

The Impact of Security Shocks in the Bitcoin Ecosystem: Evidence from Mt. Gox

Amir Feder ¹ **Neil Gandal** ¹ **JT Hamrick** ² Tyler Moore ²

¹Berglas School of Economics, Tel Aviv University

²Tandy School of Computer Science, The University of Tulsa

Workshop on the Economics of Information Security
University of California Berkeley
June 13, 2016

Outline

- 1 Motivation and Background
 - Bitcoin Currency Exchanges
 - Reported Outages
 - Research Contribution
- 2 Data Collection Methodology
 - Data Sources: Transaction Data
 - Data Sources: Events Data
- 3 Regression Model
 - Overview of Approach and Data
 - Regressions using Volume as Dependent Variable
 - Regressions using Skewness and Kurtosis as Dependent Variable

Outline

1 Motivation and Background

- Bitcoin Currency Exchanges
- Reported Outages
- Research Contribution

2 Data Collection Methodology

- Data Sources: Transaction Data
- Data Sources: Events Data

3 Regression Model

- Overview of Approach and Data
- Regressions using Volume as Dependent Variable
- Regressions using Skewness and Kurtosis as Dependent Variable

Mt. Gox

← → ↻ 🏠 🔒 K.K. Tibanne [JP] https://mtgox.com 🔍 ⭐ ⚙️ 🗨️ 📱

📈 Last price:\$93.30000 High:\$93.80000 Low:\$91.00000 Volume:20525 BTC Weighted Avg:\$92.72940 USD

MT.GOX

👤 Username Password **Login**
or [Sign up](#)

Trade with confidence on the world's largest Bitcoin exchange!

Mt.Gox is the world's most established Bitcoin exchange. You can quickly and securely trade bitcoins with other people around the world with your local currency!

SIGN UP NOW

“As of July 2011, Mt. Gox handles over 80% of all Bitcoin trade”

WIKIPEDIA

Payments made easy.

4 / 31

Bitcoin Currency Exchange Market Share

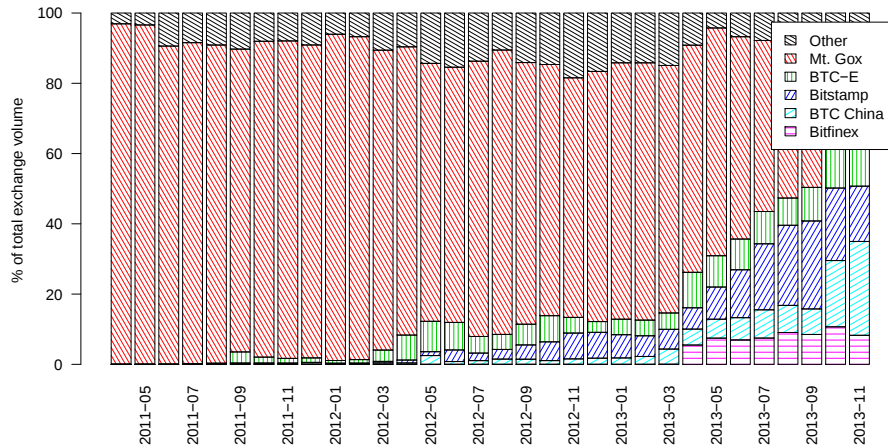


Figure: Distribution of market share among Bitcoin currency exchanges by reported trade volume, April 2011 to November 2013. (Source: bitcoincharts.com)

Reported Outage: Social Media



MtGox.com
@MtGox



Follow

@binarybits @dksdan can confirm we are eating ddos right now, and for some reason Prolexic didn't block it

Reply Retweet Favorite More

16

RETWEETS

4

FAVORITES



5:36 PM - 3 Apr 13

Reported Outage: Press Release

FOR IMMEDIATE RELEASE

Statement Regarding Recent DDoS Attacks and Mitigation

Tokyo, Japan, April 24th, 2013 - On the evening of April 21st, from 11:50 PM Tokyo time, Mt. Gox was hit by a strong DDoS (Distributed Denial of Service) attack that caused the site and trading engine to be unavailable for approximately four hours. The source of the attack is under investigation, and we are working with appropriate authorities to identify those responsible. However, the reality is that our primary goal is to stop the attacks and stabilize the exchange.

For the sake of our customers and the Bitcoin community it is important that we clarify the details of the recent attacks on Mt. Gox and what we are doing to combat them. As the operator of the largest Bitcoin exchange we have the responsibility to maintain the security of our customers' accounts, strengthen our infrastructure appropriately, and help maintain confidence in the growing Bitcoin market as a whole.

How we are being attacked:

What we are experiencing lately are "Layer 7" DDoS attacks. Unlike your average DDoS (which overloads the servers with traffic to the site as a whole) these are much more creative and harder to detect in that they target specific elements of the site and make it difficult to distinguish malicious traffic from normal traffic. The attackers' goal is to shut down the exchange, either through the DDoS itself, or by forcing Mt. Gox to take measures that have the same effect. Attached to this document (See FAQ below) are some details

Reported Outage: News

Search CNET

[Reviews](#)

[News](#)

[Video](#)

[How To](#)

[Deals](#)

US Edition



TOP STORIES



Update at 6:15 a.m. PT Friday: *Bitcoin's tumble continued after trading resumed. As of now, the digital currency is trading at \$69.*

Less than two hours after the resumption of Bitcoin trades following a lengthy suspension, currency exchange Mt. Gox is offline, the apparent victim of a distributed-denial-of-service attack.



Satoshi

"We are experiencing a stronger than usual DDoS," the Tokyo-based exchange said tonight in a **Google+** post. "We are working in it."

Mt. Gox, which handles three-quarters of the trades in the digital currency, announced a suspension of trading this morning after a rollercoaster trading day yesterday that saw Bitcoin's valuation drop 61 percent before recovering a bit with a 37 percent loss. The decentralized digital currency, which had quadrupled in value in the past four weeks, traded as high as \$266 per Bitcoin yesterday before a dramatic correction trimmed its value to \$105. It eventually recovered to trade as high as \$145 a Bitcoin.

Reported Outage: Discussion Forum

my subreddits - dashboard - front - all - random - edit | add shortcuts from the my subreddits menu at left or click the button by the subreddit name, drag and drop to sort



r/bitcoin

comments

view images (1)



This is an archived post. You won't be able to vote or comment.



I think Mt Gox is being ddos'ed right now. But they're holding! (i.imgur.com)

submitted 3 years ago by joshiwashy 9 comments source share hide all child comments

all 9 comments -

subscribe

sorted by: **best** ▼

navigate by: submitter | moderator | friend | me | admin | highlighted | gilded | IAmA | images | videos | popular | new

[-] **[deleted]** 6 points 3 years ago

⬇ We don't need threads like this. We just need threads to inform us when mtgox is *not* being ddosed.

permalink source embed save save-RES

⬆ [-] **joshiwashy** [S] 1 point 3 years ago

⬇ All the 0.0400 buy and sell orders.

permalink source embed save save-RES give gold

⬆ [-] **Juddle-Pumper** 1 point 3 years ago

⬇ Someone is putting in alot of small orders causing lag it looks like.

permalink source embed save save-RES give gold hide child comments

⬆ [-] **[deleted]** 1 point 3 years ago

Research Motivation

- We investigate how distributed denial-of-service (DDoS) attacks and other shocks affect the Bitcoin ecosystem
- Our focus: the Mt.Gox exchange
 - Mt. Gox was the largest currency exchange during Bitcoin's rise
 - Prior research (Vasek et al. 2014) has shown that Mt. Gox was targeted far more than other Bitcoin services
 - DDoS attacks may be financially lucrative to perpetrators, not only disruptive
 - After Mt. Gox collapsed, a dump of millions of transactions was publicly disclosed

Outline

- 1 Motivation and Background
 - Bitcoin Currency Exchanges
 - Reported Outages
 - Research Contribution
- 2 Data Collection Methodology
 - Data Sources: Transaction Data
 - Data Sources: Events Data
- 3 Regression Model
 - Overview of Approach and Data
 - Regressions using Volume as Dependent Variable
 - Regressions using Skewness and Kurtosis as Dependent Variable

Data Source: Leaked Transaction Data

[News](#) [Video](#) [Events](#) [CrunchBase](#)**DISRUPT SF** Shervin Pishevar, Founder Of Hyperloop One, To Speak At Disrupt SF This September **Save \$1200 On Tickets Today** ▶

btc

Bitcoin

mt.gox

Mt.Gox Hack Allegedly Reveals Bitcoin Balances, Customer Account Totals

Posted Mar 9, 2014 by [John Biggs \(@johnbiggs\)](#)



SHARES



Next Story ▶

Anonymous hackers have [defaced Mt.Gox CEO Mark Karpeles' blog](#) and have uploaded a data dump of customer data that, according to users with accounts on the site, is accurate. A Reddit user created an Excel spreadsheet [\[mirror\]](#) of anonymized user accounts with balances, and many current [Mt.Gox](#) users have found their balances present.

The text of the post reads [NSFW]:

*** SAVE THIS POST, MIRROR THE FILES, REPOST, SHARE AND KEEP THIS DATA AVAILABLE ***

Data Source: Transaction Data

Main Transaction Data:

- Publicly leaked user level transaction data
 - 8.9 million buy, 8.9 million sell between 4/2011 and 11/2013
 - 126098 unique users

Data Attributes:

- transaction time
- user identifier
- currency converting to or from bitcoin
- transaction amount
- exchange rate

Events: D1

D1 Events: Reported DDoS attacks

- Bitcointalk.org
 - 34 reports between 2/11 and 10/13
- /r/bitcoin reddit forum
 - 8 reports between 4/13 and 11/13
- Public announcements
 - 9 reports

D1 Results:

- 51 total events on 37 days between 2/2011 and 11/2013

Events: D2/D3

D2 Event: Additional security shocks

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

Additional shocks, other than DDoS, affecting Mt. Gox.

D3 Events: Confirmed DDoS attacks

- Mt. Gox acknowledged outages
 - 9 events

Outline

- 1 Motivation and Background
 - Bitcoin Currency Exchanges
 - Reported Outages
 - Research Contribution
- 2 Data Collection Methodology
 - Data Sources: Transaction Data
 - Data Sources: Events Data
- 3 Regression Model
 - Overview of Approach and Data
 - Regressions using Volume as Dependent Variable
 - Regressions using Skewness and Kurtosis as Dependent Variable

Hypotheses + Results

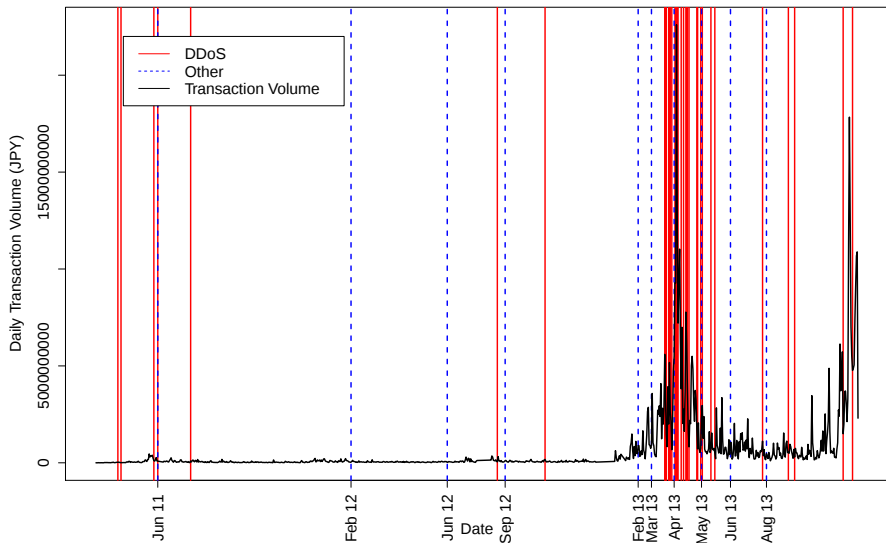
Hypotheses:

- Different users have different information
- DDos attacks should lead to less trade among large users
- Other events may also lead to less trading, but these are probably less important

Results:

- 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.

DDoS and Other Shocks Over Time



The Data - User Activity

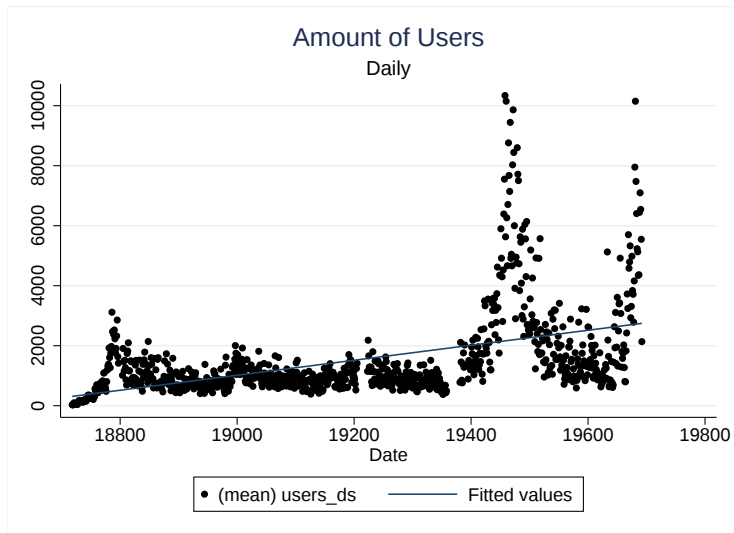


Figure: Sum of unique users per day with the trend

The Data - Daily Volume

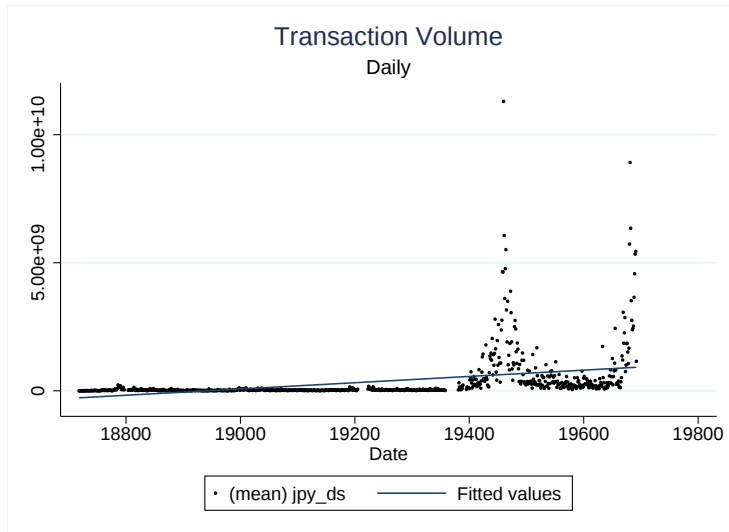


Figure: Sum of sell commands per day with the trend

The Data - Skewness Hypothesis

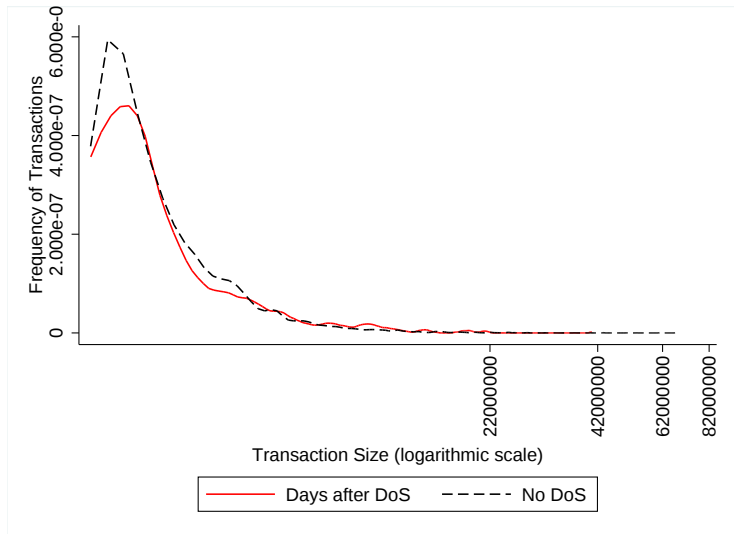


Figure: Distribution of transactions by amount in JPY on days following a DoS attack (solid red line) and on days following a DoS attack (dashed black line).

Regressions using Volume as Dependent Variable

$$TransactionVolume_t = \beta_0 + \beta_1 D1_{t-1} + \beta_2 D2_{t-1} + \beta_3 Time_t + \epsilon_t \quad (1)$$

$$Max.Transaction_t = \beta_0 + \beta_1 D1_{t-1} + \beta_2 D2_{t-1} + \beta_3 Time_t + \epsilon_t \quad (2)$$

$$LargeTransactions_t = \beta_0 + \beta_1 D1_{t-1} + \beta_2 D2_{t-1} + \beta_3 Time_t + \epsilon_t \quad (3)$$

- Likely biased since changes in volume may cause DDos attack

Results using Volume as Dependent Variable

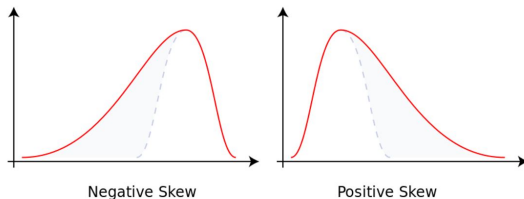
VARIABLES	(1) Transaction Volume	(2) Max. Transaction	(3) Large Transactions
D1	-2.826e+07 (1.306e+08)	-700,953 (1.265e+06)	-104.6 (277.3)
D2	1.588e+08 (1.963e+08)	1.559e+06 (1.901e+06)	311.4 (416.8)
Time	1.053e+06*** (76,263)	13,140*** (738.5)	2.246*** (0.162)
Constant	-2.334e+08*** (4.064e+07)	-2.215e+06***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

Standard errors in parentheses

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

Solving Endogeneity Problem: Using Skewness and Kurtosis

- Skewness - The asymmetry of the probability distribution of a real-valued random variable about its mean



- Kurtosis - The "tailedness" of the probability distribution of a real-valued random variable

$$Kurt[X] = \frac{\mu_4}{\sigma_4} = \frac{E[(X - \mu)^4]}{(E[(X - \mu)^2])^2} \quad (4)$$

Advantages of using Skewness and Kurtosis

- 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.
- Skewness and kurtosis captures the very essence of the hypothesis
 - DDoS attacks might affect different types of trades (large and small) in different ways.
- There is no Endogeneity
 - Changes in kurtosis and skewness are not likely to lead to an increased likelihood of a DDoS attack.

Daily Skewness

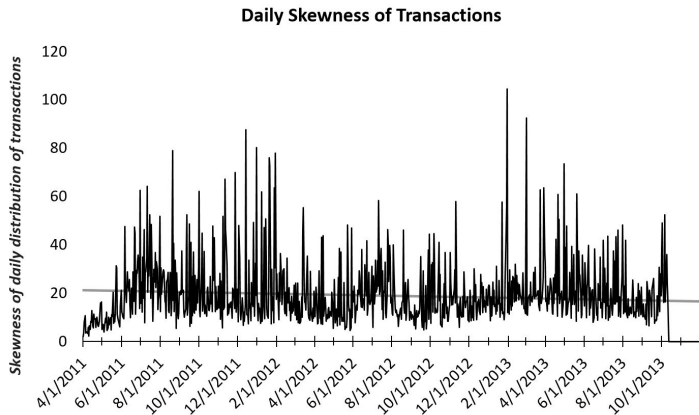


Figure: Daily Skewness of the distribution of transactions and the (insignificant) time trend

Daily Skewness

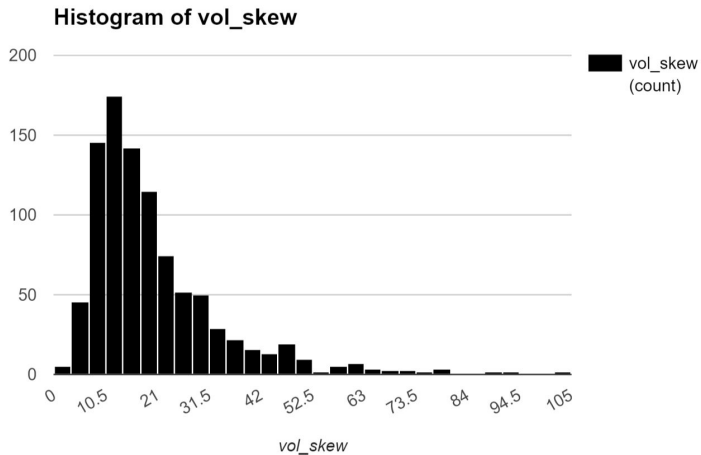


Figure: Distribution of Daily Skewness

Regression Equations

$$\ln(skew)_t = \beta_0 + \beta_1 DoS_{t-1} + \beta_2 D2_{t-1} + \beta_3 \ln(Vol)_t + \beta_4 Users_t + \beta_5 Time_t + \epsilon_t \quad (5)$$

$$\ln(kurt)_t = \beta_0 + \beta_1 DoS_{t-1} + \beta_2 D2_{t-1} + \beta_3 \ln(Vol)_t + \beta_4 Users_t + \beta_5 Time_t + \epsilon_t \quad (6)$$

Results

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

Standard errors in parentheses

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

Interpretation of Results

- DDos attacks lead to 28 percent reduction in skewness
- DDos attacks lead to 56 percent reduction in kurtosis
- Other events have no (statistically significant) effect on kurtosis and skewness
- Results very robust

Conclusions and Future Work

- First econometric study measuring the impact of DDoS attacks on Bitcoin currency exchanges.
- On days following DDoS attacks, the distribution of daily transaction volume shifts so that fewer large transactions take place.
- Future work:
 - Examine the data at the individual level.
 - Examine whether there is evidence of manipulation by profit-motivated cybercriminals who leverage these shocks.