There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams

Marie Vasek and Tyler Moore

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

Abstract. We present the first empirical analysis of Bitcoin-based scams: operations established with fraudulent intent. By amalgamating reports gathered by voluntary vigilantes and tracked in online forums, we identify 192 scams and categorize them into four groups: Ponzi schemes, mining scams, scam wallets and fraudulent exchanges. In 21% of the cases, we also found the associated Bitcoin addresses, which enables us to track payments into and out of the scams. We find that at least $11 million has been contributed to the scams from 13 000 distinct victims. Furthermore, we present evidence that the most successful scams depend on large contributions from a very small number of victims. Finally, we discuss ways in which the scams could be countered.

1 Introduction

An effective, though unfortunate, way to determine that a new technological platform has "arrived" is by observing the presence of scammers leeching off those using the system. Shortly after the advent of the telegraph, sneaky punters began placing bets on recently-completed horse races at faraway bookmakers who had not yet observed the result [1]. Once telephones became pervasive, unsolicited calls by scammers became problematic. No sooner had email become popular, then a flood of messages promising riches from Nigerian princes began filling people's inboxes.

In this paper, we investigate scams targeting the virtual currency Bitcoin, which has exploded in popularity since its introduction in 2009 [2]. As more people have been drawn to Bitcoin, frequently out of a desire to get rich quickly, more hucksters have appeared to take advantage of these eager new targets. Because Bitcoin is so new, the newly emerging scams are frequently poorly understood. The goal of this paper is to systematically investigate different types of Bitcoin scams, explain how they work, and measure their prevalence. It is hoped that by understanding how these scams work we will identify ways to arrest their rise.

To that end, we identify four types of scams currently plaguing Bitcoin: high-yield investment programs, mining investment scams, scam wallet services and scam exchanges. Using reports obtained from discussion forums and tracking websites, we study 41 distinct scams operational between 2011 and 2014 where we could find the associated Bitcoin address(es). So while the study is by no means comprehensive, we are able to analyze the block chain and provide a lower bound estimate of the prevalence and criminal profits associated with these scams.

We find that $11 million worth of bitcoin has been contributed to the scams, and that at most $4 million has been returned to the victims. For the HYIPs and mining scams, we estimate that about 13 000 victims contributed funds. We also show that the most successful scams draw the vast majority of their revenue from a few victims, presenting an opportunity for law enforcement to track down and prosecute the scammers.

Section 2 describes the methodology for identifying scams, as well as how we examine the block chain to identify payments into and out of scams. Section 3 reports on high-yield investment programs (HYIPs), online Ponzi schemes where existing investors are paid lucrative returns from the contributions of new investors. Section 4 examines mining-investment scams, which is a form of advanced-fee fraud that exploits people's interest in Bitcoin mining by promising a way to profitably mine without making large up-front investments in expensive hardware. Sections 5 and 6 cover scam wallets and exchanges, respectively. Here, the scammers provide sought-after services such as mixing at a seemingly affordable price, only to steal incoming transfers from customers. Section 7 compares the different scam categories and considers what the appropriate response, if any, should be from the Bitcoin community and policymakers. Finally, we review related work in Section 8 and conclude in Section 9.

2 Methodology for Identifying Scams and Associated Transactions

We compile a list of 349 distinct candidate scams from an aggregated thread on `bitcointalk.org`[1], a blacklist of suspected fraudulent services maintained at `http://www.badbitcoin.org/thebadlist/index.htm`, and a website tracking Bitcoin-based HYIPs called `cryptohyips.com`[2]. We manually inspected all services on the list to identify only those operations established with fraudulent intent. For instance, we exclude Hashfast, a mining company that recently filed for Chapter 11 bankruptcy protection, as well as losses from Mt. Gox, a bitcoin exchange that failed. We also removed a number of false positives with no clear connection to cryptocurrencies, such as `unclechiens.com` (a Chinese restaurant in Texas). In total, this sheds 26% of our candidate list.

We also exclude from consideration all efforts beyond the purview of this paper, such as phishing websites, malware websites, and pay-for-click websites. We are left with 192 scams to investigate further, 55% of the candidates. We categorize each scam's type by inspecting the website through the Internet Archive (since many scams have since disappeared) and targeted Google searches on the domain.

We next seek out associated Bitcoin addresses for each scam using threads on `bitcointalk.org`, `reddit.com/r/bitcoin`, and named addresses and transactions on `blockchain.info`. We exclude any "dual-use" addresses that are also used for other purposes. In all, we find usable Bitcoin addresses for 20% of the scams.

The next goal is to identify payments made into and out of the scam. To that end, we download the Bitcoin block chain using the Bitcoin Core client on August 25, 2014. Using znort987's Bitcoin blockparser [3] we query for all transactions involving our set of scammy addresses. This gives us traffic levels for incoming transactions to each

[1] `https://bitcointalk.org/index.php?topic=576337`

[2] Data and analysis scripts are publicly available at `doi:10.7910/DVN/28561`.

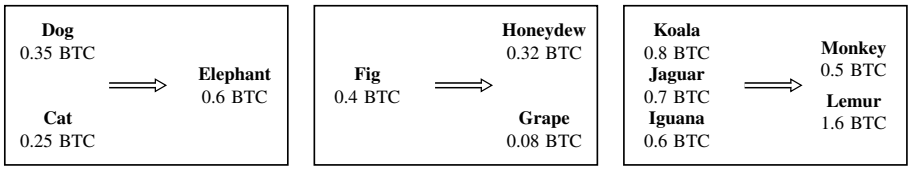

Fig. 1: Multiple-address transactions in Bitcoin.

scam. We then take a complete SQL dump of the Bitcoin block chain and query for all the transactions where the input or output address match one of our scam addresses. This gives us the Bitcoin addresses of the victims as well as the outgoing transactions from the scam. To separate out transactions made by scammers, we omit all outgoing transactions going to other addresses associated with the same scam. We also omit transactions occurring before and after the first incoming transaction to the scam.

One challenge for researchers inspecting a block chain is dealing with multiple sources and destinations in transactions. Figure 1 demonstrates the three cases where these transactions arise. We deal with multiple source–single destination transactions (Figure 1 (left)) as follows. If the destination is a scam address and the source addresses are not also identified as being part of the scam, we group the source addresses together as a single victim.[3] In general, two addresses are assigned to the same *address group* if they ever paid into the same scam during the same transaction. For multiple-source transactions involving a scam address, we only count the scam address's contribution towards the total payout from the scam.

For transactions with a single source and multiple destinations (Figure 1 (center)), we attribute only the source amount to the scam. For instance, suppose Fig is a victim address and Honeydew is the scam. Even though Fig pays 0.4 BTC, we tally only the 0.32 BTC transferred to Honeydew as part of the scam's total incoming payments.

With multiple sources and destinations (Figure 1 (right)), we assign the amount paid in or out of the scam to the corresponding address group. For example, suppose Lemur is the scam address. Here, the victim group Koala–Jaguar–Iguana contributes 1.6 BTC to Lemur's scam. While in theory services such as CoinJoin [4] could account for many such transactions, in practice we do not observe very many transactions of this type.

Finally, we note that when identifying victim groups we could mistakenly identify online web wallets that pay out multiple users from the same address as a single address group. To check for this, we inspected all multiple-destination transactions whose source address appeared more than three times. In all cases, we did not find that the source addresses corresponded to web wallets. One potential explanation for this is that many scams prohibit using web wallets as a method of payment.

In addition to gathering data directly from the blockchain, we also analyze scams that raise funds through selling shares. We gather the share holdings from BitFunder and cross list that with cost of the shares from announcements on `bitcointalk.org`. For each scam, we omit the top holding who we verify is the scammer in all instances.

[3] Note that we deliberately make no attempt to deanonymize the actual victims beyond identifying that the addresses participated in the scam.

	Victim pay in	Payout to victim	Payout to scammer
HYIPs	✓	✓	derived
Mining scams	✓	derived	derived
Scam wallets			✓
Exchange scams			✓

Table 1: For each scam category, we report whether we can directly observe transactions corresponding to what victims pay into scams, what is paid out to victims, and what is paid out to the scammer (indicated by a ✓).

Ideally, we would analyze payments from victims into scams, payments back to victims, and scammer profits. For some scams, we can observe all such payments, whereas for others we can only observe certain categories. Table 1 summarizes the types of observable transactions for each scam type. Full details are given in subsequent sections.

Finally, due to high volatility of the bitcoin exchange rate, it makes sense to also report scam revenues in terms of its dollar equivalent. In order to convert BTC to USD, we gathered the daily closing USD-BTC exchange rate from the four highest-volume USD exchanges during the period of our study (Mt. Gox, Bitstamp, Bitfinex and BTC-E), as reported to `http://www.bitcoincharts.com`. We then converted any transactions into USD using the average exchange rate on the day of the transaction.

3 High Yield Investment Programs

Moore et al. first described high-yield investment programs (HYIPs) in [5]. HYIPs are online Ponzi schemes where people are promised outlandish interest rates on deposits (e.g., 1–2% interest per day). Unsurprisingly, the schemes eventually collapse, and they are replaced by new programs often run by the same criminals. Moore et al. observed that these HYIP schemes relied on virtual currencies such as Liberty Reserve, Perfect Money, and EuroGoldCash for deposits and withdrawals. The centralized nature of these particular currencies has left them vulnerable to countermeasures by law enforcement. For example, Liberty Reserve was taken down by the US government in 2013 for money-laundering activities. In response, some programs have begun accepting decentralized digital currencies such as Bitcoin and Litecoin. Furthermore, most HYIPs directly advertise Bitcoin addresses in order to accept incoming payments, as opposed to using a payment processor such as BitPay or Coinbase.

We observe a number of different types of HYIPs that accept Bitcoin: HYIPs that stay in the traditional HYIP ecosystem; HYIPs that bridge the traditional HYIP ecosystem and the Bitcoin community; and HYIPs that originate in the Bitcoin ecosphere.

3.1 Traditional HYIPs

We first investigated the extent to which traditional HYIPs have begun to embrace Bitcoin. To our surprise, we found that most HYIPs do not accept bitcoin as payment. We believe the reason why is that the leading kit for developing HYIP websites, Gold

	Bridge HYIPs	Bitcoin-only HYIPs
# Scams	9	23
Median lifetime (days)	125	37
# still operational	1	0
Victim pay in		
# address groups (total)	9 410	3 442
# address groups (median)	298	157
Amount paid (total)	$6 456 593	$842 909
Payout to victim		
Amount paid (total)	$3 464 476	$802 655
Payout to scammer		
Amount paid (total)	$2 992 117	$40 254

Table 2: Summary statistics for HYIPs.

Coders, does not support payments in Bitcoin or other cryptocurrencies. Neisius and Clayton analyzed the HYIP ecosystem, and they estimated that between 50–80% of HYIP websites they observed used the Gold Coders kit [6].

When we observed several "aggregator" websites that track HYIPs, we found some traditional HYIPs that accept BTC or LTC. We then inspected HYIPs with a publicly-accessible incoming address but had never been mentioned on `bitcointalk.org`. All of these programs had insignificant transaction volume. Based on these findings, we do not consider traditional HYIPs further in our analysis.

3.2 Bridge HYIPs

Some scams first appear in the traditional HYIP ecosystem before being brought over to the Bitcoin world through posts on `bitcointalk.org`. In these cases we frequently find a high volume of BTC transactions. For example, Leancy claimed to have received over $5M in investments[4] from a variety of currencies. From observing payments into its Bitcoin address, we estimate $1 674 270 came from bitcoin deposits.

Overall, we observe a total of nine such scams that brought in 12 622 BTC ($6.5M) from September 2, 2013 through September 9, 2014. Table 2 reports key summary statistics for the nine bridge HYIPs observed. Median lifetime of the bridge HYIPs is 125 days, with one HYIP still in operation at the time of writing.

The $6.5M in contributions came from 9 410 distinct address groups, which provides an upper bound for the number of victims contributing to these scams. The scams in turn paid at most $3.5M back to the victims, leaving $3M in profit to the operators. It is likely that at least some of the $3.5M in payouts went to addresses controlled by scammers, so we expect the actual profit rate to be much higher.

These summary statistics obscure the details of how individual scams performed over time. Figure 2 (top) plots the aggregate payments into and out of the nine bridge

[4] `https://web.archive.org/web/20140322111925/https://leancy.com/`

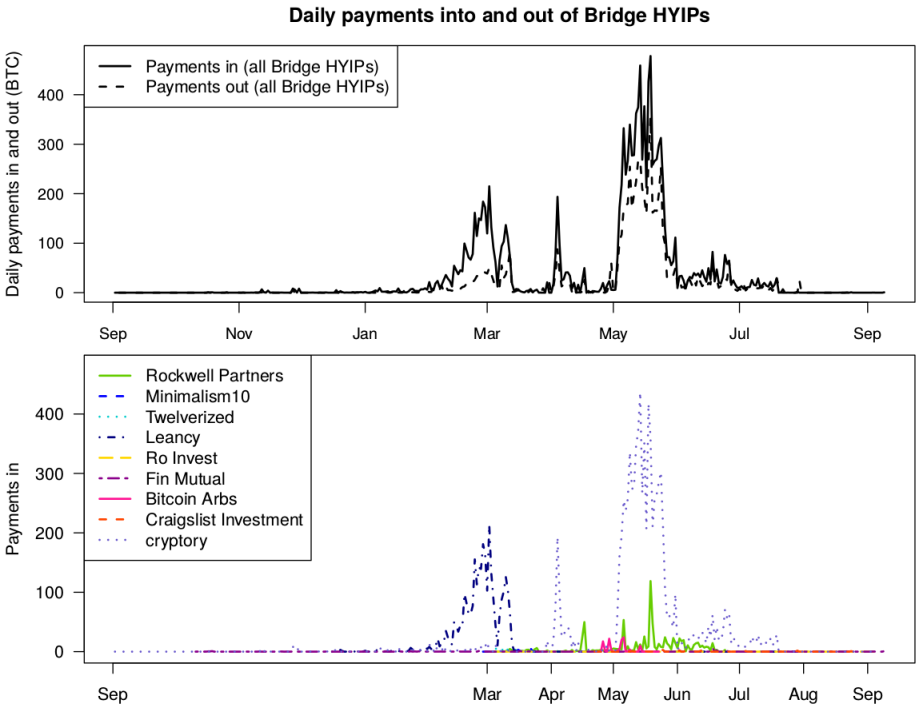

Fig. 2: Top: Daily volume of all payments into and out of Bridge HYIPs wallet incoming transactions. Bottom: daily volume of incoming payments split by HYIP.

HYIPs. We can see that, in aggregate, the payments flowing into the scams always keep pace with the payments flowing out. We also see huge spikes in the money flowing in at different points throughout the period, with nearly all of the activity taking place in 2014. Figure 2 (bottom) breaks out the incoming payments to the associated scams. We can see that the first big spike is due to the rise of Leancy, the second Cryptory, the third Rockwell Partners and the fourth Cryptory (with a small contribution form Rockwell Partners). Hence the overall burstiness observed in the scam contributions can be attributed to different scams receiving a surge of investment before falling rapidly.

Figure 3 compares the transactions in and out for the top 8 performing bridge HYIPs. The graphs are presented in decreasing order of scam size, and the graph also includes a green dotted line indicating the day the scam first appeared on the `bitcointalk.org` forum.

For example, for Leancy (top right) we see the first BTC transaction on December 16, 2013, but the volume picks way up on February 4, 2014 when a user, `LeancyBTC`, posted an advertisement for the scheme in the Bitcoin forums[5]. Most reports precede spikes in investment, though the jump is not always as immediate as in the case of `LeancyBTC`'s post.

[5] `https://bitcointalk.org/index.php?topic=448250`

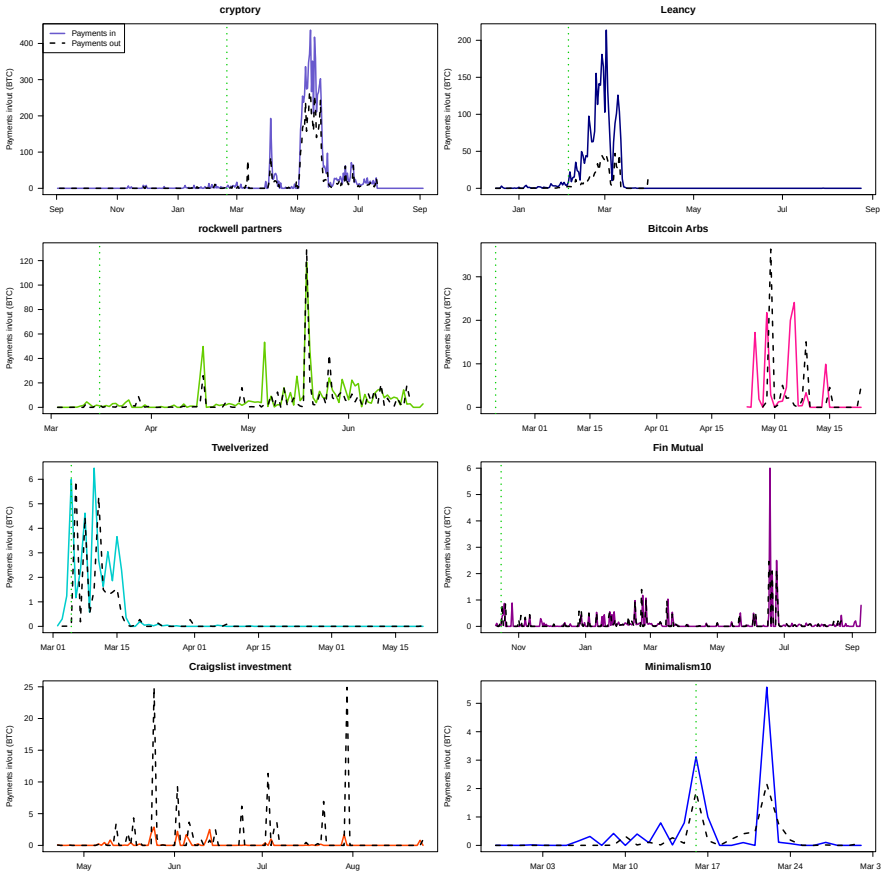

Fig. 3: Daily volume of payments into and out of Bridge HYIPs, sorted by total payments received. The green dotted line indicates when the scam is first promoted on `bitcointalk.org`.

The other key conclusion that can be drawn from these graphs is that the most successful scams manage to pay out far less than they take in, and they do so consistently over time. In theory, Ponzi schemes need not collapse until withdrawal requests overwhelm the cash reserves of the scammer. In practice, for Leancy and Cryptory, the scheme stopped paying out as soon as the funds stopped flowing in. These operators could have kept up the appearance of legitimacy by honoring withdrawal requests after new deposits stopped, but they chose not to. Instead, they found it more profitable to simply disappear once the deposits did.

For the less successful scams (bottom of graph), the outgoing payments often exceed the incoming payments. Hence, in these cases it does appear that the scammer gave up once the scam failed to take off, even after honoring withdrawal requests that exceeding available deposits.

3.3 Bitcoin-only HYIPs

In addition to HYIPs that happen to accept bitcoin, many shady operators have set up Ponzi schemes using bitcoin as a method of payment. We term these frauds *Bitcoin-only HYIPs* because they operate like HYIPs even if they do not share the same heritage as traditional HYIPs.

The premise behind Bitcoin-only HYIPs varies considerably. Some purport to be legitimate investment vehicles. The biggest of these is Bitcoin Savings and Trust (first launched under the name "First Pirate Savings and Trust") which allegedly raised 4.5 million USD [7]. (Unfortunately, since the address used for this Ponzi was also used for a legitimate Bitcoin marketplace, we do not include it in our analysis. Reported estimates in volume vary greatly[6].) Others purport to be online Bitcoin wallets offering an outlandishly high daily rate of return on the money kept in the wallet. While these schemes are fraudulent by design, they lure in unsuspecting, naïve victims as well as those fully aware that they are investing in a Ponzi scheme. The rest were transparently Ponzis. Some of these offer an "hourly" rate of return and purport to deposit that return back hourly. Others offer an increased payout upon a subsequent pay in. Some schemes just offer a lump payout after a period of time.

In total, we observed 23 Bitcoin-only Ponzi schemes, which earned 1 562 BTC (843K USD) from January 2, 2013 through September 9, 2014. Table 2 reports the key summary statistics. Compared to Bridge HYIPs, Bitcoin-only HYIPs are shorter-lived and less profitable. The schemes collapse within 37 days (median) and the scammers have collectively netted only $40K during that time. Again, we expect that some of the payouts to victims are actually addresses controlled by scammers, so the scammer's profit is likely higher.

4 Mining Scams

Since virtually every operation that sells mining equipment has been accused of being a scam, we adopt the narrower definition of scams as those mining operations that take payments from "investors" but never deliver product. Note that "cloud mining" operations that are transparently Ponzi schemes are considered in our HYIP discussion in Section 3. Furthermore, we also exclude the many "cloud mining" operations that have not been shown to be Ponzi schemes but are dubious in nature.

We analyze five mining scams (Labcoin, Active Mining Corporation, Ice Drill, `AsicMiningEquipment.com`, `Dragon-Miner.com`). We consider Labcoin here instead of Section 3 since it did not promise outrageous returns and it did purport to deliver hashing output to some degree[7]. Similarly, Active Mining and Ice Drill are operations that raised money to purportedly make ASICs and share the profits but never delivered. `AsicMiningEquipment.com` and `Dragon-Miner.com` are fraudulent mining e-commerce websites.

Relevant summary statistics are presented in Table 3. Notably, due to the nature of the scam, none of this contributed money is returned to the victims.

[6] `https://bitcointalk.org/index.php?topic=576337#post_toc_38`
[7] `https://bitcointalk.org/index.php?topic=263445.msg3417016`

5 Scam Wallets

We now consider fraudulent services that masquerade as Bitcoin wallets. Note that we categorize wallets that purport to offer a daily return on savings as Ponzi schemes and discuss them in Section 3. Scam wallets, by contrast, offer many of the features of online wallets, but with a key difference: the operators siphon some or all of the currency transferred to the wallet.

The basic ruse goes as follows:

1. Victim deposits bitcoin into scam wallet.
2. If the amount of money falls below the threshold, the money stays.
3. If the amount of money is above the threshold, the scammer moves the money into her own wallet.

We identified this process by examining 15 threads on the `bitcointalk.org` forums and 7 threads on the Bitcoin subreddit (`reddit.com/r/bitcoin`) where users complained of losing money once they began depositing larger amounts. Bitcointalk users `drgonzo`[8] and `Artificial`[9]put over 10 bitcoin into their respective Easy Coin accounts in early 2013 but were each left with 0.099 bitcoin (0.1 bitcoin minus their mixing fee) immediately following. Whereas Bitcointalk user `BitcoinOnFire` [10] reports that the first Easy Coin transaction he made worked, but when he moved over a few bitcoin in early 2014, that was quickly drained. Bitcointalk user `Kazimir`[11] reports that putting in less than 0.1 bitcoin into Bitcoinwallet.in in late 2013 which was fine. Reddit user `LutherForThePeople`[12] reports putting in a small amount of bitcoin into Easy Coin in 2013 which was fine and then upon putting in more bitcoin, the scammers drained his account.

We were able to analyze three of these services (Onion Wallet[13], Easy Coin[14], and Bitcoinwallet.in[15]), in which all transfers from the victims were ultimately delivered to the same address held by the scammer. These particular scams advertise themselves as offering a mixing service that enhances transaction anonymity for customers. In fact, all three services appear to be operated by the same scammer, because the siphoning transfers all go directly to the same Bitcoin address. The wallets do in fact operate a mixing service, which makes it impractical to trace back incoming transfers from victims into the service. However, since the scammer sends all stolen bitcoins to the same address, we are able to track the ill-gotten gains for these three scams collectively.

Figure 4 (top) plots the amount of Bitcoin drained out of victim accounts each week. The highly volatile trend suggests that the scam had more success in 2013 compared to

[8] `https://bitcointalk.org/index.php?action=profile;u=106769`
[9] `https://bitcointalk.org/index.php?action=profile;u=109912`
[10] `https://bitcointalk.org/index.php?action=profile;u=323407`
[11] `https://bitcointalk.org/index.php?action=profile;u=58460`
[12] `https://www.reddit.com/user/LutherForThePeople`
[13] `http://ow24et3tetp6tvmk.onion/`
[14] `http://easycoinsayj7p5l.onion/` and `https://web.archive.org/web/20130905204338/https://easycoin.net/`
[15] `https://web.archive.org/web/20140213235218/https://bitcoinwallet.in/`

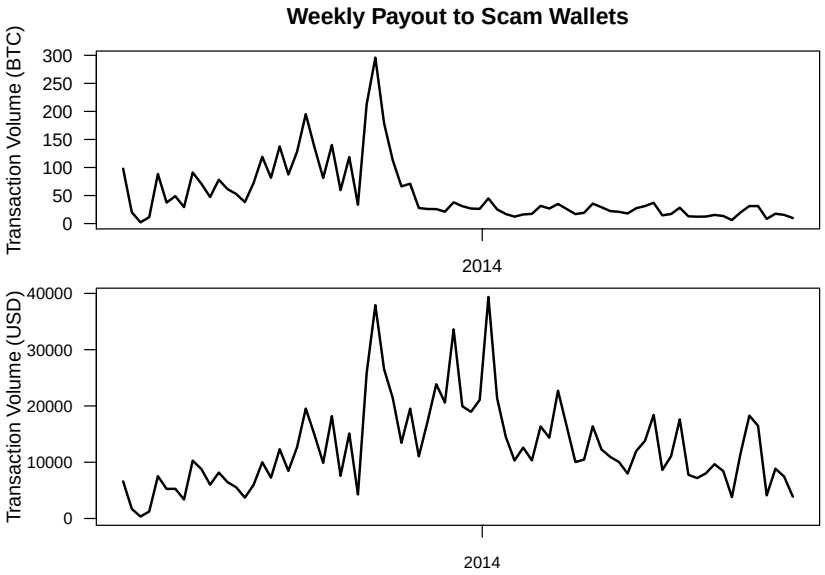

Fig. 4: Weekly payouts to scam wallets in BTC (top) and USD (bottom).

2014. However, normalizing the scammer intake against the BTC–USD exchange rate, as in Figure 4 (bottom), tells a different story. It suggests that the scammer drains off an amount of BTC corresponding to a steady USD-denominated wage. Compared to the Bitcoin HYIPs and mining scams, these wallet scams offer a much steadier stream of between $10–40K in ill-gotten gains each week. In total, this scammer's revenue (through 11 September 2014) was about 4 100 BTC, which corresponds to nearly $1 million. Finally, we note that the scam continues unabated at the time of this writing.

6 Bitcoin Exchange Scams

We look at four scams purporting to be Bitcoin exchanges: BTC Promo, btcQuick, CoinOpend, and Ubitex. Most of these scams entice victims by offering features that many other exchanges do not offer such as PayPal/Credit Card processing, or a better exchange rate than established players. Unfortunately for the customer, they they never actually receive the bitcoin or cash after making payment. Ubitex purported to be an in-person exchange, but never got off the ground. Speculation exists as to whether Ubitex is a scam or just a flopped business, but we treat it as a scam here.

Table 3 reports the key figures for the scam exchanges. The longer-lived scam exchanges survived for approximately three months, but they also drew in the least amount of money from victims. CoinOpend and btcQuick each operated for less than one month, but during that time drew in hundreds of thousands of dollars from victims.

[16] 20.189BTC corresponding to $15 515 reported invested on GLBSE, but not trackable on block chain. Address is from `bitcointalk` forum post asking for Ubitex donations.

Scam	Lifetime		Payout to scammer	
	Days	Alive?	BTC	USD
Scam wallets	535	yes	4 105	$359 902
Scam exchanges				
BTC Promo	98	yes	44	$22 112
btcQuick		no	929	$73 218
CoinOpend	29	no	575	$264 466
Ubitex	91	no	30	$96[16]
Mining scams	Data Source			
Labcoin	Blockchain		241	$48 562
AMC	BitFunder		18 041	$1 327 590
Ice Drill	BitFunder		14 426	$1 558 008
Asic Mining	Blockchain		12.6	$5 532
Dragon Miner	Blockchain		1.63	$1 019

Table 3: Lifetime and payouts for scam wallets and exchanges, plus mining scam payouts.

Scam category	Scam revenue		Hook	Victim awareness	Trackability
Bridge HYIPs	$6.5M	(in)	Greed	low–high	med.
Bitcoin-only HYIPs	$840K	(in)	Risk appetite, greed	high	high
Mining scams	$2.9M	(in/out)	Advanced-fee fraud	low	low
Wallet scams	$360K	(out)	Information asymmetry	low	low
Exchange scams	$455K	(out)	Information asymmetry	low	low

Table 4: Recap of Bitcoin scam categories and features.

7 Discussion

7.1 Revisiting the Scam Categories

The scams presented differ in several key ways, as summarized in Table 4. First, we can see that Bridge HYIPs have taken in the most revenue from victims. This may reflect the more mature nature of these scams, as traditional HYIPs have been operating for years. Thus, they already have an established base of users and extensive advertising. The Bitcoin-based schemes, by contrast, are much newer and so we would expect that the scams are not as refined. A less optimistic interpretation, therefore, is that there is considerable room for growth in the magnitude of these frauds as Bitcoin increases in popularity. Furthermore, we note that true total of scammer profits could be much higher, given that we could only track revenues for 21% of the reported scams.

The scams also differ in the way they "hook" victims. HYIPs exploit people's greed, or more precisely, their susceptibility to the narrative that it is easy to get rich quick just by using Bitcoin. Mining scams exploit this same desire, but wrap it in more measured promises of future riches. Mining scams are classic advanced-fee fraud: victims pay money in hopes of getting larger sums down the line, but that day never comes.

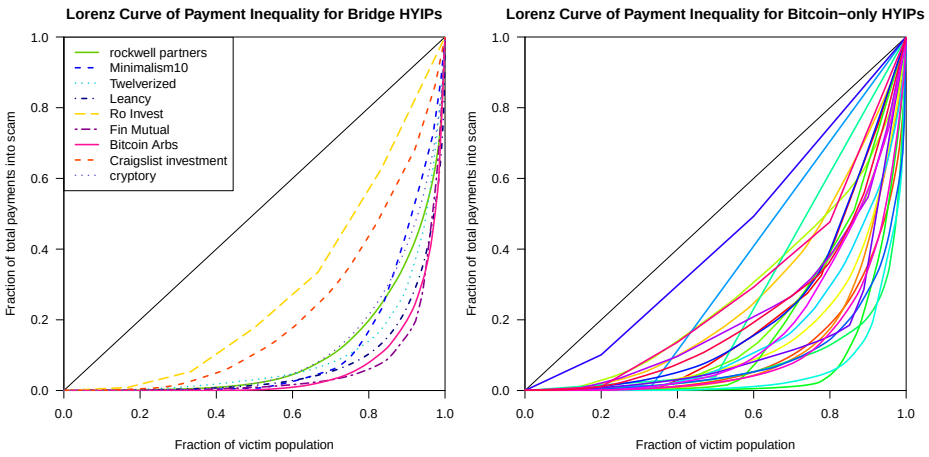

Fig. 5: Lorenz curve for Bridge HYIPs (left) and Bitcoin-only HYIPs (right).

Wallet and exchange scams, by contrast, exploit the difficulty people have in judging the legitimacy of web services. Thus, the scammers take advantage of an information asymmetry that naturally exists. So long as it is difficult to distinguish between good services and bad ones, there will remain an opening for scammers to profit.

User awareness to the scams also varies considerably. Some participants in HYIPs know that they are likely investing in a Ponzi scheme, but they hope to cash out before the scheme collapses. Most Bitcoin-based HYIPs, however, are transparent about the dodgy nature of the service. For example, Bit Twin offers to double your bitcoins within 48 hours. Hence, some scams might even be considered a form of gambling. However, investors in mining, exchange and wallet scams are usually completely unaware that anything untoward is going on with the service until they have lost their money.

Finally, we can distinguish between how inherently trackable these scams are. Some bridge HYIPs can be readily tracked, since they publish a single incoming payment address online. Others use a service such as `blockchain.info` which generates a new incoming address for each visitor. Many require investors to sign up first in order to receive the incoming payment address, which could be changed for different investors. Most Bitcoin-only HYIPs can be readily tracked, since the service usually posts the address in order to signal trustworthiness in the service. Any service that attempts to hide the payment addresses would be viewed with suspicion.

Mining, exchange and wallet scams need not be trackable. The ones we observed happened to make their addresses publicly available, but there is no reason that this should always be. Hence, we anticipate these frauds to remain difficult to track via the block chain moving forward.

7.2 How are Victim Payments into Scams Distributed?

We now examine how the size of payments into scams are distributed. This is an important question, because it influences how successful scammers select targets. A relatively

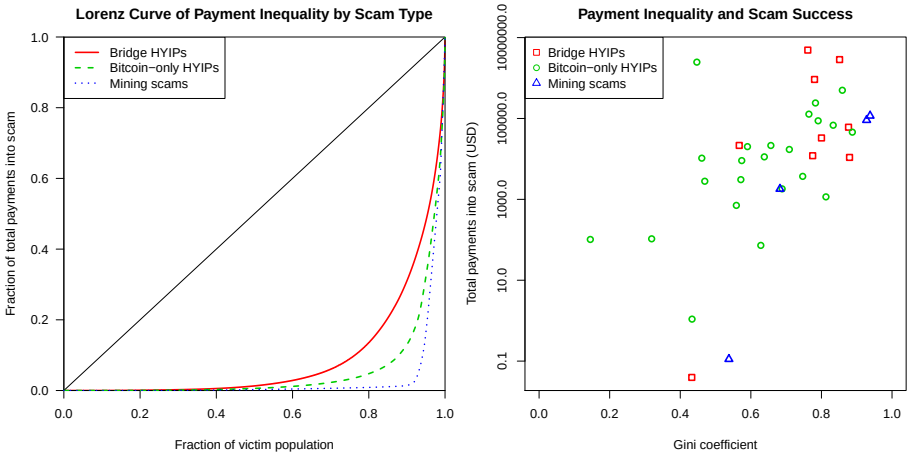

Fig. 6: Lorenz curve for total payments into scam categories (left); scatter plot comparing Gini coefficient to the amount of money stolen by scammers (right).

even distribution of payments into scams would indicate that scammers must recruit lots of victims who each contribute a small but substantial amount. By contrast, an uneven distribution suggests that scammers should focus on the small number of marks who will give away the vast majority of the money contributed to the scheme.

To answer this question, we compute measurements typically used in assessing income inequality. Figure 5 plots Lorenz curves for each of the HYIP scams we identified. Perfect equality would be indicated by a diagonal line with slope equal to 1, while curves appearing further down and to the right indicate greater inequality in payments from address groups. The left graph plots Bridge HYIPs while the right plots Bitcoin-only Ponzis. We see considerable variation, but with a small number of victims contributing much of the payments in most cases. For instance, in Leancy approximately 20% of the victim population contributed 90% of the payments to scammers. We see even greater variation in the Bitcoin-only HYIPs.

Next, we consider variations across scam categories. Figure 6 (left) plots the Lorenz curves for all payments into the 3 scam categories. Payments into mining scams are the most skewed: nearly all of the total contributions come from less than 10% of the victims. While still very skewed, Bridge HYIPs rely on contributions from more victims than do the Bitcoin-only HYIPs: the smallest 80% of address groups account for around 5% of the scammer's haul for Bitcoin-only HYIPs, compared to 15% for Bridge HYIPs.

Figure 6 (right) examines the relationship between inequality of payments into scams and the total money drawn into the scams. The graph plots the Gini coefficient for each scam (where 0 indicates all incoming payments are equal and 1 indicates complete inequality) against the total payments paid into each scam. We can see that the least successful scams tend to be the most equal, whereas the most successful scams are more unequal. Hence, for a scam to be successful, it appears that it must catch the few "big fish" who will pay the bulk of the money into the scam.

The high concentration in payment size into scams has implications for law enforcement actions against the scammers. Most successful scams have a few big contributors, who might be more willing to assist with in an investigation. Furthermore, the individual losses suffered by these victims are more likely to meet the threshold required to get the attention of high-tech crime units.

7.3 Policy Options

We have already established that different types of Bitcoin scams exist, and that many are growing in popularity. But there are many issues with Bitcoin, as well as cybercrime in general. Given that context, why might Bitcoin scams matter? Here are three plausible reasons: (i) if there are many victims, (ii) if substantial amounts of money is being lost, or (iii) if the scams undermine trust in the ecosystem.

This paper has established a lower bound on answers to the first two reasons. The number of victims and magnitude of their losses, while considerable, is substantially smaller than those afflicted by failures elsewhere in Bitcoin, such as the Mt. Gox collapse. So on the current figures alone, we cannot conclude that eradicating these scams should take priority.

However, there are two counterarguments that suggest a more robust response is warranted. First, the scams are growing substantially in popularity and profitability. Rooting out the scams at this early stage may be more feasible, and doing so we could avoid the substantial indirect costs imposed by exposing many new Bitcoin users to such a negative experience. The second counterargument is that, for the wallet and exchanges scams at least, their continued prevalence threatens to undermine trust in the overall ecosystem. If people cannot determine whether the service they are interacting with is legitimate due to an information asymmetry, then everyone in the ecosystem, even legitimate exchanges and wallets, suffers.

8 Related Work

High-yield investment programs were first documented in the research literature by Moore et al [5]. They documented over 1 000 such scams, provided a primer on the ecosystem's operation, and established that tracking websites accurately monitor the scam's operation. Neisius and Clayton also investigated HYIPs, focusing on the profits accrued by support organizations in setting up and monitoring HYIP scams [6]. Both papers focused on traditional HYIPs that have operated with impunity for several years using centralized virtual currencies such as Liberty Reserve and Perfect Money. In this paper, we have instead focused on HYIPs that use cryptocurrencies as payment. The block chain has enabled us to accurately measure, for the first time, the amount of money transferred into HYIPs by victims and out by the scam operators.

Huang et. al consider Bitcoin mining malware and quantify the amount of bitcoin that Bitcoin mining botnets have minted using the block chain [8]. Our paper does not consider malware, but our block chain analysis techniques are similar to those of Huang et. al. (as well as Meiklejohn et. al and Ron and Shamir [9–11]). Vasek et. al. examine the prevalence of denial-of-service attacks against Bitcoin services [12]. These

attacks are another avenue for criminals to profit as well as another threat to Bitcoin's success. Möser et al systematically analyze Bitcoin mixing services, which some of the scams we study purport to be [13]. Christin measures transactions made on the Silk Road, a large online marketplace that was shut down by the US federal government, and finds over 1.2 million dollars in sales monthly, despite (or because of?) the purported anonymity of the marketplace [14]. While the Silk Road is not a scam (though we do not doubt that there were scammers abusing the service), it has certainly harmed Bitcoin's reputation, much like the scams we study might if they became more prevalent. Moore and Christin studied how often and why Bitcoin-currency exchanges collapsed [15]. While in this paper we investigated fraudulent exchanges set up to steal customer deposits, Moore and Christin focused on legitimate exchanges that shut down. While some label such failed exchanges as scams, particularly when they are unable to return outstanding customer deposits, we exclude them from consideration here.

The Bitcoin Foundation surveyed prominent Bitcoin participants about different hypotheticals that could affect the Bitcoin ecosystem [16]. While they did not explicitly ask about Bitcoin scams, they found that mismanaged Bitcoin businesses was a top threat to Bitcoin's success. They also found people feared Bitcoin getting a "bad reputation" for being a haven for wicked behavior. This includes a concern over Bitcoin being used for gambling (e.g., many Bitcoin-only HYIPs). The scams presented in this paper doubtless could harm Bitcoin's reputation if they are not eradicated.

9 Concluding Remarks

Scams – operations established with fraudulent intent – pose serious dangers to the Bitcoin ecosystem. First, there is the direct harm imposed on the victims who pass money to the scammers, never to see it again. Second, and perhaps more substantially, there is indirect harm imposed on all users, even those who don't fall victim to scams. This harm manifests in damage to the reputation of legitimate operations and the undermined trust of users who become more reticent to try out new services.

Fortunately, the block chain creates an opportunity in that transactions may often be tracked, which could make it easier to assess the true risk posed by scams and make it harder for scammers to hide. To that end, in this paper we have presented the first systematic, empirical analysis of Bitcoin scams. We identified four categories of scams: Ponzi schemes, mining scams, scam wallets and fraudulent exchanges. By analyzing transactions into and out of 42 such scams, we estimate that approximately $11 million has been contributed to scams by at least 13 000 victims, much of it within the past year.

We found that Bridge HYIPs, an established scam that predates Bitcoin, take in 60% of the total revenue. The block chain has enabled us to more accurately estimate the financial success of these scams than in previous work, by directly measuring money flowing into HYIPs for the first time. We also worry that the other scam categories may soon rise to the level of HYIPs as scammers wise up to what is possible.

To combat any future rise, continued measurement of the threat as outlined in this paper is essential. Furthermore, by investigating losses from victims contributing the largest amounts, there may be an opportunity for law enforcement to crack down on scams more effectively.

Acknowledgments

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. T. Standage, *The Victorian Internet*. Walker & Company, 1998.
2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.
3. znort987, "blockparser," https://github.com/znort987/blockparser.
4. G. Maxwell, "CoinJoin: Bitcoin privacy for the real world," https://bitcointalk.org/index.php?topic=279249. Last accessed 29 August 2014.
5. T. Moore, J. Han, and R. Clayton, "The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, vol. 7397. Springer, 2012, pp. 41–56.
6. J. Neisius and R. Clayton, "Orchestrated crime: The high yield investment fraud ecosystem," in *Proceedings of the Eighth APWG eCrime Researcher's Summit*, Birmingham, AL, Sep. 2014.
7. Securities and Exchange Commission, "SEC v. Trendon T. Shavers, et al," http://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.
8. D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko, "Botcoin: Monetizing stolen cycles," in *Proceedings of the Network and Distributed System Security Symposium*, 2014.
9. 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 Internet Measurement Conference*. ACM, 2013, pp. 127–140.
10. D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science. Springer, 2013, vol. 7859, pp. 6–24.
11. ——, "How did Dread Pirate Roberts acquire and protect his Bitcoin wealth?" in *1st Workshop on Bitcoin Research*, ser. Lecture Notes in Computer Science, vol. 8438. Springer, March 2014.
12. M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of Denial-of-Service attacks in the Bitcoin ecosystem," in *1st Workshop on Bitcoin Research*, ser. Lecture Notes in Computer Science, vol. 8438. Springer, March 2014.
13. M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in *Proceedings of the Seventh APWG eCrime Researcher's Summit*. IEEE, 2013, pp. 1–14.
14. N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213–224.
15. T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, vol. 7859. Springer, Apr. 2013, pp. 25–33.

16. Bitcoin Foundation, "Removing impediments to Bitcoin's success: A risk management study," 2014, https://bitcoinfoundation.org/static/2014/04/Bitcoin-Risk-Management-Study-Spring-2014.pdf.