Impact of Successful DDoS Attacks on a Major Crypto-currency Exchange

Abhishta Abhishta
University of Twente
s.abhishta@utwente.nl

Reinoud Joosten
University of Twente
r.a.m.g.joosten@utwente.nl

Sergey Dragomiretskiy
University of Twente
sdragomiretsky@gmail.com

Lambert J.M. Nieuwenhuis
University of Twente
l.j.m.nieuwenhuis@utwente.nl

***Abstract*—Distributed Denial of Service (DDoS) attacks provide an easy option for these criminals to disrupt the business of these online platforms. We analyse the economic impact of DDoS attacks on a crypto-currency exchange using event analysis. Our contributions are fourfold: Firstly, we develop an estimation model utilising ideas from behavioural finance to predict volume of crypto-currency traded on the basis of changes in price. Secondly, we perform an event analysis to evaluate whether there is an impact of a DDoS attack on the volume traded on the exchange in 17 different cases. Thirdly, we find that in 13 cases the negative impact due to a DDoS attack is recovered within the same day by the exchange. Finally, we evaluate hourly trade data to show why in most cases the volume traded recovers within a single day.**

***Index Terms*—Bitfinex, Crypto-currency, Abnormal Trades, Economic Impact, Event Study, Cyber Security, DDoS Attacks.**

I. Introduction

The market capitalisation of global crypto-currency markets has increased from $19 billion in the beginning of 2017 to $602 billion by the end of 2017 [1]. Crypto-currencies are digital currencies based on blockchain technology. To fulfil the need of investors who wish to benefit from the sudden increase in valuation of these digital currencies, crypto-currency exchanges have come up. These exchanges allow their clients to buy, store and sell crypto-currencies by using online platforms. The clients of these exchanges are able to trade and profit due to the fluctuations in the price of crypto-currencies. The exchange charges them for each transaction made on its platform.

These platforms face security issues just like other online businesses. One of the biggest challenges faced by them is a distributed denial of service (DDoS) attack. A victim of a DDoS attack is overwhelmed by bogus requests that are directed by the attacker towards it's network infrastructure. Hence, the attack leaves the website unreachable to the desired users. We analyse the impact of DDoS attacks on the volume of Bitcoin traded one such crypto-currency exchange: Bitfinex. We apply the so-called event analysis methodology to analyse this impact.

Our contributions are as follows:

1) We develop an estimation model utilising ideas from behavioural finance to predict volume of crypto-currency traded on the basis of change in price.
2) We perform an event analysis to evaluate whether there is an impact of a DDoS attack on the volume traded on the exchange in 17 different cases.
3) We find that, on most occasions (13 of 17) the negative impact due to a DDoS attack is recovered within the same day by the exchange.
4) We evaluate hourly trade data to discuss why in most cases the volume traded recovers within a single day.

II. Impact of DDoS on the revenue stream of an exchange

At a crypto-currency exchange, a client can buy, sell and store supported digital currencies at the exchange rate. The exchange matches buyers & sellers and charges a fee for every trade made, to both parties.

A DDoS attack degrades the performance of a crypto-currency exchange. In the worst case scenario, it can cause temporary unavailability of the online platform. This would mean that when the exchange is under an attack the volume of digital currency traded would decrease. As crypto-currencies can be bought from any of the hundreds of exchanges [2] that are on the web, temporary unavailability of just one of the exchanges would not have a significant impact on the price of the crypto-currency but will have an effect on the revenues of the attacked platform. In this paper, we analyse the impact of DDoS attacks on the volume of bitcoin traded on *Bitfinex*.

Attacks on Bitfinex: Bitfinex is a Hong Kong-based crypto-currency exchange. It was founded in December 2012 as a peer-to-peer Bitcoin exchange offering trading services all around the world. The business model of this exchange is making money from providing the matching of buyers and sellers. Bitfinex charges a fee for each trade made on the exchange.

The exchange has been a victim of DDoS attack on several occasions. In order to find the dates of attacks we make use of three different sources: 1) Bitfinex twitter feed (*@Bitfinex*), 2) Bitfinex status page [3] and 3) Google news search. To scrape all the tweets from the *@Bitfinex* twitter feed we make use of an open source python project known as Twint[1] [4]. We also look for mentions of DDoS attacks on Bitfinex since 2016 on Google news search and Bitfinex status page [3]. From all the sources described above we record the dates of DDoS attacks on Bitfinex. Table I shows the list of 17 attacks that we analyse in this paper.

[1]It is an advanced Twitter scraping & OSINT tool written in Python that doesn't use Twitter's API, and allows to scrape a user's followers, following, Tweets and more while evading most API limitations.

TABLE I: Table showing the list of reported attacks on Bitfinex and the damage caused.

No.	Date	Target	Damage	Source
1	20/01/2016	Bitfinex	Temporary Unavailability	Status Page
2	04/06/2016	Bitfinex/BitGo	Temporary Unavailability	Twitter and Status Page
3	07/06/2016	Bitfinex	Degraded Performance	Status Page
4	20/06/2016	Bitfinex	Temporary Unavailability	Status Page
5	26/07/2016	Bitfinex	Temporary Unavailability	Status Page
6	09/11/2016	Bitfinex	Temporary Unavailability	Status Page
7	16/11/2016	Bitfinex	Temporary Unavailability	Status Page
8	21/02/2017	Bitfinex	Degraded Performance	News,Twitter and Status Page
9	12/06/2017	Bitfinex	Degraded Performance	News, Twitter and Status Page
10	21/08/2017	Bitfinex	Degraded Performance	News and Status Page
11	26/11/2017	Bitfinex	Temporary Unavailability	Twitter and News
12	04/12/2017	Bitfinex	Degraded Performance	News, Twitter and Status Page
13	05/12/2017	Bitfinex	Degraded Performance	News, Twitter and Status Page
14	12/12/2017	Bitfinex	Temporary Unavailability	News, Twitter and Status Page
15	17/12/2017	Bitfinex	Degraded Performance	News, Twitter and Status Page
16	31/12/2017	Bitfinex	Temporary Unavailability	News, Twitter and Status Page
17	05/06/2018	Bitfinex	Temporary Unavailability	News, Twitter and Status Page

Impact on Bitfinex: A DDoS attack makes it difficult for the clients of Bitfinex to reach its online platform. This in turn affects the number of trades made on the exchange. Thus, the economic loss to the exchange will be due to the prospective trading fee that the exchange could have earned during the unavailability. Later we use the causal relationship between a DDoS attack on the exchange and its impact on the commission earned by the exchange to formulate our hypothesis.

III. Methodology

In this section we explain our method to evaluate the impact of DDoS attacks on a crypto-currency exchange. First we elaborate on the datasets used for conducting this study. Next, we explain the event study methodology [5] used to measure the impact of the attack. Finally, we develop our null hypothesis and discuss the method of hypothesis testing.

Dataset: We use two datasets collected with the help of *www.cryptodatadownload.com*. Both datasets provide information on the bitcoin volume traded on Bitfinex, the difference is the granularity: one provides the daily amount of volume traded on the exchange with the highest and the lowest price of the day, and the other dataset provides the same information at an hourly interval. Both longitudinal datasets start on 01-12-2015 and end on 16-06-2018. We pre-processed the datasets to remove any anomalies. For instance, the security of Bitfinex was breached and $72 million of Bitcoin was stolen on 2nd August 2016 [3, 6]. All trading was halted for 7 days and normal operations were resumed on the 10th of August 2016. Hence, we observe no trades on the exchange during this period.

With relation to the models described in the following sections we get the values for the following variables are provided by the dataset: $VolumeFrom$, $VolumeTo$, P_{High} and P_{Low}. Equation 1 describes the relationship between these variables and the values of variables $ActV_t$ and ΔP_t.

Event Study Analysis: To evaluate the impact of certain events on companies' stock prices a method called event analysis has been designed in finance and economics. Mackinlay [5] has discussed the method for conducting a classical event study. Abhishta *et al.* [7] have proposed a more robust event study method especially useful in cases when the *returns* and *abnormal returns* are not normally distributed. They have shown that the classical method of event study in the case of non-normal *abnormal returns* leads to overestimation/underestimation of losses/gains [8].

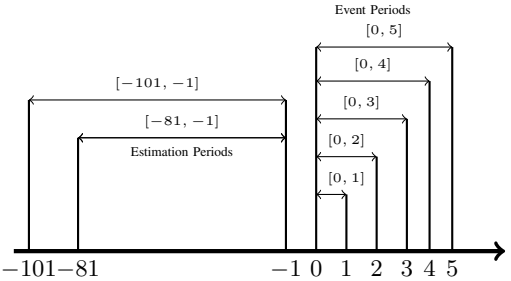


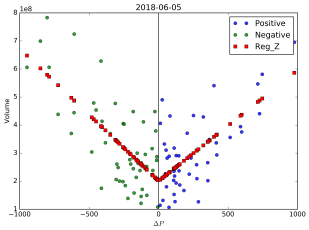
Fig. 1: Estimation and Event Periods.

To analyse the impact of DDoS attacks on the volume of Bitcoin traded on Bitfinex, we follow these steps:

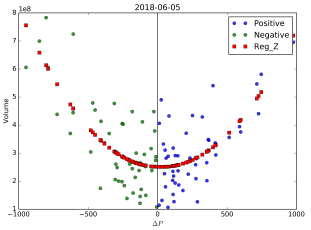
Step 1: Define estimation and event periods.
Step 2: Using the data in the estimation period, compute a model to predict volume of crypto-currency traded on Bitfinex.
Step 3: Define a null hypothesis.
Step 4: Calculate values of *abnormal volume* and *cumulative abnormal volume* in the estimation period.
Step 5: Generate an empirical distribution by bootstrapping [9].
Step 6: Use the empirical distribution for hypothesis testing.

For analysing each attack event we divide our dataset in two parts as shown in Figure 1. The common practice for stock market event studies is to use 120 days for the estimation period [5]. But, as the crypto-currency market is more volatile than the stock market we consider two slightly shorter estimation periods of 100 days and 80 days. The data in the estimation period are used to calculate the parameters of the estimation model. For further analysis we chose the estimation period that yields the highest value for the coefficient of determination (adj. R^2).

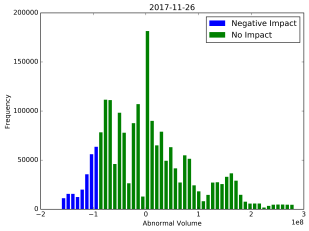
We use an additive model to predict the usual quantity of Bitcoin traded on the exchange. To determine the best estimation model we test the goodness of fit for the following two models, one is a linear and the other is a quadratic model. If $|\Delta P_t|$ represents the absolute value of price change and V_t represents the volume of Bitcoin traded on day t then the linear and quadratic estimation models explaining the relationship of volume and absolute price change can be given by Equations 2 and 3 respectively. The variables $|\Delta P_t|$ and V_t can be calculated as shown in Equation 1 where P_t is the price of Bitcoin on day t and is calculated as the average of highest (P_{High}) and lowest (P_{Low}) price of the day. The parameters α_i, β_i and γ_i can be estimated using ordinary least square (OLS) on the basis of the data in the estimation period for an event i. OLS is chosen based on the study by Karafiath *et al.* [10]. This study compared several generalized least squares and first & second order autoregressive structures and it concluded that these do not offer a material improvement over OLS in the context of event studies.



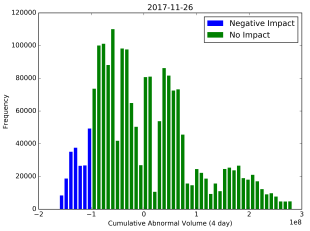
(a) Linear OLS model for the attack on 05-06-2018



(b) Quadratic OLS model for the attack on 05-06-2018



(c) Empirical Distribution for Abnormal Volume



(d) Empirical Distribution for 4 Day Cumulative Abnormal Volume

Fig. 2: OLS models showing the dissimilar effect of negative and positive price changes and Empirical distributions

$$P_t = \frac{P_{High} + P_{Low}}{2}$$
$$|\Delta P_t| = P_t - P_{t-1} \tag{1}$$

$$V_t = \beta_i |\Delta P_t| + \gamma_i \tag{2}$$

$$V_t = \alpha_i |\Delta P_t|^2 + \beta_i |\Delta P_t| + \gamma_i \tag{3}$$

In behavioural finance negative and positive price changes have been shown to have dissimilar effects on the volume traded [11]. This effect can also be observed in the case of crypto-currencies. In Figure 2 we show the OLS models for the attack on *05-06-2018* computed with the help of Equations 2 and 3. The plots show *Reg_Z* as the curve representing the OLS model for positive and negative price changes. In Figure 2a, we can clearly observe that in the case of linear model the slope for the resulting curve is different for positive and negative price changes. A similar effect is seen in case of the quadratic model as shown in Figure 2b.

$$z_t{}^{+ve} = \max\{0, \Delta P_t\}$$
$$z_t{}^{-ve} = \min\{0, \Delta P_t\} \tag{4}$$

$$V_t = \beta_i{}^{+ve} z_t{}^{+ve} + \beta_i{}^{-ve} z_t{}^{-ve} + \gamma_i \tag{5}$$

$$V_t = \alpha_i{}^{+ve}(z_t{}^{+ve})^2 + \beta_i{}^{+ve} z_t{}^{+ve} + \alpha_i{}^{-ve}(z_t{}^{-ve})^2 + \beta_i{}^{-ve} z_t{}^{-ve} + \gamma_i \tag{6}$$

Here, we use functions as shown in Equations 5 and 6 to accommodate for the dissimilar effect of positive and negative price changes on the volume traded. Where, $z_t{}^{+ve}$ and $z_t{}^{-ve}$ represent a set of positive and negative price changes respectively and are defined as shown in Equation 4. We estimate the coefficients $\alpha_i{}^{+ve}$, $\alpha_i{}^{-ve}$, $\beta_i{}^{+ve}$, $\beta_i{}^{-ve}$ and γ_i for event i for Equations 5 and 6 using OLS.

TABLE II: Table showing the adj. R^2 values for three tested models

Attack Date	LM (100 days)	QM (100 days)	QM (80 days)
20/01/2016	0.71	0.78	0.79
04/06/2016	0.78	0.79	0.85
07/06/2016	0.75	0.76	0.80
20/06/2016	0.83	0.85	0.85
26/07/2016	0.80	0.81	0.80
09/11/2016	0.77	0.78	0.84
16/11/2016	0.71	0.78	0.82
21/02/2017	0.69	0.71	0.80
12/06/2017	0.66	0.72	0.65
21/08/2017	0.49	0.51	0.54
26/11/2017	0.36	0.42	0.40
04/12/2017	0.29	0.39	0.31
05/12/2017	0.29	0.38	0.22
12/12/2017	0.66	0.70	0.69
17/12/2017	0.64	0.65	0.65
31/12/2017	0.74	0.71	0.64
05/06/2018	0.48	0.54	0.53

LM: Linear Model and QM: Quadratic Model

In Table II we show the values of coefficient of determination (adj. R^2) for three of the tested models. In most cases we observe that a quadratic model performs significantly better (higher values of adj. R^2) than a linear model. Also, while comparing on the basis of the estimation periods, we find that a shorter estimation period of 80 days improves the adj. R^2. Hence, we select a quadratic model with an estimation period of 80 days.

The next step in an event study analysis is to compute the deviation of the volume in the estimation period from the modelled volume. This deviation is referred to as *Abnormal Volume* and can be computed with the help of Equation 8. In this equation, AV_t is the abnormal volume on day t and $ActV_t$ is the actual volume of Bitcoins traded on the exchange on day t. Variable $ActV_t$ can be calculated as shown in Equation 7, where $VolumeFrom_t$ and $VolumeTo_t$ are the starting and the ending trading volume readings for the day t and their values can be found in the dataset.

$$ActV_t = VolumeTo_t - VolumeFrom_t \tag{7}$$

$$AV_t = ActV_t - (\alpha_i{}^{+ve}(z_t{}^{+ve})^2 + \beta_i{}^{+ve} z_t{}^{+ve} + \alpha_i{}^{-ve}(z_t{}^{-ve})^2 + \beta_i{}^{-ve} z_t{}^{-ve} + \gamma_i) \tag{8}$$

$$CAV_i^p = \sum_{t=n}^{n+p} AV_t \tag{9}$$

To account for more long term (more than a day) impacts of DDoS attacks we calculate a p day *Cumulative Abnormal Volume*, which can be calculated using Equation 9. The variable CAV_i^p represents the cumulative abnormal volume for p days after the attack event i and AV_t represents the

abnormal volume on day t. As shown in Figure 1 we calculate the *Cumulative Abnormal Volumes* for the following five *event periods*:

1) Day of the attack to 1 day after it $[n, n+1]$.
2) Day of the attack to 2 days after it $[n, n+2]$.
3) Day of the attack to 3 days after it $[n, n+3]$.
4) Day of the attack to 3 days after it $[n, n+4]$.
5) Day of the attack to 5 days after it $[n, n+5]$.

Finally, we formulate the null hypothesis and test it in order to evaluate the impact of DDoS attack in the *event period*.

Hypothesis: As discussed previously in Section II, we expect that a DDoS attack on crypto-currency exchange would result in decreased volume of Bitcoin. Hence, our study investigates whether the daily volume of Bitcoin traded on Bitfinex on the day of the attack is significantly lower than the volume of Bitcoin traded during the *estimation* period. Thus, the null hypothesis in this case can be stated as:

H_0: There is no difference in the average volume of Bitcoin traded on Bitfinex during the estimation period and event period.

A wide spread assumption is that the abnormal returns in case of a stock market event study are distributed according to a Gaussian distribution. This assumption was challenged in the paper by Abhishta *et al.* [7]. In this paper we distance ourself from the assumption that cumulative abnormal volumes are normally distributed as well. The unknown distribution can be approximated by an empirical distribution which can be generated by bootstrapping [9]. We use a one-tailed hypothesis test to evaluate our null hypothesis (H_0). Hence, we state the alternative hypothesis (H_1) as:

H_1: The average volume of Bitcoin traded on Bitfinex during the event period is less than the average volume traded in the estimation period.

Bootstrapping and Hypothesis Testing: We make use of Monte Carlo simulation for bootstrapping the empirical distribution of *abnormal volume* and *cumulative abnormal volume*. From the set of *abnormal volume* and *cumulative abnormal volume* values that belong to the *trend period* we draw a random value two million times. To also consider the values in the vicinity of the drawn value, we introduce an error to the drawn value as shown in Equation 10 where x_b represents the value used in the bootstrapped distribution, x_r is the random value drawn and τ is a random number in the interval $[-0.1, 0.1]$.

$$x_b = x_r + \tau x_r \text{ where } \tau \in [-0.1, 0.1] \tag{10}$$

Figures 2c and 2d shows the bootstrapped distributions used to analyse the attacks on *20-01-2016* and *04-06-2016*. For testing the statistical significance of the impact we consider that if the *abnormal volume* or the *cumulative abnormal volume* in the event periods lie in the blue portion of these distributions then the negative impact of the DDoS attack was statistically significant.

For calculating the boundaries for a significantly negative impact, we assume a confidence interval of 90%. Hence as shown in Figure 2c we consider the bottom 10 percentile of the values to be statistically significant. Hence, in terms of hypothesis testing, if the value of *abnormal volume* or *cumulative abnormal volume* lies in the bottom 10 percentile of the bootstrapped empirical distribution, then we can reject the null hypothesis.

IV. Results

We summarise the results of our analysis in two tables: Table III and Table IV. In Table III we show the values of regression parameters ${\alpha_i}^{+ve}$, ${\alpha_i}^{-ve}$, ${\beta_i}^{+ve}$, ${\beta_i}^{-ve}$ and γ_i. The coefficient of determination (adj. R^2) for the model used to estimate the traded volume is shown in Table II. We observe that the adj. R^2 values for estimation models in 2016 and end of 2017 are relatively high in comparison to the other values. This is due to sudden increase in Bitcoin prices in mid 2017. Looking at the adj. R^2 values in most cases we can say that more than 50% of the traded volume can be predicted on the basis of change in price of Bitcoin. In all 17 cases a low *p-value* also indicates a strong relationship between the dependent variable V_t (volume of bitcoin traded on day t) and independent variables ${z_t}^{+ve}$ and ${z_t}^{-ve}$ (positive and negative price change respectively).

We test for negative impact on the *Abnormal Volume* of Bitcoin traded on Bitfinex for five days after the DDoS attack (including the day of attack). We do this to check whether the impact seen in the *cumulative abnormal volume* is due to the DDoS attack or not[2]. The results are shown in Table III. We observe that in case of 4 of the 17 considered events there is a significant negative abnormal volume on the day of the attack. This means that for these 4 instances the exchange was not able to recover within a day. One of the main reasons why we do not see negative abnormal returns in all cases can be due to the fact that the attack was successful for a small duration and the trading activity just after the platform recovered compensated for the volume lost due to the short unavailability. We further observe Table IV that in case of two out of these four negative abnormal volume events, the exchange recovers within two days as the 3 day cumulative abnormal return value indicate no impact. In the other two cases we observe that the exchange does not recover within 5 days. We investigate these points in greater detail in next.

V. Discussion

We observe in Section IV that in majority of the cases (13 of 17) the loss of volume caused due to a successful DDoS attack is recovered by the exchange within a period of 1 day. For this reason we do not record a significant negative abnormal volume on the day of the attack. Figure 3 shows the hourly volume traded on the exchange. In Figures 3a and 3b we can observe periods when no or very little volume was

[2]For instance, if there is a negative impact on the day of attack but no impact one day after the attack then it means that the negative impact was recovered within one day of trading if there is no impact according to 2 day *cumulative abnormal volume* value.

TABLE III: Results: Model Parameters and Abnormal Volume

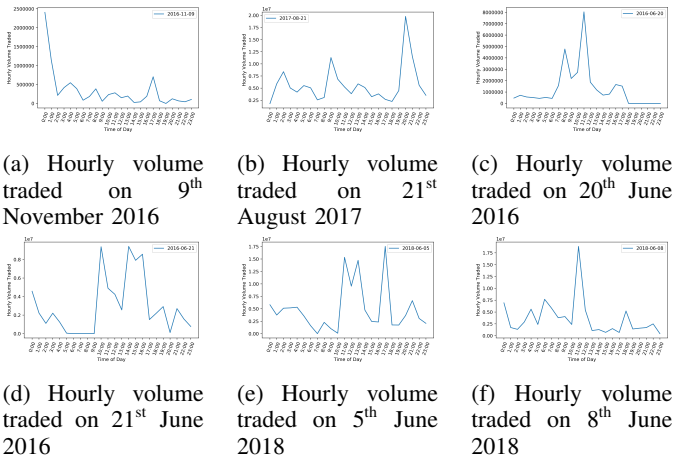
	Model Parameters					Negative Impact (Abnormal Volume)				
Attack Date	$\alpha_i{}^{+ve}$	$\alpha_i{}^{-ve}$	$\beta_i{}^{+ve}$	$\beta_i{}^{-ve}$	γ_i	1st Day	2 nd Day	3rd Day	4th Day	5th Day
20/01/2016*	34529.7	-4335.9	-214450.8	880044.9	6866249.1	No	No	No	No	**Yes**
04/06/2016*	-6687.0	7872.0	1012188.0	617831.9	2070323.8	No	No	No	No	No
07/06/2016*	-6479.9	10558.9	996953.8	549459.8	2356437.1	No	No	No	**Yes**	No
20/06/2016*	3830.4	74513.7	609420.0	-80812.8	4285488.8	**Yes**	**Yes**	No	No	No
26/07/2016*	5504.5	7183.9	475625.8	543508.0	7712740.4	**Yes**	No	No	No	**Yes**
09/11/2016*	10570.1	2673.0	84391.4	171729.4	2057886.1	No	No	No	No	No
16/11/2016*	8132.7	2681.8	145909.6	169299.8	2169077.2	No	No	No	No	No
21/02/2017*	4045.8	1641.5	121104.3	167707.4	5413822.6	No	No	No	No	No
12/06/2017*	650.1	-992.0	167009.3	472802.0	18690303.7	No	No	No	No	**Yes**
21/08/2017*	178.3	-479.7	250230.1	389380.3	40050513.6	No	No	No	No	No
26/11/2017*	-645.6	550.7	494887.0	174677.4	147126862.2	**Yes**	No	No	No	No
04/12/2017*	-212.5	895.5	217365.6	-76938.6	177704654.5	No	No	No	No	**Yes**
05/12/2017*	-195.2	1036.2	199544.5	-129388.6	179678622.2	No	No	No	**Yes**	No
12/12/2017*	74.7	406.4	109273.0	116946.1	188656983.1	No	No	No	No	No
17/12/2017*	17.5	337.0	285588.6	353096.1	180600154.9	No	No	No	No	No
31/12/2017*	15.1	47.1	286913.5	708868.2	214840630.2	No	No	No	No	No
05/06/2018*	486.0	658.3	31657.9	-56779.9	231740322.9	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

*p value$<$ 0.05

TABLE IV: Results: Cumulative Abnormal Volume

Attack Date	2 Day CAV[1]	3 Day CAV[1]	4 Day CAV[1]	5 Day CAV[1]
20/01/2016	No	No	**Yes**	**Yes**
04/06/2016	No	No	No	No
07/06/2016	No	No	No	No
20/06/2016	**Yes**	**Yes**	**Yes**	**Yes**
26/07/2016	**Yes**	No	No	**Yes**
09/11/2016	No	No	No	No
16/11/2016	No	No	No	No
21/02/2017	No	No	No	No
12/06/2017	No	No	No	No
21/08/2017	No	No	No	No
26/11/2017	**Yes**	No	No	No
04/12/2017	No	No	No	No
05/12/2017	No	No	No	No
12/12/2017	No	No	No	No
17/12/2017	No	No	No	No
31/12/2017	No	No	No	No
05/06/2018	**Yes**	**Yes**	**Yes**	**Yes**

[1]CAV: Cumulative Abnormal Volume



(a) Hourly volume traded on 9th November 2016

(b) Hourly volume traded on 21st August 2017

(c) Hourly volume traded on 20th June 2016

(d) Hourly volume traded on 21st June 2016

(e) Hourly volume traded on 5th June 2018

(f) Hourly volume traded on 8th June 2018

Fig. 3: Hourly volume of Bitcoin traded on Bitfinex.

being traded on the exchange. Some of these periods can be attributed to the platform issues caused due to a DDoS attack. On 9th November 2016, we observe that very little volume was traded on the exchange after the first hour of trading. However, on the basis of the total volume traded in the whole day we were unable to reject the null hypothesis. Similarly, on 21st August 2017, we observe a dip in volume traded after 13:00 hours (time of reported platform issues). The large volume of bitcoin traded in the end of the day however compensates for the loss. This quick recovery for Bitfinex can be partially attributed to the public relations (PR) strategy employed by the exchange. Bitfinex maintains and updates the status of platform availability on twitter and its own status page regularly. Hence, when the exchange resumes normal operations, all the customers are informed that they can resume trading. This can be one of the incentives for such businesses to publicly disclose DDoS attacks.

On two occasions (20th June 2016 and 5th June 2018) we observe that the negative impact lasts for more than 5 days. This is due to the fact that we have multiple days in the *event period* where the *abnormal volume* is significantly negative. In Figures 3c and 3d we can see that the exchange recovers on 21st June 2016 but the trading stops again after a few hours. This may be due to a second wave of unreported DDoS attacks or unresolved platform issues due to the first attack.

VI. Related Work

Feder *et al.* [12] also studied the impact of DDoS on crypto-currency exchanges, in particular, the Mt. Gox exchange. Mt. Gox was often targeted DDoS attacks and was forced to close due to a serious breach that resulted in stolen funds. They measured the kurtosis and distribution of the distribution of trades that were made on the exchange when the exchange was under attack. The conclusion of the article showed a decrease in large volume trades due to a DDoS attack. They also suggested that other type of security breaches also had a similar kind of impact.

In another work, Johnson *et al.* [13] present a game-theoretic model for the trade-off faced by mining pools between investing in upgrades for computing infrastructure and engaging in DDoS attacks. They conclude that if attacks

can be mitigated, then the size threshold for a mining pool to be safe from DDoS increases.

Similar event study methodology has also been applied to investigate the impact of DDoS attacks on stock prices and a comparison of alternatives to measure the impact of DDoS attack announcements on stock prices by Abhishta *et al.* [8]. This study looked at the impact of DDoS attacks on victim stock prices and concluded that most of the time the impact was not significant. This conclusion was also reached by Hovav *et al.* [14]. Only when the actual service of the company was down, it resulted in a statistically significant impact.

VII. Conclusion

In this paper, we present our analysis of the impact of DDoS attacks that targeted Bitfinex in the last three years. Using the data collected with the help of *www.cryptodatadownload.com* we test if there is a statistically significant negative impact on the daily volume of bitcoins that are traded on the exchange. For performing this analysis we present an event study methodology that uses the relationship between volume of bitcoin traded and change in it's price on the exchange to predict expected volume of bitcoin traded during the *event period*.

We determine the length of the *estimation period* and the degree of regression model by comparing the adj. R^2 values for multiple options. We apply our methodology to 17 different events and draw the following conclusions:

- We show that, for the investors there is a difference in the perception of positive and negative price changes. Hence, we model the impact of positive and negative price changes on the volume separately.
- We find that, on most occasions (13 of 17) the negative impact due to a DDoS attack is recovered within the same day by the exchange.
- On two instances, we find that the losses are recovered after two days of the attack.
- On two other occasions we find that the losses are not recovered within 5 days. We suppose that this is due to multiple platform un-availabilities in the *event period*.

Summarising, our study shows that in most cases this crypto-currency exchange has been able to recover from the impact of a DDoS attack within a single day. However, in the hourly data we do see the trading coming to a complete halt due to a DDoS attack. This proves that a long lasting DDoS attack can severely effect the revenues of the exchange.

Acknowledgement

This work is part of the NWO: D3 project, which is funded by the Netherlands Organization for Scientific Research (628.001.018).

References

[1] CoinMarketCap. *Cryptocurrency market capitalizations*. URL: https : / / coinmarketcap . com / currencies/bitcoin/.

[2] Kai Sedgwick. *The Number of Cryptocurrency Exchanges Has Exploded*. URL: https://news.bitcoin.com/the-number-of-cryptocurrency-exchanges-has-exploded/ (visited on 09/03/2018).

[3] *Bitfinex Status Page*. URL: https://bitfinex.statuspage.io (visited on 08/20/2018).

[4] Francesco Poldi. *TWINT - Twitter Intelligence Tool*. URL: https://github.com/twintproject/twint (visited on 08/20/2018).

[5] A. Craig MacKinlay. "Event Studies in Economics and Finance". In: *Journal of Economic Literature* 35.1 (1997), pp. 13–39.

[6] Clare Baldwin. *Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong*. URL: https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP (visited on 08/20/2018).

[7] Abhishta, Reinoud Joosten, and Lambert J. M. Nieuwenhuis. "Analysing the Impact of a DDoS Attack Announcement on Victim Stock Prices". In: *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE Press, Mar. 2017.

[8] Abhishta, Reinoud Joosten, and Lambert J.M. Nieuwenhuis. "Comparing Alternatives to Measure the Impact of DDoS Attack Announcements on Target Stock Prices". In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)* 8.4 (Dec. 2017), pp. 1–18.

[9] Bradley Efron. "Bootstrap methods: another look at the jackknife". In: *Breakthroughs in statistics*. Springer, 1992, pp. 569–593.

[10] Imre Karafiath. "Detecting cumulative abnormal volume: a comparison of event study methods". In: *Applied Economics Letters* 16.8 (2009), pp. 797–802.

[11] Jonathan M. Karpoff. "The Relation between Price Changes and Trading Volume: A Survey". In: *Journal of Financial and Quantitative Analysis* 22.1 (1987), pp. 109–126. DOI: 10.2307/2330874.

[12] Amir Feder, Neil Gandal, J T Hamrick, and Tyler Moore. "The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox". In: *Journal of Cybersecurity* 3.2 (2017), pp. 137–144.

[13] Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. "Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools". In: *Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 72–86.

[14] Anat Hovav, JinYoung Han, and Joonghyuk Kim. "Market Reaction to Security Breach Announcements: Evidence from South Korea". In: *SIGMIS Database* 48.1 (Feb. 2017), pp. 11–52.