# Event Characteristics of Crypto Currency and Security

**Jin-Keun Hong**

***Abstract: Recently, there has been a continuous occurrence of a security incident on a crypto currency exchange. This background is not related to the current social situation. This is because the social interest in crypto currency provides an attacker with a chance to attack. In this paper, we have started to investigate the relationship between crypto currency and security incidents of block chain.***

***This paper focuses on analysis of crypto currency event of block chain. In this paper, we analyzed the amount of Google data retrieval around specific keywords during a specific period. And we analysis the relevance of this keyword to specific keywords related to security. For example, we analyzed the decrypted bitch coin or etherium, the nice money exchange, nicehash, coincheck, BTCglobal, BITGRAIL, Blackwallet.***

***We are focused on the relationship between the time of the security incident and the public awareness of the related crypto currency exchange. According to the results of the study, it can be assumed that a security incident occurred at a certain point in each exchange. Through this study, we were able to confirm public interest in crypto currency miners. I was able to confirm the degree of interest by time. Cryptographic digger was mainly focused on BitMiner, CGMiner, MultiMiner, and BFGMiner. Most of the public interest in these mining equipment is peaking in December 2017. We also looked at public interest in cryptic bit coin and etherium, mainly in December 2017.***

***The results of this paper can be used to analyze the point of time of the attack on the crypto currency exchange. Crypto currency exchange attacks will continue to occur in the future. If so, when is this attack going to take place? At that point, we need to know at what point the exchange will have public interest. At that point, we should also look at the exchange for vulnerabilities.***

***Keywords : crypto currency, miner, attack, block chain, security***

## I. INTRODUCTION

When social issues arise, there are increasing instances of hacking based on this issue, seeking economic profit, gaining reputation, harming other countries or businesses, and cutting confidential information [1].

We often talk about are economic, social inequality, education, labor and occupation, mass media, health, crime, and environmental issues of block chain. However, these social issues of block chain are closely related to hacking in terms of security.

Social news refers to personalized news, such as Facebook, Twitter, etc., depending on how you use news articles from multiple sources of block chain and crypto currency. Social news sources provide a personalized experience for voting, liking, commenting, sharing, and displaying news based on interaction of block chain.

Lei Xu et al. [2] proposed a trust-based collaborative management mechanism that considers privacy in a social network environment that poses a risk to individual privacy [2]. This study deals with threats that arise from information sharing between people and people in an online environment. In this study, we use a weight based on opinions to measure user 's reliability.

Jose proposed a mechanism based on text mining and fuzzy logic for the identification of access credentials in social networks [3]. This is used to detect identity theft, taking into account frequently used words and the frequency of context. In this paper, factors such as the logon location and the number of messages sent are used as factors for decision. This paper can be said to be effective for social network identity detection. This approach also links social networks with security issues.

Marc et al. Use a graph model for big data structuring. In this study, Flink based Graph X is compared and evaluated in a graph processing framework environment based on Spark and Gelly. The topic of interest in the research is how to efficiently calculate and visualize in big data processing [4].

Michael et al. [5] have investigated approaches that define user characteristics based on social activities and language usage habits. In this study, machine learning algorithms, data sources and feature sets are considered. In this paper, it is analyzed the characteristics of Facebook users in detail. In other words, we analyze social network and structure of language function related to person interaction. The study focuses on personal activities and language orientation in the facebook environment.

Hugo et al. [6] have detected cyber violence automatically and have dealt with countermeasures against it. We apply deep learning technology to detect cyber violence and propose CNN - LSTM and CNN - LSTM - DNN which are based on neural network.

Youyang et al. proposed a hybrid privacy protection system considering privacy and location information [7]. In this study, a game - based Markov decision process is proposed.

Eric et al. attempt to solve this problem by creating a data set at the capture-the-flag event held at DEFCON [8]. We propose an argument model based on the inference framework.

**Revised Manuscript Received on September 25, 2019**

**Jin-Keun Hong,** Division of ICT, Baekseok University, Cheonan City, South Korea. Email: jkhong@bu.ac.kr

It focuses on improving the performance of the classification scheme to identify cyber attackers.

Shancang et al. emphasize the importance of the cyber physical social system to the business environment and living environment. In this paper, we propose a Hybrid Bayesian risk graph model for analyzing CPSS related risks and analyzing attack activity patterns in cyber - physics social network environment. To this end, we introduce a hidden Markov model and propose a Bayesian risk graph to evaluate risk propagation in a layered risk structure.

Tien and others are interested in compromised accounts in online social networks [10]. In this study, the language model is searched based on the artificial neural network and the user 's writing style is specified in the short text message. And to identify ways to identify a corrupted user account.

Alexei et al. [11] studied the possibility of analyzing and creating social graphs by estimating the possibility that an attacker might affect users. This study focuses on the composition and analysis of social graphs and is interested in analyzing the spread trajectory of social engineering attacks.

Based on the previous research, this paper argues that social issues and security intrusions are related. The composition of this paper is as follows. Section 2 discusses the relationship between crypto currency and security. Section 3 discusses this issue in more detail, focusing on specific keywords, with relevance to crypto currency issues and security incidents. Chapter 4 concludes the paper.

## II. ISSUE OF CRYPTO CURRENCY AND SECURITY

Social media sites are becoming a new cyber-weapon. The background to this view is that cybercriminals are not involved in all social networks. In other words, this means that cybercriminals are participating in social networks and expressing their views and using information provided by social networks as crypto currency attack information. In many cases, malicious activity is taking place through communication channels with information exposed. In the case of organizations and companies, unsafe social media practices are decreasing the brand value of organizations and companies. It also poses a serious risk to the entire organization, including customers and executives. According to the US FBI announcement, social media incidents have increased significantly.

The problem is that social networks themselves do not protect their environment. This is because cyber attackers and terrorists are targeting this, while social networks are fundamentally limited. Cyber attackers can work on any social network. This makes it very easy for attackers to manipulate data on social networks.

Social media of crypto currency becomes essential data information in big data environments. The question is how to efficiently integrate and analyze these social media content. It is very important to create an environment that can prevent security incidents and efficiently cope with security incidents. Because we think there is a close relationship between security incidents and crypto currency issues. Social issues of crypto currency need to be recognized and analyzed in real time.

Potential security incidents can range from crimes in the neighborhood to infrastructure, public transport, and natural disasters and weather issues. When large data access, refinement, analysis, and processing of such individual information are efficiently performed, security incidents can be prevented in advance. It should be noted that security threats are increasingly being created through social media. In a social network environment, malicious technicians can use their tools or platforms to threaten their organizations.

In order to prevent security incidents, real-time awareness is very important. In order to realize this real-time awareness, it is necessary to collect crypto currency information efficiently through social media. Therefore, it is best to find the information necessary to prevent security incidents. The best way to gather real-time information is to use social media over existing news channels. Therefore, it is necessary to efficiently collect information on social media about crypto currency and properly process it. The important thing is to enable keyword search. And how to have an automated process that can efficiently identify the big data content.

Among the risk factors of social media are shared information. The information such as birthday, education, affiliation, or family relationship information in social media account, is personal information. However, personal information such as e-mail can be guessed through social networks. Therefore, social media accounts can be the attacker's attack route. The more information that is disclosed to social networks, the greater the risk of exposure to information. Another risk factor is attack from phishing or spear phishing. This allows an attacker to steal a user's account and act on behalf of a friend or family member. On the other hand, comments posted on social networks of crypto currency can attract attackers and become targets of attacks. IDs and passwords used in social networks can be attacked if they do not have to set a unique password.

In this paper, we have examined the relevance of keywords and security incidents in social networks in real Google data with the relationship between these social networks and security issues. In Chapter 3, we will look at this issue based on Google data keyword search information.

## III. CASE OF CRYPTO CURRENCY ATTACK

First of all, it concerns the public interest in this malware that has become a social issue before and after security incidents and security incidents caused by malware.

As shown in figure 1, from December 2017 to January 2018, new malware was observed in the order Kovter, WannaCry, Emotet, Zeus, CoinMiner, and Gh0st. Among them, Kovert accounted for 55% of the top 10 malware. Nevertheless, based on Google data, WannaCry was the most popular malware. The following figure shows the volume of searches based on Google data for four malware out of the observed malware in January 2018. Among the malware,

WannaCry is the highest, and on May 12, 2017, the malware caused a massive cyber-attack using WannaCry malware. This indicates that WannaCry is the most affected malware in relation to social issues. Warner Cry, spread by the massive cyber-attacks worldwide on May 12, 28 days after being released by the shadow brokers on April 14, 2017, infected more than 120,000 computers in 99 countries.

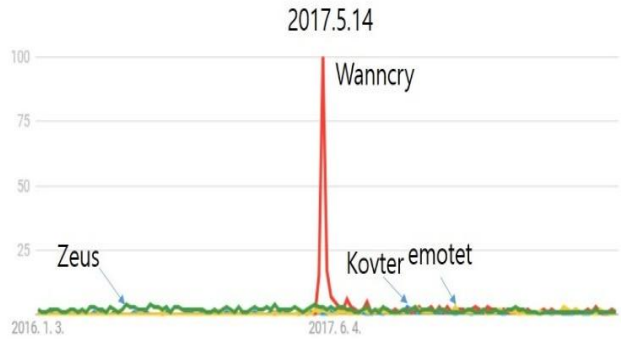


Fig. 1. Google Search Quantities of "Malware Kovter," "WannaCry," "Emotet," "Zeus"

Next, this paper looked at the social interest in crypto currency malware. Interest in crypto currency has recently been rising. Interest in cryptographic mining software in these environments is also increasing. Social interest of malware of crypto currency mining has been on the rise since May 2017, as shown in the following figure. However, this WannaCry ransomware encrypts 176 file formats for MS documents, database files, and multimedia files. However, this WannaCry infects using CVE-2017-0144 vulnerability.


Fig. 2. Google Search Quantities of "Cryptocurrency mining malware"

In figure 2, business interest in this crypto currency mining grew in 2017, but in February 2017, interest in BitMiner was particularly high. As of December 2017, interest in CGMiner, BFGMiner, MultiMiner and so on has increased. This phenomenon reflects the social issue of crypto currency at that time. BiMiner is one of the rudimentary bit mining software. CGMiner is a state-of-the-art bit-mining software that improves CPU Miner and improves graphics card and GPU mining capabilities. BFGMiner runs on an ASIC basis and is identical to CGMiner. MultiMiner is a bit mining software based on Linux, MAC OS and MS.

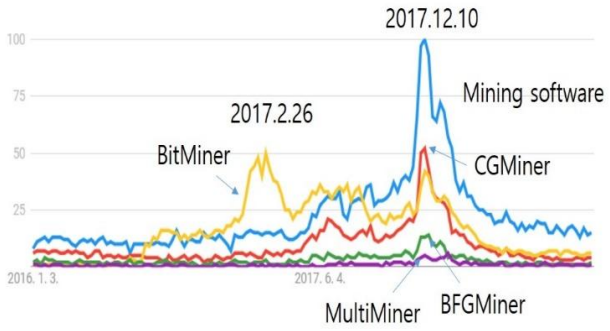


Fig. 3. Google Search Quantities of CryptMiner Software : "BitMiner," "CGMiner," "BFGMiner," "MultiMiner"

As shown in the following figure 3, social interest in the crypto currency "bitcoin", "Ethereum", "Litecoin", "Monero", and "Zcash" began to rise at May 21, 2017, Respectively, of course, "Bitcoin" is the most interesting source of money in the currency.

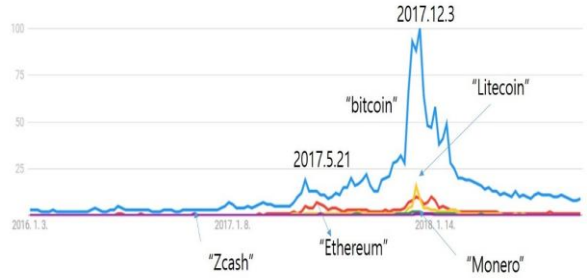


Fig. 4. Google Search Quantities of "bitcoin," "Ethereum"

Looking at figure 4 below, the public's interest in crypto currency has peaked at 31 December 2017 and has declined until May 20, 2018. Since then, it has maintained a certain level of interest. Interest in crypto currency began to increase on May 21, 2017. Interest in the block chain peaked on December 10, 2017.

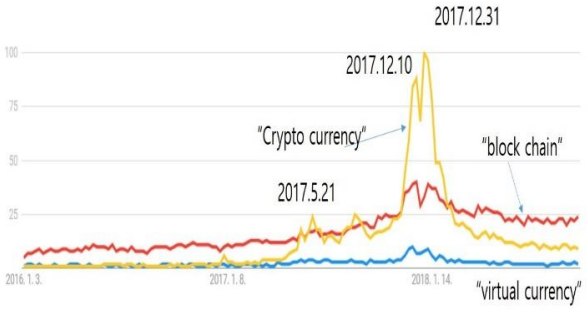


Fig. 5. Google Search Quantities of "block chain"

As shown in figure 5, social interest in crypto currency has increased as of May 21, 2017 and has risen sharply as of December 10, 2017. The highest peak is reached on December 31st. And interest in this is downwardly curved. The block chain has the highest peak on December 10, 2017, followed by a decline in the downward trend, maintaining a certain level of interest to date. The public interest in virtual currency will peak at December 10, 2017.

In figure 6, hacking on the Nicehash crypto currency exchange took place in December 2017 with a $ 62million takeover. Figure 6 shows that interest in the exchange has increased since 6 months before the hacking of the exchange.

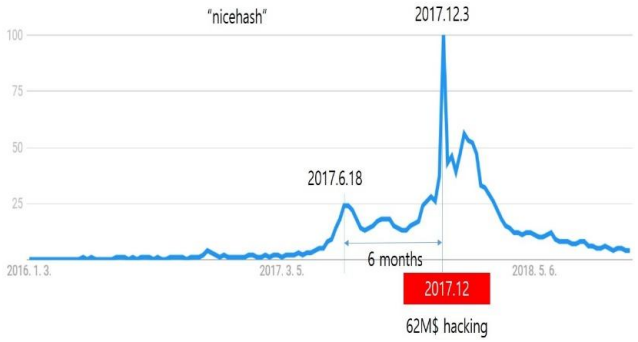


Fig. 6. Google Search Quantities of "nicehash cryptocurrency exchange"

In figure 7, hacking for the Coincheck crypto currency exchange occurred in January 2018. The amount of the stolen was 400milion $. Interest in this exchange, however, started in May 2017.


Fig. 7. Google Search Quantities of "coincheck cryptocurrency exchange"

In figure 8, hacking for the BTCglobal crypto currency exchange occurred in March 2018. At this time, the amount of stolen was 50milion $. However, interest in this exchange started in November 2017, and it was at the time of December 2017 that interest increased more than the schedule. Interest in this exchange began at least four months before the hacking of the exchange occurred. The BTCglobal crypto currency exchange has been sufficient for attackers since November 2017. As a result, after scanning, attackers have taken passwords based on vulnerable security management.

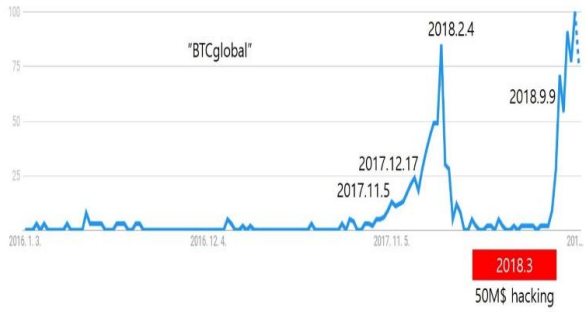


Fig. 8. Google Search Quantities of "BTCglobal cryptocurrency exchange"

In figure 9, hacking on the BTCGRAIL crypto currency exchange occurred in January 2018. Interest in this exchange, however, began in December 2017, a month earlier


Fig. 9. Google Search Quantities of "BITGRAIL cryptocurrency exchange"

In figure 10, the attack on the Blackwallet crypto currency exchange took place in January 2018. However, interest in the exchange started three months ago in October 2017.

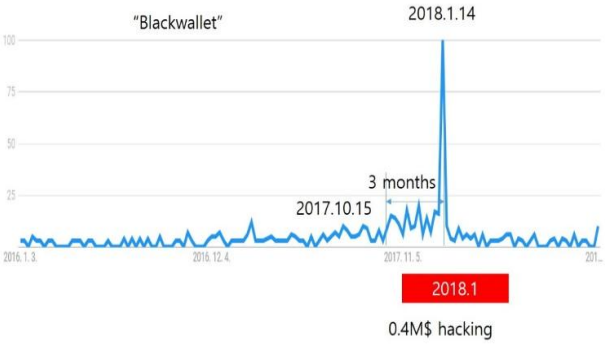


Fig. 10. Google Search Quantities of "BLACKWALLET cryptocurrency exchange"

## IV. CONCLUSION

In this paper, we have started to analysis the relationship between crypto currency and security incidents of block chain. This paper focuses on case studies of crypto currency of block chain. In this paper, we analyzed the amount of Google data retrieval around specific keywords during a specific period. And we investigated the relevance of this keyword to specific keywords related to security. We examined the relationship between the time of the security incident and the public awareness of the related crypto currency exchange. According to the results of the study, it can be assumed that a security incident occurred at a certain point in each exchange. Through this study, we were able to confirm public interest in crypto currency miners. The results of this study can be used to analyze the point of time of the attack on the crypto currency exchange.

## ACKNOWLEDGMENT

This paper is sponsored of project funding of Industrial Academia Cooperation in Baekseok University.

## REFERENCES

1. Ridhanshi Bhatia, Praveen Kumar, Shilpi Bansal, Seema Rawat, "Blockchain the technology of crypto currencies," in ICACCE2018, https://doi.org/10.1109/ICACCE.2018.8441738

2. Lei Xu, Chunxiao Jiang, Nengqiang He, Zhu Han, Abderrahim Benslimane, "Trust based collaboriative privacy management in online social networks," IEEE Transaction on Information Forensics and Security, 14(1), pp. 48-60, 2019, https://doi.org/10.1109/TIFS. 2018. 2840488
3. Jose A. Concepcion Sanchez, Jezabel Molina Gil, Pino Caballero Gil, Ivan Santos Gonzales, "Fuzzy logic system of identity theft detection in social networks," in ICBA2018, https://doi.org/10.1109/ Innovate -Data.2018.00017
4. Marc Kaeske, Olaf Zukunft, "A comparative evaluation of big data framework for graph processing," in ICBDA2018, https://doi.org/ 10.1109/Innovate-Data.2018.00012.
5. Michael M. Tadesse, Hongfei Lin, Bo Xu, Liang Yang, "Personality predictions based on user behaviour on the Facebook social media platform," IEEE Acess:1-1, 2018, https://doi.org/10.1109/ACCESS. 2018.2876502
6. Hugo Rosa, David Matos, Ricardo Ribeiro, Luisa Coheur, Joao P. Carvalho, "A deeper look at detecting cyberbullying in social networks," in IJCNN2018, http://doi.org/10.1109/IJCNN. 2018. 8489211
7. Youyang Qu, Shui Yu, Longxiang Gao, Wanlei Zhou, Sancheng Peng, "A hybrid privacy scheme in cyber physical social networks," IEEE transaction on computational social systems, 5(3), pp. 773-784, 2018, https://doi.org/ 10.1109/TCSS.2018.2861775.
8. Eric Nunes, Paulo Shakarian, Gerardo I. Simari, Andrew Ruef, "Argumentation models for cyber attribution," in IEEE/ACM ASONAM2016, https://doi.org/ 10.1109/ASONAM.2016.7752335
9. Shancang Li, Shanshan Zhao, Yong Yuan, Qindong Sun, Kewang Zhang, "Dynamic security risk evaluation via hybrid Bayesian risk graph in cyber physical social system," IEEE Transaction on computational social systems, pp. 1-9, 2018, https://doi.org/10.1109/ TCSS.2018.2858440
10. Tien D. Phan, A. Nur Zincir Heywood, "A language model for compromised user analysis," in NOMS2018, https://doi.org/10.1109 /NOMS.2018.8406317
11. Alexei Suleimanov, Maksim Abramov, Alexander Tulupyev, "Modelling of the social engineering attacks based on social graph of employees communications analysis," in ICPS2018, https://doi.org/ 10.1109/ICPHYS.2018.8390809.

## AUTHORS PROFILE

**Jin-Keun Hong** Professor in division of ICT in Baekseok University of South Korea.

It was register at Marquis Who's Who in the world, IBC, and ABI human dictionary.

His research issue is convergence information security technology. Especially, he is focusing on C-ITS and future security technology prediction.