The Fluctuations of Bitcoin Price during the Hacks

Jiarun Hu[1], Qian Luo[2], Brain Jiaen[2]

[1] Fudan University, China

[2]Zhongnan University of Economics and Law, China

[2]DePaul University, USA

Abstract

Security breaches of the cryptocurrency exchanges usually cause the price fluctuation in the market. Approximately one hundred cryptocurrency thefts, including hacks and scams, has occurred since 2012 to 2018, half of which are hacks of Bitcoins. Based on the thirty Bitcoin hacks, this study portrays the general price pattern during the hack. And it illustrates the link between the size of the hack and the subsequent price change of Bitcoin. The tests reveal that the larger the volume of the hack, the stronger the price drop. However, a similar obvious relationship does not exist for the recovery of the price. The study might be the first piece of research focus on the hacks and the price pattern in a short time period.

Keywords: Bitcoin price, price fluctuation, Bitcoin hack, cryptocurrency thefts

1. Introduction

Cryptocurrencies have caught the global attention for its unique way of the transaction and the vibrant price movements in recent years, especially at the end of 2017 when the prices of major cryptocurrencies hit historical maxima. Among all cryptocurrencies, Bitcoin is the most prominent open source peer-to-peer cryptocurrency which is operating without central authority (Nakamoto, 2008). Cryptocurrencies bring a lower-cost way of transferring assets, especially in international commerce in which the comparatively intricate procedure is required through fiat currency exchange. On the other hand, cryptocurrency serves not only as an electronic medium of exchange but also as a speculative investment asset with trading available 24-hours a day, seven days a week.

Digital currencies achieve decentralization and convenience but so far only at the cost of lower security and higher volatility. From June 13th in 2011 to February 5th in 2019, there are more than one hundred occurrences of cryptocurrency thefts (hacks and scams), of which the cases of Bitcoin thefts account for more than 90% of the total occurrences. Specifically, there are mainly two types of theft: hacks and exit scams. The exit scam cases are a basic human fraud and as such market participants do not blame the cryptocurrencies directly for them. Conversely, hacks usually bring into question the suitability and sustainability of cryptocurrency projects and thus cause the price to change. With more transactions through Bitcoin and larger investment volume from the capital market, the potential risk toward Bitcoin exchange security becomes higher than all the other time period. On February 7th of 2014, one of the largest Bitcoin exchanges in the world, Mt. Gox (Magic the Gathering Online Exchange), reported a major hack of approximately 460 million USD involving 700,000 bitcoins which at the time was 7% of the total volume of the bitcoin (DeVries, 2016). Another characteristic of bitcoin is the high volatility of its price. Although Bitcoin started at nearly zero value in 2009, the price ended around $1100 at the December of 2013. A year later, the price dropped below $300 and then started a powerful revert, resulting in a boost to $19,000 (Ciaian, Rajcaniova, & Kancs, 2016). Another dramatic example to show its price volatility is on May 22nd of 2010, the IT engineer Laszlo Hanyecz ordered a pizza with 10,000 BTC when the price of per bitcoin used to be 0.33 USD while in December of 2017, this amount of bitcoin could make him a ten billion fortune.

According to the prior researches on the topic of Bitcoin price, the traditional market determinants and digital currency-specific factors are identified as two significant factors to the price formation of Bitcoin (Ciaian et al., 2016). However, when a haphazard cryptocurrency hack happens, not only will the exchange lose a certain amount of currencies, but the value of the Bitcoins for all users will usually drop. Therefore, when the shock of a cryptocurrency hack disseminates to the market and public, the holders of Bitcoin will probably foresee the risk of a new price drop and sell the digital asset, thereby reducing its price further. Apart from the former condition of market shock, the hackers usually will transfer one cryptocurrency being hacked into another one, which usually will change the supply and demand of certain cryptocurrencies instantly.

In the present investigation, the historical price of 30 hacks (List 1 in Appendix) of Bitcoin hacks from 2012 to 2019 has been collected. For the reason that, of all kinds of cryptocurrency, Bitcoin has the most recorded hacks, the highest value and the most extensive market cap. As no research has been done to our knowledge on the impact of hacks on the Bitcoin price, we first collect the historical price data for each hack. This study investigates the hypothesis that there is an immediate price drop of Bitcoin following the news about a hack. In most cases, we find that the effect of hacks on price is negative on average, it causes the price drop in different levels but the degree to which price drops varies from large to insignificant, and even no impact in some cases. Further, we examine the impact that the scale of the hack has on the price drop by regressing the price change on the variable "adv" (the amount of bitcoin hacked divided by volume). The result shows statistical significance in the price change between 2 days before and the exact day hack happens, which proves that a hack with a larger volume will probably lead to a stronger price drop.

Another aspect of the research that we consider is the recovery of the price change after the hacks. First, however, it has to be noted that not all 30 hacks have a noticeable price decline for some hacks may have a limited scale against the market trading volume. Besides, the hacks might interfere with other material economic events. Nonetheless, by using the linear regression method, we do not find statistical significance with the scale of the hack (adv) and the price changes, which shows the hack itself is not a causal determinant for the post-hack period. However, the absolute amount of the stolen cryptocurrency has correlation with the price of the first and second day after the hack happens.

The paper is structured as follows: (2) Related works in the price and hacks of cryptocurrency area; (3) The dataset, variables the methods of the research; (4) The analysis of the research and cases study of Mt. Gox and Bitfinex Breach Hacks; (5) The conclusion and the discussion of the research. (1)

2. Related works

The topic of Bitcoin and the other cryptocurrencies has attracted a growing interest in the Bitcoin price analysis and the security risk study. However, the most of the prior researches investigate these two subjects separately. The analogous researches can be borrowed from the analysis of marketing reaction in stock market.

Among the researches of price analysis, Ciaian et al. (2016) analyze Bitcoin price formation from both the traditional determinants of currency price and digital currencies specific factors which illustrate the long-term price formation of Bitcoin price. Urquhart (2017) highlights prices ending with 00 decimals compared to other variations through his examination to Bitcoin prices for clustering, the potential trading benefit from such clustering and the determinants of the clustering.

In the security risk part, Feder and et al (2017) investigate how one such risk, distributed denial-of-service (DDoS) attack, affects the Bitcoin ecosystem and the potential to be financially lucrative from DDoS attacks on currency exchanges. Due to the extraordinary scale and influence, the Mt. Gox hack make itself a good sample for the researchers to analyze the relationship between the hacks and potential manipulation of the Bitcoin price.

Apart from the study that mainly focusing on one particular side of Bitcoin, Feng and Wang (2018) investigate informed trading in the Bitcoin market by examining the Bitcoin price sensitivity with the material events including events of market, government and hacking. By classifying the events into negative and positive ones, the research detects the quantiles of the order sizes of buyer-initiated and seller-initiated orders are abnormal and further test the timing of informed trading.

Inspired from a parallel research from the stock market, our research is similar to the market's reaction research of Carter and Simkins (2003). Unlike the earthquake and hurricanes for the airlines, the September 11th event had an influence on the all the US airline companies with no exception. Due to the panic emotion resulted from the catastrophic event, the airline company stocks plumped in the first trading date on September 17th, 2001. Further, they analyze the reaction of various airline stocks to estimate whether the price reaction was consistent with rational pricing. However, in our study toward the price of Bitcoin, more concerns are paid into the general pattern of fluctuation rather than the influence of the hack to the exchanges from the globe.

Besides, another two studies of stock price reaction to unexpected events are conducted by Salas (2009), Datta and Dhillon (1993). For instance, Salas estimated the stock market reaction to sudden executive deaths to illustrate how executive death as an unexpected event will influence the company's stock price in various conditions. Differently, Datta and Dhillon tested the reaction of stock market to unexpected earnings and found the response of the bond is symmetric with the stock market.

3. Data

The Bitcoin price data used in this paper are from Coinmarketcap.com from April 27th, 2013 to January 5th, 2019 and Investing.com for the previous data in 2012 and early 2013. We collect the historical daily price of Bitcoin during the hacks and the trading volume of the day when hacks happened. In order to observe the fluctuation during the hack, we create a new set of variables named as "pbX" and "paX" (price X days before and after hacks). For the variable

"p0" we chose the low price of the date the hack happens, which might indicate the more substantial impact compared to the close price of the day of the hack. For the other dates, close prices are used to represent the final price level after one day's fluctuation.

The scale of the hacks can be judged by two determinants: the amount measured in USD and the proportion of the market volume that the hack constituted. However, due to the different impact that a hack of a certain size can have depending on the overall size of the market, the proportion will illustrate the scale of the hack more precisely and consistently for our purposes.

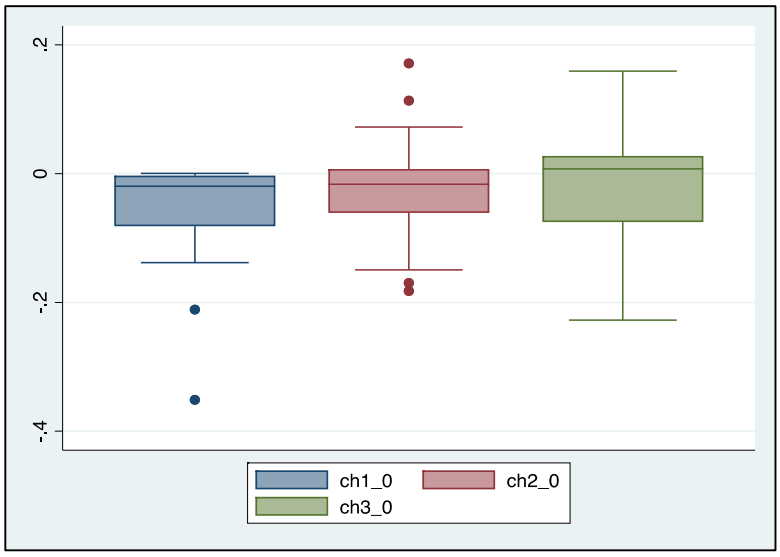
The 30 hacks cover the time from March 2nd, 2012 to December 27th, 2018. In order to obtain a more representative result, as mentioned before firstly we exclude the exit scam. These cases of financial fraud involve a long and vague timeline while the hacks are unexpectable incidents with traceable sources of information to locate the precise dates. The same approach has been taken to the two extortion cases[1]. Besides, for those hacks, the study excludes the Mt. Gox Hack as its vast amount makes it singularly unique (40 times larger than the second-largest Bitfinex Security Breach in August 2016).

4. Analysis and Case Study

We observe the price drop from the previous days. 26 of the 30 hacks had seen the price drop between the day before and the day of the hack. Additionally, the only abnormal values for ch1_0 and ch2_0 during which the price increased happened in December of 2017, when the value of Bitcoin skyrocketed to the historical price peak while the other three hacks had an increase that beneath 0.45 USD which is about 0.03% of the price. By using the box plot (attached below), we observe the price change from a number of days before the hack to the day the hack happens. For two days before, there are 17 hacks for which the change in price was negative, and the mean level of the change was -0.0252. From the box plot for 3 days before is visible that the first hypothesis for the negative impact of the hacks seems clear

Figure1: The box plot of price change

[1] Sailesh Bhatt alleged extortion (April 10th, 2018) and William Kopko Ransom extortion (October 15th,2018)



Further, we test if the size of the hack has an impact on the price fluctuation. Through our regression with "chX_0" (X=1,2,3,7,15,30) on the volume variable "adv", we find the sizes and price changes in 2 and 3 days have statistical significance (detailed results are available in the Appendix). Thus, if the proportion of the trading volume is larger, the drop in the value will be stronger in 2 and 3 days, which proves the hypothesis that not only the hacks impact the Bitcoin price negatively, but also that there exists a relationship between the size and price drop.

For the post hack period, the same regression with the price after the hack shows no statistical significance. However, the test between the actual amount of the lost value and the change in price after the hack has decent statistical significance (in regressions of the price change variables ch0_1 and ch0_2 on the stolen amount variable StolenAmountK). One possible explanation for the divergent behavior of Bitcoin price before and after the hack might be that the shock of the actual number of the stolen amount may be more effective than the trading volume in impacting the confidence for the recovery of Bitcoin price in the short term.

Although the linear regressions demonstrate the correlation between the scale of the hack and the price change pattern, the extraordinary case of 2014 Mt Gox hack deserves a closer examination of its background and the profound influence that it had on the market. Similarly, later in 2016, a large Bitfinex hack can be qualified as a representative to show the desired price pattern.

4.1 Mt.Gox Major Hack on February 7th, 2014

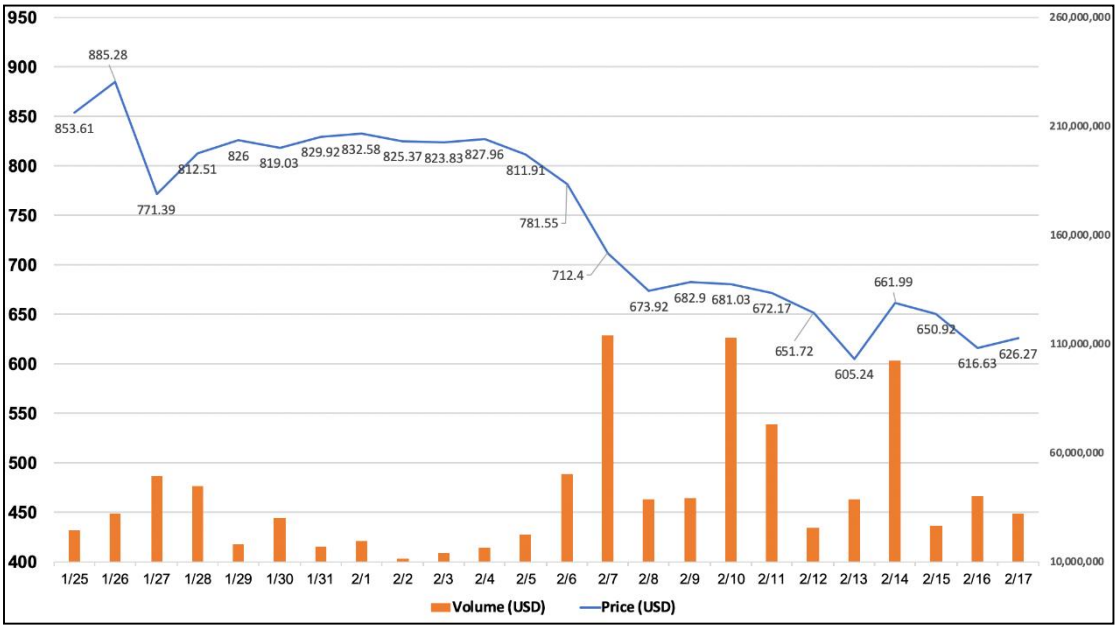
In our prior research, we regard the Mt. Gox as an extraordinary event due to its tremendous size ($300,000,000). As the historical price data graph displays, the price started to decline from

the open price of Bitcoin at $783.2 to the bottom of the day at $654.4. The drop of the day reached 16% of the value, which ranks as the second largest on the hack list.[2]

However, the background of the end of 2013 is worth our additional attention, because of another type of events which can significantly impact Bitcoin price, the government restrictions. Two months before the Mt. Gox case in the December of 2103, Chinese government banned financial institutions from using Bitcoins which already made the Bitcoin market suffer from a considerable decline (50% from the peak to the bottom) since December of 2013. Although Mt. Gox hack has an enormous size comparing to any other cryptocurrency hacks, the drop-recovery pattern can also be applied to this significant hack while the only difference is the longer time needed to recover. Only after 20 days did the price recover to 60% of the initial

value on the day when the hack happened, through a giant crash which nearly wiped off 90% of the bitcoin value. Research by Willy Report (2014) demonstrates that the trading bots of the exchange added to the problem as they magnified the trading volume before the Mt. Gox hack.

Figure2: Historical Price of Bitcoin during Mt. Gox Hack in 2014



Data source: Coinmarketcap.com

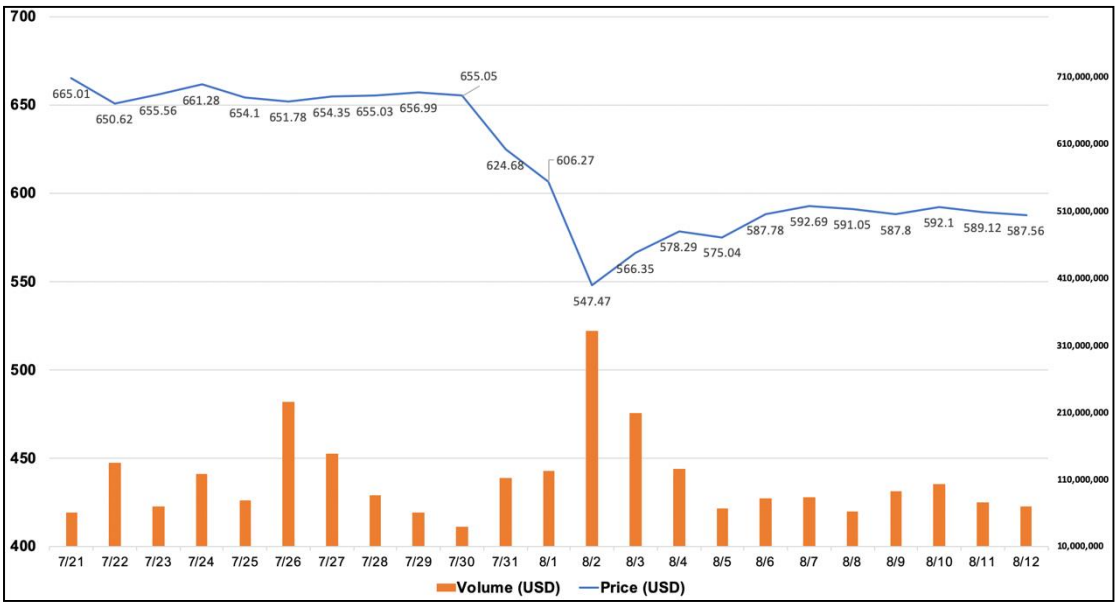
4.2 Bitfinex Security Breach on August 2nd,2016

[2] The largest one happened at October 24th, 2013, the Input.io Wallet Hack, when the price increased for more than three months to the day before the hack at $213.62 but dropped to the low price at $168.52.

The Bitfinex hack can also be qualified as a massive hack for nearly 120,000 bitcoins worth up to $72 million were stolen. Different from the Mt. Gox hack, however, during Bitfinex security breach the price change displayed a "standard" behavior without other material incidents. On the first day of the hack, the price temporarily declined by 10%. It has soon recovered, however, and returned to 93.4% of pb1 on the next day and 95.4% for the price of two days after hacking. The result also matches with our result that if a hack causes the price to decline, it leads to an insufficient recovery, in that the price does not return to the level observed before the hack. Furthermore, the second halving day of Bitcoin fell on July 9th, 2016, shortly before the hack. The halving two kinds of effects: for the Bitcoin miners, it implies the halving of the reward; for the market, the fall in the supply of Bitcoin can lead to an increase in price, at least temporarily. Thus, the price of Bitcoin was subjected to considerable fluctuation but a moderate increase after the halving.

Another difference between the Bitfinex hack and the Mt. Gox hack was that the exchange instantly reported the information of the loss and the counter-measures taken through Reddit and the status page. This could have relieved the panic of the market and made the recovery of the price closer to the average level.

Graph3: Historical Price of Bitcoin during Bitfinex Hack in 2016



Data source: Coinmarketcap.com

5. Conclusion

With increasing attention from the market and the high price fluctuations, cryptocurrency exchanges are targeted by the destructive hacks since 2012. Looking at the frequency and value of stolen cryptocurrencies, we analyze 30 Bitcoin hacks from 2012 to 2018. In the samples, 26 hacks out of 30 have seen a price drop from the first day before the hack.

Further, the study the impact of the size of the hack in two different ways, the proportion of the amount against the trading volume and the actual amount. Our study shows a positive correlation between the amount of cryptocurrencies stolen as a proportion of the trading volume and the price 2 and 3 days before the hack. At the same time the actual amount of stolen cryptocurrencies can affect the recovery of the bitcoin price in the first and second day after the hack happens.

Due to the lack of previous similar research, my paper does not explore the pattern and mechanism of the hacks. Although the research includes 30 Bitcoin hacks (the total number of the recorded hacks in the database is 54) from a time scale of six years, there are still 24 hacks excluded from our study for the ambiguity of the time or the meagre amount. Another concern for the research into the price patterns may be the multitude of the background events which happened around the same time as the hacks. Hacks are only one of the factors that disturb the price at a specified period. The essential negative or positive incidents will all contribute to the price fluctuation and may make the price change more complicated to analyze. Our research could be further improved by more endeavor to gather the data and to build a more nuanced linear regression to involve those additional factors for a better understanding of the Bitcoin price pattern in the short term, especially when the market faces unexpected incidents. Given their rising importance, we expect to see more research about the Bitcoin and other cryptocurrencies' price pattern in the near future.

6. Appendix

(1) The list of 30 Bitcoin hacks

Date	Name	Company / Victim	Amount Stolen ($K)	Amount Stolen (Crypto)
03/02/12	Linode Webhost Cloud Server Hack	Bitcoinica	228	46,703
05/06/12	Bitcoinica Hot Wallet Hack	Bitcoinica	90	18,548
09/04/12	Bitfloor Exchange Hack	Bitfloor	240	24,000
11/16/12	2012 Trojan Wallet Hack	Individual	40	3,457

01/11/13	Vircurex Exchange Hack	Vircurex	23	1,666
03/10/13	BTCGuild Mining Pool Hack	BTCGuild	58	1,254
07/15/13	Just Dice Incident	Just Dice	121	1,300
10/24/13	Input.io Wallet Hack	Tradefortress	820	4,100
11/19/13	BIPS Payment Services Hack	BIPS	1,000	1,295
11/30/13	Picostocks Cold Wallet Hack	Picostocks	6,000	5,875
03/04/14	Flexcoin Hot Wallet Hack	Flexcoin	600	896
03/11/14	CryptoRush Hack	CryptoRush	600	950
01/04/15	Bitstamp Hot Wallet Hack	Bitstamp	5,000	19,000
01/28/15	796 Exchange Hack	796 Bitcoin	230	1,000
02/15/15	BTER Cold Wallet Hack	BTER	1,750	7,170
02/19/15	Kipcoin Exchange Hack	Kipcoin	690	3,000
05/22/15	Bitfinex Hot Wallet Hack	Bitfinex	400	1,400
04/07/16	Shapeshift Exchange Hack	Shapeshift	200	469
05/13/16	Gatecoin Hack	Gatecoin	112	250
08/02/16	Bitfinex Security Breach	Bitfinex	72,000	120,000
10/14/16	Bitcurex Exchanges hack	Bitcurex	1,500	2,300
04/26/17	Yapizon Exchange Hack	Yapizon	7,600	3,831
06/29/17	Bitthumb Hack and PII Leak	Bitthumb	985	390
12/06/17	NiceHash Exchange hack	NiceHash	60,000	4,700
04/13/18	Coinsecure Exchange Hack	Coinsecure	3,300	438
09/20/18	Zaif Exchange Hack	Zaif	38,000	5,966
11/21/18	NicholasTruglia SIM Swapping Hack	Individual	1,000	230
11/26/18	Bulgaria Crypto Hack	Individual	5,000	1,370
12/27/18	Electroneum Wallet Hack	Electroneum	800	250

(2) The regression result A

The regression result from Stata of the price one day before the hack (and the price two days before the hack) on the trading volume (ch2_0 and adv, ch3_0 and adv).

```
. regress ch2_0 adv

      Source |       SS           df       MS      Number of obs   =        29
-------------+----------------------------------   F(1, 27)        =      5.23
       Model |  .027325997         1  .027325997   Prob > F        =    0.0303
    Residual |  .141186072        27  .005229114   R-squared       =    0.1622
-------------+----------------------------------   Adj R-squared   =    0.1311
       Total |  .168512069        28  .006018288   Root MSE        =    .07231

------------------------------------------------------------------------------
       ch2_0 |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
         adv |  -.0072221   .0031593    -2.29   0.030    -.0137044   -.0007398
       _cons |  -.0120137   .0146185    -0.82   0.418    -.0420085    .0179811
------------------------------------------------------------------------------

. regress ch3_0 adv

      Source |       SS           df       MS      Number of obs   =        29
-------------+----------------------------------   F(1, 27)        =      5.33
       Model |  .040615768         1  .040615768   Prob > F        =    0.0288
    Residual |  .205626088        27  .007615781   R-squared       =    0.1649
-------------+----------------------------------   Adj R-squared   =    0.1340
       Total |  .246241856        28  .008794352   Root MSE        =    .08727

------------------------------------------------------------------------------
       ch3_0 |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
         adv |  -.0088048   .0038127    -2.31   0.029    -.0166278   -.0009818
       _cons |   .0023004    .017642     0.13   0.897    -.0338979    .0384988
------------------------------------------------------------------------------
```

(3)The regression result B

The regression result from Stata of the price one day before the hack (and the price two days before the hack) on the actual amount of the lost value. (ch0_1 and StolenAmountK, ch0_2 and StolenAmountK).

```
. regress ch0_1 AmountStolenK

      Source |       SS           df       MS      Number of obs   =        29
-------------+----------------------------------   F(1, 27)        =      8.31
       Model |  .076187771         1  .076187771   Prob > F        =    0.0076
    Residual |  .247412529        27  .009163427   R-squared       =    0.2354
-------------+----------------------------------   Adj R-squared   =    0.2071
       Total |   .3236003        28  .011557154   Root MSE        =    .09573

------------------------------------------------------------------------------
       ch0_1 |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
AmountStolenK |   2.93e-06   1.01e-06     2.88   0.008     8.44e-07    5.01e-06
       _cons |   .0343823   .0192137     1.79   0.085    -.0050409    .0738055
------------------------------------------------------------------------------

. regress ch0_2 AmountStolenK

      Source |       SS           df       MS      Number of obs   =        29
-------------+----------------------------------   F(1, 27)        =      2.94
       Model |  .044563218         1  .044563218   Prob > F        =    0.0979
    Residual |  .409225765        27   .01515651   R-squared       =    0.0982
-------------+----------------------------------   Adj R-squared   =    0.0648
       Total |  .453788983        28  .016206749   Root MSE        =    .12311

------------------------------------------------------------------------------
       ch0_2 |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
AmountStolenK |   2.24e-06   1.31e-06     1.71   0.098    -4.40e-07    4.92e-06
       _cons |   .0522954   .0247105     2.12   0.044     .0015937    .1029971
------------------------------------------------------------------------------
```

References

[1] Carter, D. A., & Simkins, B. J. (2004). *The market ' s reaction to unexpected , catastrophic events : the case of airline stock returns and the September 11th attacks*. *44*, 539–558.

[2] Datta, S., & Dhillon, U. S. (n.d.). *Bond and Stock Market Response to Unexpected Earnings Announcements*. *28*(4).

[3] Feder, A., Gandal, N., Hamrick, J. T., & Moore, T. (2017). *The impact of DDoS and other security shocks on Bitcoin currency exchanges : evidence from Mt . Gox*. *3*(2), 137–144.

[4] Feng, W., Wang, Y., & Zhang, Z. (2018). Informed trading in the Bitcoin market. *Finance Research Letters*, *26*(November 2017), 63–70.

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Available at https://Bitcoinorg/Bitcoin.pdf.*

[6] Salas, J. M. (2010). Entrenchment , governance , and the stock price reaction to sudden executive deaths. *Journal of Banking and Finance*, *34*(3), 656–666.

[7] Urquhart, A. (2017). *Price clustering in Bitcoin*. *159*, 145–147.