stakeholders, policymakers, and scholars to reduce the uncertainty after breach events, which can assist them in making a coherent financial decision.

The aims of each chapter are as follows:

Chapter Two aims to trace the influences of cyberattacks that target the Bitcoin platform and incur money loss by employing the undirected network among Bitcoin prices to examine the changes that occur in the topological structure of the network pre and post each cybercrime. Also, by relying on centrality measures, one of the aims is to rank the top key players between the Bitcoin prices network and to identify whether any patterns emerge after cyberattacks.

Chapter Three aims to detect the information transmission between Bitcoin cross-market prices after Bitcoin platforms experienced a security breach that led to Bitcoin going missing. In addition, the chapter aims to recognise whether cyberattacks can change the main receivers and prime givers of information in the network. The dynamic network analysis was considered to measure the temporal dimension of the Bitcoin network and the magnitude of the information spillover between Bitcoin cross-market prices in time. Which can help to highlight the contagion risk of cyberattacks among Bitcoin prices.

Chapter Four aim to examine the influence of the different type of cyber-attacks that targeted the Bitcoin platform and conduct a comparison for the changes that may occur in the spread of information among Bitcoin cross-market prices. Moreover, one of the aims is to identify the market reaction by trace and compare the spillover effect (contagion) after the network experienced different forms of security breaches.

1.3 Research Objectives

The research objectives of the thesis were divided into the following main objectives for each chapter as follows:

The research objectives in Chapter Two are:

- To empirically quantify the relationship among Bitcoin cross-market prices.
- To examine the topological structure of the undirected network and compare the results pre and post security breaches.
- To identify the most influential Bitcoin prices in the network through centrality measures.
- To identify any response pattern that occurred after security breaches.

The research objectives in Chapter Three are:

- To design directed networks of Bitcoin pairs and the linkages in the network that depend on the effective Transfer Entropy (ETE).
- To empirically estimate the influence of breach events on the topological structure of the network.
- To detect any changes in the top transmitter and net receiver after the platform experienced cyberattacks.
- To trace the adjustment in the flow of information among Bitcoin pairs through dynamic network analysis.

The research objectives in Chapter Four are:

- To design a network that represents the causality relationship between Bitcoin cross-market prices.
- To classify security breaches that targeted Bitcoin platform depending on the threat posed.
- To detect the contagion risk of cyberattacks and create a comparison between the influences of the three main categories after the network experienced each type of attack.
- To capture any pattern that occurred after the network suffers from each category of security breach.

1.4 General Literature Review and Contributions

Recent attention has focused on Bitcoin to identify the characteristics of the new financial cash system, such as its proclivity to speculative bubbles (Cheah and Fry, 2015) and Bitcoin price's high volatility (Katsiampa, 2017). In the same vein, Bitcoin can also be described as a speculative investment (Baur et al., 2018; Baek and Elbeck, 2015). Other studies have focused on the ability of Bitcoin in hedging (Bouri et al., 2017a, 2017b). However, the main aim of this thesis is to evaluate the impact of cyberattacks on the Bitcoin cross-market prices network. Thus, the current work focuses primarily on literature that examined the influence of security breaches on virtual currency. Moreover, a number of different cryptocurrencies have unique and distinct working mechanisms; thus, focusing on the Bitcoin allows us to trace the impact of breach events more thoroughly and efficiently.

Because of the lawless nature and an uncontrollable environment, cryptocurrencies can be vulnerable to abuse by hackers and thieves (Feder et al., 2018b). Moore and Christin (2013) adopted a logistic regression to examine 40 Bitcoin exchanges and found that security breach is more likely to target well-known platforms; they reported that 45% of the platforms in the study sample had closed. Rosati et al. (2017) reported that illegal activities, such as cyberattacks, could not be predicted, either when they happen or how many times they could occur. Corbet et al. (2019) traced 17 hacking events that targeted the eight most liquid cryptocurrencies within less than a year and pointed out that volatility increases after each security breach. The Attorney General Office of New York (2018) provided a detailed report to inspect fraud and manipulation. They found that these types of events could occur only at the cryptocurrency exchange level. Furthermore, they pointed to insufficient precautionary procedures to evade suspicious behaviour in most trading platforms. Gandal et al. (2018) noted that the price of the Bitcoin in Mt.Gox was subject to manipulation motivated by the unexplained price jump within only two months. More recently, Corbet et al. (2019a) traced 17 hacking events that targeted the eight most liquid cryptocurrencies within less than a year and, after employing a DCC-GARCH model, they showed that the correlations between cryptocurrencies increase after cyberattack.

- Chapter Two contributes to the current literature that examines the influences of a security breach on Bitcoin exchange rates by providing an opportunity to advance our knowledge of the impact of the security breach on the topological structure of the Bitcoin prices network, about which little is known. It also contributes to the literature by capturing the response pattern of the Bitcoin cross-market prices network after experiencing cyberattacks, which

can provide some evidence to investors and stakeholders to take more precise financial decisions.

The hacking of cryptocurrency hot wallets and platforms has recently become more widespread and more severe (Corbet et al., 2019). There have been several cyberattacks that have managed to rob different types of cryptocurrencies. For instance, in 2018 one of the largest heists took place in Coincheck when the platform lost approximately $500[2] million. Caporale et al. (2020b) conducted a non-linear Markov switch to evaluate the cyberattack impact on the returns of four cryptocurrencies. They argued the probability of cryptocurrencies being influenced negatively by cyberattacks and remained within low volatility throughout August 2015 – February 2019. Shanaev et al. (2019) analysed the data from 13 cryptocurrencies to examine the influence of 14 individual 51% attacks. They concluded that there were 'pump and dump' schemes after each attack and that cyberattacks have a negative influence on the return of cryptocurrencies. Azqueta-Gavaldón (2020) investigated the impact of media coverage of security breach that targeted the cryptocurrencies market. After using the Granger causality test, the author described a causal relationship between narratives related to cybercrimes and cryptocurrencies prices.

- The findings in Chapter Three make an essential contribution to the field by showing that cyberattacks can change the Bitcoin prices network structure. Moreover, after using high frequency data (6-hours frequency) the chapter contributed by showing that the Bitcoin pair that represents the location of the Bitcoin platform became more active in sending information. Referring to the contagion risk of cyberattacks from one market to all other Bitcoin markets. Finally, Chapter Three aims to contribute to the growing literature by exploring the dynamic dimension of how the network of Bitcoin price evolves after breach events.

Several studies investigated the impact of cyberattack that influences the availability of the Bitcoin platform (Johnson et al., 2014, Feder et al., 2017, Abhishta et al., 2019). Meanwhile, cyberattacks can be destructive and generate money loss. Thus, a number of researchers considered this type of cyberattack that targeted the Bitcoin platform (Pinzón and Rocha, 2016, Sigurdsson et al., 2018, Hassan et al., 2020). However, only limited attention has been paid to examining the impact of breach events that cause unauthorised access to the Bitcoin cross-market prices.

[2] See www.hackmageddon.com a database collect all cyberattacks that occurred around the world.

Several attempts have been made to investigate the spillovers among cryptocurrencies. Koutmos (2018) analysed the data from 18 major cryptocurrencies and concluded that cryptocurrencies had become more interconnected so the risk of contagion had become significantly possible. Caporale et al. (2021) examined the daily data for Bitcoin, Ethereum and Litecoin to highlight the changes that may occur in the volatility spillover after the market experienced a security breach. In their comprehensive examination, they were able to show that cyberattacks increase the linkages among three major cryptocurrencies.

- Chapter Four makes a contribution to current related works on the impact of breach events by demonstrating a comparison for different type of cyberattacks to trace the changes that may occur in the information transmission among Bitcoin cross-market prices. Also, it provides evidence that each type of cyberattack has a unique impact on the Bitcoin prices network.

1.5 Thesis Structure

The structure of this thesis comprised five themed chapters, including this introductory chapter. The remaining sections are planned as the following:

Chapter Two presents the impact of the security breaches on the relationship between cross-market Bitcoin prices. In this chapter, network theory is employed to explore the changes that occurred pre- and post-cybercrimes. It also discusses who the key player among the Bitcoin pair was by relying on the network centrality measurements.

Chapter Three focuses on the changes that occurred in the causality relationship as a response to the cyberattack events and shows the impact of breach event on the top senders and receivers in the directed network. The dynamic analysis is included in this chapter to estimate the depth of the impact of cyberattacks.

Chapter Four sheds light on the different types of cyberattacks and sets up a comparison to capture the network adjustment on the Bitcoin pair interdependency. Several breach events are included in this chapter to confirm that the same pattern happened after each security breach from the same category.

Chapter Five comprises the conclusions drawn by this thesis and presents the main implications of this work.

Chapter 2

Who is the Key Player in the Cross-market Bitcoin Prices Network after a security breach?

2.1 Introduction

In 2008, a novel paper introduced a new cash system, without intervention from any authority or legal entity, known as Bitcoin (BTC) (Nakamoto, 2008a). This decentralised system provides more privacy to individuals, especially for those who unwilling to sharing their banking information, as they only need a digital signature to use Bitcoin. However, Bitcoin and other cryptocurrencies have been subjected to several cyberattacks. According to Gattiker (2004), a security breach can be defined as any event that generates unauthorised access, which bypasses the security mechanisms, to any kind of device, network, service, and database. In 2018 there was approximately $1.7 billion of theft in the cryptocurrencies market (CNBC, accessed 25 April 2019) and many Bitcoin exchange platforms dealt with several security breaches, such as the well-known Bitcoin exchange Mt.Gox, which was subjected to a number of breaches in 2012 and 2014.

The aim of this chapter was to trace the influence of hacking events that targeted Bitcoin exchange platforms and generated money loss by constructing a network dependant on the relationship among Bitcoin exchanged prices in various currencies and then examine the changes that occurred in the topological structure of the network pre- and post-cybercrime. Depending on centrality measures, the study also aimed to classify the most crucial Bitcoin pairs pre and post each event. Finally, it aimed to recognise the network response pattern as a reaction to breach events.

The present study contributes to the current literature that examines the influences of a security breach on Bitcoin exchange rates in several ways. *First*, it sheds light on the link between the size of economic losses and the impact of cyberattacks. *Second*, it contributes by introducing evidence that cyberattacks can influence the most influential and crucial player of the Bitcoin cross-market prices in the network and change the key player after an attack. *Third*, the current work contributes to the literature by examining six cyberattacks events on 14 Bitcoin markets by employing network theory.

This study addresses the central question of how cybersecurity on Bitcoin exchange platforms can influence the structure of the cross-market Bitcoin price network. Another critical question is whether there was a shifting pattern in the network over various points of attack. Drawing upon centrality measures, as specified in section three, this raises an additional question about how a security breach can impact the network and change the ranking of the most crucial Bitcoin/currency pairs pre and post each event.

The present study fills an empirical gap by providing concrete evidence that the network structure of Bitcoin market exchange prices has changed as a response to cyberattacks. Figure A 1 and Table 1- 1 in the appendix, illustrates the area that this study targets in a quest to fill the gap between three major aspects wherein the intersection between two major aspects (two circles) represents areas of study that have been investigated and there was reported evidence of the relationship between them. However, in the area where the three major aspects intersect, no previous study has investigated the impact of cyberattacks on the relationship among the Bitcoin cross-market prices network. Several studies (such as Yip et al., 2012, Leukfeldt, 2015, Phillips et al., 2015), have employed a network analysis approach to examine and assess the risks of cybercrime. Meanwhile, there has been limited use of the *network analysis* approach and *graph theory* in the Bitcoin market (Baumann et al., 2014, Lischke and Fabian, 2016). In the same vein, several studies have investigated the impact of security breaches on the Bitcoin ecosystem (Vasek and Moore, 2015, Feder et al., 2018a, 2018b). However, to the best of the author's knowledge, this is the first paper that encompasses three significant aspects and traces the impact of cybersecurity attacks and breach events on the topological structure of the cross-market Bitcoin price network.

The rest of the paper is structured as follows. Section 2 sets out the theoretical scope of the study by looking at the academic literature on Bitcoin and network theory. Section 3 describes the data and the methodology, by using network analysis and centrality measures. Section 4 presents the empirical results. Section 5 concludes.

2.2 Related Work

In recent years, there has been increasing attention to cryptocurrencies markets. The past 10 years have seen increasingly rapid advances in the field of cryptocurrencies; Bitcoin, the first cryptocurrency, was introduced in 2009 (Nakamoto, 2008a). Compared to other cryptocurrencies, Bitcoin has been identified as the major cryptocurrency with a significant market capitalisation of almost $89 billion (CoinMarketCap, 2019). Therefore, more recent attention has been given to identifying the characteristics of the new financial cash system, such as its proclivity to speculative bubbles (Cheah and Fry, 2015) and the Bitcoin price's high volatility (Katsiampa, 2017). In the same vein, Bitcoin can also be described as a speculative investment (Baur et al., 2018, Baek and Elbeck, 2015). Other studies have focused on the Bitcoin exchange rate and draw our attention to the determinant of the exchange rate and the motivation behind the price fluctuations (Li and Wang, 2017). Others have investigated the ability to use Bitcoin in hedging (Bouri et al., 2017a, Bouri et al., 2017b). Cheah et al. (2018) drew attention to crucial evidence that there is a fractional cointegration in the cross-market Bitcoin prices and point out the inefficiency of the Bitcoin market and the influence of uncertainty on the market. This point of view is supported by Gillaizeau et al. (2019a) who questioned the cross-market Bitcoin prices from another angle and pointed out that uncertainty has a high impact on the spillover into volatility. They further added that the Bitcoin exchange rate to Euro currency can be categorised as high connectivity with other cross-market prices. As the number of studies examining Bitcoin increases, it may help to expand our knowledge and understanding to obtain some insight into the characteristics of cryptocurrencies markets. Thus, this paper examines cross-market Bitcoin prices allied with a nascent but growing literature that highlight the impact of cyberattacks on Bitcoin prices.

Several attempts have reported the impact of security breach that targeted cryptocurrencies market as showed in table 1-1 in the appendix, where recent evidence suggests that cryptocurrencies market are not isolated completely. A number of authors examined the spillover among cryptocurrencies and commodities. Huynh et al. (2020) employed Transfer Entropy to examine the spillover between gold and 14 different types of cryptocurrencies. They argued that a portfolio consists of cryptocurrencies and gold can be considered as a good combination, where gold plays a significant role as a hedging tool in that portfolio. Similarly, Gkillas et al. (2020) identified the spillover effect after using high-frequency data between crude oil, gold, and Bitcoin. They described the robust association between gold and Bitcoin; likewise the relation between Bitcoin and crude oil. This point of view was supported by (Ji et al., 2019b), who addressed the weak linkage between energy commodities and the top five cryptocurrencies included in the study. Drawing on Granger

causality test and transfer entropy (Jang et al., 2019) identifies causal association between asset markets and Bitcoin market. And there was dynamic interactions from Bitcoin market with major asset markets. The volatility spillover between Bitcoin market and other asset markets such as bonds, commodities, stocks, currencies and equities was examined by Bouri et al. (2018). They argued that Bitcoin takes more volatility compared with the amount of volatility that transfers it. Furthermore, linear and non-linear contagion was studied between traditional financial markets and Bitcoin market, Matkovskyy and Jalan (2019) claimed that after the first use of Bitcoin futures there was highly contagion effect from traditional financial markets to Bitcoin market. However, Zeng et al. (2020) drew attention to the connectedness between Bitcoin and financial markets. They described the connectedness between the study variables as weak. In summary, Bitcoin plays a central role in hedging effectiveness and diversification risk for many assets, however in term of safe haven Bitcoin can only serve for a few financial markets. Furthermore, the effect of cyber-attacks on the linkages between Bitcoin markets networks and other asset markets is nearly underexplored.

2.2.1 Security breaches in cryptocurrencies markets

The digital currencies markets are unregulated and, because of the lawless nature and an uncontrollable environment, they can be vulnerable to abuse by hackers and thieves (Feder et al., 2018b). Moore and Christin (2013) recorded these by adopting a logistic regression to examine 40 Bitcoin exchanges and argued that security breach is more likely to target well-known platforms; they further pointed out that 45% of the platforms included in the study had closed, indicating that there is a higher chance that the less popular platforms shut down their services. However, the unexpected exit of one of the largest Bitcoin exchange, Mt.Gox in 2014, shows that even a well-known platform might be subjected to cyberattacks which force the platform to close. Rosati et al. (2017) reported that illegal activities, such as cyberattacks, could not be predicted, either when they happen or how many times they could occur. Numerous studies attempted to explain the influence of security breaches on the virtual currency through a variety of criminal activities, including stealing "brain" wallets (Vasek et al., 2016), money laundering (Möser et al., 2013), Pump and Dump Schemes (Feder et al., 2018b) and suspicious activity, such as Ponzi schemes (Vasek and Moore, 2015). The comprehensive study by Bacao et al. (2018) drew attention to the dominant role of Bitcoin and there was a strong correlation among the five cryptocurrencies included in their study.

Drawing on a wider range of studies, Conti et al. (2018) undertook a broad survey of the challenges faced by Bitcoin security and argued that Bitcoin has been subjected to different forms of security breaches, such as double spending, mining pool attacks and Bitcoin network attacks, all of which can

target the Bitcoin platform, wallet, and mining activities. As noted in the report released by the Attorney General's Office of New York (2018), fraud and manipulation events could occur only at the cryptocurrency exchange level. The results showed that there are insufficient precautionary procedures and a lack of cybersecurity protocols to evade suspicious behaviour in most trading platforms. The report also, unsurprisingly, pointed out that several cryptocurrency platforms did not provide security protection.

The influence of cyberattacks can depend on the nature of the breach, whereby cybercriminals have adopted several methods and different ways of attacking, each of which has its own effect on the markets (Campbell et al., 2003). Distributed denial-of-service (DDoS) is an example of such cyber-attacks that influence the availability of exchange services. Vasek et al. (2014) investigated 142 distributed denial-of-service attacks that targeted cryptocurrency markets, especially on 40 Bitcoin services, and found that this kind of attack was more likely to target platrform services, e-wallets and large mining pools because cybercriminals receive significant gains from these areas compared if they targeted individuals. In the same vein, after examining 37 DDoS attacks that targeted well-known Bitcoin exchange Mt.Gox, Feder et al. (2018a) argued that the trading activities were affected on the day the denial-of-service occurred. Indeed, mining malware or mining botnets are other methods for cybercriminals, whereby they try to hijack computer CPU power from a significant number of users around the world and use it in Bitcoin mining (Huang et al., 2014). Similarly, cybercriminals can manipulate the Bitcoin price. By relying on the data leaked from the largest Bitcoin exchange, Mt.Gox, in early 2014, Feder et al. (2018b) pointed out that the price of the Bitcoin in Mt.Gox was subject to manipulation. Motivated by the unexplained price jump within only two months, where the price rose by more than $800 in late 2013, the study presented evidence in the form of two suspicious activities that influenced the Bitcoin price. This argument was supported by Griffin and Shams (2018), who investigated the suspicious relationship between a digital currency called "Tether" and other cryptocurrencies, including Bitcoin, pointing out that when the Bitcoin price declines, the demand for Tether rises, which can later drive the Bitcoin price to increase. They concluded that Bitcoin and other cryptocurrencies prices had been manipulated, by using Tether as a tool to offer price support. Collectively, these studies can provide support to this study's argument, as they provide evidence of the critical role of breach events and their influence on the Bitcoin market.

2.2.2 Market efficiency of Bitcoin and investors' sentiment

This study is a quest to establish a network of cross-market Bitcoin prices and to evaluate how the structure of the network can change after experiencing cybercrime events over time, particularly focusing on the large-scale breaches which have occurred in the last five years. Therefore, after the security breach hit the Bitcoin market, this incident may deliver new information to the market. Thus, it is crucial to shed light on Bitcoin market efficiency to recognise to which degree Bitcoin price reacts to the news. An early study conducted by Urquhart (2016) examined the Bitcoin price in USD from 2010 until mid-2016, employing a battery of tests. The results revealed that the market was significantly inefficient over the whole period; however, the findings also showed that the market could be efficient if the sample was split and that can be only in the latter period. This argument that the Bitcoin market is inefficient was supported by (Al-Yahyaee et al., 2018, Zargar and Kumar, 2019). Conversely, following a review of Urquhart (2016), Nadarajah and Chu (2017) used eight different tests and found that the Bitcoin market could be efficient but in a weak form. Similarly, this point of view was supported by (Tiwari et al., 2018) and Sensoy (2019), who provided in-depth research by using high-frequency data to analyse Bitcoin prices in US dollars and the Euro. They found that, depending on the intraday data, the level of market efficiency increased.

The recent evidence suggests that the level of Bitcoin market efficiency has increased, as Vidal-Tomás and Ibañez (2018) showed that several pieces of research focused only on the weak form of efficiency and that there is an absence of studies that examine the other levels of market efficiency, as introduced by (Fama, 1970). Therefore, Vidal-Tomás and Ibañez presented semi-strong efficiency after adopting an event study to examine two leading Bitcoin platforms – the Mt.Gox exchange and the Bitstamp exchange. The study observed public information in the form of monetary policy news and events regarding the Bitcoin market. So, after they traced the market reaction to negative and positive news, they concluded that the Bitcoin market tends to be more efficient, particularly with its events, where the Bitcoin price is influenced by it is own good and bad announcements. On the other hand, on the subject of monetary policy news, the Bitcoin prices did not show any response, indicating that the market was not efficient in that case. Overall, drawing on the studies examining the Bitcoin market efficiency, there seems to be some evidence to indicate that the level of efficiency increases over time and that the Bitcoin Price can reflect its own incident.

In 2018 and 2019, overall of 98 published works in Finance Research Letters having the keyword Bitcoin. This growing academic attention in this topic follows one of the most important events when the price of the Bitcoin rose from $1,000 to approximately $20,000 during the 2017–2018 in

just a few months. For researchers, the Bitcoin market has received considerable critical attention because the abundance of available data and the unique structure of the new cash system. The robust attendance of individual investors make the Bitcoin market an ideal place to arbitrage opportunities between platforms, the Bitcoin price's high volatility, weak regulation and lack of fundamental value. Thus, this make Bitcoin much popular among investors and scholars.

One of the characteristics of the new financial cash system such as Bitcoin, its proclivity to speculative bubbles (Cheah and Fry, 2015). Where the sentiment can become more influence on the period around the Bitcoin price bubble (Guégan and Renault, 2021). Baig et al. (2019) examined the relationship among investors sentiment and the price level of Bitcoin and suggest that there was a strong positive relation. Furthermore, Eom et al. (2019) suggested that Investor sentiment has several effect on Bitcoin, where it has an information effect to predict Bitcoin volatility, and in term of predictability of Bitcoin price fluctuations. Several studies argued that the price of Bitcoin effect by social network sentiment (López-Cabarcos et al., 2019). Also, investors' sentiment disagreement generate significant high volatility in Bitcoin prices (Ahn and Kim, 2020). On the other hand, Happiness sentiment cab be considered as a robust predictor for Bitcoin returns, additionally, Bitcoin returns seem to be less driven to the sentiment related to macroeconomic news compared with sentiment diffused through social media (Naeem et al., 2021).

Azqueta-Gavaldón (2020) investigated the impact of media coverage of cryptocurrency narratives and its causal relationship with prices. Furthermore, he listed four types of narrative, one of which was the media coverage of security breaches in cryptocurrencies markets. The author argued that there was a unidirectional causal between narratives related to cybercrimes and prices. Thus, the announcement of the incident that the Bitcoin market or platform targeted by security breaches this might influence the investors' sentiment. Therefore, continuous security breach often triggers a collapse of investors' sentiment resulting in an expected diversification of investment across platforms or exchange currencies.

2.2.3 Social Network theory

2.2.3.1 Social network analysis

Network theory becomes a key aspect in evaluating the impact of a financial crisis and the market's turbulence (Han, 2019). In recent years, there has been increasing interest in using network analysis in different stock markets, such as the Brazilian stock market (Abreu et al., 2019), the Chinese stock market (Han, 2019), and the Global stock market (Lee et al., 2019). In addition, the use of this

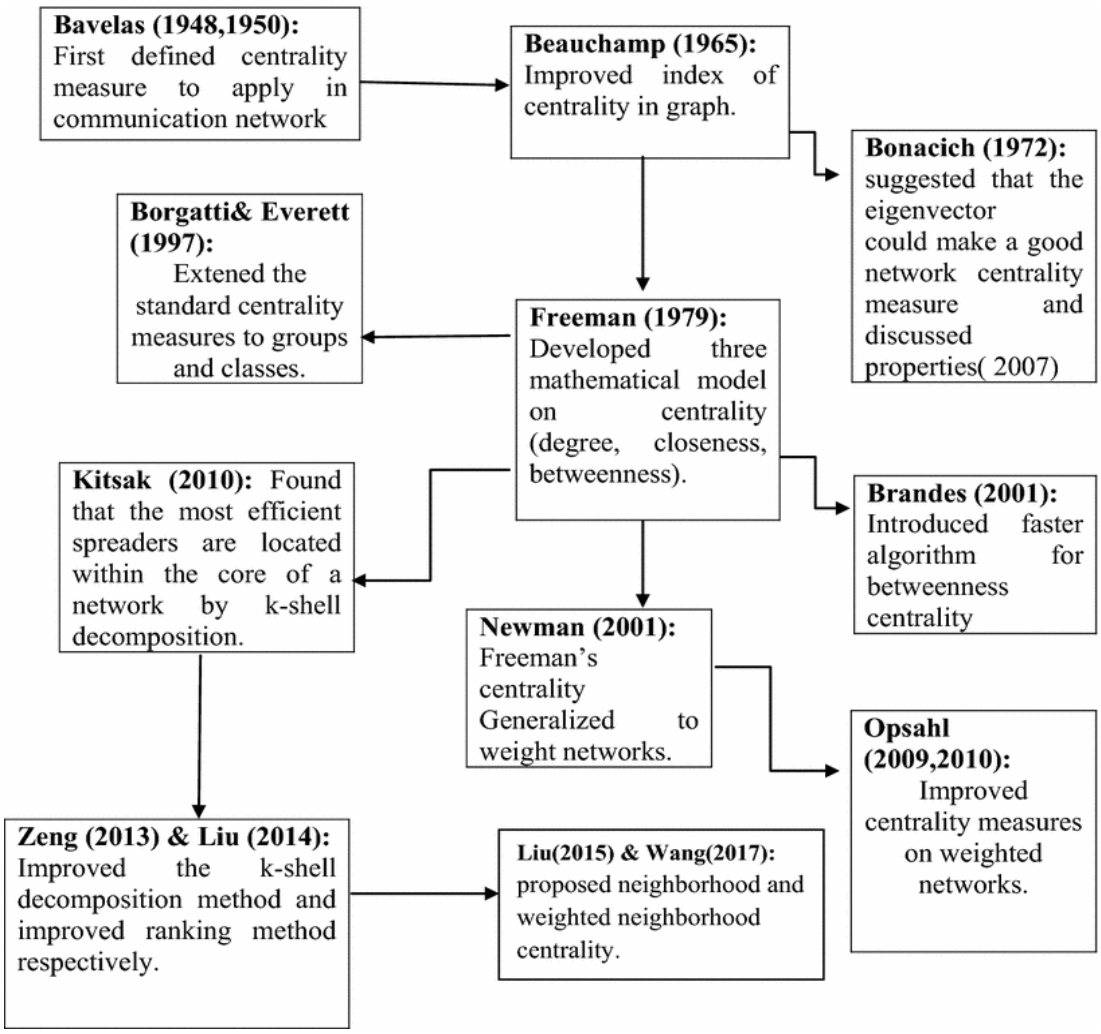
framework has also been adopted in the foreign exchange market (Mai et al., 2018) and the commodity markets (Bekiros et al., 2017, Zhang and Broadstock, 2018).

Most importantly, several studies have use network analysis to try to shed light on the changes which occur in the topology feature of the financial network after dealing with shocks (Kuzubaş et al., 2014, Cheng and Zhao, 2019). Therefore, their findings can support this paper as we aim to build a network depending on the correlation between Bitcoin exchanged prices in various currencies to assess the impact of security breach events. Thus, this framework of complex network analysis can be adopted to describe the changes in the Bitcoin network structure.

The behaviour of the individual exchange price of Bitcoin into another currency is generally examined by time series analysis. However, as the Bitcoin exchange price expands to various currencies, it becomes more challenging to capture the complex inter-relationship between cross-market prices and to show the hidden information in huge time series. Therefore, to evaluate the influence of security breaches on Bitcoin cross-market exchange prices, network theory can provide an analytical tool to view a complex interrelationship and capture the impact of a certain event on the interconnections between the variables, which can help to explain a certain phenomenon (Allen and Babus, 2009).

In complex networks, there are significant numbers of nodes that interact with other nodes and each one has a different level of impact on the network at a certain point of time. Hence, it is important to minimise losing valuable information in the network and to recognise the vital nodes during any events, or to identify the most vulnerable nodes throughout a time of turbulence, which can enable an appropriate response. Thus, centrality measures have a crucial role in social network analysis, by offering a mechanism to rank and classify the nodes in the network (Heiberger, 2014). Recently, many researchers have paid particular attention to using centrality measures to categorise and rank the key players in a complex network (Riquelme et al., 2018, Saito et al., 2016, Bloch et al., 2017). The development of this concept is shown as a flowchart in Figure 1, below.

Figure 1: Development of previous studies introduced by well-known researchers.



(Bavelas, 1950) (Beauchamp, 1965, Bonacich, 1972, Borgatti and Everett, 1997, Freeman, 1978, Brandes, 2001, Kitsak et al., 2010, Newman, 2001, Opsahl et al., 2010, Zeng and Zhang, 2013, Liu et al., 2013, Liu et al., 2016, Wang et al., 2017).

2.2.3.2 Bitcoin and Network analysis

A growing body of literature has examined Bitcoin by using network analysis from a different point of view. Lischke and Fabian (2016) examined the Bitcoin network by presenting graph analysis and used centrality measures to characterise the Bitcoin network. They pointed out that the small-world phenomenon can be present in the network. On the other hand, Ober et al. (2013) adopted network theory to examine the degree of anonymity in Bitcoin. Zięba and Śledziewska (2018) studied the relationship between prices of cryptocurrencies by using the *minimum spanning tree* method, and they reported that Bitcoin plays crucial roles in the cryptocurrency market. They also pointed out

that there was no significant contagion from Bitcoin demand shocks to other virtual currency in the market. Drawing on the same method, (Francés et al., 2018) employed the minimum spanning tree technique, and analysed 16 cryptocurrencies, to show that Ethereum has a vital role and plays as a benchmark currency instead of Bitcoin. In the same vein, Stosic et al. (2018) questioned the behaviour of the cryptocurrency network and compared it to the different financial markets and, by using minimum spanning trees, they argued that the cryptocurrency market has a unique behaviour that can differ from other financial markets.

2.3 Data and Methodology

2.3.1 Data characteristics

The data in this chapter were collected from two websites (www.bitcoinity.org and www.bitcoincharts.com), covering the period between 1/11/2013 – 30/12/2018, for the 14 Bitcoin/currency pairs that are included in this chapter, as shown in Table A 1, in the appendix. The cross-market Bitcoin price was obtained from different exchange platforms, which can fairly represent the market trading activities, and have a decent market share in the targeted currency over the study period. Moreover, the reason behind selecting several platforms for one Bitcoin pair was back to the reason that some platforms closed after a certain time; for instance, Mt.Gox, in the case of BTC/JPY. Therefore, to construct continuous time series data, the author gathered data from other exchange platforms that can fairly represent the whole market. In addition, this study employed a daily weighted price which can reflect the trading activities throughout the day.

As mentioned earlier in the second part of this chapter, a security breach can target a Bitcoin mining platform, wallets, individuals, or exchange platforms. In addition, these cybercriminals can cause enough chaos beginning with stealing Bitcoin from different targets or blocking platform services and even diverting computer power from a significant number of users around the world to achieve control of mining power (Shanaev et al., 2019). Therefore, the damage caused by cyberattacks may pose a systemic threat to the exchange platforms and may also cause reputational penalties that can devalue traded Bitcoin. Thus, this chapter examines the influence of breach events that have targeted Bitcoin exchanges and caused money loss. The security breaches considered in this chapter were collected depending on public sources on the Internet that published reports and news articles over the period 2014–2018, which covers several episodes of security breaches, as presented in **Table 1**. The table consists of a list of six events and contains the dates of cybercrime and the names of the Bitcoin platforms that experienced large-scale security breaches, recording the amount of Bitcoin missed and the cost of each breach at the time it happened.

Table A 3 in the appendix reports the summary statistics for each returns series. The number of observations, 1,887, are for all variables except for BTC/CNY, where in October 2017, the chain government decided to end Bitcoin trading. BTC/SGD have the highest value of standard deviation where BTC/JPY and BTC/GBP show a high range of maximum value. On the other hand, BTC/VND reported the minimum values of returns compared with other cross-Bitcoin exchange rates. BTC/RUB and BTC/VND achieved the highest daily average return. In addition, all positive values of skewness imply that the cross-market exchange returns are skewed to the right, while in cases of

negative value they are skewed to the left. Meanwhile, all cross-market returns series displays leptokurtic behaviours, with higher values for BTC/JPY and BTC/GBP. The Jarque-Bera test results for all returns series indicate a non-normality distribution.

Table 1: Cyberattacks targeted Bitcoin exchange platforms between (2014- 2018).

No	Date	Bitcoin Missed	Amount	Platform	Country of Platform
1	14-Feb-2014	850,000	$473,000,000	Mt.Gox	Japan
2	5-Jan-2015	19,000	$5,200,000	Bitstamp	EU
3	15-Jan-2016	1,300	$6,000,000	Cryptsy	United States
4	2-Aug-2016	120,000	$72,000,000	Bitfinex	Hong Kong
5	22-Apr-2017	3,816	$5,000,000	Yapizon	South Korea
6	20-Sep-2018	5,966	$38,000,000	Zaif	Japan
Total		1,000,082	$599,200,000		

Note: The event collection depended on public sources that published reports and news regarding each breach.

2.3.2 Methodology

The impact of cyber-attacks on the cryptocurrencies market has been measured using several approaches (Conti et al., 2018). This study employed social network analysis to capture the influence of security breaches on the cross-market Bitcoin prices network. The advantages of adopting this method are reflected in its ability to display results as a visualised network or as a graph, which can give the chance to examine the impact pre and post each event for all the variables included in the study. Moreover, this model can provide tools that assess the topological structure of the Bitcoin exchange prices network and sort them according to the role they played in the network. Finally, by establishing a network of Bitcoin exchange prices pre and post each attack considered in this chapter, the method helps by detecting and capturing whether a pattern emerged after cyber-attacks.

To estimate the effect of these events, the analysis was conducted in two steps. First, the data were divided into six samples. Each sample represented an event where cyberattacks targeted a Bitcoin exchange platform. The study focused on each attack by analysing the three months pre and post each attack. After selecting a time window, the weighted undirected network constricted, depending on the significant correlation between the cross-market Bitcoin prices. Second, the key factors of the topological structure of the cross-market Bitcoin price network were computed and the results were compared to assess any influence that may have occurred in the network. Also, the study used

centrality measures, which enabled the ranking of the Bitcoin exchange prices to illustrate the changes that may have occurred pre and post each cyber-attack.

2.3.2.1 Network constriction

A network representation of cross-market Bitcoin prices can be shown by a graph G (V, E), where the notation V signifies the actors, elements, or nodes In this study, it refers to the Bitcoin prices in various currencies which are drawn in the asset graph as circles. On the other hand, E is a set of edges or links that state the relations between Bitcoin exchange prices. Edges can be drawn as a line that connects two Bitcoin markets in cases there was a significant correlation between nodes (Lee et al., 2019). Networks can be classified depending on the direction of the relationship between nodes, where, in an undirected network, the edges between two nodes are always the same, indicating that there is a relationship but without any information about the direction of this relationship and which nodes influence the other nodes. On the other hand, in a directed network, the edges represent the connection between nodes and also show the direction of this relationship. In network theory, the two nodes i and j can be called connected if there exists at least one way that i and j lie in one path in the network. The network can be considered connected when every pair of its nodes is connected; otherwise, it is called disconnected (Serrat, 2017). Moreover, the density of a graph is the total number of present edges divided by the maximum number of possible edges in this graph (Silverman, 2018). The value of density ranges between zero and one, and if all possible pairs of edges are present, then the density of the network equals one, and the network can be considered as a complete graph. However, if all possible edges are not present in the network, then the density equals zero, and the network is a disconnected graph. Therefore, the higher value of density can be a positive indicator that signifies a decent level of the interrelationship between the nodes (Bitcoin/ currency). In an undirected network with N nodes, the maximum possible number of links equals:

$$\text{the density of a network} = \frac{N(N-1)}{2}. \quad (1)$$

The daily continuously compounded Bitcoin exchange rate return was computed by taking the first difference of the log-transformed daily weighted price series, and by using the Pearson correlation coefficient, a well-known measure that can capture the relationship to compute the correlations between variables of a study. It can be expressed as follows:

$$\rho_{ij} = \frac{\sum_{i=1}^{n}(e_i - \bar{e})(c_i - \bar{c})}{\sqrt{\sum_{i=1}^{n}(e_i - \bar{e})}\sqrt{\sum_{i=1}^{n}(c_i - \bar{c})}}, \quad (2)$$

where ρ_{ij} is the significant correlation for two variables e_i and c_i. The average returns of the cross-market Bitcoin prices were denoted as $\bar{e}$ and $\acute{c}$, with n being the sample size. In this chapter, correlations between cross-market Bitcoin returns are estimated over the whole period, as well as in rolling samples (with each sample representing an event where cyber-attacks hit Bitcoin platforms) to uncover possible differences in "normal" and "cyber-attack" times. The two pairs of Bitcoin exchange prices are assumed to behave similarly if the correlation ρ_{ij} between the returns of Bitcoin exchange prices is equal to or higher than the specified threshold ($\theta = 0.6$). Therefore, for any relationships under the specified threshold, these values are ignored. This study employs a different level of threshold to check the robustness of this study's analysis results by changing the specified threshold to $\theta = 0.7$ and examining the changes that may occur in the Bitcoin network structure after cyberattacks and any difference of centrality measurement. To visualise a network graph based on the correlation results between all cross-market Bitcoin prices, the adjacent matrix A is constructed as:

$$A_{ij} = \begin{cases} 1 & \text{if } \rho_{ij} \geq= \theta \text{ and } i \neq j \\ 0 & \text{otherwise.} \end{cases}$$

2.3.2.2 Centrality measurement

A significant volume of published studies has highlighted the importance of centrality in the context of network theory, where researchers used centrality measures to categorise and rank the key players in a complex network (Du et al., 2015, Nie et al., 2016, Grassi et al., 2019). Each one of these centrality measures has a certain role that can capture the unique features of each variable in the network (nodes). In the network, a node that has a higher centrality value may consider a crucial element. Thus, the researcher employed several centrality measurements in this chapter and computed the centrality measurements pre and post each cyberattack to assess the influence of these events on the unique features of Bitcoin prices. Additionally, the aim was to capture and understand the changes that occurred in the network's behaviour after the experience of security breaches.

2.3.2.3 Degree Centrality (DC)

Degree centrality is a well-known concept in graph theory and it can be a useful measurement to examine the centrality in undirected networks. It measures the importance of a node due to its connection with other nodes, which is defined by the number of links or edges that exist with other

nodes in the graph. In this current case, this measurement helps to rank Bitcoin prices due to the number of connections with other cross-market Bitcoin prices. In undirected networks, the degree of node i is given as:

$$D_c(i) = \sum_{j=1}^{N} A_{ij} = \sum_{i=1}^{N} A_{ji} \quad , \qquad (3)$$

Where N is the number of neighbours for node$i$. Indeed, a higher value of node degree implies that the Bitcoin pair has more relationships than other nodes in the network. However, this measurement looks only at the numbers of edges linked into a node and ignores the weight of the edge. Therefore, as this study employed undirected weighted networks, the analysis was extended to include the weighted degree centrality (WDC) of a node to label how strong the relationships among Bitcoin markets are. This can be defined as follows:

$$WD_C(i) = \sum_{j=1}^{N} W_{ij} \quad , \qquad (4)$$

Where N represents the number of neighbours of node i and $W_{i,j}$ states the weighted value of edge that linked node i with node j. A higher value of weighted degree centrality (WDC) implies that Bitcoin exchanged currencies have a higher association to other Bitcoin prices. Comparing the results of the DC and WDC measurements pre and post breach events can provide a better understanding of the changes that happened in the network structure. Also, such a comparison can indicate any changes in the most critical players in the Bitcoin prices network.

2.3.2.4 Betweenness centrality (BC)

The second notable centrality measurement is betweenness centrality (BC) which measures and ranks all nodes in the network that acts as a gatekeeper between other nodes. In other words, it measures the number of times that a node is found as a bridge to link other nodes on the shortest path. Freeman (1978) initially developed this concept and later Brandes (2001) and Opsahl et al. (2010) developed a formula of betweenness to be calculated on weighted networks. The Bitcoin pair that has the higher value of betweenness indicates the important role of this pair in the network, by being a gatekeeper or acting as a reference for other Bitcoin prices. Therefore, those Bitcoin exchange rate prices with a higher value of betweenness, in general, perform a vital role in the Bitcoin cross-market price network, due to their capability to raise the overall efficiency of the network (Kim et al., 2011). The betweenness centrality of node i is given as:

$$C_b(i) = 2/(N-1)(N-2)\sum_{r\neq n\neq d}\left(\frac{\sigma_{r,d}(n)}{\sigma_{r,d}}\right) \quad , (5)$$

Where r and d are nodes in the network. In this current case it is the cross-market Bitcoin price, $\sigma_{r,d}$ signifies the number of shortest paths from r to d, and $\sigma_{r,d}$ (n) is the number of shortest paths that n found between the r to d nodes. Again, the higher value of BC for a specific Bitcoin pair implies the vital role that the node played in the network because it can control the flow and movement of information and news between many other Bitcoin exchange rate nodes. After examining the influence of pre and post security breach on Bitcoin prices, this type of centrality can help to indicate the behavioural pattern emerging in the network after suffering from breach events. In particular, this can be shown by tracing the performance of the Bitcoin pair that represents the location of the trading platform that was damaged by cyberattacks.

2.3.2.5 Closeness centrality (CC)

Closeness centrality was first introduced by Dijkstra (1959) to calculates the shortest paths between node (i) to all other nodes in the network. Over the past decade, much more published research on computing the shortest paths in the network has become available (Peay, 1980, Wasserman and Faust, 1994, Newman, 2001; Yang and Knoke, 2001, Opsahl et al., 2010). This measurement ranks all nodes in the network as being a broadcaster. In other words, closeness centrality computes the time that is needed to disseminate some information from a particular Bitcoin/currency to other cross-market Bitcoin prices in the network. Although it is quite similar to betweenness centrality, this measurement (CC) is more appropriate in conditions where a Bitcoin/currency acts as a generator of information, rather than being a gatekeeper in a case of betweenness. However, this type of centrality measurement in the network is influenced by the numbers of nodes in the network. It can be expressed as follows:

$$C_C(i) = 1/< L(s,t) > \quad , \qquad (6)$$

Where <L(s,t)> is denoted as the length of the shortest path between node s and node t. The value of closeness centrality (CC) ranges from zero to one for each node in the network. In our case, the higher value of closeness centrality signifies that a pair of Bitcoin impacts the whole cross-market Bitcoin network prices and has the ability to quickly disseminate information.

2.3.2.6 Eigenvector Centrality (EC)

The final centrality measurement is eigenvector centrality (EC), which was first introduced by Katz (1953) and developed by Bonacich (1972). The idea was to classify the nodes in the network not only based on how many nodes have a direct connection with other nodes in the network, but to extend this further by focusing on the influential role of the node over the whole network and include other indirect connections in the count. Eigenvector Centrality (EC) takes into account the power of the connection or the weight of edges. Therefore, the node that has a relationship with other influential nodes (in this study's case, with other influential Bitcoin/currency) will have a higher value of eigenvector centrality. In other words, this type of measurement sorts the nodes, depending on the most active node in the network that has a connection with other higher effective nodes. It can be calculated as follows:

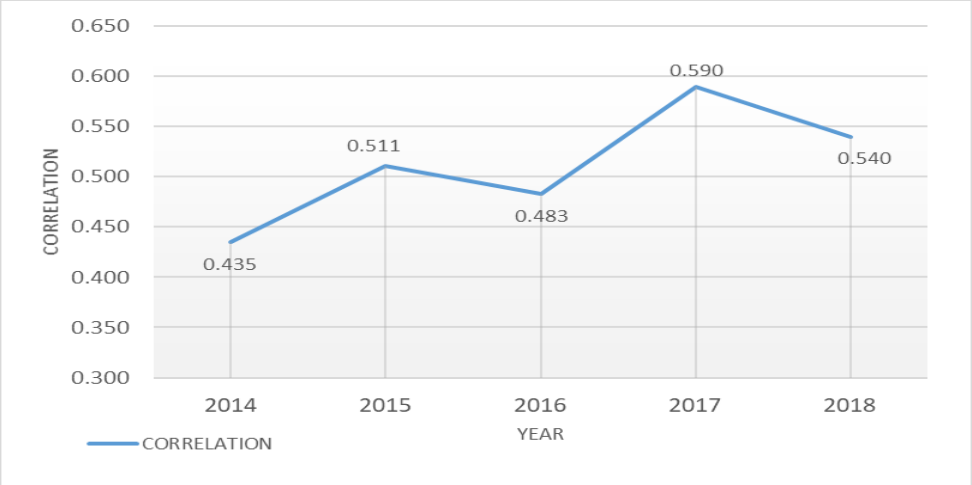
$$EC_{x_i} = \frac{1}{\lambda} \sum_{j \in M_{(v)}} X_j = \frac{1}{\lambda} \sum_{j \epsilon G} A_{ij}\, x_j \,, \qquad (7)$$

Where λ denotes as a constant. A_{ij} indicates the adjacency matrix, G is the total graph, and $M_{(V)}$ implies the number of neighbours to node Xi. In our analysis, a higher value of eigenvector centrality (EC) between Bitcoin cross-market prices implies that this pair has a connection to other strong Bitcoin pairs and might be important to help shed light on the role that Bitcoin/currency plays in the network.

2.4 Main Results

Before analysing the influence of cybercrime on the cross-market Bitcoin price network from time window to time window, the author first looks to the evolution of the Bitcoin prices associations through the years included in this study. The findings are represented in **Figure 2**, below, and show the evolutionary behaviour of the average significant correlation between all Bitcoin cross-market returns included in this study. In 2014 the average correlation was 0.435 compared to 0.54 in 2018; in total, the average correlation in Bitcoin cross-market prices had significantly increased. Thus, the density of the network of Bitcoin exchange rate dependant on the relationship is expected to increase, referring to more association within the undirected network.

Figure 2: Evolution of Bitcoin prices relationship.



2.4.1 Network analysis and centrality measurement

The core aim of this chapter was to investigate the influence of security breaches on the Bitcoin prices network. In this part, evidence of the influence of cybersecurity in the form of six sections is presented. Each one represents an event where a Bitcoin platform experienced significant cyberattack events that generated money loss and Bitcoin theft, as shown in **Table 1**, above. In general, the line (edges) in all graphs in this section represents a significant correlation between nodes, and the thickness of the line shows the value of the correlation, while a thin line implies a weak correlation.

2.4.2 Mt.Gox Bitcoin platform

During the beginning of 2014 – specifically 1 February – the well-known Japanese Bitcoin exchange, Mt.Gox, was subjected to massive cyberattacks, which resulted in more than 850 thousand Bitcoin missed, with a total cost of around 470 million dollars being stolen, as reported in **Table 1**. Also, **Figure A 3** in the appendix demonstrates the structure of the Bitcoin exchange rate network before the Mt.Gox experienced cybercrime, and illustrates the changes that occurred in the network after the cybercrime. However, because of the high network density, the comparison is difficult. Thus, **Table A 4** in the appendix shows the basic topological features of cross-market Bitcoin prices network pre- and post-cyberattack. The results indicate that the number of edges decreased after Mt.Gox suffered from the security breach, implying that the relationship among Bitcoin exchange rates dropped. In the same vein, the average degree, Avg. weighted degree and network density dropped as a response to cyberattacks, which implies that the network topological structure changed, and the cross-market Bitcoin price became less correlated after the cyberattack.

Next, the author computed the centrality measurement for the correlation network of cross-market Bitcoin prices for a different level of threshold (θ), as specified in section four in this paper. **Figure A 3** in the appendix demonstrates the Bitcoin cross-market prices pre- and post- cyber-attacks at the threshold value of $\theta > 0.6$. The results of the network graph show that several Bitcoin/currency pairs disconnected at this level of threshold. On the other hand, after adjusting the value of the threshold to $\theta > 0.7$, the same results indicate that the most crucial Bitcoin/currency changed in the network. To find the most central Bitcoin pair depending on centrality measurement, the top five Bitcoin markets that have the highest value for each centrality measurement were selected. **Table A 5** and **Table A 6** in the appendix show the rank of the best Bitcoin pair that played a significant role in the network. indeed, the top five Bitcoin exchange rates had more relationships than the other pairs, and they had more control in distributing the information across the Bitcoin network. Also, they were capable of spreading or receiving any newly arrived news or information more quickly to other nodes in the network. but as this study employs an undetected network, it can only be argued that the top five Bitcoin pairs can play an important role without referring to the direction of the influences. Thus, after the cyberattack hit Mt.Gox, the ranking of the essential Bitcoin/currency pairs changed. Notably, as the Mt.Gox platform is a Japanese platform, the BTC/JPY pairs lost the role they was playing before the cybercrime event in both levels of thresholds. Before the cyberattacks, BTC/JPY was in the top five Bitcoin pairs that have a unique role in the network, but after the cyberattacks, BTC/JPY lost its influences in the network compared with other Bitcoin markets and had fewer relationships in the network.

2.4.3 Bitstamp Bitcoin exchange

At the beginning of 2015, the European platform was subjected to a security breach. In total, at least 19 thousand Bitcoin went missing, with approximately $5 million stolen, as reported in **Table 1**. Thus, **Figure A 4** in the appendix represents the Bitcoin networks pre and post the breach events. The asset graph indicates that the network becomes more active after the breach and more connected; however, the graph is complex and it is hard to notice the differences. Thus, the changes in the key factor of the topological features are reported in **Table A 7** in the appendix and signify the response of the Bitcoin network to the cyberattack event. In this event, the topological features of the network increased, with significant changes at threshold level 0.7, inferring that the network becomes more active and the relationships among Bitcoin pairs increased. However, the topological features pattern changed compared with the pattern that occurred in Mt.Gox where the key factor of topological features decreased after the security breach.

The impact of cyberattacks on the most crucial player in the network, depending on the centrality measurement, can be seen in **Table A 8** and **Table A 9** in the appendix, which represents the Bitcoin network pre and post the breach event for thresholds of 0.6 and 0.7 respectively. The results reported in **Table A 8** indicate that the BTC/EUR, BTC/USD and BTC/CNY were the top three influential currencies in the network and the BTC/EUR still played a crucial role since the Mt.Gox incident or post the cyberattack. Interestingly, post the cyberattacks, BTC/USD became the first key player in most measurements (EC, DC and WDC) and such as BTC/JYP back to perform an important role depending on CC measurement. In addition, BTC/CNY became more active and influential in the network depending on BC measurement after the attack. The same results hold after using a threshold equal to 0.7, where pre the attacks the market was still influenced by the breach that happened on the Mt.Gox platform. Here it can be seen that BTC/EUR was at the top in the list; however, the same pattern appears again, where the currencies that represent the location of the Bitcoin platform that were influenced by the security breach become less active in the network and the pair lost its unique role in the network. This argument can be supported if the pattern also occurred in all events included in this chapter.

2.4.4 Cryptsy Bitcoin exchange

In the middle of January 2016, another Bitcoin platform located in The United States of America experienced a security breach that resulted in losing more than 1300 Bitcoin. The estimated cost of the breach was more than $US6 million, depending on the price during that period. **Figure A 5** in the

appendix indicates the structure of the Bitcoin exchange rate network pre and post the cybercrime that targeted the Cryptsy platform. Moreover, it illustrates the changes that occurred in the network. The basic topological features of cross-market Bitcoin prices network pre and post the cyberattack are reported in **Table A 10** in the appendix. The findings show the same pattern of topological features after cyberattacks hit the Bitstamp platform where the number of all topological features increases after the attacks at all levels of threshold. Therefore, the Bitcoin network topological structure changed, and the cross-market Bitcoin price became more connected after this cyberattack.

The results of the centrality measurement in **Table A 11** in the appendix indicate the strongest and the most influential Bitcoin/currency pairs where at a threshold level 0. 6, we can see that pre the cybercrime the influence role of BTC/USD in the network were the highest powerful pairs in the network depending on all centrality measurement. It is noted that the Bitcoin network was still under the influence of the previous cyberattacks that targeted Bitstamp in 2015. However, BTC/JPY and BTC/EUR started to gain significant roles in the network. On the other hand, after the Cryptsy platform experienced the security breach the rank of most influencers among Bitcoin pairs changed, whereby the BTC/USD dropped to fourth place, and other Bitcoin markets became more active in the network. Other evidence in **Table A 12** in the appendix shows the results at the 0.7 threshold, which confirms the same change that occurred to the response pattern after cybercrime, where the rank of the key player changed. Thus, these results provide further evidence that cyberattacks can change the topological structure of the Bitcoin and change the key player in the network. In addition, the results for the Cryptsy platform support the claim that the Bitcoin/currency pairs that represent the location of Bitcoin platform that suffered from cyber-attacks become less active in the network.

2.4.5 Bitfinex Bitcoin exchange

The well-known Bitcoin platform located in Hong Kong experienced cybercrime in 2016. As reported in Table 1, the total amount stolen was approximately 72 million dollars which makes this security breach the second largest attacks on a Bitcoin platform since Mt.Gox in 2014. **Figure A 6** in the appendix illustrates the Bitcoin cross-market prices network pre and post the attacks. In this event, the topological features' pattern after each attack changed dramatically. All topological structures of the network sharply decreased, as reported in **Table A 13** in the appendix. For instance, the total number of edges pre-cybercrime was 91; however, post the breach event, the number of edges decreased to 76. This decrease applied on all network features which indicates that the level of the

relationship among Bitcoin markets decreased. Remarkably, the same network adjustment occurred after the security breach hit Bitfinex and Mt.Gox. Indeed, the Bitcoin prices network react differently compared with what happened with the Bitstamp and Cryptsy platforms that did not experience cyberattacks on such a large scale as Mt.Gox and Bitfinex did. This offers further evidence that the size of the cybercrime can have different influences on the topological features of the Bitcoin prices network.

The centrality measurement results indicate adjustment in the top five influential Bitcoin markets at both the threshold values of 0.6 and 0.7. **Figure A 6** presents the changes that happened after cyberattacks in comparison with several levels of threshold. The asset graph depicts the reaction of the Bitcoin prices network, where the network became less connected and some Bitcoin pairs disconnected in the network – for example, BTC/SGD and BTC/RUB. In the same vein, the breach event also impacted the most influencing Bitcoin pair. **Table A 14** and **Table A 15** in the appendix report the changes pre and post the breach event where the effect of the cyberattacks changed the rank of the strongest and influential currencies, whereby the Bitcoin pair BTC/USD was playing a significant role in the network pre the breach event. However, after the cybercrime, BTC/EUR and BTC/JPY become more central in the network at threshold levels of 0.6 and 0.7, respectively. On the other hand, the cyberattacks targeted a Bitcoin platform (Bitfinex) which is located in Hong Kong and BTC/HKD not included in this study. Thus, we can only shed light on the changes that took place at the top key Bitcoin pair without tracing the previous pattern.

2.4.6 Yapizon Bitcoin exchange

Another Bitcoin exchange in South Korea was targeted by cybercrime. The Yapizon platform suffered a security breach that resulted in more than 3800 Bitcoin missing, which was estimated more than $5 million based on the prices during the time of the event. **Figure A 7** in the appendix demonstrates a comparison between Bitcoin pairs network pre and post the cyberattack with several levels of threshold, where BTC/CNY had weak connections with other Bitcoin markets in both time windows. Notably, that was before the china government decided to end Bitcoin trading. The basic topological features in **Table A 16** in the appendix show that all the topological factors increased markedly after the cyberattack. Moreover, the Bitcoin prices network became more connected and with a higher network density in different values of the threshold. Therefore, the results confirm the pattern that occurred after security breach and support this study's claim that the size of the cyberattacks has different influences on the Bitcoin topological factors. Conversely, in the case of Yapizon platform, the response pattern is the same as the response pattern in the cases of Bitstamp and Cryptsy.

The centrality measurement results, reported in **Table A 17** and **Table A 18** in the appendix, show that the ranking of the most central nodes in the network changed. Although BTC/ KRW played a critical role before the attack, the central role for BTC/KRW did not remain after the cybercrime. The same behaviour of the Bitcoin network pre and post each cyberattack depending on centrality measurement results. Where the Bitcoin cross-market price that represents the location of the Bitcoin platform became less active in the network after the event at the different threshold values.

2.4.7 Zaif Bitcoin exchange

The final event included in this chapter occurred in Japan. The Zaif platform was targeted by cybercrime in 2018 and lost around 38 million dollars. There were slight changes in the key factor of the topological features to cross-market Bitcoin prices network pre and post the cyberattacks on the Zaif platform. The changing results in the graph can be noticed in **Figure A 8:** The Bitcoin cross-market price network pre- and post-cybercrime on Zaif platform. in the appendix. The results of the influences of the breach event illustrates the same behaviour when Bitcoin cross-market prices network received the announcement of cyberattacks. In this case, all key factors of the topological features to cross-market Bitcoin prices network post-cyberattacks increased. This provides further evidence that the size of security breach has a vital power to influence the topological features of the Bitcoin prices network.

The centrality measurement results indicate the changes in the top five most influential currencies in the Bitcoin cross-market prices network for both threshold levels, 0.6 and 0.7. Also, the findings display the same behaviour of main players in the Bitcoin network pre and post each cyberattack. When the cyberattacks targeted a Japanese platform (Zaif) there was a significant role for BTC/JPY in the network pre the attacks at all threshold levels as shown in **Table A 20** and **Table A 21**, where BTC/JPY and BTC/USD were the top central Bitcoin pairs in the network. However, after the cybercrime, BTC/PLN and BTC/KRW came in the top list of the most influencers in the network. Therefore, the effects of cyberattacks on the centrality and influential currencies have the same pattern regardless of the size of the cyberattacks. The Bitcoin pairs that denote the location of the platform become inactive in the network after the breach event, and this can be found at different levels of threshold.

2.4.8 Robustness.

Figure A 9 in the appendix displays the Histogram of the probability distributions for Bitcoin cross market prices. The correlation matrix among all Bitcoin pairs present a strong relationship, where the correlation submatrices tilted to higher values heavily, but with some spikes at the right side. Which the histogram and The Jarque-Bera test results in section three indicates to non-normality distribution. Therefore, we implemented assessments to the probability distributions to make sure that the Bitcoin prices network did not built depends on random relations. We considered the time series for each Bitcoin cross market prices and re-sort them depending on a random variable. Consequently, we generated 10,000 simulations, to re-estimate the correlation matrix relaying on the new randomized Bitcoin cross market prices series. As a results we built a probability distribution that depicted in Figure A 10 in the appendix. Referring that the correlations below -0.3 or above 0.3 not caused by random effects. We observe very similar results for the rest of events included in this chapter. Therefore, the results of the correlation that was used to build the Bitcoin prices network was statistical significance, as we employed higher value of correlation at level 0.6 and 0.7.

2.5 Conclusions

The central questions posed at the opening of this chapter were how cybersecurity that targeted Bitcoin exchange platforms can influence the structure of Bitcoin network prices. The study also enquired how the security breaches can impact the network and change the ranking of the most crucial Bitcoin pair pre and post each breach event. It is now possible to state that the investigation shows the changes that occurred in the topology structure after using rolling estimations pre and post security attacks and differentiate between the influence of cyberattacks depending on the size of the breach event and the amount of Bitcoin lost because of this type of criminal activity. Also, by using centrality measurement to assess the influence of a security breach on the crucial active Bitcoin pairs in the network, the most obvious finding was that these types of shocks can change the ranking of the central Bitcoin/currency pair in the network.

Depending on the centrality measurement results, one can clearly observe that there was a pattern after all security breaches included in the study. It was shown that the performance of the Bitcoin pairs that represented the place of trading platform that was subjected to cyberattacks became less active and dominant in the network regardless of the size of attack. Moreover, a pattern appeared depending on the size of the cyberattacks; the large scale of cybercrime decreased the topological features to cross-market Bitcoin prices network. On the other hand, the small scale of cyber-attacks increased the topological features of the cross-market Bitcoin prices network.

Not surprisingly, the influence of cybersecurity on Bitcoin is one of the most significant current discussions in this nascent literature, particularly amongst portfolio managers, who want to understand how the Bitcoin exchange prices interact in the market after dealing with cyberattacks. The results hold implications for investors and portfolio managers to construct the best investment strategy that reduces the expected loss after a breach event because, as the finding suggests, security breaches strengthen cross-market linkages among Bitcoin markets, therefore decreasing portfolio diversification. Also, investors should not ignore the risk of cyberattacks if they occurred in other platforms in which they did not hold investments, and should also pay particular attention to the Bitcoin pairs that represent the place where the trading platform was hacked. Another important practical implication is that cryptocurrency investors need to understand the role of security breaches' scale that targeted Bitcoin platforms. These findings suggest several courses of action that can be taken by platform supervisors and information security managers of the Bitcoin exchange platforms to be aware of the potential risk of a security breach on the Bitcoin network structure. The findings also raise the need to develop policies for avoiding the spread of

cyberattacks' influences on the Bitcoin cross-market prices. Finally, the current findings add to a growing body of literature and enhance our understanding of the influences of cybercrimes, and the role of key players in the Bitcoin cross-market prices to act as gatekeeper or their ability to spread information as a response to this type of security breaches. The current study has only examined the cyberattacks that targeted Bitcoin platform; however there were several cyber-attacks that targeted mining platform and cryptocurrency investors. The most significant limitation lies in the fact that the study cannot examine the security breaches that occurred before 2014 due to the missing data in the Bitcoin cross-market prices.

This work plants the seeds for future research that assesses the impact of cybercrime on Bitcoin cross-market prices. The results of the study reveal the need for further investigation to show the impact of different types of cyberattacks on the relationships among Bitcoin cross-market prices. The findings also highlight the need to analyse the size of cyberattacks impact on other cryptocurrencies markets. In future investigations, it might be possible to use a different method to examine the influence of cybercrime on the Bitcoin market.

Chapter 3

Information Spillover, Cross-Market Bitcoin Prices and Cyberattacks: Evidence from a Dynamic Entropy Network

3.1 Introduction

Trust is an essential component in the financial transactions and payments systems. Therefore, the cash system was built on trust (Marmefelt, 2018, Tsiakis and Sthephanides, 2005). However, with new Internet technologies and the evolution of e-commerce, the need for a new cash payment system has emerged, with different online payment systems being introduced, such as PayPal (Chuen, 2015). Meanwhile, during the financial crisis in 2008 and when people's trust in traditional financial systems was at its lowest level, a paper introduced a new cash system which was without intervention from authority or any legal entity and known as Bitcoin (BTC) (Nakamoto, 2008). As cryptocurrencies – particularly Bitcoin – adopted Blockchain technology, the level of transparency increased compared with the traditional financial system. Because of this, people's trust in this system increased and they began to use cryptocurrencies to transfer money across international borders (Marella et al., 2020). However, cryptocurrencies such as Bitcoin suffer from serious drawbacks. First, because there is no intervention from authorities or any legal entities, this may make Bitcoin vulnerable to manipulation, which may generate more risk (Gandal et al., 2018). Second, cryptocurrencies do not employ names or social security as proof of ownership; instead, they use a public key address, which is a 32-bit code comprising a combination of numbers and characters (Nakamoto, 2008). As a result, cryptocurrencies offer an instrument for illegal trade, tax evasion and money laundering (Brezo and Bringas, 2012). Finally, sometimes the cryptocurrencies market prices are extremely volatile for several reasons (Conti et al., 2018), one of which is the impact of security breaches that target cryptocurrency wallets or exchange platforms – for instance, the large scale cyberattacks that hit Mt.Gox in 2014.

In general, the estimated cost of security breaches in 2014 was about $500 billion for the global economy, equivalent to around 0.7% of the world's income. However, this amount significantly increased in 2018 to almost $600 billion of cybercrime events, or 0.8% of the world's income (Lewis, 2018). In 2019 there was approximately more than $4 billion of theft in the cryptocurrencies market, compared to $1.7 billion of crypto crimes in 2018 (Forbes, 2019). The aim of the current study was to investigate the influence of cyberattacks on information transmission between Bitcoin cross-market prices and to trace the changes that may occur in the causal relationships among Bitcoin prices. In addition, the study aimed to shed light on the temporal evolution of Bitcoin cross-market prices pre, during, and post each security breach, and to classify the main senders and receivers of information among Bitcoin pairs pre and post breach events, which can help to detect any contagion risk after Bitcoin prices network experienced security breach. The central question in this chapter seeks to address how the security breaches influence the flow of information between Bitcoin cross-market

prices and whether security breaches that target the Bitcoin platforms can change the leading Bitcoin exchange price sender or receiver of information.

This study contributes to the growing area of research by exploring Bitcoin markets' exchanges in various currencies over the last five years, which covers several major security breach events. Also, the current study investigated diverse periods by employing Effective Transfer Entropy and presenting the results using asset graphs to capture the co-movements and dynamic causalities of the examined networks. Another contribution was to capture the response pattern, which occurred in the flow of information between the cross-market Bitcoin prices after experiencing cyberattacks and the response pattern in the temporal evolution of Bitcoin cross-market prices pre, during, and post each security breach. Finally, the study findings reveal the potential impacts of cybercrime for investors, speculators, and Bitcoin exchange platform managers.

Several studies have shown an increased interest in the role of cyberattacks influencing the cryptocurrencies market, but few researchers have been able to draw on any systematic research (Conti et al., 2018, Corbet et al., 2019b). Meanwhile, this concept of cybercrime and its impact on cryptocurrencies has recently been challenged by a number of scholars (Hamrick et al., 2018, Shanaev et al., 2019, Azqueta-Gavaldón, 2020, Caporale et al., 2020b), demonstrating the impact from several points of view. However, in reviewing the literature, as showing in Table 1-2 in the appendix show the two groups of studies where group A represents the works that addressed the influence of cybercrimes in the cryptocurrencies market, meanwhile group B represent the studies that examined the spillover in the cryptocurrencies market. Thus, it was identified that little is known about the impact of security breaches on the information spillover among Bitcoin cross-market prices. Also, much uncertainty still exists about the temporal evolution of the Bitcoin cross-market prices network after experiencing a security breach.

The rest of this paper is structured as follows. Section 2 discusses works related to the study by looking at the academic literature on the cybercrime-targeted cryptocurrencies market. Section 3 describes the data and the methodology, which was network analysis and Effective Transfer Entropy (ETE). Section 4 presents the empirical results. Finally, Section 5 conclude.

3.2 Related Work

A large and growing body of literature is paying particular attention to the impact of cybercrime on the financial sector as a whole (Lagazio et al., 2014, Kopp et al., 2017, Bouveret, 2018), as well as banking sectors (Malik and Islam, 2019, Wang et al., 2020), stock markets (Anderson et al., 2013, Kamiya et al., 2020) and the Bond market (Iyer et al., 2020). In the case of cryptocurrencies, a number of studies examined the impact of cybercrimes on cryptocurrencies (Gandal et al., 2018, Shanaev et al., 2019, Caporale et al., 2020b). Cybercrimes in cryptocurrencies can be distinguished into two general forms. First, there is cybercrime arising from cryptocurrency usage; for instance, money laundering (Vandezande, 2017), ransomware (Zimba et al., 2018), terrorism financing and darknet markets (Chainalysis, 2020). The immoral uses of cryptocurrencies have led to an increase in the number of related ethical problems (Martin and Christin, 2016). The Silk Road website is the best example of cyber criminality using darknet markets. Because of the lawless nature and the provision of anonymity in digital currencies, users of the Silk Road abuse this feature by using Bitcoin or other cryptocurrencies to complete drugs or guns deals. However, the FBI arrested the owner of Silk Road and shut down the website in November 2013. The price of Bitcoin fell after the closure of the Silk Road website from approximately 146$ to 108$. The FBI reported that Silk Road accounts formed approximately 5% of the Bitcoin economy (Hill, 2013). However, the survival of Bitcoin following the closing of the Silk Road website is an indication of Bitcoin's resilience.

The second form of cybercrimes are the security breaches that target the cryptocurrencies themselves. The hacking of cryptocurrency hot wallets and platforms has become more widespread recently and more severe. Several cyberattacks have managed to steal different types of cryptocurrencies. For instance, the largest heist in the Bitcoin market occurred in 2014, when Mt.Gox lost approximately $470 million (Gandal et al., 2018). Another large hacking event in the cryptocurrencies market was in 2018, when Coincheck lost $500 million in the initial offering for NEM coins. Therefore, in this chapter the author examined the influences of security breaches that targeted Bitcoin platform and caused money loss by showing the changes that occurred in the causal relationships among Bitcoin pairs, and also traced the dynamic evolution of Bitcoin cross-market prices network after each security breach.

Drawing on a broader range of studies, Conti et al. (2018) provided a broad review of the challenges that Bitcoin faces and argued that Bitcoin has been subjected to different types of cybercrime, such as double spending, mining pool attacks and Bitcoin network attacks, all of which can target the Bitcoin platform, wallet, and mining activities. In another major study, Corbet et al. (2019b)

reviewed the published literature based on the cryptocurrencies market for the period 2009 -2018. The authors set out four main categories of the current literature, each covering a distinct areas. They argued that cyber criminality in the cryptocurrencies market distinctly investigated. However, drawing on extensive range of sources, they identified 10 research gaps in the current literature.

Shanaev et al. (2019) analysed the data from 13 cryptocurrencies to examine the influence of 14 individual 51% attacks. They concluded that there were 'pump and dump' schemes after each attack, and the market becomes more efficient after 51% attacks, indicating that cyberattacks have a negative effect on the return of cryptocurrencies. However, most of the cryptocurrencies included in the study were not leading cryptocurrencies. Therefore, the study did not provide evidence of the influence of 51% attacks on the leading cryptocurrencies, such as Bitcoin or Ethereum. Thus, it would be beneficial to examine the influences of this type of cyberattack, especially after the Crypto platform Gate.io announced at the beginning of January 2019 that it had suffered a 51% attack. The hacker managed to transfer a total of 54,200 Ethereum Classic (HUILLET, 2019).

Caporale et al. (2020a) draw our attention to distinctive groups of cyberattacks affecting the returns for five leading cryptocurrencies – Bitcoin, Ethereum, Litecoin, XRP and Stellar. They also claimed that cyberattacks can affect cryptocurrencies platforms in all countries included in their study, although the US cryptocurrency platforms were less vulnerable to a security breach. However, this research was unable to make a distinction between the types of cyberattacks that targeted cryptocurrencies: for example, *DDoS* attacks on cryptocurrencies platforms (Feder et al., 2018), *51%* attacks (Caporale et al., 2020a), *double-spend* attacks (Pinzón and Rocha, 2016), and *pump and dump* schemes (Hamrick et al., 2018). In the same vein, Azqueta-Gavaldón (2020) investigated the impact of media coverage of cryptocurrency narratives and its causal relationship with prices. Furthermore, he listed four types of narrative, one of which was the media coverage of security breaches in cryptocurrencies markets. After using the Granger causality test, the author argued that there was a unidirectional causal between narratives related to cybercrimes and prices. However, this method of analysis has several limitations; the most serious limitation is that it depends heavily on the number of lags selected. Moreover, the study used the BTC/USD as a proxy of cryptocurrencies prices. Likewise, Francés et al. (2018) drew on the minimum spanning tree technique, by analysing 16 cryptocurrencies, and concluded that Ethereum has a vital role and acts as the benchmark currency rather than Bitcoin.

A number of authors reported the impact of cyberattacks on cryptocurrencies. Caporale et al. (2020b) conducted a non-linear Markov switch to evaluate the cyberattack impact on the returns of

four cryptocurrencies. They argued for the probability of cryptocurrencies being influenced negatively by cyberattacks and remaining within low volatility throughout August 2015 – February 2019. Similarly, Corbet et al. (2019a) traced 17 hacking events that targeted the eight most liquid cryptocurrencies within less than a year and, after employing a DCC-GARCH model, they pointed out several findings. First, the correlations between cryptocurrencies increase after cyberattack. Second, the volatility also increases after each security breach. Finally, they provide evidence that in the hours before a hacking event there were abnormal returns and drop to zero when the hack event is revealed publicly. However, the findings would have been much more persuasive if the authors had considered a period of more than one year.

This chapter was a quest to analyse the exchange of information between Bitcoin cross-market prices as seen by Transfer Entropy. The concept of Transfer Entropy has been addressed in several scientific investigations, relating to, for instance, social networks (Ver Steeg and Galstyan, 2012), in the context of medicine (Valenza et al., 2017), dynamical systems (Mao and Shang, 2017), causal influences (Razak and Jensen, 2014), and in the field of thermodynamics (Auconi et al., 2019). A number of studies in the finance literature have applied Transfer Entropy, such as in the Stock markets (He and Shang, 2017, Dimpfl and Peter, 2018), Real Estate markets (Ji et al., 2018) and Commodity markets (Bekiros et al., 2017). In terms of application in the cryptocurrency field, a growing body of literature has employed this concept; for example, drawing on the concept of Transfer Entropy, Ji et al. (2019) were able to construct a network to show the information spillover between various commodities and five major cryptocurrencies. In addition, Dimpfl and Peter (2019) investigated the four major cryptocurrencies (Bitcoin, Ethereum, Litecoin, and Ripple) to show the differences between using linear methods and nonlinear approaches to detect information transfer. Moreover, they argued that Granger-causality tests or VAR model are not suitable to capture the dependencies within a system, particularly with the new financial products such as cryptocurrencies. Moreover, depending on intraday data, they highlighted how the linkages and dependencies between cryptocurrencies mostly have a nonlinear nature. Thus, in this chapter the author employed the nonlinear Transfer Entropy model to trace the change contagion risk of cyberattacks among Bitcoin markets.

3.3 Data and Methodology

3.3.1 Data characteristics

The data were collected from the www.bitcoincharts.com website, covering the period between 1/10/2014 – 5/8/2019, for the 10 major Bitcoin/currency pairs included in this chapter, as shown in **Table B 1**, in the appendix. The cross-market Bitcoin price was obtained from different exchange platforms for each currency, which were selected because they would fairly represent the market trading activities and have a decent market share in the targeted currency over the study period. Moreover, the reason behind selecting several platforms for one exchange currency was because some platforms closed after a particular time; for instance, the Japanese Bitcoin platform, Zaif, stopped providing services in the market after security breach. Moreover, some of the platforms lost their market share, such as in the case of the Canadian platform Quadrigacx, where the data were obtained from this platform until December 2018, and then the rest of the data were gathered from the Karken platform. Therefore, to construct continuous time-series data, data were gathered from other exchange platforms in order to fairly represent the whole market, since Bitcoin was traded every minute throughout the entire year.

As this study uses specific events related to security breaches that rarely occurred during the entire sample period the examination of narrow window lengths is required. This study employed 6-hours frequency depending on the Coordinated Universal Time (UTC) timestamp. The market liquidity plays a crucial role in selection of the data frequency. For instance, employing less than 6 hours, such as 1, 5, 10, 15, 30 or 60 minutes, may often lead to unreliable and spurious results because there were missing data due to low liquidity in the cross-Bitcoin prices, particularly during 2015 and 2016. On the other hand, statistical problems may have arisen if the study had used more than 6-hours frequency, which would have influenced the results because of the effects of small sample size.

A security breach was considered in this study to be any attack that targeted only the Bitcoin platform and generated money loss. The breach events were collected from public sources on the Internet that published reports and news articles over the period 2015–2019, which included several episodes of security breach and covered several cybersecurity scales, to shed light on the influence of the size of the breach on the information flow between Bitcoin cross-market prices. Table 2, below, lists seven events and contains the dates of the cybercrime and the names of the Bitcoin platforms that experienced security breaches, recording the amount of Bitcoin missed and the cost of each breach at the time it happened.

The daily continuously compounded Bitcoin exchange rate return was computed by taking the first difference of the log-transformed daily weighted price series.**Table B 2** in the appendix reports the summary statistics for each returns series. The number of observations was 6236 for all variables except for BTC/CNY, whereas in October 2017, the China government decided to end Bitcoin trading; thus, the number of observations was 3533 for BTC/CNY. BTC/AUD has the highest value of standard deviation, followed by BTC/CAD. The maximum Bitcoin return was in BTC/BRL, and minimum values were for BTC/PLN. Depending on the average return, BTC/CAD, BTC/GBP and BTC/EUR achieved the highest daily average returns. Also, the positive values of skewness implies that the cross-market exchange returns were skewed to the right. In contrast, they were skewed to the left in cases of negative value. Meanwhile, the All Cross-market returns series displayed leptokurtic behaviours, with higher values for BTC/PLN and BTC/CNY. The Jarque-Bera test was significant and the results for all returns series indicated a non-normality distribution. Augmented Dickey Fuller test signified that all returns series are stationary.

Table 2: Cyberattack-targeted Bitcoin exchange platforms between 2015 and 2019

No	Date	Bitcoin missed	Amount	Platform	Country of platform
1	5-Jan-2015	19,000	5,200,000	Bitstamp	UK
2	15-Jan-2016	1,300	6,000,000	Cryptsy	United States
3	2-Aug-2016	120,000	72,000,000	Bitfinex	Hong Kong
4	22-Apr-2017	3,816	5,000,000	Yapizon	South Korea
5	20-Sep-2018	5,966	38,000,000	Zaif	Japan
6	26-Jan-2019	8	28,200	LocalBitcoins	Finland (EU)
7	7-May-2019	7,000	41,000,000	Binance	Malta
Total		157,090	167,228,200		

Note: The event collection depended on public sources that published reports and news regarding each breach.

3.3.2 Methodology

In order to understand how cyberattacks influence the flow of information between cross-Bitcoin prices and the dynamic causalities, the sample was divided into seven sections. Each section represents an event or security breach that targeted the Bitcoin platform. Furthermore, for analysis purposes, each section was also divided into pre-cyberattack and post-cyberattack. There were 360 observations for every window span, which represented three months pre the breach, and three months post the cyberattack. This might be characterised as an acceptable compromise, and not to dilute too many extreme/peak events. Moreover, not applying a small sample size had a simultaneous effect.

Identifying the magnitude and the direction of interdependence and flow of information among time series in any systems is a crucial topic. Different authors have measured causalities and the flow of information in a range of approaches. Granger causality is one of the most well-known tools to capture the causality relationship. Urquhart (2018) examined the causality relationship between Bitcoin volatility and return from one side, and Bitcoin attention, in the form of Google trends, from the other side. Furthermore, he argued that there was no significant causal relationship between the variables of the study. However, Corbet et al. (2019b) proposed using Granger causality to study the same variables examined by Urquhart (2018) and found that there was a bi-directional causality between the variables. Similarly, Shen et al. (2019) also found significant causality between Bitcoin return and the number of tweets. A significant problem with the Granger causality method is that it depends highly on the number of lags chosen. Also, Granger causality is limited in its capacity to examine the amount or the magnitude of information flow between nodes in the network; it can only show the direction of the relationship.

In this chapter, the author suggests using the nonlinear approach, Transfer Entropy, which is a tool for analysing time-series causalities. Dimpfl and Peter (2019) showed the differences between using linear methods and nonlinear approaches to detect information flow and argued that Granger-causality tests or VAR are limited in their ability to capture the dependencies within a system, particularly in the new financial product such as cryptocurrencies markets. Therefore, the author decided to employ Effective Transfer Entropy (ETE), as this method avoids the limitations of the previously mentioned approaches.

3.3.2.1 Transfer Entropy

To capture the contagion effect among the Bitcoin market and to recognise the source of the information transmitter pre and post cyberattacks, the nonparametric method of Transfer Entropy was adopted. This method was developed by Schreiber (2000) and can help to capture the directionality between Bitcoin prices. More importantly, this method can be considered as a powerful technique to quantify the connection strength and asymmetric properties in a dynamic system. Generally, the Shannon Transfer entropy was derived by the theory of information, which was introduced by the American mathematician, Claude Shannon. The main challenge According to Shannon was how to re-create a message sent from another location (Shannon, 1948). When anyone analyzes a group of potential incidents with probability of occurrence $p_{i,i} = 1, \cdots, n$, then a measure $H(p_1, p_2, \cdots, p_n)$ of the uncertainty of an event's result given such a distribution of probabilities should have the main aspects:

- $H(p_i)$ should be continuous in p_i.
- If all probabilities are similar, then H should be a monotonically climbing function of n.
- If a selection is decomposed into different options with probability c_j, $j = 1,\ldots., k$, then $H = \sum_{i=1}^{k} ci\ Hk$ where H_k is the value of the function H for every selection.

Therefore, Claude Shannon identified the function which meets all three characteristics by

$$H = -\sum_{i=0}^{n} p_i\ log_2 p_i \qquad (1)$$

The Shannon entropy quantifies the average amount of bits required to encode a variable X. However, variable X may influenced from the interaction with other variables. Therefore, we can assume that variable X is a Markov process of degree k, on another words the state i_{n+1} of the variable X is determined by its k past states. More mathematically, the time series of variable X is a Markov state of degree k if

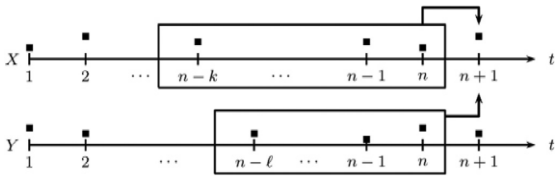
$$p\ (i_{n+1}|i_n, i_{n-1}, \ldots, i_0) = p\ (i_{n+1}|i_n, i_{n-1}, \ldots, i_{n-k+1}) \qquad (2)$$

Where $p(A|B)$ is the conditional probability of A given B, defined as :

$$p(A|B) = \frac{p\ (A,B)}{p\ (B)} \qquad (3)$$

The expression (2) referring to the conditional probability of state i_{n+1} of variable X on all its earlier states is the equal as the conditional probability of i_{n+1} on its k prior statuses, meaning that it does not depend on states previous to the k th previous states of the same variable. Transfer Entropy measures the amount of information that flows from one variable to another variable which can reduce the uncertainty, the concept is represented in Figure 1. More formally, suppose there are two discrete and stationary variables (X and Y) and they interact within a period. Therefore, to compute the flow of information from Y to X, we cannot only rely on the past state of variable X, but also need to include the information contained in variable Y. Where in the process of communication between the two-time series (X and Y). That interaction may generate influences from the time series of variable Y to another time series of variable X.

Figure. 1: Schematic representation of transfer entropy.



Thus, The Transfer Entropy is defined as:

$$TE_{Y\to X}(K,l) = \sum_{i_{n+1},i_n^{(k)},j_n^{(l)}} \left[P\left(i_{n+1},i_n^{(k)},j_n^{(l)}\right) log_2\, p\left(i_{n+1},\left|i_n^{(k)},j_n^{(l)}\right.\right)\right] - \sum_{i_{n+1},i_n^{(k)},j_n^{(l)}} \left[P\left(i_{n+1},i_n^{(k)},j_n^{(l)}\right) log_2\, P\left(i_{n+1},\left|i_n^{(k)}\right.\right)\right]$$

The Transfer Entropy of Y to X becomes simpler:

$$TE_{Y\to X}(K,l) = \sum_{i_{n+1},i_n^{(k)},j_n^{(l)}} \left[P\left(i_{n+1},i_n^{(k)},j_n^{(l)}\right) log_2 \frac{p\left(i_{n+1},\left|i_n^{(k)},j_n^{(l)}\right.\right)}{P\left(i_{n+1},\left|i_n^{(k)}\right.\right)}\right], \quad (4)$$

where i_n is the number of observations of X series, j_n refers to the number of elements for variable Y, the element K donates previous states of the variable X, and ℓ shows the prior states of the variable Y. $P\left(i_{n+1},i_n^{(k)},j_n^{(l)}\right)$ represents joint probability between the previous states of the variables, and $P\left(i_{n+1},\left|i_n^{(k)}\right.\right)$ denotes the conditional probability of the state of variable X on all its past states. Meanwhile, regarding $p\left(i_{n+1},\left|i_n^{(k)},j_n^{(l)}\right.\right)$, this part of the equation shows the conditional

probability, where, if variable X depends on another variable Y, we assume that the state of X depends on the previous states of the source Y. We assume that k = ℓ = 1 following the previous literature from empirical research in financial markets (Bekiros et al., 2017) and other literature which analyses information interdependence in cryptocurrency markets (Ji et al., 2019). However, we will verified by computing the case where k = ℓ = 2, and tracing whether using greater values k and ℓ may provide some better outcomes. Figure B 12 and Figure B 13 displays a heat map of effective transfer entropy matrix (ETE), displaying higher-value causal relationships with brighter color and lower value interactions with darker tones. Figure B 12 display effective transfer entropy matrix (ETE) in case of k = ℓ = 1. Meanwhile, Figure B 13 demonstrate the effective transfer entropy matrix (ETE) in case of k = ℓ = 2. By comparing the first Figure and the second heat maps, there was no noticeable change between them. Thus, calculating transfer entropy can be time-consuming, especially when there are a number of events to evaluate. Therefore, throughout this chapter the k = ℓ = 1 employed to compute effective transfer entropy matrix (ETE).

3.3.2.2 Effective Transfer Entropy (ETE)

Effective Transfer Entropy (ETE) was proposed by Sensoy et al. (2014) and can be considered as an improved approach to Transfer Entropy. This method can help to reduce the limitations of Transfer Entropy that usually contain much noise caused by random series and the data may be non-stationary. These effects can be reduced if the Transfer Entropy of a randomised time series can be calculated. To break any causality relation between variables and elements in the time series dependencies, this approach randomly shuffles each time series individually, but preserves the individual probability distributions for each variable. An Effective Transfer Entropy matrix (ETE) may be calculated as shown in equation (2), below, whereby subtracting the Randomised Transfer Entropy matrix (RTE) from the Transfer Entropy matrix (TE) is defined as follows:

$$ETE_{Y\rightarrow X} = TE_{Y\rightarrow X} - RTE_{Y\rightarrow X.} \quad (5)$$

The calculation of Effective Transfer Entropy may involve a significant computational burden, particularly as the influences pre and post of seven breach events are examined, as shown before in Table 2. Therefore, this study used the results of the Effective Transfer Entropy, since it provides more accurate and robust results compared with Transfer Entropy. The “RTransferEntropy” package proposed by Behrendt et al. (2019) was used to analyse the data.

3.3.2.3 Asset Graphs of Effective Transfer Entropy

Depending on the network theory, there are two types of network – *directed* and *undirected*. The classification of network type depends on the direction of the relationship between nodes. In an undirected network, the edges between two nodes are always the same, indicating that there is a relationship, but without any evidence about the direction of this relationship and which nodes influence the other nodes. On the other hand, in a directed network, the edges represent the connection between nodes and also show the direction of this relationship. This study employed a method that could capture the magnitude and the direction of flow of information among Bitcoin cross-market prices, and thus it adopted the asset graph method to represent the results of Effective Transfer Entropy (ETE) and to reveal the hidden information within the results of ETE.

To estimate the effect of these cybercrime events on Bitcoin markets, the analysis was conducted in two stages. First, the influence of security breach pre and post each attack was measured, where every time window represented three months, with 360 observations for the Bitcoin cross-market returns. Depending on the Effective Transfer Entropy matrix the author built a directed network in the form of an asset graph. Thus, the key factors of the topological structure of the network were computed, and the results were compared to results gained pre- and post-cybercrimes. Furthermore, the top senders and receivers of information pre and post each attack were ranked which can provide evidence of whether there was a contagion effect generated after the security breach. The second stage shed light on the network dynamics analysis, to trace the dynamic influences of the security breaches on the Bitcoin cross-markets and provide evidence on the adjustment of the flow of information as a dynamic response regarding breach events. The study applied moving windows, each period covering one month, with 120 observations for each period.

The network consists of a node linked with edges. In this chapter, the node in the network signifies Bitcoin cross-market prices for 10 Bitcoin pairs. Moreover, the network edges represent the significant value of Effective Transfer Entropy and the direction of information flow. The changes in the main factors of the topological structure of the network were the central focus of the chapter. To trace the influence of security breaches in the Bitcoin platforms, each key factor was computed pre and post each cyberattack to compare the results and to evaluate the impact of this type of breach. The number of edges represents the total number of connections in the network; moreover, the average degree denotes the number of each Bitcoin exchange price having direct connections with another Bitcoin pair. Also, the graph density shows the total number of present edges divided by the maximum number of possible edges in the graph. All these key factors of the topological

structure can help to provide an indicator of the level of interaction in the network. Similarly, as this study employs a directed network, the edges can be divided into ingoing and outgoing links. Therefore, the node degree is also divided into the IN-Node Degree (Nd_{in}), which computes the sum of all edges pointing to a particular node, and the Out-Node Degree, which measures the sum of all edges pointing out to a specific node. Finally, IN-Node Strength (NS_{in}) represents the sum of the weights of all edges that point to a certain node, whilst Out-Node Strength (NS_{out}) calculates the sum of the weights of all edges that begin pointing to a specific node.

Closeness centrality was first introduced by Dijkstra (1959) to calculates the shortest paths between node (i) to all other nodes in the network. Over the past decade, much more published research on computing the shortest paths in the network has become available (Peay, 1980, Wasserman and Faust, 1994, Newman, 2001; Yang and Knoke, 2001, Opsahl et al., 2010). This measurement ranks all nodes in the network as being a broadcaster. In other words, closeness centrality computes the time that is needed to disseminate some information from a particular Bitcoin/currency to other cross-market Bitcoin prices in the network. this measurement (CC) is more appropriate in conditions where a Bitcoin/currency acts as a generator of information, rather than being a gatekeeper in a case of betweenness. can be expressed as follows:

$$C_C(i) = 1/< L(s,t) > \quad , \qquad (6)$$

Where <L(s,t)> is denoted as the length of the shortest path between node s and node t. The value of closeness centrality (CC) ranges from zero to one for each node in the network. In our case, the higher value of closeness centrality signifies that a pair of Bitcoin impacts the whole cross-market Bitcoin network prices and has the ability to quickly disseminate information. For directed networks the Closeness centrality can be divided into IN- Closeness and OUT- Closeness. And we will employ this measurement to calculate how many steps need to infect all other nodes. As we estimating the influence of cyberattacks on Bitcoin cross market price, it would be helpful to identify the contagion risk and how the cyberattacks change the interactions among Bitcoin prices network.

3.4 Main Results

Several studies have highlighted the impact of cybercrimes on the cryptocurrencies market, as discussed in the related work section (Gandal et al., 2018, Corbet et al., 2019a, Shanaev et al., 2019, Caporale et al., 2020b). This study aimed to measure the influence of security breaches that targeted the Bitcoin platforms, by tracking the influences of seven cybercrime events and by calculating the Effective Transfer Entropy to show the changes that could happen to the information spillover and the contagion risk of breach events in the network.

3.4.1 Asset graphs for Effective Transfer Entropy

In this section, the study employed Effective Transfer Entropy to evaluate the causal relationship among Bitcoin cross-market prices, presenting the results by using asset graphs. The study considered several key factors to trace the changes in the topological structure of the network and also to examine the changes in the direction and the magnitude of information flow in the network. The analysis is divided into two sections, whereby the first section focused on the changes that occurred in the network within the three-month period, and the second section analysed the temporal (dynamic) dimension of Effective Transfer Entropy linkages between Bitcoin cross-market prices.

3.4.1.1 Information flow using Effective Transfer Entropy

The study was designed to assess the influence of cyber-attacks on Bitcoin cross-market prices. The effect of the security breach on information flows was traced by analysing pre and post each breach event. Based on the results of Effective Transfer Entropy, **Figure B 1** in the appendix illustrates the Bitcoin cross-market prices pre and post the cyberattacks that targeted the Bitstamp platform in 2015. However, it was shown that after the Bitcoin platform suffers from loss as the result of a security breach, the network of information interchange between the Bitcoin cross-market prices interacts as a response to this event. The reaction post the breach event is depicted in **Figure B 1** in the appendix whereby it can be seen that the number of links between nodes increased dramatically, and the direction of the information flow also changed. Furthermore, the network becomes more active after the breach event. The differences between pre and post security breach are highlighted in **Table B 3** in the appendix. This reveals several findings: (i) the cyber-attack that targeted Bitstamp influences the topological features of the network; (ii) all the key factors increased after the attack, indicating that the amount of information flows increased after the attack

and (iii) the network became more active in comparison with the network before the security breach.

Moreover, the results obtained from **Table B 4** in the appendix present the changes which occurred to the directions of the causality or information flows among Bitcoin markets, whereby the top senders and receivers of the Effective Transfer Entropy pre and post the cybercrime have changed due to breach events. Before the attack, BTC/BRL, BTC/ GBP and BTC/PLN were the top three receivers of information. However, after the breach, the top Bitcoin receivers of information became BTC/AUD, BTC/BRL, and BTC/JPY, respectively. Meanwhile, the top senders of ETE also changed to become BTC/USD, BTC/GBP and BTC/EUR, which are the three main transmitters of information in the network after the breach event. Nevertheless, the Bitcoin pair, BTC/EUR, continued to have a significant role in the network and remained an influential sender of the information in the network. Interestingly, the Bitcoin pair that represented the location of the Bitcoin platform became more active in the network when sending information while, in the case of the Bitcoin platform Bitstamp, the BTC/EUR continued to play a central role in the network. These findings can indicate the contagion risk of a security breach in the Bitcoin markets.

The network of information flow for the bitcoin prices pre and post the American platform Cryptsy, cybercrime can be compared in Figure B 2 in the appendix. It can be seen that the network become more connected, which refer to the increase of information transferred between bitcoin cross prices after the security breach Table B 5 in the appendix compares the key factor of topological features results obtained from ETE. It is apparent from this table that the number of edges and the Graph density increased, meaning that the information transferred in the network increased. However, the node strength was decreased as a response of cyber-attacks. Signify the influence of this type of event on the strength of the information spillover between bitcoin cross market prices.

On the other hand, the rank of the most senders and receivers of the Effective Transfer Entropy pre and post the cybercrime reported in Table B 6 in the appendix. Where before the cybercrime BTC/BRL, BTC/ AUD and BTC/PLN was the top three receivers of information. However, after the breach event, the top bitcoin receivers of information become BTC/AUD, BTC/EUR and BTC/GBP, respectively. Strong evidence of the influence of cyber-attacks on the network, where pre the breach the BTC/EUR was the top sender of information in the network, however after the breach BTC/EUR become in the top list of receivers of information. In the same vine, the top senders of ETE also changed. Where the leading ETE sender pre the security breach was BTC/GBP and BTC/EUR, but after the breach occurred the results indicate that the top senders of information become BTC/USD,

BTC/KRW and BTC/CAD respectively. Interestingly, the Bitcoin pair that represents the location of the Bitcoin platform become more active in the network. Where in the case of Cryptsy platform, the pair BTC/USD convert from receiving information to become the top sender of the information in the network after the breach.

Effective Transfer Entropy analysis was used to measure the impact of the security breach that targeted the Bitfinex exchange in 2016. Figure B 3 in the appendix compares the impact of cyber-attacks. To distinguish between these two networks, Table B 7 in the appendix differentiate the critical factor of topological features outcomes obtained from analysis pre and post the cyber-attacks. Obviously, from this table, the number of edges and the Graph density marked increase, showing that the transfer of information in the network raised and the network become more connected. However, the node strength in the network was decreased as a response of cyber-attacks. Denote the influence of this type of event on the amount of information spillover between bitcoin cross market prices. The rank of the most senders and receivers of the Effective Transfer Entropy pre and post the cybercrime reported in Table B 8 in the appendix. Where before the cybercrime BTC/GBP, BTC/ BRL and BTC/PLN was the top three receivers of information. However, after the breach event, the top bitcoin receivers of information become BTC/BRL, BTC/AUD and BTC/PLN, respectively. In the same vine, the top senders of ETE also changed. Where the key players of sending ETE pre the security breach was BTC/CNY and BTC/EUR, but after the breach occurred the results indicate that the top senders of information become BTC/JPY, BTC/EUR and BTC/ KRW respectively. Therefore, this is strong evidence of the influence of cyber-attacks on the network, where pre the breach the BTC/CNY was the top sender of information in the network, however, after the breach, BTC/JPY become in the top list of the sender of information.

The impact of the security breach that targeted the Yapizon platform in 2017 is depicted in Figure B 4 in the appendix. To compare between these two networks, Table B 9 in the appendix summarised the results of topological features obtained from ETE analysis. Obviously from this table, the number of edges and the density of the graph marked raised, referring to the bitcoin cross market prices network become more connected, also the transmission of information in the network raised. However, the node strength in the network was slight decrease as a response of cyber-attacks. Denote the influence of this type of event on the Effective Transfer Entropy between bitcoin cross market prices. The rank of the most senders and receivers of the Effective Transfer Entropy pre and post the cybercrime reported in Table B 10 in the appendix. The results show that pre the cybercrime BTC/BRL, BTC/ JPY and BTC/PLN was the top three receivers of information. But after the breach event targeted the South Korea platform, the top bitcoin receivers of information become

BTC/PLN, BTC/EUR and BTC/GBP respectively. In the same vine, the top senders of ETE also changed. Where the key players of the top node that transfer ETE pre the security breach was BTC/USD and BTC/GBP, on the other hand after the breach occurred the results reveal that the main senders of information become BTC/JPY, BTC/KRW and BTC/ CNY respectively. Interestingly, the Bitcoin pair that represents the location of the Bitcoin platform BTC/KRW become more active in the network.

Under the same rationale as before, the study employs the ETE asset graphs to examine the rest of the events included in the study. Where the comparison between the bitcoin cross market prices networks pre and post each attack is depicted in Figure B 5 in the appendix for the cybercrime that targeted Zaif platform. The most striking result to emerge from the data is that the results signify that the security breach always has the same influences on the topological features of the network and the strength of the information spillover between bitcoin prices. Table B 11 in the appendix, show the results of the changes occur in the topological features for Zaif and LocalBitcoins respectively. This result shows that every time that bitcoin platform experience security breach, the network becomes more connected compared with network pre the attacks. The number of edges and the graph density increased. Further analysis showed that the security breach changes the main senders and receivers in the bitcoin prices network. Table B 12 in the appendix presents the impact of cybercrime on the top node strengths. The most surprising findings that the Bitcoin pair that represents the location of the Bitcoin platform become more active in the network. Where in the case of the Japanese Bitcoin exchange Zaif, BTC/JPY become in the top list of the sender of information.

Meanwhile, in case of the LocalBitcoins exchange located in Finland, the BTC/EUR played a crucial role after the cyber-attacks. Figure B 6 in the appendix compares the impact of cyber-attacks. To distinguish between these two networks, Table B 13 in the appendix differentiate the critical factor of topological features outcomes obtained from analysis pre and post the cyber-attacks. Obviously, from this table, the number of edges and the Graph density marked increase, showing that the transfer of information in the network raised and the network become more connected. However, the node strength in the network was decreased as a response of cyber-attacks. Denote the influence of this type of event on the amount of information spillover between bitcoin cross market prices. The rank of the most senders and receivers of the Effective Transfer Entropy pre and post the cybercrime reported in Table B 14 in the appendix. Where before the cybercrime BTC/BRL, BTC/ PLN and BTC/KRW was the top three receivers of information. However, after the breach event, the top bitcoin receivers of information become BTC/GBP, BTC/BRL and BTC/CAD, respectively. In the same

vine, the top senders of ETE also changed. Where the key players of sending ETE pre the security breach was BTC/GBP and BTC/BRL, but after the breach occurred the results indicate that the top senders of information become BTC/KRW, BTC/EUR and BTC/ AUD respectively. Therefore, this is strong evidence of the influence of cyber-attacks on the network.

The network of information flow for the bitcoin prices pre and post for the well-known Bitcoin platform Binance can be compared in Figure B 7 in the appendix. It can be seen that the network become more connected, which refer to the increase of information transferred between bitcoin cross prices after the security breach Table B 15 in the appendix compares the key factor of topological features results obtained from ETE. It is apparent from this table that the number of edges and the Graph density increased, meaning that the information transferred in the network increased. However, the node strength was decreased as a response of cyber-attacks. Signify the influence of this type of event on the strength of the information spillover between bitcoin cross market prices.

On the other hand, the rank of the most senders and receivers of the Effective Transfer Entropy pre and post the cybercrime reported in Table B 16 in the appendix. Where before the cybercrime BTC/GBP, BTC/ CAD and BTC/KRW was the top three receivers of information. However, after the breach event, the top bitcoin receivers of information become BTC/KRW, BTC/ GBP and BTC/JPY, respectively. In the same vine, the top senders of ETE also changed. Where the leading ETE sender pre the security breach was BTC/AUD and BTC/KRW, but after the breach occurred the results indicate that the top senders of information become BTC/USD, BTC/ CAD and BTC/JPY respectively.

Table B 25 in the appendix, show the IN- closeness node of the ETE to cross-market Bitcoin prices in time. Which can gives some information on the numbers of steps to cyberattack risk infect all the nodes in the Bitcoin cross market prices. Overall, there was no fix pattern after the cyberattack event where in case of Bitstamp, Yapizon and Zaif platform the number of steps to send the risk of breach events increased, where the total steps in case of Bitstamp raise from 33 to 66, Yapizon from 37 to 63. Lastly, after the security breach targeted Zaif platform the distance of spread the risk of cyberattack increased 45 to 50. On the other hands, after the cybercrime targeted Cryptsy, Bitfinex, LocalBitcoins and Binance. The number of edges needed to spread the infection dropped to more than half in case of LocalBitcoins and Binance. On the same vein, the average in- Closeness centrality indicates to the average numbers of connections that each node need it to spread or broadcast the information transmitted among the nodes in the network.

Closeness centrality computes the time that is needed to disseminate some information from a particular Bitcoin pairs to other cross-market Bitcoin prices in the network. Table B26 to Table 32 in the appendix, present in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks. Knowing that closeness centrality did not only considered the direct edges or connections but also compute the indirect relation between Bitcoin pairs node. The difference between in and out closeness is the direction of the edges. Thus in the out- closeness considered only the edges that indicate from targeted node to its relation with other node in the network. it can be seen from the tables the changes occurred pre and post the breach events.

Overall, two main findings signify the impact of breach events on the Bitcoin prices network. First, the network becomes more active after the cyberattacks but with less information exchanged among the Bitcoin pairs. Second, the pattern that appears signifies that the Bitcoin pairs that represent the location of the Bitcoin platform that suffered a security breach become the main source of information in the network; therefore, the finding indicates the contagion risk of security breaches in the Bitcoin markets.

3.4.1.1.1 Robustness Test

Transfer Entropy usually suffers from the noise contained in the TE matrices due to non-stationarity variables. However, these effects can be reduced if the model proposed by (Sensoy et al., 2014) is adopted. Effective Transfer Entropy (ETE) can be seen as a more efficient and consistent estimation method of Transfer Entropy (TE) that provides robust results. To eliminate any causality among variables, this method randomly shuffles each time series individually to subtract the effects of noise. Figure B 14 and Figure B 15 in the appendix represent the heat map of Transfer Entropy matrix and Effective Transfer Entropy matrix respectively. while the values of the TE was much higher than the value of ETE, where the range values of TE was from 0 to 0.108, meanwhile the range of ETE was from 0 to 0.07. Notably, the results of Effective Transfer Entropy smaller than TE by 0.0379 which is represent the Randomised Transfer Entropy. And by calculating ETE we subtracting the random values which is depicted in Figure B 15.

3.4.1.2 Dynamic analysis

In this section, the study analyses the dynamic dimension of causality relations among the examined Bitcoin cross-market prices, which helps to follow the adjustment of ETE. To achieve this, the study employed non-overlapping windows, each comprising data of one month, with 120 observations for each window span. The reason for this was to avoid the statistical problems caused by small sample sizes and to reduce the possibility of a particular event occurring during the examined period, which might influence the analysis. The dynamic network structure in this section was computed on the basis of significant ETE for non-overlapping windows and to rolling window approach.

Figure B 8 and **Figure B 9** in the appendix represent the Out-Node strengths and IN-Node strengths of ETE between Bitcoin cross-market prices respectively. Indeed, each line graph represents a breach event included in this chapter, and each line reflects the flow of information for each Bitcoin pair. Periods 1 to 3 represent the episodes pre the security breach, while periods 4 to 6 show the exchange of information among Bitcoin cross-market prices as a reaction to the cybercrime. Thus, Period 4 represents one month after the cyberattack hit the Bitcoin platform. In general, the trends of Out-Node strengths and IN-Node strengths usually rise and fall together. Therefore, Bitcoin pairs behave similarly as a block in most cases. However, the interesting result was in Period 4, where the Bitcoin market received the news or the announcement of cyber-attack, thus, there was a sharp increase in the exchange of information in the Bitcoin prices network during the cybercrime period.

Moreover, although there was a strong peak in the exchange of information during the breach period, there was a dramatic drop in Out-Node strengths and IN-Node strengths after one month following the event. This can be seen in all events included in the study. Throughout Period 5, the exchange of information was at the lowest level for all Bitcoin cross market prices, and there was a little spillover of information between Bitcoin cross-market prices after the breach events.

Table B 17 in the appendix compares the main factors of topological features obtained from ETE analysis in time. It can be seen from the results that all topological features rose during the cybercrime time (period 4). The rapid increases indicate that the networks became more connected and the flow of information also increased during the attack period. However, after one month following the cybercrime, all topological features dropped dramatically. Where in case of Bitstamp platform the spillover information increased after the breach event to 0.24, but the information transition decreased to 0.05. The strong degree before the cyberattack targeted Cryptsy platform was 0.13 but after the breach event the strong degree rise to 0.31 and later dropped to 0.07. the information flow during the security breach event increased to 0.27, however after only one month of the attack the information flow declined to 0.048. On the other hand, in case of Yapizon, Zaif, LocalBitcoins and Binance the strong degree during the cybercrime steep rise by 0.37, 0.22, 0.13 and 0.06 respectively. Although there is a clear peak but after one month of the announcement of the breach event the information spillover dropped to 0.13, 0.06, 0.01 and 0 correspondingly. Under the same rationale as before the rest of topological features show the same response pattern after all the cyberattacks.

Moreover, **Table B 18** to **Table B 24** in the appendix show a statistic of ETE that captures evolutionary pattern of network following various magnitudes of cyberattacks. The most surprising finding is that the Bitcoin pair that represented the location of the Bitcoin platform became more active in the network. In the case of the Cryptsy platform, the pair BTC/USD transformed from being receivers of information pre the breach event, to become the top source of information in the network after the breach. Where pre the breach event the average ETE for BTC/USD was around 0.10, but after the security breach the average ETE for the pair BTC/USD become 0.31. In the same vein, after the security breach targeted the Yapizon platform, the BTC/KRW became more active in the network with average ETE post the cyber attack 0.32 . Conversely, the Japanese Bitcoin exchange Zaif that suffered from cyberattack BTC/JPY became the main transmitter of information in the network with average ETE about 0.25 . While, in the case of the LocalBitcoins exchange located in Finland, the BTC/EUR played a crucial role after the cyberattacks. Thus, the results signifies that the

Bitcoin pairs that represent the location of the Bitcoin platform that suffered a security breach become the main source of information in the network; therefore, the finding indicates the contagion risk of security breaches in the Bitcoin markets.

According to recent research, while studying financial time series, some structural breaks should be taken into account. However, a few sub-samples or non-overlapping periods may insufficient to highlight the dynamic interaction (Sensoy and Tabak, 2016). Therefore, we adopt a rolling window approach to do a robustness check for the previous dynamic analysis to obtain more reliable findings of the dynamic causality relations among the examined Bitcoin cross-market prices. We choose six months (720 observations) time window and a 7-day shift (28 observations), with 120 observations for every window span. Since it is long enough to avoid the statistical problems caused by small sample sizes. Also, to reduce the possibility of a particular event occurring during the examined period. Jiang et al. (2018) estimate data obtained to Bitcoin market and show that rolling window method can serve to obtain more robust results and reduce the random errors.

In **Figure B 8** and **Figure B 9** in the appendix represent the rolling window estimation of IN-Node strengths and OUT-Node strengths between Bitcoin cross-market prices respectively. We plot the separate node IN and Out strengths for each of the cyber attacks included in this chapter. Notably, the IN and Out strengths only rise sharply during the period that Bitcoin platform influenced by breach event. although there is a clear peak in IN and Out strengths but there is a sharp drop of flow of information among Bitcoin prices, in another words, Both In and Out strengths of ETE rose during the cyber attack event before rapidly dropping afterward. Which indicates that that there was fast rise and fast drop of spillover of information transmitted among Bitcoin cross market returns during the breach events. the uniform behavior for IN and Out strengths of Bitcoin cross market prices usually rise and fall together, probably because they behave like a block during severe episodes. Lastly, the results from the rolling window method of the ETE are in full accordance with the aforementioned findings of non-overlapping estimations.

The Bitcoin platform has valuable databases and assets in the form of cryptocurrencies that could be hacked. Initially, the Bitcoin platform invests in security management to mitigate the risk of security breach. The probability of a successful cybercrime depend on the level of the Bitcoin platform investment in security management. However, maintaining a lower likelihood of getting security breach is more expensive. As a result, removing the threat of being hacked is surprisingly difficult. Therefore, the impact of cybercrime can take several form. Where some of security breach goal is to steal money (Gandal et al., 2018), steal sensitive information or to block the services provided by

cryptocurrencies platforms which may influence the Bitcoin platform reputation (Kamiya et al., 2021).The aim of the current chapter was to examine the influence of cyberattacks that targeted Bitcoin platform and generate money loss. From the Table **B 17** in the appendix we can compare and rank the significance of cyberattacks depending on the change that occurred to the amount of information pre and post each breach events. Overall the amount of strong degree decreased on average after the cybercrimes. Where the average of ETE decreased by 12%, 4%, 42%, 28% and 82% for Bitstamp, Cryptsy, Bitfinex, Zaif and Binance respectively. Under the same rationale as before, the amount of strong degree increased on average after cyberattacks on Yapizon and LocalBitcoins by 32% and 20% respectively. The non-uniform behaviour of the market reaction to the breach event probably because of the size of the money theft, Table 2 show that breach event that targeted Yapizon and LocalBitcoins platform generated less stolen money compared with other cyberattacks. Therefore, we can rank the significance of cyberattacks depends on the size of the security breach.

To sum up, the dynamic analysis indicates that during the breach period Bitcoin prices began to interact with this type of event. It also signifies the spread of the impact of security breaches among Bitcoin prices as the average degree increased. In addition, the evidence that emerged from the findings especially after the significant decrease in the exchange of information one month after the breach event indicates the contagion risk and the spread of the impact of cyber-attacks among Bitcoin markets.

3.5 Conclusions

The purpose of the current chapter was to determine the impact of a security breach on the causal relationships between Bitcoin cross-market prices, by adopting the complex network theory and analysing the data based on Effective Transfer Entropy (ETE). Overall, the current study found that the results indicate several crucial patterns that occur after the Bitcoin platform suffers a security breach. First, after a cybercrime, the topological features of the Bitcoin prices network increased and the network became more connected, whereby the number of edges, the graph density and the average node degree increased after all the breach events included in this chapter. However, the transfer of information between Bitcoin prices decreased. Second, the amount of exchanged information or the magnitude of interdependence among Bitcoin markets reduced after the cyber-attack. Third, the most interesting pattern was that the Bitcoin pair that represents the location of the Bitcoin platform became more active in the network. Therefore, the security breach can generate contagion risk as the findings suggest that the Bitcoin pair that represents the location of

the breach event becomes the main source of information in the network. However, this finding might support the formation of an adaptive prediction of Bitcoin prices.

Further analysis showed that the size of cyberattack did not play a crucial role in changing the response pattern in the spillover of the information network. Where such a breach generated a high amount of loss, for instance, the Bitfinex event, it had the same results as cyberattacks that did not generate a significant amount of loss, such as the LocalBitcoins event. The dynamic analysis was implemented to trace the impact of cyberattacks on Bitcoin cross-market price networks over time. The dynamic analysis has shown that during the security breach period all topological features rise quickly after a Bitcoin network suffers from a cyberattack. Meanwhile, one month after the breach, all network topological features drop quickly. As this pattern was repeated post all events included in the chapter. Therefore, it can be concluded that the changes in the network were caused by the influence of cyberattacks that may compromise the Bitcoin markets network to the contagion risk of spreading the impact of breach events in all Bitcoin cross-market prices. Indeed, these results match earlier studies; for Corbet et al. (2019a) traced 17 hacking events that targeted the eight most liquid cryptocurrencies within less than a year. They pointed out that volatility increased after each security breach and provided evidence that, in the hours prior to a hacking event, there were abnormal returns; however, the abnormal returns dropped to zero when the hacking event was revealed publicly. The present chapter makes several contributions to the literature and adds to the growing body of works about the way this type of cybercrime influences the Bitcoin exchange prices. It also enhances our understanding of the ability of criminals to generate contagion risk in the Bitcoin markets. Therefore, the finding raises the importance of improving security measures and techniques to reduce the frequency of hacking events, and to maintain efficient policies and protocols that can avoid the spread of security breach influences. The present study findings suggest to portfolio managers and investors the need to understand that, if a security breach targeted another Bitcoin platform located in a different country that they do not have investments in, they should not feel that their investment is safe, because the impact of cyberattacks still exists and because the contagion risk of a security breach that may expose their investment to the risk remains. Therefore, they need to consider several procedures to construct the best investment strategy. Also, security managers of cryptocurrency platforms need to enhance their security measures to reduce the risk of similar future cybercrime. In the same vein, Bitcoin exchange managers need to be aware of the impact of security breaches, which may result in the loss of traders' confidence in the platform and lead traders to place their trust in other competitors, which can mean the platform faces significant reputational and financial risks.

Several limitations need to be acknowledged. The author planned to use weekly moving widows in the dynamic analysis. However, the data frequency affected the selection of the sample size. The study could not employ less than 6 hours, such as 1, 5, 10, 15, 30 and 60 minutes, because of the missing data due to low liquidity in the Bitcoin markets in some periods, particularly during 2015. Moreover, the current chapter has only examined the impact of hacking events that targeted cryptocurrency exchanges and generated substantial monetary losses. Therefore, it would be interesting to examine the influences of a security breach that targeted other cryptocurrencies. Moreover, future research could assess the effect of different types of a security breach, which not only generate monetary losses.

Chapter 4

Revisiting the Risks of Various Types of Cyberattack on Bitcoin Markets

4.1 Introduction

Blockchain can be considered as the heart of Bitcoin, thus, this innovative technology makes Bitcoin relatively safer (Chuen, 2015). However, Bitcoin is still susceptible to the impact of cyberattacks where the risk of cyberattacks does not come from breaching the Bitcoin algorithm itself; instead, the cybercriminals can use malicious methods to harm the holders of Bitcoin such as Account Hijacking, 51% attack, site defacing, SIM Hijacking, and many other methods (Conti et al., 2018). A security breach can generate several forms of damage. Some of the cyberattacks result in money loss (Gandal et al., 2018). Another type of breach event can create unauthorised access to a customer's personal data, or a security breach can influence the web page of a platform to become inaccessible for the traders (Feder et al., 2017).

It can be very complicated to examine the influence of cyberattacks = very (Sigurdsson et al., 2018). The cost of a security breach does not stop only in the amount of money that the platform lost from the attack, but exceeds that to include the costs related to identifying and fixing problems caused by the security breach. Another cost is the possibility that the cryptocurrency platform can face legal liability. The negative effect of the announcement of cybercrime can be destructive to the platform's reputation and investor trust which may lead to a loss in current and future traders. Therefore, some cryptocurrency platforms did not report the hack event at the time of the breach; for instance, in the case of the Cryptsy platform that was subjected to a security breach in 2014, but the exchange management did not inform the investors of the incident until 2016 (Higgins, 2016). The current chapter aims to classify cyber security attacks into three main categories to understand how the nature of cybercrimes can influence Bitcoin cross-market price network and to identify the market reaction by tracing and comparing the spillover effect (contagion) after the network experienced each type of attack. Also, the study aims to trace the changes in the top transmitter and receivers of information between Bitcoin/currency pairs pre and post each event.

The present chapter contributes to the current literature that studies the effects of cybercrimes on the Bitcoin markets in several ways. Initially, it sheds new light on the influence of the different type of cyberattacks and conducts a comparison of the changes that may occur in the information transmission among Bitcoin cross-market prices. Furthermore, it provides evidence that each type of cyberattack has a unique impact on the Bitcoin network. In addition, the finding in this chapter may enhance our knowledge to differentiate between cyberattacks, as much uncertainty still exists where, to the best of the author's knowledge, no previous studies have attempted to differentiate between the impact of cyberattacks in terms of it unique influences in the Bitcoin prices network.

Several studies attempted to investigate the linkages between cryptocurrencies, and the changes that may occur over time (Boako et al., 2019, Ji et al., 2019a, Antonakakis et al., 2019, Katsiampa, 2019, Koutmos, 2018). Meanwhile, the influence of security breach on cryptocurrencies markets was also examined by several studies (Shanaev et al., 2019, Gandal et al., 2018, Caporale et al., 2020, Xia et al., 2020). The summary of the relevant literature that collaborate to examine the main classifications of security breach that targeted the Bitcoin market shown in table 1-3 in the appendix . Until recently, little discussion has focused on the impact of cyberattacks on the linkages between Bitcoin and other cryptocurrencies (Caporale et al., 2021). However, the effect of cybercriminals on the linkages among Bitcoin cross-market prices requires further attention. Also, much uncertainty still exists about how different types of security breaches can influence the information spillover among Bitcoin cross-market prices differently.

The rest of this chapter is structured as follows. Section 2 presents the literature related to the study. Section 3 describes the data and the methodology and addresses the network analysis and Effective Transfer Entropy (ETE). Section 4 presents the empirical results. Section 5 concludes the chapter.

4.2 Related Work

A large and growing body of literature pays particular attention to the impact of cybercrime on the cryptocurrencies market. The current literature that studied the influence of security breach can be divided into two main categories. The first group examined the impact of the security breach as a general concept without determining a specific method of cybercrime. Some of the literature examined the impact of security breaches that influence the Bitcoin platforms. Moore and Christin (2013) examined the impact of cybercrimes that targeted cryptocurrencies platforms and concluded that there was an inverse relationship between platform closures that suffered from breach events and the transaction volume. This argument was supported by (Moore, 2018) after he tracked the impact of cyberattacks on Bitcoin platforms, and pointed out that after the platform faced the risk of breach events the possibility of shutdown increased. However, a recent study by Oosthoek and Doerr (2020) posited that exchange closures as a result of hacking events show a declining trend.

By drawing on the general concept of cyberattacks and without determining which type of cyberattack was included in the study Corbet et al. (2019) traced 17 hacking events that targeted the eight most liquid cryptocurrencies within less than a year. They found that volatility increased after each security breach. Also, the study provided evidence that hours before a hacking event there were abnormal returns. However, the abnormal returns drop to zero when the hack event is revealed publicly. The study was limited, though, as the authors considered a short period of time within less than a year. On the other hand, after including a more extended period throughout August 2015 – February 2019, Caporale et al. (2020) argued that the probability of cryptocurrencies influenced negatively by cyber-attacks and remained within low volatility.

The second group of studies examined the impact of cybercrimes. Those studies pay particular attention to the impact of a certain type of security breach that targeted the cryptocurrencies market. These included double spending attacks (Ruffing et al., 2015, Hassan et al., 2020, Pinzón and Rocha, 2016), 51% attacks on Bitcoin (Shanaev et al., 2019), pump and dump schemes(Hamrick et al., 2018), DDoS attacks (Abhishta et al., 2019, Feder et al., 2017), Bitcoin hijacking (Apostolaki et al., 2017) and spam transactions in Bitcoin (McGinn et al., 2016).

Collectively, although these groups of studies examined the influence of security breaches on the cryptocurrencies market from different perspectives. However, many of the studies have a limitation to differentiate between several forms of security breaches that may influence the market differently. In contrast, other researchers have been able to specify the analysis depending on a

certain method of cyberattacks. Therefore, the present study attempted to distinguish between the impacts of several forms of security breaches and shed light on the market reaction after experiencing each kind of security breach.

4.2.1 Determinants of cyberattacks

It is crucial to understand the incentives behind security breaches where the damage generated from security breaches vary depending on the attacker's aims. In some cases, the cybercriminals found a security defect in the cryptocurrencies platform system and took the opportunity to steal money from the market or trader's accounts; for example, the security breach that incurred Mt.Gox significant losses of around US$470 million in 2014 (Gandal et al., 2018). On the other hand, some of the security breaches aimed to obtain non-economic gains, by gaining unauthorised access to stored data, aiming to steal sensitive information that can be used in future cybercrime. Moreover, several cybercrimes intended to block the services provided by cryptocurrencies platforms (Abhishta et al., 2019). Thus, this paper introduces three main classifications for the security breach that targeted the Bitcoin platforms depending on the threat posed. Further, it examines whether there were any influences on the interdependency between Bitcoin cross-market prices and compares the impact for the three main categories.

4.2.1.1 Confidentiality.

In this category, the study includes any security breaches that cause unauthorised access and create a leak of personal information for traders. In any cash system trust is an important element and plays a critical role (Khairuddin, 2019). However, the trust in the traditional finance system has been tested as a result of incidents causing challenges in accountability and integrity; for instance, the financial crisis in 2008 and the collapse of Lehman Brothers (Marella et al., 2020). Therefore, as the concept of trust evolves (Luna-Reyes et al., 2004), these incidents opened up the opportunity to suggest a new cash system (peer-to-peer) without intervention from a third party (Nakamoto, 2008b). However, trust in the electronic cash system such as Bitcoin and other cryptocurrencies faced major challenges; for example, cyberattacks that break the confidentiality may reduce the level of trust in the Bitcoin traders (Sas and Khairuddin, 2015, Xia et al., 2020). There is limited knowledge among the cryptocurrencies traders about how the new electronic cash system such as Bitcoins works, and the need to protect their investment from any risk. Therefore, building confidence in Bitcoin users was the responsible of the cryptocurrencies market by providing a set of procedures that ensure the investments' protection for Bitcoin users (Marella et al., 2020).

To use the services that are provided from any Bitcoin platform the customers need to follow several procedures to verify their identity. The process is known as “Know-Your-Customer” (KYC) where, in general, the cryptocurrencies market requires personal information such as name, date of birth, email, physical address and a scanned copy of the customer’s ID document. However, on several occasions, the databases that include the personal information of the Bitcoin customers were targeted from a security breach.

Group	**Types of security breaches**	**Authors**
Theft	dropping transactions	Sigurdsson et al., (2018)
	51% attacks	Shanaev et al., (2019)
	double-spending attacks	Hassan et al., (2020)
	malleability attacks	Pinzón and Rocha, (2016)
	DNS hijacking	Dai et al., (2017)
	account hijacking	Mirian et al.,(2019)
	SIM swapping	Sigurdsson et al., (2018)
	price manipulation	Gandal et al.,(2018)
	mining botnets	Huang et al., (2014)
	prices manipulated	Griffin and Shams (2018)
Confidentiality	Fake app	Xia et al., (2020)
	Site defacing	Weimann (2016)
	phishing scams	Chen et al., (2020)
Availability	DDoS	Vasek et al. (2014)
	DDoS	Johnson et al., (2014)
	DDoS	Feder et al. (2017)
	DDoS	Abhishta et al. (2019)
	DDoS	Feder et al. (2018a)

Note: Categorize the literature into three different classes, each category represent the works that examined the impact of cyber attacks on Bitcoin markets

Table C. 1 in the appendix shows an example of five breach events that caused the leak of the personal data of thousands of customers.

Cybercriminals follow several methods to steal private data. Vulnerability in the platform security system can be an invitation to the attackers to steal all the data that they can get. For example, the Ledger platform experienced a cyberattack that compromised the personal details of one million clients (Ledger, 2020). Site defacing, fake app (Xia et al., 2020) or phishing scams (Chen et al., 2020) are other techniques that the attackers use to deception the users of cryptocurrencies. In this scam, the attacker created a fake website by using the Google AdWords service. The reason behind that was to make their fake website show at the top of Google search results, as shown in Figure C. 2 in the appendix. This scam targeted Bittrex platform users (hackread.com, 2017). The fake address directed the users to a phishing website that looked identical to the original site as shown in **Figure C. 3** in the appendix. The cybercriminal then not only could steal credentials data, but could also take all the cryptocurrencies in the victim's account (Weimann, 2016).

4.2.1.2 Availability.

The availability category includes any cyberattacks that prevent traders from using the website services in the targeted platform. This kind of cyber criminality do not create a leak of private data or money loss; however, it does harm the platform which incurs costs after dealing with a cyberattack where the platform needs labour and time to repair the system damaged. Moreover, if the cryptocurrencies platform experienced cyberattacks that influence the availability, where the website of the platform will be unreachable for brokers and investors for hours, this might sustain loss for them, as they missed any opportunity to make a profit during the unavailability hours. In addition, this type of attack may harm the reputation of the exchange, the result being that the cryptocurrencies platforms may suffer from losing the opportunity to expand their client's base in the future (Feder et al., 2017).

A distributed denial-of-service (DDoS) attacks one of the common examples of cyberattacks that influence the availability of cryptocurrencies platforms. In denial-of-service (DoS), as shown in Figure C. 1 in the appendix, the attacker tries to send a significant amount of requests to flood the victim's machine or network and prevent all services on the website from being fulfilled (Eliyan and Di Pietro, 2021). However, this kind of attack can be solved by blocking the source of this attack. On the other hand, a distributed denial-of-service (DDoS) attack is a step further from DoS attacks. In this case,

the criminal first recruits thousands of computers around the world by infecting them with malware, as shown in Figure C. 1 in **Supplement to Chapter 4**

the appendix. The attacker uses those infected devices to create thousands of requests to overload the platform servers and prevent any user from accessing the services in the targeted website (Hoque et al., 2017). However, as the attacker uses more than one source of the attack, unlike the case with the DoS attack that only uses one source, it takes several hours to solve the problem. The DDoS attack can shut down all website services, degrade the website performance, or influence part of the platform services' availability. These methods do not stop all trading activities on the website but force the platform to temporarily disable some of its services. For example, in 2018 the well-known cryptocurrency platform Binance announced that new registration services temporarily closed as a response to 240,000 fake new account registrations within only one hour (Binance, 2018).

Previous studies have examined the impact of distributed denial-of-service (DDoS) attacks on Bitcoin. Vasek et al. (2014) examined 40 DDoS attacks events between 2011 and 2013. And they argue that DDoS attacks targeted big mining pool much more than smaller ones. And mining pools were much attractive to DDoS attacks compared with platform services. This point of view was supported by (Johnson et al., 2014). In the same vein, Feder et al. (2017) traced the impact of DDoS attacks on Mt.Gox exchange, one of the biggest Bitcoin platforms during the study sample and reported that, during the days of the attacks, there was a shift in transaction volume. However, the study was limited as they employed a model that suffers from endogeneity issues to estimate the impact. Recently, Abhishta et al. (2019) questioned whether DDoS attacks can influence the cryptocurrency platform and pointed out that, after including 17 DDoS events that targeted the Bitfinex platform, on 13 occasions the market recovered within a short period. However, in other events, the market needed more than one day to recover the losses. Therefore, they provided evidence of the negative impact of DDoS on the platform and stated that the impact depends on the size of the attack and how long the DDoS lasts until the market is able to provide the normal services before the breach event took place.

4.2.1.3 Theft.

The theft category consists of any cyberattacks that targeted cryptocurrencies platform to steal Bitcoin and incur losses. In 2019 there was approximately more than $4 billion of theft in the cryptocurrencies market, compared to $1.7 and $1.2 billion of crypto crimes in 2018 and 2017, respectively (Forbes, 2019). The most destructive cybercrime was in the well-known Japanese Bitcoin exchange, Mt.Gox, with 470 million dollars being stolen (Bloomberg, 2014). In general, users, platforms or wallets, merchants, and Bitcoin miners are the main four interested parties of Bitcoin (Shcherbak, 2014). However, each Bitcoin stakeholder was exposed to certain kinds of risk that arise from cyberattacks. For instance, Bitcoin miners are exposed to several types of security breaches, such as dropping transactions (Sigurdsson et al., 2018) and 51% attacks (Shanaev et al., 2019). On the other hand, merchants that accept Bitcoin as a medium of exchange also suffer from double-spending attacks and malleability attacks (Hassan et al., 2020, Pinzón and Rocha, 2016). Meanwhile, Bitcoin users have to deal with several cybercrime techniques; for example, DNS hijacking (Dai et al., 2017), account hijacking (Mirian et al., 2019), SIM swapping and site defacing (Sigurdsson et al., 2018).

The Bitcoin market and wallets also face the same risk of security breach events. The security system vulnerability of Bitcoin platforms is one of the methods that malicious entities exploit when they plan to steal money from any platform (Conti et al., 2018) as well as Bitcoin market price manipulation (Gandal et al., 2018). Thus, there was a significant impact of security breaches that targeted the Bitcoin platform as the evidence presented in Chapter Two and Three shows. The Bitcoin cross-market price network depending on the correlation and Transfer Entropy was influenced from this type of events.

4.2.2 Spillover and contagion in Bitcoin Market.

The interconnection among cryptocurrencies and the linkages with other investment have become crucial topic for arbitrage, management of risk, portfolio management and hedging (Antonakakis et al., 2019). In particular, when investing in the cryptocurrencies market, customers need to be aware of the possibility that they may be vulnerable to the contagion risk. Recently, spillover in the cryptocurrencies market has been researched from different perspectives. The relation between spillover across the cryptocurrency and the changes of regulation were investigated by Borri and Shakhnov (2020), they pointed out that if the country adjusts the regulations related to the

investment in the cryptocurrencies market, that may influence on domestic and international cryptocurrency markets.

A number of authors examined the spillover among cryptocurrencies and commodities. Huynh et al. (2020) employed Transfer Entropy to examine the spillover between gold and 14 different types of cryptocurrencies. They argued that a portfolio consists of cryptocurrencies and gold can be considered as a good combination, where gold plays a significant role as a hedging tool in that portfolio. Similarly, Gkillas et al. (2020) identified the spillover effect after using high-frequency data between crude oil, gold, and Bitcoin. They described the robust association between gold and Bitcoin; likewise the relation between Bitcoin and crude oil. This point of view was supported by (Ji et al., 2019b), who addressed the weak linkage between energy commodities and the top five cryptocurrencies included in the study. On the other hand, by drawing on the concept of spillover effects between cross-market Bitcoin prices, Gillaizeau et al. (2019b) tracked the effects of volatility spillover among the top five cross-market Bitcoin prices. They provided some evidence that Bitcoin to EUR was playing a central part as it represents the net receiver of volatility and that, when the uncertainty in the cross-market price increased, this may possess more chance to the effect of volatility spillover in the market.

Several attempts have been made to investigate the spillover among cryptocurrencies. Koutmos (2018) analysed the data from 18 major cryptocurrencies and concluded that cryptocurrencies had become more interconnected, and that the risk of contagion become significantly possible. Also, they confirmed the central role of Bitcoin among the top 18 cryptocurrencies included in the study. Likewise, Qureshi et al. (2020) asserted that the dependency between cryptocurrencies has increased. Moreover, Katsiampa et al. (2019) analysed the direction of spillover volatility among Bitcoin, Ether and Litecoin and they found that Bitcoin transfers its shock effects to both cryptocurrencies. However, the study would have made more contributions to the field if the authors had considered more than three cryptocurrencies in the study. Meanwhile, the arguments that Bitcoin has a leading role in the cryptocurrencies market have been contested recently by several researchers. In their detailed analysis of the contagion and the connectedness across the top nine cryptocurrencies, Antonakakis et al. (2019) concluded that Ethereum transfers shock to Bitcoin and connectedness among cryptocurrencies increased over time. This argument was supported by a more recent study, where Lahiani and Jlassi (2021) were able to show the leading role of Ethereum in the cryptocurrencies market.

There has been little quantitative analysis of the impact of security breaches on the spillover effect in the cryptocurrencies market. Caporale et al. (2021) examined the daily data for Bitcoin, Ethereum and Litecoin to highlight the changes that may occur in the volatility spillover after the market experienced a security breach. In their comprehensive examination, they were able to show that cyberattacks increase the linkages among three major cryptocurrencies and they also addressed the leading role of Bitcoin compared with the rest of the cryptocurrencies included in the study. However, the study would have been more persuasive if the authors did not include all cyberattacks that occurred in all sectors, such as Government, Industry and Financial during 2015-2020 but instead focused on the cybercrime that targeted the cryptocurrencies market. Moreover, the study examined all security breach events that targeted the cryptocurrencies market, but the main weakness was including all breach events regardless of the nature of the cybercrime, where each type of cyberattack creates unique damage that might have a different kind of influence.

Although several studies have examined the impact of a security breach on cryptocurrencies, so far, however, there has been little discussion about the impact of cybercrime on the spillover in the cryptocurrencies market. The need to highlight the impact of different kinds of cyberattacks on the Bitcoin cross-market prices also needs more study.

4.3 Data and methodology

4.3.1 Data

4.3.1.1 Bitcoin cross-market price data

Several platforms provide the service to buy/sell Bitcoin at diverse exchange prices. In this chapter, all data of exchange rates against Bitcoin are obtained from Bitcoincharts website[3]. This chapter considers eight major Bitcoin/currency pairs, which may provide a robust view of the Bitcoin market performance; namely, the US dollar (USD), the South Korean Won(KRW), the Japanese yen (JPY), the Australian dollar (AUD), the British pound (GBP), the Euro (EUR), the Polish zlotys (PLN) and the Canadian dollar (CAD). The data covered the period between 1 January 2017 and 31 October 2020, which incorporates several security breach events, as shown from

Group	**Types of security breaches**	**Authors**
Theft	dropping transactions	Sigurdsson et al., (2018)
	51% attacks	Shanaev et al., (2019)
	double-spending attacks	Hassan et al., (2020)
	malleability attacks	Pinzón and Rocha, (2016)
	DNS hijacking	Dai et al., (2017)
	account hijacking	Mirian et al.,(2019)
	SIM swapping	Sigurdsson et al., (2018)
	price manipulation	Gandal et al.,(2018)
	mining botnets	Huang et al., (2014)
	prices manipulated	Griffin and Shams (2018)
Confidentiality	Fake app	Xia et al., (2020)
	Site defacing	Weimann (2016)
	phishing scams	Chen et al., (2020)
Availability	DDoS	Vasek et al. (2014)
	DDoS	Johnson et al., (2014)
	DDoS	Feder et al. (2017)
	DDoS	Abhishta et al. (2019)
	DDoS	Feder et al. (2018a)

Note: Categorize the literature into three different classes, each category represent the works that examined the impact of cyber attacks on Bitcoin markets

[3] www.Bitcoincharts.com

Table C. 1 to **Table C. 3**, in the appendix.

The platform that owns the most market trading activities and market share was the method to select the ideal platform. Therefore, to compare between several markets the Bitcoinity [4]website was accessed for further evaluation between Bitcoin platforms. In some cases, the cross-market Bitcoin price was obtained from different exchange platforms for each currency to construct continuous time series, as shown in **Table C. 4** in the appendix. Because some platforms such as the Canadian Bitcoin platform Quadrigacx, quit the market and stopped providing services during 2019, thus data were gathered from other exchange platforms.

Because one of the aims of this paper is to trace the influence of a different class of security breach on the Bitcoin cross-market price network, several security breaches are included in this chapter. However, recently, cyberattacks and hacking events have become more frequent (Caporale et al., 2021). Thus, to focus on the impact of breach events and to reduce any chance that the data may be influenced by other news or information arrival to the market, the author employed high-frequency data at the level of 15-min frequency. The intention behind using a 15-min frequency was for several reasons. First, choosing less than 15 min data may lead to an increase in the amount of missing data due to low liquidity in some markets. Second, as the aim was to examine the data within narrow window lengths for each event, thus, less frequent data such as daily or hourly data may expose the model to statistical issues due to the small sample size.

Table C. 5 in the appendix reports the descriptive statistics. Among the Bitcoin cross-market prices, the GBP (0.00254) shows the highest return followed by the USD (0.00253), while the EURO (0.00238) witnessed the lowest return compared with others Bitcoin returns. On the other hand the standard deviation is bouncing from KRW (0.08328) with the highest value, while PLN (0.06998) is the least. According to the Dickey-Fuller test, all Bitcoin exchange rates series are stationary. Moreover, the Jarque-Bera test indicates that all the series under examination in this study exhibit departure from normality.

4.3.1.2 Cyber-attack data

The damage caused by breach events differs based on the cybercriminal's intentions. Therefore, in this chapter cyberattacks were classified into three main categories in order to explore their different impacts, as shown in Tables C.1- C.3 in the appendix. The hack events were obtained from

[4]www. Bitcoinity.org

the Hackmageddon[5]website, a public source of any security breach that happened around the world. Security breach influences all Bitcoin traders, platforms or wallets, merchants, and Bitcoin miners (Shcherbak, 2014). Thus, only cyberattacks that targeted the Bitcoin platforms were included. Since the study aimed to classify the breach events, the author examined each events and gathered more specific information about them from several sources, such as blogs, status page or Twitter account for the platform that suffered from the breach, Google news search, and news sites.

Because of the uniqueness of each category of cyberattack, a specific type of evidence or information was needed. The specific information cannot only help with differentiating between the three main categories but also to compare between the breach events in the same category. The availability group include any cyberattacks that block customers from using the website services in the targeted platform; for example, a DDoS attack. The time of the breach and the damage caused to the trading platform was a piece of critical information for the availability category. On the other hand, the theft category consists of any cyberattacks that targeted cryptocurrencies platform to steal Bitcoin and incur losses. Thus, the numbers of Bitcoin missed, the time of the breach, and the amount of economic loss was essential information for this category. Finally, the confidentiality category consists of any cyberattacks that targeted the Bitcoin platform to gain unauthorized access to a database and generate leaks of personal information. The category also includes the number of traders who incurred damage from having their personal information exposed and the time of the announcement of the breach events.

[5] www.hackmageddon.com

4.3.2 Methodology

The study aims to estimate the influence of the different types of cyberattacks that take place and conduct a comparison for the changes that may occur in the information transmission among Bitcoin cross-market prices. Therefore, the data were divided into sections. Each section represents an event or security breach that targeted a Bitcoin platform. Then to trace the adjustment of spillover effects in the network, each breach event was divided into 14 days pre- and post-cyberattacks included in the study. The narrow window lengths have a number of attractive benefits. First, they focus more on the events and gain close insights into the impact of the incident. Second, hacking events become more frequent (Caporale et al., 2021); thus, increasing the window lengths may influence the results because an extended period can include more events within the same sample which may affect the analysis. Therefore, using narrow window lengths helps avoid the problem with the analysis. There were 2688 observations for each breach event. The Bitcoin return was calculated by logarithm return.

The aim of this chapter was to estimate the risk of cyberattacks on the interconnections of the Bitcoin prices network, we will divided the sample into two sub sample to compare the influence pre- and post each breach events. However, identifying the potential location of the break point in the sample is often unknown. Thus, a number of methods were used to detect the structural break. Such as The Chow Test (Chow, 1960), The CUSUM Test (Brown et al., 1975) and The Hansen and Nyblom Tests (Hansen, 1992). Depending on least squares principles Bai and Perron (2003) proposed a model to capture structural break by employing multiple linear regression with N breaks.

$$y_t = x_t'\beta + z_t'\delta_j + u_t \qquad (1)$$

$$t = T_{j-1} + 1, \dots, T \qquad (2)$$

where $j = 1, \dots, m+1$. The dependent variable y_t is to be modeled as a linear combination of regressors with both time-invariant coefficients x_t', and time variant coefficients z_t'. This model can be rewritten in formation of matrix as

$$Y = X\beta + Z\delta + U \qquad (3)$$

This approach requires a specific number of Maximum breaks be given. Thus, we select one break point for each sample and for the test specification we choose global information criteria as a test

method. Table C24 in the appendix, show the Bai & Perron results. Thus, depending on the break point date we divided the sample into pre and post sub sample to examine the significance of security breaches.

A number of methods were used to measure the interconnectedness in the cryptocurrencies markets. Koutmos (2018) used the VAR model to examine the volatility spillover in the cryptocurrencies market. On the other hand, volatility spillover among the cryptocurrencies market was studied by Omane-Adjepong and Alagidede (2019) and they employed the wavelet-based methods. Similarly, extreme price and extreme correlation approach were used to analyse the contagious risk in the cryptocurrencies market (Gkillas and Katsiampa, 2018, Gkillas and Longin, 2018). Corbet et al. (2019b) proposed using Granger causality to trace the relationship in the cryptocurrencies markets. However, each model has its advantages and drawbacks.

using a mean-variance decision-theoretic framework for Bitcoins, following the papers of (Mukherjee and Padhi, 2021); (Mukherjee et al., 2021); (Broll and Mukherjee, 2017); (Eichner and Wagener, 2012). Direct risk can be modelled in a similar way to (Bolt and van Oordt, 2019), by modelling the decision of the speculator between investing in a risk-free bond denominated in the established currency and speculation on Bitcoins. Under the assumption of absence of lending and borrowing in virtual currency, the return on a position in Bitcoins in terms of the established currency is determined only by the change in the (spot) exchange rate (in terms of Bitcoins defined in units of actual currency: GBP, USD etc.), S. Let us consider one period with two dates: t=0, t=1 (where t=1 is the steady state, where we have, two potential outcomes. Given technological uncertainties, potentially adverse regulatory policies, or successful introductions of other virtual currencies, two extreme events may occur at t=1. Either the cryptocurrency payment network will end up in its stationary equilibrium. This stationary equilibrium is such that the number of Bitcoin users (i.e., consumers and merchants) equal the equilibrium values obtained from two-sided market theory. It is assumed that the number of Bitcoin users remains in this equilibrium thereafter. Alternatively, the payment network will be abandoned, in which case, there will be no users at t=1 and thereafter. Let us, here consider the first possibility in this context of the decision problem). Hence, at t=1, the wealth of a speculator investing in z_0 units of virtual currency is,

$$W_1=R\ (W_{W0}-S_0z_0)+S_1z_0 \qquad (4)$$

Decision variable is z_0. where W_1 is wealth at time t, R denotes the gross return on bonds denominated in the traditional currency and where S_1 denotes the imperfectly predictable future

exchange rate. We assume that individual risk-averse speculators take the current exchange rate S_0 as given. In (4), cyber-attacks can be introduced as:

$W_1=(W_0-S_0z_0)+S_1\ (1-\tilde{e})z_0$ (5)

Where $\tilde{e}$ is the ex-post loss in the future spot rate of BTC owing to cyber-attacks. We assume $\tilde{e}$ is a mean-zero background risk. In this framework, we assume the speculator's preferences are given by a two-parameter utility function:

$U=(v_W,\mu_W)$ (5)

We are making the following assumption regarding the speculator's preference function. The marginal utility with respect to (w.r.t. hereafter) μ_W is positive while the marginal utility w.r.t. v_W as negative: i.e., $U(v_W,\mu_W)>0$, $Uv(v_W,\mu_W)< 0$. In other words, we are assuming that the preference satisfies non-satiation (increasing in μ_W) and the speculator is risk-averse (decreasing in v_W). The indifference curves are upward-sloped and strictly convex in (v_W,$_W$)-plane.

the selection of the method adopted in this chapter depended on the finding by Dimpfl and Peter (2019) where they highlighted the differences between using linear methods and nonlinear approaches to detect interconnectedness in the cryptocurrencies markets. They concluded that the nonlinear model avoids the limitations of linear methods, particularly in the case of dealing with cryptocurrencies data. Thus, the nonlinear model Transfer Entropy (ET) proposes better approaches to trace the impact of cyberattacks on the interconnectedness among Bitcoin cross-market price.

4.3.3 Transfer Entropy and Effective Transfer Entropy (ETE)

The term 'Entropy' was first recognised in the thermodynamics field (Dugdale, 2018). It was used to describe the dispersion of heat or the temperature in any system (Greven et al., 2014). In other words, Entropy was labelled as the amount of chaos in any system. Later, in his theory of information, Claude Elwood Shannon reflected the concept of Entropy in the Communication framework (Shannon, 1948) which is known as the Shannon Entropy. More recently the concept of Transfer Entropy was developed by Schreiber (2000). Notably, this non-parametric model can be considered as a measure of interdependency and can capture the flow of information in a dynamic system. More formally, suppose we have two discrete and stationary variables, X and Y and that, in the case of computing the next state of variable X, knowing that there was interaction among X and Y. Therefore, the next state of the variable X will depend on its previous state and the information transaction from a variable Y to a variable X, which can be considered as the average of information contained in the variable Y (source of information) about the next state of the destination X (receiver of information) that did not already exist in the previous state of X. The Transfer Entropy from Y to X is defined as follows:

$$TE_{Y\to X}(K,l) = \sum_{i_{n+1},i_n^{(k)},j_n^{(l)}} \left[P\left(i_{n+1}, i_n^{(k)}, j_n^{(l)}\right) log_2 \frac{p\left(i_{n+1}, \middle| i_n^{(k)}, j_n^{(l)}\right)}{P\left(i_{n+1}, \middle| i_n^{(k)}\right)} \right], \quad (6)$$

where i_n is the number of observations of X series, and j_n refers to the number of elements for variable Y; the element K donates to previous states of the variable X, and ℓ shows the prior states of the variable Y. $P\left(i_{n+1}, i_n^{(k)}, j_n^{(l)}\right)$ represents the joint probability between the previous states of the variables, and $P\left(i_{n+1}, \middle| i_n^{(k)}\right)$ denotes the conditional probability of the state of variable X on all its prior states. Meanwhile, $p\left(i_{n+1}, \middle| i_n^{(k)}, j_n^{(l)}\right)$ in this part of the equation shows the conditional probability, where, if variable X depends on another state of variable Y, we assume that the state of X depends on the previous states of the source Y. Also, we conjecture that $k = \ell = 1$ follows the previous literature from empirical research in financial markets (Bekiros et al., 2017) and other literature which analyses information interdependence in cryptocurrency markets (Ji et al., 2019b, Huynh et al., 2020).

Transfer Entropy usually suffers from the noise contained in the TE matrices due to non-stationarity variables. However, these effects can be reduced if the model proposed by (Sensoy et al., 2014) is adopted. Effective Transfer Entropy (ETE) can be seen as a more efficient and consistent estimation

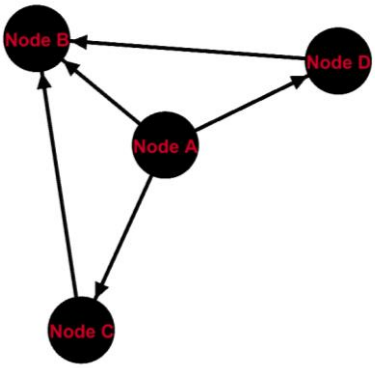
method of Transfer Entropy (TE) that provides robust results. To eliminate any causality among variables, this method randomly shuffles each time series individually to subtract the effects of noise. An Effective Transfer Entropy matrix (ETE) can be calculated as shown in equation (2), below, whereby the Randomized TE matrix is subtracted from the TE matrix as follows:

$$ETE_{Y\to X} = TE_{Y\to X} - RTE_{Y\to X} \quad (7),$$

where $RTE_{Y\to X}$ indicates the shuffled version of the TE which breaks the dependencies among X and Y. The "RTransferEntropy" package proposed by (Behrendt et al., 2019) was used to analyse the data. And we considered the Effective Transfer Entropy matrix since it provides more robust results compared with Transfer Entropy.

In this chapter, the aim is to explore both interdependences among Bitcoin prices and contagions in the form of the change in the Bitcoin network topological features pre- and post-cyberattacks. Network theory can provide a comprehensive tool to understand the contagion effects among Bitcoin cross-market prices resulting from the influences of security breaches. It can also provide an analytical method to view the complex relationship in the form of a graph. This helps to capture the changes in the interconnections among Bitcoin prices under examination to explain certain phenomena. Figure 1 illustrates an example of a directed network where the network consists of a number of nodes linked with edges. In this example as depicted in Figure 1, Node (A) has a significant role as a top sender to other nodes. Thus, Node (A) can be called a hub. However, in the case of Node (B) which can represents the top receiver in the network, as all the edges or links were pointing to Node (B), therefore it can be called authority. In the same vein, Node (A) has the top Out-Node Degree (ND_{out}), while Node B can be classified as the top IN-Node Degree (Nd_{in}) since all the links show only one direction toward Node (B). The graph density shows all possible links that can be in the network. The value of graph density ranges from zero which mean no links between all the nodes in the network. Meanwhile, when the network density is equal to one, that means that all possible links in the network exist. In Figure 1 the maximum number of the edges in the network equals 12. Therefore, graph density in the network depicted in Figure 1 equals 0.417 as several edges were missing.

Figure 3: Directional Network



4.4 Main Results

In this chapter, three main classifications were introduced for the security breach that targeted the Bitcoin platform depending on the threat posed as shown in Tables C1 to C3, in the appendix. Furthermore, the author examined whether there were any influences on the spillover among Bitcoin cross-market price and differentiated between the impacts of each main category.

The first set of analyses traces the influence of security breach depending on the availability category. Table C.2 in the appendix presents the DDoS attacks that targeted the Bitcoin platform Bitfinex on several occasions. Figures C.4 to C.8 in the appendix present the network transformation that occurs in the net receivers and senders after the market suffers from cyberattack. Table C.6 in the appendix compares the network topological features among the five events included in this study. It can be seen from Table C.6 that the spillover among the eight bitcoin prices was increased. On average, the number of edges after most breach events steady increased. Therefore, the findings indicate the network adjustment, where the Bitcoin market network becomes more connected and the transfer of information among Bitcoin prices increased. Also, the graph density increased after the Bitcoin market experienced the DDoS attacks on the Bitfinex platform. However, no significant network reaction was found in the case of a DDoS attack in February 2017 where all the network topological features remain at the same level pre and post the breach event.

The flow of information in the Bitcoin network was examined to observe the impact of DDoS attacks on the Bitcoin prices network. Interestingly, strong evidence was found to signify that DDoS attacks increase the dependency between Bitcoin prices. However, depending on the damage generated from DDoS attacks, the results show that the network reacts differently. On the other hand, in the case of DDoS attacks that create a reduction of the performance of the platform, there were no dramatic changes in the network – for instance, the DDoS attacks in February 2017 and June 2017. Meanwhile, the results show a significant change in the spillover among Bitcoin network prices in the case of the DDoS attack that forced the Bitcoin platform to stop the services temporarily where, on average, effective Transfer Entropy reveals that there has been a marked rise in the flow of information in the network. The interdependency between Bitcoin prices increased by 25%, 19% and 279% in the case of events that occurred in December 2017, May 2018, and February 2020, respectively. In contrast, Tables C.9 to C.13 in the appendix compared the top sender and receiver in the network. Although there was a change pre and post the breach events for the key sender and receiver, no significant pattern appears after the breach events in the top receivers and transmitters in the network.

The second set of analyses focuses on the effect of different types of vulnerabilities that caused the stealing of money. Table C.3 in the appendix shows the security breach events based on economic loss generated. Table C.8 in the appendix summarises the topological features pre and post breach events. It is apparent from this table that the Bitcoin prices network become more connected, as the number of edges increased after all breach events. Moreover, the magnitude of transfer information among the Bitcoin prices raised as the average node strength increased, indicating that the connections or the information transaction in Bitcoin cross-market prices network increased as a response to the announcement of this type of cybercrime. Figures C.14 to C.18 in the appendix illustrate the adjustment on the network after the platform experienced a security breach. There was a clear trend of graph density, which highlights the influence of the theft breach on the Bitcoin cross-market prices.

The results shown in Tables C.19 to C.23 in the appendix indicate that the main senders and receivers in the network have been changed after theft breaches. The most striking result to emerge from the analysis confirms the same pattern mentioned in the third chapter where the Bitcoin pair that represents the Headquarter location of the Bitcoin platform that experienced a breach became more active in sending information in the network. Initially, BTC/KRW was the top receiver of the information in the network before the South Korean platform Yapizon experienced a cyberattack. However, after the attack, BTC/KRW played a significant role to become the third transmitter of information in the network. In the same vein, BTC/JPY become more active after the Japanese platform Zaif suffered a cyberattack. Also, BTC/UK remained as the top sender of information even after a British platform, Cashaa, deal with a security breach. Therefore, the results reveal evidence that the contagion risk of security breach can be seen, particularly if the platform suffers economic loss.

The final set of analyses examined the influence of certain type of security breaches depending on the confidentiality category. In several events, security breaches can lead to the leak of personal data for traders. Table C.1 in the appendix shows the cyberattacks that gain unauthorised access to steal personal data for thousands of traders. The results obtained from the preliminary analysis are summarised in Table C.7 in the appendix. Interestingly the number of edges decreased after this kind of breach, indicating the reduction of the flow of information between the network nodes. In addition, the amount of information transmitted dropped after the platform suffered the data leak. Also, the analysis showed that the same pattern occurred in all events included in this category, where all network topological features declined after confidentiality breaches. Figures C.9 to C.13 in the appendix reveal the dramatic vicissitudes in the network where the graph density decreased

after the cyberattacks. Interestingly, there was a kind of a relationship between the size of the breach and the reduction of dependency among Bitcoin prices. The more users that were affected by the security breaches, the greater the decline in the amount of information exchanged in the network. In the case of Trezor, Ledger, and Keepkay the number of accounts subject to leaks was nearly 80000 and the reduction of ETE was approximately 24%compared with the Ledger where personal data were exposed for almost one million users, causing a severe decline in the interdependency among Bitcoin price to 45%. The same pattern applies to the rest of the events, where Coinmama, Bithumb and Trident suffered from unauthorised access to steal personal data for 450,000, 318,000 and 266,000 users respectively. Also the decrease of the strength of the information spillover between Bitcoin prices was 45%, 31% and 31%, correspondingly. Tables C.14 to C.18 in the appendix report the dominant role of top receivers and the main source of information. Most notably the BTC/USD and BTC/JPY play a leading role as sources of information after the confidentiality cyberattacks. Meanwhile, no significant changes were found on the recipient of the information, where BTC/ PLN remains as the top information receiver pre and post the security breach.

Notably, the distribution of in-degree and out-degree values show the possible to find certain memory distribution. Real-world networks, whether biological or social, can be decried as inhomogeneous connective structures, in which interconnections are almost distributed as a power-law, where few nodes in the network have a number of relationships compared with the vast majority of node in the same network with very few edges commonly known as scale-free networks (Barabási and Albert, 1999). Thus, we took the recent two breach events for each category and try to examine the distribution of in-degree and out-degree for each breach events. Figures C.19 to C.24 display the histogram pre- and post each cyberattacks. Regarding to availability cybercrime depicted in Figures C.19 to C.20. The evidence suggested that there was very weak form of scale-free in case of Bitfinex 5-2018 for both out degree and in degree. Meanwhile, there was a strong form of scale-free in case of Bitfinex 2-2020, where both in degree and out degree distribution clustered into one side. On the other hand, the form of the distribution of in-degree and out-degree after theft events represented in Figures C.21 to C.22. There was moderated form of scale-free property post the security breach that targeted KuCoin 9-2020. However, after the breach event on Cashaa 7-2020 the degree distribution show a strong form of scale-free. Remarkably, regarding to confidentiality category the histogram of in and out degree post the cybercrimes did not present a strong form of scale-free property.

Based on the evidence previously reported, it is possible to characterize the networks under analysis as scale-free in the sense of

Overall, these results provide important insights into the diverse influences of cyberattacks on the Bitcoin cross-market prices. The observed differences were spotted in the network adjustment and the contagion risk of cyberattacks, where (i) the network reacts similarly in the case of availability attacks and theft breaches, (ii) the linkages or edges increased after breach events and (iii) the amount of information transmitted among Bitcoin price are also increased. Thus, the findings are consistent with previous research by Caporale et al. (2021) which shows that cyberattacks increase the linkages among cryptocurrencies. On the other hand, the network reacts contrarily in case of confidentiality breaches where there has been a marked decline in the linkages among Bitcoin price, and the amount of information diminished after the breach events.

4.5 Conclusions

The main aim of this chapter was to differentiate among the effect of several categories on the Bitcoin cross-market prices. Thus, since this difference has been found between the three main classifications, the findings reported in this chapter appear to support the assumption that each type of cyberattack has it is own influences on the Bitcoin cross-market prices where the impact of the availability category appears to increase the links between the Bitcoin prices network. This indicates that the risk of cyberattacks has spread, but the effect has actually been that the network has become more active and information spillover has increased. However, the magnitude of the impact of the availability attack depends on the damage caused; that is, the DDoS attacks that led to the temporary suspension of the platform services caused much more damage in the network compared to the attacks that only affected the performance of the website.

On the other hand, the confidentiality group impacted the Bitcoin markets differently. As the volume of information exchange between the Bitcoin prices network decreased after this type of breach. The effect of contagion risk under the confidentiality class was in the form of reducing the transfer of information in the network. Also, the finding sheds new light on the issue as the size of the data leak plays a central role; more personal data leaked can cause a greater decrease in the linkages between Bitcoin price, and. the risk of cyberattack become more contagious in the Bitcoin price network. This highlights the leading role of Bitcoin pairs BTC/JPY and BTC/USD to become the source of information after this type of breach event.

In terms of the theft category, the interconnectedness of the Bitcoin price network increased after the breach events. The contagion risk of cyberattacks was in the form of increasing the amount of information exchanged and the dependence between Bitcoin prices. It is also worth noting that the location of the platform that experienced a security breach has a significant role to indicate the main information transmitter after the cybercrime.

The evidence from this chapter suggests fundamental implications for both trade and platform managers. First, traders in the cryptocurrencies market can build an investment strategy to gain speculative profits particularly after the Bitcoin platform influenced by a cyberattack. Also, the traders should pay particular attention to the risk of the security breach as it can be a contagion even if it happened on a different platform. Moreover, investors need to gain more knowledge about different techniques and methods to secure their accounts; for example, using web browsers with security extension, or having software that can reduce phishing schemes. The cryptocurrencies

users need to follow several procurers to protect their investment, by activating two-factor authentication, avoiding using untrusted public Wi-Fi, and not choosing weak passwords. In addition, the cryptocurrencies investors that trade in several platforms should be aware not to appoint the same email or password.

Second, platform managers gain more knowledge about the way that security breach risk can spread in the Bitcoin market; therefore there is the need to have a controlling strategy that can reduce the influences of cyberattacks. Platform managers need to make additional efforts to separate more literacy about the best procedures that traders can follow to protect their accounts. Also, they need to increase the awareness of the common fraud schemes so the traders can avoid cybercriminals. Moreover, security managers in any Bitcoin platform should look forward to developing new technologies that can help to reduce cybercrimes and employ new practices such as machine learning, or fingerprinting devices.

The study has confirmed the findings of Caporale et al. (2021) which found that security breach plays a significant role in raising in the relations among cryptocurrencies. Thus, this chapter extends the body of knowledge by providing additional evidence that different types of breach event can affect the Bitcoin market in diverse ways. However, the current investigation has only shed light on the influence of cybercrime on the Bitcoin market. More broadly, it would be interesting to compare the influence of the different types of security breaches that targeted several cryptocurrencies.

Chapter 5 Conclusion

The main aim of this thesis was to evaluate the impact of cyberattacks on the Bitcoin cross-market prices network from various perspectives. The thesis sheds light on cyberattacks that only targeted the Bitcoin platform, as security breach can target other cryptocurrencies or other Bitcoin stakeholders – for example, Bitcoin miners. The major findings are that security breach events influenced the Bitcoin market prices and changed the structure of Bitcoin prices. In respect to Chapter Two, after using rolling estimations pre and post each event, the investigation has shown that the size of the attacks plays a crucial role. The results found evidence that large-scale breach events reduce the relationship between Bitcoin pairs. Moreover, the results of the centrality measurement analysis refer to the influence of cyberattacks on the Bitcoin pair that represents the location of the platform that suffers the cyberattack, where the Bitcoin pair lost the central role in the network that was built on the significant relationship among Bitcoin cross-market prices. The pattern was confirmed based on the appearance of the same pattern in all breach events.

Chapter Three investigated the causality relationship among Bitcoin markets and the network adjustments after the Bitcoin platform suffered from cyberattacks. The findings in this chapter suggest that breach events influenced the network of the Bitcoin price structure where, during the breach events, the network become more connected as the information transactions increased, referring to high interdependency among network nodes during the attack episode. Meanwhile, the dynamic network analysis indicates that, one month after the security breach event, the flow of information in the Bitcoin prices network dropped, pointing to the destructive power of cyberattacks that can impact the Bitcoin markets network. Finally, the effective Transfer Entropy (ETE) confirmed the pattern that the Bitcoin pair that represents the location of the platform that suffers the cyberattack becomes more active in sending information to other Bitcoin markets. Therefore, this finding provides crucial evidence of the contagion risk of cyberattack among Bitcoin cross-market prices.

Chapter Four was designed to classify security breaches that targeted the Bitcoin platforms depending on the threat posed, determine the effect of different types of cyberattacks that targeted the Bitcoin platform, and conduct a comparison for the changes that may occur in the Bitcoin network. The most obvious finding that each breach category has a unique impact on the Bitcoin

prices network where a cyberattack that caused money loss and influenced the platform availability increased the interdependency among Bitcoin markets. But breach events that cause a leak of personal data influenced the network differently, where the network became less connected and the flow of information between Bitcoin pairs decreased. Also, the results of the confidentiality group indicate the relation between the size of the breach and the reduction of the flow of information magnitude in the network.

The results hold implications for investors and portfolio managers to be aware of the contagion risk of the security breaches. Thus, they can construct an investment strategy to reduce the risk of money loss after breach events. In addition, these results suggest that Bitcoin platforms managers need to take set courses of action to enhance the security protocols and increase Bitcoin traders' awareness on how to secure their account and not to fall victim to cybercriminals. The current findings have thrown up general suggestions required to be addressed when tracing the impact of cyberattacks. Accordingly, further research that is interested in the influence of security breaches needs to pay particular attention to the nature of the cyberattacks and the damage that they generated as the finding in Chapter Four shows evidence that each type of security breach poses different influences in the Bitcoin markets. Moreover, the market has become more attractive as a result of which the frequency of breach events has increased recently. Therefore, including high frequent data can provide more accurate results, because it may help to reduce the chance that the analysis is influenced by other breach events.

This work plants the seeds for future studies that aim to further analyse the influences of breach events on the relationship among Bitcoin cross-market prices. More investigation is needed to compare the impact of different types of cyberattacks on the cryptocurrencies network.

References

ABHISHTA, A., JOOSTEN, R., DRAGOMIRETSKIY, S. & NIEUWENHUIS, L. J. Impact of successful ddos attacks on a major crypto-currency exchange. 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2019. IEEE, 379-384.

ABREU, M. P., GRASSI, R. & DEL-VECCHIO, R. R. 2019. Structure of control in financial networks: An application to the Brazilian stock market. Physica A: Statistical Mechanics and its Applications, 522, 302-314.

ALLEN, F. & BABUS, A. 2009. Networks in finance. The network challenge: strategy, profit, and risk in an interlinked world, 367.

AL-YAHYAEE, K. H., MENSI, W. & YOON, S.-M. 2018. Efficiency, multifractality, and the long-memory property of the Bitcoin market: A comparative analysis with stock, currency, and gold markets. Finance Research Letters, 27, 228-234.

ANDERSON, R., BARTON, C., BÖHME, R., CLAYTON, R., VAN EETEN, M. J., LEVI, M., MOORE, T. & SAVAGE, S. 2013. Measuring the cost of cybercrime. The economics of information security and privacy. Springer.

ANISE, O. & LADY, K. 2017. State of the auth: experiences and perceptions of multi-factor authentication. Duo Security. Tillgänglig: https://duo. com/assets/ebooks/state-of-the-auth. pd f.

ANTONAKAKIS, N., CHATZIANTONIOU, I. & GABAUER, D. 2019. Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. Journal of International Financial Markets, Institutions and Money, 61, 37-51.

APOSTOLAKI, M., ZOHAR, A. & VANBEVER, L. Hijacking bitcoin: Routing attacks on cryptocurrencies. 2017 IEEE Symposium on Security and Privacy (SP), 2017. IEEE, 375-392.

AUCONI, A., GIANSANTI, A. & KLIPP, E. 2019. Information Thermodynamics for Time Series of Signal-Response Models. Entropy, 21, 177.

AZQUETA-GAVALDÓN, A. 2020. Causal inference between cryptocurrency narratives and prices: Evidence from a complex dynamic ecosystem. Physica A: Statistical Mechanics and its Applications, 537, 122574.

BAEK, C. & ELBECK, M. 2015. Bitcoins as an investment or speculative vehicle? A first look. Applied Economics Letters, 22, 30-34.

BAUR, D. G., HONG, K. & LEE, A. D. 2018. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money, 54, 177-189.

BAVELAS, A. 1950. Communication patterns in task-oriented groups. The Journal of the Acoustical Society of America, 22, 725-730.

Bacao, P., Duarte, A.P., Sebastiao, H., Redzepagic, S., 2018. Information transmission between cryptocurrencies: does Bitcoin rule the cryptocurrency world?.Sci. Ann. Econom. Busin. 65 (2), 97–117.

BEAUCHAMP, M. A. 1965. An improved index of centrality. Behavioral science, 10, 161-163.

BEHRENDT, S., DIMPFL, T., PETER, F. J. & ZIMMERMANN, D. J. 2019. RTransferEntropy—Quantifying information flow between different time series using effective transfer entropy. SoftwareX, 10, 100265.

BEKIROS, S., NGUYEN, D. K., JUNIOR, L. S. & UDDIN, G. S. 2017. Information diffusion, cluster formation and entropy-based network dynamics in equity and commodity markets. European Journal of Operational Research, 256, 945-961.

BINANCE. 2018. Binance Will Temporarily Disable New User Registrations [Online]. Available: https://binance.zendesk.com/hc/en-us/articles/115003773671 [Accessed 15/2/2021].

BLOCH, F., JACKSON, M. O. & TEBALDI, P. 2017. Centrality measures in networks. Available at SSRN 2749124.

BLOOMBERG. 2014. Mt.Gox Seeks Bankruptcy After $480 Million Bitcoin Loss [Online]. Available: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy [Accessed 2/5/2019].

BOAKO, G., TIWARI, A. K. & ROUBAUD, D. 2019. Vine copula-based dependence and portfolio value-at-risk analysis of the cryptocurrency market. International Economics, 158, 77-90.

BONACICH, P. 1972. Factoring and weighting approaches to status scores and clique identification. Journal of mathematical sociology, 2, 113-120.

Bonacich, P., 1972. Factoring and weighting approaches to status scores and clique dentification. Journal of mathematical sociology, 2(1), pp.113-120.

BORGATTI, S. P. & EVERETT, M. G. 1997. Network analysis of 2-mode data. Social networks, 19, 243-269.

BORRI, N. & SHAKHNOV, K. 2020. Regulation spillovers across cryptocurrency markets. Finance Research Letters, 36, 101333.

BOURI, E., GUPTA, R., TIWARI, A. K. & ROUBAUD, D. 2017a. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. Finance Research Letters, 23, 87-95.

BOURI, E., MOLNÁR, P., AZZI, G., ROUBAUD, D. & HAGFORS, L. I. 2017b. On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? Finance Research Letters, 20, 192-198.

BOUVERET, A. 2018. Cyber risk for the financial sector: A framework for quantitative assessment, International Monetary Fund.

BRANDES, U. 2001. A faster algorithm for betweenness centrality. Journal of mathematical sociology, 25, 163-177.

BREZO, F. & BRINGAS, P. G. 2012. Issues and risks associated with cryptocurrencies such as Bitcoin. In: INTERNATIONAL, T. S. & CONFERENCE ON SOCIAL ECO-INFORMATICS (eds.). http://www.thinkmind.org/index.php?view=article&articleid=sotics_2012_1_40_30101.

BUREAU, C. F. P. 2016. Risk to consumer posed by virtual currencies [Online]. Available: http://www.fatf-gafi.org/topics/ [Accessed Retrieved April 5, 2020].

CAMPBELL, K., GORDON, L. A., LOEB, M. P. & ZHOU, L. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11, 431-448.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2020. Non-linearities, cyber attacks and cryptocurrencies. Finance Research Letters, 32, 101297.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2020a. Cyber-Attacks and Cryptocurrencies. CESifo Working Paper No. 8124, 1-40.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2020b. Non-linearities, cyber attacks and cryptocurrencies. Finance Research Letters, 32, 101297.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2021. Cyber-attacks, spillovers and contagion in the cryptocurrency markets. Journal of International Financial Markets, Institutions and Money, 101298.

CHEAH, E.-T. & FRY, J. 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economics Letters, 130, 32-36.

CHEAH, E.-T., MISHRA, T., PARHI, M. & ZHANG, Z. 2018. Long memory interdependency and inefficiency in Bitcoin markets. Economics Letters, 167, 18-25.

CHENG, X. & ZHAO, H. 2019. Modeling, analysis and mitigation of contagion in financial systems. Economic Modelling, 76, 281-292.

CHUEN, D. L. K. 2015. Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data, Academic Press.closure. ACM Transactions on Internet Technology (TOIT), 18, 1-18.

CNBC. (2019). $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. [online] Available at: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html [Accessed 25 Apr. 2019].

CNBC. 2016. Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong [Online]. Available: https://www.cnbc.com/2016/08/03/hong-kong-bitcoin-exchange-says-it-was-hacked-trading-suspended.html [Accessed 1/5/2020 2020].

CoinMarketCap. (2019). Cryptocurrency Market Capitalizations | CoinMarketCap. [online] Available at: https://coinmarketcap.com/ [Accessed 12 Apr. 2019].

COINMARKETCAP. 2021. Today's Cryptocurrency Prices by Market Cap [Online]. Available: https://coinmarketcap.com/ [Accessed 15/4/2021].

CONTI, M., KUMAR, E. S., LAL, C. & RUJ, S. 2018. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20, 3416-3452.

CORBET, S., CUMMING, D. J., LUCEY, B. M., PEAT, M. & VIGNE, S. 2019a. Investigating the dynamics between price volatility, price discovery, and criminality in cryptocurrency markets. Price Discovery, and Criminality in Cryptocurrency Markets (May 3, 2019).

CORBET, S., LUCEY, B., URQUHART, A. & YAROVAYA, L. 2019b. Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis, 62, 182-199.

DICKEY, D. A. & FULLER, W. A. 1981. Likelihood ratio statistics for autoregressive time series with a unit root. Econometrica: journal of the Econometric Society, 1057-1072.

Dijkstra, E.W., 1959. A note on two problems in connexion with graphs. Numerische mathematik, 1(1), pp.269-271.

DIMPFL, T. & PETER, F. J. 2018. Analysing volatility transmission using group transfer entropy. Energy Economics, 75, 368-376.

DIMPFL, T. & PETER, F. J. 2019. Group transfer entropy with an application to cryptocurrencies. Physica A: Statistical Mechanics and its Applications, 516, 543-551.

Du, Y., Gao, C., Chen, X., Hu, Y., Sadiq, R. and Deng, Y., 2015. A new closeness centrality measure via effective distance in complex networks. Chaos: An Interdisciplinary Journal of Nonlinear Science, 25(3), p.033112.

DUGDALE, J. S. 2018. Entropy and its physical meaning, CRC Press.

ELIYAN, L. F. & DI PIETRO, R. 2021. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems.

FAMA, E. F. 1970. Efficient Capital Markets: A Review of Theory and Empirical Work." Journal of Finance 25: 385-417.. 1980. Agency Problems and the Theory of the Firm." Journal of Political Economy, 88, 288-307.

FEDER, A., GANDAL, N., HAMRICK, J. & MOORE, T. 2017. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt.Gox. Journal of Cybersecurity, 3, 137-144.

FEDER, A., GANDAL, N., HAMRICK, J., MOORE, T., MUKHERJEE, A., ROUHI, F. & VASEK, M. 2018b. The Economics of Cryptocurrency Pump and Dump Schemes. CEPR Discussion Papers.

FORBES. 2019. Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018 [Online]. Forbes. Available: https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#6ab4b35a55f5 [Accessed 1 May 2020].

FRANCÉS, C. J., GRAU-CARLES, P. & ARELLANO, D. J. 2018. The cryptocurrency market: A network analysis. Esic Market Economics and Business Journal, 49, 569-583.

FREEMAN, L. C. 1978. Centrality in social networks conceptual clarification. Social networks, 1, 215-239.

GANDAL, N., HAMRICK, J., MOORE, T. & OBERMAN, T. 2018. Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics, 95, 86-96.

Gattiker, U.E., 2004. The information security dictionary: Defining the terms that define security for E-business, Internet, information, and wireless technology. Springer Science & Business Media. Vol. 767.p 292

GILLAIZEAU, M., JAYASEKERA, R., MAAITAH, A., MISHRA, T., PARHI, M. & VOLOKITINA, E. 2019. Giver and the receiver: Understanding spillover effects and predictive power in cross-market Bitcoin prices. International Review of Financial Analysis.

GKILLAS, K. & KATSIAMPA, P. 2018. An application of extreme value theory to cryptocurrencies. Economics Letters, 164, 109-111.

GKILLAS, K. & LONGIN, F. 2018. Is Bitcoin the new digital gold. Evidence from extreme price movements in financial markets. Evidence From Extreme Price Movements in Financial Markets.

GKILLAS, K., BOURI, E., GUPTA, R. & ROUBAUD, D. 2020. Spillovers in Higher-Order Moments of Crude Oil, Gold, and Bitcoin. The Quarterly Review of Economics and Finance.

Gorokhova, S., Sboev, A.G., Kukin, K.A., Rybka, R.B., Muraseeva, E.V. and Atkov, O.Y., 2013. Network Topologies: Types, Performance Impact and Advantages/Disadvantages.

Grassi, R., Calderoni, F., Bianchi, M. and Torriero, A., 2019. Betweenness to assess leaders in criminal networks: New evidence using the dual projection approach. Social Networks, 56, pp.23-32.

GREVEN, A., KELLER, G. & WARNECKE, G. 2014. Entropy, Princeton University Press.

Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (June 13, 2018). Available at SSRN: https://ssrn.com/abstract=3195066 or http://dx.doi.org/10.2139/ssrn.3195066

HACKREAD.COM 2017. Fake Bittrex cryptocurrency exchange site stealing user funds.

HAMRICK, J., ROUHI, F., MUKHERJEE, A., FEDER, A., GANDAL, N., MOORE, T. & VASEK, M. 2018. An examination of the cryptocurrency pump and dump ecosystem. Available at SSRN 3303365.

HAN, D. 2019. Network analysis of the Chinese stock market during the turbulence of 2015–2016 using log-returns, volumes and mutual information. Physica A: Statistical Mechanics and its Applications.

HASSAN, A., MAS' UD, M. Z., SHAH, W. M., ABDUL-LATIP, S. F., AHMAD, R. & ARIFFIN, A. 2020. A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. OIC-CERT Journal of Cyber Security, 2, 1-17.

HE, J. & SHANG, P. 2017. Comparison of transfer entropy methods for financial time series. Physica A: Statistical Mechanics and its Applications, 482, 772-785.

HEIBERGER, R. H. 2014. Stock network stability in times of crisis. Physica A: Statistical Mechanics and its Applications, 393, 376-381.

HIGGINS, S. 2015. Details of $5 Million Bitstamp Hack Revealed [Online]. coindesk. Available: https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange [Accessed 1/5/2020 2020].

HIGGINS, S. 2016. Cryptsy CEO: Bitcoin Theft Kept Hidden to Avoid 'Panic' [Online]. coindesk. Available: https://www.coindesk.com/cryptsy-bitcoin-theft-avoid-panic [Accessed 1/5/2020].

HIGGINS, S. 2016. The website for Cryptsy has been taken offline. [Online]. coindesk. Available: https://www.coindesk.com/cryptsy-bankruptcy-millions-bitcoin-stolen [Accessed 21/1/2021].

HILL, K. 2013. The FBI's Plan For The Millions Worth Of Bitcoins Seized From Silk Road [Online]. Forbes. Available: https://www.forbes.com/sites/kashmirhill/2013/10/04/fbi-silk-road-bitcoin-seizure/#26b6e2032848 [Accessed 24/4/2020].

HOQUE, N., KASHYAP, H. & BHATTACHARYYA, D. K. 2017. Real-time DDoS attack detection using FPGA. Computer Communications, 110, 48-58.

HUANG, D. Y., DHARMDASANI, H., MEIKLEJOHN, S., DAVE, V., GRIER, C., MCCOY, D., SAVAGE, S., WEAVER, N., SNOEREN, A. C. & LEVCHENKO, K. Botcoin: Monetizing Stolen Cycles. NDSS, 2014. Citeseer.

HUILLET, M. 2019. Crypto Exchange Gate.io Confirms 51% Attack on Ethereum Classic, Promises Refunds [Online]. Cointelegraph. Available: https://cointelegraph.com/news/swipe-visa-card-adds-crypto-travel-booking-sites-ava-token [Accessed 22/4/2020].

HUYNH, T. L. D., NASIR, M. A., VO, X. V. & NGUYEN, T. T. 2020. “Small things matter most”: The spillover effects in the cryptocurrency market and gold as a silver bullet. The North American Journal of Economics and Finance, 54, 101277.

IYER, S. R., SIMKINS, B. J. & WANG, H. 2020. Cyberattacks and impact on bond valuation. Finance Research Letters, 33, 101215.

JI, Q., BOURI, E., LAU, C. K. M. & ROUBAUD, D. 2019a. Dynamic connectedness and integration in cryptocurrency markets. International Review of Financial Analysis, 63, 257-272.

JI, Q., BOURI, E., ROUBAUD, D. & KRISTOUFEK, L. 2019b. Information interdependence among energy, cryptocurrency and major commodity markets. Energy Economics, 81, 1042-1055.

JI, Q., MARFATIA, H. & GUPTA, R. 2018. Information spillover across international real estate investment trusts: Evidence from an entropy-based network analysis. The North American Journal of Economics and Finance, 46, 103-113.

JOHNSON, B., LASZKA, A., GROSSKLAGS, J., VASEK, M. & MOORE, T. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. International Conference on Financial Cryptography and Data Security, 2014. Springer, 72-86.

KAMIYA, S., KANG, J.-K., KIM, J., MILIDONIS, A. & STULZ, R. M. 2020. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics.

KATSIAMPA, P. 2017. Volatility estimation for Bitcoin: A comparison of GARCH models. Economics Letters, 158, 3-6.

KATSIAMPA, P. 2019. An empirical investigation of volatility dynamics in the cryptocurrency market. Research in International Business and Finance, 50, 322-335.

KATSIAMPA, P., CORBET, S. & LUCEY, B. 2019. Volatility spillover effects in leading cryptocurrencies: A BEKK-MGARCH analysis. Finance Research Letters, 29, 68-74.

Katz, L., 1953. A new index derived from sociometric data analysis. Psychometrika 18, 39–43.

KHAIRUDDIN, I. 2019. Understanding and designing for trust in Bitcoin Blockchain. Lancaster University.

Kim, T. Y. Choi, T. Yan, and K. Dooley. 2011. Structural investigation of supply networks: a social network analysis approach, Journal of Operations Management, vol. 29, no. 3,pp. 194–211,

KITSAK, M., GALLOS, L. K., HAVLIN, S., LILJEROS, F., MUCHNIK, L., STANLEY, H. E. & MAKSE, H. A. 2010. Identification of influential spreaders in complex networks. Nature physics, 6, 888.

KOPP, E., KAFFENBERGER, L. & JENKINSON, N. 2017. Cyber risk, market failures, and financial stability, International Monetary Fund.

KOUTMOS, D. 2018. Return and volatility spillovers among cryptocurrencies. Economics Letters, 173, 122-127.

KUZUBAŞ, T. U., ÖMERCIKOĞLU, I. & SALTOĞLU, B. 2014. Network centrality measures and systemic risk: An application to the Turkish financial crisis. Physica A: Statistical Mechanics and its Applications, 405, 203-215.

LAGAZIO, M., SHERIF, N. & CUSHMAN, M. 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.

LAHIANI, A. & JLASSI, N. B. 2021. Nonlinear tail dependence in cryptocurrency-stock market returns: The role of Bitcoin futures. Research in International Business and Finance, 56, 101351.

LEDGER. 2020. Addressing the July 2020 e-commerce and marketing data breach — A Message From Ledger's Leadership [Online]. Available: https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach [Accessed 13/2/2021].

LEE, T. K., CHO, J. H., KWON, D. S. & SOHN, S. Y. 2019. Global stock market investment strategies based on financial network indicators using machine learning techniques. Expert Systems with Applications, 117, 228-242.

LI, X. & WANG, C. A. 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems, 95, 49-60.

LISCHKE, M. & FABIAN, B. 2016. Analyzing the bitcoin network: The first four years. Future Internet, 8, 7.

LIU, J.-G., REN, Z.-M. & GUO, Q. 2013. Ranking the spreading influence in complex networks. Physica A: Statistical Mechanics and its Applications, 392, 4154-4159.

LIU, Y., TANG, M., ZHOU, T. & DO, Y. 2016. Identify influential spreaders in complex networks, the role of neighborhood. Physica A: Statistical Mechanics and its Applications, 452, 289-298.

LUNA-REYES, L. F., CRESSWELL, A. M. & RICHARDSON, G. P. Knowledge and the development of interpersonal trust: A dynamic model. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, 2004. IEEE, 12 pp.

LEWIS, J. 2018. Economic Impact of Cybercrime, No Slowing Down. McAfee. *Center for Strategic and International Studies (CSIS). https://www. mcafee. com/enterprise/en-us/solutions/lp/economics-cybercrime. html. Zugegriffen am,* 13**,** 2019.

MAI, Y., CHEN, H., ZOU, J.-Z. & LI, S.-P. 2018. Currency co-movement and network correlation structure of foreign exchange market. Physica A: Statistical Mechanics and its Applications, 492, 65-74.

MALIK, M. S. & ISLAM, U. 2019. Cybercrime: an emerging threat to the banking sector of Pakistan. Journal of Financial Crime, 26 50-60.

MAO, X. & SHANG, P. 2017. Transfer entropy between multivariate time series. Communications in Nonlinear Science and Numerical Simulation, 47, 338-347.

MARELLA, V., UPRETI, B., MERIKIVI, J. & TUUNAINEN, V. K. 2020. Understanding the creation of trust in cryptocurrencies: the case of Bitcoin. Electronic Markets, 1-13.

MARMEFELT, T. 2018. The History of Money and Monetary Arrangements: Insights from the Baltic and North Seas Region, Routledge.

MARTIN, J. & CHRISTIN, N. 2016. Ethics in cryptomarket research. International Journal of Drug Policy, 35, 84-91.

MCGINN, D., BIRCH, D., AKROYD, D., MOLINA-SOLANA, M., GUO, Y. & KNOTTENBELT, W. J. 2016. Visualizing dynamic bitcoin transaction patterns. Big data, 4, 109-119.

MOORE, T. & CHRISTIN, N. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. International Conference on Financial Cryptography and Data Security, 2013. Springer, 25-33.

MOORE, T., CHRISTIN, N., AND SZURDI, J 2018. Revisiting the risks of bitcoin currency exchange

MÖSER, M., BÖHME, R. & BREUKER, D. An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG eCrime Researchers Summit, 2013. Ieee, 1-14.

NADARAJAH, S. & CHU, J. 2017. On the inefficiency of Bitcoin. Economics Letters, 150, 6-9.

NAKAMOTO, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

NEWMAN, M. E. 2001. Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. Physical review E, 64, 016132.

Nie, T., Guo, Z., Zhao, K. and Lu, Z.M., 2016. Using mapping entropy to identify node centrality in complex networks. Physica A: Statistical Mechanics and its Applications, 453, pp.290-297.

OBER, M., KATZENBEISSER, S. & HAMACHER, K. 2013. Structure and anonymity of the bitcoin transaction graph. Future internet, 5, 237-250.

OMANE-ADJEPONG, M. & ALAGIDEDE, I. P. 2019. Multiresolution analysis and spillovers of major cryptocurrency markets. Research in International Business and Finance, 49, 191-206.

OOSTHOEK, K. & DOERR, C. From hodl to heist: Analysis of cyber security threats to bitcoin exchanges. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020. IEEE, 1-9.

OPSAHL, T., AGNEESSENS, F. & SKVORETZ, J. 2010. Node centrality in weighted networks: Generalizing degree and shortest paths. Social networks, 32, 245-251.

Peay, E.R., 1980. Connectedness in a general model for valued networks. Social Networks, 2(4), pp.385-410.

PINZÓN, C. & ROCHA, C. 2016. Double-spend attack models with time advantange for bitcoin. Electronic Notes in Theoretical Computer Science, 329, 79-103.

QURESHI, S., AFTAB, M., BOURI, E. & SAEED, T. 2020. Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency. Physica A: Statistical Mechanics and its Applications, 559, 125077.

RAUCHS, M. & HILEMAN, G. 2017. Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance Reports.

RAZAK, F. A. & JENSEN, H. J. 2014. Quantifying 'causality' in complex systems: understanding transfer entropy. PLoS One, 9, e99462.

REDMAN, J. 2017. Hacked South Korean Bitcoin Exchange Yapizon Offers IOUs [Online]. Bitcoin.com. Available: https://news.bitcoin.com/hacked-korean-bitcoin-exchange-yapizon-offers-ious/ [Accessed 1/5/2020].

RESNICK, P., ZECKHAUSER, R., SWANSON, J. & LOCKWOOD, K. 2006. The value of reputation on eBay: A controlled experiment. Experimental economics, 9, 79-101.

RIQUELME, F., GONZALEZ-CANTERGIANI, P., MOLINERO, X. & SERNA, M. 2018. Centrality measure in social networks based on linear threshold model. Knowledge-Based Systems, 140, 92-102.

ROSATI, P., CUMMINS, M., DEENEY, P., GOGOLIN, F., VAN DER WERFF, L. & LYNN, T. 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. International Review of Financial Analysis, 49, 146-154.

RUFFING, T., KATE, A. & SCHRÖDER, D. Liar, liar, coins on fire! Penalizing equivocation by loss of bitcoins. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. 219-230.

SAITO, K., KIMURA, M., OHARA, K. & MOTODA, H. 2016. Super mediator–A new centrality measure of node importance for information diffusion over social network. Information Sciences, 329, 985-1000.

SAS, C. & KHAIRUDDIN, I. E. Exploring trust in Bitcoin technology: a framework for HCI research. Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction, 2015. 338-342.

SCHREIBER, T. 2000. Measuring information transfer. Physical review letters, 85, 461.

SCHWEIKART, L. 1991. US commercial banking: a historiographical survey. The Business History Review, 606-661.

SENSOY, A. 2019. The inefficiency of Bitcoin revisited: A high-frequency analysis with alternative currencies. Finance Research Letters, 28, 68-73.

SENSOY, A., SOBACI, C., SENSOY, S. & ALALI, F. 2014. Effective transfer entropy approach to information flow between exchange rates and stock markets. Chaos, solitons & fractals, 68, 180-185.

Serrat, O., 2017. Social network analysis. In Knowledge solutions (pp. 39-43). Springer, Singapore.

SHANAEV, S., SHURAEVA, A., VASENIN, M. & KUZNETSOV, M. 2019. Cryptocurrency value and 51% attacks: evidence from event studies. The Journal of Alternative Investments, 22, 65-77.

SHANNON, C. E. 1948. A mathematical theory of communication. The Bell system technical journal, 27, 379-423.

SHCHERBAK, S. 2014. How should Bitcoin be regulated. Eur. J. Legal Stud., 7, 41.

SHEN, D., URQUHART, A. & WANG, P. 2019. Does twitter predict Bitcoin? Economics Letters, 174, 118-122.

SIGURDSSON, G., GIARETTA, A. & DRAGONI, N. Vulnerabilities and Security Breaches in Cryptocurrencies. International Conference in Software Engineering for Defence Applications, 2018. Springer, 288-299.

Silverman, B.W., 2018. Density estimation for statistics and data analysis. Routledge.

STOSIC, D., STOSIC, D., LUDERMIR, T. B. & STOSIC, T. 2018. Collective behavior of cryptocurrency price changes. Physica A: Statistical Mechanics and its Applications, 507, 499-509.

TIWARI, A. K., JANA, R., DAS, D. & ROUBAUD, D. 2018. Informational efficiency of Bitcoin—An extension. Economics Letters, 163, 106-109.

TSIAKIS, T. & STHEPHANIDES, G. 2005. The concept of security and trust in electronic payments. Computers & Security, 24, 10-15.

URQUHART, A. 2016. The inefficiency of Bitcoin. Economics Letters, 148, 80-82.

URQUHART, A. 2018. What causes the attention of Bitcoin? Economics Letters, 166, 40-44.

VALENZA, G., FAES, L., CITI, L., ORINI, M. & BARBIERI, R. 2017. Instantaneous transfer entropy for the study of cardiovascular and cardiorespiratory nonstationary dynamics. IEEE Transactions on Biomedical Engineering, 65, 1077-1085.

VANDEZANDE, N. 2017. Virtual currencies under EU anti-money laundering law. Computer law & security review, 33, 341-353.

VASEK, M. & MOORE, T. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. International conference on financial cryptography and data security, 2015. Springer, 44-61.

VASEK, M., BONNEAU, J., CASTELLUCCI, R., KEITH, C. & MOORE, T. 2016. The Bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets. Financial Cryptography and Data Security, Lecture Notes in Computer Science. Springer.

VASEK, M., THORNTON, M. & MOORE, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. International conference on financial cryptography and data security, 2014. Springer, 57-71.

VER STEEG, G. & GALSTYAN, A. Information transfer in social media. Proceedings of the 21st international conference on World Wide Web, 2012. 509-518.

VIDAL-TOMÁS, D. & IBAÑEZ, A. 2018. Semi-strong efficiency of bitcoin. Finance Research Letters, 27, 259-265.

WANG, J., HOU, X., LI, K. & DING, Y. 2017. A novel weight neighborhood centrality algorithm for identifying influential spreaders in complex networks. Physica A: Statistical Mechanics and its Applications, 475, 88-105.

WANG, V., NNAJI, H. & JUNG, J. 2020. Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 100415.

Wasserman, S. and Faust, K., 1994. Social network analysis: Methods and applications (Vol. 8). Cambridge university press.

WRAY, L. R. 2012. Introduction to an alternative history of money. Levy Economics Institute. Working Paper.

XIA, P., WANG, H., ZHANG, B., JI, R., GAO, B., WU, L., LUO, X. & XU, G. 2020. Characterizing cryptocurrency exchange scams. Computers & Security, 98, 101993.

Yang, S. and Knoke, D., 2001. Optimal connections: strength and distance in valued graphs. Social networks, 23(4), pp.285-295.

ZARGAR, F. N. & KUMAR, D. 2019. Informational inefficiency of Bitcoin: A study based on high-frequency data. Research in International Business and Finance, 47, 344-353.

ZENG, A. & ZHANG, C.-J. 2013. Ranking spreaders by decomposing complex networks. Physics Letters A, 377, 1031-1035.

ZHANG, D. & BROADSTOCK, D. C. 2018. Global financial crisis and rising connectedness in the international commodity markets. International Review of Financial Analysis.

ZHAO, W. 2018. Crypto Exchange Zaif Hacked In $60 Million Bitcoin Theft [Online]. coindesk. Available: https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft?amp=1& [Accessed 1/5/2020].

ZIĘBA, D. & ŚLEDZIEWSKA, K. 2018. Are demand shocks in Bitcoin contagious?. (No. 2018-17).

ZIMBA, A., WANG, Z. & CHEN, H. 2018. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express, 4, 14-18.

ABHISHTA, A., JOOSTEN, R., DRAGOMIRETSKIY, S. & NIEUWENHUIS, L. J. Impact of successful ddos attacks on a major crypto-currency exchange. 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2019. IEEE, 379-384.

ABREU, M. P., GRASSI, R. & DEL-VECCHIO, R. R. 2019. Structure of control in financial networks: An application to the Brazilian stock market. *Physica A: Statistical Mechanics and its Applications,* 522**,** 302-314.

AHN, Y. & KIM, D. 2020. Sentiment disagreement and bitcoin price fluctuations: a psycholinguistic approach. *Applied Economics Letters,* 27**,** 412-416.

AL-YAHYAEE, K. H., MENSI, W. & YOON, S.-M. 2018. Efficiency, multifractality, and the long-memory property of the Bitcoin market: A comparative analysis with stock, currency, and gold markets. *Finance Research Letters,* 27**,** 228-234.

ALLEN, F. & BABUS, A. 2009. Networks in finance. *The network challenge: strategy, profit, and risk in an interlinked world,* 367.

ANISE, O. & LADY, K. 2017. State of the auth: experiences and perceptions of multi-factor authentication. Duo Security. *Tillgänglig: https://duo. com/assets/ebooks/state-of-the-auth. pd f*.

ANTONAKAKIS, N., CHATZIANTONIOU, I. & GABAUER, D. 2019. Cryptocurrency market contagion: Market uncertainty, market complexity, and dynamic portfolios. *Journal of International Financial Markets, Institutions and Money,* 61**,** 37-51.

APOSTOLAKI, M., ZOHAR, A. & VANBEVER, L. Hijacking bitcoin: Routing attacks on cryptocurrencies. 2017 IEEE Symposium on Security and Privacy (SP), 2017. IEEE, 375-392.

BAEK, C. & ELBECK, M. 2015. Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters,* 22**,** 30-34.

BAI, J. & PERRON, P. 2003. Computation and analysis of multiple structural change models. *Journal of applied econometrics,* 18**,** 1-22.

BAIG, A., BLAU, B. M. & SABAH, N. 2019. Price clustering and sentiment in bitcoin. *Finance Research Letters,* 29**,** 111-116.

BARABÁSI, A.-L. & ALBERT, R. 1999. Emergence of scaling in random networks. *science,* 286**,** 509-512.

BAUR, D. G., HONG, K. & LEE, A. D. 2018. Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money,* 54**,** 177-189.

BAVELAS, A. 1950. Communication patterns in task-oriented groups. *The Journal of the Acoustical Society of America,* 22**,** 725-730.

BEAUCHAMP, M. A. 1965. An improved index of centrality. *Behavioral science,* 10**,** 161-163.

BEHRENDT, S., DIMPFL, T., PETER, F. J. & ZIMMERMANN, D. J. 2019. RTransferEntropy—Quantifying information flow between different time series using effective transfer entropy. *SoftwareX,* 10**,** 100265.

BEKIROS, S., NGUYEN, D. K., JUNIOR, L. S. & UDDIN, G. S. 2017. Information diffusion, cluster formation and entropy-based network dynamics in equity and commodity markets. *European Journal of Operational Research,* 256**,** 945-961.

BINANCE. 2018. *Binance Will Temporarily Disable New User Registrations* [Online]. Available: https://binance.zendesk.com/hc/en-us/articles/115003773671 [Accessed 15/2/2021].

BLOCH, F., JACKSON, M. O. & TEBALDI, P. 2017. Centrality measures in networks. *Available at SSRN 2749124*.

BLOOMBERG. 2014. *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss* [Online]. Available: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy [Accessed 2/5/2019].

BOAKO, G., TIWARI, A. K. & ROUBAUD, D. 2019. Vine copula-based dependence and portfolio value-at-risk analysis of the cryptocurrency market. *International Economics,* 158**,** 77-90.

BOLT, W. & VAN OORDT, M. 2019. Speculation and the price of virtual currency.

BONACICH, P. 1972. Factoring and weighting approaches to status scores and clique identification. *Journal of mathematical sociology,* 2**,** 113-120.

BORGATTI, S. P. & EVERETT, M. G. 1997. Network analysis of 2-mode data. *Social networks,* 19**,** 243-269.

BORRI, N. & SHAKHNOV, K. 2020. Regulation spillovers across cryptocurrency markets. *Finance Research Letters,* 36**,** 101333.

BOURI, E., DAS, M., GUPTA, R. & ROUBAUD, D. 2018. Spillovers between Bitcoin and other assets during bear and bull markets. *Applied Economics,* 50**,** 5935-5949.

BOURI, E., GUPTA, R., TIWARI, A. K. & ROUBAUD, D. 2017a. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. *Finance Research Letters,* 23**,** 87-95.

BOURI, E., MOLNÁR, P., AZZI, G., ROUBAUD, D. & HAGFORS, L. I. 2017b. On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? *Finance Research Letters,* 20**,** 192-198.

BRANDES, U. 2001. A faster algorithm for betweenness centrality. *Journal of mathematical sociology,* 25**,** 163-177.

BROLL, U. & MUKHERJEE, S. 2017. International trade and firms' attitude towards risk. *Economic Modelling,* 64**,** 69-73.

BROWN, R. L., DURBIN, J. & EVANS, J. M. 1975. Techniques for testing the constancy of regression relationships over time. *Journal of the Royal Statistical Society: Series B (Methodological),* 37**,** 149-163.

BUREAU, C. F. P. 2016. *Risk to consumer posed by virtual currencies* [Online]. Available: http://www.fatf-gafi.org/topics/ [Accessed Retrieved April 5, 2020].

CAMPBELL, K., GORDON, L. A., LOEB, M. P. & ZHOU, L. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security,* 11**,** 431-448.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2020. Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters,* 32**,** 101297.

CAPORALE, G. M., KANG, W.-Y., SPAGNOLO, F. & SPAGNOLO, N. 2021. Cyber-attacks, spillovers and contagion in the cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money***,** 101298.

CHEAH, E.-T. & FRY, J. 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters,* 130**,** 32-36.

CHEAH, E.-T., MISHRA, T., PARHI, M. & ZHANG, Z. 2018. Long memory interdependency and inefficiency in Bitcoin markets. *Economics Letters,* 167**,** 18-25.

CHEN, L., PENG, J., LIU, Y., LI, J., XIE, F. & ZHENG, Z. 2020. Phishing scams detection in ethereum transaction network. *ACM Transactions on Internet Technology (TOIT),* 21**,** 1-16.

CHENG, X. & ZHAO, H. 2019. Modeling, analysis and mitigation of contagion in financial systems. *Economic Modelling,* 76**,** 281-292.

CHOW, G. C. 1960. Tests of equality between sets of coefficients in two linear regressions. *Econometrica: Journal of the Econometric Society***,** 591-605.

CHUEN, D. L. K. 2015. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*, Academic Press.

COINMARKETCAP. 2021. *Today's Cryptocurrency Prices by Market Cap* [Online]. Available: https://coinmarketcap.com/ [Accessed 15/4/2021].

CONTI, M., KUMAR, E. S., LAL, C. & RUJ, S. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials,* 20**,** 3416-3452.

CORBET, S., CUMMING, D. J., LUCEY, B. M., PEAT, M. & VIGNE, S. 2019. Investigating the dynamics between price volatility, price discovery, and criminality in cryptocurrency markets. *Price Discovery, and Criminality in Cryptocurrency Markets (May 3, 2019).*

DAI, F., SHI, Y., MENG, N., WEI, L. & YE, Z. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI), 2017. IEEE, 975-979.

DIMPFL, T. & PETER, F. J. 2019. Group transfer entropy with an application to cryptocurrencies. *Physica A: Statistical Mechanics and its Applications,* 516**,** 543-551.

DUGDALE, J. S. 2018. *Entropy and its physical meaning*, CRC Press.

EICHNER, T. & WAGENER, A. 2012. Tempering effects of (dependent) background risks: A mean-variance analysis of portfolio selection. *Journal of Mathematical Economics,* 48**,** 422-430.

ELIYAN, L. F. & DI PIETRO, R. 2021. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*.

EOM, C., KAIZOJI, T., KANG, S. H. & PICHL, L. 2019. Bitcoin and investor sentiment: statistical characteristics and predictability. *Physica A: Statistical Mechanics and its Applications,* 514**,** 511-521.

FAMA, E. F. 1970. Efficient Capital Markets: A Review of Theory and Empirical Work." Journal of Finance 25: 385-417.. 1980. *Agency Problems and the Theory of the Firm." Journal of Political Economy,* 88**,** 288-307.

FEDER, A., GANDAL, N., HAMRICK, J. & MOORE, T. 2017. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity,* 3**,** 137-144.

FEDER, A., GANDAL, N., HAMRICK, J. & MOORE, T. 2018a. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. *Journal of Cybersecurity,* 3**,** 137-144.

FEDER, A., GANDAL, N., HAMRICK, J., MOORE, T., MUKHERJEE, A., ROUHI, F. & VASEK, M. 2018b. The Economics of Cryptocurrency Pump and Dump Schemes. CEPR Discussion Papers.

FORBES. 2019. *Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018* [Online]. Forbes. Available: https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#6ab4b35a55f5 [Accessed 1 May 2020].

FRANCÉS, C. J., GRAU-CARLES, P. & ARELLANO, D. J. 2018. The cryptocurrency market: A network analysis. *Esic Market Economics and Business Journal,* 49**,** 569-583.

FREEMAN, L. C. 1978. Centrality in social networks conceptual clarification. *Social networks,* 1**,** 215-239.

GANDAL, N., HAMRICK, J., MOORE, T. & OBERMAN, T. 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics,* 95**,** 86-96.

GILLAIZEAU, M., JAYASEKERA, R., MAAITAH, A., MISHRA, T., PARHI, M. & VOLOKITINA, E. 2019a. Giver and the receiver: Understanding spillover effects and predictive power in cross-market Bitcoin prices. *International Review of Financial Analysis*.

GILLAIZEAU, M., JAYASEKERA, R., MAAITAH, A., MISHRA, T., PARHI, M. & VOLOKITINA, E. 2019b. Giver and the receiver: Understanding spillover effects and predictive power in cross-market Bitcoin prices. *International Review of Financial Analysis,* 63**,** 86-104.

GKILLAS, K., BOURI, E., GUPTA, R. & ROUBAUD, D. 2020. Spillovers in Higher-Order Moments of Crude Oil, Gold, and Bitcoin. *The Quarterly Review of Economics and Finance*.

GKILLAS, K. & KATSIAMPA, P. 2018. An application of extreme value theory to cryptocurrencies. *Economics Letters,* 164**,** 109-111.

GKILLAS, K. & LONGIN, F. 2018. Is Bitcoin the new digital gold. *Evidence from extreme price movements in financial markets. Evidence From Extreme Price Movements in Financial Markets*.

GREVEN, A., KELLER, G. & WARNECKE, G. 2014. *Entropy*, Princeton University Press.

GRIFFIN, J. M. & SHAMS, A. 2018. Is bitcoin really un-tethered?

GUÉGAN, D. & RENAULT, T. 2021. Does investor sentiment on social media provide robust information for Bitcoin returns predictability? *Finance Research Letters,* 38**,** 101494.

HACKREAD.COM 2017. Fake Bittrex cryptocurrency exchange site stealing user funds.

HAMRICK, J., ROUHI, F., MUKHERJEE, A., FEDER, A., GANDAL, N., MOORE, T. & VASEK, M. 2018. An examination of the cryptocurrency pump and dump ecosystem. *Available at SSRN 3303365*.

HAN, D. 2019. Network analysis of the Chinese stock market during the turbulence of 2015–2016 using log-returns, volumes and mutual information. *Physica A: Statistical Mechanics and its Applications*.

HANSEN, B. E. 1992. Testing for parameter instability in linear models. *Journal of policy Modeling,* 14**,** 517-533.

HASSAN, A., MAS' UD, M. Z., SHAH, W. M., ABDUL-LATIP, S. F., AHMAD, R. & ARIFFIN, A. 2020. A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency. *OIC-CERT Journal of Cyber Security,* 2**,** 1-17.

HEIBERGER, R. H. 2014. Stock network stability in times of crisis. *Physica A: Statistical Mechanics and its Applications,* 393**,** 376-381.

HIGGINS, S. 2016. *The website for Cryptsy has been taken offline.* [Online]. coindesk. Available: https://www.coindesk.com/cryptsy-bankruptcy-millions-bitcoin-stolen [Accessed 21/1/2021].

HOQUE, N., KASHYAP, H. & BHATTACHARYYA, D. K. 2017. Real-time DDoS attack detection using FPGA. *Computer Communications,* 110**,** 48-58.

HUANG, D. Y., DHARMDASANI, H., MEIKLEJOHN, S., DAVE, V., GRIER, C., MCCOY, D., SAVAGE, S., WEAVER, N., SNOEREN, A. C. & LEVCHENKO, K. Botcoin: Monetizing Stolen Cycles. NDSS, 2014. Citeseer.

HUYNH, T. L. D., NASIR, M. A., VO, X. V. & NGUYEN, T. T. 2020. "Small things matter most": The spillover effects in the cryptocurrency market and gold as a silver bullet. *The North American Journal of Economics and Finance,* 54**,** 101277.

JANG, S. M., YI, E., KIM, W. C. & AHN, K. 2019. Information flow between Bitcoin and other investment assets. *Entropy,* 21**,** 1116.

JI, Q., BOURI, E., LAU, C. K. M. & ROUBAUD, D. 2019a. Dynamic connectedness and integration in cryptocurrency markets. *International Review of Financial Analysis,* 63**,** 257-272.

JI, Q., BOURI, E., ROUBAUD, D. & KRISTOUFEK, L. 2019b. Information interdependence among energy, cryptocurrency and major commodity markets. *Energy Economics,* 81**,** 1042-1055.

JIANG, Y., NIE, H. & RUAN, W. 2018. Time-varying long-term memory in Bitcoin market. *Finance Research Letters,* 25**,** 280-284.

JOHNSON, B., LASZKA, A., GROSSKLAGS, J., VASEK, M. & MOORE, T. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. International Conference on Financial Cryptography and Data Security, 2014. Springer, 72-86.

KAMIYA, S., KANG, J.-K., KIM, J., MILIDONIS, A. & STULZ, R. M. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics,* 139**,** 719-749.

KATSIAMPA, P. 2017. Volatility estimation for Bitcoin: A comparison of GARCH models. *Economics Letters,* 158**,** 3-6.

KATSIAMPA, P. 2019. An empirical investigation of volatility dynamics in the cryptocurrency market. *Research in International Business and Finance,* 50**,** 322-335.

KATSIAMPA, P., CORBET, S. & LUCEY, B. 2019. Volatility spillover effects in leading cryptocurrencies: A BEKK-MGARCH analysis. *Finance Research Letters,* 29**,** 68-74.

KHAIRUDDIN, I. 2019. *Understanding and designing for trust in Bitcoin Blockchain.* Lancaster University.

KITSAK, M., GALLOS, L. K., HAVLIN, S., LILJEROS, F., MUCHNIK, L., STANLEY, H. E. & MAKSE, H. A. 2010. Identification of influential spreaders in complex networks. *Nature physics,* 6**,** 888.

KOUTMOS, D. 2018. Return and volatility spillovers among cryptocurrencies. *Economics Letters,* 173**,** 122-127.

KUZUBAŞ, T. U., ÖMERCIKOĞLU, I. & SALTOĞLU, B. 2014. Network centrality measures and systemic risk: An application to the Turkish financial crisis. *Physica A: Statistical Mechanics and its Applications,* 405**,** 203-215.

LAHIANI, A. & JLASSI, N. B. 2021. Nonlinear tail dependence in cryptocurrency-stock market returns: The role of Bitcoin futures. *Research in International Business and Finance,* 56**,** 101351.

LEDGER. 2020. *Addressing the July 2020 e-commerce and marketing data breach — A Message From Ledger's Leadership* [Online]. Available: https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach [Accessed 13/2/2021].

LEE, T. K., CHO, J. H., KWON, D. S. & SOHN, S. Y. 2019. Global stock market investment strategies based on financial network indicators using machine learning techniques. *Expert Systems with Applications,* 117**,** 228-242.

LI, X. & WANG, C. A. 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems,* 95**,** 49-60.

LISCHKE, M. & FABIAN, B. 2016. Analyzing the bitcoin network: The first four years. *Future Internet,* 8**,** 7.

LIU, J.-G., REN, Z.-M. & GUO, Q. 2013. Ranking the spreading influence in complex networks. *Physica A: Statistical Mechanics and its Applications,* 392**,** 4154-4159.

LIU, Y., TANG, M., ZHOU, T. & DO, Y. 2016. Identify influential spreaders in complex networks, the role of neighborhood. *Physica A: Statistical Mechanics and its Applications,* 452**,** 289-298.

LÓPEZ-CABARCOS, M. Á., PÉREZ-PICO, A. M., PIÑEIRO-CHOUSA, J. & ŠEVIĆ, A. 2019. Bitcoin volatility, stock market and investor sentiment. Are they connected? *Finance Research Letters***,** 101399.

LUNA-REYES, L. F., CRESSWELL, A. M. & RICHARDSON, G. P. Knowledge and the development of interpersonal trust: A dynamic model. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, 2004. IEEE, 12 pp.

MAI, Y., CHEN, H., ZOU, J.-Z. & LI, S.-P. 2018. Currency co-movement and network correlation structure of foreign exchange market. *Physica A: Statistical Mechanics and its Applications,* 492**,** 65-74.

MARELLA, V., UPRETI, B., MERIKIVI, J. & TUUNAINEN, V. K. 2020. Understanding the creation of trust in cryptocurrencies: the case of Bitcoin. *Electronic Markets***,** 1-13.

MATKOVSKYY, R. & JALAN, A. 2019. From financial markets to Bitcoin markets: A fresh look at the contagion effect. *Finance Research Letters,* 31**,** 93-97.

MCGINN, D., BIRCH, D., AKROYD, D., MOLINA-SOLANA, M., GUO, Y. & KNOTTENBELT, W. J. 2016. Visualizing dynamic bitcoin transaction patterns. *Big data,* 4**,** 109-119.

MIRIAN, A., DEBLASIO, J., SAVAGE, S., VOELKER, G. M. & THOMAS, K. Hack for hire: Exploring the emerging market for account hijacking. The World Wide Web Conference, 2019. 1279-1289.

MOORE, T. & CHRISTIN, N. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. International Conference on Financial Cryptography and Data Security, 2013. Springer, 25-33.

MOORE, T., CHRISTIN, N., AND SZURDI, J 2018. Revisiting the risks of bitcoin currency exchange

closure. *ACM Transactions on Internet Technology (TOIT),* 18**,** 1-18.

MÖSER, M., BÖHME, R. & BREUKER, D. An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG eCrime Researchers Summit, 2013. Ieee, 1-14.

MUKHERJEE, S., STAMATIS, D., BERTSCH, J., OVCHINNIKOVA, G., SUNDARAMURTHI, J. C., LEE, J., KANDIMALLA, M., CHEN, I.-M. A., KYRPIDES, N. C. & REDDY, T. 2021. Genomes OnLine Database (GOLD) v. 8: overview and updates. *Nucleic Acids Research,* 49**,** D723-D733.

MUKHERJEE, T. & PADHI, A. K. 2021. Investigating stability in ethical ideologies as moral personalities: understanding ethical shifts through centrality approach. *Current Psychology***,** 1-15.

NADARAJAH, S. & CHU, J. 2017. On the inefficiency of Bitcoin. *Economics Letters,* 150**,** 6-9.

NAEEM, M. A., MBARKI, I. & SHAHZAD, S. J. H. 2021. Predictive role of online investor sentiment for cryptocurrency market: Evidence from happiness and fears. *International Review of Economics & Finance,* 73**,** 496-514.

NAKAMOTO, S. 2008a. Bitcoin: A peer-to-peer electronic cash system.

NAKAMOTO, S. 2008b. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf,* 4.

NEWMAN, M. E. 2001. Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. *Physical review E,* 64**,** 016132.

OBER, M., KATZENBEISSER, S. & HAMACHER, K. 2013. Structure and anonymity of the bitcoin transaction graph. *Future internet,* 5**,** 237-250.

OMANE-ADJEPONG, M. & ALAGIDEDE, I. P. 2019. Multiresolution analysis and spillovers of major cryptocurrency markets. *Research in International Business and Finance,* 49**,** 191-206.

OOSTHOEK, K. & DOERR, C. From hodl to heist: Analysis of cyber security threats to bitcoin exchanges. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020. IEEE, 1-9.

OPSAHL, T., AGNEESSENS, F. & SKVORETZ, J. 2010. Node centrality in weighted networks: Generalizing degree and shortest paths. *Social networks,* 32**,** 245-251.

PINZÓN, C. & ROCHA, C. 2016. Double-spend attack models with time advantange for bitcoin. *Electronic Notes in Theoretical Computer Science,* 329**,** 79-103.

QURESHI, S., AFTAB, M., BOURI, E. & SAEED, T. 2020. Dynamic interdependence of cryptocurrency markets: An analysis across time and frequency. *Physica A: Statistical Mechanics and its Applications,* 559**,** 125077.

RAUCHS, M. & HILEMAN, G. 2017. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance Reports*.

RESNICK, P., ZECKHAUSER, R., SWANSON, J. & LOCKWOOD, K. 2006. The value of reputation on eBay: A controlled experiment. *Experimental economics,* 9**,** 79-101.

RIQUELME, F., GONZALEZ-CANTERGIANI, P., MOLINERO, X. & SERNA, M. 2018. Centrality measure in social networks based on linear threshold model. *Knowledge-Based Systems,* 140**,** 92-102.

ROSATI, P., CUMMINS, M., DEENEY, P., GOGOLIN, F., VAN DER WERFF, L. & LYNN, T. 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis,* 49**,** 146-154.

RUFFING, T., KATE, A. & SCHRÖDER, D. Liar, liar, coins on fire! Penalizing equivocation by loss of bitcoins. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. 219-230.

SAITO, K., KIMURA, M., OHARA, K. & MOTODA, H. 2016. Super mediator–A new centrality measure of node importance for information diffusion over social network. *Information Sciences,* 329**,** 985-1000.

SAS, C. & KHAIRUDDIN, I. E. Exploring trust in Bitcoin technology: a framework for HCI research. Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction, 2015. 338-342.

SCHREIBER, T. 2000. Measuring information transfer. *Physical review letters,* 85**,** 461.

SCHWEIKART, L. 1991. US commercial banking: a historiographical survey. *The Business History Review***,** 606-661.

SENSOY, A. 2019. The inefficiency of Bitcoin revisited: A high-frequency analysis with alternative currencies. *Finance Research Letters,* 28**,** 68-73.

SENSOY, A., SOBACI, C., SENSOY, S. & ALALI, F. 2014. Effective transfer entropy approach to information flow between exchange rates and stock markets. *Chaos, solitons & fractals,* 68**,** 180-185.

SENSOY, A. & TABAK, B. M. 2016. Dynamic efficiency of stock markets and exchange rates. *International Review of Financial Analysis,* 47**,** 353-371.

SHANAEV, S., SHURAEVA, A., VASENIN, M. & KUZNETSOV, M. 2019. Cryptocurrency value and 51% attacks: evidence from event studies. *The Journal of Alternative Investments,* 22**,** 65-77.

SHANNON, C. E. 1948. A mathematical theory of communication. *The Bell system technical journal,* 27**,** 379-423.

SHCHERBAK, S. 2014. How should Bitcoin be regulated. *Eur. J. Legal Stud.,* 7**,** 41.

SIGURDSSON, G., GIARETTA, A. & DRAGONI, N. Vulnerabilities and Security Breaches in Cryptocurrencies. International Conference in Software Engineering for Defence Applications, 2018. Springer, 288-299.

STOSIC, D., STOSIC, D., LUDERMIR, T. B. & STOSIC, T. 2018. Collective behavior of cryptocurrency price changes. *Physica A: Statistical Mechanics and its Applications,* 507**,** 499-509.

TIWARI, A. K., JANA, R., DAS, D. & ROUBAUD, D. 2018. Informational efficiency of Bitcoin—An extension. *Economics Letters,* 163**,** 106-109.

URQUHART, A. 2016. The inefficiency of Bitcoin. *Economics Letters,* 148**,** 80-82.

VASEK, M., BONNEAU, J., CASTELLUCCI, R., KEITH, C. & MOORE, T. 2016. The Bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets. *Financial Cryptography and Data Security, Lecture Notes in Computer Science. Springer*.

VASEK, M. & MOORE, T. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. International conference on financial cryptography and data security, 2015. Springer, 44-61.

VASEK, M., THORNTON, M. & MOORE, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. International conference on financial cryptography and data security, 2014. Springer, 57-71.

VIDAL-TOMÁS, D. & IBAÑEZ, A. 2018. Semi-strong efficiency of bitcoin. *Finance Research Letters,* 27**,** 259-265.

WANG, J., HOU, X., LI, K. & DING, Y. 2017. A novel weight neighborhood centrality algorithm for identifying influential spreaders in complex networks. *Physica A: Statistical Mechanics and its Applications,* 475**,** 88-105.

WEIMANN, G. 2016. Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism,* 39**,** 195-206.

WRAY, L. R. 2012. Introduction to an alternative history of money. Levy Economics Institute. Working Paper.

XIA, P., WANG, H., ZHANG, B., JI, R., GAO, B., WU, L., LUO, X. & XU, G. 2020. Characterizing cryptocurrency exchange scams. *Computers & Security,* 98**,** 101993.

ZARGAR, F. N. & KUMAR, D. 2019. Informational inefficiency of Bitcoin: A study based on high-frequency data. *Research in International Business and Finance,* 47**,** 344-353.

ZENG, A. & ZHANG, C.-J. 2013. Ranking spreaders by decomposing complex networks. *Physics Letters A,* 377**,** 1031-1035.

ZENG, T., YANG, M. & SHEN, Y. 2020. Fancy Bitcoin and conventional financial assets: Measuring market integration based on connectedness networks. *Economic Modelling,* 90**,** 209-220.

ZHANG, D. & BROADSTOCK, D. C. 2018. Global financial crisis and rising connectedness in the international commodity markets. *International Review of Financial Analysis*.

ZIĘBA, D. & ŚLEDZIEWSKA, K. 2018. Are demand shocks in Bitcoin contagious?

Appendix

A. Supplement to Chapter 2

Table 1 - 1: summary of the relevant literature.

Group	Authors	Summary of points of view
Group A	Moore and Christin (2013)	Security breach is more likely to target well-known platforms.
	Möser et al., (2013)	Bitcoin can be used for illegal activities such as money laundering.
	Vasek et al. (2014)	DDoS attack was more likely to target platform services, e-wallets and large mining pools.
	Huang et al., 2014)	Mining botnets are other methods for cybercriminals that impact the Bitcoin mining activities.
	Pinzón and Rocha, (2016)	The influence of double-spend attacks in cryptocurrencies market.
	Rosati et al. (2017)	Cyberattacks could not be predicted, either when they happen or how many times they could occur.
	Conti et al. (2018)	Bitcoin platform, wallet, and mining activities can be influenced from several forms of cyber attacks.
	Feder et al. (2018a)	Trading activities were affected on the day the denial-of-service occurred.
	Feder et al. (2018b)	The price of the Bitcoin in Mt.Gox was subject to manipulation.
	Griffin and Shams (2018)	Bitcoin and other cryptocurrencies prices had been manipulated, by using Tether as a tool to offer price support.
	Shanaev et al. (2019)	They concluded that there were 'pump and dump' schemes after each cyber attack.
	Corbet et al. (2019b)	Reviewed the published literature based on the cryptocurrencies market and they identified 10 research gaps in the current literature.
	Chainalysis, 2020	Bitcoin cab be used for terrorism financing and darknet markets.
	Caporale et al. (2020a)	They claimed that cyberattacks can affect cryptocurrencies platforms in all countries included in their study.
	Azqueta-Gavaldón (2020)	There was a unidirectional causal between narratives related to cybercrimes and prices.
	Caporale et al. (2020b)	They argued for the probability of cryptocurrencies being influenced negatively by cyberattacks.
	Caporale et al. (2021)	They were able to show that cyberattacks increase the linkages among three major cryptocurrencies and they also addressed the leading role of Bitcoin.
Group B	Ober et al. (2013)	Adopted network theory to examine the degree of anonymity in Bitcoin.
	Lischke and Fabian (2016)	The small-world phenomenon can be present in the Bitcoin network.

	Zięba and Śledziewska (2018)	Bitcoin plays crucial roles in the cryptocurrency market.
	Francés et al.,(2018)	Ethereum has a vital role and plays as a benchmark currency instead of Bitcoin.
	Stosic et al. (2018)	The cryptocurrency market has a unique behaviour that can differ from other financial markets.

Note: group A represents the literature that addresses the impact of security breaches that targeted Bitcoin markets. On the other hand, group B highlight the works that adopted network theory to analyse the Bitcoin market.

Table A 2: The countries included in the paper, respective currency symbols, and the Bitcoin platform.

No.	*Country*	*Currency*	*Bitcoin Platform*		
1	Australia	AUD	Btcmarkets	Mt.Gox	
2	Brazil	BRL	Mercado Bitcoin		
3	Canada	CAD	Mt.Gox	quadrigacx	
4	China	CNY	Btcchina		
5	Europe	EUR	Kraken		
6	British	GBP	Coinfloor	Mt.Gox	
7	Japan	JPY	Mt.Gox	btcbox	Bitflyer
8	South Korea	KRW	Korbit		
9	Polish	PLN	bitbay		
10	Russia	RUB	BTCe	CEX.IO	
11	Singapore	SGD	FYB-SG		
12	United States	USD	Bitstamp		
13	South Africa	ZAR	BitX		
14	Vietnam	VND	VBTC		

Table A 3: Summary statistics, Bitcoin exchange rate returns

Exchange Rate	Mean	Maximum	Minimum	Std. Dev.	Skewness	Kurtosis	Jarque-Bera	Prob
CAD	0.0011	0.0946	-0.1228	0.0150	-0.57	13.8	6538.8	0.0
USD	0.0011	0.0914	-0.1142	0.0149	-0.41	11.3	3884.9	0.0
GBP	0.0006	0.2716	-0.2071	0.0205	-0.66	47.5	110847.0	0.0
JPY	0.0006	0.2749	-0.1985	0.0204	-0.57	48.6	116388.2	0.0
AUD	0.0011	0.0993	-0.1357	0.0155	-0.53	14.0	6860.5	0.0
EUR	0.0011	0.0908	-0.1122	0.0144	-0.37	12.0	4598.1	0.0
PLN	0.0011	0.0976	-0.1082	0.0137	-0.25	13.1	5768.2	0.0
KRW	0.0011	0.1286	-0.1368	0.0164	-0.11	16.8	10624.0	0.0
RUB	0.0013	0.1905	-0.2026	0.0202	0.29	27.1	32467.8	0.0
SGD	0.0010	0.1457	-0.1712	0.0298	-0.05	7.7	1253.3	0.0
CNY	0.0011	0.1456	-0.1246	0.0167	-0.04	19.0	14406.7	0.0
BRL	0.0012	0.1066	-0.1119	0.0141	-0.05	17.0	11028.8	0.0
VND	0.0013	0.2459	-0.2117	0.0249	0.12	17.7	12041.6	0.0
ZAR	0.0012	0.1657	-0.1671	0.0231	0.55	14.6	7589.6	0.0

Figure A 2: The three major areas of study considered in this paper.

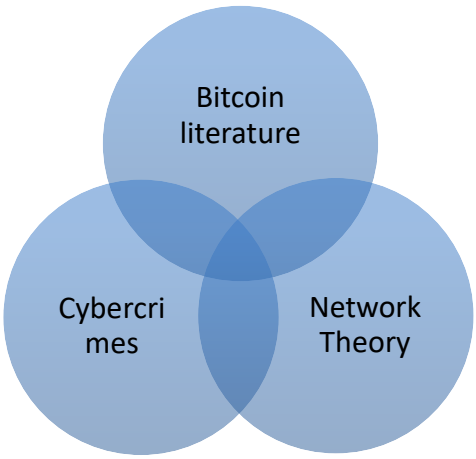
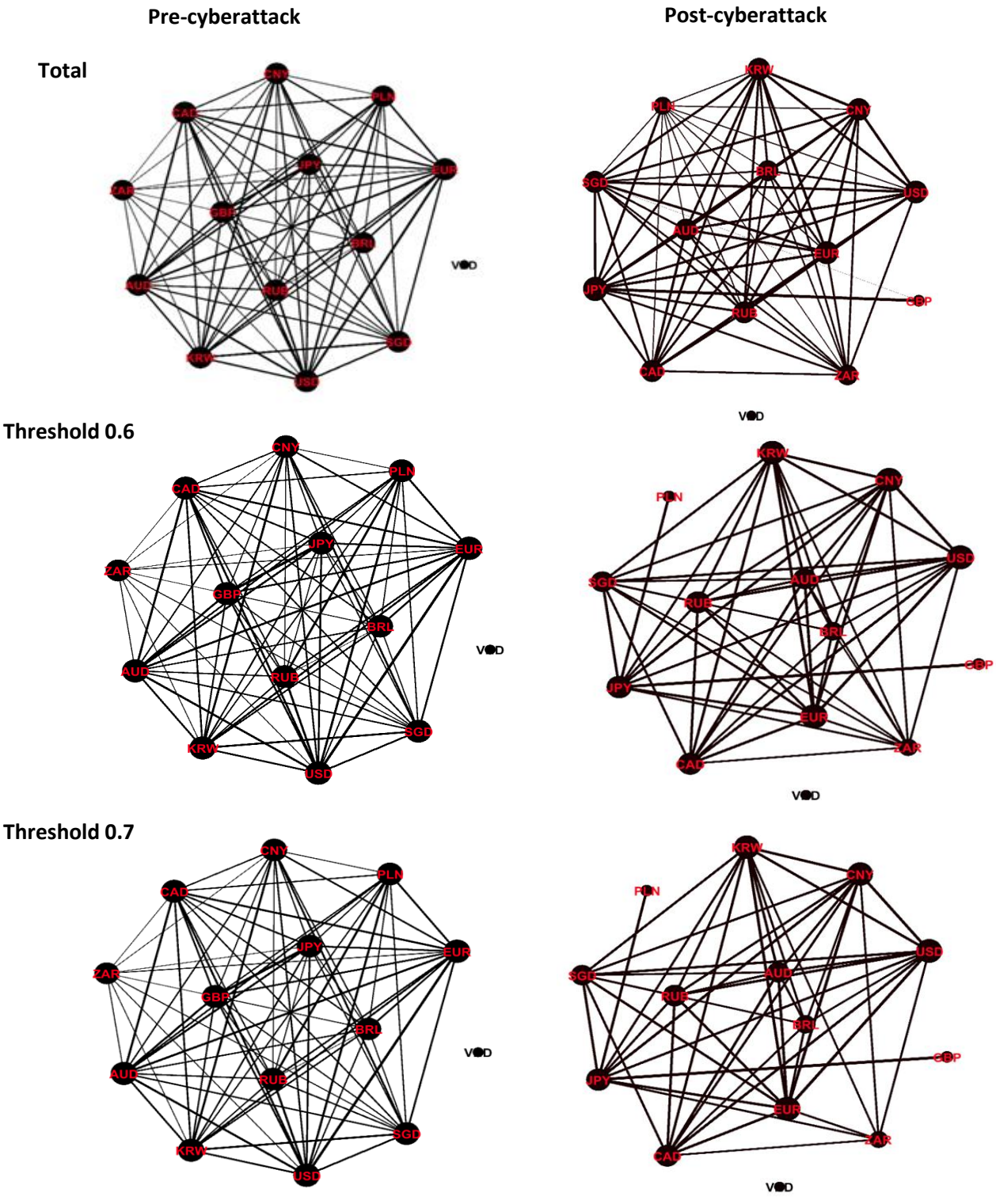


Figure A 3: The Bitcoin cross-market prices pre- and post-cyber-attacks on Mt.Gox platform



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 4: The key factor of the topological features to cross-market Bitcoin prices network pre- and post- cyberattacks on Mt.Gox platform 2014.

	Pre the cybercrime			Post the cybercrime		
Threshold	*Total*	*0.6*	*0.7*	*Total*	*0.6*	*0.7*
Edges	*78*	*78*	*78*	*68*	*57*	*49*
Average Degree	*11.1*	*11.1*	*11.1*	*9.7*	*8.1*	*7*
Avg. Weighted Degree	*9.9*	*9.9*	*9.9*	*7.5*	*6.7*	*5.9*
Graph Density	*0.85*	*0.85*	*0.85*	*0.75*	*0.63*	*0.54*

Note: The table represents the summary of basic topological features pre- and post-cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

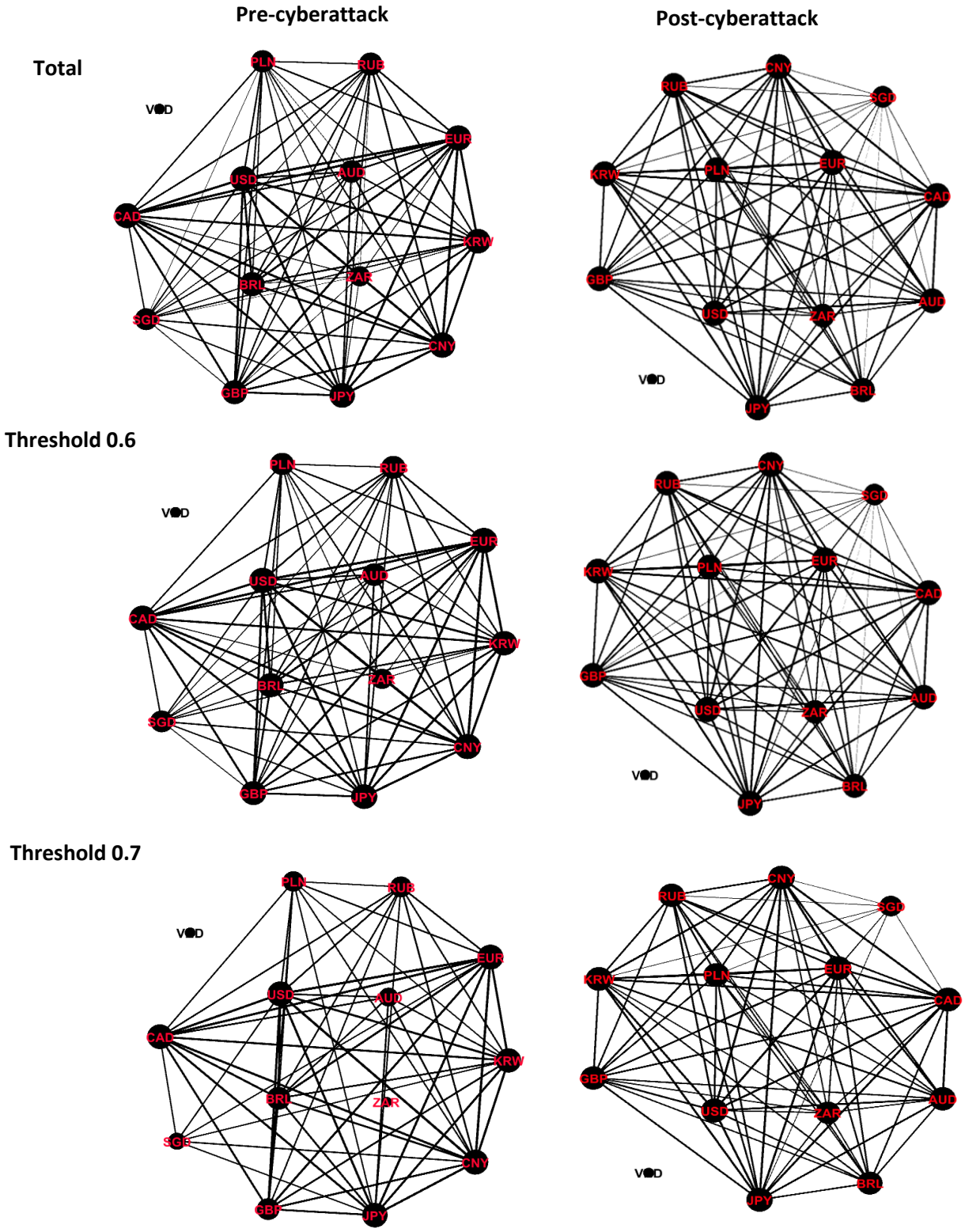
Table A 5: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post- cyberattacks on Mt.Gox platform 2014 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	USD	USD	USD	post-cyberattacks	EUR	EUR	EUR	EUR	EUR
	EUR	EUR	EUR	EUR	EUR		USD	USD	USD	USD	USD
	JPY	JPY	JPY	JPY	JPY		CNY	CNY	CNY	CNY	CNY
	AUD	AUD	AUD	AUD	AUD		KRW	KRW	KRW	KRW	KRW
	GBP	GBP	GBP	GBP	GBP		CAD	CAD	CAD	JPY	JPY

Table A 6: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Mt.Gox platform 2014 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	USD	USD	USD	post-cyberattacks	EUR	EUR	EUR	EUR	EUR
	EUR	EUR	EUR	EUR	EUR		USD	USD	USD	USD	USD
	JPY	JPY	JPY	JPY	JPY		CNY	CNY	CNY	CNY	CNY
	AUD	AUD	AUD	AUD	AUD		KRW	KRW	KRW	KRW	KRW
	PLN	PLN	PLN	PLN	PLN		RUB	RUB	RUB	RUB	RUB

Figure A 4: The Bitcoin cross-market price network pre- and post-cybercrime on Bitstamp platform.



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 7: Key factor of topological features to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015.

	Pre the cybercrime			**Post the cybercrime**		
threshold	Total	0.6	0.7	Total	0.6	0.7
edges	78	70	58	78	78	74
average degree	11.1	10	8.3	11.2	11.2	10.6
Avg. weighted degree	8.6	8	6.9	9.8	9.8	9.5
Graph Density	0.86	0.77	0.64	0.86	0.86	0.81

Note: The table represents the summary of basic topological features pre- and post-cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

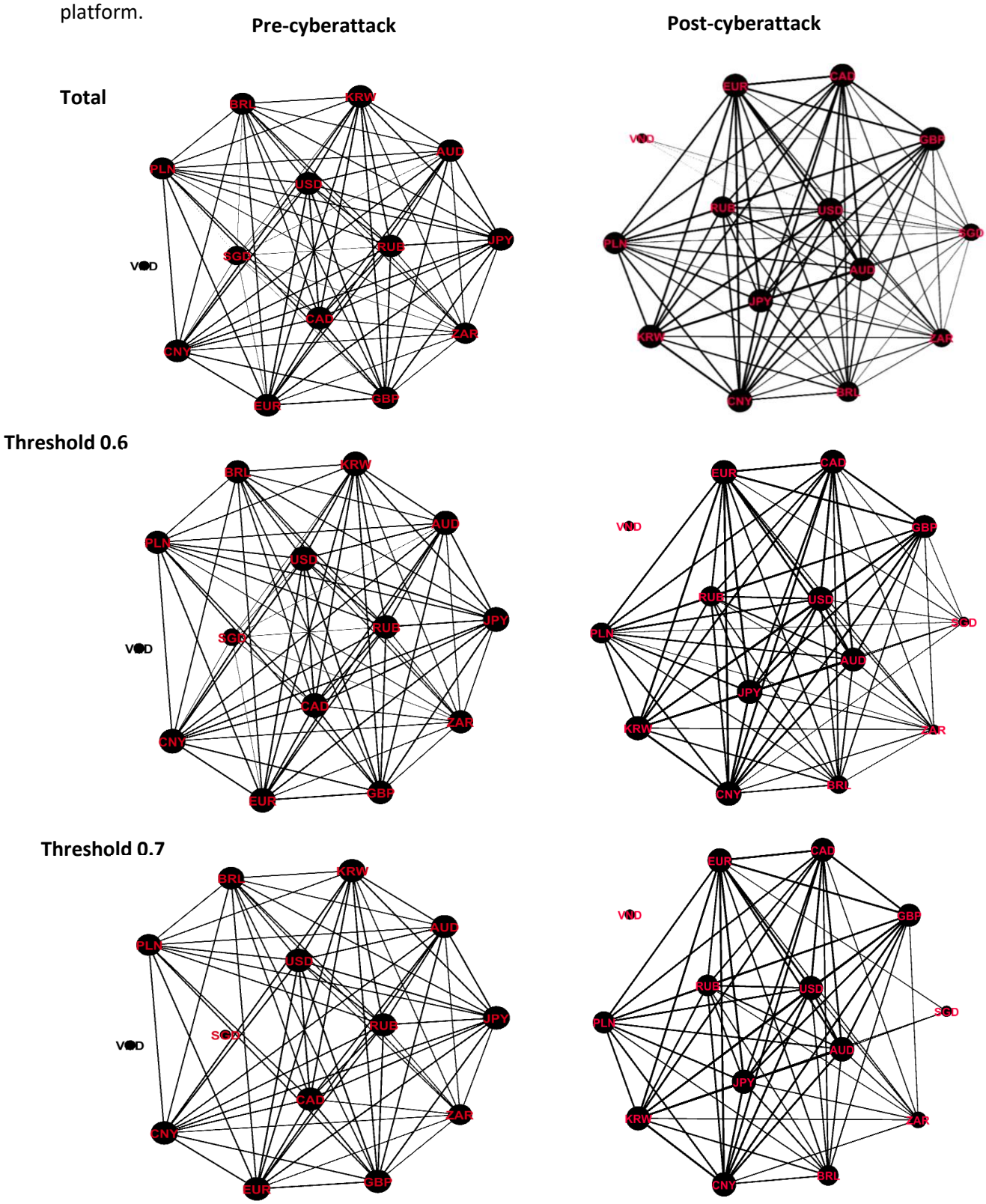
Table A 8: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	EUR	EUR	EUR	EUR	EUR	post-cyberattacks	JPY	CNY	USD	USD	USD
	USD	USD	USD	USD	USD		USD	CAD	JPY	JPY	JPY
	CNY	CNY	CNY	CNY	CNY		BRL	KRW	EUR	EUR	EUR
	CAD	CAD	CAD	CAD	CAD		AUD	AUD	CNY	CNY	CNY
	KRW	KRW	KRW	KRW	KRW		CAD	GBP	CAD	CAD	CAD

Table A 9: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	EUR	EUR	EUR	EUR	EUR	post-cyberattacks	USD	USD	USD	USD	USD
	USD	USD	USD	USD	USD		CNY	CNY	CNY	CNY	CNY
	CNY	CNY	CNY	CNY	CNY		CAD	CAD	CAD	CAD	CAD
	CAD	CAD	CAD	CAD	CAD		JPY	JPY	EUR	EUR	EUR
	JPY	JPY	KRW	KRW	JPY		KRW	KRW	KRW	KRW	KRW

Figure A 5: The Bitcoin cross-market price network pre- and post-cybercrime on the Cryptsy platform.



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 10: The key factor of topological features to cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platforms 2016.

	Pre the cybercrime			Post the cybercrime		
threshold	Total	0.6	0.7	Total	0.6	0.7
edges	78	74	65	82	75	67
average degree	11.1	10.5	9.3	11.7	10.7	9.5
Avg. weighted degree	8.6	8.2	7.5	8.6	8.3	7.8
Graph Density	0.86	0.81	0.71	0.9	0.82	0.74

Note: The table represents the summary of basic topological features pre- and post-cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

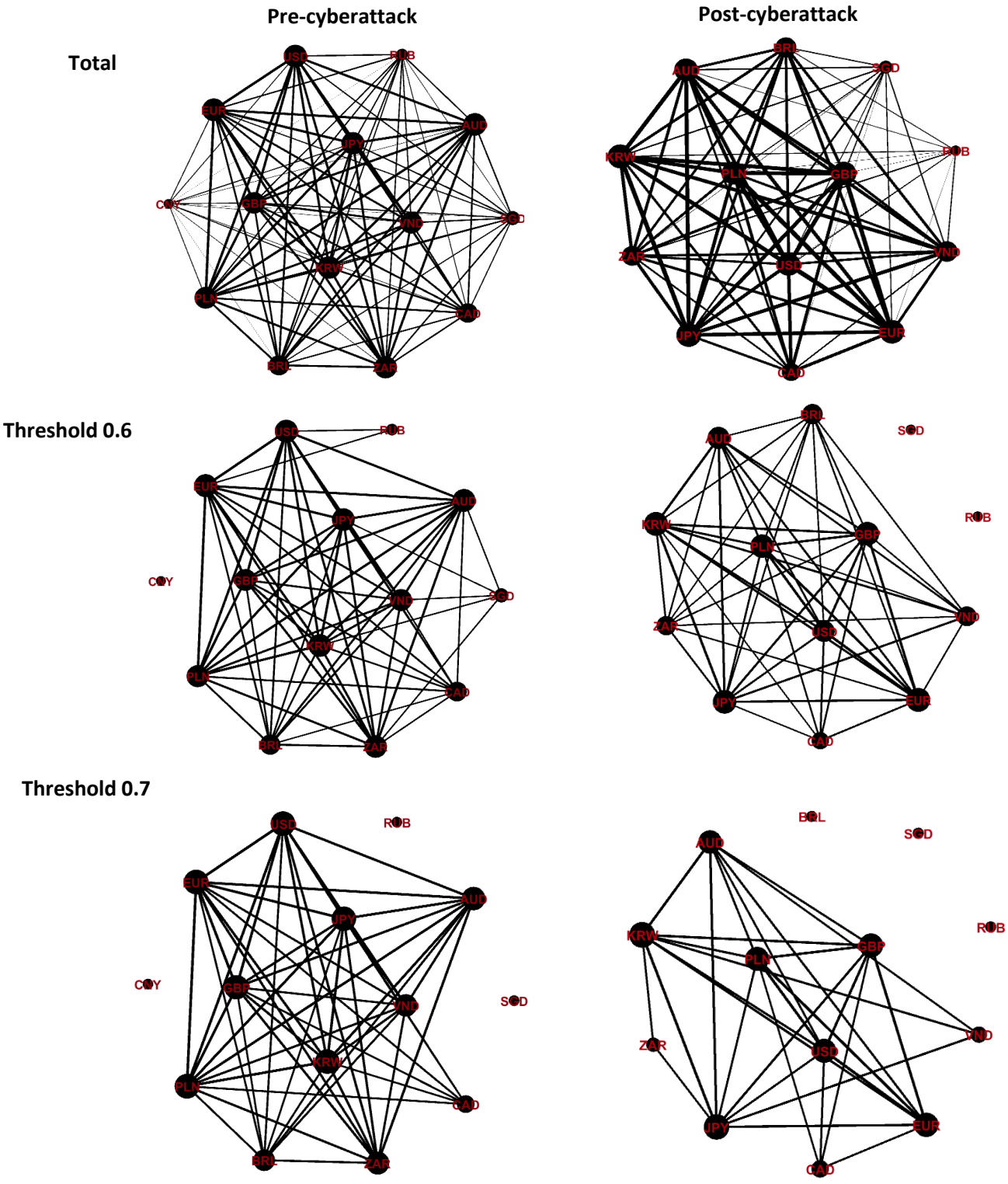
Table A 11: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platforms 2016 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	USD	USD	USD	post-cyberattacks	AUD	EUR	EUR	EUR	EUR
	JPY	JPY	JPY	JPY	JPY		CNY	CNY	CNY	CNY	CNY
	EUR	EUR	EUR	EUR	EUR		EUR	KRW	KRW	KRW	KRW
	CNY	CNY	CNY	CNY	CNY		JPY	USD	USD	USD	USD
	CAD	CAD	CAD	CAD	CAD		KRW	JPY	JPY	JPY	JPY

Table A 12: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platforms 2016 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	USD	USD	USD	post-cyberattacks	EUR	EUR	EUR	EUR	EUR
	EUR	EUR	EUR	EUR	EUR		CNY	CNY	CNY	CNY	CNY
	AUD	AUD	AUD	AUD	AUD		KRW	KRW	KRW	KRW	KRW
	PLN	PLN	PLN	PLN	PLN		USD	USD	USD	USD	USD
	GBP	GBP	GBP	GBP	GBP		JPY	JPY	JPY	JPY	JPY

Figure A 6: The Bitcoin cross-market price network pre- and post-cybercrime on Bitfinex platform.



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 13: The key factor of topological features to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitfinex platform 2016.

	Pre the cybercrime			Post the cybercrime		
threshold	Total	0.6	0.7	Total	0.6	0.7
edges	91	62	51	76	49	30
average degree	13	8.85	7.28	11.69	7.53	4.6
Avg. weighted degree	9.2	7.28	6.28	7.33	5.71	3.8
Graph Density	1	0.68	0.56	0.97	0.62	0.38

Note: The table represents the summary of basic topological features pre- and post- cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

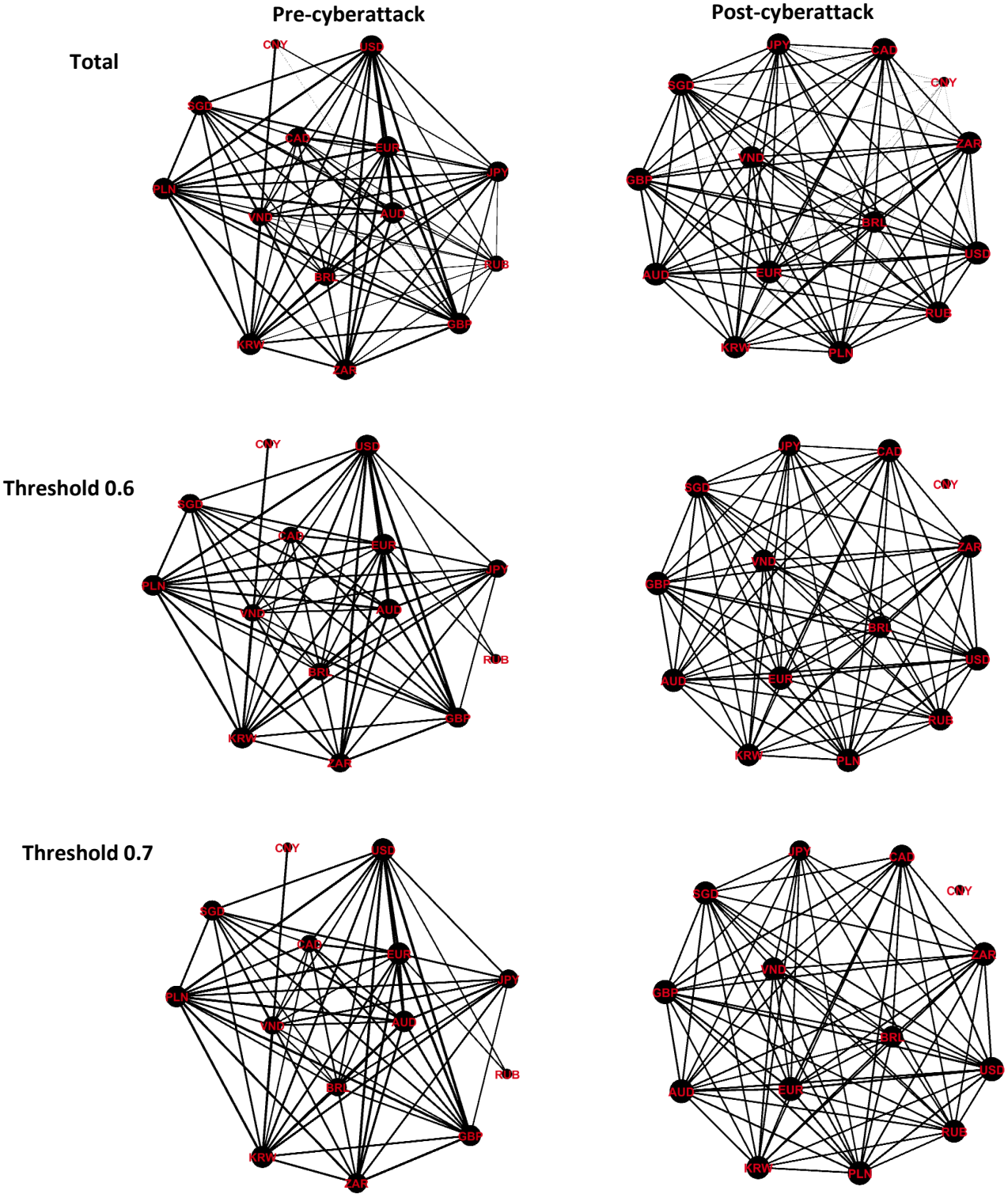
Table A 14: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Bitfinex platform 2016 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	AUD	USD	USD	post-cyberattacks	EUR	EUR	EUR	EUR	EUR
	EUR	EUR	JPY	EUR	EUR		KRW	KRW	KRW	KRW	KRW
	AUD	AUD	KRW	AUD	AUD		JPY	JPY	JPY	JPY	JPY
	KRW	KRW	EUR	KRW	KRW		GBP	GBP	GBP	GBP	GBP
	JPY	JPY	USD	JPY	JPY		PLN	PLN	PLN	PLN	PLN

Table A 15: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Bitfinex platform 2016 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	USD	JPY	EUR	PLN	post-cyberattacks	JPY	JPY	EUR	JPY	KRW
	EUR	EUR	KRW	JPY	EUR		KRW	KRW	GBP	KRW	JPY
	JPY	JPY	EUR	USD	USD		AUD	AUD	JPY	USD	EUR
	GBP	GBP	GBP	KRW	KRW		EUR	EUR	KRW	EUR	USD
	KRW	KRW	PLN	GBP	JPY		GBP	GBP	PLN	GBP	GBP

Figure A 7: The Bitcoin cross-market price network pre- and post-cybercrime on Yapizon platform.



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 16: Key factor of topological features to cross-market Bitcoin prices network pre- and post-cyberattacks on Yapizon platform 2017.

	Pre the cybercrime			Post the cybercrime		
threshold	Total	0.6	0.7	Total	0.6	0.7
edges	81	66	48	85	78	76
average degree	11.5	9.42	6.85	12.1	11.1	10.9
Avg. weighted degree	8.28	7.21	5.54	9.2	9.2	9
Graph Density	0.89	0.72	0.52	0.93	0.86	0.84

Note: The table represents the summary of basic topological features pre- and post-cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

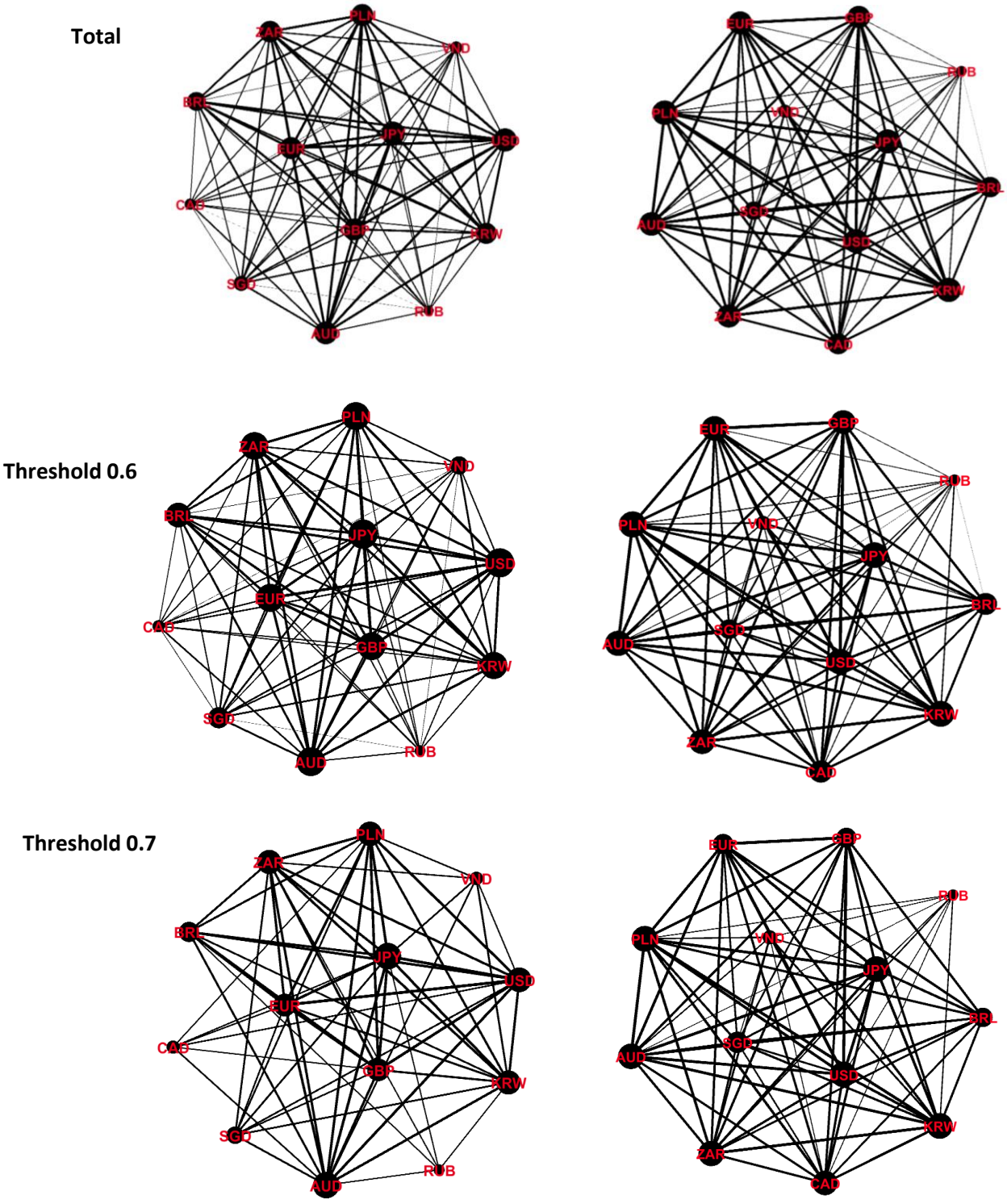
Table A 17: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post- cyberattacks on Yapizon platform 2017 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	USD	KRW	AUD	KRW	USD	post-cyberattacks	USD	USD	ZAR	USD	USD
	EUR	USD	PLN	EUR	EUR		GBP	GBP	USD	GBP	GBP
	KRW	EUR	USD	USD	KRW		EUR	EUR	EUR	EUR	EUR
	PLN	PLN	KRW	PLN	PLN		ZAR	ZAR	GBP	ZAR	ZAR
	AUD	AUD	ZAR	SGD	AUD		PLN	PLN	PLN	PLN	PLN

Table A 18: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Yapizon platform 2017 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	KRW	KRW	AUD	KRW	AUD	post-cyberattacks	GBP	PLN	GBP	GBP	GBP
	USD	AUD	PLN	AUD	KRW		PLN	GBP	PLN	PLN	PLN
	EUR	USD	USD	PLN	USD		USD	KRW	AUD	AUD	AUD
	AUD	PLN	KRW	USD	PLN		AUD	SGD	USD	USD	USD
	PLN	JPY	ZAR	SGD	EUR		KRW	ZAR	EUR	KRW	KRW

Figure A 8: The Bitcoin cross-market price network pre- and post-cybercrime on Zaif platform.



Note: the thickness of edges' lines reflects the strength of correlation between Bitcoin exchange rates.

Table A 19: Key factor of topological features to cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018.

	Pre the cybercrime			Post the cybercrime		
threshold	Total	0.6	0.7	Total	0.6	0.7
edges	78	76	61	78	78	71
average degree	12	11.6	9.4	12	12	10.9
Avg. weighted degree	10.41	10.2	8.4	10.8	10.8	9.9
Graph Density	1	0.97	0.78	1	1	0.91

Note: The table represents the summary of basic topological features pre- and post-cyberattacks for the total significant correlation in the network and different threshold levels (θ>0.6 and θ>0.7).

Table A 20: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018 for θ>0.6.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	JPY	JPY	JPY	JPY	JPY	post-cyberattacks	PLN	PLN	PLN	PLN	PLN
	USD	USD	USD	USD	USD		KRW	KRW	KRW	KRW	KRW
	AUD	AUD	AUD	AUD	AUD		USD	USD	USD	JPY	USD
	PLN	PLN	EUR	PLN	PLN		CAD	CAD	CAD	USD	JPY
	EUR	EUR	PLN	EUR	EUR		JPY	JPY	JPY	CAD	CAD

Table A 21: Summary of centrality measurement results of cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018 for θ>0.7.

	CC	*BC*	*EC*	*DC*	*WDC*		*CC*	*BC*	*EC*	*DC*	*WDC*
pre-cyberattack	JPY	JPY	JPY	JPY	JPY	post-cyberattacks	PLN	PLN	PLN	KRW	PLN
	USD	USD	USD	USD	USD		KRW	KRW	KRW	PLN	USD
	AUD	AUD	AUD	AUD	AUD		USD	USD	BRL	JPY	JPY
	PLN	PLN	PLN	PLN	PLN		JPY	JPY	JPY	ZAR	KRW
	EUR	EUR	EUR	EUR	EUR		EUR	EUR	USD	BRL	EUR

Figure A 9: The Probability distribution of Bitcoin cross market price correlation matrices during the period of cybercrime on Mt.Gox platform.

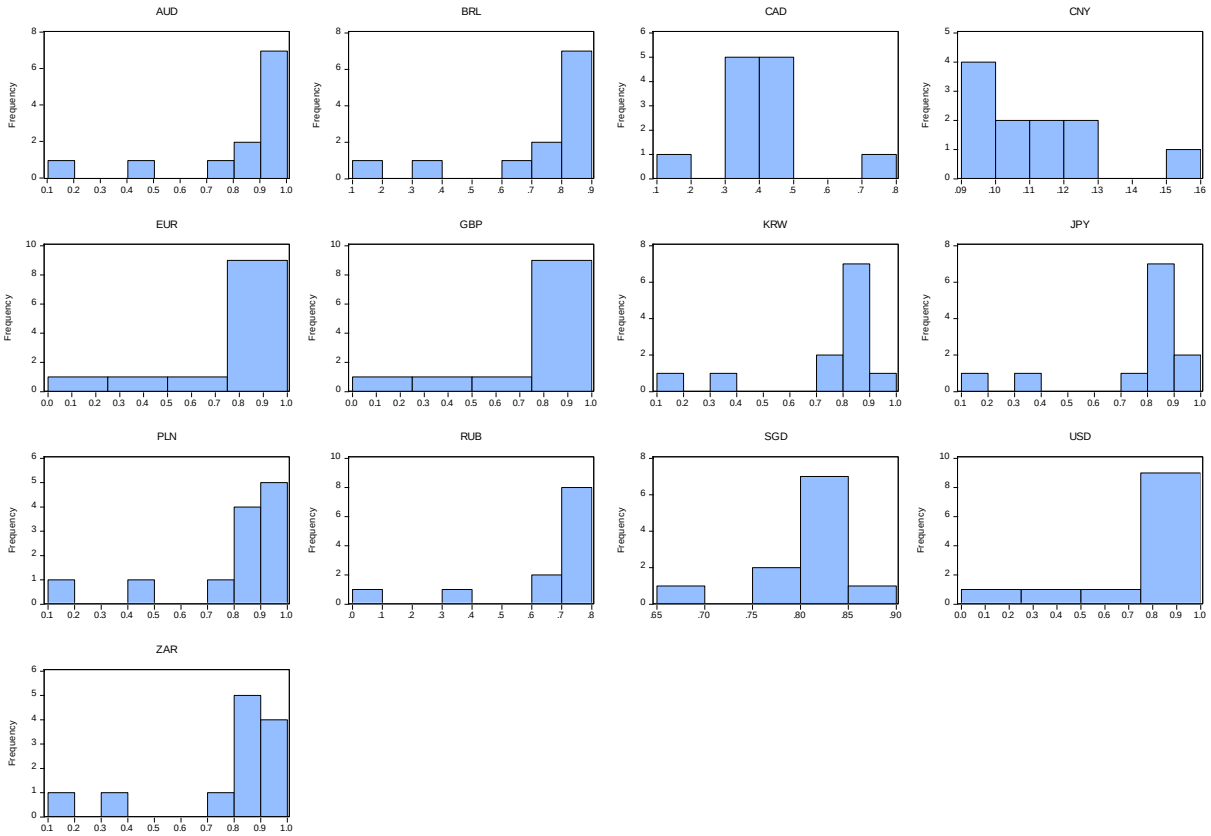
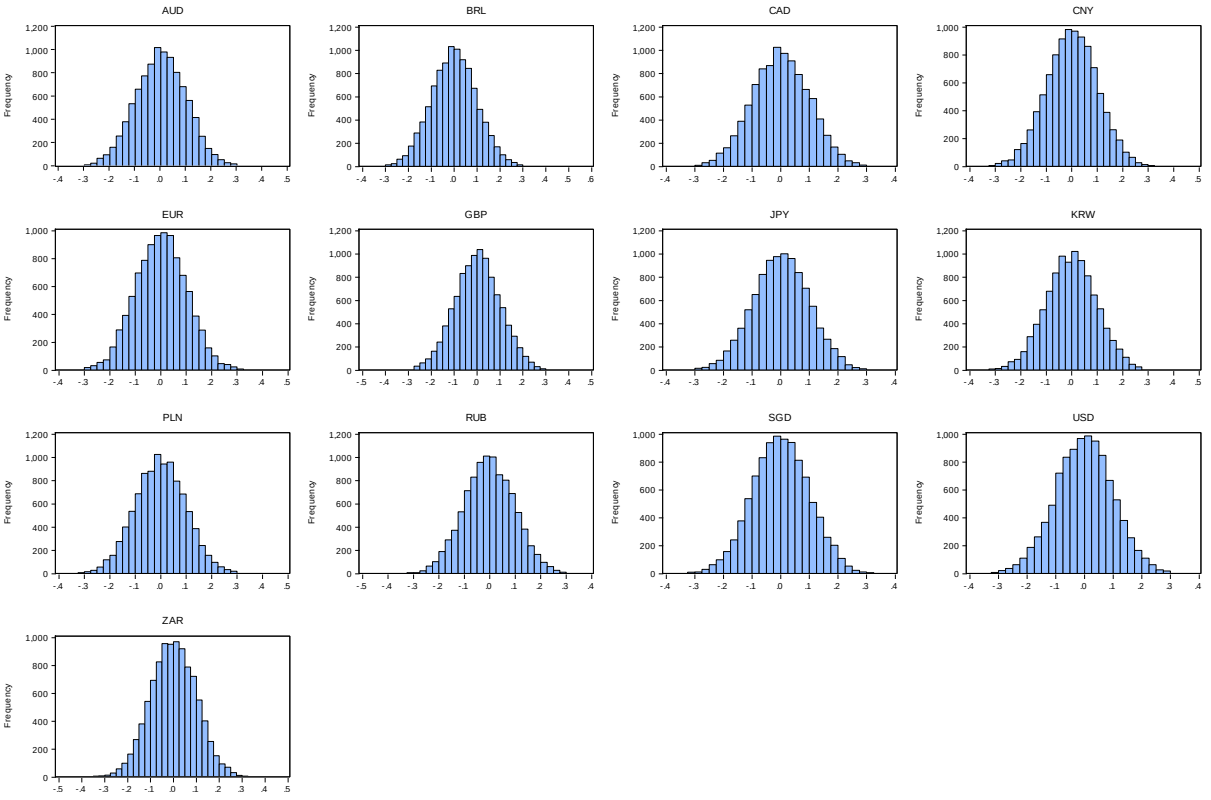


Figure A 10: The Probability distribution of Bitcoin cross market price based on randomized correlation matrices during the period of cybercrime on Mt.Gox platform.



B. Supplement to Chapter 3

Table 1 - 2: summary of the relevant literature.

Group	Authors	Summary of points of view
Group A	Martin and Christin (2016)	The immoral uses of cryptocurrencies have led to an increase in the number of related ethical problems
	Pinzón and Rocha, (2016)	the influence of double-spend attacks in cryptocurrencies market
	Corbet et al. (2019a)	the correlations between cryptocurrencies increase after cyberattack
	Shanaev et al. (2019)	They concluded that there were 'pump and dump' schemes after each cyber attack
	Corbet et al. (2019b)	reviewed the published literature based on the cryptocurrencies market and they identified 10 research gaps in the current literature
	Chainalysis, 2020	terrorism financing and darknet markets
	Caporale et al. (2020a)	They claimed that cyberattacks can affect cryptocurrencies platforms in all countries included in their study.
	Azqueta-Gavaldón (2020)	there was a unidirectional causal between narratives related to cybercrimes and prices
	Caporale et al. (2020b)	They argued for the probability of cryptocurrencies being influenced negatively by cyberattacks
Group B	Koutmos (2018)	that cryptocurrencies had become more interconnected, and the risk of contagion become significantly possible
	Ji et al.,(2019b)	addressed the weak linkage between energy commodities and the top five cryptocurrencies included in the study
	Gillaizeau et al. (2019b)	Tracked the effects of volatility spillover among the top five cross-market Bitcoin prices.
	Ji et al. (2019)	they constructed a network to show the information spillover between various commodities and five major cryptocurrencies
	Katsiampa et al. (2019)	They found that Bitcoin transfers its shock effects to cryptocurrencies markets.
	Dimpfl and Peter (2019)	investigated the differences between using linear methods and nonlinear approaches to detect information transfer
	Borri and Shakhnov (2020)	Pointed out that if the country adjusts the regulations related to the investment in the cryptocurrencies market, that may influence on domestic and international cryptocurrency markets.
	Huynh et al. (2020)	Employed Transfer Entropy to examine the spillover between gold and 14 different types of cryptocurrencies.
	Gkillas et al. (2020)	identified the spillover effect after using high-frequency data between crude oil, gold, and Bitcoin
	Qureshi et al. (2020)	asserted that the dependency between cryptocurrencies has increased
	Caporale et al. (2021)	they were able to show that cyberattacks increase the linkages among three major cryptocurrencies and they also addressed the leading role of Bitcoin

Note: group A represents the literature that addresses the impact of security breaches that targeted Bitcoin markets. On the other hand, group B highlight the works that examined the spillover and contagion in Bitcoin Market.

Table B 1: The countries included in the paper, respective currency symbols, and the Bitcoin platform.

No.	Country	Currency	Bitcoin Platform
1	Australia	AUD	Btcmarkets
2	Brazil	BRL	Mercado Bitcoin
3	Canada	CAD	Quadrigacx Karken
4	China	CNY	Btcchina
5	Europe	EUR	Kraken
6	British	GBP	Coinfloor
7	Japan	JPY	Bitflyer Zaif
8	South Korea	KRW	Korbit
9	Polish	PLN	Bitbay
10	United States	USD	Bitstamp

Table B 2: Summary statistics, cross-market Bitcoin returns for the complete study sample.

	Mean	Median	Max	Min	Std. Dev.	Skewness	Kurtosis	Jarque-Bera	ADF
AUD	0.000274	0.000303	0.0558	-0.0631	0.0075	-0.6642	13.58	16570.59	-34.0942
BRL	0.000282	0.000204	0.0673	-0.0557	0.0068	0.1608	17.83	32092.18	-31.3324
CAD	0.000293	0.000235	0.065	-0.0721	0.0074	-0.4403	12.69	13812.07	-51.1966
CNY	0.000291	0.000256	0.0468	-0.1049	0.0072	-1.6916	26.25	80498.89	-37.2327
GBP	0.000292	0.000416	0.0506	-0.0687	0.0071	-0.7912	14.76	20524	-34.9662
EUR	0.000292	0.000357	0.0606	-0.0547	0.0067	-0.5847	13.64	16707.41	-35.0402
JPY	0.000284	0.000343	0.0525	-0.0939	0.0072	-1.143	21.13	48658.7	-33.8853
KRW	0.000284	0.000251	0.0431	-0.0662	0.0071	-0.767	17.04	29083.41	-30.5328
PLN	0.000286	0.000238	0.0638	-0.1222	0.0066	-1.9412	47.91	296289.7	-27.3008
USD	0.000281	0.000376	0.0488	-0.0543	0.0069	-0.7686	12.61	13804.23	-34.9112

Note: all the values of the Jarque-Bera test and the Augmented Dickey Fuller test are significant at the 1% level.

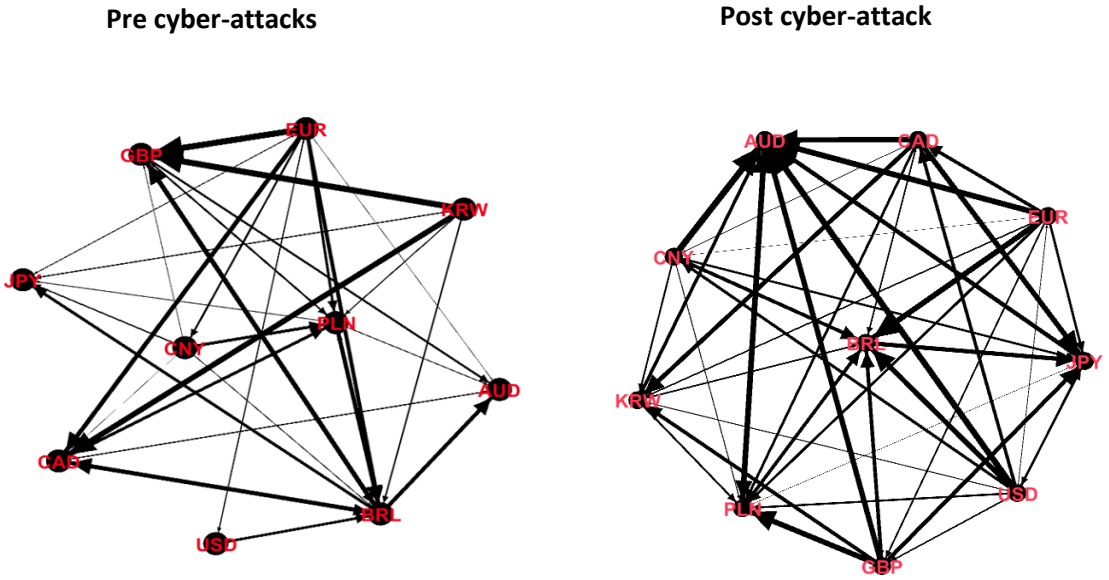
Table B 3: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015.

	Pre the cybercrime	**Post the cybercrime**
Edge	38	58
Avg. Degree	3.8	5.8
Node Strength Degree	0.097	0.16
Graph Density	0.422	0.644

Table B 4: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015.

Pre the Cybercrime				**Post the Cybercrime**			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
BRL	EUR	BRL	EUR	BRL	USD	AUD	USD
PLN	BRL	GBP	BRL	JPY	EUR	BRL	GBP
GBP	PLN	PLN	KRW	AUD	BRL	JPY	EUR
JPY	CNY	CAD	PLN	PLN	CAD	PLN	CAD
AUD	KRW	AUD	CNY	CNY	CNY	KRW	CNY

Figure B 1: The Bitcoin cross-market prices pre and post cyber-attacks on Bitstamp platform based on the Effective Transfer Entropy.



Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

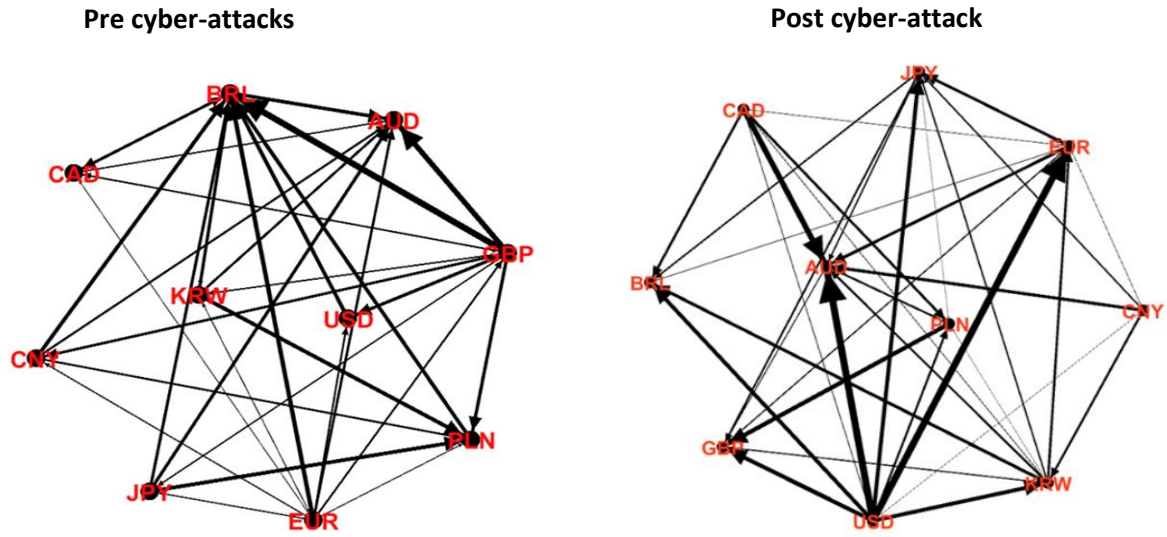
Table B 5: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platform 2016.

	Pre the cybercrime	Post the cybercrime
Edge	39	41
Avg. Degree	3.9	4.1
Node Strength Degree	0.11	0.092
Graph Density	0.433	0.456

Table B 6: Node Strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platform 2016.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
BRL	EUR	BRL	GBP	AUD	USD	AUD	USD
AUD	GBP	AUD	EUR	EUR	KRW	EUR	KRW
PLN	BRL	PLN	KRW	GBP	JPY	GBP	CAD
KRW	KRW	USD	CNY	KRW	CAD	BRL	JPY
CAD	CNY	CAD	BRL	JPY	CNY	JPY	CNY

Figure B 2: The Bitcoin cross-market prices pre and post cyber-attacks on Cryptsy platform based on the Effective Transfer Entropy



Note: the thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

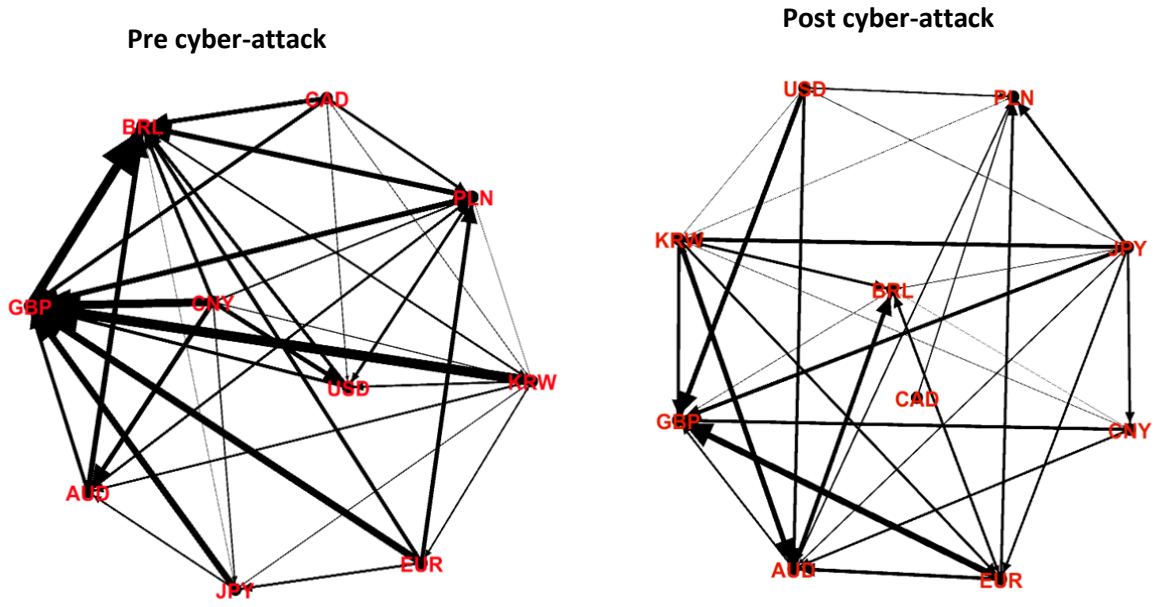
Table B 7: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post- cyberattacks on Bitfinex platform 2016.

	Pre the cybercrime	Post the cybercrime
Edge	31	38
Avg. Degree	3.1	3.8
Node Strength Degree	0.108	0.082
Graph Density	0.344	0.422

Table B 8: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitfinex platform 2016.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
GBP	CNY	GBP	CNY	GBP	JPY	BRL	JPY
BRL	PLN	BRL	EUR	AUD	KRW	AUD	EUR
PLN	EUR	PLN	KRW	PLN	BRL	PLN	KRW
AUD	KRW	AUD	PLN	KRW	EUR	GBP	USD
USD	AUD	USD	AUD	BRL	AUD	KRW	AUD

Figure B 3: The Bitcoin cross-market prices pre and post cyber-attacks on Bitfinex platform based on the Effective Transfer Entropy



Note: the thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

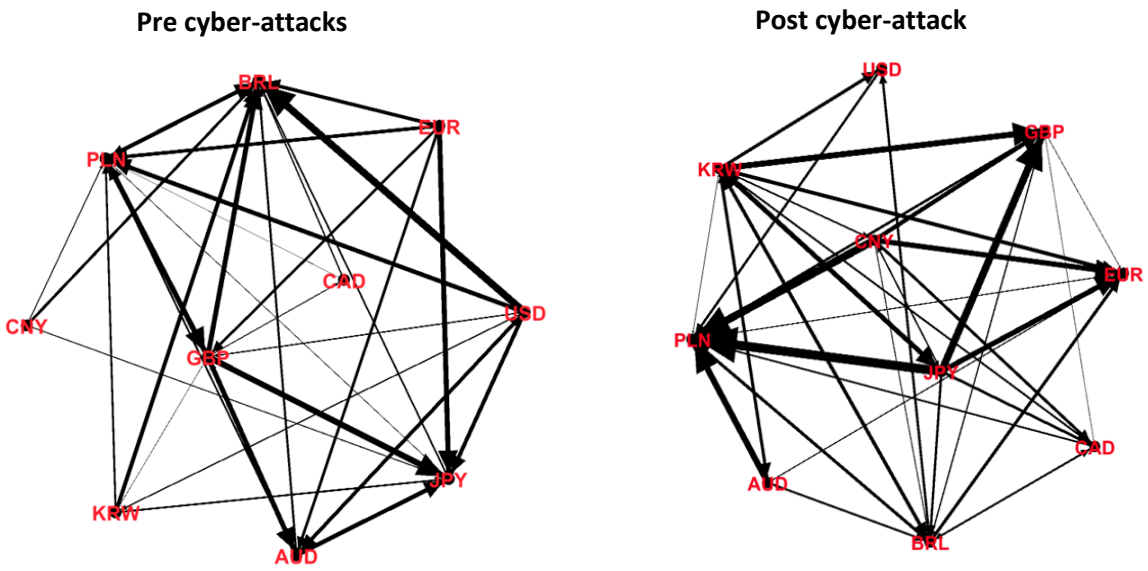
Table B 9: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post- cyberattacks on Yapizon platform 2017.

	Pre the cybercrime	Post the cybercrime
Edge	42	50
Avg. Degree	4.2	5
Node Strength Degree	0.15	0.143
Graph Density	0.467	0.556

Table B 10: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Yapizon platform 2017.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
PLN	USD	BRL	USD	PLN	KRW	PLN	JPY
BRL	GBP	JPY	GBP	BRL	BRL	EUR	KRW
JPY	AUD	PLN	EUR	EUR	JPY	GBP	CNY
GBP	EUR	AUD	AUD	KRW	CNY	BRL	BRL
AUD	PLN	GBP	PLN	JPY	GBP	KRW	AUD

Figure B 4: The Bitcoin cross-market prices pre and post cyber-attacks on Yapizon platform based on the Effective Transfer Entropy



Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

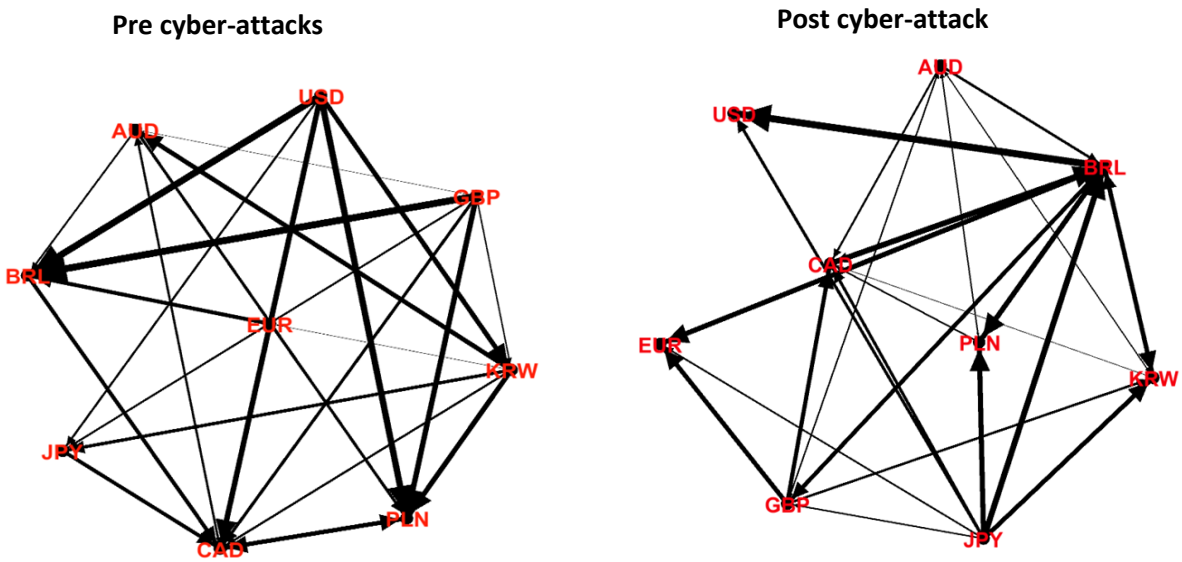
Table B 11: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018.

	Pre the cybercrime	Post the cybercrime
Edge	34	36
Avg. Degree	3.78	4
Node Strength Degree	0.087	0.085
Graph Density	0.47	0.5

Table B 12: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
CAD	KRW	CAD	USD	BRL	BRL	BRL	JPY
PLN	GBP	PLN	GBP	CAD	JPY	CAD	GBP
BRL	CAD	BRL	KRW	GBP	GBP	KRW	AUD
KRW	EUR	JPY	EUR	AUD	AUD	GBP	KRW
JPY	USD	KRW	CAD	KRW	KRW	EUR	PLN

Figure B 5: The Bitcoin cross-market prices pre- cyber-attacks on Zaif platform based on the Effective Transfer Entropy.



Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

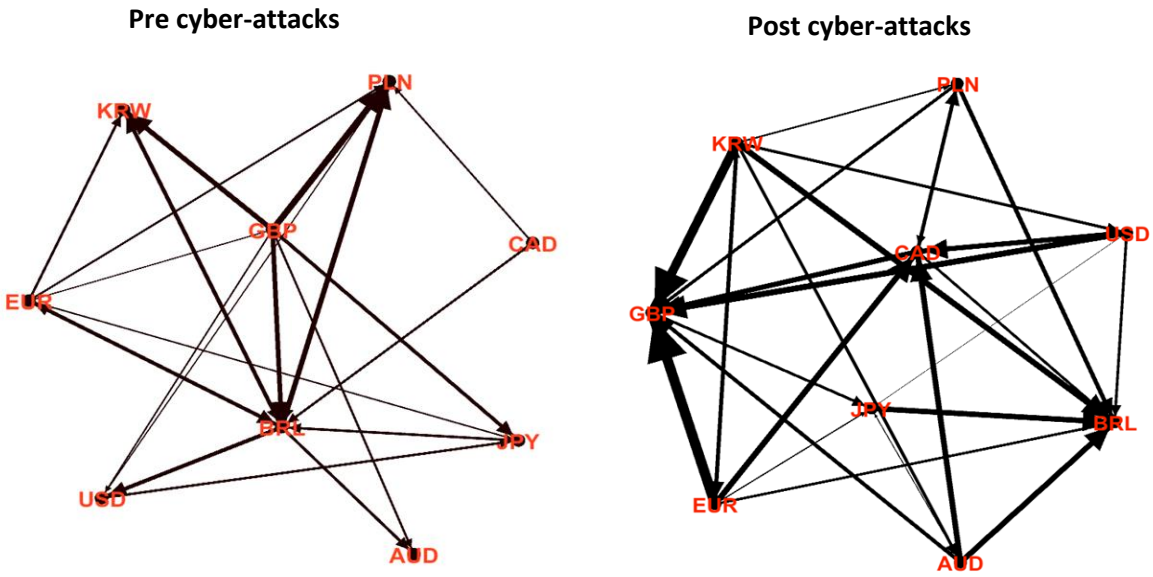
Table B 13: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on LocalBitcoins platform 2019.

	Pre the cybercrime	Post the cybercrime
Edge	24	28
Avg. Degree	2.78	3.1
Node Strength Degree	0.07	0.067
Graph Density	0.33	0.39

Table B 14: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on LocalBitcoins platform 2019.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
PLN	BRL	BRL	GBP	BRL	KRW	GBP	KRW
BRL	GBP	PLN	BRL	GBP	EUR	BRL	EUR
AUD	JPY	KRW	USD	CAD	USD	CAD	AUD
JPY	USD	AUD	JPY	JPY	AUD	JPY	USD
KRW	EUR	JPY	EUR	USD	CAD	PLN	CAD

Figure B 6: The Bitcoin cross-market prices pre- and post-cyberattacks on the LocalBitcoins platform based on the Effective Transfer Entropy.



Note: the thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

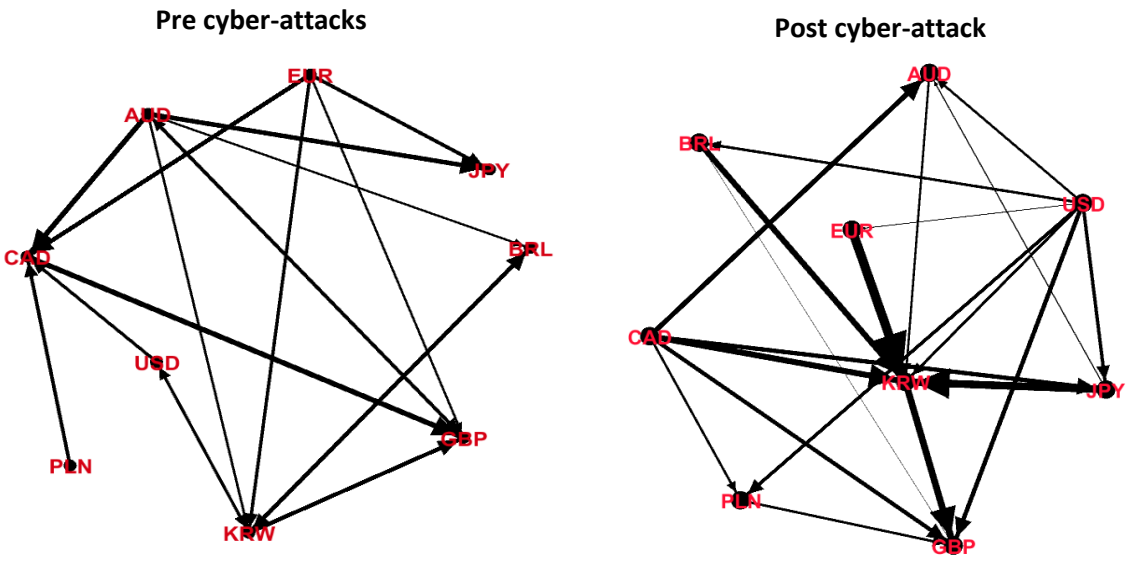
Table B 15: The key factor of topological features based on ETE to cross-market Bitcoin prices network pre- and post- cyberattacks on Binance platform 2019.

	Pre the cybercrime	Post the cybercrime
Edge	18	21
Avg. Degree	2	2.3
Node Strength Degree	0.047	0.046
Graph Density	0.25	0.292

Table B 16: Node strengths based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Binance platform 2019.

Pre the cybercrime				Post the cybercrime			
IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
GBP	KRW	GBP	AUD	KRW	USD	KRW	USD
CAD	AUD	CAD	KRW	GBP	CAD	GBP	CAD
JPY	GBP	KRW	EUR	JPY	KRW	JPY	JPY
KRW	CAD	JPY	CAD	AUD	JPY	AUD	KRW
BRL	USD	BRL	USD	PLN	BRL	PLN	BRL

Figure B 7: The Bitcoin cross-market prices pre and post cyber-attacks on Binance platform based on the Effective Transfer Entropy



Note: the thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates.

Figure B 8: Out-Node strengths of ETE between Bitcoin cross-market prices in time.

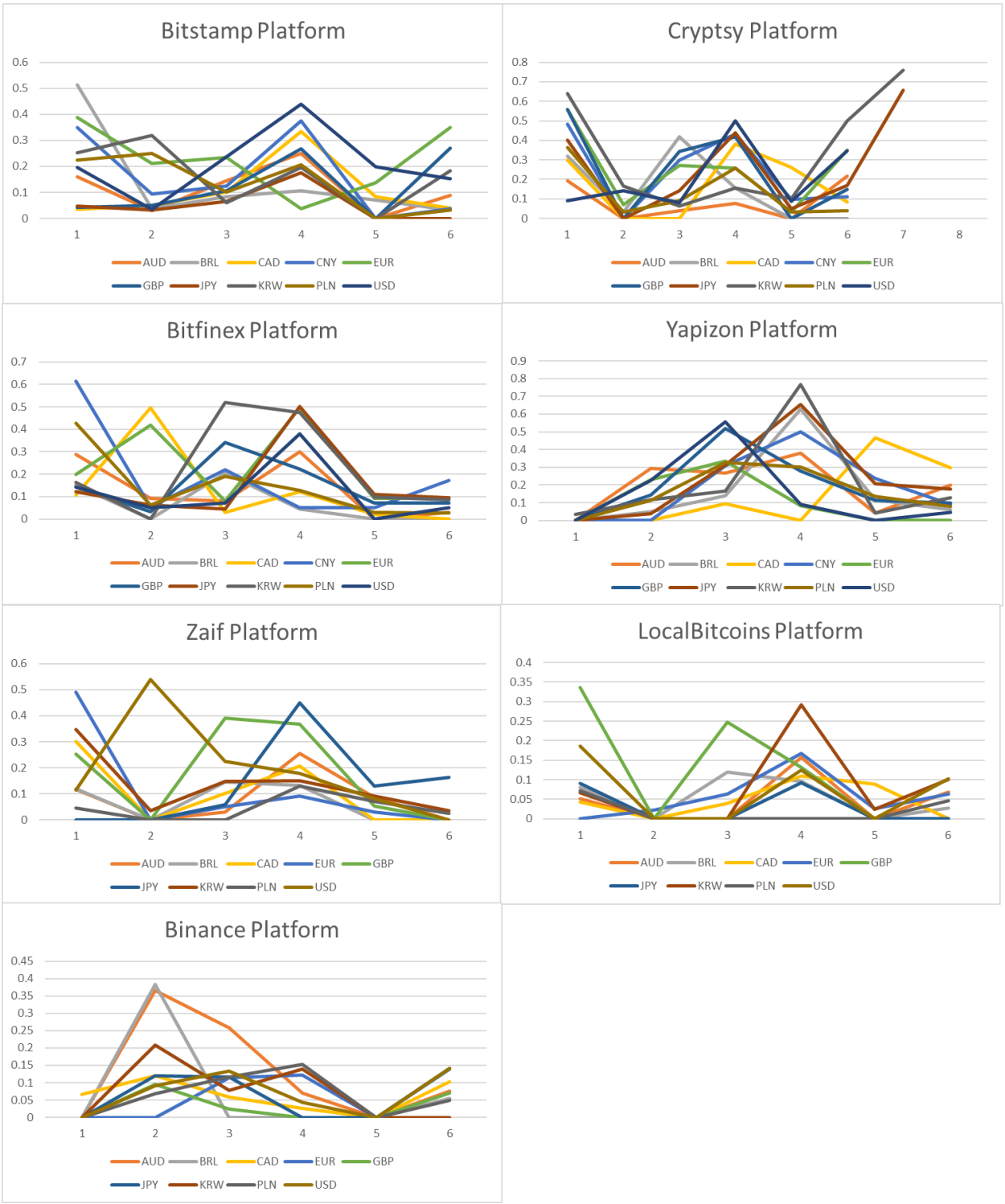


Figure B 9: IN-Node strengths of ETE between Bitcoin cross-market prices in time.

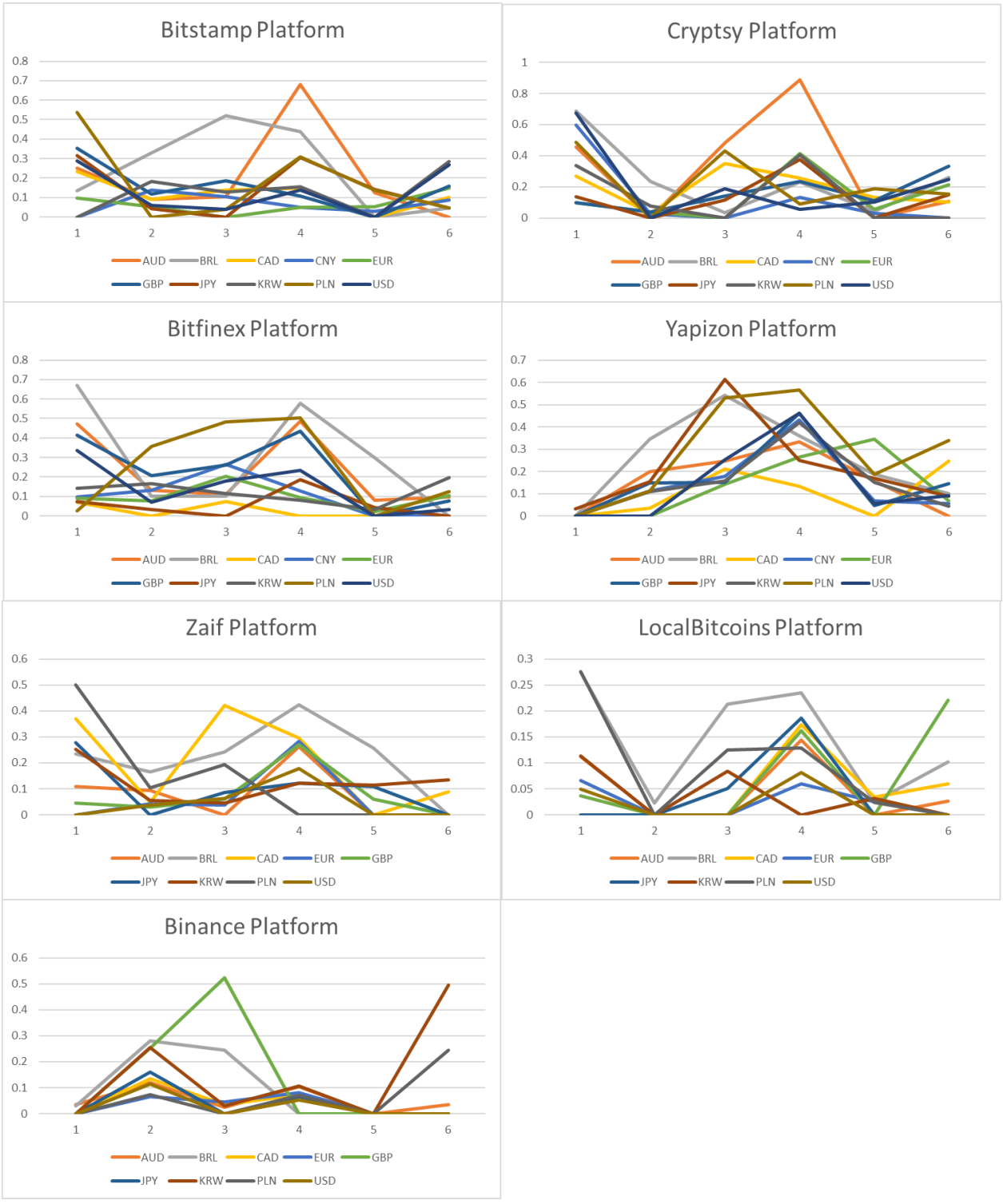


Table B 17: The key factor of topological features based on ETE to cross-market Bitcoin prices in time.

	Period	1	2	3	4	5	6
Bitstamp	Edge	38	25	25	43	10	26
	avg. degree	3.8	2.5	2.5	4.3	1	2.6
	strong degree	0.22	0.11	0.126	0.239	0.049	0.119
	density	0.422	0.278	0.278	0.478	0.11	0.289
Cryptsy	Edge	60	11	28	49	13	33
	avg. degree	6	1.1	2.8	4.9	1.3	3.3
	strong degree	0.39	0.04	0.175	0.31	0.07	0.2
	density	0.667	0.122	0.311	0.544	0.144	0.366
Bitfinex	Edge	45	22	32	39	10	15
	avg. degree	4.5	2.2	3.2	3.9	1	1.5
	strong degree	0.239	0.127	0.179	0.273	0.048	0.063
	density	0.5	0.244	0.356	0.433	0.11	0.16
Yapizon	Edge	1	23	49	53	24	24
	avg. degree	0.1	2.3	4.9	5.3	2.4	2.4
	strong degree	0.003	0.121	0.3	0.368	0.136	0.118
	density	0.01	0.256	0.544	0.589	0.267	0.26
Zaif	Edge	30	9	22	35	9	2
	avg. degree	3.3	1	2.44	3.889	1	0.22
	strong degree	0.198	0.064	0.127	0.218	0.06	0.025
	density	0.417	0.125	0.306	0.486	0.125	0.028
LocalBitcoins	Edge	16	1	9	20	5	11
	avg. degree	1.78	0.011	0.1	2.22	0.056	0.122
	strong degree	0.10	0.002	0.05	0.130	0.015	0.045
	density	0.22	0.014	0.125	0.278	0.069	0.153
Binance	Edge	2	25	17	14	0	14
	avg. degree	0.22	2.7	1.88	1.56	0	1.55
	strong degree	0.007	0.161	0.1	0.061	0	0.086
	density	0.028	0.347	0.236	0.194	0	0.194

Table B 18: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Bitstamp platform 2015.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.2507278	0.090395	0.105223	0.68087016	0.12412	0
BRL	0.13473555	0.327751	0.519391	0.43934144	0	0.04454
CAD	0.23231475	0.090395	0.136851	0.14814717	0	0.100747
CNY	0	0.138772	0.104145	0.0513175	0.030349	0.088514
EUR	0.0967152	0.052805	0	0.04798345	0.053434	0.146964
GBP	0.35191532	0.119134	0.185437	0.10927432	0	0.158851
JPY	0.31623216	0.044339	0	0.3068814	0.14324	0.046001
KRW	0	0.182308	0.126916	0.15670631	0	0.284067
PLN	0.53801661	0	0.037808	0.30846202	0.138321	0.046001
USD	0.2882115	0.061309	0.039801	0.13998901	0	0.269473

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.16089524	0.029437	0.14439	0.24994095	0	0.089109
BRL	0.51343601	0.037788	0.084123	0.10752925	0.070702	0.033472
CAD	0.03418602	0.050127	0.100295	0.33363046	0.083783	0.038873
CNY	0.34959446	0.094549	0.124395	0.37532345	0	0.036318
EUR	0.38843597	0.210309	0.234997	0.03678035	0.137284	0.349279
GBP	0.04151616	0.050127	0.105565	0.26739927	0	0.270164
JPY	0.04816747	0.031846	0.064561	0.17593779	0	0
KRW	0.25191029	0.319143	0.059755	0.1958096	0	0.181943
PLN	0.22534029	0.250272	0.101	0.20701557	0	0.033472
USD	0.19538698	0.033611	0.236489	0.43960608	0.197695	0.152528

Table B 19: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Cryptsy platform 2016.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.45587131	0.075317	0.481792	0.889042	0	0.506392
BRL	0.74712584	0.23687	0.035929	0.130576	0.032201	0
CAD	0.3379542	0	0	0.255142	0.131186	0.101071
CNY	0.59643609	0.027717	0	0.232534	0.041096	0.259902
EUR	0.09855868	0.038587	0	0.088013	0.188243	0.154864
GBP	0.6759419	0	0.189758	0.406928	0	0
JPY	0.13753883	0	0.116606	0.412848	0.055604	0.214247
KRW	0.26988731	0.030731	0.348539	0.234699	0.112049	0.332065
PLN	0.48814711	0	0.431556	0.37445	0	0.150058
USD	0.09855868	0.037354	0.141183	0.053802	0.101484	0.246878

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.19460081	0	0.039228	0.076976	0	0.217577
BRL	0.29830418	0	0	0.156506	0	0
CAD	0.48349159	0	0.297817	0.257417	0.032333	0.039549
CNY	0.32055642	0.033095	0.41982	0.257367	0.032678	0.348941
EUR	0.55800796	0	0.343244	0.432158	0.099183	0.110053
GBP	0.64111528	0.167051	0.062143	0.419308	0	0.501556
JPY	0.39991127	0	0.140593	0.157242	0.099399	0.082534
KRW	0.0893419	0.141167	0.080618	0.381946	0.262388	0.148197
PLN	0.36268258	0.034328	0.089694	0.4394	0.04974	0.16885
USD	0.55800796	0.070935	0.272204	0.499712	0.086142	0.34822

Table B 20: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Bitfinex platform 2016.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.335132	0.070003	0.177661	0.486016437	0.080836	0.098241
BRL	0.414525	0.207995	0.261693	0.434544418	0	0.076483
CAD	0.068397	0	0.071961	0	0	0
CNY	0.098861	0.132047	0.264994	0.128024906	0	0
EUR	0.091909	0.077084	0.202819	0.094176915	0.022351	0.102822
GBP	0.671172	0.099142	0.100587	0.503876209	0	0.124847
JPY	0.471739	0.132047	0.10975	0.184952412	0.043377	0
KRW	0.1404	0.165515	0.115064	0.07906409	0.031331	0.1958
PLN	0.925681	0.355463	0.481704	0.579103611	0.299866	0
USD	0.072234	0.032791	0	0.235347245	0	0.0311

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.288678	0.093343	0.081555	0.379717243	0	0.050468
BRL	0.152315	0	0.20602	0.044512983	0	0
CAD	0.296541	0.496543	0.028782	0.121677849	0.022351	0
CNY	0.427426	0.063031	0.191392	0.300339144	0	0.028888
EUR	0.543123	0.03354	0.34242	0.495147231	0.092989	0.096584
GBP	0.238476	0.417375	0.079165	0.223923586	0.072981	0.071484
JPY	0.121214	0.063031	0.04555	0.47611182	0.098171	0.086436
KRW	0.263362	0	0.519198	0.052300435	0.049539	0.171613
PLN	0.144167	0.050924	0.072155	0.128414385	0.031331	0.02796
USD	0.814748	0.0543	0.219996	0.502961566	0.1104	0.095861

Table B 21: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Yapizon platform 2017.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0	0.148191	0.152156	0.333113	0.156289	0
BRL	0.032647	0.153651	0.613795	0.263665	0.345711	0.068327
CAD	0	0.034888	0.211103	0.132751	0	0.244915
CNY	0	0.111803	0.176527	0.460545	0.04756	0.145174
EUR	0	0	0.142991	0.420207	0.151158	0.042773
GBP	0	0.111037	0.528441	0.430199	0.068634	0.054187
JPY	0	0.345966	0.541107	0.360073	0.186013	0.101016
KRW	0	0.199506	0.247659	0.248483	0.167288	0.089308
PLN	0	0.107755	0.15783	0.566091	0.185349	0.34019
USD	0	0	0.251357	0.461849	0.056504	0.091031

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0	0.144152	0.518485	0.628832	0.117018	0.061207
BRL	0	0.049859	0.138336	0.499563	0.235558	0.090106
CAD	0	0	0.094803	0	0.467255	0.299023
CNY	0	0.292207	0.266339	0.30148	0.136315	0.078027
EUR	0	0.226724	0.558256	0.081841	0	0
GBP	0	0	0.306737	0.278114	0.114641	0.097796
JPY	0	0.039789	0.31321	0.766043	0.041828	0.129901
KRW	0	0.114853	0.329163	0.653064	0.208599	0.1757
PLN	0.032647	0.115999	0.164219	0.378903	0.043293	0.198314
USD	0	0.229216	0.333418	0.089135	0	0.046845

Table B 22: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Zaif platform 2018.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.1085	0.0931	0.0000	0.2633	0.0000	0.0000
BRL	0.2513	0.0548	0.0439	0.0000	0.0000	0.0000
CAD	0.3690	0.0480	0.4220	0.4229	0.2580	0.0000
EUR	0.0000	0.0424	0.0376	0.2966	0.0000	0.0879
GBP	0.0451	0.0291	0.0607	0.1224	0.1141	0.1349
JPY	0.5000	0.1043	0.1935	0.1228	0.1098	0.0000
KRW	0.2772	0.0000	0.0867	0.2827	0.0000	0.0000
PLN	0.2345	0.1654	0.2411	0.2706	0.0610	0.0000
USD	0.0000	0.0384	0.0618	0.1779	0.0000	0.0000

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.2525	0.0000	0.3896	0.1327	0.0000	0.0000
BRL	0.1193	0.0000	0.1446	0.2561	0.0856	0.0000
CAD	0.1170	0.0000	0.0292	0.2063	0.0000	0.0000
EUR	0.3010	0.0000	0.1018	0.1492	0.0905	0.0351
GBP	0.4903	0.0000	0.0499	0.0912	0.0311	0.0000
JPY	0.0000	0.0000	0.0583	0.4497	0.1306	0.1639
KRW	0.1139	0.5391	0.2254	0.3669	0.0536	0.0000
PLN	0.0451	0.0000	0.0000	0.1285	0.0700	0.0238
USD	0.3464	0.0363	0.1484	0.1786	0.0815	0.0000

Table B 23: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on LocalBitcoins platform 2019.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.0493	0.0000	0.0000	0.1437	0.0000	0.0268
BRL	0.0000	0.0000	0.0000	0.1624	0.0000	0.2210
CAD	0.0367	0.0000	0.0000	0.1867	0.0000	0.0000
EUR	0.0664	0.0000	0.0000	0.0599	0.0256	0.0000
GBP	0.2759	0.0000	0.1252	0.1735	0.0346	0.0591
JPY	0.0000	0.0000	0.0500	0.2352	0.0244	0.1014
KRW	0.1130	0.0000	0.0833	0.0000	0.0314	0.0000
PLN	0.2741	0.0229	0.2127	0.1292	0.0236	0.0000
USD	0.1121	0.0000	0.0000	0.0816	0.0000	0.0000

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.0899	0.0000	0.0000	0.2925	0.0244	0.1011
BRL	0.3367	0.0000	0.2483	0.1093	0.0896	0.0000
CAD	0.0810	0.0000	0.1205	0.0951	0.0000	0.0268
EUR	0.0000	0.0229	0.0634	0.1572	0.0000	0.0689
GBP	0.1870	0.0000	0.0000	0.1322	0.0000	0.0000
JPY	0.0523	0.0000	0.0000	0.1677	0.0256	0.0640
KRW	0.0671	0.0000	0.0000	0.0932	0.0000	0.0000
PLN	0.0716	0.0000	0.0000	0.0000	0.0000	0.0456
USD	0.0421	0.0000	0.0390	0.1251	0.0000	0.1018

Table B 24: IN-and OUT Node strengths of the ETE to cross-market Bitcoin prices in time during the cyberattack on Binance platform 2019.

IN-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.0355	0.1185	0.0243	0.1036	0.0000	0.0354
BRL	0.0305	0.2814	0.2454	0.0000	0.0000	0.0000
CAD	0.0000	0.1355	0.0339	0.0726	0.0000	0.0000
EUR	0.0000	0.0642	0.0445	0.0797	0.0000	0.0000
GBP	0.0000	0.2521	0.5226	0.0000	0.0000	0.0000
JPY	0.0000	0.1589	0.0000	0.0663	0.0000	0.0000
KRW	0.0000	0.2534	0.0289	0.1067	0.0000	0.4939
PLN	0.0000	0.0723	0.0000	0.0713	0.0000	0.2456
USD	0.0000	0.1135	0.0000	0.0528	0.0000	0.0000

Out-Node strengths	**1**	**2**	**3**	**4**	**5**	**6**
AUD	0.0000	0.3650	0.2589	0.0707	0.0000	0.0766
BRL	0.0000	0.3830	0.0000	0.0000	0.0000	0.0541
CAD	0.0660	0.1198	0.0587	0.0267	0.0000	0.1034
EUR	0.0000	0.0000	0.1148	0.1218	0.0000	0.1400
GBP	0.0000	0.0947	0.0243	0.0000	0.0000	0.0701
JPY	0.0000	0.1195	0.1162	0.0000	0.0000	0.1405
KRW	0.0000	0.2079	0.0771	0.1394	0.0000	0.0000
PLN	0.0000	0.0681	0.1169	0.1518	0.0000	0.0498
USD	0.0000	0.0919	0.1326	0.0426	0.0000	0.1405

Figure B 10: Rolling window estimation of IN-Node strengths between Bitcoin cross-market prices.

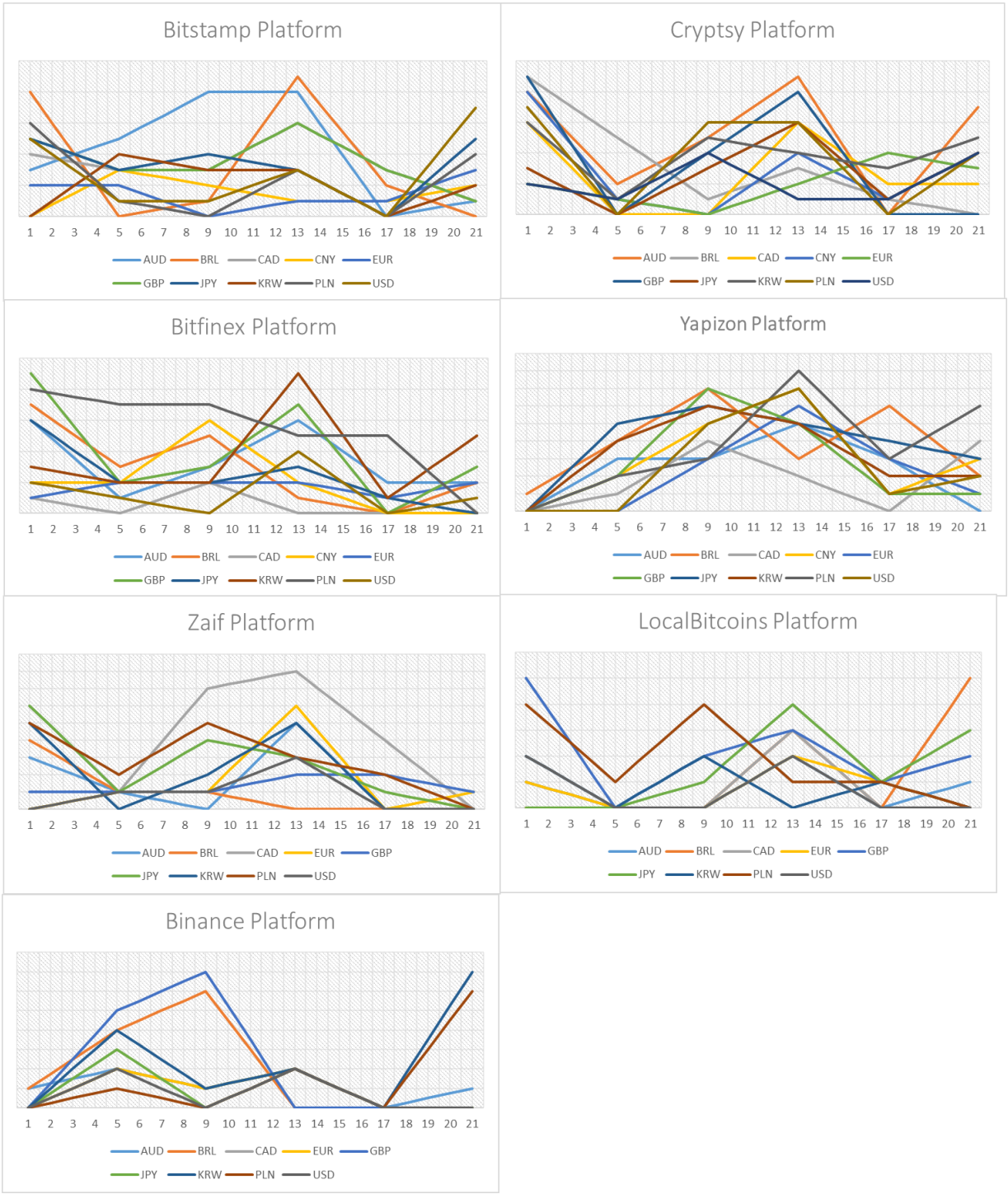


Figure B 11: Rolling window estimation of Out-Node strengths between Bitcoin cross-market prices.

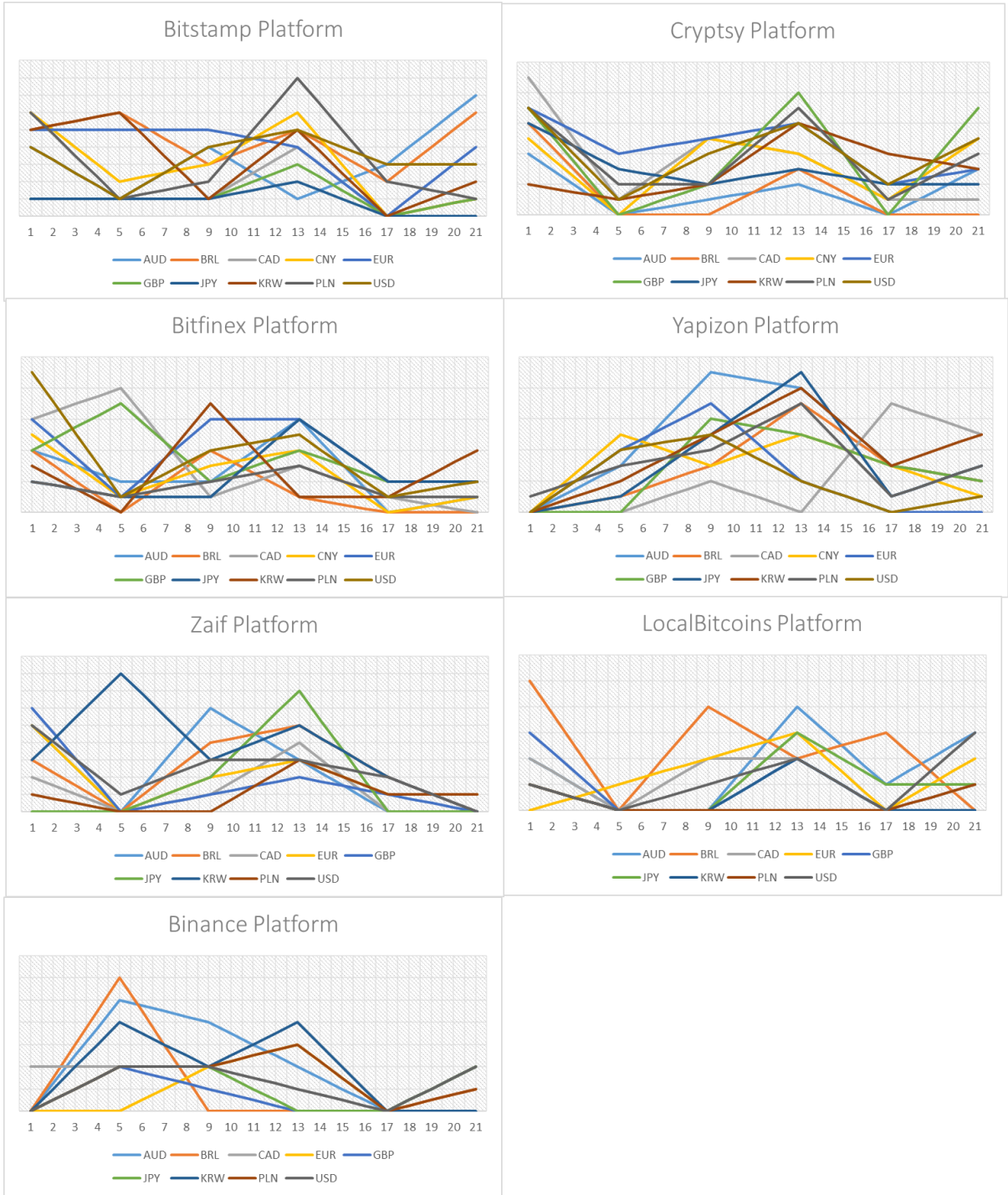


Figure B 12: Effective Transfer Entropy matrix (ETE) in case of $k = \ell = 1$

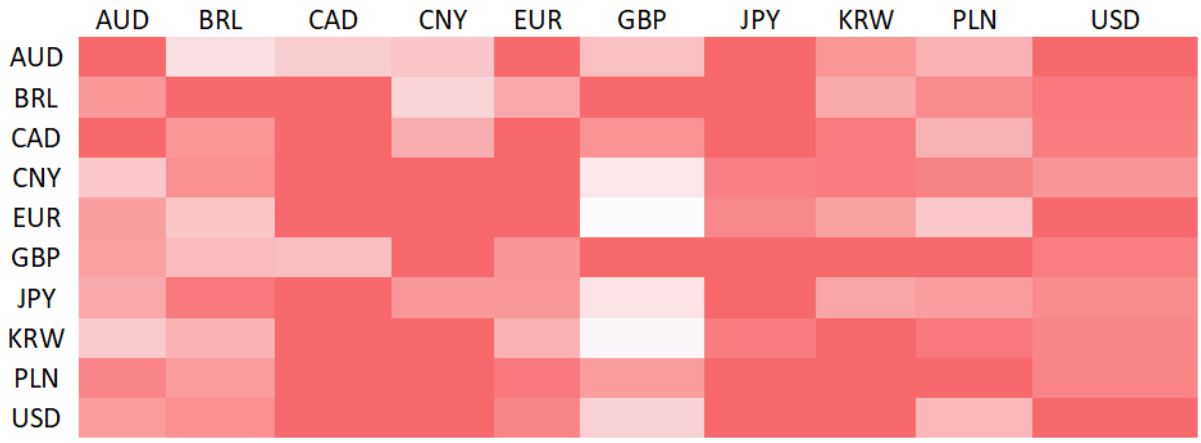


Figure B 13: Effective Transfer Entropy matrix (ETE) in case of $k = \ell = 2$

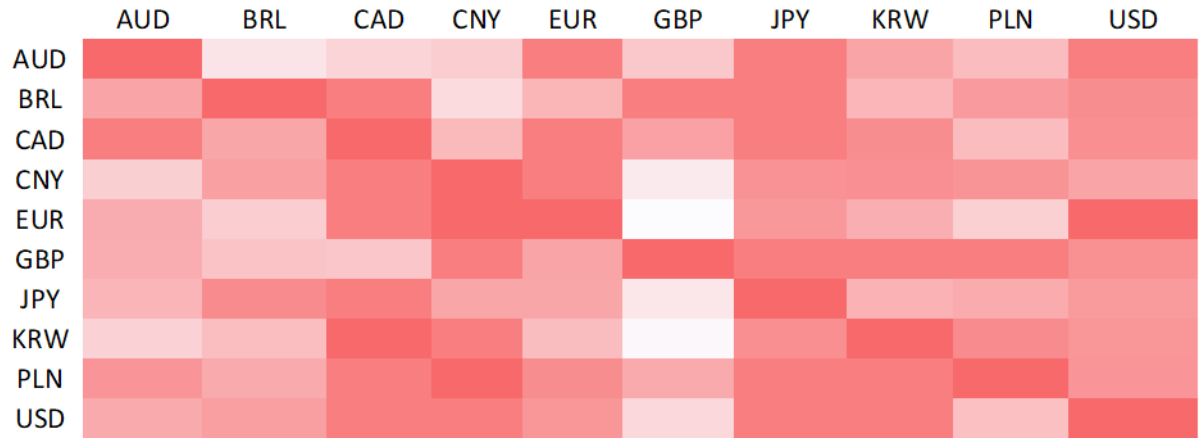


Figure B 14: Transfer Entropy (TE) matrix of cross market Bitcoin price.

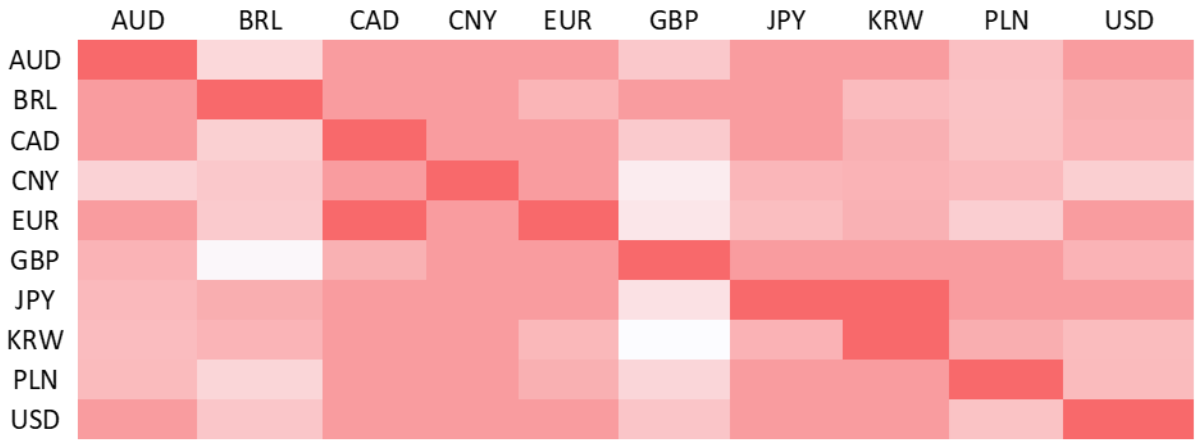


Figure B 15: Effective Transfer Entropy (ETE) matrix of cross market Bitcoin price.

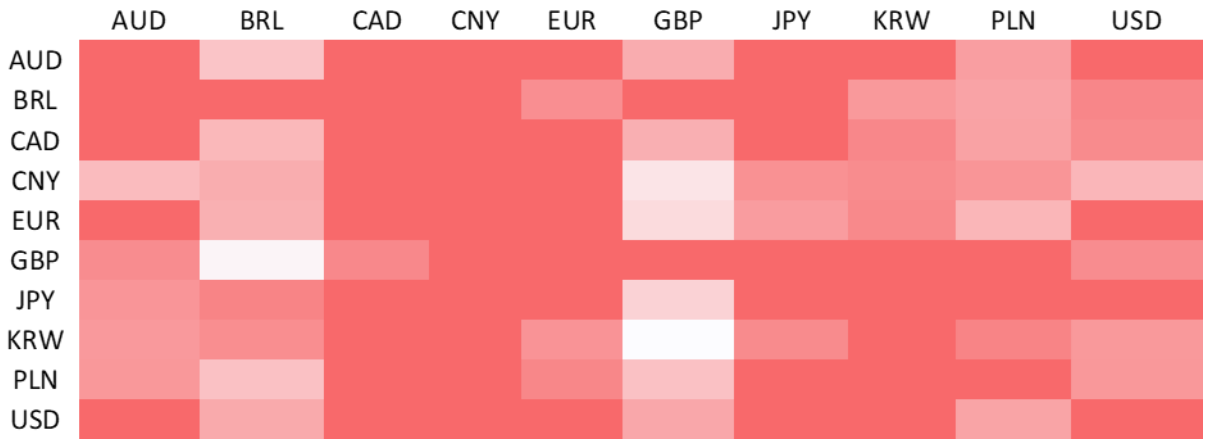


Table B 25: IN- Closeness Node of the ETE to cross-market Bitcoin prices in time.

		Pre the cybercrime	*Post the cybercrime*
Bitstamp	avg. IN-Closeness	0.37	0.74
	avg. steps to contagion	3.34	6.67
	Steps to contagion	33.39	66.67
Cryptsy	avg. IN-Closeness	0.58	0.44
	avg. steps to contagion	5.25	3.99
	Steps to contagion	52.49	39.89
Bitfinex	avg. IN-Closeness	0.45	0.36
	avg. steps to contagion	4.05	3.20
	Steps to contagion	40.52	31.99
Yapizon	avg. IN-Closeness	0.42	0.71
	avg. steps to contagion	3.76	6.36
	Steps to contagion	37.57	63.58
Zaif	avg. IN-Closeness	0.63	0.70
	avg. steps to contagion	5.04	5.57
	Steps to contagion	45.39	50.10
LocalBitcoi	avg. IN-Closeness	0.67	0.33
	avg. steps to contagion	5.37	2.67
	Steps to contagion	48.33	24.04
Binance	avg. IN-Closeness	0.61	0.20
	avg. steps to contagion	4.86	1.64
	Steps to contagion	43.70	14.72

Table B 26: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitstamp platform 2015.

	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.1	0.692	0.563	0.9
BRL	0.45	0.474	0.818	0.9
CAD	0.375	0.409	0.75	0.75
CNY	0.429	0.375	0.75	0.818
EUR	0.5	0.346	0.9	0.529
GBP	0.375	0.429	0.692	0.563
JPY	0.36	0.429	0.692	0.9
KRW	0.692	0.1	0.643	0.818
PLN	0.429	0.45	0.6	0.9
USD	0.375	0.375	1	0.5

Table B 27: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Cryptsy platform 2016.

	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.1	0.818	0.29	0.9
BRL	0.643	0.5	0.333	0.6
CAD	0.563	0.391	0.391	0.529
CNY	0.6	0.3	0.409	0.409
EUR	1	0.31	0.36	0.818
GBP	0.9	0.346	0.375	0.75
JPY	0.474	0.391	0.409	0.6
KRW	0.643	0.409	0.474	0.6
PLN	0.5	0.409	0.391	0.5
USD	0.409	0.391	1	0.1

Table B 28: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Bitfinex platform 2016.

	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.375	0.692	0.409	0.321
BRL	0.391	1	0.45	0.3
CAD	0.429	0.5	0.111	0.1
CNY	0.818	0.1	0.375	0.273
EUR	0.429	0.6	0.429	0.3
GBP	0.391	0.9	0.321	0.333
JPY	0.391	0.5	0.5	0.265
KRW	0.474	0.643	0.45	0.31
PLN	0.429	0.818	0.1	0.75
USD	0.375	0.75	0.409	0.273

Table B 29: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Yapizon platform 2017.

	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.45	0.643	0.643	0.529
BRL	0.36	1	0.818	0.818
CAD	0.346	0.45	0.643	0.643
CNY	0.529	0.1	0.75	0.6
EUR	0.429	0.409	0.5	0.75
GBP	0.45	0.692	0.692	0.692
JPY	0.36	0.818	0.818	0.75
KRW	0.391	0.563	1	0.75
PLN	0.409	1	0.6	1
USD	0.45	0.6	0.6	0.529

Table B 30: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Zaif platform 2018.

	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.667	0.615	0.727	0.667
BRL	0.421	0.727	1	0.2
CAD	0.667	1	0.533	0.8
EUR	0.727	0.571	0.571	0.615
GBP	0.8	0.533	0.727	0.727
JPY	0.444	0.571	0.889	0.533
KRW	0.8	0.533	0.667	0.667
PLN	0.421	0.8	0.615	0.615
USD	0.727	0.364	0.533	0.571

Table B 31: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on LocalBitcoins platform 2019.

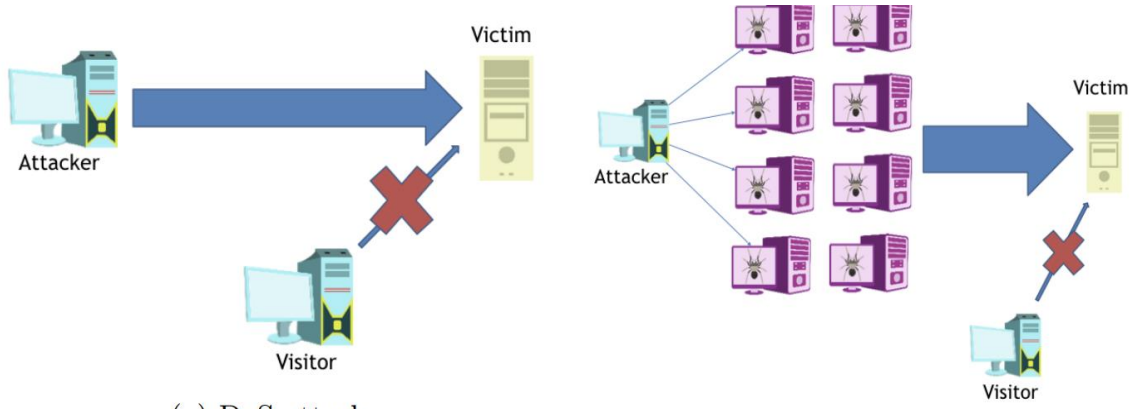
	Pre the cybercrime		*Post the cybercrime*	
	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
AUD	0.381	0.727	0.308	0.14
BRL	1	0.889	0.111	0.889
CAD	0.571	0.5	0.235	0.308
EUR	0.8	0.533	0.727	0.125
GBP	0.889	0.533	0.222	0.333
JPY	0.667	0.615	0.125	0.421
KRW	0.533	0.571	0.8	0.125
PLN	0.533	0.889	0.235	0.276
USD	0.667	0.571	0.242	0.286

Table B 32: in-and out-closeness based on ETE to cross-market Bitcoin prices network pre- and post-cyberattacks on Binance platform 2019.

	pre		*post*	
	Pre the cybercrime		Post the cybercrime	
AUD	IN-Closeness	Out-Closeness	IN-Closeness	Out-Closeness
BRL	0.727	0.471	0.16	0.276
CAD	0.471	0.571	0.186	0.125
EUR	0.615	0.571	0.25	0.111
GBP	0.667	0.444	0.182	0.125
JPY	0.667	0.727	0.111	0.727
KRW	0.348	0.727	0.163	0.296
PLN	0.8	0.727	0.163	0.333
USD	0.5	0.533	0.125	0.143

C. Supplement to Chapter 4

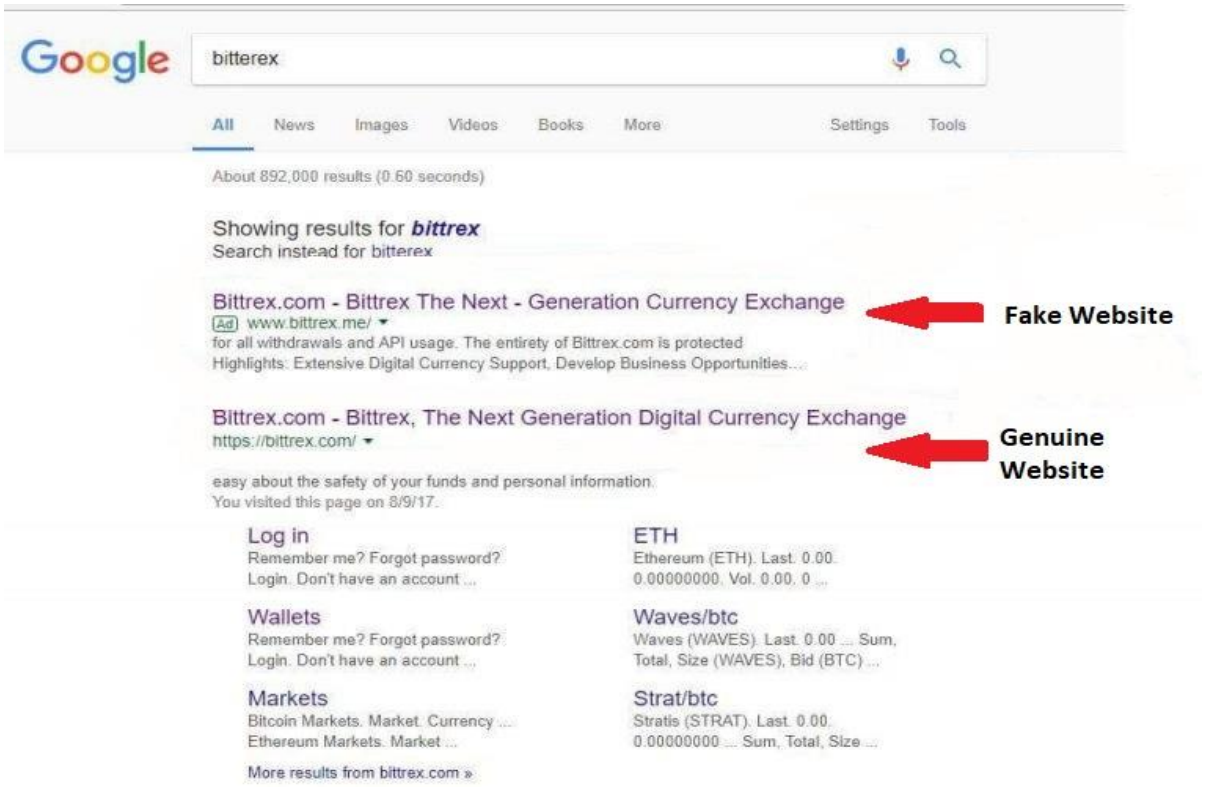
Figure C. 1: DoS and DDoS attacks.



(a) DoS attack.

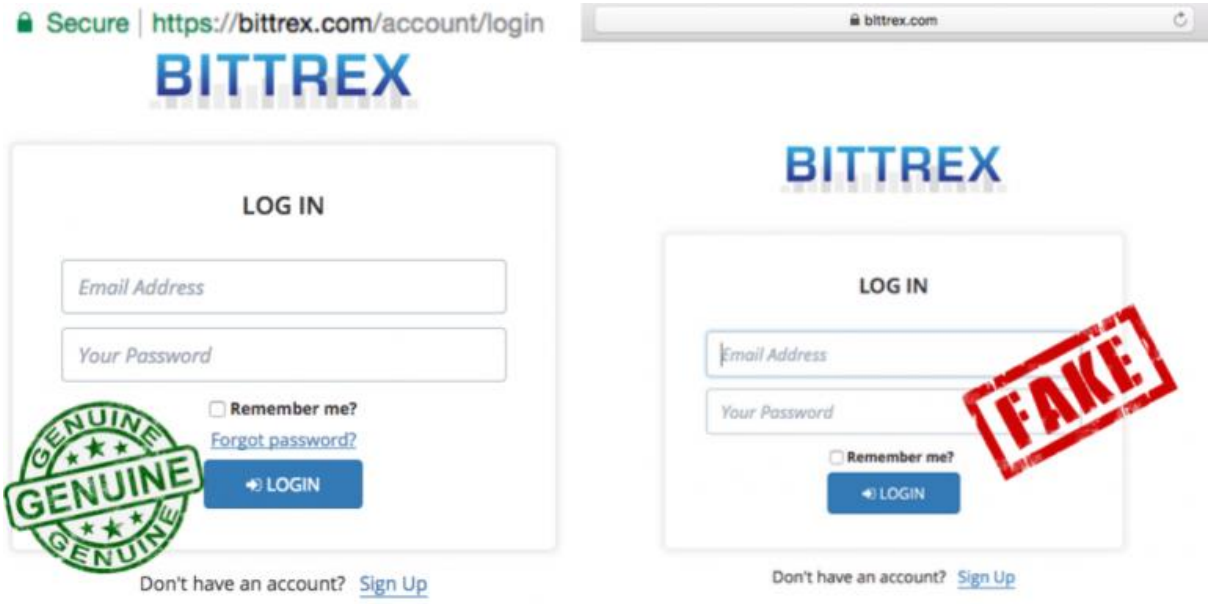
(b) DDoS attack.

Figure C. 2: Phishing attacks on Bittrex users in August 2017



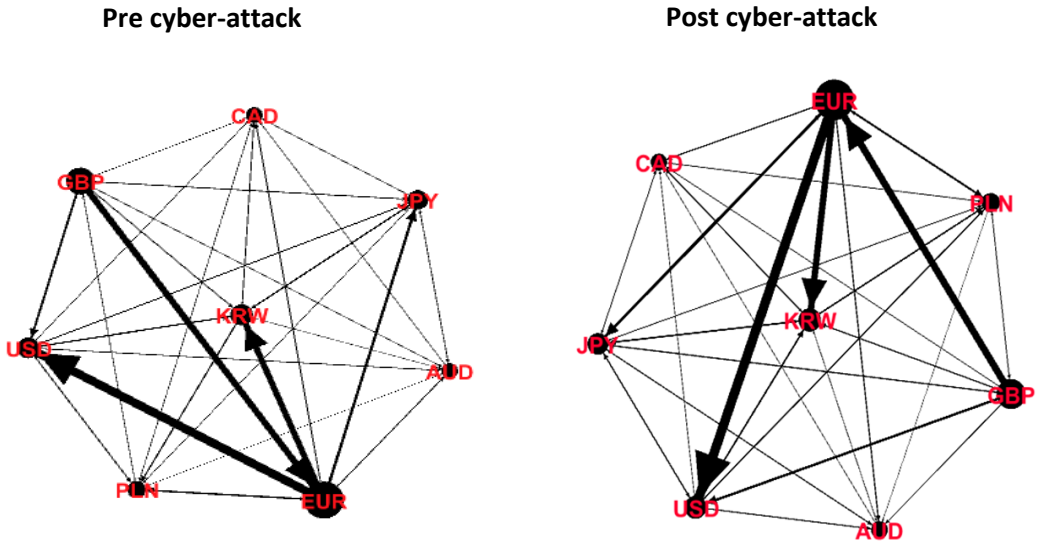
Note: image soure (hackread.com, 2017)

Figure C. 3: Fake Bittrex cryptocurrency exchange site defacing



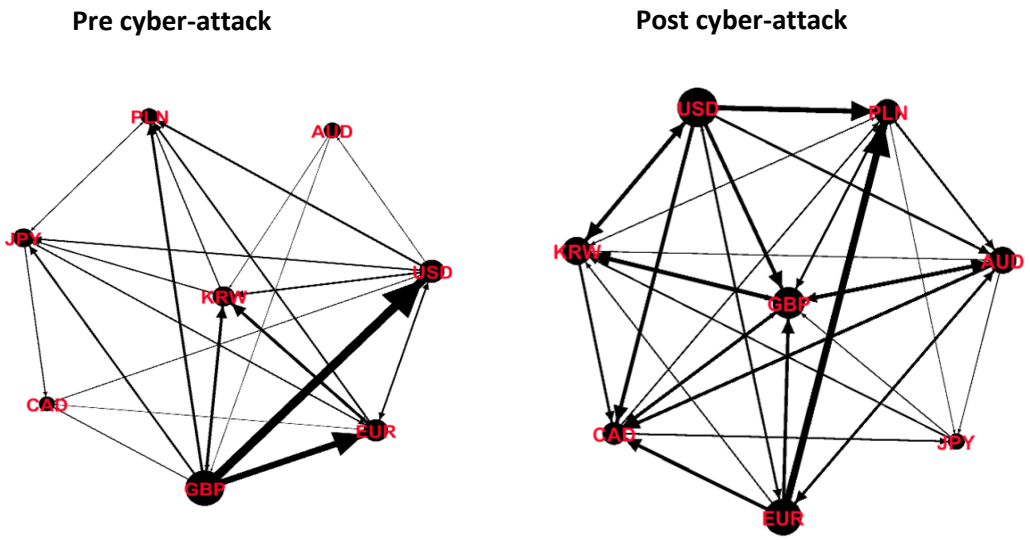
Note: Image source (hackread.com, 2017)

Figure C. 4 : The Bitcoin cross-market prices pre- and post-cyberattacks on Bitfinex 2-2017 platform.



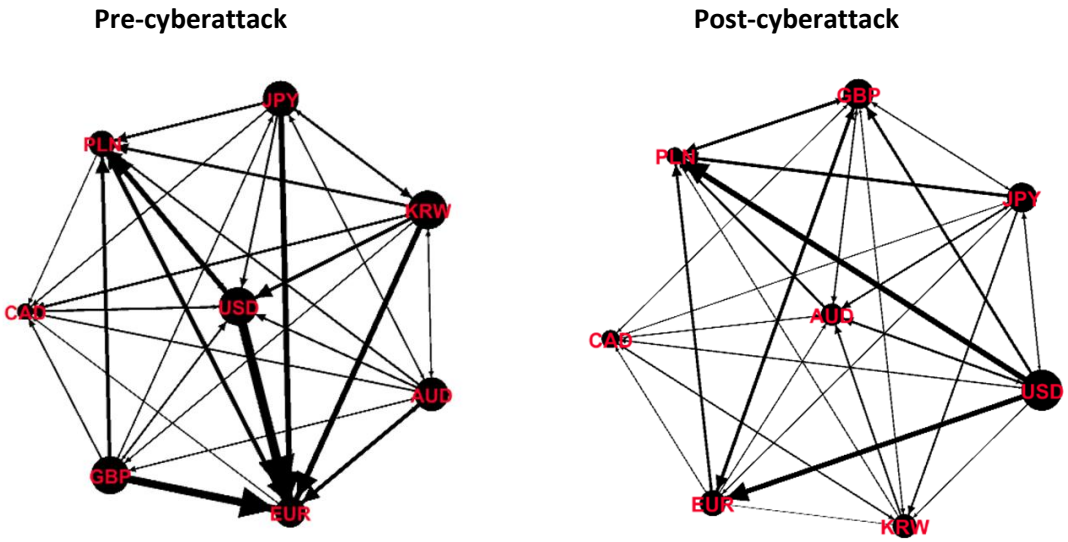
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 5 : The Bitcoin cross-market prices pre and post cyber-attacks on Bitfinex 6-2017 platform.



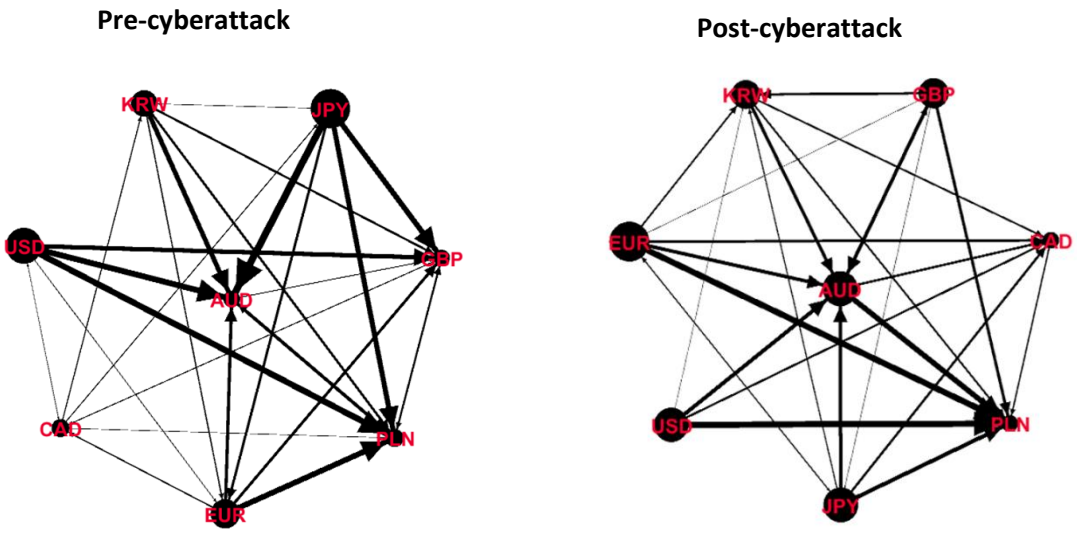
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 6 The Bitcoin cross-market prices pre- and post-cyberattacks on Bitfinex 12-2017 platform.



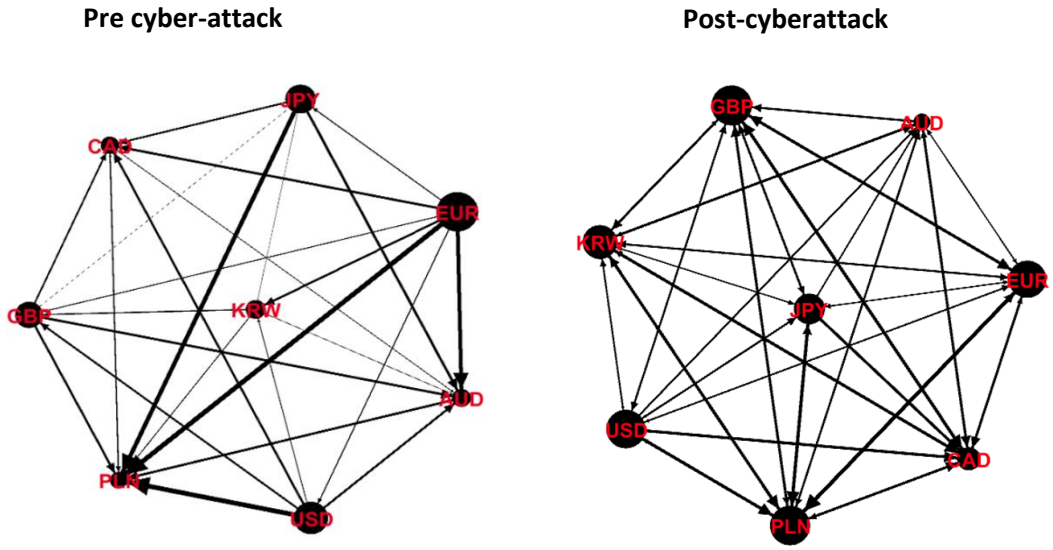
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 7 The Bitcoin cross-market prices pre- and post-cyberattacks on Bitfinex 5-2018 platform.



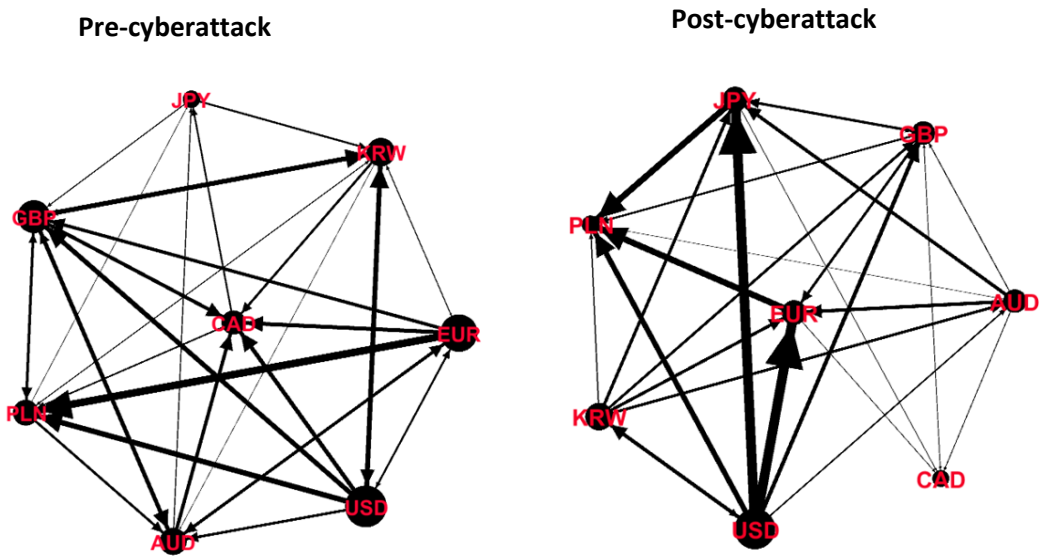
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 8 The Bitcoin cross-market prices pre- and post-cyberattacks on Bitfinex 2-2020 platform.



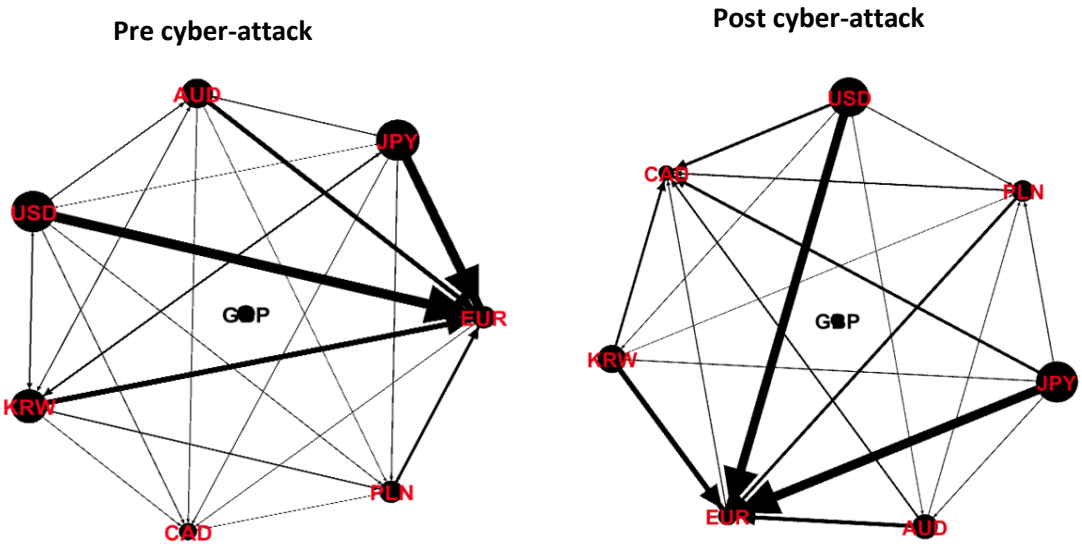
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 9 The Bitcoin cross-market prices pre- and post- cyberattacks on Bithumb 6-2017 platform.



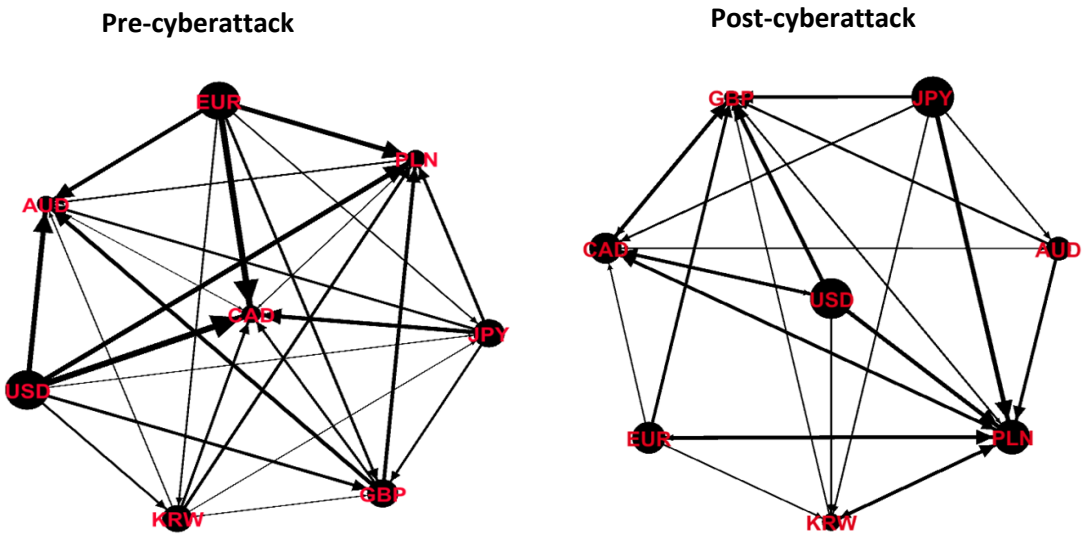
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 10 The Bitcoin cross-market prices pre- and post- cyberattacks on Coinmama 2-2019



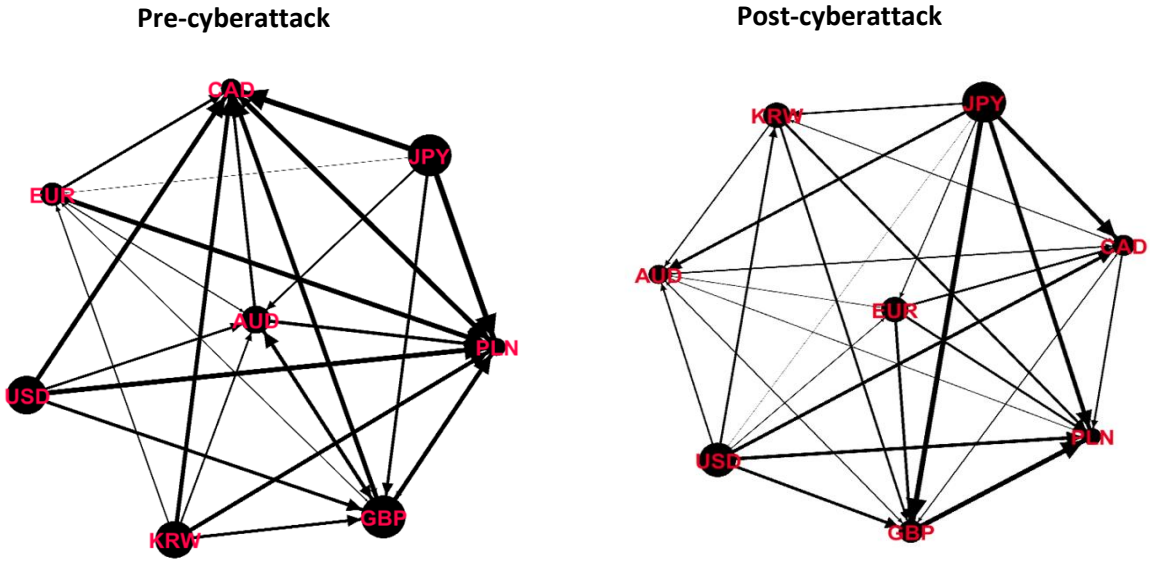
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 11 The Bitcoin cross-market prices pre- and post- cyberattacks on Trident 3-2020 platform.



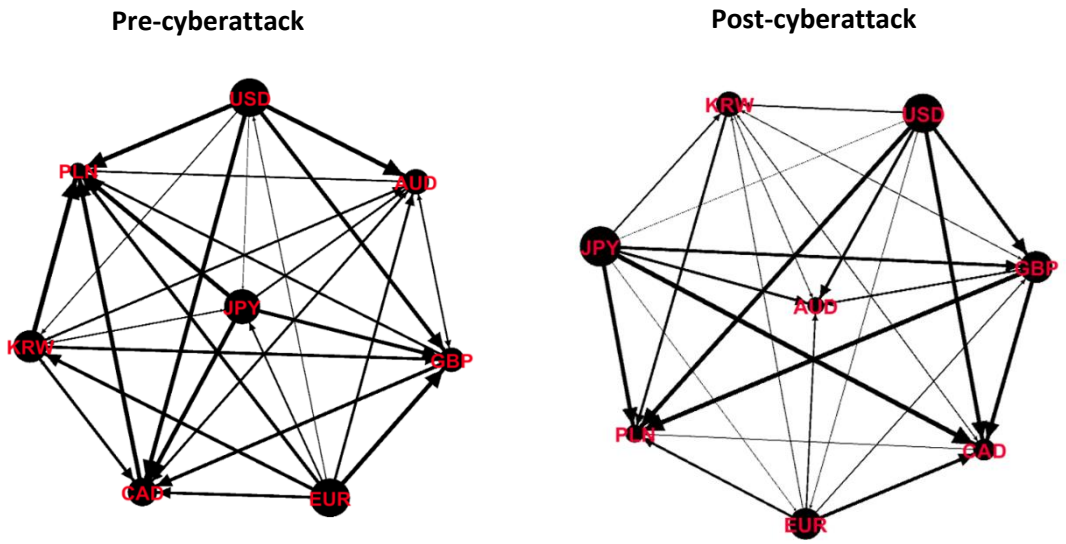
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 12 The Bitcoin cross-market prices pre- and post-cyberattacks on Keepkay 5-2020 platform.



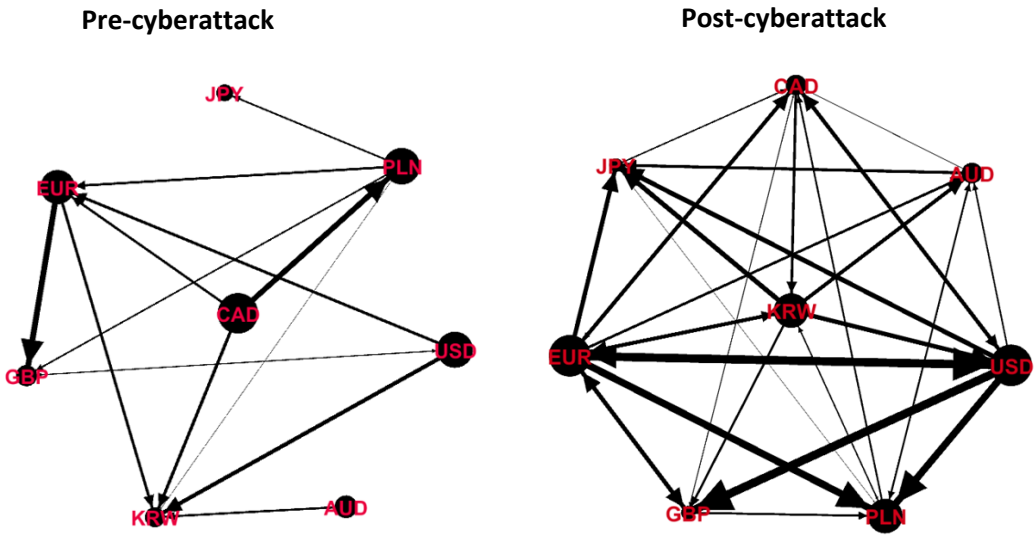
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 13 The Bitcoin cross-market prices pre- and post- cyberattacks on Ledger 7-2020 platform.



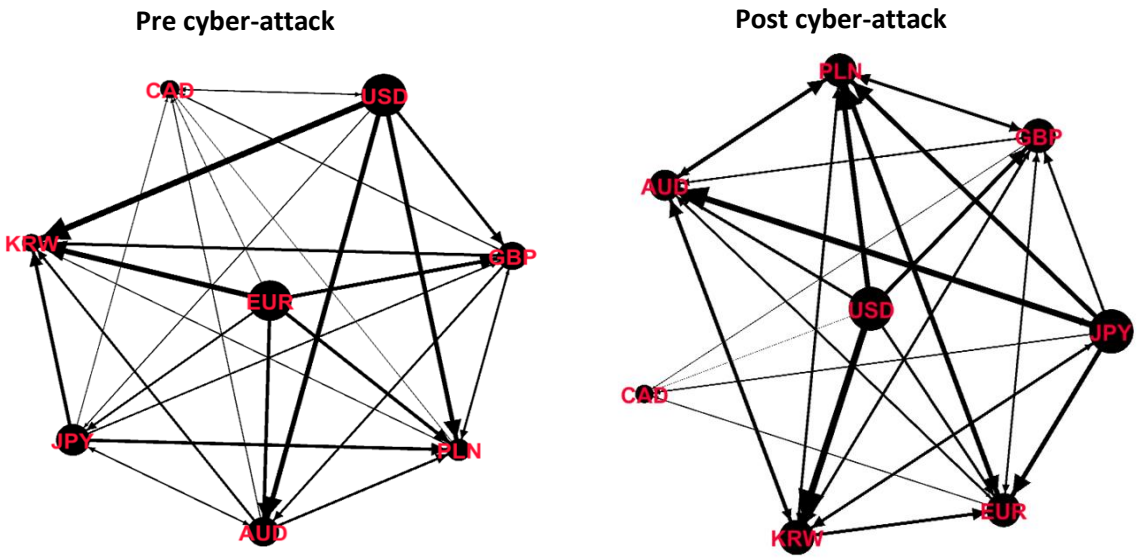
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 14 The Bitcoin cross-market prices pre- and post-cyber-attacks on Yapizon 4-2017 platform.



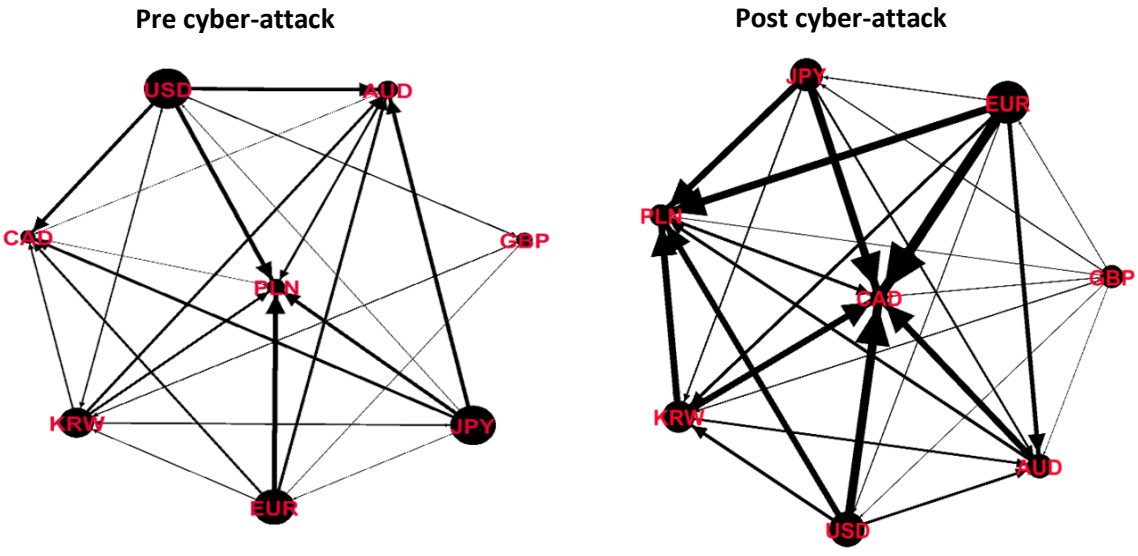
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 15 The Bitcoin cross-market prices pre- and post-cyberattacks on Zaif 9-2018 platform.



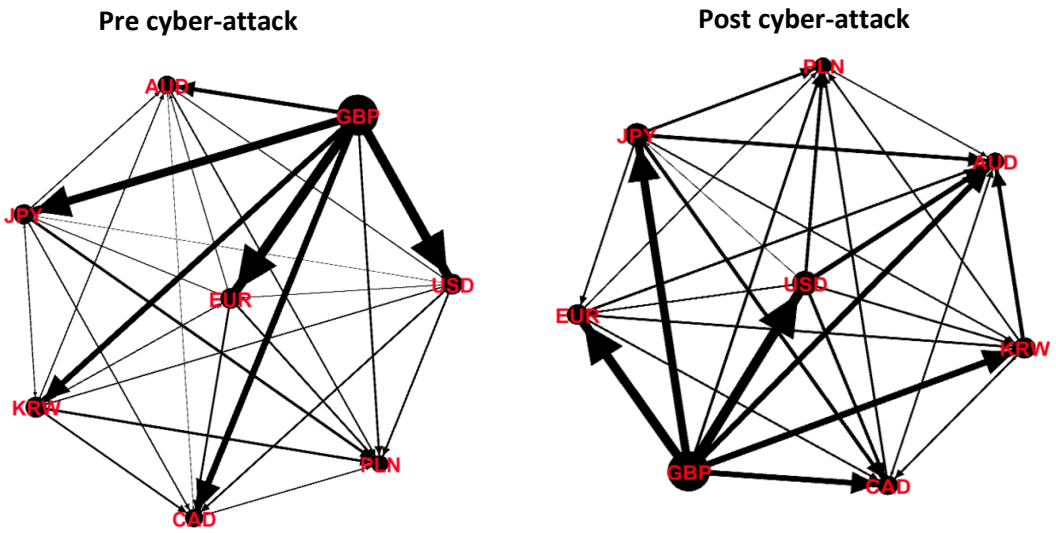
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 16 The Bitcoin cross-market prices pre- and post-cyberattacks on Binance 5-2019 platform.



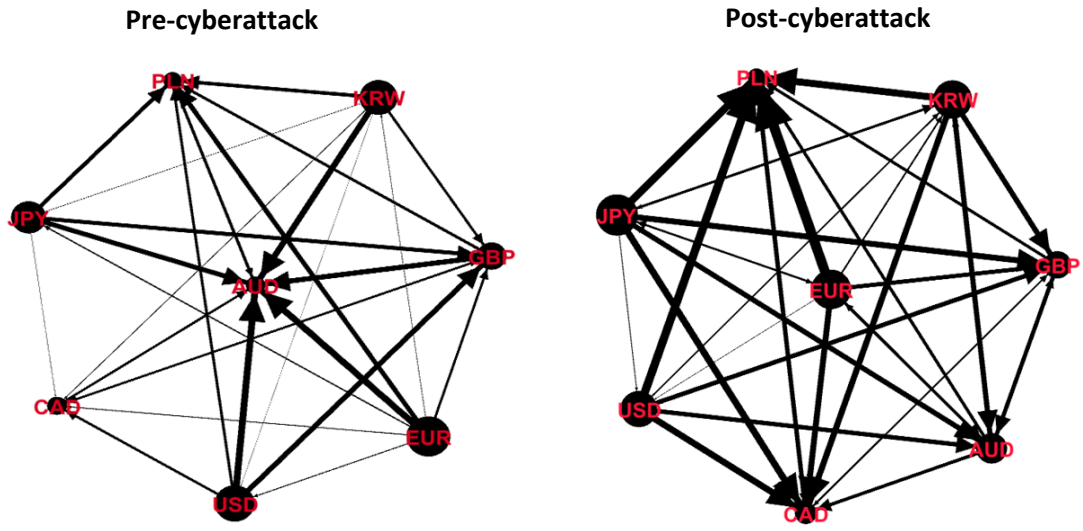
Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 17 The Bitcoin cross-market prices pre- and post-cyberattacks on Cashaa 7-2020 platform.



Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 18 The Bitcoin cross-market prices pre- and post-cyberattacks on KuCoin 9-2020 platform.



Note: The thickness of edges' lines reflects the strength of the information spillover between Bitcoin exchange rates. The size of the node refers to the Out-Node Strength (NS_{out}) where the higher the value of NS_{out}, means more transmitting risk in the network.

Figure C. 19: IN and Out Degree histogram pre- and post cyberattacks on Bitfinex 5-2018 platform.

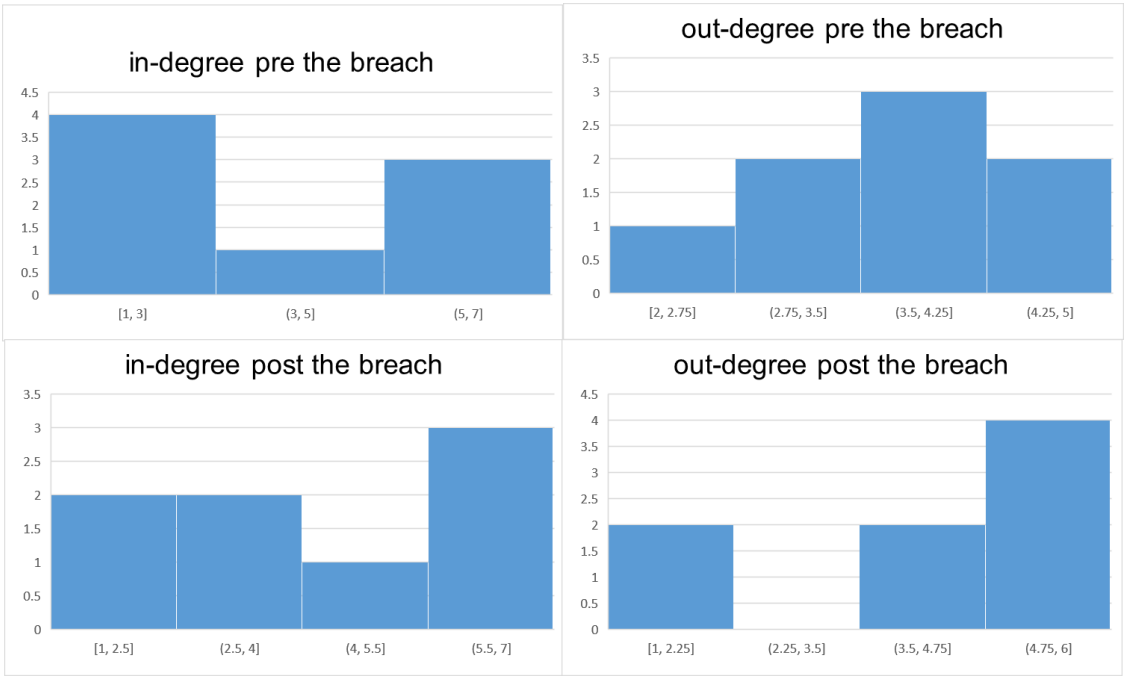


Figure C. 20: IN and Out Degree histogram pre- and post cyberattacks on Bitfinex 2-2020 platform.

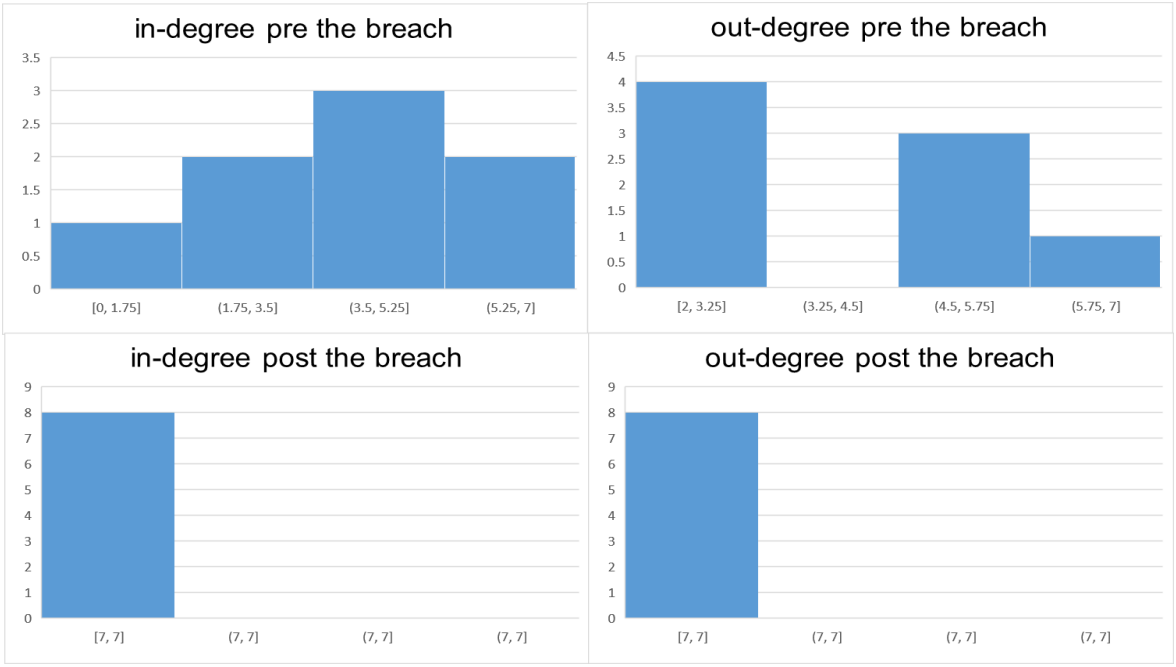


Figure C. 21: IN and Out Degree histogram pre- and post cyberattacks on KuCoin 9-2020 platform.

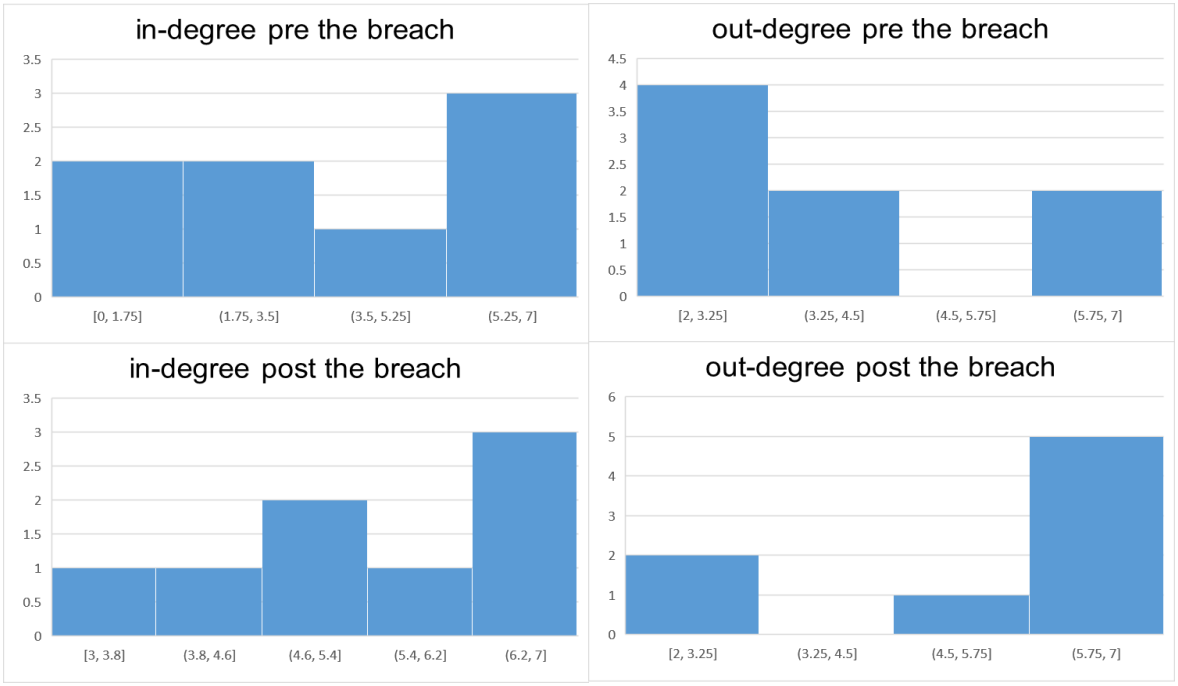


Figure C. 22: IN and Out Degree histogram pre- and post cyberattacks on Cashaa 7-2020 platform.

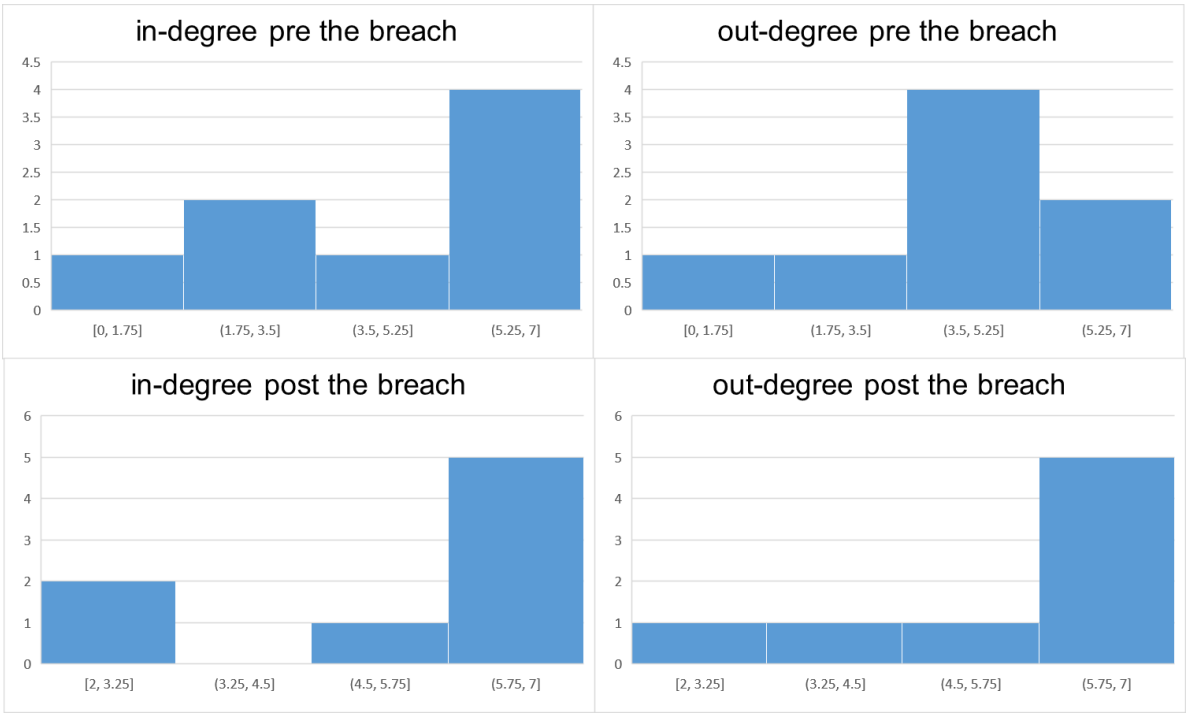


Figure C. 23: IN and Out Degree histogram pre- and post cyberattacks on Ledger 7-2020 platform.

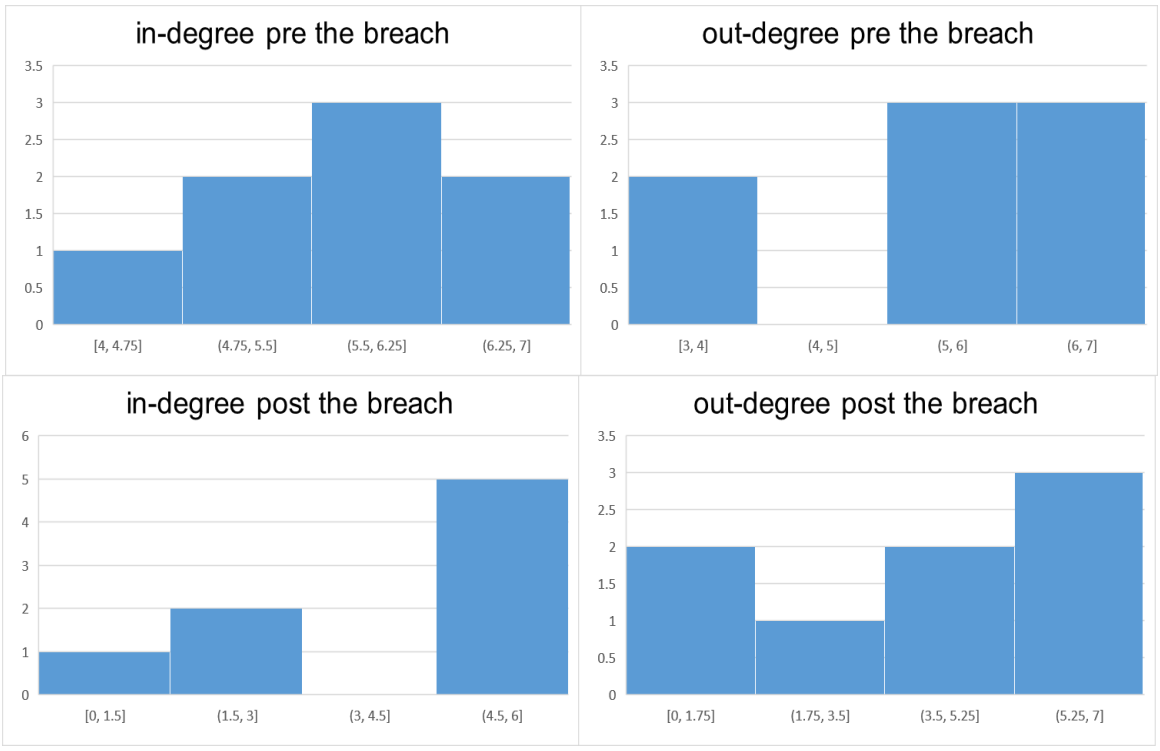


Figure C. 24: IN and Out Degree histogram pre- and post cyberattacks on Keepkay 5-2020 platform.

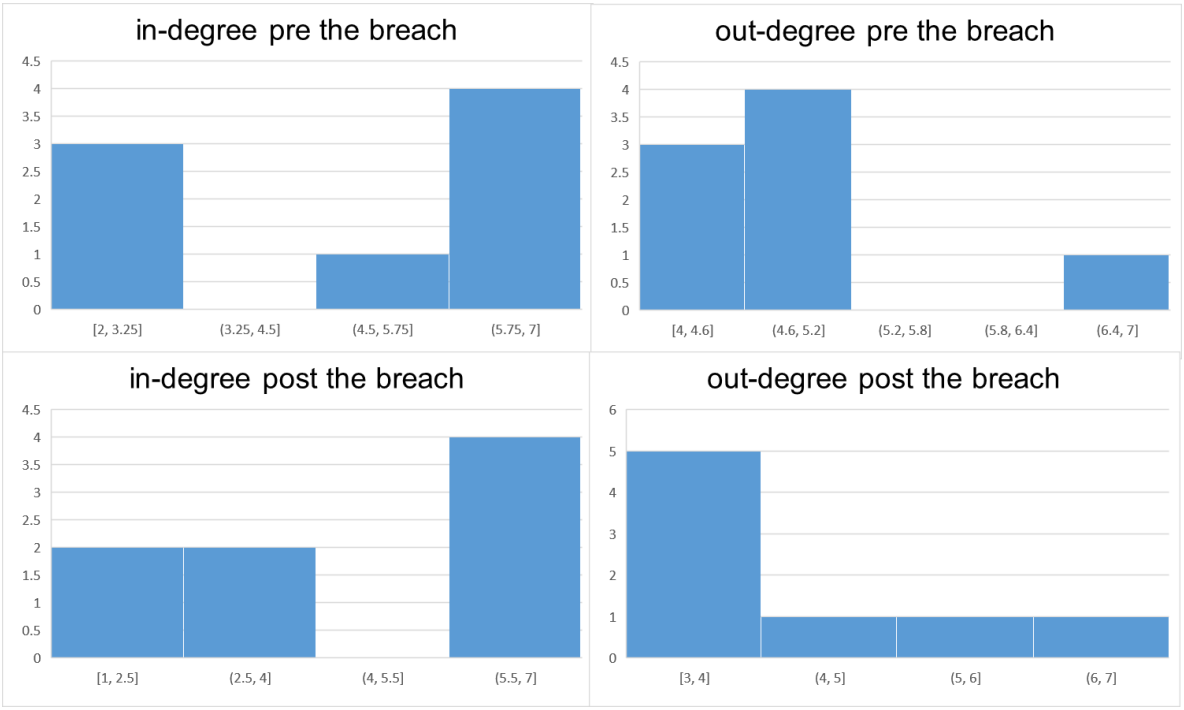


Table 1 - 3 Summary of the relevant literature that collaborate to examine the main classifications of security breach that targeted the Bitcoin market.

Group	**Types of security breaches**	**Authors**
Theft	dropping transactions	Sigurdsson et al., (2018)
	51% attacks	Shanaev et al., (2019)
	double-spending attacks	Hassan et al., (2020)
	malleability attacks	Pinzón and Rocha, (2016)
	DNS hijacking	Dai et al., (2017)
	account hijacking	Mirian et al.,(2019)
	SIM swapping	Sigurdsson et al., (2018)
	price manipulation	Gandal et al.,(2018)
	mining botnets	Huang et al., (2014)
	prices manipulated	Griffin and Shams (2018)
Confidentiality	Fake app	Xia et al., (2020)
	Site defacing	Weimann (2016)
	phishing scams	Chen et al., (2020)
Availability	DDoS	Vasek et al. (2014)
	DDoS	Johnson et al., (2014)
	DDoS	Feder et al. (2017)
	DDoS	Abhishta et al. (2019)
	DDoS	Feder et al. (2018a)

Note: Categorize the literature into three different classes, each category represent the works that examined the impact of cyber attacks on Bitcoin markets

Table C. 1 The list of security breaches that led to leach in customer's personal data.

No.	Date	UTC Time	Number Of Users	Databases
1	30/6/2017	7:37	318,000	Bithumb
2	15/2/2019	11:00	450,000	Coinmama
3	6/3/2020	0:01	266,000	Trident Crypto Fund
4	24/5/2020	8:39	80000	Trezor, Ledger, and Keepkay
5	29/7/2020	0:01	1,000,000	Ledger

Note: The time of each incident was considered from the web page of the database that announced the time of the attack. The time of each event was measured depending on Coordinated Universal Time (UTC) Timestamp.

Table C. 2 The list of security breaches that led to unavailability of the targeted platform.

No.	Date	UTC Time	Platform	Damage
1	21/02/2017	9:40 PM	Bitfinex	Degraded Performance
2	15/06/2017	7:32 AM	Bitfinex	Degraded Performance
3	12/12/2017	2:44 PM	Bitfinex	Temporary Unavailability
4	06/05/2018	2:51 PM	Bitfinex	Temporary Unavailability
5	27/02/2020	9:21 AM	Bitfinex	Temporary Unavailability

Note: The time of each incident was considered from the web page of the platform that announced the time of the attack. The time of each event was measured depending on Coordinated Universal Time (UTC) Timestamp.

Table C. 3 The list of security breaches that led to economic lost in the targeted platform.

No.	Date	UTC Time	Bitcoin missed	Amount	Platform	Headquarter
1	22/04/2017	02:00	4000	$5,000,000	Yapizon	South Korean
2	20/09/2018	02:15	5,966	$38,000,000	Zaif	Japan
3	7/5/2019	17:15	7000	$41,000,000	Binance	Malta
4	11/7/2020	17:54	336	$3,100,000	Cashaa	UK
5	26/9/2020	11:05	1008	$11,000,000	KuCoin	Singapore

Note: The time of each incident was considered from the web page of the platform that announced the time of the attack. The time of each event was measured depending on the announcement time of security breach at Coordinated Universal Time (UTC) Timestamp. Headquarters of platform considered at the time of the security breach. In the case of KuCoin the cyberattack cost the platform around $150,000,000. Thus, we only include the amount of Bitcoin missed.

Table C. 4 The countries included in the paper, respective currency symbols, and the Bitcoin platform.

No.	*Country*	*Currency*	*Bitcoin Platform*	*Market Share*
1	Australia	AUD	Btcmarkets	86%
2	Canada	CAD	Quadrigacx	66%
3	Europe	EUR	Kraken	48%
4	British	GBP	Coinfloor	33.2%
5	Japan	JPY	Bitflyer	96.8%
6	South Korea	KRW	Korbit	76.3%
7	Polish	PLN	bitbay	74.4%
8	United States	USD	Bitstamp	20%

Note: The data for BTC/CAD after 1/1/2019 were obtained from Kraken, as the Quadrigacx platform shut down.

Table C. 5 Summary statistics, Bitcoin exchange rate returns

	USD	PLN	KRW	JPY	GBP	EUR	CAD	AUD
MEAN	0.0253	0.0243	0.0246	0.0243	0.0254	0.0238	0.0251	0.0248
MEDIAN	0.0285	0.0209	0.0250	0.0262	0.0348	0.0286	0.0264	0.0286
MAXIMUM	0.050	0.061	0.199	0.061	0.057	0.061	0.822	0.060
MINIMUM	-0.065	-0.073	-0.219	-0.094	-0.070	-0.065	-0.851	-0.074
STD. DEV.	0.008	0.007	0.008	0.008	0.008	0.008	0.018	0.008
SKEWNESS	-0.456	-0.434	-1.191	-0.629	-0.479	-0.376	-1.848	-0.438
KURTOSIS	10.199	13.861	147.186	14.656	12.082	11.162	176.858	12.703
JARQUE-BERA	12821	28908	50640	33465	20309	16359	758000	23113
ADF	-38.984	-38.232	-33.992	-38.101	-39.127	-39.134	-54.671	-38.358

Note: All the values of Jarque-Bera test and the Augmented Dickey Fuller test are significant at the 1% level.

Table C. 6 Key factor of topological features to cross-market Bitcoin prices network pre- and post-availability cyberattacks.

Platform	Period	Edge	Avg. Degree	Node Strength Degree	Graph Density
Bitfinex 2-2017	pre	47	5.87	0.11	0.839
	post	47	5.87	0.11	0.839
Bitfinex 6-2017	pre	34	4.25	0.057	0.607
	post	42	5.25	0.058	0.75
Bitfinex 12-2017	pre	46	5.75	0.067	0.821
	post	47	5.87	0.084	0.839
Bitfinex 5-2018	pre	30	3.75	0.048	0.536
	post	33	4.13	0.057	0.59
Bitfinex 2-2020	pre	31	3.875	0.052	0.554
	post	56	7	0.197	1

Table C. 7 Key factor of topological features to cross-market Bitcoin prices network pre- and post-confidentiality cyberattacks.

Platform	Period	Edge	Avg. Degree	Node Strength Degree	Graph Density
Bithumb 6-2017	pre	44	5.5	0.072	0.786
	post	38	4.75	0.05	0.679
Coinmama 2-2019	pre	30	3.75	0.164	0.536
	post	25	3.12	0.091	0.446
Trident 3-2020	pre	34	4.25	0.086	0.607
	post	29	3.625	0.059	0.518
Keepkay 5-2020	pre	39	4.8	0.071	0.696
	post	35	4.375	0.054	0.625
Ledger 7-2020	pre	46	5.75	0.093	0.821
	post	31	3.875	0.051	0.55

Table C. 8 Key factor of topological features to cross-market Bitcoin prices network pre- and post-theft cyberattacks.

Platform	Period	Edge	Avg. Degree	Node Strength Degree	Graph Density
Yapizon 4-2017	pre	15	1.875	0.015	0.268
	post	38	4.75	0.055	0.679
Zaif 9-2018	pre	34	4.25	0.058	0.607
	post	37	4.625	0.059	0.661
Binance 5-2019	pre	26	3.25	0.068	0.464
	post	36	4.5	0.076	0.643
Cashaa 7-2020	pre	35	4.375	0.114	0.625
	post	43	5.375	0.116	0.768
KuCoin 9-2020	pre	30	3.75	0.043	0.536
	post	44	5.5	0.089	0.786

Table C. 9 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bitfinex 2-2017.

Pre the Cybercrime				**Post the Cybercrime**			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
JPY	JPY	USD	EUR	CAD	JPY	USD	EUR
CAD	USD	EUR	GBP	JPY	KRW	EUR	GBP
AUD	KRW	KRW	KRW	AUD	USD	KRW	KRW
EUR	GBP	JPY	USD	EUR	GBP	JPY	USD
PLN	EUR	PLN	JPY	KRW	EUR	PLN	JPY

Table C. 10 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bitfinex 6-2017.

Pre the Cybercrime				**Post the Cybercrime**			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
GBP	USD	USD	GBP	GBP	KRW	PLN	USD
KRW	GBP	EUR	USD	PLN	PLN	GBP	EUR
JPY	JPY	KRW	EUR	AUD	EUR	CAD	GBP
PLN	EUR	PLN	KRW	CAD	USD	KRW	KRW
EUR	KRW	JPY	JPY	EUR	GBP	AUD	AUD

Table C. 11 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bitfinex 12-2017.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
CAD	GBP	EUR	KRW	GBP	GBP	PLN	USD
USD	JPY	PLN	USD	AUD	USD	GBP	GBP
EUR	AUD	USD	GBP	PLN	JPY	AUD	JPY
GBP	KRW	CAD	JPY	CAD	KRW	EUR	EUR
JPY	USD	JPY	AUD	USD	EUR	CAD	KRW

Table C. 12 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bitfinex 5-2018.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
PLN	JPY	PLN	JPY	PLN	AUD	PLN	EUR
AUD	USD	AUD	USD	AUD	EUR	AUD	AUD
GBP	CAD	GBP	EUR	CAD	KRW	CAD	JPY
CAD	EUR	EUR	KRW	KRW	JPY	KRW	USD
EUR	KRW	CAD	PLN	GBP	GBP	GBP	GBP

Table C. 13 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bitfinex 2-2020.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
AUD	EUR	PLN	EUR	CAD	GBP	CAD	GBP
PLN	GBP	AUD	USD	PLN	PLN	PLN	PLN
CAD	JPY	CAD	JPY	GBP	USD	GBP	USD
GBP	USD	GBP	GBP	KRW	EUR	KRW	EUR
KRW	KRW	KRW	KRW	EUR	KRW	EUR	KRW

Table C. 14 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Bithumb 6-2017.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
GBP	KRW	PLN	USD	GBP	EUR	PLN	USD
AUD	PLN	GBP	EUR	PLN	JPY	EUR	KRW
PLN	CAD	CAD	GBP	EUR	USD	JPY	EUR
KRW	EUR	KRW	KRW	JPY	KRW	GBP	JPY
CAD	USD	AUD	AUD	AUD	GBP	AUD	AUD

Table C. 15 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Coinmama 2-2019.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
CAD	AUD	EUR	USD	AUD	EUR	EUR	JPY
EUR	JPY	PLN	JPY	CAD	USD	CAD	USD
PLN	KRW	KRW	KRW	EUR	JPY	PLN	KRW
AUD	EUR	CAD	AUD	KRW	AUD	AUD	AUD
USD	USD	AUD	EUR	PLN	CAD	KRW	PLN

Table C. 16 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Trident 3-2020.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
CAD	KRW	CAD	USD	PLN	PLN	PLN	JPY
PLN	USD	PLN	EUR	GBP	JPY	GBP	USD
AUD	EUR	AUD	JPY	CAD	CAD	CAD	PLN
GBP	GBP	GBP	GBP	KRW	USD	KRW	EUR
JPY	JPY	JPY	KRW	USD	EUR	AUD	CAD

Table C. 17 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Keepkay 5-2020.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
AUD	GBP	PLN	GBP	CAD	JPY	PLN	JPY
CAD	AUD	CAD	JPY	GBP	USD	GBP	USD
GBP	PLN	GBP	USD	PLN	KRW	CAD	KRW
PLN	KRW	AUD	KRW	AUD	CAD	AUD	EUR
EUR	JPY	EUR	AUD	KRW	EUR	KRW	GBP

Table C. 18 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Ledger 7-2020.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
GBP	EUR	PLN	EUR	PLN	JPY	PLN	JPY
PLN	USD	CAD	USD	CAD	EUR	CAD	USD
AUD	CAD	GBP	JPY	GBP	USD	AUD	GBP
CAD	AUD	AUD	KRW	KRW	GBP	GBP	EUR
KRW	KRW	KRW	CAD	AUD	KRW	KRW	KRW

Table C. 19 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Yapizon 4-2017.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
KRW	PLN	KRW	CAD	EUR	EUR	KRW	USD
EUR	USD	GBP	PLN	KRW	USD	EUR	EUR
GBP	CAD	EUR	USD	CAD	PLN	USD	KRW
USD	EUR	PLN	EUR	PLN	CAD	JPY	PLN
PLN	KRW	USD	AUD	USD	KRW	GBP	CAD

Table C. 20 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Zaif 9-2018.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
CAD	AUD	USD	USD	AUD	GBP	PLN	JPY
KRW	JPY	EUR	EUR	EUR	JPY	AUD	USD
PLN	EUR	JPY	JPY	KRW	USD	KRW	KRW
AUD	USD	CAD	AUD	PLN	EUR	EUR	GBP
GBP	PLN	GBP	GBP	GBP	KRW	GBP	EUR

Table C. **21** Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Binance 5-2019.

Pre the Cybercrime				Post the Cybercrime			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
PLN	JPY	PLN	USD	AUD	GBP	CAD	EUR
AUD	KRW	AUD	JPY	CAD	EUR	PLN	USD
CAD	USD	CAD	EUR	PLN	KRW	AUD	JPY
KRW	EUR	KRW	KRW	KRW	PLN	KRW	KRW
GBP	AUD	GBP	AUD	USD	USD	JPY	AUD

Table C. **22** Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on Cashaa 7-2020.

Pre the Cybercrime				**Post the Cybercrime**			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
PLN	GBP	CAD	GBP	AUD	GBP	AUD	GBP
AUD	USD	PLN	KRW	CAD	USD	CAD	USD
CAD	AUD	EUR	USD	PLN	CAD	PLN	JPY
JPY	KRW	JPY	EUR	EUR	JPY	EUR	KRW
KRW	EUR	USD	JPY	JPY	KRW	KRW	EUR

Table C. 23 Top senders and receivers of ETE in the cross-market Bitcoin prices network, pre- and post-cyberattacks on KuCoin 9-2020.

Pre the Cybercrime				**Post the Cybercrime**			
In-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength	IN-Node Degree	Out-Node Degree	In-Node Strength	Out-Node Strength
AUD	EUR	AUD	EUR	AUD	JPY	PLN	JPY
GBP	KRW	PLN	USD	CAD	EUR	CAD	EUR
PLN	JPY	GBP	KRW	PLN	KRW	AUD	KRW
CAD	USD	CAD	JPY	GBP	AUD	GBP	USD
JPY	GBP	JPY	GBP	KRW	GBP	KRW	AUD

Table C. 24 Bai & Perron test results.

	Platform	Date of breach	Break point
1	Bithumb	30/6/2017	28/06/2018
2	Coinmama	15/2/2019	16/02/2020
3	Trident Crypto Fund	05/03/2020	06/03/2020
4	Trezor, Ledger, and Keepkay	24/5/2020	22/05/2021
5	Ledger	29/7/2020	30/07/2021
6	Bitfinex	21/02/2017	23/02/2017
7	Bitfinex	15/06/2017	15/06/2017
8	Bitfinex	12/12/2017	13/12/2017
9	Bitfinex	06/05/2018	08/05/2018
10	Bitfinex	27/02/2020	26/02/2021
11	Yapizon	22/04/2017	24/04/2017
12	Zaif	20/09/2018	20/09/2019
13	Binance	07/05/2019	08/05/2019
14	Cashaa	11/07/2020	11/07/2020
15	KuCoin	26/9/2020	28/09/2021