The Crypto-currency and Cyber-attack: Evidence from Causality Techniques

Ersin Caglar[*1], Dervis Kirikkaleli[#2]

[1]European University of Lefke, Department of Management Information Systems, Northern Cyprus, TR-10 Mersin, Turkey

[2]European University of Lefke, Faculty of Economic and Administrative Sciences, Department of Banking and Finance, Lefke, Northern Cyprus, TR-10 Mersin, Turkey

[1]ecaglar@eul.edu.tr, [2]dkirikkaleli@eul.edu.tr

Abstract *- With the rapid development of internet and information technology, crypto-currency has become accessible technology established on the blockchain. Based on popular demand, cryptocurrencies are available in the internet environment. Bitcoin is the most popular one among the crypto-currencies. Recently, the USA, Japan, and Canada have accepted Bitcoin as a method of payments in various business platforms as an alternative to currencies. With this opportunity, cryptocurrency and Bitcoin have gained a few disadvantages, such as insecurity and cyber-attacks. This paper aim is to investigate if there exists a causal linkage between BC (Bitcoin price) and CA (cyber-attack) in the USA by using monthly data, covering the period 2010M07 to 2017M06. We employed traditional Granger causality and Toda-Yamamoto causality tests as a robust causality test. We also performed the newly-developed Fourier Toda-Yamamoto causality test to capture gradual developed structural changes. Our findings reveal that there is unilateral (independent) causality that runs from BC to CA. In other words, changes in BC significantly led to changes in CA in the USA.*

Keywords — *Crypto-currency, Cyber-attack, Blockchain, Bitcoin, Fourier Toda-Yamamoto causality, Granger causality*

I. INTRODUCTION

With the rapid improvement of information technologies and the internet, electronic currencies have gradually become popular in recent years, which provide many conveniences for people trading online. This new type of currency is virtual emerging, performed as a digital representation of value, having no physical store, in contrast to currency [17]. Approximately 2000 cryptocurrencies are available in the internet environment. Table 1 illustrates the 20 representative cryptocurrencies listed in CoinMarketCap as the top 20 cryptocurrencies used as market value [26]. By definition, cryptocurrency is some kind of currency that uses block-chain technology with cryptography to secure transactions and to verify the transfer of digital assets over the internet without a centralized banking system [11].

TABLE I

CRYPTOCURRENCIES ACCORDING TO MARKET CAPITALIZATION

Rank	Name	Symbol	Market cap.	Launch date
1	Bitcoin	BTC	$60,487,274,403	03/01/2009
2	Ripple	XRP	$12,332,456,700	01/01/2013
3	Ethereum	ETH	$9,412,363,620	30/06/2015
4	Stellar	XLM	$2,242,342,123	31/07/2014
5	Bitcoin Cash	BCH	$1,849,915,763	01/08/2017
6	EOS	EOS	$1,721,739,810	31/01/2018
7	Bitcoin SV	BSV	$1,630,340,022	15/11/2018
8	Litecoin	LTC	$1,462,669,804	07/10/2011
9	TRON	TRX	$876,293,455	25/06/2018
10	Cardano	ADA	$774,454,858	02/10/2017
11	Monero	XMR	$736,489,666	18/04/2014
12	NEM	XEM	$644,111,777	31/03/2015
13	MIOTA	MIOTA	$638,974,642	11/06/2016
14	Dash	DASH	$583,803,256	18/01/2014
15	Ethereum Classic	ETC	$414,897,833	30/07/2015
16	NEO	NEO	$397,103,949	17/10/2016
17	Zcash	ZEC	$304,593,595	28/10/2016
18	Dogecoin	DOGE	$244,170,721	06/12/2013
19	Tezos	XTZ	$216,903,705	02/09/2014
20	VeChain	VET	$210,400,115	30/06/2018

Source: CoinMarketCap

A. Blockchain and Bitcoin

Historically, in 1991, a group of researchers invented blockchain, and they intend to mark the timestamp of digital documents so that it is possible to restore or tamper with them. According to the researchers, blockchain is a collection of nodes (computers) that all have the same history of transactions, validated by every new computer that developed to be part of the transaction [23]. In other words, blockchain is a collection of blocks that distribute, decentralized, and shared "state machine." According to researchers, this means that all connecting nodes will independently hold and save their copy of the blockchain, and the current known "state" calculated by processing every transaction in the order of their appearance in the blockchain [27]. With these opportunities, blockchain can be used in various fields such as healthcare, telecommunications, and finance [8], respectively.

Crypto-currency is another area where blockchain technology is performing. In the internet environment, there are other kinds of cryptocurrencies, namely Bitcoin, Ethereum, and Ripple. Some studies argued that cryptocurrencies are not money, while others have opposed the idea and accept cryptocurrencies as money [20, 7]. At the same time, some governments, like Japan and Canada, have accepted cryptocurrencies as a method of payment [24]. Further, in the USA, the Financial Crimes Enforcement Network (FinCEN) defines Bitcoin as a medium of exchange but not an official US currency [12].

As shown in Table 1 above, Bitcoin has much more market capital than the others do; in regard, the concept of Bitcoin is no longer new; it is almost ten years since the idea was to introduce on the currencies markets [16]. As noted, a group of hackers or a single hanker under the name Satoshi Nakamoto created Bitcoin based on blockchain technology [14]. Accordingly, Bitcoin is a peer-to-peer (P2P) and decentralized financial system; widely, it is the first system of currency that is beyond the control of any monetary or government power [13]. Because of this relevant, Bitcoin has no third-party transactions, all results of transactions recorded in a public distributed ledger as a blockchain [2].

Bitcoin is old technology; however, it is only in recent years when Bitcoin has attracted much attention from many sectors, such as academics and industry practitioners. In 2017, the Bitcoin market value increased to a maximum of almost $19,500 per 1 BTC [25]. Now a day, the momentum of Bitcoin continues rising and is being supported by many countries [1]. Apart from this popularity and advantages, Bitcoin has many vulnerabilities protection problems and illegal actions [22]. Hence, Bitcoin is at all times a clear target by hackers [21; 20].

A new developing show that, now a day, Bitcoin carries a severe cyber risk due to cyber-attacks. Researchers have noted cyber-attack to be an attack launched from one or more computers against other computer devices or networks [10]. Unfortunately, Bitcoin is an instrument of computer led-online transactions; it assumed to be vulnerable to cyber-attacks. Therefore, the purpose of this article is to test whether there is a link between Bitcoin and cyber-attacks.

II. Data and Methodology

Based on the literature and other attributes of cryptocurrencies, such as lack of regulation, no inflationary pressures, low transaction costs, anonymity, and price volatility, the latter has particularly have attracted investors' attention. Thus this study investigates the link between Bitcoin and cyber-attacks employing time series variables covering the period of 2010M7 to 2017M6 (84 observations). Specifically, variables of interest include CA and BC. CA and BC dataset were extracted from the VIZSET and investing.com, respectively.

This paper employed the econometric techniques of augmented Dickey-Fuller (ADF) unit root test developed by Dickey and Fuller (1979) [3], and Elliot Rothenberg and Stock (1996) [4] modified the ADF test of Dickey and Fuller (1979), which are Dickey-Fuller Generalized Least Squares (DF-GLS). The main advantage of these modified versions of the ADF test is that it provides improved power over the ADF test when an unknown trend exists. Therefore, in this paper, we employed DF-GLS and ADF tests at the same time to check the order of integration in the variables. Further, we performed the Granger causality –proposed by Granger (1969), Toda-Yamamoto causality - proposed by Toda and Yamamoto (1995), and Fourier Toda-Yamamoto causality - proposed by Nazlioglu et al. (2016) [15], respectively. Particularly, we employed Granger (1969) linear causality test to investigate whether the G time series variable causes the M time series variable or vice versa. The model specifications of the Granger causality test are [6]:

Eq.(1); $BC_t = \beta_1 + \sum_{i=1}^{n} \alpha_1 CA_{t-i} + \sum_{i=1}^{n} \mu_1 BC_{t-i} + e_t$

Eq.(2); $CA_t = \beta_2 + \sum_{i=1}^{n} \alpha_2 CA_{t-i} + \sum_{i=1}^{n} \mu_2 BC_{t-i} + e_t$

Where n indicates the numbers of lag, which were determined by the information criteria, β_{1-2}, α_{1-2}, and μ_{1-2} are parameters for estimation, and e_t is a residual term.

Following, Toda and Yamamoto (1995) modified Wald test statistic (MWALD), the bias in models are augmented by VAR analysis. To deal with smooth structural shifts, we also perform Fourier Toda-Yamamoto causality test, which is embedded in a Fourier approximation. Also, to have information about the number, dates, and forms of structural breaks, we used the developed version of the Toda-Yamamoto causality test [5].

III. Empirical Findings

Holding to the research methodology, in order to explore the causal link between BC and CA, we first employ ADF and DF-GLS unit root tests to check the order of integration of BC and CA variables. The results of ADF and DF-GLS tests for the BC and CA variables are in Table 2. The BC and CA variables seem non-stationary at these levels but at the first differences, the BC and CA variables are stationary at the 5% level, meaning that the order of integration of BC and CA variables is I (1).

TABLE II

Unit Root Test

	DF-GLS	ADF	DF-GLS	ADF
	(Including only constant)		(Including constant and trend)	
BC	1.081	1.832	-0.577	0.439
ΔBC	-8.763***	-8.744**	-9.229***	-9.165***
CA	-1.397	-2.364	-2.244	-2.215
ΔCA	-5.447***	-3.685***	-5.508**	-3.737**

Note: Δ symbol indicates the first difference of the variables. ** and ***denote statistically significant at the 5% and 1 % significance level, respectively.

After the unit root test, the next step is, we perform Granger causality, Toda-Yamamoto causality tests, and Fourier Toda-Yamamoto Causality tests, categorically. The main aims of this study are to check whether CA causes BC and whether BC causes CA by using the USA data. Our findings of these tests are illustrated in Table 3. The result of the Granger causality test shows that the null hypothesis of BC does not Granger cause CA; that is, it rejected the F-stat of 3.928, and the p-value is 0.011 at a 5 percent significance level. This implied that changes in BC led to subsequent changes in CA in the USA. This result shows that BC is an essential factor for CA. Contrary, the model for Granger causality failed to identify the causal link between CA and BC. It is worthy of mentioning that, these findings are in line with the findings of Toda-Yamamoto Causality, as shown in Table 3.

As mentioned by Kocaarslan et al. (2017) [9], in the VAR model, the size of frequency effects F-stats; therefore, we apply the bootstrap sampling and reported the bootstrap p-values for Fourier Toda-Yamamoto Causality test. The findings from traditional Granger causality and Toda-Yamamoto tests are consistent with that of Fourier Toda-Yamamoto Causality. This result suggests that the causality running from BC to CA shows the robust structural shifts in the series, and thus the result is highly robust or stronger [18].

TABLE III

Causality Tests

Granger Causality			F-stat.	P-value
CA	→	BC	0.568	0.637
BC	→	CA	3.928	0.011**
Toda- Yamamoto Causality			MWALT	P-value
CA	→	BC	2.034	0.565
BC	→	CA	8.779	0.032**
Fourier Toda- Yamamoto Causality			T-stat	P-value
CA	→	BC	1.711	0.634
BC	→	CA	10.756	0.013**

Note: ** and * indicate statistical significance at the 5% and 10% levels, correspondingly. Maximum integration number (k) and lag(p) are sets to 5 and 12, respectively, and then optimal k and p are determined by following modified LR test statistics (LR) and Hannan-Quinn information criterion (HQ). The optimal lag is determined as a three by the LR and HQ information criteria. → indicates the direction of causality. In the Fourier Toda-Yamamoto Causality, maximum integration number (k) is also selected at 1, while the number of Fourier is selected 2.

IV. CONCLUSION

With the rapid development of internet and information technology, the crypto-currency research topic has attracted many researchers. This study aims to shed further light on the characteristics of cryptocurrencies by exploring whether there is a causal linkage between Bitcoin price and cyber-attacks in the USA. The study covered monthly data from the period of 2010M07 to 2017M06. The present study employs Granger causality, Toda-Yamamoto causality and Fourier Toda- Yamamoto causality tests. Our findings reveal that there is unilateral causality runs from Bitcoin price to cyber-attacks, indicating that Bitcoin price is an essential predictor for cyber-attacks in the USA economy. This result allows investors to compare the return on Bitcoin price and cyber-attacks across asset classes. Although the present study identifies robust empirical findings, further studies should advance this research by adding other macro-level variables in order to capture the linkage between crypto-currencies and cyber-attacks.

REFERENCES

[1] P. Bartusiak, "*«Judicial Finding» of the Legal Nature of Cryptocurrency.*" *Ehrlich's Journal-Ерліхівський журнал* 2, pp. 24-36, 2018.

[2] M. Conti, et al. "*A survey on security and privacy issues of bitcoin.*" *IEEE Communications Surveys & Tutorials*, 20(4), pp. 3416-3452, 2018.

[3] D.A. Dickey, and W.A. Fuller, "*Distribution of the estimators for autoregressive time series with a unit root.*" *Journal of the American statistical association* 74.366a, pp.427-431, 1979.

[4] G. Elliott, T.J. Rothenberg, and J.H. Stock, *"Efficient tests for an autoregressive unit root (No. t0130)"*. National Bureau of Economic Research, 64(8), pp. 13-36, 1996.

[5] W. Enders, and J. Lee. *"A unit root test using a Fourier series to approximate smooth breaks"*. Oxford bulletin of Economics and Statistics 74.4, 574-599, 2012.

[6] C.W. Granger, *"Investigating causal relations by econometric models and cross-spectral methods."* Econometrica: Journal of the Econometric Society, 424-438, 1969.

[7] P.K. Hazlett, and W.J. Luther. "*Is bitcoin money? And what that means."* The Quarterly Review of Economics and Finance, 2019.

[8] İ. KIRBAŞ, *"Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları"*. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9(1), 75-82, 2018.

[9] B. Kocaarslan, et al. "*Dynamic correlations between BRIC and US stock markets: The asymmetric impact of volatility expectations in oil, gold and financial markets."* Journal of Commodity Markets, 7, pp. 41-56, 2017.

[10] E. Kopp, L. Kaffenberger, and N. Jenkinson. "*Cyber risk, market failures, and financial stability"*. International Monetary Fund, 2017.

[11] J.H. Lee, *"Rise of Anonymous Cryptocurrencies: Brief Introduction"*. IEEE Consumer Electronics Magazine, 8(5), pp. 20-25, 2019.

[12] P. Mullan, "*The digital currency challenge: Shaping online payment systems through US financial regulations"*. Springer, 2014.

[13] S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system"*. Manubot, 2019.

[14] S. Nakamoto, *"Bitcoin: A peer-to-peer electronic cash system,"* http://bitcoin. org/bitcoin. pdf. 2008.

[15] S. Nazlioglu, N.A. Gormus, and U. Soytas, "*Oil prices and real estate investment trusts (REITs): Gradual-shift causality and volatility transmission analysis*". Energy Economics, 60, pp. 168-175, 2016.

[16] M. Raskin, and D. Yermack, *"Digital currencies, decentralized ledgers and the future of central banking"*. In Research Handbook on Central Banking. Edward Elgar Publishing, 2018.

[17] H. Sebastião, and P. Godinho, "*Bitcoin futures: An effective tool for hedging cryptocurrencies"*. Finance Research Letters, 2019.

[18] H.Y. Toda, and T. Yamamoto, *"Statistical inference in vector autoregressions with possibly integrated processes"*. Journal of econometrics, 66(1-2), pp. 225-250, 1995.

[19] D. Yermack, "*Is Bitcoin a real currency? An economic appraisal*". In Handbook of digital currency (pp. 31-43). Academic Press, 2015.

[20] Sapirshtein, Y. Sompolinsky, and A. Zohar, "*Optimal selfish mining strategies in bitcoin. International Conference on Financial Cryptography and Data Security*". Springer, Berlin, Heidelberg, pp. 515-532, 2016.

[21] M. Apostolaki, A. Zohar, and L. Vanbever, "*Hijacking bitcoin: Routing attacks on cryptocurrencies*". In 2017 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 375-392, 2017.

[22] J. Zhu, P. Liu, and L. He, "*Mining information on Bitcoin network data*". In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 999-1003). IEEE, 2017.

[23] V. Vallois, and F.A. Guenane, "*Bitcoin transaction: From the creation to validation, a protocol overview*". In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-7). IEEE, 2017.

[24] S. Ghimire, and H. Selvaraj, "*A survey on bitcoin cryptocurrency and its mining*". In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE, 2018.

[25] F. Aiolli, M. Conti, A. Gangwal, and M. Polato, "*Mind your wallet's privacy: identifying Bitcoin wallet apps and user's actions through network traffic analysis*". In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 1484-1491, 2019.

[26] Z. Li, et al. "*A landscape of cryptocurrencies*." 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019.

[27] S. Erfani, and M. Ahmadi, "*Bitcoin Security Reference Model: An Implementation Platform*". *In 2019 International Symposium on Signals, Circuits and Systems (ISSCS)* (pp. 1-5). IEEE, 2019.