The Impact of DDoS and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox

Amir Feder
Berglas School of Economics
Tel Aviv University, Israel
amirfeder@mail.tau.ac.il

Neil Gandal
Berglas School of Economics
Tel Aviv University, Israel
gandal@post.tau.ac.il

JT Hamrick
Tandy School of Computer Science
University of Tulsa, USA
jth563@utulsa.edu

Tyler Moore
Tandy School of Computer Science
University of Tulsa, USA
tyler-moore@utulsa.edu

Abstract

We investigate how distributed denial-of-service (DDoS) attacks and other disruptions affect the Bitcoin ecosystem. In particular, we investigate the impact of shocks on trading activity at the leading Mt. Gox exchange between April 2011 and November 2013. We find that following DDoS attacks on Mt. Gox, the number of large trades on the exchange fell sharply. In particular, the distribution of the daily trading volume becomes less skewed (fewer big trades) and had smaller kurtosis on days following DDoS attacks. The results are robust to alternative specifications, as well as to restricting the data to activity prior to March 2013, i.e., the period before the first large appreciation in the price of and attention paid to Bitcoin.

1 Introduction

The recent rise in digital currencies, led by the introduction of Bitcoin in 2009 [8], creates an opportunity to measure information security risk in a way that has often not been possible in other contexts. Digital currencies (or cryptocurrencies) aspire to compete against other online payment methods such as credit/debit cards and PayPal, as well as serve as an alternative store of value. They have been designed with transparency in mind, which creates an opportunity to quantify risks better. While Bitcoin's design provides some safeguards against 'counterfeiting' of the currency, in practice the ecosystem is vulnerable to thefts by cybercriminals, frequently targeting intermediaries such as wallets or exchanges.

Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 13–14, 2016.

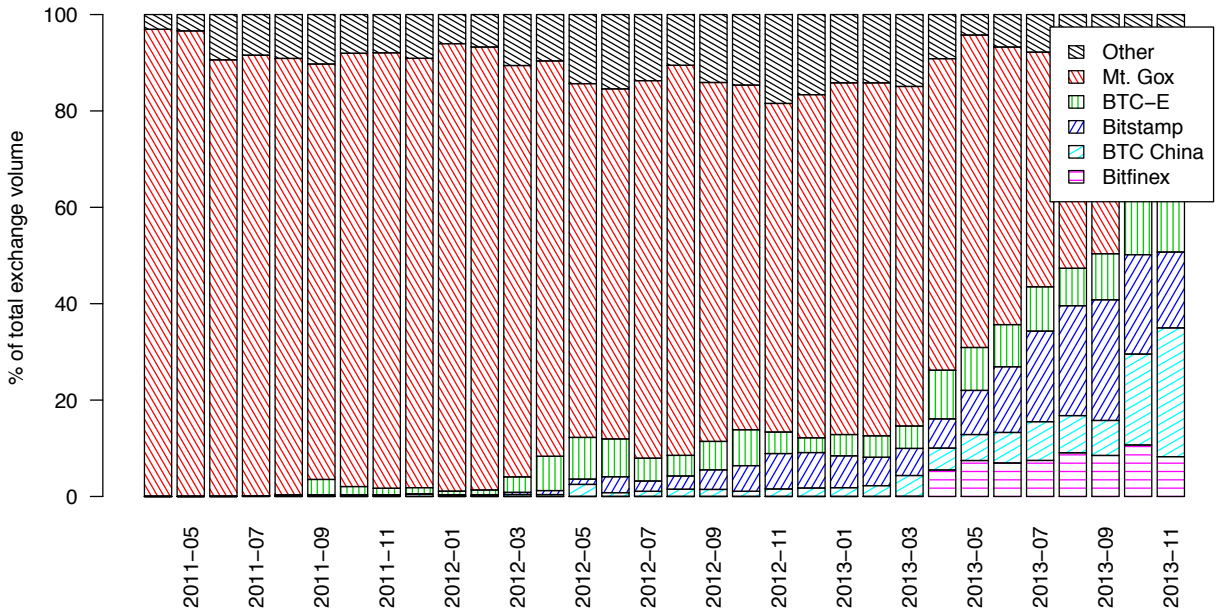

Figure 1: Distribution of market share among Bitcoin currency exchanges by reported trade volume, April 2011 to November 2013. (Source: `bitcoincharts.com`)

In this paper, we investigate how one such risk, distributed denial-of-service (DDoS) attack, affects the Bitcoin ecosystem. While denial-of-service attacks have been launched on a wide range of Bitcoin services, from gambling sites to mining pools [12, 4], we focus our investigation on how DDoS attacks affected the Mt.Gox exchange. We do so for several reasons. First, prior research has established that Mt. Gox has been targeted by DDoS attacks far more than any other Bitcoin service [12]. Second, DDoS attacks on currency exchanges have the potential to be financially lucrative to its proponents as well as extremely disruptive: preventing others from buying or selling creates an unfair financial advantage for the perpetrator at the expense of ordinary participants. Third, following Mt. Gox's collapse, a dump of millions of transactions was publicly disclosed, creating a unique opportunity to quantify the impact of DDoS attacks on trading. Finally, as Figure 1 shows, Mt. Gox was by far the leading Bitcoin exchange during most of the 2.5-year period for which we have data.

Using an event study design, we find that following DDoS attacks on Mt. Gox, there was a significant reduction in the number of large trades on the exchange. In particular, the distribution of the daily trading volume becomes less skewed (fewer big trades) on days following DDoS attacks. The results are robust to alternative specifications and to restricting the data to the period March 2013, i.e., the period before the big appreciation in the price of Bitcoin.

The question is important because exchanges are critical institutions in the Bitcoin ecosystem. In the exchanges, sellers benefit from a larger number of buyers, and buyers benefit from a larger number of sellers (so-called positive cross-side network effects). An exchange is an example of a platform; in order for an exchange to succeed, it must build up trust among its users, since a loss of confidence in an exchange can quickly lead to a downwards spiral in which buyers and sellers quickly cease trading on the platform.

The market for cryptocurrency exchanges is very vibrant. The exchanges considered to be the major players changed significantly over time. New ones appeared, and existing ones were pushed out of the market. The Mt. Gox failure in February 2014 showed that even a large exchange may suddenly exit the market.

2 Related Work

The popularity of Bitcoin, especially when compared to prior cryptocurrencies, has spawned a huge amount of research activity. Bonneau et al. review the (primarily) technical research, ranging from vulnerabilities in the implementation and operation to the development of alternative systems aiming to improve on Bitcoin's design [2]. Böhme et al. discuss Bitcoin's design, risks and open challenges geared toward a social science audience [1]. Taken together, these articles offer a baseline understanding of key issues facing cryptocurrencies identified by scholars.

A growing number of researchers have leveraged Bitcoin's transparency to study user behavior and attacks. Some have mined the blockchain, the public ledger of completed transactions. Meiklejohn et al. conducted a large-scale investigation of the blockchain in part to trace transactions back to popular Bitcoin service providers, such as currency exchanges [5]. Ron and Shamir constructed a graph of Bitcoin transactions from the blockchain in order to identify suspicious transaction chains [9]. Several studies mine the blockchain to document the prevalence of undesirable activity, including money laundering [7], mining botnets [3], scams such as Ponzi schemes [11], and stolen "brain" wallets [10].

Currency exchanges have been recognized to play a central role in the Bitcoin ecosystem. Moore and Christin reported that by early 2013, 45% of Bitcoin currency exchanges had closed, and that many are plagued by frequent outages and security breaches [6]. Vasek et al. documented reports of denial-of-service attacks targeting a range of Bitcoin services, including 58 attacks on exchanges [11].

These disruptions may reflect the volatility of today's Bitcoin ecosystem, but they might also represent something more sinister. People could deliberately introduce shocks to Bitcoin exchanges in order to profit financially (e.g., by preventing others from buying to bid up low

prices). A denial-of-service attack might introduce enough instability for a malevolent actor to exploit. We hope to explore this issue in future work. In this paper, we conduct the first econometric study of the impact of denial-of-service attacks on trading activity at Bitcoin exchanges.

3 Methodology

3.1 Data Sources

3.1.1 Exchange Activity

Shortly after filing for bankruptcy in early 2014, a trade history of Mt. Gox transactions was publicly leaked. The leaked data includes transaction time, user identifier (numeric, apparently for internal use only), currency converting to/from bitcoins, transaction amount and exchange rate. This data offers much finer granularity than is typically available, since most buy and sell transactions are recorded only by the exchange and never appear on the blockchain. The data can be leveraged to monitor changes in user participation as well as overall transaction volume at times surrounding shocks. In total, nearly 18 million matching buy and sell transactions are reported between April 2011 and November 2013.

We supplemented these data with daily transaction volumes reported by the `bitcoincharts.com` website for all monitored Bitcoin exchanges, in addition to Mt. Gox. Because some entries obtained from `bitcoincharts.com` included missing values, we also gathered weekly transaction data from `bitcoinity.org` in order to validate the gathered data.

Dataset Validation While it is impossible to directly ascertain the validity of the Mt. Gox transaction data, we did conduct a few sanity checks to ensure that the data is consistent. As a first check, we verified that the total buy transactions are matched in number and aggregate value for the sell transactions.

Upon delving deeper into the Mt. Gox leaked data, we identified that there are many duplicate entries in the dump file. We have found that the Mt. Gox registry sometimes had multiple entries for transactions with the same user id, transaction time, transaction type (buy/sell) and transaction amount. We considered two forms of de-duplication. The more conservative approach is to treat each (user id, timestamp, transaction type, amount in BTC, amount in Japanese Yen) tuple as unique (de-duplication strategy 1). Removing such duplicates narrows the data from approximately 18 million to 14 million transactions[1].

[1]Note that each completed transaction has both a buy and sell record, which means that the total number of unique completed transactions is 7 million.

A more aggressive de-duplication strategy is to consider "user id, timestamp, transaction type, amount in BTC" tuples as unique (de-duplication strategy 2). Using this strategy, transactions that are reported at the same time but at different exchange rates are treated as duplicates.

As a further sanity check, we compared the de-duplicated data with other data reported by others. To that end, we compared the Mt. Gox transaction volumes to the daily totals reported on `bitcoincharts.com` to the leaked dataset. Both de-duplicated datasets are more consistent with the daily totals found on `bitcoincharts.com` than original leaked data.

Figure 2 plots the daily differences in transaction between leaked dataset and totals reported by `bitcoincharts.com`. Differences are normalized as a fraction of the leaked daily volume. Positive numbers indicate that the leaked data reported higher volume. Note that some difference is expected, particularly if the time zones used in the leaked data and on `bitcoincharts.com` differ. Also, note that there were a few gaps in when data was reported by `bitcoincharts.com` (e.g., in mid-2012 and January 2013). These gaps only affect the comparisons between datasets, not the subsequent analysis.

Overlaid on the graph is a red dotted line on days where DDoS attacks are reported at Mt. Gox, and a blue dashed line for other shocks. From this we can see that data is available during the shocks, and there does not appear to be any increase in the disparity between sources on days where shocks occurred.

The top graph reports on de-duplication strategy 1. We can see that the transaction volume is always the same or higher in the leaked data. The difference, while volatile, increases somewhat as time passes. The bottom graph reports on de-duplication strategy 2. During 2011, `bitcoincharts.com` reports higher volumes than Mt. Gox tracked internally, but this changed as time progressed, and the overall trend lines are similar in both graphs.

Finally, we note that we have communicated with multiple Mt. Gox users, who confirmed that their own transactions were accurately reported in the leaked data.

From this analysis, we conclude that the de-duplicated leaked data appears robust enough to provide a reliable signal of the true levels of trade activity at Mt. Gox. We use de-duplication strategy 1 for the subsequent analysis in the paper, but we note that the results remain consistent regardless of the de-duplication strategy used (including even when not removing any duplicates).

Ethical Considerations We elected to use the leaked Mt. Gox data in our research because the data had already been publicly disclosed by others. Consequently, our examination of the data does not add to any existing harms imposed by the dataset's initial publication.

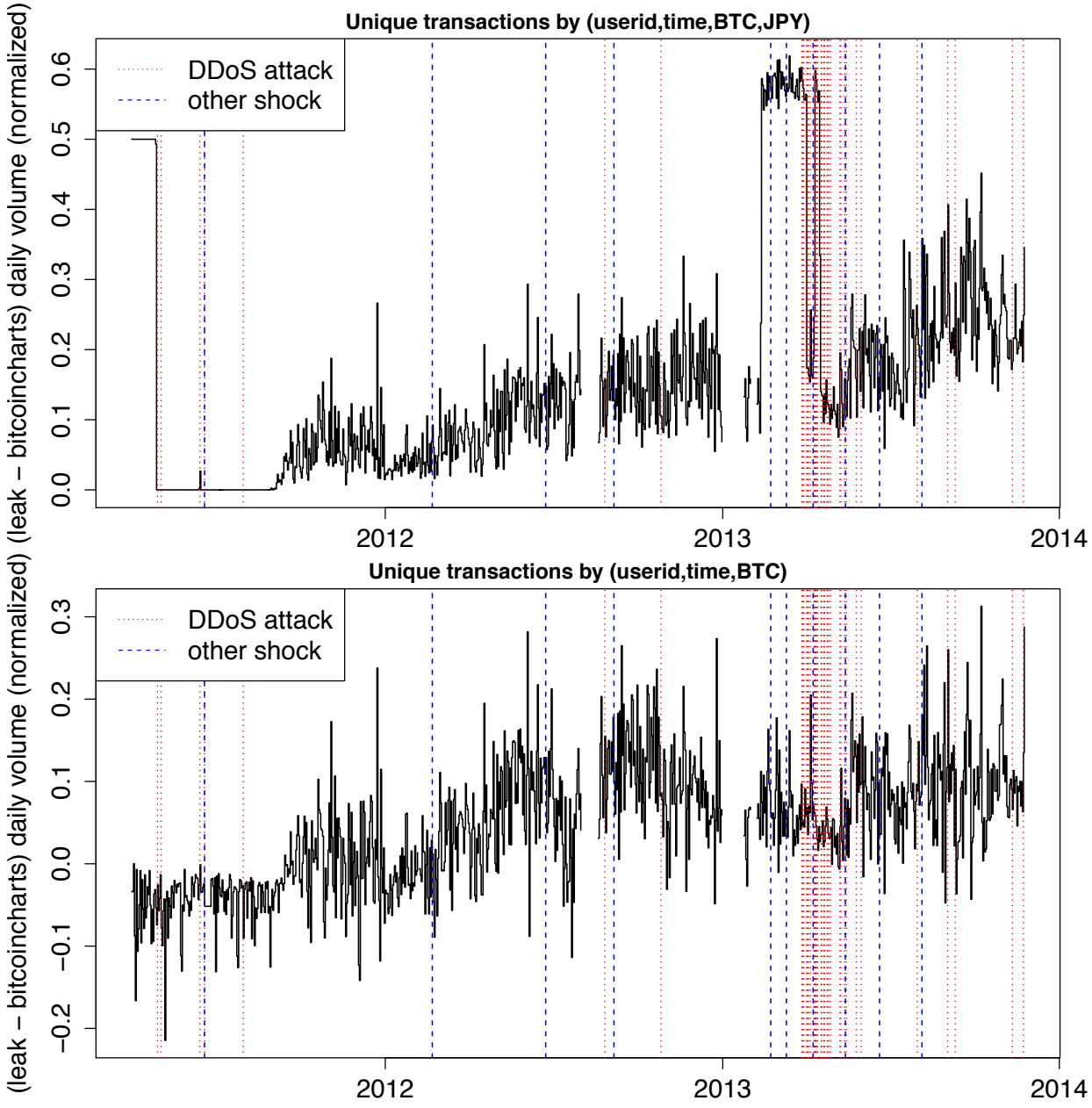

Figure 2: Daily differences in transaction volume between leaked dataset and totals reported by `bitcoincharts.com`. Differences are normalized as a fraction of the leaked daily volume. Positive numbers indicate that the leaked data reported higher volume.

In fact, by analyzing the transactions for a prominent closed exchange, we hope to shed light on how denial-of-service attacks might impact today's exchanges.

3.1.2 Shocks to Mt. Gox

We are primarily interested in measuring the impact of reported denial-of-service attacks targeting the Mt. Gox exchange on Mt. Gox itself, as well as any secondary impact on other Bitcoin exchanges. We examine several sources of data on shocks affecting Mt. Gox.

Dataset D1: Reported DDoS attacks We combine three sources of reported DDoS attacks affecting Mt. Gox: user reports in the `bitcointalk.org` forum, user reports in the /r/bitcoin Reddit sub-forum, and public announcements by Mt. Gox in the press and on social media.

In [12], Vasek et al. measure the prevalence of DDoS attacks on a range of Bitcoin services by inspecting posts on the popular `bitcointalk.org` discussion forum. We use the data published by the authors (available from `doi:10.7910/DVN/25541`), which reports the day that a thread describing a reported DDoS attack on Mt. Gox is started. The authors in [12] used a keyword-based classifier to identify candidate threads discussing DDoS attacks, then manually inspected all threads to ensure that a purported DDoS attack is in fact being discussed (as opposed to a general discussion of DDoS attacks or their hypothetical impact). Reports were gathered between February 2011 and October 2013, with 34 attacks reported on Mt. Gox.

The /r/bitcoin forum on Reddit is another popular discussion forum. We inspected historical posts using the Reddit API, following the same procedure as the authors in [12]. In all, we found 8 reported DDoS attacks on Mt. Gox discussed on Reddit, reported between April and November 2013. Three of these attacks were also reported on `bitcointalk.org`.

Of course, what's being measured here are *reported* DDoS attacks, not confirmed events. It is possible that some of the outages experienced by users were caused by other reasons than a DDoS attack.

Mt. Gox frequently issued press releases via its website and social media whenever outages occurred. Sometimes the outages were directly attributed to DDoS attacks. Unfortunately, after Mt. Gox collapsed, most of these pages were deleted, and so their public statements have been lost forever[2]. In a few cases, however, reports could be obtained from third-party websites or Gox's Google+ page (that was seemingly forgotten when the other social media accounts were deleted). In total, we found direct acknowledgment of DDoS attacks by Mt. Gox on 9 occasions.

[2]We even checked `archive.org`, which did not preserve the pages with public statements.

Date	Description
2011-06-19	Security breach causes BTC fall to 0.01 USD
2012-02-21	Kernel panic triggers outage
2012-06-23	Invalid trading causes outage
2012-09-05	Unplanned trading outage
2013-02-22	Dwolla AML efforts cancel USD transfers
2013-03-11	Blockchain fork glitch
2013-04-09	Outage reportedly caused by high trade volume
2013-05-14	DHS seizes cash in court action
2013-06-20	Suspends USD withdrawals
2013-08-05	Announces significant losses due to early crediting

Table 1: Additional shocks, other than DDoS, affecting Mt. Gox.

Some of the attacks were reported in more than one source. Across all three data sources, DDoS attacks were reported on 37 days.

D2: Additional security shocks DDoS attacks were far from the only adverse event afflicting Mt. Gox while operating. The exchange faced pressure from regulators, thefts from users, and self-inflicted IT outages. We have documented 10 publicly-available shocks by examining statements from Mt. Gox obtained from news reports, press releases and social media. The events are described in Table 1.

D3: Confirmed DDoS attacks Because we cannot be certain that all DDoS attacks reported on the discussion forums actually transpired, we also examine a narrow subset of 9 DDoS attacks that Mt. Gox directly acknowledged.

While the possibility false negatives (i.e., shock events that transpired but we did not observe) cannot be eliminated, we are confident that most events affecting Mt. Gox are included. By scouring public reports from the two most popular discussion forums and direct acknowledgments by the company, we believe that the number of missing events is likely quite small.

3.2 Model

We now describe the regression models used. Section 3.2.1 describes a first attempt, using transaction volumes and large trades as the dependent variable, while Section 3.2.2 describes the more robust dependent variables of skewness and kurtosis of daily transaction volumes.

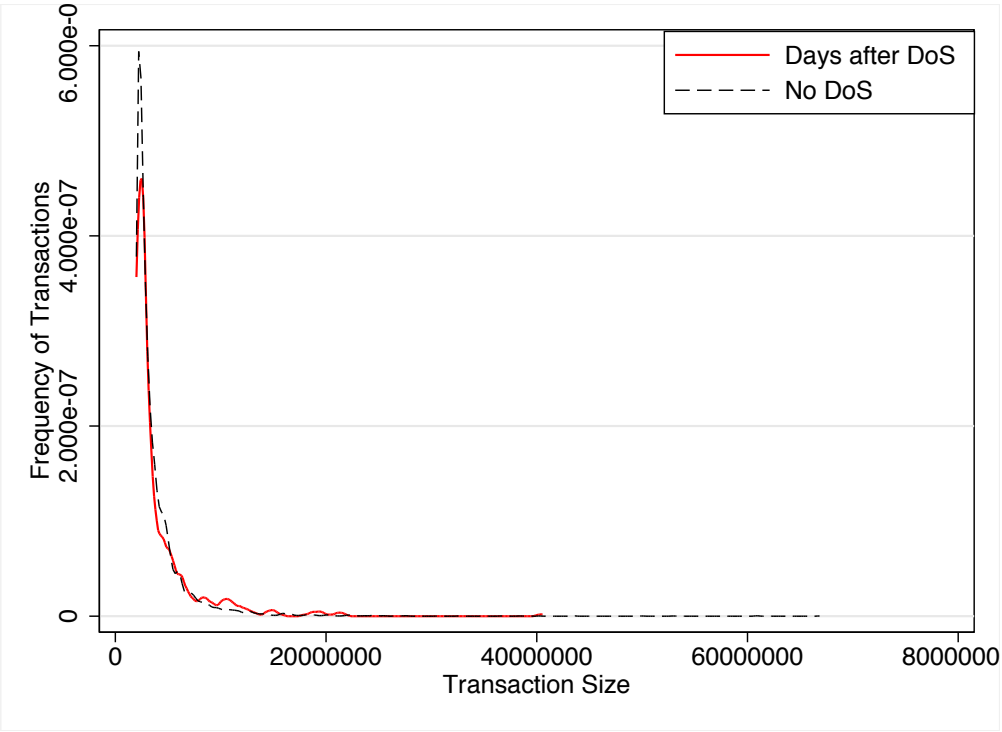

Figure 3: Distribution of transactions by amount in JPY on days following a reported DDoS attack (in red) and on all other days (in black)

3.2.1 Transaction Volume and Large Trades

A security shock increases the probability of a failed trade, and in some reported incidents entire value of the transaction can be lost. Therefore, it would seem reasonable for users to refrain from buying or selling Bitcoins on an exchange after witnessing attacks. To measure the effect of those shocks on the Bitcoin ecosystem, we turn to transaction volume, the most common indicator of user activity.

We start by looking at the effect of reported events from the D1 and D2 data sets on the transaction volume. We aggregate the daily transactions listed in the Mt. Gox leaked data set and use this daily sum as our independent variable. At this point, it is crucial to keep in mind that our 924 observations (one for each day) in the Mt. Gox data set, are by no means identically and independently distributed. This time series has a positive trend that is not linear and is highly correlated with the sharp appreciation in the price of Bitcoin that occurred between April and October 2013. Assuming a linear time trend, we estimate the following regression equation:

$$TransactionVolume_t = \beta_0 + \beta_1 D1_t + \beta_2 D2_t + \beta_3 Time_t + \epsilon_t \quad (1)$$

Transaction volume is the daily volume of trade in Japanese Yen (JPY). D1 is a dummy variable that takes on the value one the day following a DDoS attack and zero otherwise. D2 is a dummy variable that takes on the value one on the day following the other 10 shocks as described above. The variable "Time" is a time trend, and ϵ is the error term. The subscript t indicates that the data we employ are daily observations.

Since the hypothesis is that there is a drop in relatively large transactions following a DDoS attack, we also can use the daily highest transaction (denoted Max. Transaction) as an independent variable and check weather there is indeed a substantial change on the day after the attack. For the same reasons noted above, we employ a time trend and estimate the following regression equation:

$$Max.Transaction_t = \beta_0 + \beta_1 D1_t + \beta_2 D2_t + \beta_3 Time_t + \epsilon_t \tag{2}$$

Since testing the size of the biggest daily transaction can only shed a bit of light on the effect of a shock, we also compute the daily number of very large transactions and use that as our independent variable. The threshold is of course debatable, but we have found similar results with all the definitions we tried. In the results section, we present results for large transactions defined as those exceeding 1000 USD, taking into account the exchange rate to JPY, the currency Mt. Gox had used for its internal storage. Again, we employ a regression with the same dependent variables:

$$LargeTransactions_t = \beta_0 + \beta_1 D1_t + \beta_2 D2_t + \beta_3 Time_t + \epsilon_t \tag{3}$$

3.2.2 Skewness and kurtosis

Since the data set is comprised of daily aggregates listed in a chronological order, we must deal with problems that might arise when using time series data. Prior work has shown that attempted attacks are correlated with the volume of Bitcoins traded [12], meaning it is more likely the attacks will occur in periods with high liquidity and larger volume of transactions. This important finding means that high volumes of trade can lead to an increased likelihood of a DDoS attacks. In such a case, the regressions described above in equations (1), (2) and (3) would all suffer from endogeneity bias.

For this reason, we employ kurtosis and skewness as dependent variables. Using the skewness and kurtosis of the daily transaction distribution as dependent variables is important for several reasons.[3]

[3]We will report results from equations (2) and (3) above, but because of the potential endogeneity, the parameter estimates from these OLS regressions are likely biased.

- First, there is no significant time trend in skewness and kurtosis; the data show that while the volume of trade to grow over time, the distribution of daily trades (in the form of kurtosis and skewness) does not change at all.

- Second, the variables skewness and kurtosis captures the very essence of the hypothesis we are interested in testing, namely that DDoS attacks might affect different types of trades (large and small) in different ways.

- Finally, there is no potential endogeity; that is, changes in kurtosis and skewness are not likely to lead to an increased likelihood of a DDoS attack.

Both kurtosis and skewness are higher when the distribution has heavy tails. In the case of trades at Mt. Gox, in general, most of the trades are for small amounts and there are a smaller number of trades involving larger amounts. Hence, if the DDoS attacks lead to a reduction in the number and/or size of the large trades, the kurtosis and skewness will fall. We use the natural log of kurtosis and skewness as the dependent variables, but the results are robust to using levels of these variables.

The key independent variable is the incidence of DDoS attacks. The variable D1 takes on the value one if an attack occurred the previous day and zero otherwise. Sometimes a DDoS attack lasted for more than one day. In such a case, we considered two alternatives: (1) define D1 as the day after the end of the continuous attack and (2) define D1 to also include day two and three etc. of the attack as "days after an attack." Our results are robust to either of these specifications. In our main results in Table 2, we report results using the first definition for D1.

Other independent (control) variables include the number of users on the exchange, the total volume of the exchange, and a time trend. While the number of unique users (denoted users) and the transaction volume are co-determined in the system, there is no reason why there should be correlation between these variables and the error term when the dependent variable is either skewness or kurtosis. Hence, there is no bias introduced by including these measures as explanatory variables; thus ordinary least squares (OLS) regressions are appropriate. (We also ran regressions without these variables and the results are very similar and extremely robust.)

Our main results come from the following regression equations:

$$ln(skewness)_t = \beta_0 + \beta_1 D1_t + \beta_2 D2_t + \beta_3 ln(TransactionVolume)_t + \beta_4 Users_t + \beta_5 Time_t + \epsilon_t \quad (4)$$

Table 2: Transaction Volume and Large Trades

VARIABLES	(1) Transaction Volume	(2) Max. Transaction	(3) Large Transactions
D1	-2.826e+07	-700,953	-104.6
	(1.306e+08)	(1.265e+06)	(277.3)
D2	1.588e+08	1.559e+06	311.4
	(1.963e+08)	(1.901e+06)	(416.8)
Time	1.053e+06***	13,140***	2.246***
	(76,263)	(738.5)	(0.162)
Constant	-2.334e+08***	-2.215e+06***	-537.5***
	(4.064e+07)	(393,531)	(86.28)
Observations	924	924	924
Adjusted R-squared	0.171	0.255	0.172

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

$$ln(kurtosis)_t = \beta_0 + \beta_1 D1_t + \beta_2 D2_t + \beta_3 ln(TransactionVolume)_t + \beta_4 Users_t + \beta_5 Time_t + \epsilon_t \quad (5)$$

4 Results

Looking first at the effects of D1 and D2 events on the transaction volume and large trades on the Mt. Gox, the regression results are inconclusive. From the regression results in Table 2, the sign of the estimated coefficient on D1 is negative as we hypothesized, but the estimates are not significant. This may be because of the endogeneity bias discussed above, which would lead to upper-ward biased estimates. The estimated coefficient on D2 is positive, but again insignificant. These estimates may also be biased upwards.[4] For the reasons discussed above, the endogeneity bias is a severe handicap in identifying what exactly happens after users realize that a DDoS attack has occurred.

As noted above our preferred models have kurtosis and skweness as dependent variables. In Table 3, we report results from the regressions that examine the effect of D1 and D2 events on the Skewness and Kurtosis of the transaction distribution. We use the natural

[4]The relatively high values of adjusted R-squares are due to the extremely significant time trend in the data.

Table 3: Skewness and Kurtosis

VARIABLES	(1) ln(Skewness)	(2) ln(Kurtosis)
D1	-0.276**	-0.560***
	(0.112)	(0.214)
D2	-0.0766	-0.160
	(0.168)	(0.322)
Users	-0.000144***	-0.000247***
	(2.32e-05)	(4.44e-05)
ln(Transaction Volume)	0.327***	0.640***
	(0.0279)	(0.0534)
Time	-0.000889***	-0.00167***
	(0.000107)	(0.000206)
Constant	-2.358***	-4.192***
	(0.432)	(0.828)
Observations	924	924
Adjusted R-squared	0.166	0.194

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

logarithm of both Skewness/Kurtosis, but qualitatively similar results obtain with levels of these variables.

The results in Table 3 show that a DDoS attack changes both Skewness and the Kurtosis in the days following the attack. In fact, we see a significant drop of 56 percent in the Kurtosis and 28 percent in the Skewness following a DDoS attack. The sign of the coefficient estimate associated with D2 is now negative as expected, but it is not statistically significant in either of the regressions in Table 3. This suggests that DDoS attacks had more serious effects than other types of shocks Mt.Gox incurred.

The estimated effect of the (natural logarithm of the) daily transaction volume is as expected positive and significant in both equations. This variable is primarily included as a control variable. Excluding transaction volume has no effect on our main results, namely that DDoS attacks lead to a significant drop in both Kurtosis and Skewness.

4.1 Robustness Analysis

In this section, we want to examine whether the regression results we reported in Table 3 are robust. Hence four robustness regressions are shown in Table (4.) In the first two

regressions, we re-estimate equations (4) and (5) and include the variable D3, which takes on the value one for DDoS attacks Mt. Gox acknowledged. In these regressions, the variable "$D1 - without - D3$" only includes the attacks not acknowledged by Mt. Gox. Hence, the DDoS attacks are split between attacks not acknowledged by Mt. Gox ($D1 - without - D3$) and attacks acknowledged by Mt. Gox (D3.) The regressions show that attacks not acknowledged by Mt. Gox lead to significant reductions of skewness (by 37 percent) and kurtosis (by 74 percent.) Attacks acknowledged by Mt. Gox lead to reductions of skewness and kurtosis, but this effect is not significant.[5]

In the third and forth regressions in Table (4,) we we re-estimate equations (4) and (5) using the alternative definition for D1, namely that in the case of a continuous attack, all days except for the first day of the attack have the variable "$D1 - alt - withoutD3$" equal to one. Of course, for the day following each attack, ($D1 - alt - without - D3$) takes on the value one. The results in these regressions show that our findings are robust to this alternative definition as well.

Finally, our results from estimating equations (4) and (5) are extremely robust in general. In particular they are robust to the following:

- Including or excluding a time trend.
- Including or excluding transaction volumes and the number of users.
- Estimating (4) and (5) in levels and not logarithms.
- All combinations of the above.[6]

[5]This may be because there are a very small number of attacks acknowledged by Mt. Gox.
[6]For ease of presentation, these regressions are not shown in the paper.

Table 4 - Robustness Analysis

VARIABLES	(1) ln(Skewness)	(2) ln(Kurtosis)	(3) ln(Skewness)	(4) ln(Kurtosis)
D1-without-D3	-0.365***	-0.742***		
	(0.133)	(0.255)		
D1-alt-without-D3			-0.241**	-0.497**
			(0.112)	(0.215)
D2	-0.0663	-0.140	-0.0789	-0.165
	(0.168)	(0.322)	(0.168)	(0.322)
D3	-0.0535	-0.150	-0.0208	-0.0825
	(0.201)	(0.385)	(0.202)	(0.387)
Users	-0.000147***	-0.000252***	-0.000145***	-0.000248***
	(2.33e-05)	(4.45e-05)	(2.33e-05)	(4.46e-05)
ln(TransactionVolume)	0.328***	0.644***	0.327***	0.641***
	(0.0279)	(0.0534)	(0.0279)	(0.0535)
Time	-0.000890***	-0.00167***	-0.000885***	-0.00166***
	(0.000107)	(0.000205)	(0.000107)	(0.000206)
Constant	-2.383***	-4.242***	-2.363***	-4.202***
	(0.432)	(0.828)	(0.433)	(0.829)
Observations	924	924	924	924
Adjusted R-squared	0.166	0.195	0.164	0.192

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

5 Discussion

5.1 Additional Analysis – User Activity

Since our main hypothesis is that there is a significant drop in large trades following an attack, it could worth investigating how the composition of users change in response to a DoS security shock. Our Mt. Gox leaked data set gives us a unique opportunity to see how different users response to an attack, or more precisely a reported attack. It is reasonable to suspect that not all users are even aware that an attack has occurred and are not a part of the forum communities that we have monitored in this research. If this is true, it would

be reasonable to expect different responses for different subgroups of users. So, a deeper look into patterns of trade by different type of users could shed some light on the observed change in the distribution of transactions. We intend to address this issue in future work.

5.2 Additional Analysis – Effect on Other Exchanges

Since Mt. Gox was by far the dominant exchange during this period, it would be interesting to examine whether DDoS attacks on Mt. Gox led users to conduct more trades on other exchanges. We will also address this issue in future work.

6 Conclusion

In this paper we have conducted the first econometric study measuring the impact of distributed denial-of-service attacks on Bitcoin currency exchanges. We gathered evidence of reported DDoS attacks from two popular Bitcoin discussion forums, finding attacks targeting Mt. Gox on 37 days between April 2011 and November 2013. We also investigated the impact of 10 additional shocks affecting Mt. Gox during the period, such as security breaches and unplanned outages. We compared these data sets against transaction data obtained from Mt. Gox over 2.5 years.

We constructed a series of regressions to measure the effect of shocks on transaction volume. Unfortunately, using the transaction volume directly as the dependent variable in the regressions is problematic, due to endogeneity issues and the rising trend in transaction volume over time. Consequently, we selected skewness and kurtosis of the daily transaction volume, which does not suffer from the same problems as measuring transaction volume directly. With these measures, we find that on days where DDoS attacks or other shocks occur, both the skewness and kurtosis decrease. In other words, the distribution of daily transaction volume shifts so that fewer extremely large transactions take place when shocks occur.

In future work, we plan to carry out similar analysis on cryptocurrency exchanges active today, as well as on other Bitcoin services. Furthermore, the analysis presented here has only measured the direct impact of DDoS attacks on transaction volume. Our eventual goal is to measure any effect of active manipulation by profit-motivated cybercriminals who can leverage the manipulation in financial markets afforded by these shocks.

Acknowledgments

The authors gratefully acknowledge support from a research grant from the Interdisciplinary Cyber Research Center, Tel Aviv University.

References

[1] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–38, 2015.

[2] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *IEEE Symposium on Security and Privacy*, May 2015.

[3] Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Chris Grier, Damon McCoy, Stefan Savage, Nicholas Weaver, Alex C Snoeren, and Kirill Levchenko. Botcoin: Monetizing stolen cycles. In *Proceedings of the Network and Distributed System Security Symposium*, 2014.

[4] Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In *1st Workshop on Bitcoin Research*, volume 8438 of *Lecture Notes in Computer Science*, pages 72–86. Springer, March 2014.

[5] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of Bitcoins: Characterizing payments among men with no names. In *Proceedings of the Internet Measurement Conference*, pages 127–140. ACM, 2013.

[6] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 25–33. Springer, April 2013.

[7] Malte Möser, Rainer Böhme, and Dominic Breuker. An inquiry into money laundering tools in the Bitcoin ecosystem. In *Proceedings of the Seventh APWG eCrime Researcher's Summit*, pages 1–14. IEEE, 2013.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008.

[9] Dorit Ron and Adi Shamir. Quantitative analysis of the full Bitcoin transaction graph. In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 6–24. Springer, 2013.

[10] Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore. The Bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets. In *Financial Cryptography and Data Security*, Lecture Notes in Computer Science. Springer, 2016.

[11] Marie Vasek and Tyler Moore. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security*, volume 8975 of *Lecture Notes in Computer Science*, pages 44–61. Springer, January 2015.

[12] Marie Vasek, Micah Thornton, and Tyler Moore. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In *1st Workshop on Bitcoin Research*, volume 8438 of *Lecture Notes in Computer Science*, pages 57–71. Springer, March 2014.