The influence of DDoS attacks on cryptocurrency exchanges

Sergey Dragomiretskiy
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
s.n.dragomiretskiy@student.utwente.nl

ABSTRACT

Cryptocurrency exchanges are becoming increasingly more targeted by attacks executed by cybercriminals because of the exploding growth of the crypto markets. Distributed Denial of Service (DDoS) attacks are chosen more often because of the easiness, cheapness, and anonymity of the attack. This paper provides an investigation into the influence of DDoS attacks on cryptocurrency exchanges. In particular, it investigates the influence of the denial of service on trading activity over a period of 3 years on currently one of the biggest cryptocurrency exchanges: Bitfinex. This study examines how and why DDoS attacks influence companies, the size of the impact of a DDoS attack on Bitfinex, and the significance of this influence. First, it uses a literature review to answer questions about DDoS in general and then it makes use of statistical methods to analyze the impact of 18 DDoS attacks done on the Bitfinex exchange. It uses an event study and proposes a prediction model for the estimation of the number of trades in a novel and extremely volatile market. The results of this study conclude that the impact of the attacks was not significantly negative. This means that trading on the exchange did not significantly decrease in the days after a DDoS attack.

Keywords

DDoS attacks, Cryptocurrency, Bitcoin, Exchanges, Cyber Security, Event Study

1. INTRODUCTION

The market capitalization of the global cryptocurrency markets increased from $19 billion to $602 billion in the year 2017 according to coinmarketcap.com [20]. This is an increase of $583 billion or 3068%. The hype of this technology attracted amateur investors that lack best practices of investing and preserving money. These markets are relatively novel and do not have the regulations and protections the stock market offers.

The billions of invested money, the many new investors, and a market that has minimal regulations make it a perfect target for abuse. Thus, it attracted many criminals that are looking for financial gain. The blockchain technology makes the job of criminals more reliable. This reliability comes from the indisputability of transactions and the relative anonymity. Once a crypto transaction is sent from one address to another, there is no way of getting it back. This is because there is no central authority in the cryptocurrency space. An example of this is the hack on the Mt. Gox cryptocurrency exchange. This exchange went bankrupt because of a large-scale breach resulting in all its funds being stolen [29]. Because of the increase in cybercrime and the relatively new research field, this study will focus on the influence of such cybercrime.

The increase of cybercrime in the crypto markets provided the criminals with stronger tools. One of the most used tools is the DDoS attack. The increasing amount of these attacks, especially on cryptocurrency exchanges, can be attributed to the availability of cybercrime-as-a-service tools: Booters. These are online websites where DDoS attacks can be ordered. Thus, technical knowledge of executing such an attack is not required and the costs are minimal [39].

Although extensive research is done on DDoS attacks as well as on the blockchain technology, there is relatively little research on the combination of these two topics. The papers that did combine the topics were done in a time where cryptocurrencies were not popular yet and the studies also made questionable assumptions [41, 29]. This paper will challenge those assumptions by not assuming the abnormal trades to be normally distributed out of ease. Instead, it will make use of the Empirical Distribution to estimate abnormal trades according to Abhishta et al.[25]. This study will also analyze the most recent DDoS attacks using an event study analysis [33].

29^{th} *Twente Student Conference on IT* July 6^{th}, 2018, Enschede, The Netherlands.

2. METHODOLOGY

2.1 Research question

The goal of this paper is to answer the main research question: *What is the influence of DDoS attacks on cryptocurrency exchanges?*

To answer this research question in a structured way, the following three subquestions will be addressed:

1. How and why does a DDoS attack influence a company?
2. What is the size of the impact of a DDoS attack on a cryptocurrency exchange?
3. Is the impact done significant, and if so, is there a recovery from the impact?

The answer to question (1) will be given by doing a literature review which will provide general insights into DDoS attacks done on companies. It will show how such attacks are executed and the reasons behind them. This will give an understanding of how an attack works and why it can

be effective. The answer is important for the research because it will lay the groundwork for the next questions.

The answer to question (2) will be given by looking at the specific example of a cryptocurrency exchange: Bitfinex. Firstly, All the DDoS attacks this exchange experienced from 2015 until 2018 are gathered. Then, these DDoS attacks are analyzed and the level of damage done is calculated using the amount of money the exchange loses in the time service is denied. The answer will show if an attack is a significant negative factor for the exchange. It will also provide a reason why trading behaviour could change. Together with the first question, an argument is formed of how strong the influence is of an attack to an exchange.

Lastly, the answer to question (3) provides clearance to if the attack is actually impactful and if leaves permanent damage or if it is just a short-term inconvenience. This will be done by comparing the number of trades before the attack to the trading behaviour in the days after the attack. A prediction model will be made for the estimation of the number of trades for the event study [28]. This model will be used to mathematically represent the portion of this volatile market. After applying the event study, the cumulative abnormal returns will be calculated. Using an Empirical distribution and a statistical test, the significance of the impact of an attack can be obtained. If this significance holds, a check will be done to see if trading levels come back to the levels before the attack using the prediction model.
Combined, the answers give a solid overview of how an attack can influence the trading behaviour on a cryptocurrency exchange.

3. BACKGROUND

3.1 Blockchain

A blockchain is a data structure which consists of lists of transactions called blocks. Each block has a hash that links it to the previous block, a timestamp and the transaction data. This way the blocks are cryptographically linked together in a chronological order. Users offer their computing power to verify and record payments into the public ledger [35]. This is called mining. The blockchain can record transactions between two parties efficiently and on a verifiable and permanent way [42]. Cryptocurrencies are based on the blockchain technology.
Bitcoin is the most popular and the first widely adopted cryptocurrency [37]. It uses the distributed transaction ledger in a peer-to-peer network. A protocol is set in place for creating and validating new blocks. Cryptocurrencies like Bitcoin can be used as a store of value and as digital currency.

3.2 Cryptocurrency Exchanges

Trading cryptocurrencies can be done on crypto exchanges. At a cryptocurrency exchange, a client can buy, sell, or store digital currencies at the exchange rate and in the currency supported by that particular exchange. Typically, exchanges are matching buyers and sellers together and charge a fee for this service. There are many crypto exchanges currently with Bitfinex being one of the biggest.

3.3 Bitfinex

Bitfinex is a Hong Kong-based cryptocurrency exchange. It is founded in December in 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 with every trade made for this service. They also make money from margin funding and by charging a fee on withdrawing currencies. Since this paper focuses on trading behaviour only, we will only take the trading fees into account. The exchange has much controversy around itself and was a victim of numerous cybercrime attacks including stolen funds by hacks and multiple DDoS attacks.

3.4 DDoS Attacks

A distributed denial of service attack is when multiple computers make repeated requests for data to one computer. This is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DDoS attacks can cost an organization both time and money while their resources and services are inaccessible [40]. DDoS attacks are often performed with a large number of infected computers, called a botnet, and are targeted against websites. There are two different types of attacks focused on different network layers. Network attacks are done on the 3rd and 4th layer and application layer attacks on layer 7 [23]. Both attacks are used at exchanges, so this paper will not make a difference between them.

4. RELATED WORK

A similar research has been done on 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. [24]. 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. [30]. Only when the actual service of the company was down, it did make a significant impact. Because this research is focused on the denial of critical services of exchanges, a significant impact can be expected.
There is also a study done on the impact of DDoS on cryptocurrency exchanges, in particular, the Mt. Gox exchange [29]. This exchange was often terrorized with DDoS attacks and reached an inevitable downfall when it got breached and all the funds got stolen. Mt. Gox does not exist anymore. This paper assumed that the abnormal returns were normally distributed. This was probably done out of ease. This study will contribute to this by not assuming the distribution to be normally distributed but using Empirical methods to estimate the distribution. This is a better way of providing conclusions based on Abhishta et al. [25]. In their further work, the study wanted to look at the same impact but for exchanges that are currently active. This further research fits well with the contribution of this paper.
The study from Moore et al. was the first study on Bitcoin exchanges. The study conducted a survival analysis on 40 Bitcoin exchanges [36]. The conclusion was that the average transaction volume was negatively correlated to the probability that an exchange will close prematurely. The study also found, based on a regression analysis, that transaction volume is positively correlated with experiencing a breach. Hence operating on a high transaction volume makes the exchange more valuable for thieves.
Vasek et al. provided an empirical analysis of DDoS attacks in the Bitcoin ecosystem [41]. They concluded that currency exchanges are attacked most often followed by mining pools and gambling operators. Another conclusion was that services who have been attacked once most often use a DDoS protection. They asked for further research

on this topic with more robust datasets since they gathered their data from an online forum. They also wanted to investigate any consistent variation between trade volumes and exchange rates before and after a DDoS attack. This paper will try to gather this robust dataset with a conclusion on this variation.
Böhme et al. provided motives in their study of Bitcoin economics, technology and governance about the various ways of why a service might be attacked by a DDoS attack [27]. Ross Anderson et al. measured the cost of cybercrime including DDoS attacks. Not only direct costs but also indirect costs and defence costs apply when an attack is successful [26]. These are the costs that apply to DDoS attacks and these will be used to explain the impact on exchanges.

5. IMPACT OF DDOS ATTACKS

5.1 The motives behind a DDoS attack

A cyber-criminal can have various reasons why to execute a DDoS attack on a cryptocurrency exchange. This depends mostly on what kind of motive the person has. The following groups are all known to perform DDoS attacks with their own motives [23]:
Vandalism: Usually, this is a very young group consisting of teenagers who are interested in the underworld of hacking. They like to figure things out on their own and they do not realize how much damage they are doing with their actions. Because of this, most often the victims are websites that are disliked by this group and the internet connections of other people on the internet. There is no plan to gain anything from the attack aside from knowledge and adrenaline.
Hacktivism: The hacktivists are widely known because of the hacker group "Anonymous". This group used to DDoS websites as a form of protest against governments or big corporations with opposing ideologies. The reason for the attacks is often to make a statement and to bring attention to the, according to them, wrong actions of the target. [34]
Extortion: This group consists also of vandals, but their motive is to get financial gain. This is done by threatening a company to pay a certain amount of money or else an attack will follow. It differs on the attacker if such a follow-up attack will come or not. Sometimes multiple waves of attacks happen. Then the ransom and the strength of the attack start small and grow larger by each ransom not paid. These ransoms are often calculated based on the estimation of downtime an attacker can achieve just as this study will do in section 4.3 [26]. The practice shows that paying this ransom is never a good decision.
Business competition: The competitors can also be the initiators of an attack. By executing successful attacks the victim gets reputation damage because of an unreliable website or network. Thus, the reason is to gain market share by making the other competitors worse and then trying to steal the customers. From this interview with an individual who executed DDoS attacks, it appears that this hacker got paid to put websites offline, including Coinbase, the most popular cryptocurrency exchange [21].
Manipulation: Manipulation is possible when the target is the network of a cryptocurrency. This is harder to do but a successful attack can make investors lose trust in the cryptocurrency and start selling this coin. The attacker could have traded on beforehand knowledge to make financial gains because of the DDoS attack. There is also a possibility that an inexperienced trader can launch a DDoS attack on a wrong target without realizing it will not impact the price of the currency. The reason for this is to get favourable trading conditions, but these attacks are not successful.

5.2 Reasons for a DDoS attack

The most favourable reason to execute a DDoS attack is that it can be done anonymously. Because of this, there is a low likelihood of getting caught by law enforcement. DDoS attacks are mostly done by botnets controlled by a bot herder. This is a network of infected machines of unknowing owners. A bot herder can then command these machines to all send requests to a certain website. Since all the traffic is coming from random machines all around the world, it is impossible to trace back the person with bad intentions. If the DDoS attack does not come from a botnet, an executor can use IP spoofing to hide the true source address. This is done by forging a source IP of the packets of the attack. The second reason why DDoS attacks gained popularity is that they are extremely cheap. Online Booters hire out their cybercrime-as-a-service botnets to perform DDoS attacks. A simple attack of guaranteed 20 Gbit for 20 minutes could cost €15 and a week-long attack around €150. The initiator does not need to have any technical knowledge about DDoS attacks anymore. This makes it very easy for the initiator to order an attack. Hiring a Booter is also very cheap. This drastically lowers the threshold to commit online cybercrime.
Exchanges can be valuable targets to attacks by the groups described in the previous section. First of all, the cryptocurrency hype added lots of new traffic to the exchanges. Most exchanges do not have a long life [36], so new ones replace them quickly. Since these novel exchanges are not prepared for a sudden large increase in traffic, many will not work optimally in the first place. These exchanges also profit from cross-side network effects. This means that it is in the interest of the buyers to have many sellers, and for the sellers, it is also in their interest to have many buyers. Because of this an optimal price and liquidity can be achieved. DDoS attackers can profit from this large amount of activity since it assists in adding a load on the exchange. Thus, a less powerful attack can be maximally effective.
Secondly, these exchanges function on a built trust with their users. Customers choose to invest significant amounts of their money through these services. The choice of an exchange is largely based on how trustworthy it is. If an exchange is hacked often and functions poorly, customers will leave it for another exchange. This adds to the fact that a DDoS attack can hurt this trust and do significant indirect damage with the attack.
The last important aspect of a DDoS attack is described in the Kaspersky Lab's quarterly DDoS attacks report of Q3 [32]. This report touched on how some DDoS attacks can be used as a smokescreen for more sophisticated attacks like heists to steal funds from the exchange for example.

5.3 Calculation of impact

During a DDoS attack, the exchange will see a decrease in trading since the systems cannot process the trades anymore. The impact will be that the exchange will lose out on profits it could have made from the trading fees. The causation model can be seen in Figure 1. Using the data provided by data.bitcoinity.org an estimation of the impact of a DDoS attack on the Bitfinex exchange is calculated. This is estimation is done in the following way:
On the data from 2015 to 2018, on average, the Bitfinex daily USD volume was $167 million with 50.000 transactions per day. Thus, the average transaction was around $3300. The Bitfinex trading fees can be found on their

website [1]. For buying and selling these fees are 0.02% and 0.01% respectively. Added together gives it a 0.03% fee per trade. This means that for every average transaction made, Bitfinex earns $10. If Bitfinex would be hit with a successful DDoS attack which put it offline for 1 hour, the company would lose a total of $21.000. If the attack period was longer and Bitfinex would need a whole day to repair the issue: $500.000 of fee profit alone would be lost.
If Bitfinex was hit with such an attack in the hype period of December 2017 and the end of January 2018, it would lose a total of $2.8 million in trading fees in a single day. The full data can be found in Appendix A. These calculations show how significant the impact is of a well-timed DDoS attack on an exchange like Bitfinex.

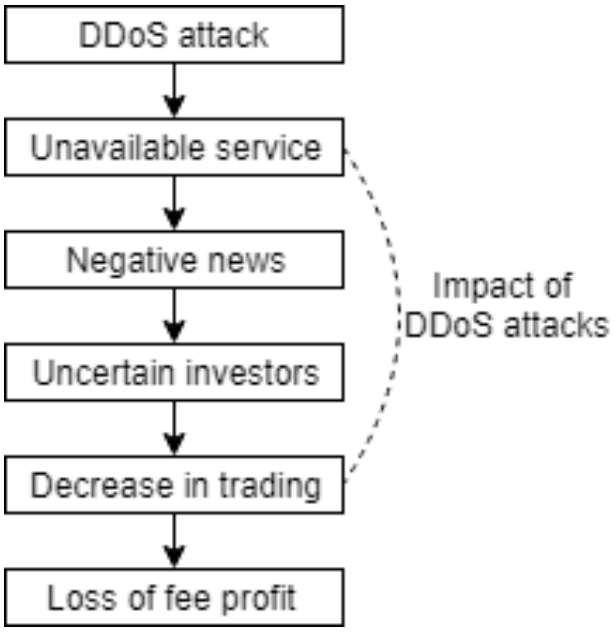

Figure 1. The causation model of a DDoS attack on a cryptocurrency exchange

5.4 Decrease in trading

The paper of Mt. Gox looked at a decrease in trading after a DDoS attack, especially on the decrease of large trades. The arguments were that the large traders may struggle to find sufficient debt in the markets to complete large volume trades after a DDoS attack [29]. In contrary, this paper looks at the whole trading behaviour after a DDoS attack in general.
After a DDoS attack has happened the website of the exchange will most likely not function or function minimally. Logging in authentication will be slowed down which will already add to the uncertainty of investors. Then when investors will try to buy or sell assets, the trades most likely will fail because the system cannot register them in the order book. Then the exchange, if one of its core values is transparency, will announce the attack officially via social media channels. This will make the investors more uncertain and cautious. Many investors will decide not trying to make transactions because of the unreliability of them getting registered. Security shocks increase the probability of trades failing and in some cases, the entire value of the transaction is lost. Therefore it would seem reasonable for users to refrain from exchanging assets on that exchange after witnessing such an attack [29].

6. MODEL

First, a description is given of how the gathering of DDoS attacks from public sources was done and then the design of the analysis for the model is explained.

6.1 Data sources

The DDoS data is collected from three main sources: The Bitfinex incident page, The official Bitfinex twitter page and online articles. A contact was made with Bitfinex. Their response was that they are a transparent exchange and every DDoS attack gets announced on their social media channels. The evidence shows that this is true, although their social media channels are not consistent with each other. Some attacks get announced on one channel while other channels stay silent about it. All the attacks with the sources can be found in Appendix B

Online articles

A Google alert system was set up to collect all articles that were posted online containing the words "DDoS attacks". From those alerts, the ones that contained "Bitfinex" were filtered out and manually analyzed. Out of 174 articles, 15 attacks were distilled by removing duplicates and irrelevant articles. These attacks confirmed the transparency of Bitfinex.

Bitfinex incident page

The website bitfinex.statuspage.io/history provides problems which Bitfinex encountered during its history. All of the found attacks from the articles were confirmed and multiple were added to the list. A total of 22 denial-of-service incidents were found. This data was filtered further by applying the rule that if multiple attacks were executed on consecutive days, the earliest was considered in accordance with previously done research [24, 29]. This concluded a list of 18 unique attacks.

Trading, price and volume data

The daily data of the trading activity, price, and volume of Bitcoin on Bitfinex were gathered from data.bitcoinity.org. Daily data from 01-06-2015 till 16-06-2018 was used for this research. The original data included the trades per minute in a day. The trades per day were calculated using Equation 1 to form the basis of the data.
An anomaly in the data was found and removed. The security of Bitfinex was breached and $72 million of Bitcoin was stolen in 2016 on the second of August [22, 38]. All trading was halted for 7 days. Trading was continued on the 10th of August. This showed up as a blank spot in the data which was then removed from the dataset.

$$T_{day} = T_{minute} \cdot 60 \cdot 24 \tag{1}$$

6.2 Analysis

The analysis was set up in two parts. First, an event study design was created together with a novel estimation model proposal to predict the number of trades per day. Then a statistical test is applied using an empirical distribution to check whether the cumulative abnormal returns were significant in the days after the event.
The event study: Researchers use event studies to study the impact of an event on a firms stock price. Mackinlay discussed this method including several market estimation models [33]. Usually, the prediction model uses a risk-free rate which is based on a market index like the S&P 500 index. Since cryptocurrency does not have such an index, another model is proposed. The prediction model is based on the model used in an earlier study [30]. The estimation model used for the prediction of trades per day is shown in Equation 2.

$$T_n = \alpha|\Delta P_n| + \beta + \epsilon_0 \tag{2}$$

Where the variables α and β are cryptocurrency dependent coefficients and can be estimated using ordinary least squares (OLS). $|\Delta P_n|$ is the absolute price of Bitcoin on day n and it is calculated by the formula given in Equation 3 using the absolute of the price of Bitcoin on day n-1 subtracted from the price of Bitcoin on day n. The stochastic variable ϵ is the error term with the expected value going to 0. Thus, $\mathbb{E}[\epsilon_0] = 0$.

$$|\Delta P_n| = |P_n - P_{n-1}| \tag{3}$$

OLS is chosen as a regression based on the study of Karafiath et al. [31]. This study compared several generalized least squares and first and second order autoregressive structures and it concluded that these do not offer a material improvement over OLS. The estimation model is derived from the correlation between the price change on a given day and the trading done on a given day. Vasek et al. already suggested that attacks follow soon after a hype period [41]. This is argued because when the valuation of a currency changes significantly, independent of the change being positive or negative, the number of trades done will increase. When the price increases this is explained by the Fear of Missing Out (FOMO) buying of investors or the selling of profit taking. When the price decreases weak hands start selling their currencies in expectation of a bigger drop or buyers that were looking for a cheaper price are buying in. This concludes causation with $|\Delta P_n|$ being the independent variable and T_n being the dependent variable. This causation first needs to be checked by using the OLS on both variables and checking the R^2 value of the regression. This is a statistical measure of how close the data are to the fitted regression line. By using this model an attempt is made to mathematically represent the portion of this volatile market.
Using the estimation of each coefficient of the regression formula for each estimation period prior to each attack, the abnormal trades (AT_n) can be calculated for each attack. This is done using the formula 4

$$AT_n = T_n - (\alpha|\Delta P_n| + \beta) \tag{4}$$

After the estimation of each coefficient regression formula for each estimation period prior to each attack, the For the windows of the event study, an estimation and an event window are chosen. The practice for stock market event studies is to use 120 days for the estimation period [33]. Although this is a robust period to choose, we argue that for a novel and extremely volatile market like cryptocurrency this period is too long. Therefore, several estimation windows are applied and compared. These are 30 days, 60 days and 120 days respectively. As for the event period to calculate the cumulative trades (CATs), also multiple periods were chosen. The periods are [0,1], [0,2], [0,3], [0,4], and [0,5]. All the periods can be seen in Figure 2. For stock analysis, it is common to use -1 as the starting date for the event period to accommodate for information leaks. But because the data that is used for in this paper is direct data from the exchange with no possible information leaks, 0 is used as an alternative.
Over these various time-windows, we will cumulate abnormal trades using Formula 5.

$$CAT_{L1,L2} = \sum_{n=L1}^{L2} AT_n \tag{5}$$

Where $CAT_{L1,L2}$ is the cumulative abnormal trades from time L1 to time L2 of the event period and AT_n are the abnormal trades on day n.
The statistical testing: The general wide-spread assumption is that the short-term returns are distributed according to a Gaussian distribution. This assumption was challenged in the paper of Abhishta et al. [25]. The conclusion is that this leads to overestimation/underestimation of the impact. This paper will avoid route and assume that the cumulative trades follow an unknown distribution. This unknown distribution is going to be approximated by the empirical distribution. For similar hypothesis testing, this paper used the bootstrapping method [28]. We use it by generating a large amount of multi-day number of trades. This is done by using the Monte Carlo method by generating a million abnormal trades. Then a statistical test is performed to check the significance. This is done by checking if the CAT's lie in the bottom 15th percentile or the top 85th percentile of this empirical distribution. The 15 percentile scenarios in the left tail are representative of a negative impact and the 85 percentile scenarios in the right tail represent a positive impact. This is seen in Figure 3. Note that even if it looks like a normal distribution, this is not assumed.

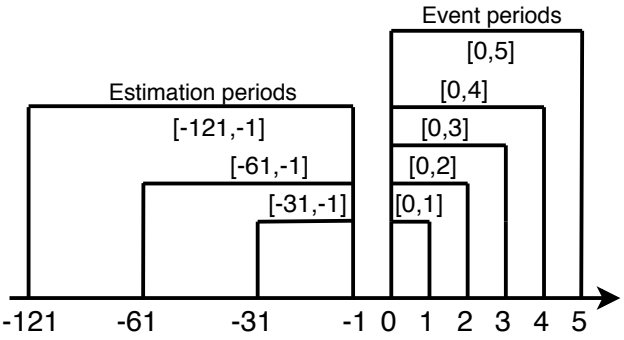

Figure 2. Estimation and Event periods of the event study

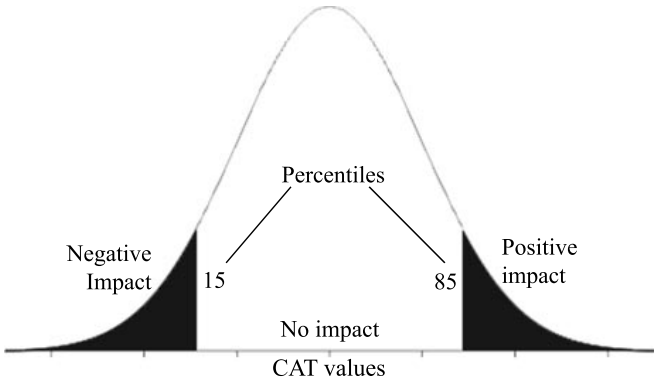

Figure 3. The percentiles used for the statistical test

7. RESULTS

The logistic regression on $|\Delta P_n|$ as independent variable and T_{day} as independent variable on the total three year data gives an R^2 value of 0.71. The closer the R-value to 1 the more dependent the two variables are. This value concludes that the variables are significantly correlated and are viable for our prediction model. The OLS is shown in Figure 4.
After this, an OLS and a Monte Carlo simulation were done for each unique DDoS attack with the corresponding

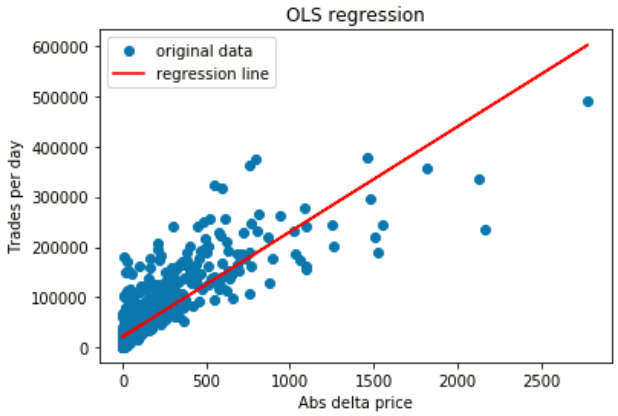

Figure 4. The OLS regression on $|\Delta P_n|$ and T_{day}

estimation and event periods. An example of the first attack can be seen in Figure 5. Checking this data with the statistical test shows that for each estimation period 30, 60, and 120 the attacks do not return a significant negative impact.

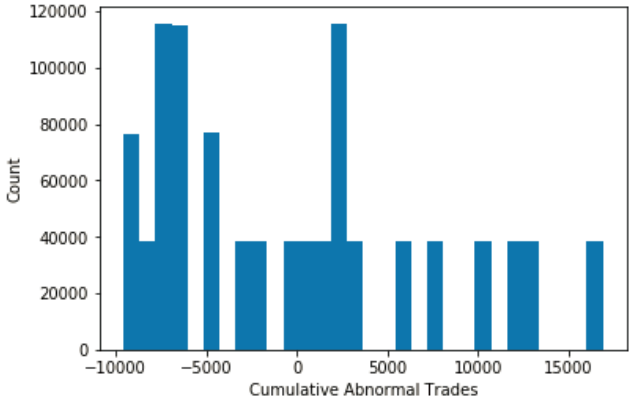

Figure 5. The 5-DAY CAT$_{Attack1}$

8. DISCUSSION

The dataset used for this research was robust in addition to the further work of Vasek et al. because it was primary data gathered from the exchange and not secondary data from online forums [41]. The research is also done on a currently popular and online exchange which has one of the largest volumes of Bitcoin per day. This was asked in the further work of [29]. While a successful attack can impact the exchange, this was not found in the analysis of the data used. This study also could not conclude that the influence of a DDoS attack on a cryptocurrency exchange is significantly negative like the other studies that are done in this field [29, 41]. Perhaps the exchanges are well equipped to tackle the problems that arrive from DDoS attacks on their own. They also use professional social media crisis handling to give investors security in the uncertain periods after the attack. Feder et al. also noted that endogeneity might play a role in the measuring of DDoS attacks on exchanges. This means that the increasing amount of trading will also increase the chance of a DDoS attack. So the variables are correlated with each other. This endogeneity might also skew the results of this study. Perhaps a way to remove this endogeneity can be found and applied to this paper.

9. CONCLUSIONS

The answers to how and why a DDoS attack influences a company were given through the use of a literature review. It is found that DDoS attacks are very easily accessible to the whole public because of cybercrime-as-a-service websites called Booters. No technical knowledge is needed for these and these services are also very cheap. These services can be used by a range of attackers with bad intent. This all depends on the motives of the attacker. Attacks can be done with the intent to do pure damage or can be used to get financial gain through extortion or the worsening of competition. Since these attacks can be done anonymously there is no way of finding the real attacker. The companies are influenced by these attacks because they have to put resources aside to protect themselves from these attacks and the damage they gain from a successful attack. The damage can be anything from financial loss to reputation damage and the losing of customers.
The size of the impact of a DDoS attack on a crypto exchange is measured using the business model of the exchange Bitfinex. This exchange makes money from every trade happening on the platform by charging a fee for it. If a DDoS attack is successful and the service of the exchange will be denied, a large amount of money can be lost. On average the exchange would lose $21.000 per hour or $500.000 per day of revenue if trading is denied.
Using a proposed prediction model for the number of trades for the event study with various estimation and event windows, a significant impact to the cryptocurrency exchange could not be found.

10. ACKNOWLEDGMENTS

I want to thank Abhishta from the IEBIS faculty at the University of Twente for the supervision and the great guidance throughout this research. The weekly meetings and the fast amount of knowledge helped out constructing the arguments and methods used in the paper. The door was always open whenever I ran into a trouble spot or had a question about my research or writing.

11. REFERENCES

[1] Bitfinex - Our fees. "accessed 01-07-2018".
[2] Bitfinex Status - Bitgo DDoS Attack – Delayed Deposit/Withdrawal Processing 05-06-16. "accessed 01-07-2018".
[3] Bitfinex Status - Degraded performance 07-06-16. "accessed 01-07-2018".
[4] Bitfinex Status - Denial of Service 21-02-17. "accessed 01-07-2018".
[5] Bitfinex Status - Distributed Denial of Service (DDoS) 20-01-16. "accessed 01-07-2018".
[6] Bitfinex Status - Incapsula Downtime 10-03-16. "accessed 01-07-2018".
[7] Bitfinex Status - Investigating Denial-of-service attack 07-12-17. "accessed 01-07-2018".
[8] Bitfinex Status - Investigating Denial-of-service attack 13-12-17. "accessed 01-07-2018".
[9] Bitfinex Status - Platform issues 09-11-16. "accessed 01-07-2018".
[10] Bitfinex Status - Platform issues 16-11-16. "accessed 01-07-2018".
[11] Bitfinex Status - Platform issues 21-06-16. "accessed 01-07-2018".
[12] Bitfinex Status - Platform issues 27-07-16. "accessed 01-07-2018".

[13] Bitfinex Status - Platform outage 31-12-17. "accessed 01-07-2018".

[14] Bitfinex Status - Platform under heavy load. "accessed 01-07-2018".

[15] Bitfinex Status - Platform under heavy load 04-12-17. "accessed 01-07-2018".

[16] Bitfinex Status - The platform is experiencing performance issues. 21-08-17. "accessed 01-07-2018".

[17] Bitfinex Status - The platform is under DDoS attack. We are enabling a stricter protection level. 13-06-17. "accessed 01-07-2018".

[18] Bitfinex Twitter - Bitfinex is under DDoS attack 26-11-17. "accessed 01-07-2018".

[19] Bitfinex Twitter - Platforum is currently under heavy DDoS. "accessed 01-07-2018".

[20] Cryptocurrency Market Capitalizations | CoinMarketCap. "accessed 01-07-2018".

[21] Meet An0CBR, the Scourge of Bitcoin Payment Portals - EXCLUSIVE. "accessed 01-07-2018".

[22] Security Breach - Bitfinex blog. "accessed 01-07-2018".

[23] What does DDoS Mean? | Distributed Denial of Service Explained | Incapsula. "accessed 01-07-2018".

[24] Abhishta, R. Joosten, and L. 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)*, pages 354–362. IEEE, 2017.

[25] A. Abhishta, R. Joosten, and B. Nieuwenhuis. Comparing Alternatives to Measure the Impact of DDoS Attack Announcements on Target Stock Prices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 8:1–18, 2017.

[26] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the Cost of Cybercrime.

[27] R. Böhme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspective Volume*, 29(2 Spring):213–238, 2015.

[28] B. Efron. *Bootstrap Methods: Another Look at the Jackknife*. Number 1. Institute of Mathematical Statistics, jan 1992.

[29] A. Feder, N. Gandal, J. T. Hamrick, and T. Moore. The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox.

[30] A. Hovav and J. D'Arcy. The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Managemen and Insurance Review*, 6(2):97–121, sep 2003.

[31] I. Karafiath. Detecting cumulative abnormal volume: a comparison of event study methods. 2009.

[32] I. K. Khalimonenko Alexander, Kupreev Oleg. DDoS attacks in Q3 2017. "accessed 01-07-2018".

[33] A. C. Mackinlay. Event Studies in Economics and Finance. *Source Journal of Economic Literature Journal of Economic Literature*, 35(1):13–39, 1997.

[34] S. Mansfield-Devine. Anonymous: serious threat or mere annoyance? *Network Security*, 2011:4–10, 2011.

[35] Melanie Swan. *Blockchain: Blueprint for a new economy*. O'Reilly Media Inc., 2015.

[36] T. Moore and N. Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk.

[37] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.

[38] Reuters. Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong | Fortune. "accessed 01-07-2018".

[39] J. J. Santanna, R. Van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras. Booters - An analysis of DDoS-as-a-service attacks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pages 243–251, 2015.

[40] US-CERT. Understanding Denial-of-Service Attacks | US-CERT. "accessed 01-07-2018".

[41] M. Vasek, M. Thornton, and T. Moore. Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem.

[42] Wikipedia. Blockchain — Wikipedia, The Free Encyclopedia.

APPENDIX

A. CALCULATIONS OF THE IMPACT OF DDOS ON BITFINEX

	2015-2018 data	Average	Worst day	Best day	Hype (2017 nov-dec)
	Volume in $	1.67E+08	5.69E+05	2.25E+09	9.52E+08
	Transactions per day	49937	1249	489725	213561
	USD per transaction	3341			4458
	USD per minute	115861			661213
	Buying fee bitfinex	0.002	0.002	0.002	0.002
	Selling fee bitfinex	0.001	0.001	0.001	0.001
	Total fee per transaction:	0.003	0.003	0.003	0.003
Bitfinex gain	Fee/transaction	$10			$13
	Fee/minute	$347.58	$1.19	$4,686	$1,984
	Fee/hour	$20,855	$71	$281,150	$119,018
	Fee/day	$500,520	$1,708	$6,747,588	$2,856,438
	Yearly revenue	$182,689,960	$623,387	$2,462,869,675	$1,042,599,918

B. DDOS ATTACK DATA ON BITFINEX

Table 1. DDoS attacks on Bitfinex with an estimation period of 60.

Attack	Source	CAT1	CAT2	CAT3	CAT4	CAT5
1	[5]	5987	-1835	22534	26608	22696
2	[6]	-1658	-3732	1649	394	-958
3	[2]	-3188	3511	8235	18512	25812
4	[3]	9899	16764	19500	22811	27703
5	[11]	18633	72963	117435	186053	173697
6	[12]	3422	5677	6665	5297	903
7	[9]	1345	4354	4407	8619	13304
8	[10]	7706	10026	12389	13425	19397
9	[4]	-4939	-5928	-2997	7133	16116
10	[17]	84006	122658	174820	275080	277879
11	[16]	24626	81079	83890	85536	81203
12	[18]	34	23386	63117	272258	512372
13	[15]	81128	117683	182524	243590	481917
14	[7]	63825	298292	537249	837850	822484
15	[8]	86572	277253	426323	504535	552819
16	[19]	10715	160562	366093	681917	883303
17	[13]	13073	8612	45703	-10298	76798
18	[14]	-6735	-38444	-72168	-84305	-113015