Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem

Marie Vasek, Micah Thornton, and Tyler Moore

Computer Science and Engineering Department
Southern Methodist University, Dallas, TX
Email: {mvasek,mathornton,tylerm}@smu.edu

Abstract. We present an empirical investigation into the prevalence and impact of distributed denial-of-service (DDoS) attacks on operators in the Bitcoin economy. To that end, we gather and analyze posts mentioning "DDoS" on the popular Bitcoin forum `bitcointalk.org`. Starting from around 3 000 different posts made between May 2011 and October 2013, we document 142 unique DDoS attacks on 40 Bitcoin services. We find that 7% of all known operators have been attacked, but that currency exchanges, mining pools, gambling operators, eWallets, and financial services are much more likely to be attacked than other services. Not coincidentally, we find currency exchanges and mining pools are much more likely to have DDoS protection such as CloudFlare, Incapsula, or Amazon Cloud. We show that those services that have been attacked are more than three times as likely to buy anti-DDoS services than operators who have not been attacked. We find that big mining pools (those with historical hashrate shares of at least 5%) are much more likely to be DDoSed than small pools. We investigate Mt. Gox as a case study for DDoS attacks on currency exchanges and find a disproportionate amount of DDoS reports made during the large spike in trading volume and exchange rates in spring 2013. We conclude by outlining future opportunities for researching DDoS attacks on Bitcoin.

1 Introduction

Bitcoin [1] is the first cryptocurrency that has been widely adopted. Whereas previously digital currencies sought to be as perfect a substitute for cash as possible (e.g., DigiCash emulated the anonymity of cash with the convenience of electronic payments [2]), Bitcoin has tried to improve on the perceived shortcomings of traditional currencies. For example, Bitcoin offers a money supply with limited growth enforced by its design and without relying on a central bank. This has appealed to inflation hawks and libertarians alike.

Another key reason behind Bitcoin's meteoric rise is how its design creates opportunities for participants to strike it rich. For instance, new cash is introduced into the system by so-called miners, who are paid to solve puzzles that aid in the verification of past transactions. Additionally, the relatively fixed money supply is susceptible to deflation, which helps drive up the exchange rate against

hard currencies and attract the attention of speculators. These opportunities for wealth have also created problems, as those competing for riches sometimes cheat in order to gain an advantage.

Indeed, the Bitcoin ecosystem remains a "Wild West" of sorts. In an environment with scores of unregulated financial products, scammers have set up Ponzi schemes to defraud those holding Bitcoins [3, 4]. Because Bitcoin transactions are non-revocable, hackers have frequently stolen Bitcoins of individuals and companies, leaving the victims without any recourse [5]. Currency exchanges are frequently hit with security breaches to steal coins, prompting the weaker ones to close [6]. Other times exchanges simply shut down without explanation, often with customers losing their "deposits".

Perhaps the most common scourge to afflict Bitcoin participants, however, has been denial-of-service attacks. These are inexpensive to carry out and quite disruptive. Competing services launch them in order to improve market share, traders target exchanges to buy or sell at favorable prices [7], and miners outgunned in the rush to increase computational power could try to cripple larger pools in order to increase their odds of solving the hash puzzle first [8].

Despite their apparent frequency, very little is known about the true prevalence of service-denial attacks on Bitcoin. To that end, we carry out an empirical analysis of reports of such attacks made on the popular `bitcointalk.org` discussion forum. We begin in Section 2 by outlining how we gather reports of DDoS attacks from public sources. We employ a simple rule-based classifier that distinguishes between the discussion of those experiencing attacks from other messages mentioning DDoS attacks.

We present our analysis in Section 3. We identify 142 distinct DDoS attacks taking place between May 2011 and October 2013. We first explain how these attacks vary over time and by category of service affected (e.g., currency exchanges, mining pools, gambling websites). We present evidence that those services that have suffered DDoS attacks are much more likely to now take steps to prevent future DDoS-es. We examine the relationship between a mining pool's size and its susceptibility to attacks, and we look at how attacks relate to the trading volumes and exchange rate at Mt. Gox, the largest currency exchange. We review related work in Section 4, and we discuss opportunities for further research on DDoS attacks with the gathered dataset in Section 5.

2 Methodology

We first set out our approach to data collection in Section 2.1. Then we describe and evaluate our method for identifying posts that report DDoS attacks in Section 2.2. The collected data and analysis scripts are publicly available for replication purposes at `doi:10.7910/DVN/25541`.

2.1 Data Collection

Identifying when a denial-of-service attack has taken place can be difficult. If we knew in advance the websites to monitor, we could run a regular script

that attempts to visit the websites. However, simply because we can connect to a website does not mean that others are being blocked. Furthermore, some services (e.g., mining pools) are not run as websites, so non-standardized means of connecting would be required. Finally, it would be desirable to peer back further into the past to check for historical reports of DDoS attacks.

To that end, we decided to inspect reports of DDoS attacks posted to the popular `bitcointalk.org` forum. Using the Google Custom Search API, we identified all posts including the term "ddos" on the website appearing between February 2011 and October 2013. Because the Google API limits the results to the top 100 results, we issued queries restricted to week-long intervals. In only 3 weeks (during April and May 2013) did the API return the maximum 100 results. In those cases we shortened the time interval further to ensure that we obtained all results including "ddos".

In total, we identified 2 940 distinct pages on `bitcointalk.org` that mentioned "ddos". However, many duplicates existed in these pages, such as when a single thread spans multiple pages. Consequently, we identified 1 355 distinct pages comprised of the first page of the thread. For each page, we then fetched a local copy of the page and automatically extracted the thread title, plus the first post's text, URLs, poster handle and date. We also extracted the forum title. Not all posts actually described DDoS attacks, however. In Section 2.2 we explain how to distinguish between discussion of perceived DDoS attacks and other DDoS-related threads.

We collected additional information to complement the information gathered on DDoS reports. For instance, we fetched a directory of 1 240 online services supporting Bitcoin [9] and 32 mining pools [10]. We extracted category and subcategory information for these services from parsing the directory. We threw out any services that did not resolve after an automatic and manual check.

Subsequently, we identified the use of anti-DDoS providers by resolving the websites of all known Bitcoin services and comparing against known IP ranges for CloudFlare [11], Incapsula [12], and Amazon Web Services [13]. CloudFlare and Incapsula are content distribution networks (CDNs), whereas Amazon hosts material. All three are identifiable by IP range. For services not resolving to these networks, we looked up their AS number using the IP address. We did not find any other content distribution networks serving more than two Bitcoin services. Therefore, we are confident we found all significant network-based anti-DDoS protections. Other forms of protection, such as DDoS detection built in to security appliances, could not be identified and are beyond this paper's scope.

Finally, we identified historical market share of mining pools from 22 Internet Archive snapshots of `http://blockchain.info/pools` dating to October 2011.

2.2 Classification of Posts Describing Attacks

As noted above, many of the posts mentioning "ddos" do not actually describe experiences with denial-of-service attacks. Instead, users discussed ways to defeat DDoS attacks, posted advertisements for services with built-in protections against attacks, and speculated on the motivations behind prior attacks.

We built a simple word-based classifier to identify just those threads describing DDoS attacks currently in progress. Of course, we cannot confirm that what the posters describe is actually a DDoS attack rather than a server overloaded with demand. Nonetheless, user reports do provide a useful indication of when such attacks most likely occur. We flagged all posts with the following words and phrases in the title as DDoS attacks: "unreachable", "offline", "online", "down","flooding","attack","ddos","unavailable","blocking", and "connect". Any posts including the words "anti-ddos" or "vote" in the title were marked as not describing attacks.

	Actual	
	DDoS	Not DDoS
Predicted DDoS	42	36
Predicted Not DDoS	15	114
Precision 54%, Recall 74%, Accuracy 75%		

Table 1: Confusion matrix plus precision, recall and accuracy measures for the word-based classifier.

To evaluate the classifier's accuracy, we compared it against a manually labeled set of 207 posts. The results are given in Table 1. Overall accuracy is 75%. The false negative rate is modest (26%), but false positives are problematic. Thus the classifier does a pretty good job at finding DDoS reports, whereas many posts flagged as DDoS in fact are not.

Consequently, we manually inspected the 362 posts identified by the classifier as describing attacks from the full dataset. We found that 200 posts actually described attacks. We use these posts in the analysis that follows below. Based on the observed recall rates, we expect that there are around 70 more posts describing attacks not included in our analysis. However, we defer improving the classifier further and identifying those posts to future work.

There is one final subtlety in the data collection that bears mentioning. Sometimes multiple posts discuss the same DDoS event. To account for that, we define distinct DDoS attacks as any post mentioning a service on a given day. For instance, if three posts describe an attack on Mt. Gox on April 26, 2013, we count that as a single attack. If however, a single post mentions a DDoS on three different services, we count that as three attacks. Using this approach, the 200 posts correspond to 142 distinct DDoS attacks.

3 Empirical Analysis

We first discuss how DDoS attack targets have changed over time in Section 3.1, along with an examination of which service categories are targeted more and less often. We then study attacks on mining pools in Section 3.3, followed by attacks on currency exchanges in Section 3.3.

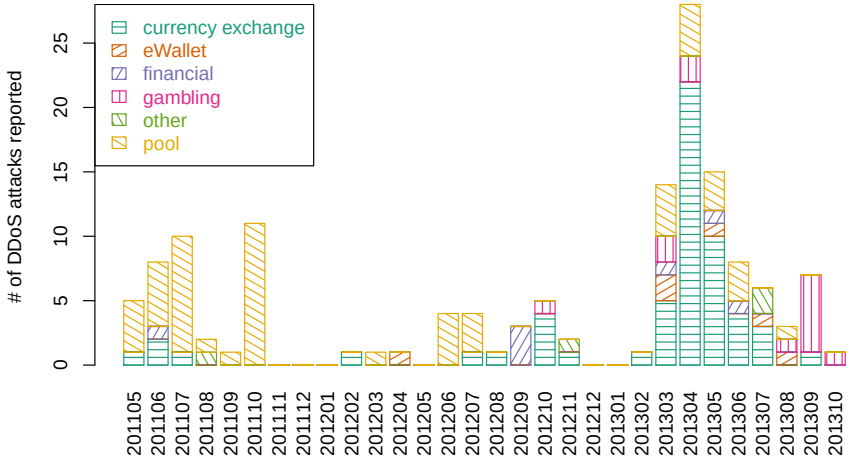

Fig. 1: Reported DDoS attacks over time, split up by category of targeted service.

3.1 DDoS Attacks over Time and by Target

We begin by examining how reports of DDoS attacks on Bitcoin services have evolved over time. Figure 1 plots the number of reported DDoS attacks per month since May 2011. We can see that the number and target of reported attacks varies greatly over time. Initially, in the second half of 2011, most DDoS reports concerned mining pools. Then there were very few reported attacks of any kind during the first half of 2012. During the second half of 2012, DDoS attacks picked up again, initially targeting pools, but more frequently targeting currency exchanges and other websites. During 2013, attacks on pools continued, but they were joined by DDoS on gambling websites, eWallets, and currency exchanges. Attacks on currency exchanges dominated the totals from March–June 2013, coinciding with rising exchange rates and unprecedented interest in Bitcoin. While we expect that some of these reported DDoSes were in fact triggered by customer demand, it is nonetheless interesting to see the rise in reported abuses. Finally, DDoS on exchanges fell sharply in August. However, Bitcoin-based gambling websites experienced a surge of DDoS activity in its place.

Figure 2 (left) shows how DDoS attacks stack up by category over all time. The most targeted service category is currency exchanges (41%), followed closely by mining pools (38%). These were trailed by gambling (9%), finance (5%), and eWallets (4%). DDoS attacks on other services accounted for 3% of the total.

While some services are targeted only once by DDoS attacks, others are repeatedly hit by them. Figure 2 (right) plots a CDF of the number of times a

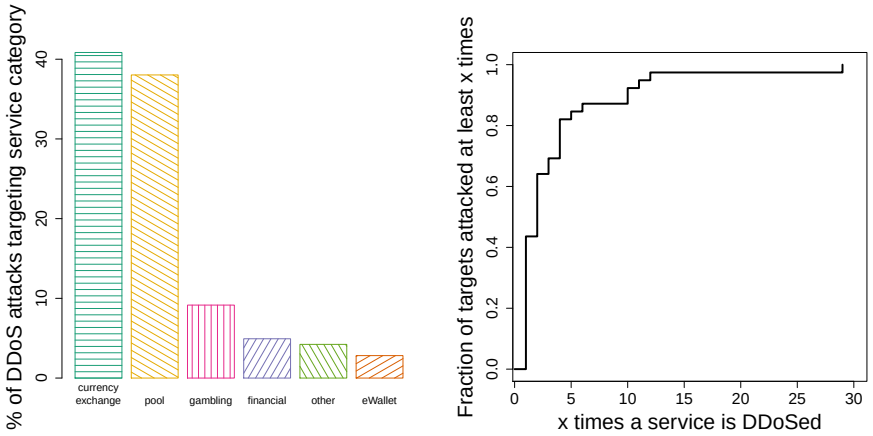

Fig. 2: Percentage of DDoS attacks targeting each major category (left); cumulative distribution function of the number of attacks targeting each service (right).

service is DDoSed. Out of the services targeted by a DDoS attack, 44% are only attacked once, while 15% are attacked on at least five occasions. One service, the Mt. Gox currency exchange, suffered 29 DDoS attacks on different days. We study the timing of attacks on Mt. Gox in greater detail in Section 3.3 below.

Table 2 shows another way to look at the breakdown of DDoS attacks by category. The first column lists the number of services for each category that are still operational (i.e., their listed websites resolve), followed by the percentage of services in each category that have suffered DDoS attacks. Overall, 7.3% of services actually experienced a DDoS attack. The variation across categories is substantial: 27% of pools have experienced DDoS attacks compared to just 0.7% of shops selling physical products. Currency exchanges, mining pools, financial services and eWallets are targeted more frequently than other categories. These differences compared to the average are statistically significant with 95% confidence according to a χ^2 test. One surprise is that Bitcoin payment systems are not targeted by DDoS attacks any more than average.

Given the very real threat of DDoS attacks on Bitcoin services, it is not surprising that many services take steps to defend against these attacks. Moving over to the next column grouping, we report for each category the percentage of services that use anti-DDoS services (either Amazon, Incapsula, or CloudFlare). Overall, around 20% of online Bitcoin services have anti-DDoS protection.

Anti-DDoS protection is more popular in some categories than others. Around one third of exchanges and pools have anti-DDoS protection. This difference in proportion (compared to the 20% average) is statistically significant according to a χ^2 test. Shops selling material and physical products and accepting Bitcoin were substantially less likely to be protected from DDoS attacks – only 10.5% rely on these services. Financial firms and eWallets also frequently employ anti-DDoS protection, but the differences are not statistically significant.

Category	#	Suffer DDoS %	Sig.?	Anti-DDoS (AD) %	Sig.?	AD + DDoS	AD Only	DDoS Only
Material/physical products	295	**0.7**	−	**10.5**	−	2	29	0
Internet & mobile services	225	1.8		16.9		0	38	4
Online products	185	3.8		14.6		3	24	4
Professional services	137	0		10.2		0	14	0
Currency exchanges	119	**10.9**	+	**36.1**	+	10	33	3
Travel/tourism/leisure	78	0		10.3		0	8	0
Commerce & community	71	1.4		12.7		1	8	0
Getting started	31	0		12.9		0	4	0
Financial	26	**15.4**	+	26.9		1	6	3
Pool	41	**26.8**	+	**34.1**	+	5	9	6
Bitcoin eWallets	17	**17.6**	+	35.3		2	4	1
Bitcoin payment systems	11	9.1		18.2		1	1	0
Average		*7.3*		*19.9*				

Table 2: Prevalence of DoS attacks and anti-DDoS uptake by service category.

Finally, the last grouping in Table 2 shows for each category how many services have anti-DDoS protection and have been attacked, how many have anti-DDoS and have not been attacked, and how many have been DDoSed but do not have anti-DDoS protection from Amazon, Incapsula, or CloudFlare. It is noteworthy that across categories it is far more common to have anti-DDoS protection than it is to have actually experienced a DDoS attack. Even in categories where no service has experienced a DDoS attack (e.g., travel and professional services), there is substantial uptake of anti-DDoS protection.

We can also answer a related question: Are services that have experienced DDoS in the past more likely to get anti-DDoS protection afterwards? Table 3 helps to answer the question for all services.

	Use Anti-DDoS #	%	No Anti-DDoS #	%
Suffered DDoS	25	54%	21	46%
No DDoS	178	15%	1 012	85%

Table 3: Contingency table comparing the uptake of anti-DDoS protection based on whether or not the service has experienced DDoS attacks.

Of the 46 distinct services that have experienced DDoS attacks, more than half now have anti-DDoS protection. It is impossible to tell whether or not they had such service at the time of attack. Among services that have not yet experienced a DDoS attack, only 15% have anti-DDoS protection. The difference

in proportion (15% vs. 54%) is statistically significant, according to a χ^2 test ($p \ll 0.0001$ with χ^2 value of 47.232). We conclude that providers are much more likely to obtain anti-DDoS protection if they are targeted by DDoS attacks.

3.2 DDoS Attacks on Mining Pools

Given that mining pools are frequently targeted by DDoS attacks, we now study them in greater detail. We first investigate whether the size of a mining pool affects its chances for being DDoSed. Mining pool size constantly changes, sometimes in response to DDoS attacks. Hence, we needed a historical record of mining pool market shares. Using the Internet Archive, we accessed 22 historical copies of `blockchain.info/pools` that breaks down hashrate by pool. We deem a pool to be "big" if it is observed to have at least a 5% share of the hashrate during two or more observations. All other pools are deemed "small".

Table 4 shows how the incidence of DDoS attacks vary by pool size. 5 out of 8 big pools (63%) have suffered DDoS attacks, compared to just 7 out of 41 small pools (17%). These percentage differences are statistically significant, according to a χ^2-test with a p-value of 0.022. Why would large pools be targeted for DDoS attacks more than small pools? Attackers gain more by targeting large pools, since taking one out can substantially increase the odds of winning the round.

	Small Pools		Big Pools	
	#	%	#	%
Suffered DDoS	7	17.1%	5	62.5%
No DDoS	34	82.9%	3	37.5%

Table 4: Contingency table comparing the size of a mining pool to whether or not the pool has experienced DDoS attacks.

Figure 3 examines the historical hashrate-based market share for six of the larger pools. DDoS reports are indicated by the vertical dashed lines. Some pools seem unfazed by DDoS attacks (e.g., Slush's Pool, Eclipse MC, and Eligius). BTC Guild actually increased its market share following a DDoS attack in mid-2012. However, substantial declines followed a later attack in mid-2013. Furthermore, one can see that sometimes DDoS attacks target multiple pools simultaneously. For example, DeepBit was targeted by attacks at the same time as BTC Guild and Eclipse MC. DeepBit's share of the hashrate tumbled, while it appears that Eclipse MC and BTC Guild benefited as a result. Later attacks in 2013 on BTC Guild and Eclipse MC reduced their own shares, with Eligius benefiting this time even though it too had been hit by DDoS attacks.

Based on this analysis, we reject the notion that DDoS attacks always trigger a decline in market share for affected mining pools. Instead, we see that DDoS attacks often precede shakeups in pool market share. However, at this point we cannot reliably predict who the winners and losers will be as a result.

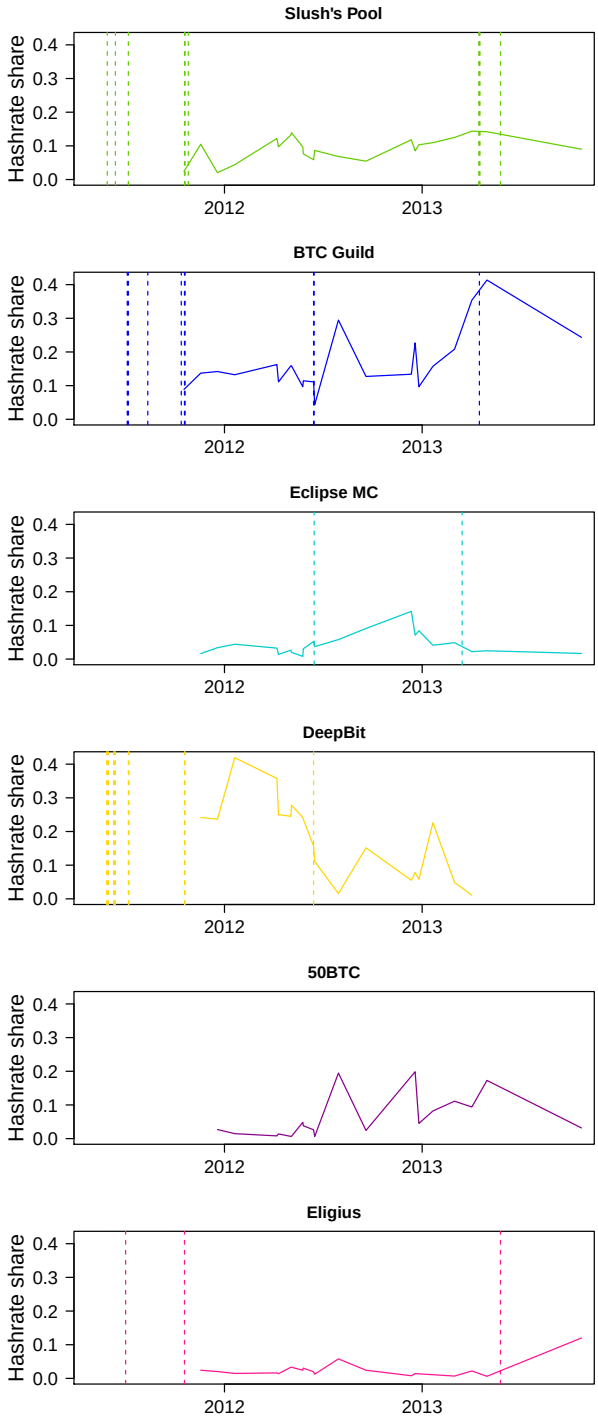

Fig. 3: Mining pool hashrate market share (solid line) over time, compared to timing of DDoS attacks (dashed lines).

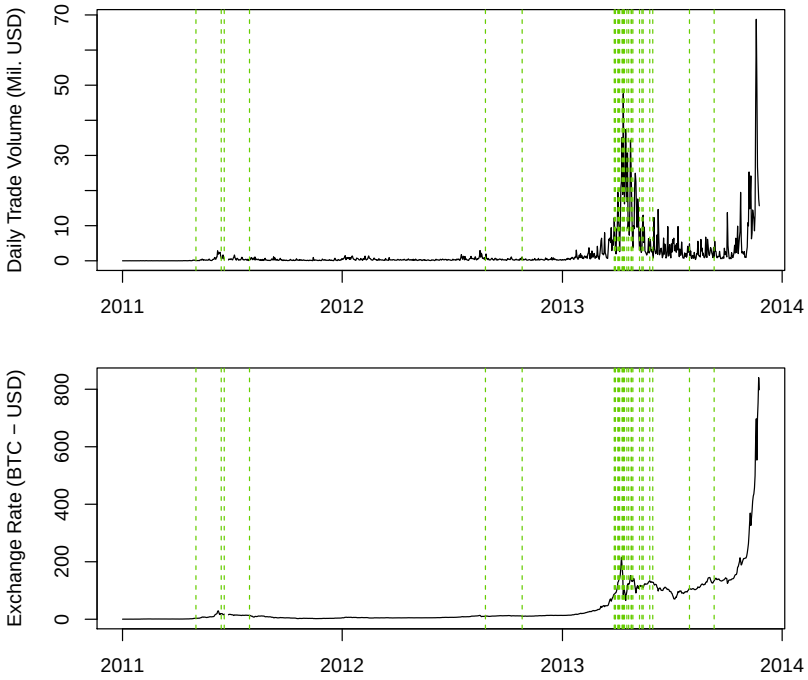

Fig. 4: Daily trade volumes (top) and USD-BTC exchange rate (bottom) at Mt. Gox. Dashed green lines indicate when DDoS attacks on Mt. Gox were reported.

3.3 DDoS Attacks on Currency Exchanges

Currency exchanges are the most frequent target of DDoS attacks. We defer to future work a more detailed analysis of how DDoS attacks affect exchange operations in general. Instead, we take a closer look at attacks targeting Mt. Gox, the largest currency exchange during the time of our study and most frequent attack target.

Figure 4 plots trade volumes and USD-BTC exchange rates at Mt. Gox, along with DDoS attacks as dashed green lines. We can see that Gox suffered some DDoS attacks in 2011 shortly after experiencing unprecedented peaks in trading volume. (It can be difficult to see on the current graph since trading has exploded so much since early 2013.) Note that these early attacks, plus one in late 2012, came shortly after a fall from a new peak in the exchange rate. This behavior is consistent with the modus operandi of blocking exchanges in order to slow down a panicked sell-off.

When Bitcoin's exchange rate shot up in spring 2013, trading volume also soared to unprecedented heights. Dozens of DDoS claims were made in April and

Δ **Transaction Vol.**	**# of Attacks**	**% Attacks**	**% Change** (median)
Increase	12	41.4%	53.3%
Decrease	17	58.6%	34.2%

Table 5: Changes in transaction volume on Mt. Gox after a DDoS attack.

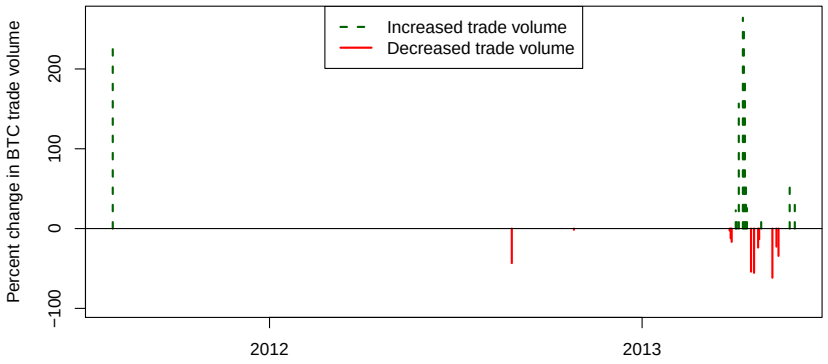

Fig. 5: Changes in transaction volume on Mt. Gox after a DDoS attack over time.

May 2013, eventually subsiding. Two more reports were made later in 2013, but these were one-off reports rather than a chorus as in the spring. Doubtless, some reports were caused by surging demand rather than by a botnet. The blogger *organofcorti* observed a drop in trading volume at Mt. Gox after Mt. Gox's Dwolla account was seized in spring 2013 [14], which could explain some of the reported attacks in times of lower trading volume.

In the (slight) majority of cases, we observe a decrease in transaction volume in the week following a DDoS attack compared to the week prior, as seen in Table 5. We also notice that the median size of the transaction volume change is greater when the transaction volume increases. Figure 5 show this trend over time. We observe that the increases and decreases tend to be clustered together in time. This suggests that certain DDoS attack campaigns can be recovered from quickly while others cannot.

4 Related Work

As interest in Bitcoin has exploded, researchers have undertaken a number of measurement studies to improve our understanding of how Bitcoin is used and abused in practice. Ron and Shamir reconstruct a transaction graph from the Bitcoin block chain in order to find out how money changes hands and identify suspicious transactions (e.g., attempts to launder identity) [15]. Meiklejohn et al. also leverage the block chain in order to measure the traceability of transactions initiated at many Bitcoin service providers [16]. Möser et. al also investigate

the traceability of Bitcoin transactions by evaluating the protection offered by three popular transaction-anonymizing services [17]. Christin crawled advertisements on the now-defunct Silk Road, which shed light on how that marketplace was employing Bitcoin-based transactions to facilitate the sale of illegal goods, notably drugs [18]. Moore and Christin gathered public records of transactions taking place at 40 Bitcoin-currency exchanges in order to find out how often the exchanges shut down [6]. They constructed statistical models to help explain why exchanges close, finding that while more popular exchanges are more likely to be hacked, they are less likely to close.

The present work continues in the vein of these measurement studies, in that it collects publicly-available data to explain better the prevalence of DDoS attacks affecting Bitcoin. We are not aware of any prior work measuring the occurrence of DDoS attacks on Bitcoin. There has been one large-scale study that measures how prevalent DDoS attacks are in the context of websites and blogs [19]. But there are several reasons why we believe Bitcoin DDoS attacks are worth studying on their own. First, there are unique incentives at play that reward DDoS attacks, such as traders who benefit by blocking others' transactions. Second, Bitcoin's unregulated environment has facilitated criminality in pursuit of profits, with DDoS an attractive tool for unscrupulous operators. Indeed, the most closely related work to our own is that of Johnson et al., who present a game-theoretic model of the trade-offs mining pools face between investing in upgrades to computing infrastructure and engaging in DDoS attacks [8]. Their model nicely complements the empirical work undertaken in this paper.

Of course, there are many other attacks besides DDoS involving miners that have been discussed in the literature. Barber et. al. describe a Doomsday, "51%", attack where a miners enter false transactions into the block chain [20]. Eyal and Sirer further refine the attack assuming colluding miners, lowering the threshold from 50% to 33% of total mining hashrate needed to control the blockchain [21]. Kroll et. al. model whether a miner should join a mining pool using game theory. They expand their model to describe a "Goldfinger" attack on the Bitcoin network [22]. Finally, Rosenfeld describes a double-spending attack [23].

5 Concluding Remarks

We have presented an empirical study of DDoS attacks targeting a wide range of operators in the Bitcoin ecosystem. Using posts to the popular `bitcointalk.org` forum, we identify and analyze 142 distinct DDoS attacks. We find that 7.4% of Bitcoin-related services have experienced DDoS attacks. Currency exchanges are targeted most often, followed by mining pools, gambling operators, financial service providers, and eWallet operators. Attack frequency is highly variable: pools were targeted most often back in 2011, followed by a wave of attacks targeting currency-exchanges in Spring 2013. DDoS on gambling operators, nonexistent until December 2012, have picked up considerably in the latter part of 2013.

We also carried out preliminary analysis into the effects of DDoS attacks on mining pools and currency exchanges. One striking finding is that over 60% of

large mining pools have been DDoSed, compared to just 17% of small ones. This suggests that the large pools are big targets for unscrupulous miners hoping to increase their odds of winning freshly minted Bitcoins.

Our results indicate that Bitcoin DDoS attacks merit further investigation. Nonetheless, the findings often raise more questions than they answer. To get those answers, a richer and more robust dataset is needed. Our dataset is based on circumstantial evidence of DDoS attacks reported on a single, albeit popular, web forum. Such reports do not constitute definitive evidence that a DDoS has taken place. Future investigations could corroborate reports with supplementary evidence, such as directly measuring inaccessibility from probes and incorporating reports from additional sources besides `bitcointalk.org`.

Therefore, much work remains to be done. In future work, we would like investigate the following:

- Check for any consistent variation between trade volumes and exchange rate before and after a DDoS attack on a currency exchange.
- Explore the relationship between DDoS attacks on other digital currencies such as Litecoin. Mt. Gox was subject to a DDoS attack which delayed their acceptance to trade Litecoin. Furthermore, some speculate that Bitcoin enthusiasts are attacking other currencies to ensure Bitcoin's market dominance in the market of digital currencies.
- We investigated three leading forms of anti-DDoS protection, but there are others. Furthermore, protection such as CloudFlare doesn't protect against certain types of DDoS attacks.
- Study how other factors such as type of mining pool influence the prevalence and success of DDoS attacks. For instance, the supposedly DDoS-resistant P2P mining pool `altcoin.pw` was shut down. Are P2P pools inherently more "DDoS-able", or is this a function of something else?
- Moore and Christin found that transaction volume mattered more than attack susceptibility when predicting the future viability of a Bitcoin exchange [6]. Does this model carry over to Bitcoin mining pools? The case study of DeepBit which has lost its market dominance due to repeated DDoS attacks would suggest not.

In addition to these avenues for analytical investigation, we would also like to refine the classification mechanism for automatically identifying posts that describe DDoS attacks. Given that DDoS is an ongoing and sporadically-occurring problem for Bitcoin, it would be useful to develop a tool that can automatically generate reliable attack indicators that do not require manual removal of false positives.

Acknowledgments

We thank the anonymous reviewers and paper shepherd Fergal Reid for their helpful feedback. This work was partially funded by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) Broad Agency Announcement 11.02, the Government of

Australia and SPAWAR Systems Center Pacific via contract number N66001-13-C-0131. This paper represents the position of the authors and not that of the aforementioned agencies.

References

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009, http://www.bitcoin.org/bitcoin.pdf.
2. D. Chaum, "Achieving electronic privacy," *Scientific American*, pp. 96–101, Aug. 1992.
3. J. Gallu, "Bitcoin Ponzi scheme alleged by SEC in lawsuit against Texas man," *Bloomberg*, Jul. 2013, http://www.bloomberg.com/news/2013-07-23/bitcoin-ponzi-scheme-alleged-by-sec-in-lawsuit-against-texas-man.html.
4. A. Jeffries, "Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt," *The Verge*, August 2012, http://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down.
5. J. Leyden, "Linode hackers escape with $70k in daring Bitcoin heist," *The Register*, March 2012, http://www.theregister.co.uk/2012/03/02/linode_bitcoin_heist/.
6. T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, vol. 7859. Springer, 2013, pp. 25–33.
7. J. Leyden, "How mystery DDoSers tried to take down Bitcoin exchange with 100Gbps crapflood," *The Register*, Oct. 2013, http://www.theregister.co.uk/2013/10/17/bitcoin_exchange_ddos_flood/.
8. B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools," in *1st Workshop on Bitcoin Research*, ser. Lecture Notes in Computer Science, vol. (to appear). Springer, March 2014.
9. Bitcoin Wiki, "Trade," https://en.bitcoin.it/wiki/Trade. Last accessed November 21, 2013.
10. ——, "Category: Pool operators," https://en.bitcoin.it/wiki/Category:Pool_Operators. Last accessed November 21, 2013.
11. CloudFlare, "Cloudflare IP ranges," http://www.cloudflare.com/ips. Last accessed November 21, 2013.
12. U. Harel, "Restricting direct access to your website (Incapsula's IP addresses)," http://support.incapsula.com/hc/en-us/articles/200627570-Restricting-direct-access-to-your-website-Incapsula-s-IP-addresses-. Last accessed January 15, 2014.
13. Amazon Web Services, "Announcement: Amazon EC2 public IP ranges," https://forums.aws.amazon.com/ann.jspa?annID=1701. Last accessed November 21, 2013.
14. organofcorti, "MTGOX volume post Dwolla: A single statistical test," *Neighbourhood Pool Watch*, July 2013, http://organofcorti.blogspot.com/2013/07/114-mtgox-volume-post-dwolla-single.html.
15. D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, vol. 7859. Springer, 2013, pp. 6–24.
16. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," in *Proceedings of the 2013 Conference on Internet Measurement Conference*, ser. IMC '13. New York, NY, USA: ACM, 2013, pp. 127–140.

17. M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *8th APWG eCrime Researchers Summit*. IEEE, 2013.
18. N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd International Conference on the World Wide Web*. International World Wide Web Conferences Steering Committee, 2013, pp. 213–224.
19. E. Zuckerman, H. Roberts, R. McGrady, J. York, and J. G. Palfrey, "2010 report on distributed denial of service (DDoS) attacks," Berkman Center Research Publication, Tech. Rep. 2010-16, Dec. 2010, http://ssrn.com/abstract=1872065.
20. S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better – How to make Bitcoin a better currency," in *Proceedings of the 16th International Conference on Financial Cryptography and Data Security*. Springer, 2012, pp. 399–414.
21. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proceedings of the 18th International Conference on Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, vol. (to appear). Springer, March 2014.
22. J. Kroll, I. Davey, and E. Felten, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in *Proceedings of the Twelfth Annual Workshop on the Economics of Information Security (WEIS'13)*, Washington, DC, Jun. 2013.
23. M. Rosenfeld. (2012) Analysis of hashrate-based double-spending. [Online]. Available: https://bitcoil.co.il/Doublespend.pdf