Price Manipulation in the Bitcoin Ecosystem

Neil Gandal[a], JT Hamrick[b], Tyler Moore[b,*], Tali Oberman[a]

[a] *Berglas School of Economics, Tel Aviv University*
[b] *Tandy School of Computer Science, The University of Tulsa*

Abstract

To its proponents, the cryptocurrency Bitcoin offers the potential to disrupt payment systems and traditional currencies. It has also been subject to security breaches and wild price fluctuations. This paper identifies and analyzes the impact of suspicious trading activity on the Mt. Gox Bitcoin currency exchange, in which approximately 600,000 bitcoins (BTC) valued at $188 million were fraudulently acquired. During both periods, the USD-BTC exchange rate rose by an average of four percent on days when suspicious trades took place, compared to a slight decline on days without suspicious activity. Based on rigorous analysis with extensive robustness checks, the paper demonstrates that the suspicious trading activity likely caused the unprecedented spike in the USD-BTC exchange rate in late 2013, when the rate jumped from around $150 to more than $1,000 in two months.

Keywords: Bitcoin, cryptocurrencies, fraud, exchange rate manipulation
JEL classification: E42, E31, E39.

1. Introduction

Bitcoin has experienced a meteoric rise in popularity since its introduction in 2009 (Nakamoto, 2008). While digital currencies were proposed as early as the 1980s, Bitcoin was the first to catch on. The total value of all bitcoins in circulation today is around $28 billion (CoinMarketCap, 2017a), and it has inspired scores of competing cryptocurrencies that follow a similar design. Bitcoin and most other cryptocurrencies do not require a central authority to validate and settle transactions. Instead, these currencies use only cryptography (and an internal incentive system) to control transactions, manage the supply, and prevent fraud. Payments are validated by a decentralized network. Once confirmed, all transactions are stored digitally and recorded in a public "blockchain," which can be thought of as an accounting system.

While bitcoin shows great promise to disrupt existing payment systems through innovations in its technical design, the Bitcoin ecosystem[1] has been a frequent target of attacks by financially-motivated criminals. This paper leverages a unique and very detailed data set to examine suspicious trading activity that occurred over a ten-month period in 2013 on Mt. Gox, the leading Bitcoin currency exchange at the time.[2] The first step is to quantify the extent of the suspicious trading activity and show that it constitutes a large fraction of trading on the days the activity occurred. The next step is to examine whether and how this trading activity impacted Mt. Gox and the broader Bitcoin ecosystem.

Our main results are as follows. Prices rose on approximately 80 percent of the days that the suspicious trading activity occurred. By contrast, prices rose on approximately 55 percent of the days in which no

[*]Corresponding Author.
Email addresses: `gandal@post.tau.ac.il` (Neil Gandal), `jth563@utulsa.edu` (JT Hamrick), `tyler-moore@utulsa.edu` (Tyler Moore), `otalika@yahoo.com` (Tali Oberman)

[1]The Bitcoin ecosystem includes the core network for propagating transactions, the blockchain, and many intermediaries such as currency exchanges, mining pools and payment processors that facilitate trade. This paper uses "Bitcoin" with a capital "B" to refer to the ecosystem and "bitcoin " with a small "b" or BTC to refer to the coin.

[2]See Appendix A for the market share of the cryptocurrency exchanges.

Please cite the article as: Neil Gandal, JT Hamrick, Tyler Moore, Tali Oberman, Price Manipulation in the Bitcoin Ecosystem, *Journal of Monetary Economics* (2017), DOI: 10.1016/j.jmoneco.2017.12.004

suspicious trading activity occurred. Further, during days with suspicious trades, on average, the USD/BTC exchange rate increased by approximately four to five percent a day. During the same period when no suspicious trades occurred, on average the exchange rate was flat to slightly decreasing. Trading volume increased substantially on days with suspicious trading activity, over and above the suspicious activity.

Rising exchange rates and increased trading volume occurred both (I) on the Mt. Gox exchange where the suspicious trades took place and (II) on the other leading currency exchanges on the days the suspicious activity took place. The price rises on all exchanges were virtually identical, which makes sense given the ability of traders to engage in arbitrage across exchanges.

The suspicious trading activity of a single actor was the likely cause of the massive spike in the USD/BTC exchange rate in which the rate rose from around $150tooover1,000$ in just two months in late 2013. The fall was nearly as precipitous: the Mt. Gox exchange folded due to insolvency in early 2014 and it has taken more than three years for bitcoin to match this rise.

1.1. Why Does Bitcoin Manipulation Matter?

As this paper will show, the first time Bitcoin reached an exchange rate of more than $1,000, the rise was likely driven by manipulation. It took more than three years for these exchange rates to be reached again, and we are left to wonder whether the current spike was driven by legitimate interest or by something more nefarious. But, why should anyone care about possible price manipulation in bitcoin during 2013? After all, the Bitcoin ecosystem is not nearly as important as the New York Stock Exchange. Nonetheless, recent trends indicate that bitcoin is becoming an important online currency and payment system.

Additionally, the total market capitalization cryptocurrency assets has grown stunningly since the end of the period covered by our analysis. In January 2014, the market capitalization of all cryptocurrencies was approximately $14 Billion. As of September 2017, total market capitalization is approximately $145 Billion. That is a ten-fold increase.

In the case of bitcoin, during the one year period ending in mid-May 2017, the market capitalization increased massively, from around 7 Billion USD to 28 Billion USD (CoinMarketCap, 2017a). That is an increase of approximately 300 percent in one year. The market cap of other cryptocurrencies surged by even more. In the one year period ending in mid-May 2017, the market value of cryptocurrencies excluding bitcoin surged by more than 1,900 percent (CoinMarketCap, 2017b). Hence, cryptocurrencies are becoming more important. So it is important to understand how the Bitcoin ecosystem works or does not.

Further, despite the huge increase in market capitalization, similar to the bitcoin market in 2013 (the period examined), markets for these other cryptocurrencies are very thin. The number of cryptocurrencies has increased from approximately 80 during the period examined to 843 today! Many of these markets are thin and subject to price manipulation.

As mainstream finance invests in cryptocurrency assets and as countries take steps toward legalizing bitcoin as a payment system (as Japan did in April 2017), it is important to understand how susceptible cryptocurrency markets are to manipulation. Our study provides a first examination.

In terms of the macro-economic lessons, cryptocurrency manipulations tie in to a concern in trading in unregulated financial exchanges. The potential for manipulation in the Over-the-Counter (OTC) markets is a significant concern for financial regulators. OTC trading is conducted directly between two parties, without going through a stock exchange. In a recent white paper, the SEC noted that "OTC stocks are also frequent targets of market manipulation by fraudsters."[3] The SEC report also documents that OTC trading has increased significantly over time.[4]

For all of these reasons, it is important to understand how the Bitcoin ecosystem works and how it could be abused. This paper takes an initial step in that direction by quantifying the impact of one prominent manipulation.

[3] Outcomes of Investing in OTC Stocks, by Joshua White, December 16, 2016, U.S. Securities and Exchange Commission Division of Economic and Risk Analysis (DERA).

[4] In 2008 around 16 percent of U.S. stock trades were of the OTC type. By 2014, OTC trades accounted for forty percent of all stock trades in the US. Like cryptocurrency trading, OTC trades are not transparent and not regulated, and there is concern that such trading is more harmful than high-frequency trading via regulated exchanges (McCrank, 2014).

1.2. Road Map

The paper proceeds as follows. Section 2 discusses background and related work. Section 3 explains our methodology for identifying the STA and details evidence for why these transactions are deemed suspicious. Sections 4 and 5 examine the data in detail, present the findings and show that the results are robust. Section 6 documents the potential for fraudulent trading in the cryptocurrency market today, while Section 7 concludes with further discussion.

2. Background and Related Work

Cryptocurrencies and associated markets represent a nascent but growing force within the financial sector. Bitcoin, which became the first popular decentralized cryptocurrency in 2009, is the most researched because it is the most successful of the digital currencies. Within the finance literature, there is growing interest in discovering what drives a "value-less" currency. Li and Wang (2016) investigate the bitcoin exchange rate in an effort to expand our understanding of the motivation behind the rise and fall of cryptocurrency values. Bolt and van Oordt (2016) build a theoretical model to examine the exchange rate of virtual currencies. Additionally, Hayes (2016) constructs a model for determining the value of a bitcoin-like cryptocurrency by calculating its cost of production. Rajcaniova and d'Artis Kancs (2016) concluded that investor attractiveness has had a significant impact on Bitcoin's price.[5] While the potential for manipulation to influence valuations is sometimes acknowledged, none of these papers considered how unauthorized trades could affect valuations.

Unregulated cryptocurrency exchanges, such as Mt. Gox, are an essential part of the Bitcoin ecosystem. For most users, it is through currency exchanges that bitcoins are first acquired. As exhibited by the rise and fall of Mt. Gox, no cryptocurrency exchange is too big to fail. As reported by Moore and Christin (2013), by early 2013, 45% of Bitcoin exchanges had closed, and many of the remaining markets were subject to frequent outages and security breaches. Vasek and Moore (2015) performed an in-depth investigation of denial-of-service attacks against cryptocurrency exchanges and other Bitcoin services, documenting 58 such attacks. Feder et al. (2016) conducted the first econometric study of the impact of denial-of-service attacks on trading activity at Bitcoin exchanges, leveraging Vasek et al.'s data on attacks. They show that trading volume becomes less skewed (fewer large trades) the day after denial-of-service attacks targeted the Mt. Gox exchange. The same data are used here to identify unauthorized trading and examine the effects of such trading on the Bitcoin ecosystem.

Due to their relatively lawless nature, cryptocurrencies are under constant threat of attack. Numerous researchers have conducted studies in order to document and combat threats such as Ponzi schemes (Vasek and Moore, 2015), money laundering (Möser et al., 2013), mining botnets (Huang et al., 2014), and the theft of "brain" wallets (Vasek et al., 2016). Ron and Shamir (2013) attempt to identify suspicious trading activity by building a graph of Bitcoin transactions found in the public ledger. Meiklejohn et al. (2013) examine the blockchain to determine whether bitcoin transactions are are truly anonymous. They successfully link transactions back to popular Bitcoin service providers, such as currency exchanges. None of these papers can associate individual transactions with specific users at currency exchanges. Our data includes the user ID. Hence, we can associate trades with particular users.

For a more complete review of the literature, see Bonneau et al. (2015) for coverage of technical issues and Böhme et al. (2015) for a discussion of Bitcoin's design, risks and open challenges.

2.1. Related Work on Price Manipulation

The academic literature on price manipulations of stocks includes Aggarwal and Wu (2006); they examined U.S. Securities and Exchange Commission litigation against market manipulators in OTC markets. They find small, illiquid stocks are subject to manipulation and that stock prices, volume, and volatility increase during the alleged manipulation period, but end quickly once the scheme is over. They note "while

[5] Gandal and Halaburda (2016) examine competition among cryptocurrencies. They find that the data are consistent with strong network effects and winner-take-all dynamics.

manipulative activities seem to have declined on the main exchanges, it is still a serious issue in the over-the-counter (OTC) market in the United States." Many of the more than 800 cryptocurrencies available today are illiquid and are characterized by very low volumes on most days and volume and price spikes. Massoud et al. (2016) studied OTC companies that hire promoters to engage in secret stock promotions to increase their stock price and trading volume. They find that the "promotions" coincide with trading by insiders. Brüggemann et al. (2013) show that OTC stocks have lower levels of liquidity than a matched sample of similar NASDAQ-listed stocks.

3. Identifying Suspicious Trading Activity on Mt. Gox

3.1. Exchange Activity

In early 2014, in the midst of theft allegations, the Mt. Gox transaction history was leaked. The Mt. Gox data dump gave access to approximately 18 million matching buy and sell transactions which span April 2011 to November 2013. These data are much more finely grained than data one could obtain from the blockchain or public APIs for two reasons. First, a majority of the trading activity is recorded only by the exchange. Second, the exchange links transactions by the user account.

Data from the dump include fields such as transaction ID, amount, time, currency, and user country and state codes. Also included is the user ID, which is the internal number associated with Mt. Gox users. The user ID is crucial as it enables us to link transactions by the same actor.

The Mt. Gox data were supplemented with publicly available daily aggregate values from `bitcoincharts.com`. This data was used to verify trading volumes, to compare Mt. Gox exchange rates to other leading platforms, and to verify daily USD to BTC exchange rates. A detailed discussion of how the dataset was built is in Appendix B.

3.2. Suspicious Trading Activity

In early 2014, after the Mt. Gox data leak, several individuals trading on Mt. Gox found what they considered "suspicious activity" and wrote extensively about it (Anonymous, 2014a,c). We conducted our own analysis of the data, confirming much of what was reported on the blogs.[6] In Appendix B, the discussion shows why this trading activity should be deemed suspicious, along with a description of the behavior. The appendix carefully goes through the details that confirmed that the relevant transactions were suspicious. What follows here is a brief description of the trading activity and what effect it had on the markets. The rest of the paper uses the names given by the blogs to the suspicious traders: (1) the"Markus bot" and (2) the "Willy bot".

3.2.1. Suspicious Trader 1: the Markus Bot

Markus began "buying" bitcoin on 2013-02-14 and was active until 2013-09-27. His account was fraudulently credited with claimed bitcoins that almost certainly were not backed by real coins. Furthermore, because transactions were duplicated, no legitimate Mt. Gox customer received the currency Markus supposedly paid to acquire these claimed coins. On 33 of the 225 days the account was active, Markus acquired 335,898 bitcoins (worth around $76 million).

3.2.2. Suspicious Trader 2: The Willy Bot

Unlike Markus, Willy did not use a single ID; instead, it was a collection of 49 separate accounts that each rapidly bought exactly 2.5 million USD in sequential order and never sold the acquired bitcoin. The first Willy account became active on 2013-09-27, a mere 7 hours and 25 minutes after Markus became permanently inactive, and one can track Willy activity until the data cutoff on 2013-11-30. Each account proceeded to spend exactly 2.5 million USD before becoming inactive. Then the next account would become active and the process would repeat. Unlike Markus, it appears that Willy was interacting with real users.

[6] Online commentary about these trades frequently refer to the traders as 'bots' (e.g., (Anonymous, 2014a,c)).

While accounts of these users were "nominally" credited with fiat currency, Willy likely did not pay for the bitcoins.

Willy traded on 50 of the 65 days before the data cutoff. In total, Willy acquired 268,132 bitcoin, nominally for around $112 million. While Willy acquired slightly fewer bitcoins than Markus, the Markus activity occurred on 33 days spread over a 225-day period. Thus, the Willy activity was much more intense. Together, the bots acquired around 600,000 bitcoins by November 2013.

Recently, in a trial in Japan, the Former Mt. Gox, CEO Mark Karpeles, confirmed that the exchange itself operated the "Willy" accounts and that the trades were issued automatically (Suberg, 2017).[7]

What motivated the operation of these bots?. The publicly reported trading volume at Mt. Gox included the fraudulent transactions, thereby signaling to the market that heavy trading activity was taking place. Indeed, the paper later shows that even if the fraudulent activity is set aside, average trading volume on all major exchanges trading bitcoins and USD was much higher on days the bots were active. The associated increase in "non-bot" trading was, of course, profitable for Mt. Gox, since it collected transaction fees.

But the Willy Bot likely served another purpose as well. A theory, initially espoused in a Reddit post shortly after Mt. Gox's collapse (Anonymous, 2014b), is that hackers stole a huge number (approximately 650,000) of bitcoins from Mt. Gox in June 2011 and that the exchange owner Mark Karpales took extraordinary steps to cover up the loss for several years.[8]

Note that Bitcoin currency exchanges function in many ways like banks. Customers buy and sell bitcoins, but typically maintain balances of both fiat currencies and bitcoins on the exchange without retaining direct access to the currency. If Mt. Gox was trying to hide the absence of a huge number of BTC from its coffers, it could succeed so long as customers remained confident in the exchange. By offering to buy large numbers of bitcoins, Willy could prop up the trading volume at Mt. Gox and "convert" consumer "bitcoin" balances to fiat money. This could work, i.e., stave off collapse of the exchange, as long as users who sold bitcoin had enough confidence to leave the bulk of their fiat balance at Mt. Gox. If consumers wanted to take out bitcoins, Mt. Gox would immediately have to supply them. On the other hand, if consumers wanted to redeem the fiat cash in their accounts, Mt. Gox could delay the withdrawal by saying that their bank was placing limits on how much fiat cash Mt. Gox could withdraw in a particular period. This indeed happened, and some (but not all) consumers could not withdraw cash from their fiat accounts during the last couple of months before Mt. Gox shut down. By using this strategy, the Willy bot could turn the Mt. Gox' "bitcoin deficit" into a fiat currency deficit. This may have delayed the inevitable crash of Mt. Gox. Although this cannot work in the long-term, Bernie Madoff, a once respected stockbroker, kept a similar scheme running for many years.

4. Impact of Suspicious Purchases: Preliminary Analysis

[Figure 1 about here.]

Figure 1 shows that the USD/BTC exchange rate increased dramatically during the period Willy was active. We are, of course, not the first to notice that. But that in itself does not mean that Willy's activity *caused* the price rise. In this section and the next, compelling evidence is presented that the fraudulent activity likely *caused* the price rise. The next two subsections examine the impact on trading volume and then prices.

[Table 1 about here.]

[7] It also appears that Karpeles operated the Markus Bot as well, and this is where most of the prosecutor's evidence against Karpales has focused.

[8] When Mt. Gox folded, it initially announced that around 850,000 bitcoins belonging to customers and the company were missing and likely stolen. Shortly thereafter, Mt. Gox found an additional 200,000 bitcoins. Hence, the total loss was 650,000 bitcoins.

4.1. Suspicious Purchases and Trade Volume

On the days they were active, Markus and Willy purchased large amounts of bitcoins. As Table 1 shows, Markus purchased on average $9,302$ BTC, which accounted for approximately 21 percent of Mt.Gox's daily volume of trades. On the days Willy was active, he purchased on average $4,962$ BTC, which accounted for 18 percent of Mt. Gox's daily volume of trades. Figure 2 gives a more detailed breakdown. It shows the fraction of daily BTC traded on the Mt. Gox exchange platform that were carried out by Markus and Willy, respectively.

The share of total trading volume remains significant, even taking into account trades on other platforms. Markus accounted for 12 percent and Willy 6 percent of the total trade on the four main exchanges trading bitcoin and USD on the days they were active. In addition to Mt. Gox, the other main exchanges trading USD/BTC during this time period were Bitstamp, Bitfinex and BTC-e. These exchanges accounted for more than 80 percent of the trading activity in BTC/USD during the period studied.

[Figure 2 about here.]

[Table 2 about here.]

The data are divided into four equal three-month periods, starting from December 1, 2012 (2.5 months before Markus was active) and ending when the leaked Mt.Gox dataset ends at the end of November 2013. The bulk of Markus's trades occur in period 3, while all of Willy's take place in period 4.

The increase in total trading volume cannot be accounted for by the rogue trades alone. Both Markus' Willy's activity were associated with much higher trading volume above and beyond their own contributions. On the days these actors were purchasing bitcoins, total volume on Mt. Gox and the other leading exchanges was significantly higher than on days when these bots were not active. Table 2 shows that during the 50 days Willy was active in period 4, he "purchased" approximately 3,900 bitcoins per day on Mt. Gox. Total median daily volume on Mt. Gox during these 50 days was approximately 26,000 bitcoins. During the 41 days that Willy was not active in the period, median daily volume on Mt. Gox was approximately 10,500 bitcoins. The differences in volume are similar across the other three platforms as well. Median total volume on the four exchanges was approximately 83,000 bitcoins on days Willy was active versus approximately 29,500 on days Willy was not active.

The same holds true for days that Markus was active in period 3. On the days that Markus was active during period 3 he "purchased" approximately 8,900 bitcoins per day on Mt.Gox. The total median daily volume on Mt.Gox on the days he was active in this period was 42,000 bitcoins, but only 17,400 bitcoins on the days he was not. The differences in volume are similar across the other three platforms as well. Median total volume on the four exchanges was approximately 68,000 bitcoins on days Markus was active in period 3 versus approximately 31,000 on days Markus was not active in period three. (See Table 2.) For a full breakdown of volumes on individual exchanges, see the tables in Appendix C.

Hence, although these bots differed in their method of operation, days in which either was active were associated with very high volume beyond the bots' direct contributions. It is likely their activity sent a signal to the market and encouraged others to enter and purchase bitcoins. This may be one of the reasons why their activity could have such a large effect on the bitcoin price. The next section conducts a preliminary examination of their effect on prices.

4.2. Suspicious Purchases and Price Changes: Preliminary Analysis

One would expect an association between the suspicious purchases and a rise in prices on Mt. Gox (and other exchanges as well.) This is because an upward shift in demand should lead to a rise in price. Although the activity took place exclusively on Mt. Gox, it is also important to examine how it affected the other exchanges in the Bitcoin ecosystem.

On the days that there was suspicious trading activity on Mt. Gox, the descriptive evidence suggests that prices also tended to rise. The lines in the Figure 2 are colored green if the exchange rate rose and red if the exchange rate fell. Next, it is examined whether the price changes differed on the days in which the fraudulent activity occurred. This was done first for the 9.5 months Markus and Willy were active (and for which data are available) and observed how often the exchange rate rose on Mt. Gox, as indicated in Table 3. One can see that on days without suspicious activity, 55% of the time the exchange rate did in fact rise. But on the 82 days that there was suspicious purchasing activity, 79% of the time the exchange rate rose. According to a chi-squared test of proportions, it is unlikely that this difference was due to randomness ($p < 0.05$). This is preliminary evidence that this activity was associated with the price rise on Mt. Gox.

[Table 3 about here.]

Not surprisingly, similar patterns of price appreciation took place at other exchanges during this period. As shown in Appendix C, on days without unauthorized activity, the exchange rate on Bitstamp rose 55% of the time. However, on the 82 days that Markus or Willy acquired bitcoins, the exchange rate rose more than 80 percent of the time. This suggests that the suspicious trading on Mt. Gox spilled over to other exchanges. This makes sense because all of these platforms traded the same USD-BTC currency pair.

[Table 4 about here.]

Table 4 shows the percent of days in each period, in which there was suspicious trading activity. Markus was active over 8 months, which span over 4 periods. However, he was primarily active in period 3. Willy on the other hand was active for less than three months and all of the activity occurred in period 4. No data are available on any unauthorized activity from the end of period 4. Mt. Gox shut down shortly thereafter.

[Table 5 about here.]

Table 5 shows how the daily movement in the exchange rate (closing price less opening price) changed, on average, on four main exchange platforms.[9] Since fraudulent activity essentially only occurred in the third and fourth periods, the focus is on these two periods. Periods one and two can be viewed as benchmarks.

In period 3, when Markus' activity peaked, there is not see much change overall in the daily exchange rate. However, looking at the days Markus is active, the average daily price increase is higher. This is true, both on Mt. Gox and on all the other platforms too.

In period 4, the sole period in which Willy was active, there is a big jump in the average daily exchange rate change. Separating the days on which Willy was active from those he was not, reveals a dramatic difference: In the case of Mt. Gox, the average USD/BTC rate increased by $21.85 on the 50 days Willy was active; it actually fell (by $0.88 on average) on days when Willy was not active. The same dramatic difference holds for the other exchanges as well.

Daily return is the typical measure for assessing the performance of assets. Daily returns are defined to be the percentage change in the daily exchange rate, i.e., the closing price less the opening divided by the opening price. Table 5 also shows the daily returns (in parentheses) for the four periods for days that Willy and Markus were active and days that they were not active. The table shows that the average daily returns when Markus was active in period 3 (which was his peak activity period) ranged from 1.9-2.9 percent on all four exchanges. On other days, the average return was slightly negative or all four exchanges.

Similarly, table 5 shows the daily returns (in parentheses) that the average daily returns when Willy was active (period 4) ranged from 4.8-5.0 percent on all four exchanges. On other days, the average return was slightly negative on all four exchanges.

These results are striking and make it very clear that the suspicious purchasing activity could have caused the huge price increases. The average daily returns when Markus was active were somewhat smaller than when Willy was active, but these daily rates of return appear non-trivial as well. In the following section, regressions are run to control for other possible effects on the exchange rate.

[9] There is 24 hour trading, so the closing rate on one day is exactly the same as the opening rate on the following day. Bitfinex has fewer observations as it was not active until April, 2013.

5. Regression Analysis

The analysis in the previous section provides strong evidence that the suspicious activity on Mt. Gox may have affected prices on all exchanges. In this section, regression analysis is used to control for other events (like distributed denial of service (DDoS) attacks) that may have caused the changes in the exchange rate. Regressions are run with the dependent variables being (I) the absolute daily price changes and (II) the daily returns on all four exchanges.

5.1. Daily Price Changes

The following regressions are employed:

$$RateChange_t = \beta_0 + \beta_1 Markus_t + \beta_2 Willy_t + \beta_3 DDoS_t + \beta_4 DayAfterDDoS_t + \beta_5 Other_t + \epsilon_t \quad (1)$$

$$Returns_t = \beta_0 + \beta_1 Markus_t + \beta_2 Willy_t + \beta_3 DDoS_t + \beta_4 DayAfterDDoS_t + \beta_5 Other_t + \epsilon_t \quad (2)$$

Our first dependent variable, *RateChange*, is the daily difference in the exchange rate of BTC, i.e. the daily difference between the closing and opening prices.[10] Our second dependent variable, *Returns*, is the daily difference in the exchange rate of BTC, i.e. the daily difference between the closing and opening prices

The independent variable include *Markus*, which is a dummy variable that takes on the value one on the days Markus is active as a buyer. The dummy variable *Willy* is defined similarly. *DDoS* is a dummy variable that takes on the value one on days a DDoS attack on Mt. Gox occurred. *Day after DDoS* is a dummy variable that takes on the value one on the day after a DDoS attack on Mt. Gox occurred. The variable *Other* (or *OtherAttacks*) is a dummy variable that takes on the value one on days that non DDoS attacks occurred.[11] ϵ_t is a white noise error term.[12] The subscript "t" refers to time. There are a total of 365 observations, except for Bitfinex which was not operating during period period one.

Equations (1) and (2) are reduced-form regressions. That is, we are not estimating demand or supply, but rather the effect of changes in exogenous right-hand-side variables on the endogenous variables (the daily rate change and the daily returns in percentage terms.) But in our case, the coefficients from these reduced form regressions are exactly what one wants to measure. Summary statistics (and all other tables not in the text) appear in Appendix C.

[Table 6 about here.]

The results in Table 6 show that the coefficient representing Willy's activity is positive and significant: hence there is a very strong positive association between activity by Willy and prices on Mt. Gox. This regression confirms the striking results of Section 4. The estimated coefficient on the "dummy" variable for Willy is \$21.65, while the "estimate" in section 4 was \$21.85. This again suggests that the USD/BTC exchange rate rose on Mt. Gox by more than 20 dollars a day on average on the days that Willy was active. The regressions for the other exchanges in the same table shows that price on that exchange also rose by 19-20 dollars a day on average on the days that Willy was active. Again the estimated coefficients are consistent with the "estimates" from the summary statistics in section 4.[13]

[10] Recall that closing prices on day t equal opening prices of day $t+1$ since there is 24 hour trading. The opening/closing price is at 24:00 GMT.

[11] Perhaps because it was the leading exchange during the period of our data, most of the DDoS attacks were on Mt. Gox.

[12] Autocorrelation of errors is checked for by calculating the Durbin Watson (DW) statistic for each regression. The value of DW is not statistically different from two in any of the four cases; this strongly suggests that there is no autocorrelation and a white noise error term is appropriate.

[13] Controlling for other factors, the price change on days when the bots were not active was essentially zero, as the estimates of the constant show.

The estimated coefficient on the dummy variable representing Willy's activity is the only coefficient which is significant. Notably, denial-of-service attacks and other shocks do not appear to influence the exchange rate. While this does not conclusively prove that Willy's activity caused the price rise, it suggests that it was the likely cause of the significant price rise in the price of Bitcoin during this period. The estimated coefficient associated with Markus's activity is positive, but not significant, suggesting that Markus' more diffused activity was not associated with a large rise in the daily change (in levels) of the USD-BTC exchange rate.

[Table 7 about here.]

5.2. Daily Percentage Returns

Typically, in the finance literature, researchers examine daily returns to currencies in percentage terms, that is closing price less opening price divided by opening price. Hence, the same exercise is repeated using daily percentage returns as the dependent variable, and employ the same independent variables as in the previous regressions.[14]

Table 7 shows that activities of the two bots led to similar rates of returns and that these returns were significantly higher than the returns earned during days in which the bots were not active. On days in which the bots were not active, the average rate of return was less than one percent (as the estimates of the constant show.) From the coefficients in Table 7, in the case of Willy, the daily returns across all exchanges were in a fairly tight range, ranging from 4.1 to 4.7 percent more when Willy was active than when he was not active. (On days when the suspicious actors were not active, there was no percentage change in the exchange rate.) All of the "Willy"coefficient estimates are significant at the 99% level of confidence.

In the case of Markus, the estimated coefficients in Table 7 show that the daily returns across the exchanges ranged from 2.7-4.3 percent more than when Markus was not active. The rates are similar to those when Willy was active. With the exception of Bitfinex, the "Markus" coefficient estimates are significant at the 99% level of confidence.[15]

6. Testing for Potential Price Manipulation Today

Aggarwal and Wu (2006) describe one of the cases that involved price manipulation of "penny stocks." In that case, according to the SEC, the defendant placed purchase orders in small blocks at successively rising prices. The SEC alleged that this was part of a manipulative scheme to create the artificial appearance of demand for the securities in question, enabling unidentified sellers to profit and inducing others to buy these stocks based on unexplained increases in the volume and price of the shares."

Intentionally or not, this method resembles the one employed by the Markus and Willy bots. This suggests that one way to examine whether such price manipulation exists is to follow individual trades over time for each cryptocurrency - and see whether a pattern of systematic buying over time has occurred and whether such buying was associated with an increase in price. In order to control for periods of high demand for cryptocurrencies in general, one can compare these buying patterns with trends in bitcoin, the leading cryptocurrency.

[Table 8 about here.]

Researchers can use publicly available data on trading volume and price to raise red flags regarding possible price manipulation. To examine the effects of increased trading volume on the price of cryptocurrencies, publicly available data was gathered from `coinmarketcap.com`. These data provide access to cryptocurrencies tracked by the platform, which is an extensive though incomplete list. The data include daily market

[14] Virtually identical results are obtained using the natural log of returns i.e., the natural log of the closing price divided by the opening price.

[15] In the case of Bitfinex, the estimated coefficient on Markus' activity is 2.7, which is significant at the 10 percent level of confidence. Recall that the Bitfinex exchange was not operating in period one.

cap, trading volume and the open, high, low, and close price in USD for all currencies tracked. Starting from a total of 843 publicly traded currencies and 477,039 daily summaries for those cryptocurrencies, we sought to identify circumstances that might resemble the effects of fraudulent trades found in this paper.

Two criteria were used to pare down the candidates for manipulation. First, coins should have a substantial enough market capitalization to make profits but simultaneously thin enough for fraud to succeed. Second, coins should experience a spike in daily trading volume that might drive returns higher. On the first count, there are 308 currencies which had a maximum market capitalization between $1-100 million. On the second count, a comparison of the daily volume of each cryptocurrency to the average daily volume for that month and computed summary statistics for two overlapping groups. The first group consists of coins whose daily trading volume increased by at least 150% of the average daily trading volume for that month (e.g., the coin's trading volume jumped to $2.5 million from a daily average of $1 million). The second group considers more extreme jumps of at least 200% compared to that month's average trading volume. The reason to seek out these volume spikes is that Section 4.1 observed that the trading volume jumped over 200% on days when the bots were active.

As shown in Table 8, the first group (150%) consists of 19,212 events for 304 unique currencies. On the days when trading volume spiked, the coin's USD exchange rate increased by 26.8% on average (1.5% median.) By contrast, when the volume did not jump, the average price increase was 8.6% (median 0%).

For the second group requiring a 200% jump, the difference is even more stark. On days with volume spikes, the average price increase was 30.5% (median 2%), compared to an average price increase of 8.8% (0% median) on other days. While these jumps in trading volume and prices could certainly have an innocuous explanation, they nonetheless demonstrate the potential for fraud in a very opaque and unregulated market.

7. Concluding Remarks

In this paper, trade data delineated by user were used to conclude that the suspicious trading activity on the Mt. Gox exchange was highly correlated with the rise in the price of Bitcoin during the period studied. If the bot activity was indeed the cause, we have shown that manipulations can have important real effects. The suspicious trading activity of two actors were associated with a daily 4% rise in the price, which in the case of the second actor combined to result in a massive spike in the USD-BTC exchange rate from around $150 to over $1 000 in late 2013. The fall was even more dramatic and rapid, and it has taken more than three years for Bitcoin to match the rise during this period.

Given the recent meteoric rise in bitcoin to levels beyond the peak 2013 (and the huge increase in the prices of other cryptocurrencies), it is important for the exchanges to ensure that there is not fraudulent trading. The potential for manipulation has grown despite the increase in total market capitalization because there has been a very large increase in the number of cryptocurrencies. Currently, there are more than 300 cryptocurrencies with market capitalization between $1 Million and $100 Million. In January 2014, there were less than 30 coins with market capitalization between $1 million and $100 million. Hence, there are many more markets with relatively small market capitalization than there were in 2014. Thus, despite the 10-fold increase in market capitalization, the addition of so many "thin" markets in cryptocurrencies means that price manipulation remains quite feasible today. As shown in the prior section, these thin markets do exhibit sudden spikes in trading volume that drive the exchange rate upwards.

Since the Bitcoin ecosystem is currently unregulated, "self-policing" by the key players and organizations is essential. Further, as the Bitcoin ecosystem becomes more integrated into international finance and payment systems, regulators may want to reassess the policies that leave the ecosystem unregulated and take an active oversight role.

Acknowledgements

We are extremely grateful to the editor, Urban Jermann, and an anonymous referee; their comments and suggestions significantly improved the paper. We gratefully acknowledge support from research grants from the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, US–Israel Binational

Science Foundation Grant No. 2016622, and US National Science Foundation Award No. 1714291. We thank Maarten van Oordt and Nittai Bergman for very helpful and suggestions suggestions that greatly improved the paper. We also thank participants at the Central Bank Research Association conference at the Bank of Canada and the Workshop on the Economics of Information Security (WEIS) 2017 for helpful suggestions and comments.

References

Aggarwal, R. K., Wu, G., 2006. Stock market manipulations. The Journal of Business 79 (4), 1915–1953. URL http://www.jstor.org/stable/10.1086/503652

Anonymous, January 2014a. Free willy! – identifying the gox buy bot. https://www.reddit.com/r/Bitcoin/comments/20k4zc/free_willy_identifying_the_gox_buy_bot/.

Anonymous, March 2014b. Peter Rs theory on the collapse of Mt. Gox. https://www.reddit.com/r/Bitcoin/comments/1zdnop/peter_rs_theory_on_the_collapse_of_mt_gox/.

Anonymous, May 2014c. The Willy Report. https://willyreport.wordpress.com/.

Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives 29 (2), 213–38. URL http://www.aeaweb.org/articles.php?doi=10.1257/jep.29.2.213

Bolt, W., van Oordt, M. R., 2016. On the value of virtual currencies. http://www.bankofcanada.ca/wp-content/uploads/2016/08/swp2016-42.pdf.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., Felten, E. W., 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 104–121.

Brüggemann, U., Kaul, A., Leuz, C., Werner, I. M., 2013. The twilight zone: Otc regulatory regimes and market quality. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2290492

CoinMarketCap, 2017a. Cryptocurrency market capitalizations. https://coinmarketcap.com/currencies/bitcoin/. Last accessed May 16, 2017.

CoinMarketCap, 2017b. Total market capitalization (excluding bitcoin). https://coinmarketcap.com/currencies/bitcoin/. Last accessed May 16, 2017.

Feder, A., Gandal, N., Hamrick, J., Moore, T., 2016. The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. In: 15th Workshop on the Economics of Information Security (WEIS). URL http://tylermoore.ens.utulsa.edu/weis16gox.pdf

Gandal, N., Halaburda, H., 2016. Can we predict the winner in a market with network effects? Games 7 (3), dOI: 10.3390/g7030016.

Hayes, A. S., May 2016. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. Telematics and Informatics. URL http://www.sciencedirect.com/science/article/pii/S0736585315301118

Huang, D. Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., McCoy, D., Savage, S., Weaver, N., Snoeren, A. C., Levchenko, K., 2014. Botcoin: Monetizing stolen cycles. In: Proceedings of the Network and Distributed System Security Symposium.

Li, X., Wang, C. A., December 2016. The technology and economic determinants of cryptocurrency exchange rates: The case of bitcoin. Decision Support Systems. URL http://www.sciencedirect.com/science/article/pii/S0167923616302111

Massoud, N., Ullah, S., Scholnick, B., 2016. Does it help firms to secretly pay for stock promoters? Journal of Financial Stability 26, 45–61.

McCrank, J., apr 2014. Dark markets may be more harmful than high-frequency trading. Reuters Business Newshttp://www.reuters.com/article/us-dark-markets-analysis-idUSBREA3508V20140406.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., Savage, S., 2013. A fistful of Bitcoins: Characterizing payments among men with no names. In: Proceedings of the Internet Measurement Conference. ACM, pp. 127–140.

Moore, T., Christin, N., April 2013. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In: Financial Cryptography and Data Security. Vol. 7859 of Lecture Notes in Computer Science. Springer, pp. 25–33. URL http://tylermoore.ens.utulsa.edu/fc13.pdf

Möser, M., Böhme, R., Breuker, D., 2013. An inquiry into money laundering tools in the Bitcoin ecosystem. In: Proceedings of the Seventh APWG eCrime Researcher's Summit. IEEE, pp. 1–14.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Rajcaniova, P. C. M., d'Artis Kancs, May 2016. The economics of bitcoin price formation. Applied Economics 48, 1799–1815. URL http://www.tandfonline.com/doi/full/10.1080/00036846.2015.1109038

Ron, D., Shamir, A., 2013. Quantitative analysis of the full Bitcoin transaction graph. In: Financial Cryptography and Data Security. Vol. 7859 of Lecture Notes in Computer Science. Springer, pp. 6–24.

Suberg, W., jul 2017. Mt. Gox trial update: Karpeles admits Willy Bot existence. Coin Telegraphhttps://cointelegraph.com/news/mt-gox-trial-update-karpeles-admits-willy-bot-existence.

Vasek, M., Bonneau, J., Castellucci, R., Keith, C., Moore, T., 2016. The Bitcoin brain drain: Examining the use and abuse of Bitcoin brain wallets. In: Grossklags, J., Preneel, B. (Eds.), Financial Cryptography and Data Security. Vol. 9603 of Lecture Notes in Computer Science. Springer, pp. 609–618. URL https://tylermoore.utulsa.edu/fc16.pdf

Vasek, M., Moore, T., January 2015. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In: Böhme, R., Okamoto, T. (Eds.), Financial Cryptography and Data Security. Vol. 8975 of Lecture Notes in Computer Science. Springer, pp. 44–61. URL http://tylermoore.ens.utulsa.edu/fc15.pdf

List of Figures

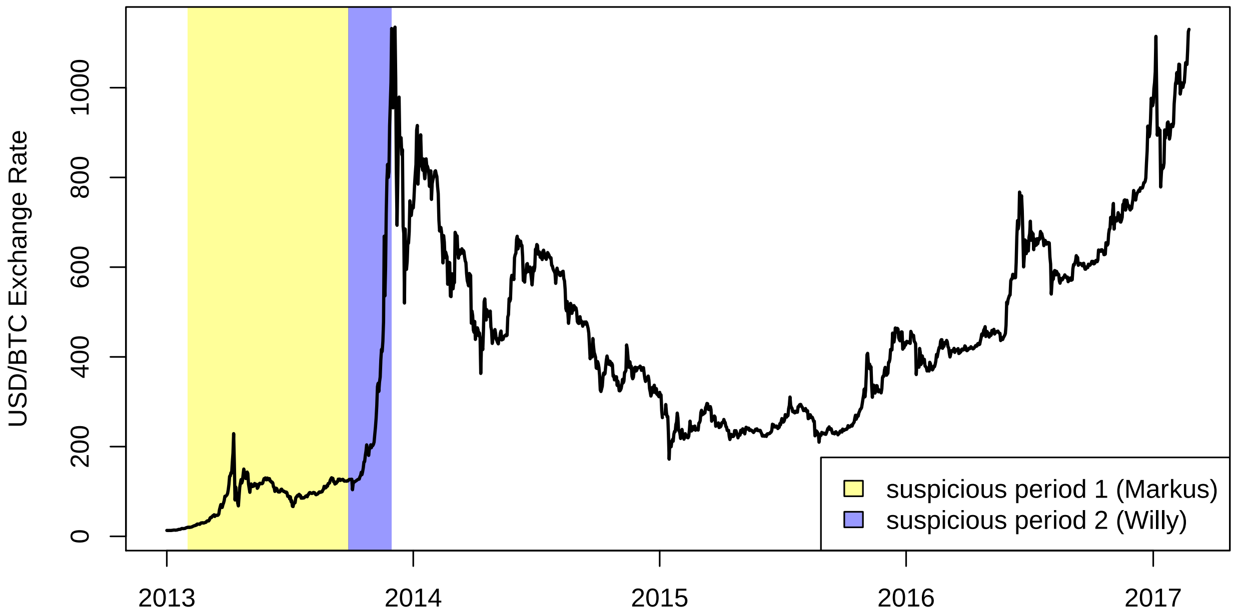

Figure 1: Bitcoin-USD exchange rate with periods of suspicious activity shaded.

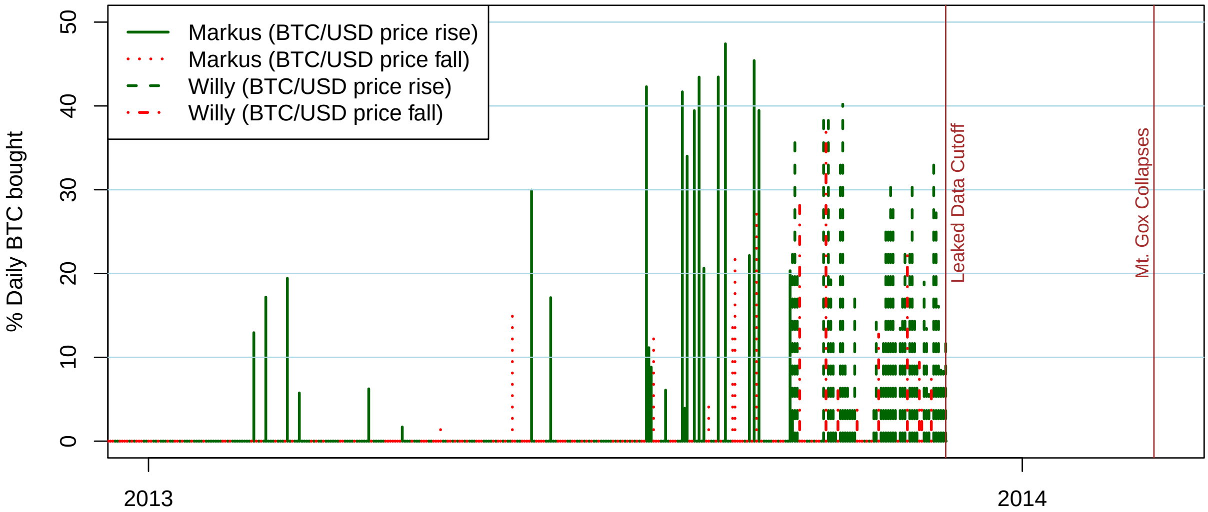

Figure 2: Percentage of total daily trade volume at Mt. Gox when Willy and Markus are active; shaded green if the BTC/USD exchange rate closed higher and red otherwise.

List of Tables

Table 1: Daily BTC purchased by Markus and Willy on days they were active.

	Mean	SD	Median	N
Markus:				
BTC purchased	9,302	7,310	5,874	33
% of Mt.Gox daily trade	21		17	
% of total trade at 4 main exchanges	12		10	
Willy:				
BTC purchased	4,962	4,462	3,881	50
% of Mt.Gox daily trade	18		15	
% of total trade at 4 main exchanges	6		5	

Table 2: Comparison of daily BTC volumes on days when suspicious trades occurred and did not.

				Daily BTC Volume		
Buyer	Period	Bot?	Exchange	Mean	Median	N
Markus	3	Active	Mt. Gox	10,056	8,901	17
Everyone	3	Active	Mt. Gox	39,619	42,022	17
Everyone	3	Inactive	Mt. Gox	27,672	17,421	75
Everyone	3	Active	Overall	63,984	67,691	17
Everyone	3	Inactive	Overall	46,962	31,173	75
Willy	4	Active	Mt. Gox	4,962	3,881	50
Everyone	4	Active	Mt. Gox	30,854	25,939	50
Everyone	4	Inactive	Mt. Gox	17,472	10,444	41
Everyone	4	Active	Overall	90,611	82,779	50
Everyone	4	Inactive	Overall	46,263	29,476	41

Table 3: Unauthorized activity and price changes on Mt. Gox

		Days with no bots		Days with bots	
		Days	%	Days	%
Markus	Daily rate decrease	84	44	7	21
	Daily rate increase	109	56	26	79
Willy	Daily rate decrease	9	60	10	20
	Daily rate increase	6	40	40	80
Total	Daily rate decrease	93	45	17	21
	Daily rate increase	115	55	65	79

Table 4: Suspicious trading activity: % of days active during each period

	Period 1 2012-12-01 – 2013-02-28	Period 2 2013-03-01 – 2013-05-31	Period 3 2013-06-01 – 2013-08-31	Period 4 2013-09-01 – 2013-11-30
Markus	3%	5%	19%	9%
Willy	0	0	0	55%
N	90	92	92	91

Table 5: Average daily rate change (in $) and percentage rate change (in parentheses) in USD-BTC exchange rate by period

	Period 1	Period 2	Period 3			Period 4		
			All	Markus active	Markus not active	All	Willy active	Willy not active
Rate change Mt.Gox	0.21 [1%]	1.00 [1.8%]	0.16 [0.2%]	3.15 [2.9%]	-0.51 [-0.4%]	11.61 [2.6%]	21.85 [5%]	-0.88 [-0.2%]
Rate change Bitstamp	0.23 [1.1%]	1.02 [2.1%]	0.02 [0.1%]	2.35 [2.3%]	-0.51 [-0.4%]	10.99 [2.6%]	20.37 [4.9%]	-0.45 [-0.05%]
Rate change Bitfinex	. .	0.92 [1.3%]	0.04 [0.1%]	2.14 [2.2%]	-0.44 [-0.3%]	10.75 [2.7%]	19.54 [5%]	0.03 [-0.07%]
Rate change BTC-e	0.22 [1%]	1.05 [2.1%]	-0.1 [0.01%]	1.81 [1.9%]	-0.53 [-0.4%]	10.30 [2.6%]	19.22 [4.8%]	-0.58 [-0.07%]
N	90	92	92	17	75	91	50	41

Table 6: Examining Price Changes Within Mt. Gox and the other Exchanges

Independent Variables / Dependent Variable	Mt.Gox Rate Change	Bitstamp Rate Change	Bitfinex Rate Change	BTC-e Rate Change
Markus	2.79	3.24	2.06	2.37
	(0.72)	(0.96)	(0.31)	(0.71)
Willy	21.65***	20.21***	19.23***	19.04***
	(6.66)	(7.18)	(3.63)	(6.81)
DDoS	-2.38	-1.67	-1.87	-2.01
	(-0.55)	(-0.44)	(-0.26)	(-0.54)
Day After DDoS	-3.50	-3.25	-2.9	-2.68
	(-0.80)	(-0.86)	(-0.41)	(-0.72)
Other Attacks	7.16	5.70	7.35	5.61
	(0.82)	(0.75)	(0.44)	(0.75)
Constant	0.37	0.30	0.45	0.32
	(0.28)	(0.26)	(0.17)	(0.28)
N	365	365	244	365
adj. R^2	0.10	0.12	0.037	0.11

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 7: Examining Percent Price Changes Within Mt. Gox and the other platforms

Dependent Variable / Independent Variables	Mt.Gox % Rate Change	Bitstamp % Rate Change	Bitfinex % Rate Change	BTC-e % Rate Change
Markus	0.0371**	0.0434***	0.0272*	0.0348**
	(3.18)	(3.55)	(1.66)	(2.90)
Willy	0.0433***	0.0423***	0.0469***	0.0413***
	(4.45)	(4.14)	(3.54)	(4.12)
DDoS	-0.0182	-0.00758	-0.00391	-0.00903
	(-1.40)	(-0.55)	(-0.22)	(-0.67)
Day After DDoS	-0.0144	-0.0128	-0.0167	-0.0111
	(-1.10)	(-0.94)	(-0.94)	(-0.83)
Other Attacks	0.0374	0.0234	0.0239	0.0235
	(1.43)	(0.85)	(0.57)	(0.87)
Constant	0.0071	0.0065	0.0032	0.0069
	(1.77)	(1.57)	(0.46)	(1.68)
N	365	365	244	365
adj. R^2	0.075	0.064	0.044	0.054

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 8: Prevalence and Impact of Trading Volume Spikes on Prices in Cryptocurrencies Today

	Days			Rate Change	
Volume	#	%	Currencies	Median	Mean
$\geq 150\%$	$19,212$	8%	304 of 308	1.5%	26.8%
$< 150\%$	$220,988$	92%	–	0%	8.6%
$\geq 200\%$	$14,110$	6%	301 of 308	2%	30.5%
$< 200\%$	$226,090$	94%	–	0%	8.8%