

Measuring Bitcoin-based Cybercrime

Marie Vasek
Dissertation Defense
29 March 2016

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - **Ch. 2 - Bitcoin Primer (covered in proposal)**
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Bitcoin

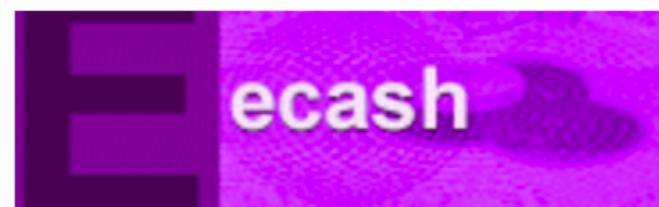
- Bitcoin is a **public, digital, decentralized** currency.
- Public
 - Every transaction (past or current) can be read by anybody.
- Digital
 - There are no bills, only bits to represent transactions.
- Decentralized
 - Bitcoins are mined, not minted, by a collection of actors, not a central bank.
 - Anybody can create an account and receive bitcoin.
 - Anybody can try to mine bitcoin.
 - Rules are set by computer code and changed upon a consensus of the actors.



welcome

to the DigiCash Webserver

numbers that are money ...



This server supports [keyword search](#).

We welcome your [electronic feedback](#) about our server!



We support the [Golden Key campaign of the Internet Privacy Coalition](#).



[LibertyGuard](#)
[Services](#) new!
[Service Fees](#)
[Buy/Sell LR](#)
[Merchants](#)
[Downloads](#)
[Consumer Alert](#)
[Credit Card Funding](#) new!



Featured Merchants

[Marketiva.com](#) — Popular Forex company!

[Instaforex.com](#) — Award winning forex.

[Masterforex.org](#) — Award winning forex.

Featured Exchange Services

[wm-center.com](#) (English, Russian) — Fast and reliable service 24/7.

[e-Naira.com](#) (English) — Reputable exchanger located in Africa.

[ExchangeZone.com](#) (English)

Wholesale Exchange Services

[eCardOne.com](#) (English, Italian, Spanish, German, Czech) — Authorized reseller, official debit card provider

[SwiftExchanger.com](#) (English) — Official Liberty Reserve merchant wholesaler

Quick Payments

An easy access to your funds to make payments quickly.

This feature allows you to make quick payments without accessing your main Liberty Reserve account. Just set daily, weekly or monthly limit of funds you wish to use for handy Quick Payments and do transfers to your partners quickly and safely.

Live Chat

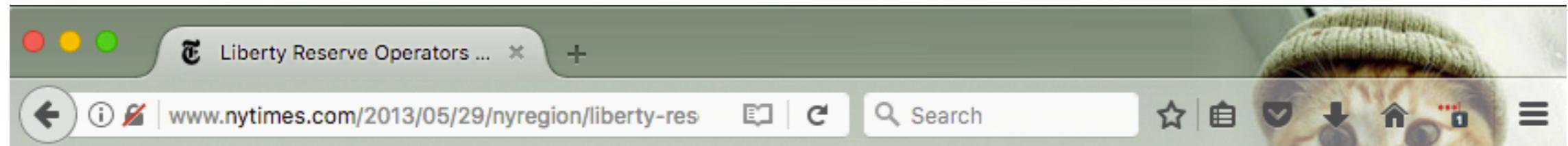
Have questions? Liberty Reserve provides personal, live, one-to-one chat with a customer support representative to answer your questions. No more waiting hours or days to get a simple question answered. Our representatives can also push a URL onto your computer as a pop-up so that you do not have to go looking for a particular link.

You can also get the chat history automatically emailed to you!



[SCI/API Guides](#)

[FAQ](#)



≡ SECTIONS

THE NEW YORK TIMES

The New York Times

SUBSCRIBE

LOG IN



N.Y. / REGION

Online Currency Exchange Accused of Laundering \$6 Billion

By MARC SANTORA, WILLIAM K. RASHBAUM and
NICOLE PERLROTH MAY 28, 2013



The operators of a global currency exchange ran a \$6 billion money-laundering operation online, a central hub for criminals trafficking in everything from stolen identities to child pornography, federal prosecutors in New York said on Tuesday.

Why Scammers Use Bitcoin

- Lower fees (more profit for criminals)
- Large userbase (compared to other digital currencies)
- Easy to get (can exchange Bitcoin for cash on the street)
- Distributed system (no Bank of Bitcoin to forcibly shut down)
- Less direct regulatory oversight (anti-money laundering efforts only on some endpoints)

I use the public nature of Bitcoin to directly measure cybercrime.

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - **Research Questions (covered in proposal)**
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Security Economics

- Security economics literature has identified several key reasons for security failure:
 - incentives: profit motivated attackers [Ch. 3-6]
 - information asymmetries: hard to ascertain whether service is legitimate or not [Ch. 4-5]
 - externalities: when harm is directed elsewhere; DDoS attacks [Ch. 3]; can't trust the ecosystem [Ch. 4]

Cybercrime Measurement

- Large body of research on improving understanding of how cybercriminals operate so that we might more effectively dismantle their networks:
 - DDoS attacks: existing work measuring, categorizing DDoS attacks
 - HYIPs: Moore et al. monitored over 1000 scams and estimated their profits using inferred approximations
 - Passwords: existing work on password dumps, which passwords are being used, frequency of password use
- This thesis contributes to the knowledge on these threats by studying their prevalence in the Bitcoin ecosystem

Publications

- In dissertation:
 - [Ch 6] **Marie Vasek**, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore. "The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets". In Financial Cryptography and Data Security, February 2016.
 - [Ch 4] **Marie Vasek** and Tyler Moore. "There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams". In Financial Cryptography and Data Security, January 2015.
 - [Ch 3] **Marie Vasek**, Micah Thornton, and Tyler Moore. "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem". In 1st Workshop on Bitcoin Research, March 2014.
- Other publications:
 - **Marie Vasek**, Matthew Weeden, and Tyler Moore. "Measuring the Impact of Sharing Abuse Data with Web Hosting Providers". In 3rd ACM Workshop on Information Sharing and Collaborative Security, October 2016.
 - **Marie Vasek**, John Wadleigh, and Tyler Moore. "Hacking is not Random: A Case-Control Study of Webserver-Compromise Risk". In IEEE Transactions on Dependable and Secure Computing, 13(2):206-219, 2016.
 - **Marie Vasek** and Tyler Moore. "Identifying Risk Factors for Webserver Compromise". In Financial Cryptography and Data Security, March 2014.
 - Benjamin Johnson, Aron Laska, Jens Grossklags, **Marie Vasek**, and Tyler Moore. "Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools". In 1st Workshop on Bitcoin Research, March 2014.
 - **Marie Vasek** and Tyler Moore. "Empirical Analysis of Factors Affecting Malware URL Detection". In 8th APWG eCrime Researchers Summit (eCrime), September 2013.
 - **Marie Vasek** and Tyler Moore. "Do Malware Reports Expedite Cleanup? An Experimental Study". In 5th USENIX Workshop on Cyber Security Experimentation and Test (CSET), Berkeley, CA, August 2012.

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - **Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)**
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Research Contributions

- Method to collect cybercrime data:
 - Inferring DDoS attacks from user reports
 - Reliable estimation of attack targets and date
- Analysis of gathered data:
 - Summary statistics of prevalence over time
 - Quantifying impact of attacks (on mining pools and exchanges)

Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem

Topic: BTC GUILD Down because of DDOS Attack (Read 1611 times)



BTC GUILD Down because of DDOS Attack

July 05, 2011, 02:02:53 PM

BTC Guild down because of ddos attack?

can someone from BTC Guild let us know whats going on, please?

Author

Topic: 2012-09-15 walletbit.com - WalletBit Under DDOS - 1000BTC Demanded (Read 518 times)

Kris

Donator

Hero Member



Activity: 645

2012-09-15 walletbit.com - WalletBit Under DDOS - 1000BTC Demanded

#1

September 21, 2012, 05:13:46 PM

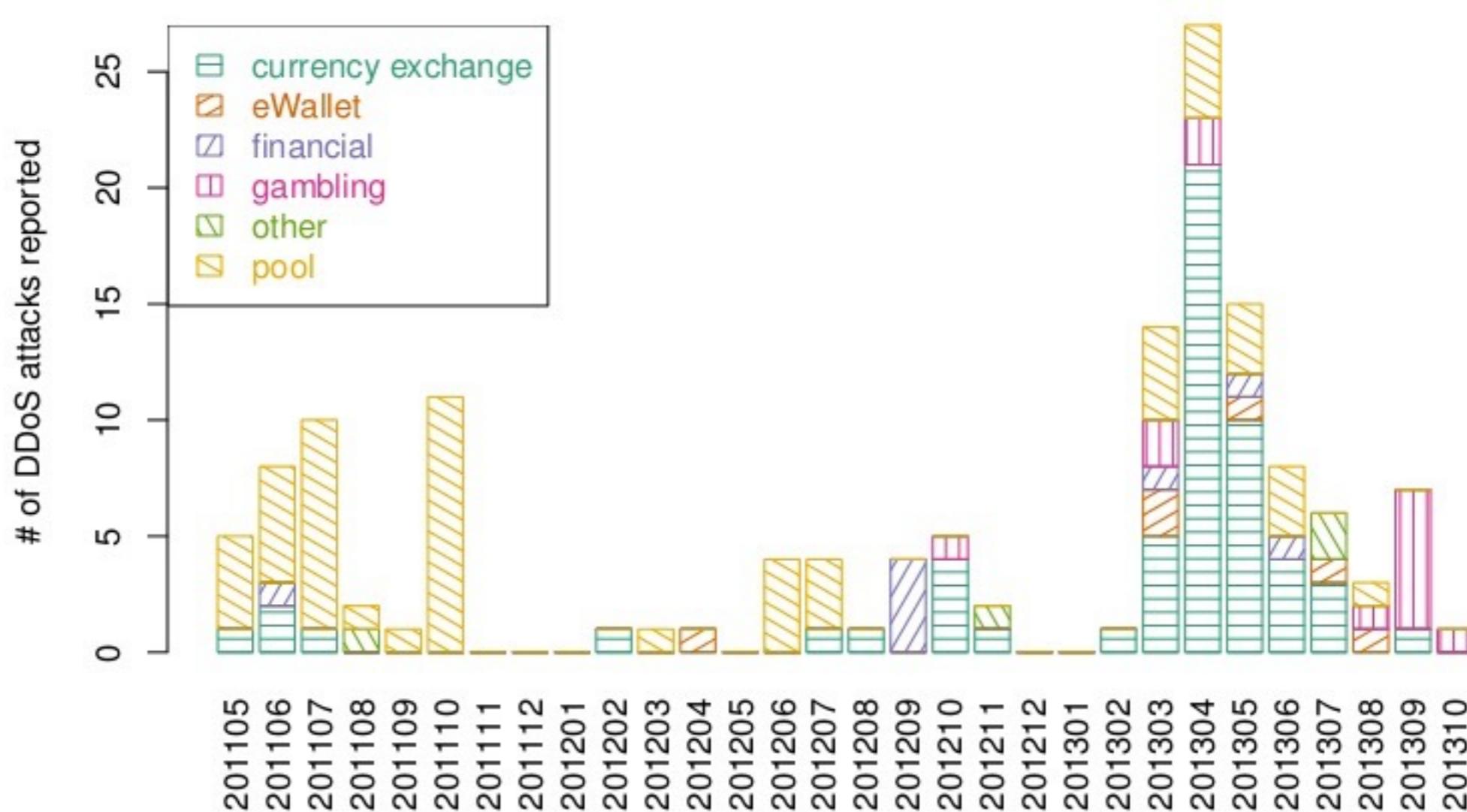
Quote

The WalletBit website and service came under DDOS attack on September 15, 2012, completely disabling the services as of around 9:00 PM GMT.



Source: <http://bitcoinmagazine.net/walletbit-under-ddos-1000btc-demanded/>

Reported DDoS over time by category



Chapter 3 Conclusions

- Developed methodology for measuring DDoS on Bitcoin services
- Found circumstantial evidence for profit-motivated DDoS attacks on the Bitcoin ecosystem
- Data produced for this chapter already used by other researchers to advance understanding of DDoS impact
 - Feder et al. (WEIS 2016) found that the distribution of the daily trading volume at Mt. Gox becomes less skewed (fewer big trades) after DDoS attacks

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - **Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)**
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Research Contributions

- Method to collect cybercrime data:
 - Find candidate scams using aggregated defender data
 - Confirm scams through manual inspection
 - Measure money in/out of scams using data from the public Bitcoin blockchain
- Analysis of gathered data:
 - Construct taxonomy of scam categories and document prevalence and revenues
 - Provide first longitudinal analysis of HYIP cash flows and victim losses

Measuring the Profits of Bitcoin Scams

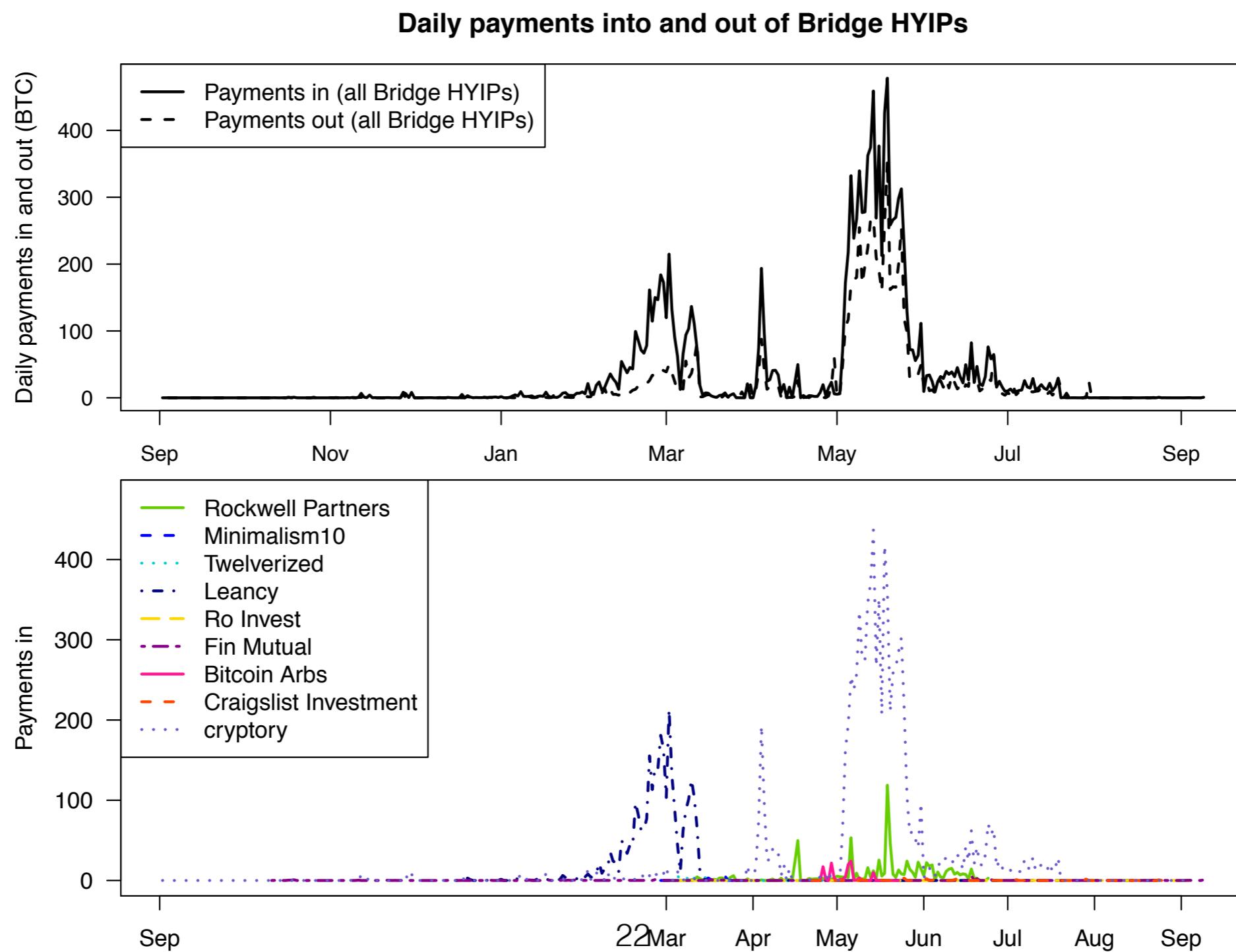
Screenshot of a web browser showing a forum post on bitcointalk.org about a Bitcoin scam.

The post, titled "[SCAM] Leancy Ltd - Bitcoin Investment - 150% Return & 5% Daily Interest", was made by user LeancyBTC on February 04, 2014, at 07:28:40 AM. The post contains a warning in red text: "LEANCY HAS NOT BEEN PAYING SINCE 03/11/14. NO ADMINS COULD BE REACHED. DO NOT DEPOSIT ANY FUNDS INTO LEANCY." Below the post, another user, Mivexil, responded with "Re: Leancy Ltd - Invest w/ Bitcoins 150% Yields".

The forum header includes a login form, a news banner about OpenSSL upgrades, and a navigation bar with links for Home, Help, Search, Donate, Login, and Register. The footer features an advertisement for FortuneJack.com and a note about advertising policies.

Page number 21 is visible at the bottom center of the screenshot.

Profits of Ponzi



Bitcoin Wallet Scams

The screenshot shows the homepage of EasyCoin.net. At the top left is a cartoon snail with a red rocket on its shell, carrying two gold Bitcoin coins on its antennae. To its right is the logo "EasyCoin.net" in bold, with "Your rocket fast Bitcoin wallet" in smaller text below it. To the right of the logo is a cartoon illustration of a brown sack overflowing with gold Bitcoin coins. Below the header is a navigation bar with yellow buttons: "Home", "Login", "Register", "Buy Bitcoins", and "FAQ". To the right of the navigation bar are flags for Germany and the United States. The main content area has a light orange background and contains the following text:

Welcome to EasyCoin.net Bitcoin Wallet

Now with free Bitcoin mixer, you will always get new coins back when you withdraw from your EasyCoin.net wallet!

You only pay the Bitcoin transaction fee (0.001 BTC).

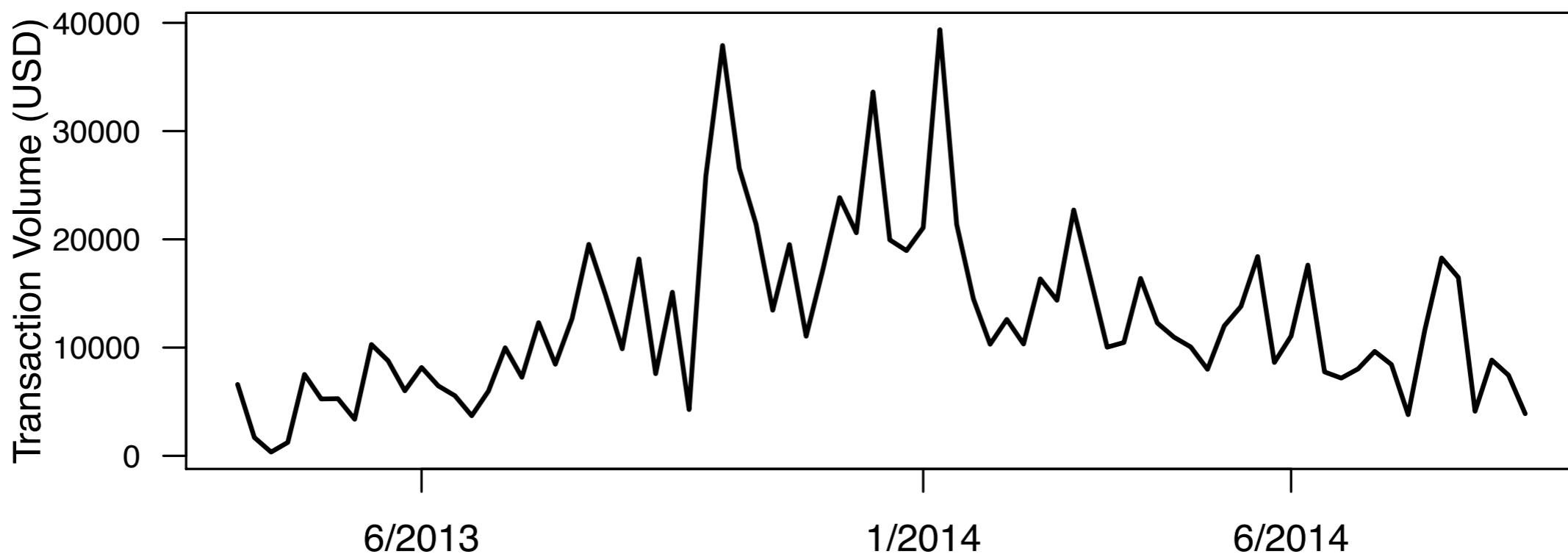
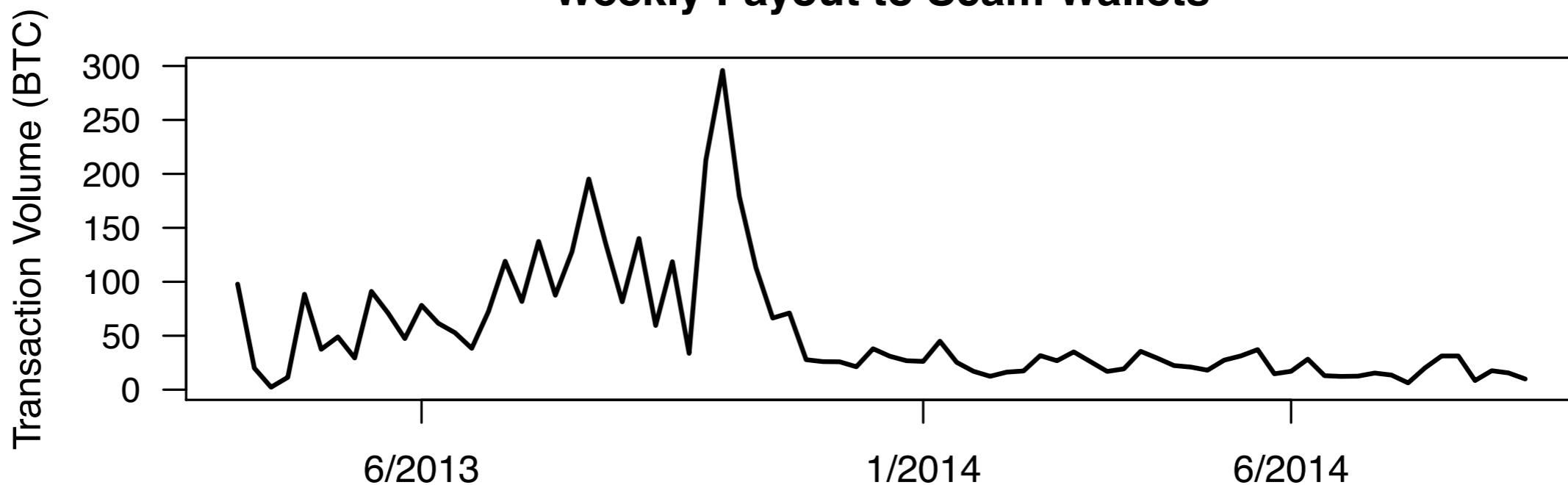
We also support completely free account to account transfers.

→ Click here to sign up now!

At the bottom of the main content area are three cartoon illustrations: a snail with a rocket on its shell, a stack of gold coins inside a safe, and another snail with a rocket on its shell.

Bitcoin Wallet Scams: Profit

Weekly Payout to Scam Wallets



Chapter 4 Conclusions

- Developed manually intensive methodology for measuring profits of Bitcoin scams
- Found \$11 million revenue over 42 scams
- Indirect harm from scams — undermine trust in the Bitcoin ecosystem

Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - **Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)**
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - Ch. 7 - Conclusions

Research Contributions

- Method to collect cybercrime data:
 - Gather candidate scam data directly from scammer advertising venues
 - Automatically confirm scams by inspecting payout mechanisms
 - For confirmed scams, collect usage, performance and demographic indicators from forum posts
- Analysis of gathered data:
 - Describe supply-side characteristics of scams, scammers
 - Describe demand-side characteristics of victims

Ch 4 and Ch 5 Differences

Ch 4	Ch 5
Identify candidate scams using aggregate defender data	Identify candidate scams using attacker advertisement sources
False positives are not scams	False positives are postings which are about gambling
Only include scams with Bitcoin addresses	Only include scams with URLs or Bitcoin addresses
Manually intensive scam identification	Semi-automated scam identification
Consider a variety of scam types	Only consider Ponzi schemes

Measuring the Supply and Demand for Bitcoin Scams



Author

Topic: GET 100X BITCOIN INVESTMENT IN 24 HOURS (Read 7402 times)

manojbashu

Newbie



Activity: 1



GET 100X BITCOIN INVESTMENT IN 24 HOURS

March 30, 2015, 04:15:31 PM

GET 100X BITCOIN INVESTMENT IN 24 HOURS

<http://bitcoin-profit.site.bz>



tech-tools

Newbie



Activity: 1



Re: GET 100X BITCOIN INVESTMENT IN 24 HOURS

November 19, 2015, 05:25:43 AM

I did sent 0.2 and I got nothing back!!!

Status: 171 confirmations

Date: 11/17/15 20:52

To: 100x 19BtphFr6kWqYyqoAmSv5d2TZ4uwH56dCd

Debit: -0.20000000 BTC

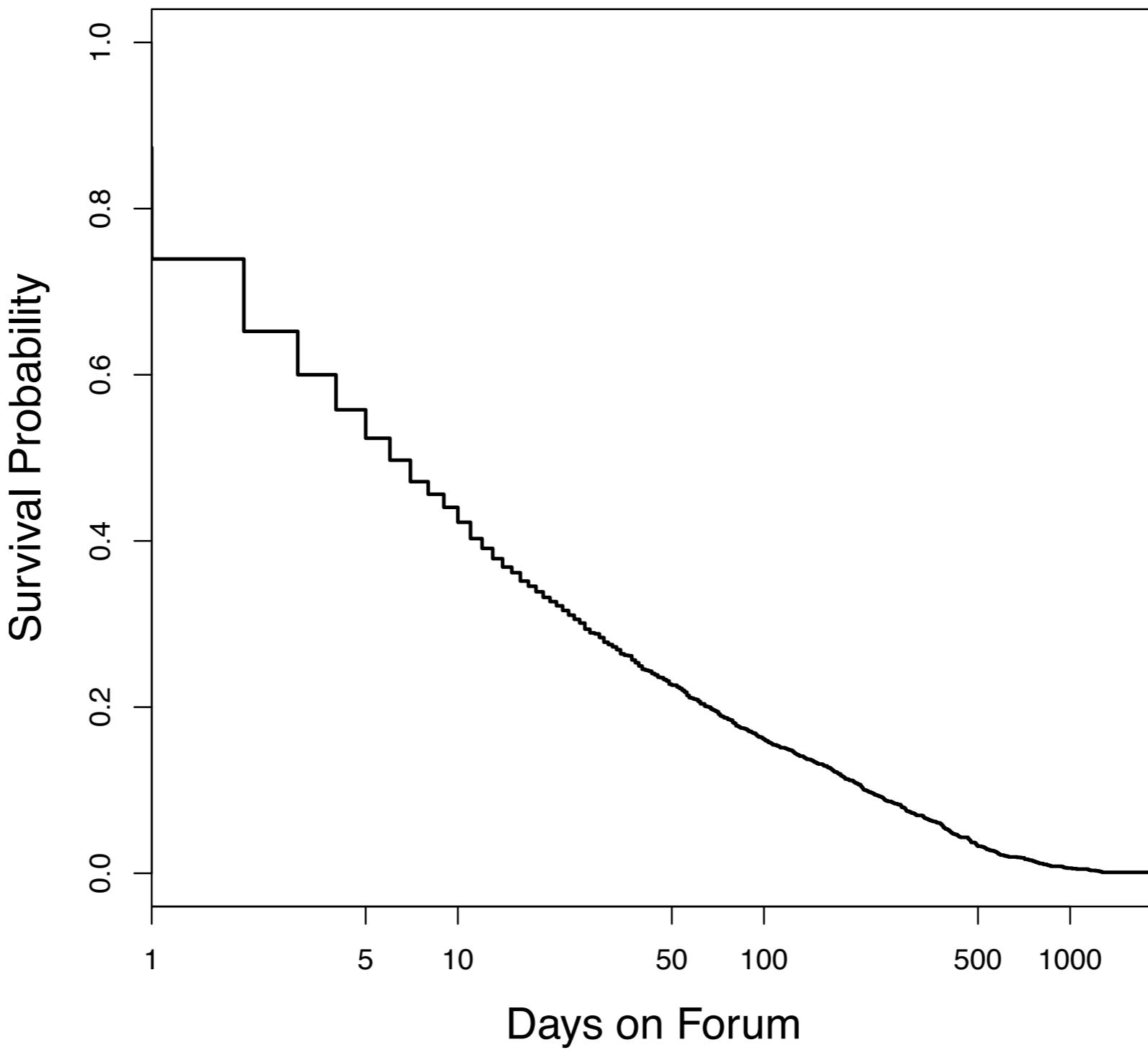
Transaction fee: -0.00004070 BTC

Net amount: -0.20004070 BTC

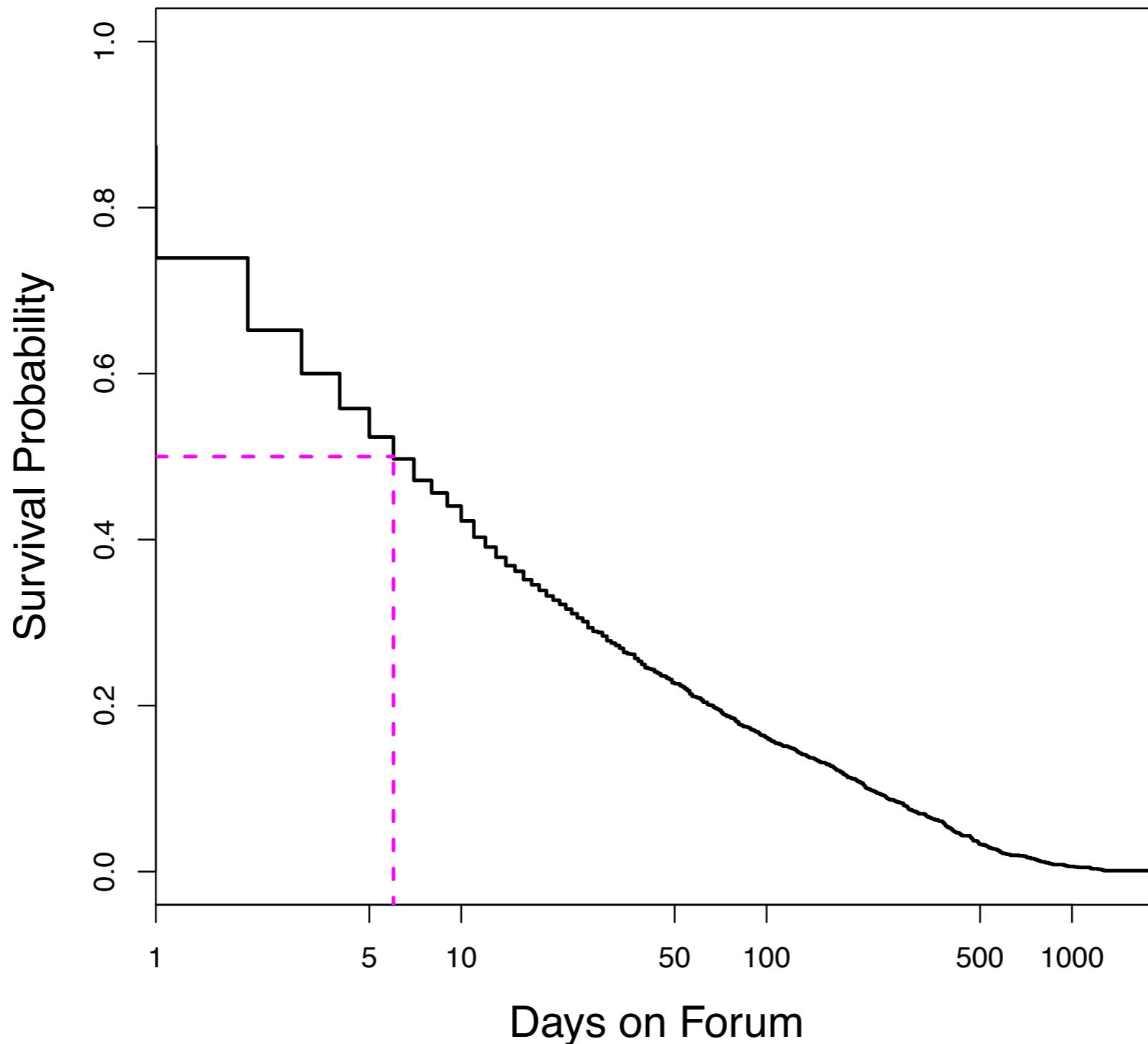
Data Collection Methodology

- Crawled 11,424 threads on the three subforums of bitcointalk.org:
 - Scam accusations
 - Gambling: Games and Rounds
 - Gambling: Investment Games
- Refined this further to find 1,780 scams advertised through 1,804 ponzi-registered domains as well as 1,448 Bitcoin addresses collated from 2,617 threads.

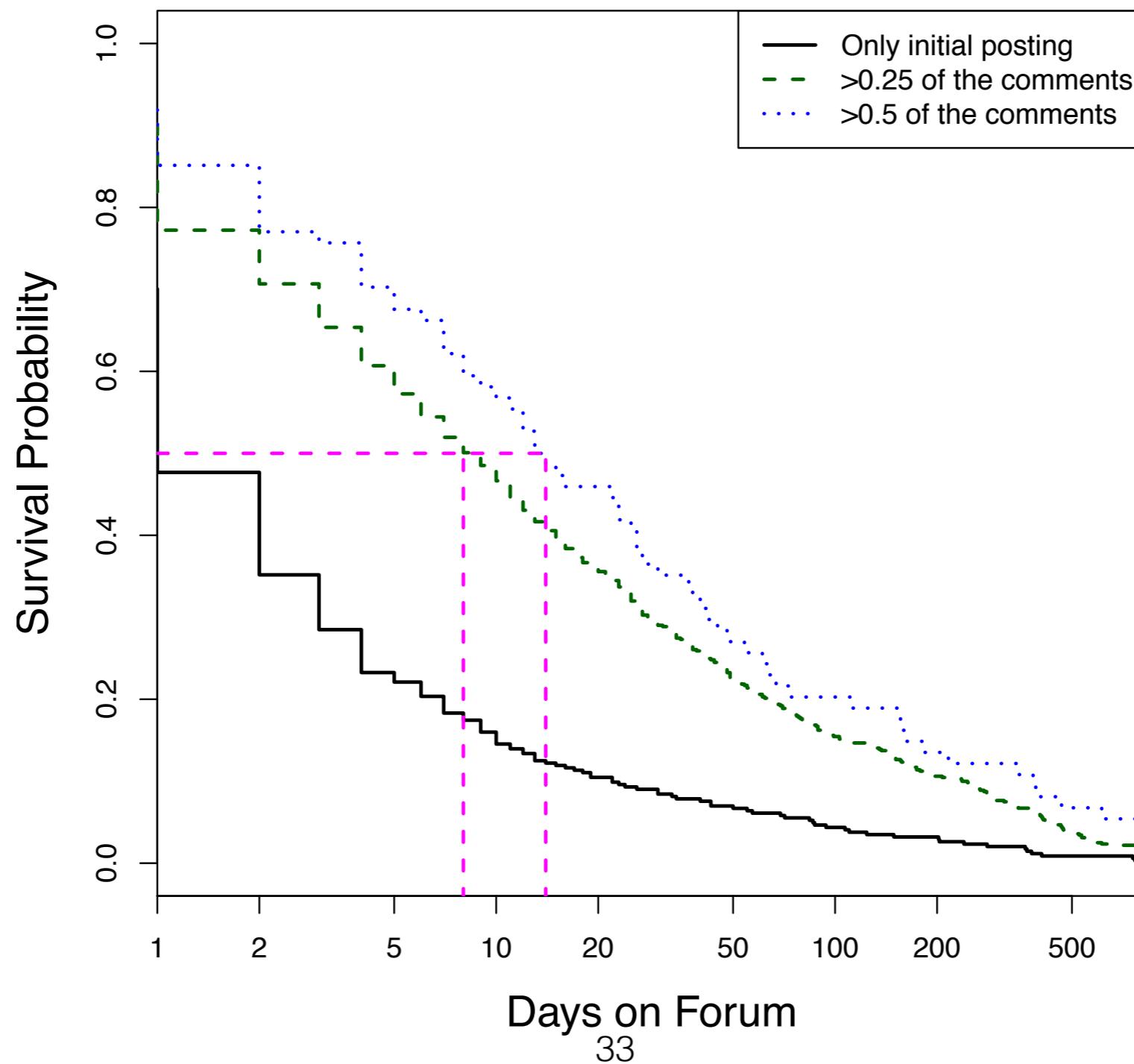
Lifetime of Scams



Lifetime of Scams



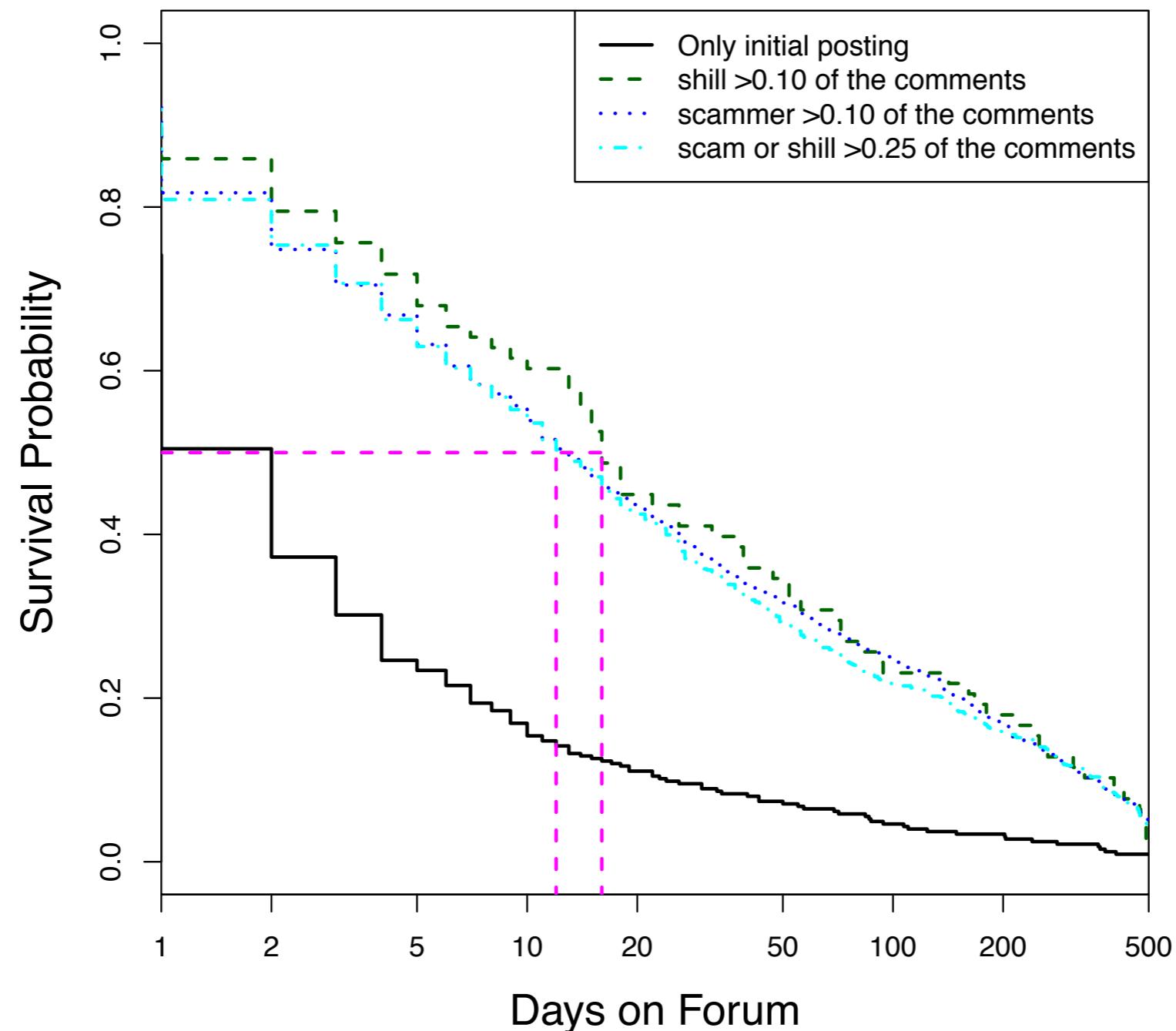
Scammer Interaction



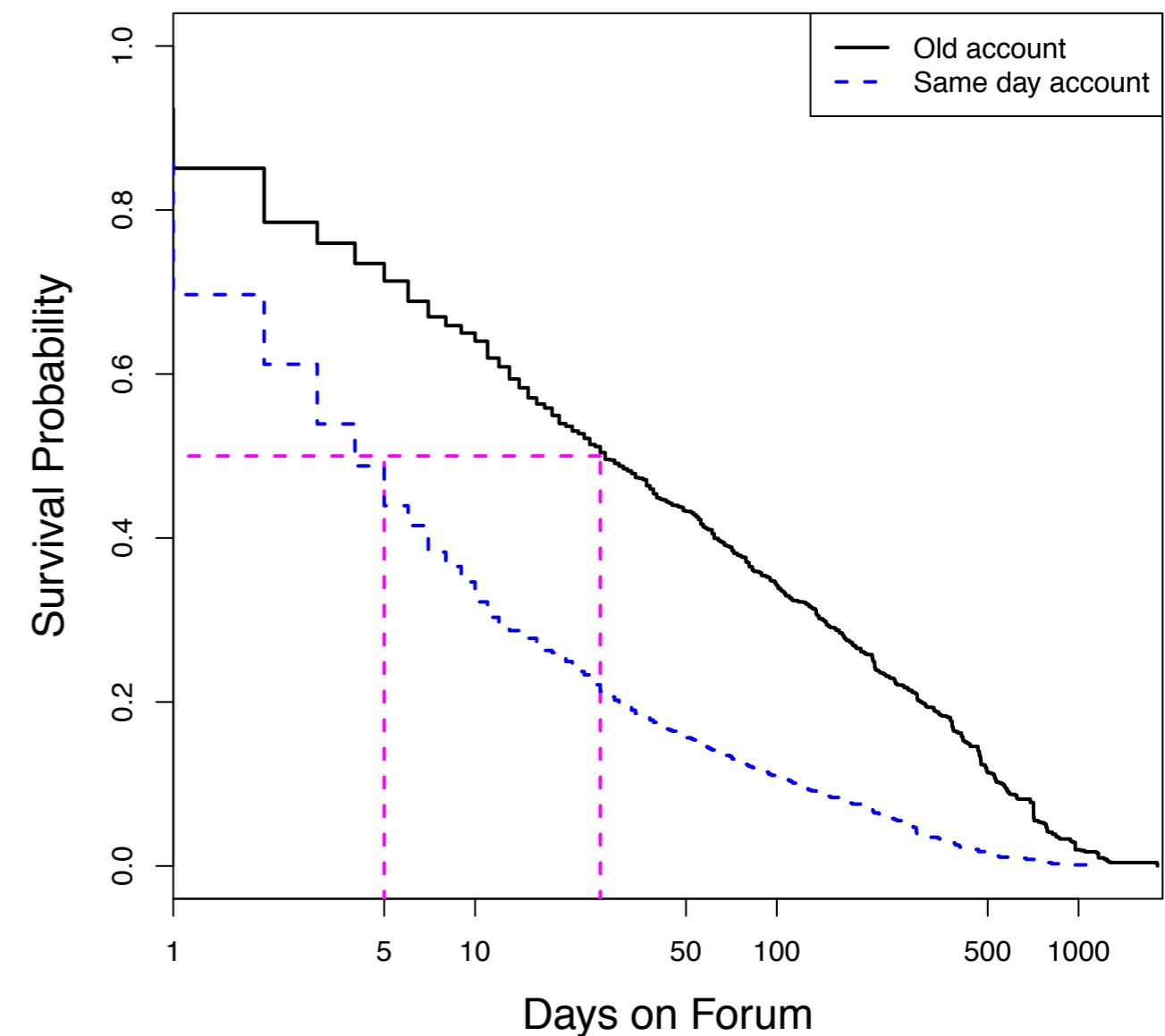
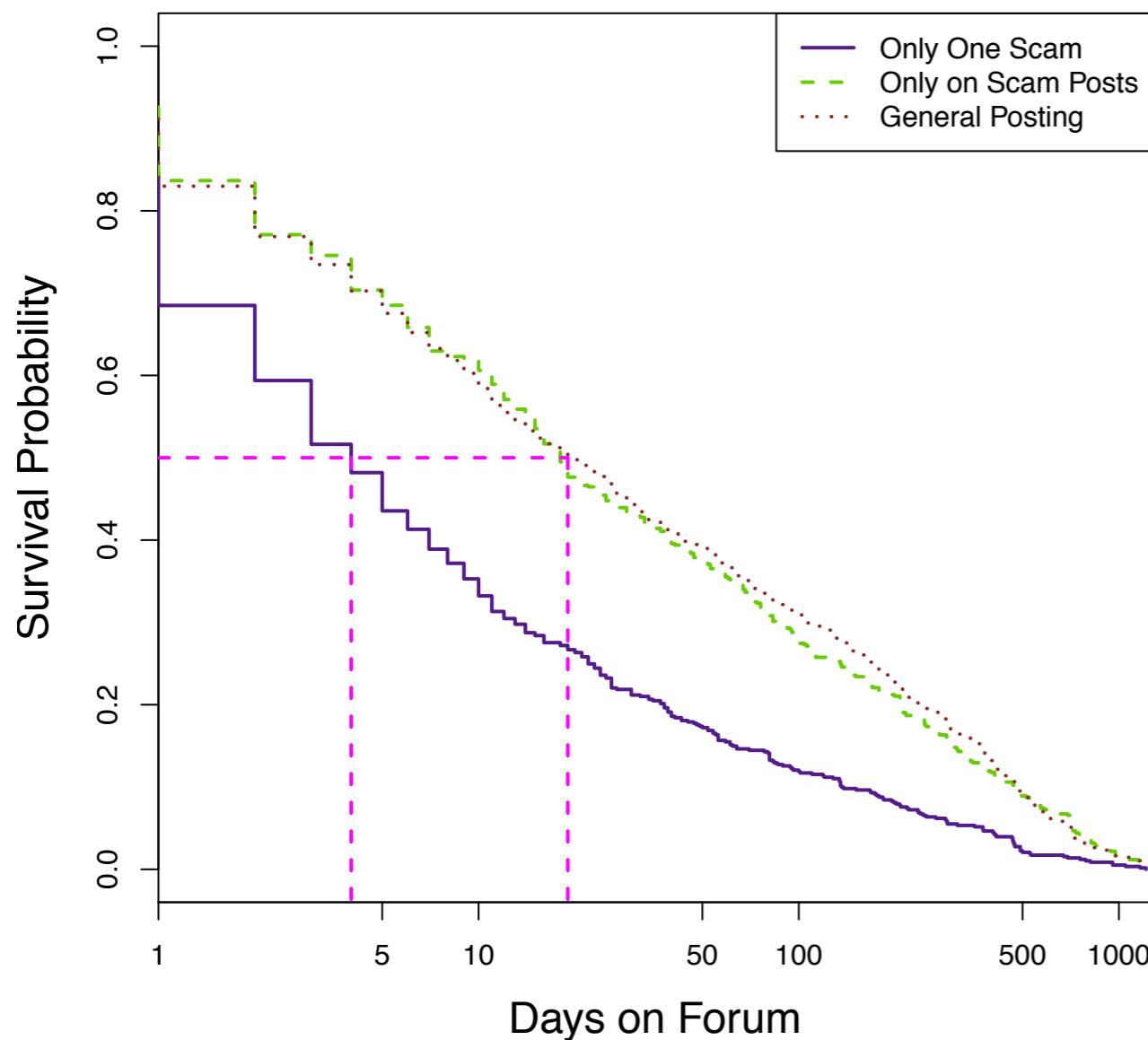
Identifying shills

- Shills: users which we believe are the attacker under a different name
- Finding ground truth on shills: manually inspect threads, look for unusually positive posters & strong but false or unverifiable information
- Use forum history (only posts about one scam) to identify most of these users

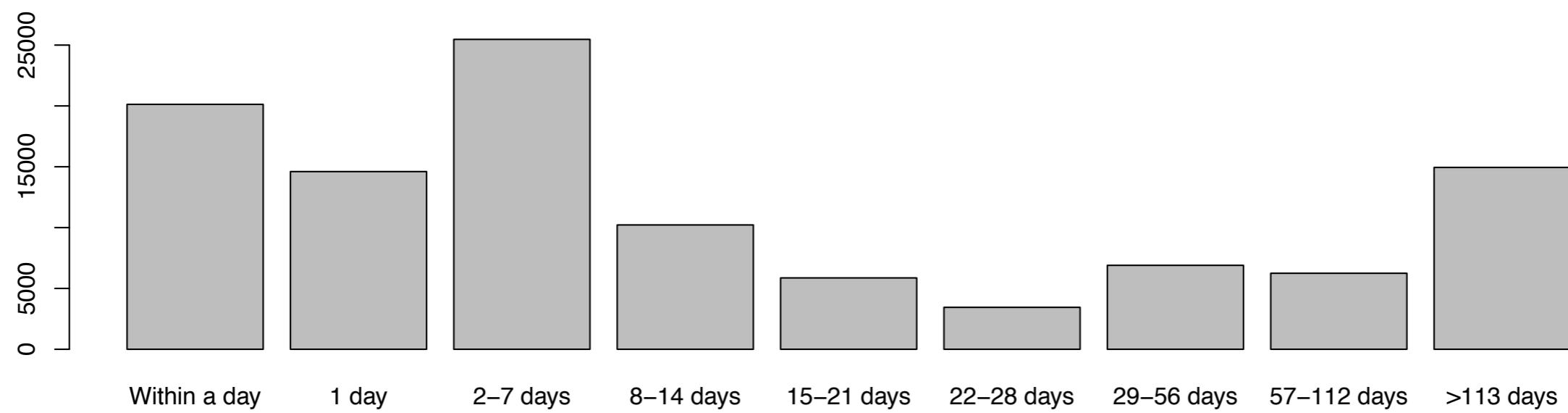
Shill Interaction



Scammer Forum History



Ponzi Victims over Time



Forum History of Ponzi Victims

Category	# Victim Posts	# Other Posts	
Altcoins (all)	32 536	5 429 022	(-)
Alternative Clients	106	54 159	(-)
Bitcoin Discussion	8 872	998 246	(+)
Development & Technical Discussion	683	162 405	(-)
Group Buys	498	84 734	
Hardware	2 730	518 728	(-)
Mining	427	1 044 148	(-)
Mining software (miners)	274	67 561	(-)
Mining speculation	616	63 071	(+)
Pools	885	177 985	(-)
Press	696	74 437	(+)
Project Development	1 526	137 245	(+)
Technical Support	586	58 952	(+)
Auctions	1 865	108 048	(+)
Collectibles	1 063	60 745	(+)
Computer hardware	1 462	118 584	(+)
Currency exchange	3 124	138 264	(+)
Digital goods	7 303	277 903	(+)
Economics	3 692	1 204 450	(-)

Forum History of Ponzi Victims

Gambling	12 070	1 297 038	(+)
Gambling discussion	5 677	340 593	(+)
Games and rounds	23 331	388 689	(+)
Goods	1 251	587 681	(-)
Investor-based games	15 402	115 454	(+)
Lending	3 230	138 108	(+)
Marketplace	517	5 372 844	(-)
Micro Earnings	3 694	144 797	(+)
Scam Accusations	4 643	116 151	(+)
Securities	1 338	202 813	
Service Announcements	2 338	288 993	(+)
Service Discussion	3 692	330 535	(+)
Services	8 528	407 342	(+)
Speculation	5 058	883 584	(-)
Trading Discussion	1 678	257 930	
Local (all)	14 932	4 454 405	(-)
Archival	1 026	147 836	
Beginners & Help	3 923	564 720	
Meta	1 960	134 319	(+)
Off-topic	8 309	563 710	(+)
Politics & Society	2 181	290 782	

Cox Proportional Hazards Model

- Lots of measurable variables seem to affect lifetime — but which variables are responsible?
- A proportional hazards model lets us disentangle the effects of various measures on **lifetime**.
 - Dependent variable: lifetime
 - Independent variables: explanatory factors

Cox Proportional Hazards Model: Independent Variables

- **daily # victim comments**
 - Number of victim comments over the lifetime of the scam.
- **daily # scammer comments**
 - Number of scammer comments over the lifetime of the scam.
- **shill has posted?**
 - True if a “shill” has posted anywhere in the thread. (30% of the time)
- **same day account**
 - True if the scammers’ bitcointalk account was registered the same day as the original post for the scam. (43% of the time)

Cox Proportional Hazards Model: Results

	coef	exp(coef)	95% CI	p value
Daily # victim comments	0.028	1.029	(1.022, 1.036)	<<0.0001
Daily # scammer comments	0.022	1.022	(1.002, 1.043)	0.034
Shill has posted?	-0.846	0.429	(0.385, 0.479)	<<0.0001
Same day account	0.374	1.1453	(1.320, 1.599)	<<0.0001

Log-rank test: $Q=4389.2$, $p<<0.0001$, $R^2 = 0.218$

Chapter 5 Conclusions

- Developed semi-automated methodology for finding Bitcoin Ponzi schemes
- Found over 1,700 of these scams, half of which end within a week of being started.
- Frequency of victim and scammer posts is negatively correlated with scam survival
- Forum history positively correlated with scam survival

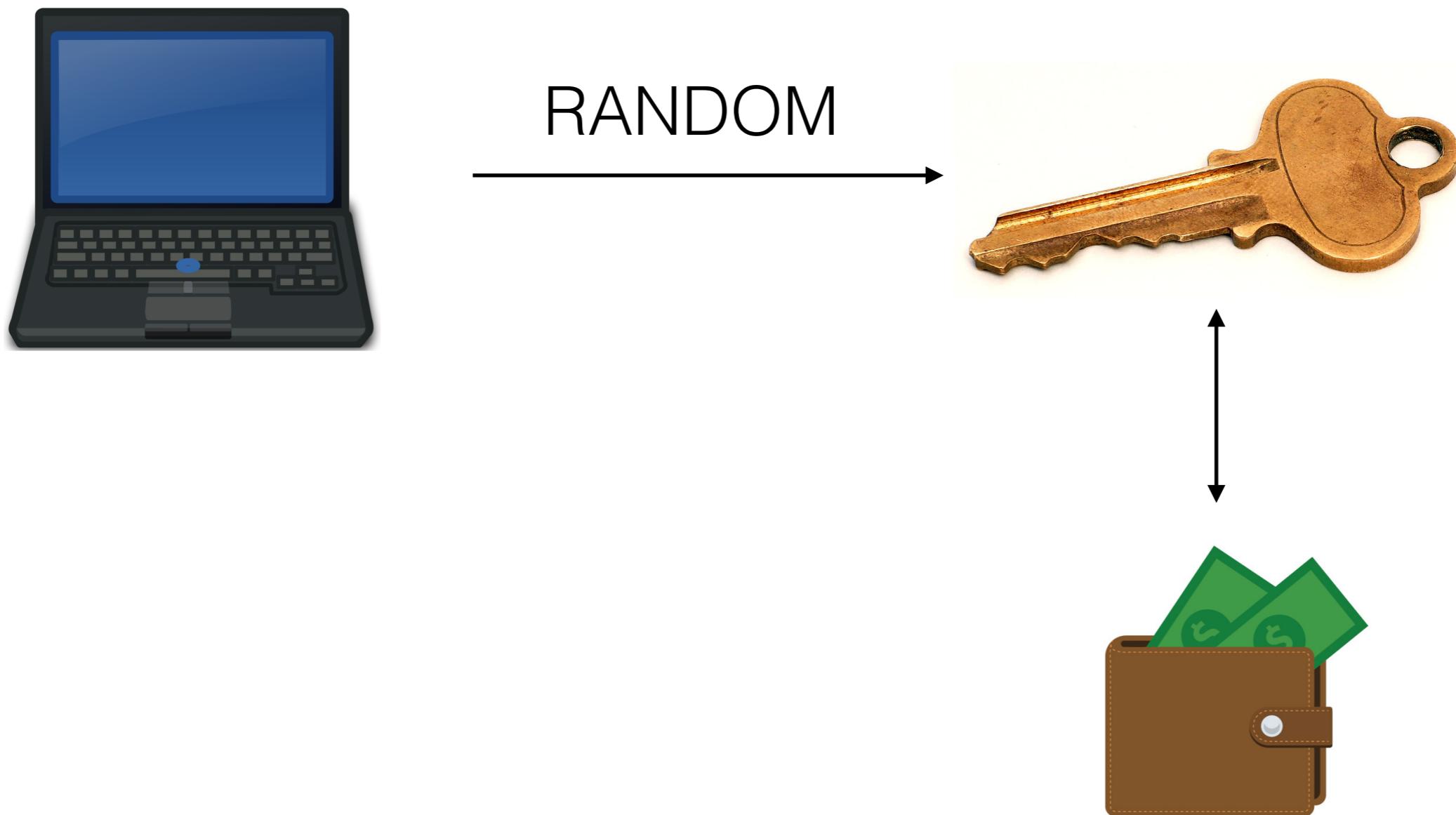
Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - **Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)**
 - Ch. 7 - Conclusions

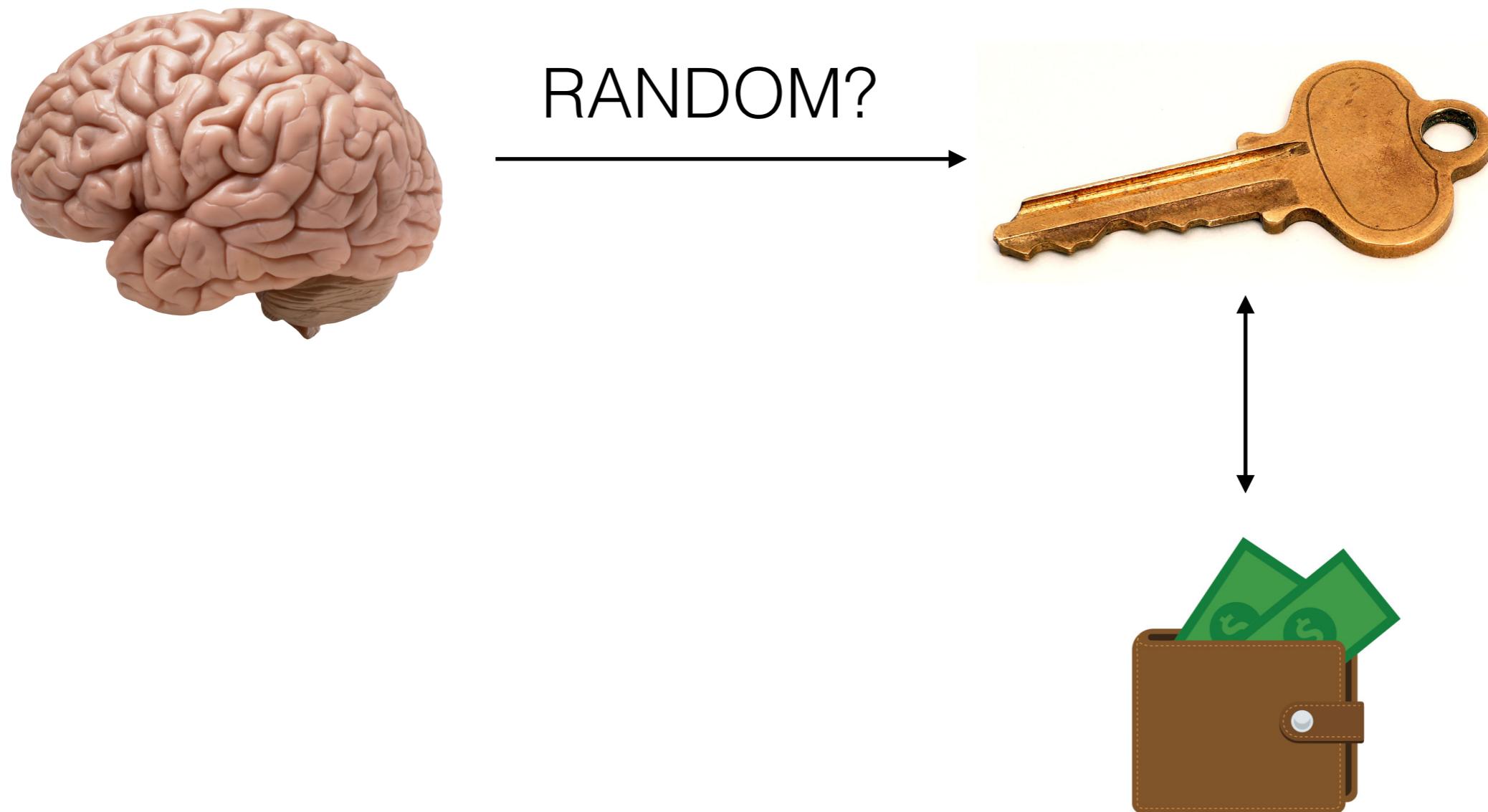
Research Contributions

- Method to collect cybercrime data:
 - Generate large corpus of candidate passwords/phrases
 - Efficiently use blockchain to study attacker draining behaviors
- Analysis of gathered data:
 - Use Bitcoin to quantify passphrase selection
 - Measure attacker draining performance using timing data

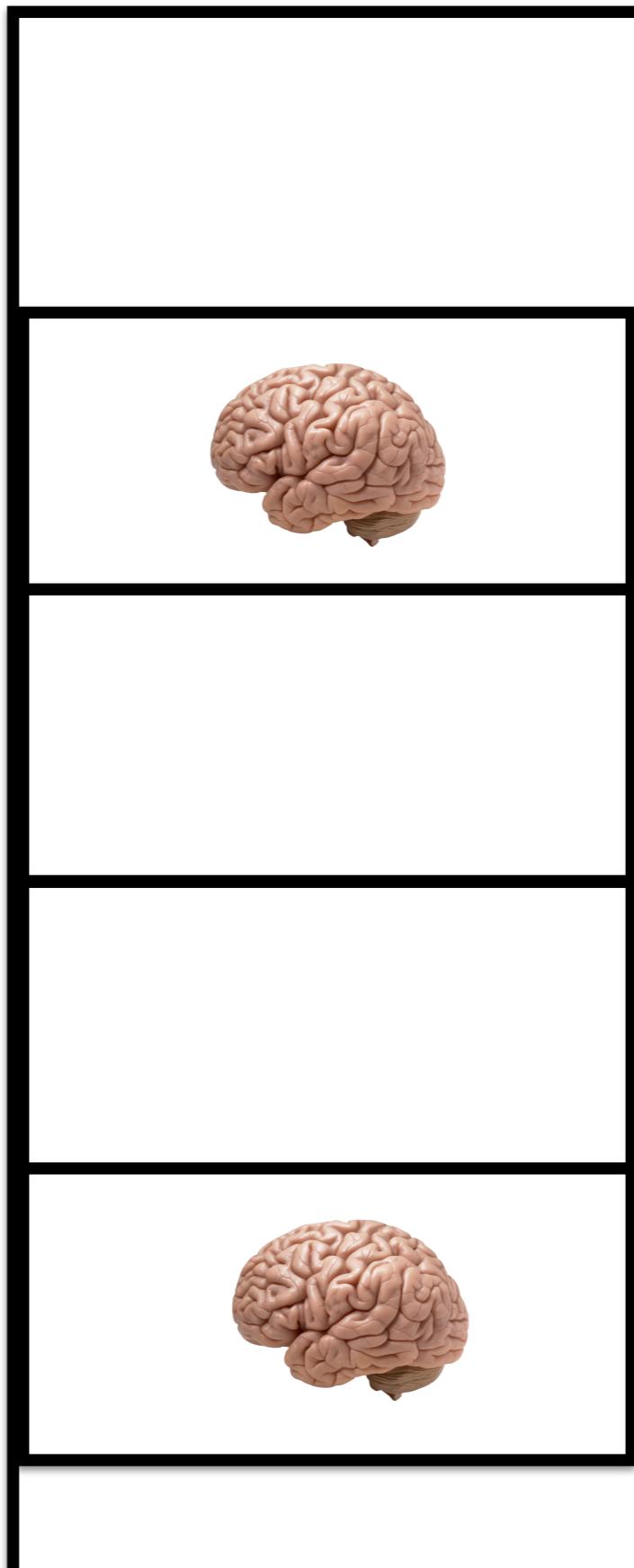
Measuring the Use and Abuse of Brain Wallets



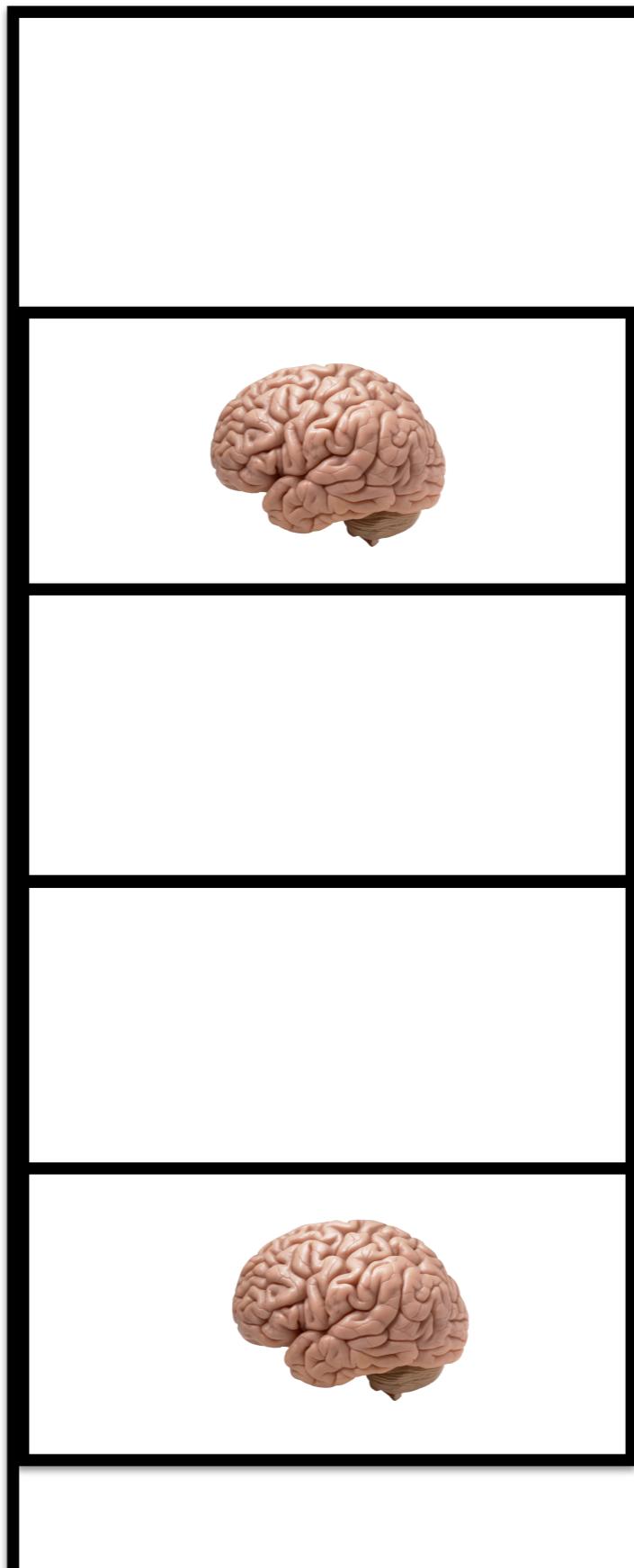
Measuring the Use and Abuse of Brain Wallets



Bitcoin Wallets: a Universal Bug Bounty

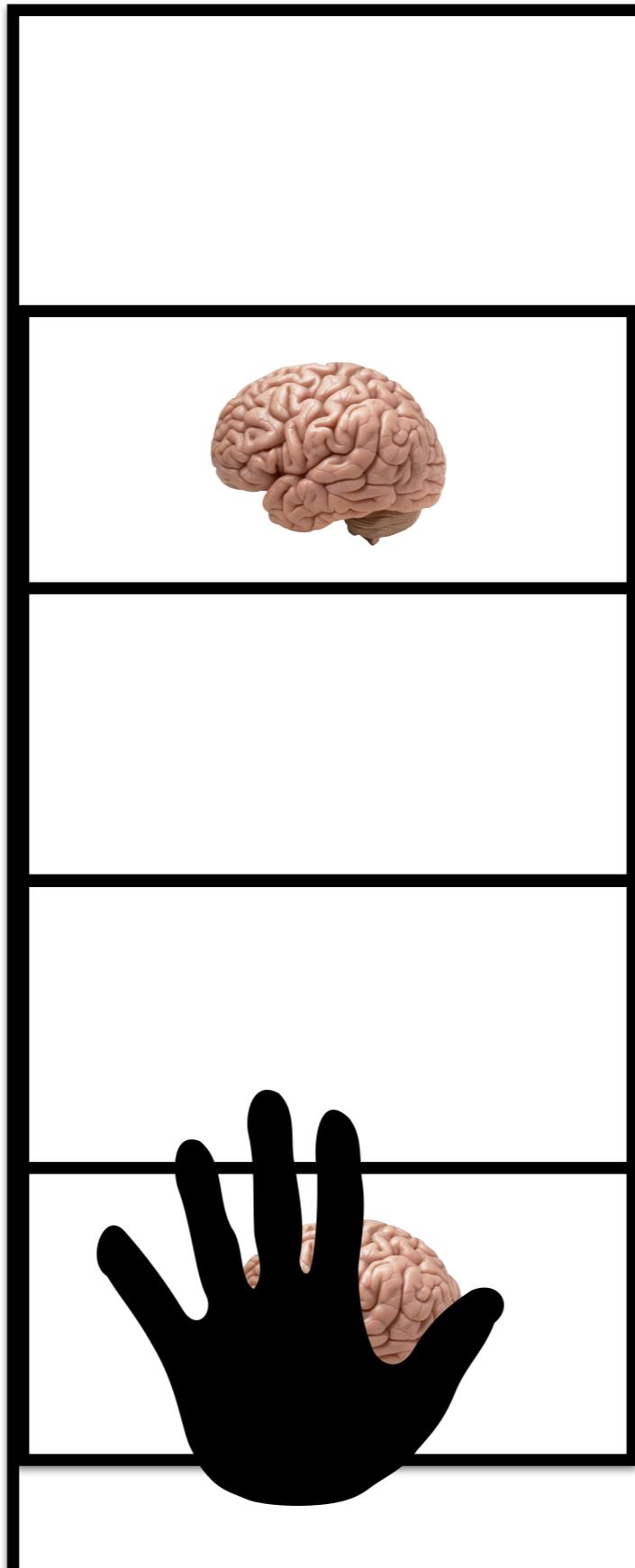


Bitcoin Wallets: a Universal Bug Bounty



“deadsheep”

Bitcoin Wallets: a Universal Bug Bounty



“deadsheep”

Measuring the Use and Abuse of Brain Wallets

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

Be careful with brain wallets, there are people sitting on the common ones! Lost 5 BTC. (self.Bitcoin)
submitted 2 years ago by swhitt

I'm not sure how many of you use brain wallets, but PLEASE be very careful messing around with them. For those of you who don't know, they are a deterministic way of generating a Bitcoin keypair using a passphrase. I read this post^[1] on Hacker News 3 weeks ago and started messing around with bitaddress.org^[2] to see if I could find any of the 1 BTC bounties. I found a few bitcents at 13w4Hn1BJQM4bjZZgYtXpyp4cioiw29tKj^[3] (I think the wallet passphrase was something simple like "satoshinakamoto" but I forgot the exact phrase) and to see if it would actually work I tried adding it into blockchain.info's wallet. Fast forward to today. I was moving some funds around^[4] and I just sent 5 BTC to the last address on my blockchain.info wallet (why on earth didn't I generate a new one?). I sent 0.1 BTC to SatoshiDICE for the hell of it and went about my business. A few minutes later, I went back to check the result of my bet and BAM. Someone had swept up my funds^[5] less than 10 minutes after I put them in there. So yes, I was an idiot and it was a very (very) expensive lesson in being careful with what addresses you send to and what brain wallet passphrases to use :(Hopefully some of you can read this and avoid a similar fate.

127 comments source hide all child comments

all 127 comments - [subscribe](#)
sorted by: best

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

[–] frequently-confused 29 points 2 years ago
I've got dibs on CorrectHorseBatteryStaple, guys.
permalink source save save-RES give gold hide child comments

[–] hvyrms 5 points 2 years ago
That's okay, my BTC is in correcthorsebatteryঠাপ্টে :)

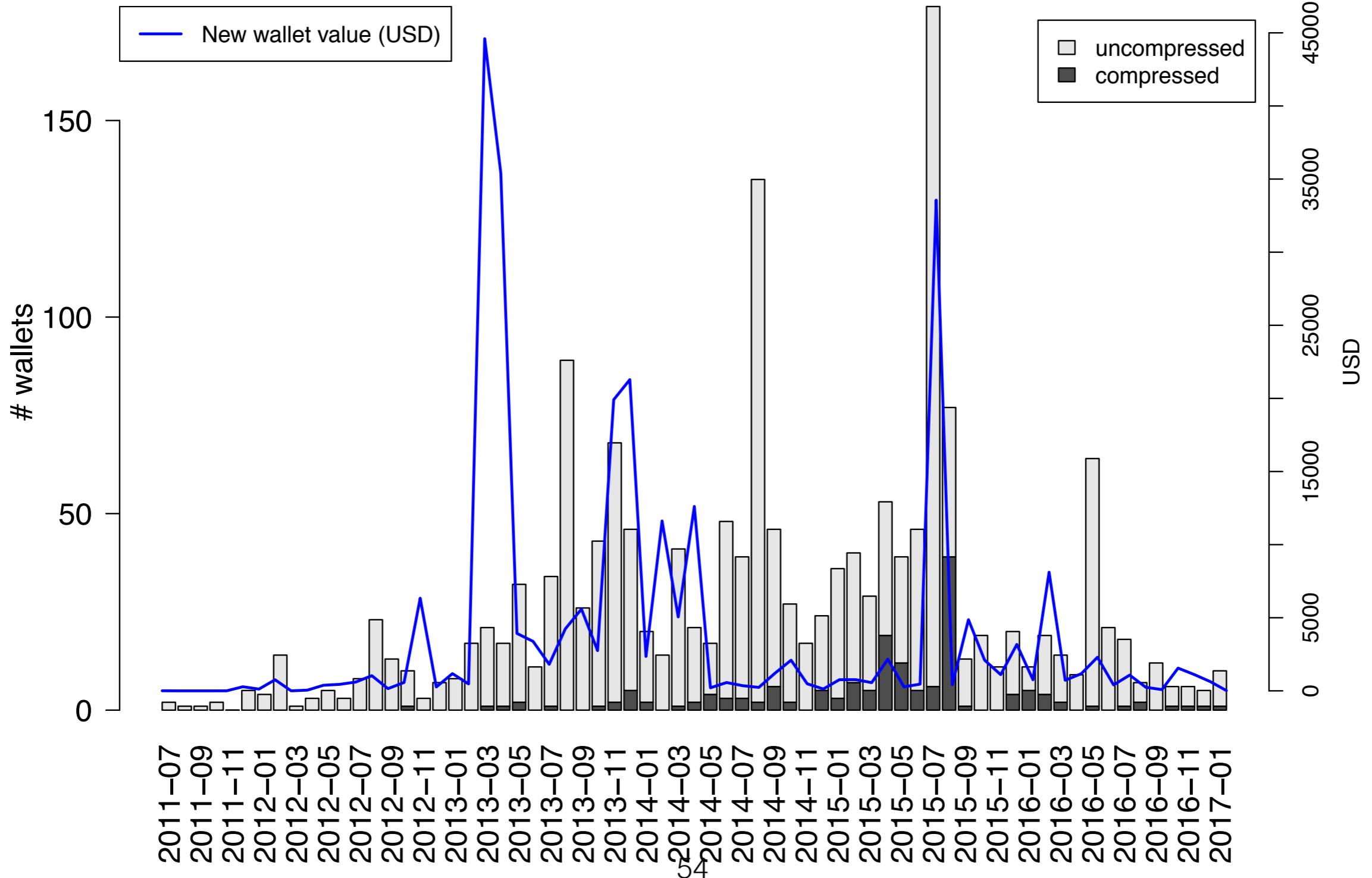
Password Corpora: 3.9 trillion Candidate Passwords

Source	# Wallets	(non-empty)	Unique	90%	# drains	Total BTC	Total USD
<i>Word lists</i>							
xkcd	155	3	8		8	126.94	8 857.49
Urban Dictionary	244	0	1		3	51.01	54 411.56
Password dumps	815	0	44		3	199.20	39 155.22
Industry lists	876	0	32		3	364.91	37 096.71
Facebook names	364	0	23		4	107.78	14 425.13
BitSig	235	0	71		8	1 586.78	63 818.81
Bitcoin IRC	454	1	17		6	777.52	25 355.79
Reddit	843	8	120		3	2 175.42	99 089.43
WikiQuote	281	0	3		7	113.60	17 700.88
BrainyQuote	61	0	0		6	85.12	14 037.94
Wiki/Brainy	83	0	0		6	101.05	14 481.48
Lyrics	438	0	17		4	270.28	19 257.41
Wikipedia	176	0	5		6	565.77	15 645.48
Openwall	456	0	0		3	60.69	14 097.56
Purdue	424	0	0		3	118.95	14 983.66
Keyboard Patterns	19	0	0		5	0.96	246.96
<i>Non-word lists</i>							
Brute Force	586	2	84		2	96.44	23 796.09
Misc	268	7	268		1	73.67	26 941.39
Overall	1 730	21	488		3	2 846.23	260 792.30

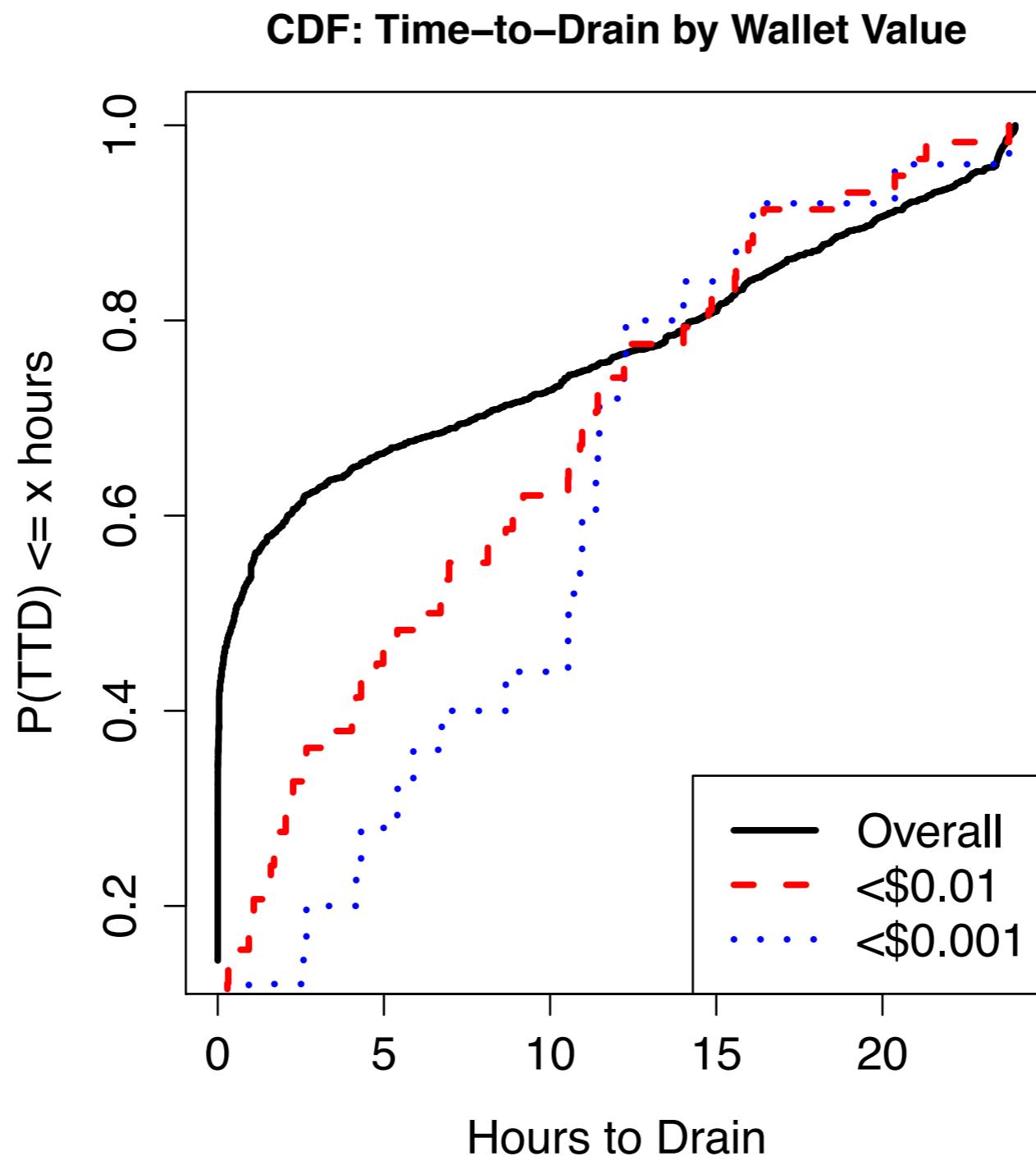
Brain Wallet Usage

- 1,730 distinct brain wallets
- 1,686 passwords and passphrases
- 2,846 BTC (approximately 261K USD)
- Notable Passwords/phrases:
 - This string contains 0.25 BTC hiding in plain sight.
 - “”
 - how much wood could a woodchuck chuck if a woodchuck could chuck wood

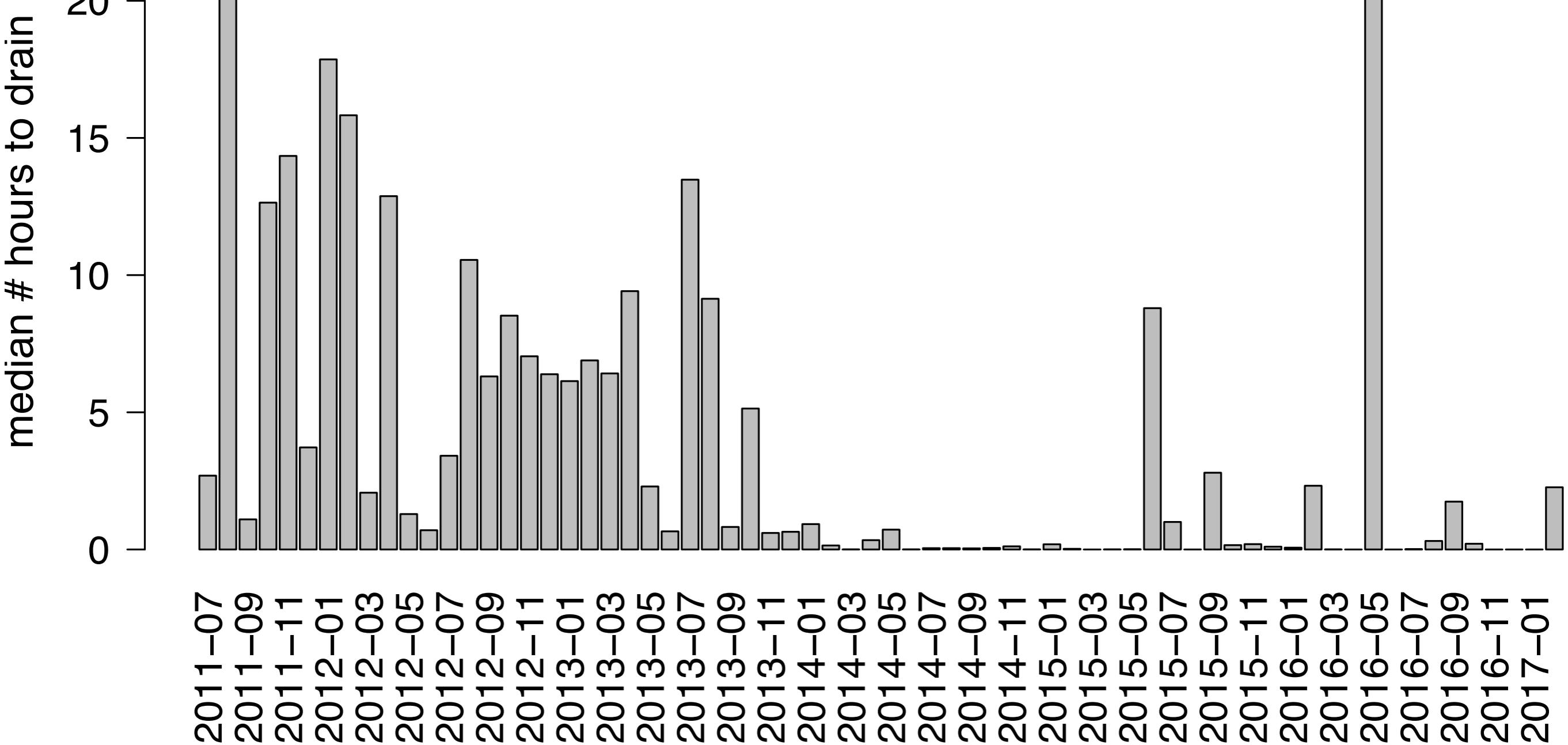
New Brain Wallet Usage by Month



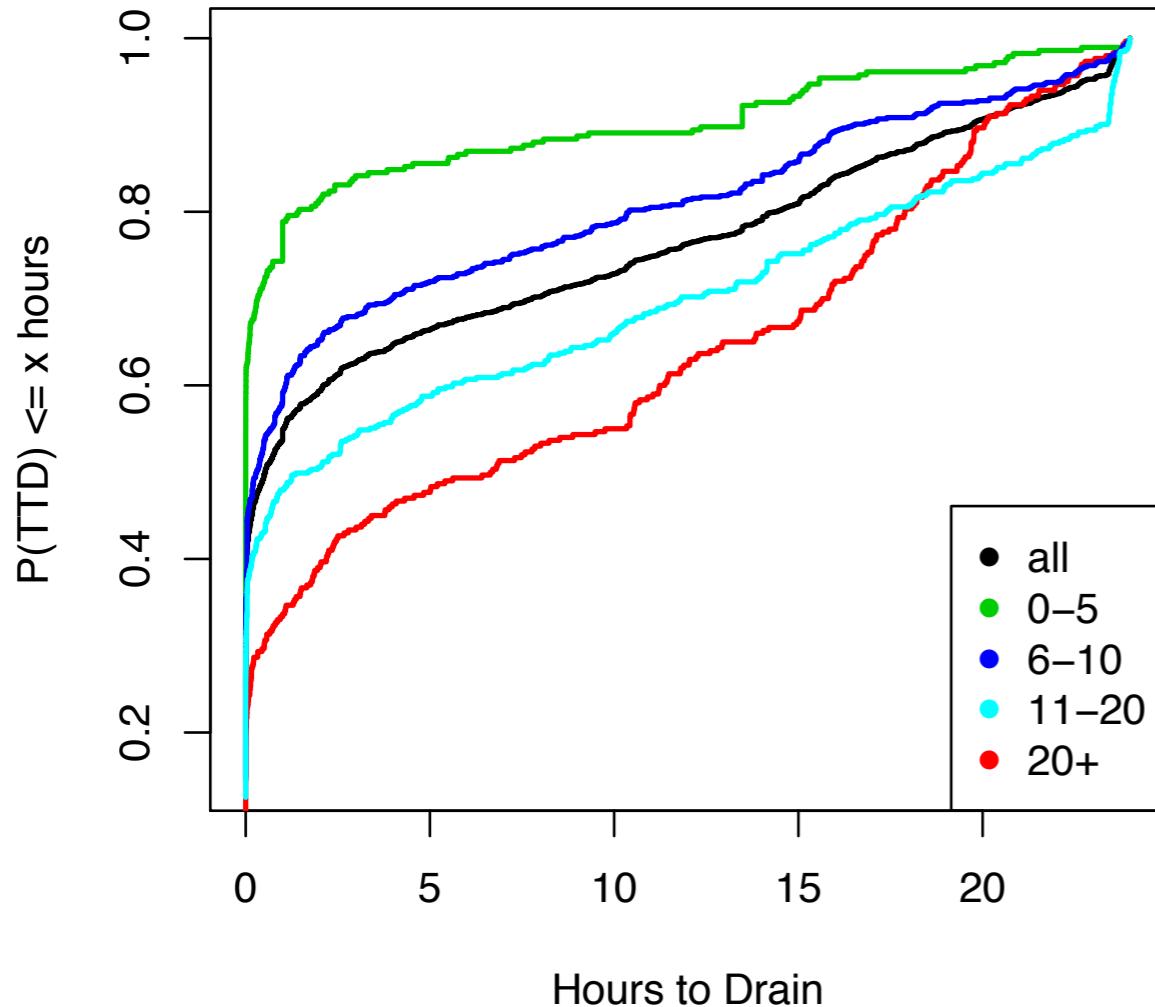
Brain Drain Time



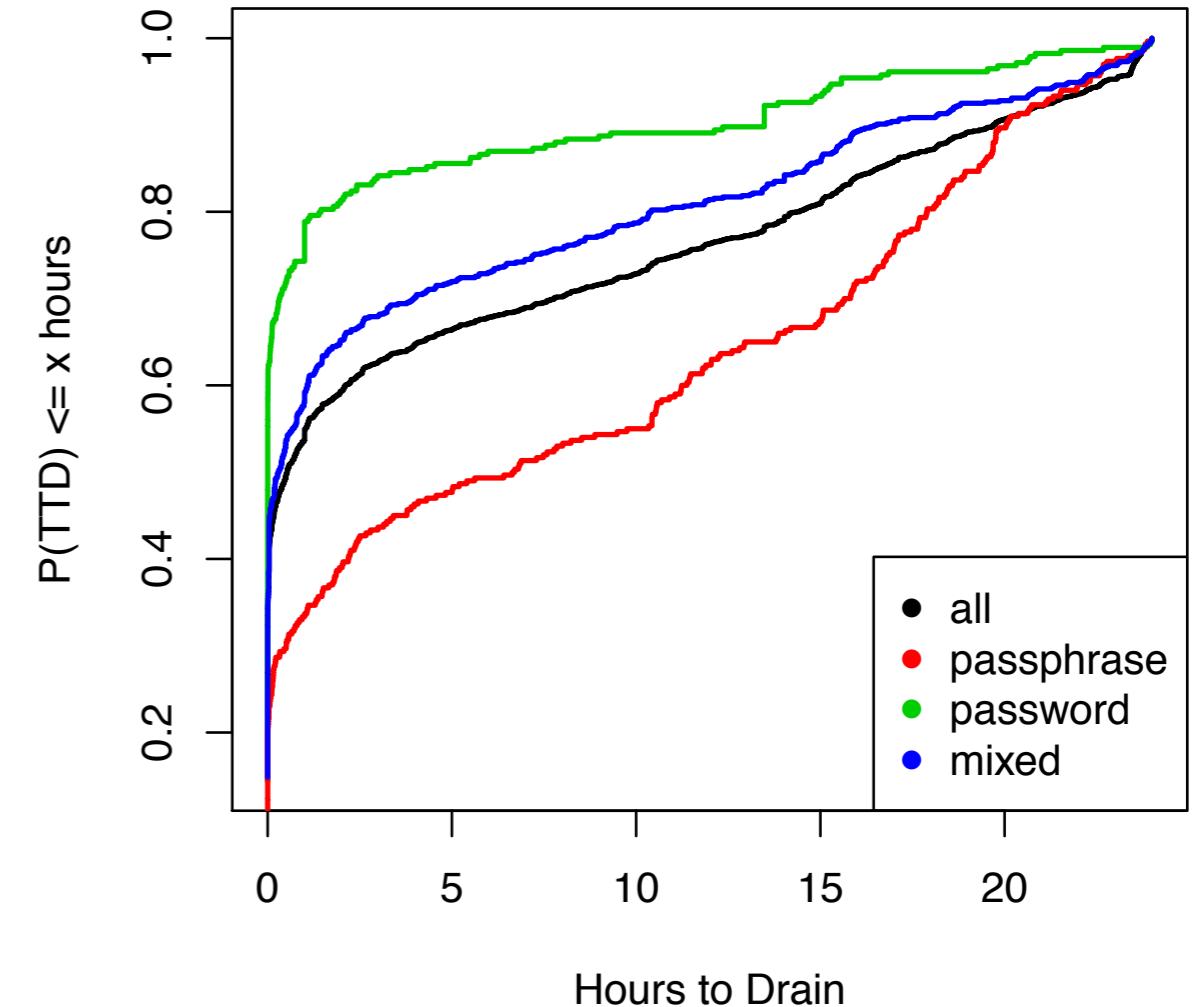
Brain Wallet Drains over Time



Draining: Passphrases vs. Passwords



Time to Drain
by Password Length



Time to Drain
by Password List

Chapter 6 Conclusions

- Developed methodology for measuring the use of brain wallets and their subsequent drains.
- Tested 3.9 trillion candidate passwords and passphrases.
- Found 1,730 brain wallets using 1,686 different passwords which have received 2,846 BTC (approx. \$261K).
- Nearly all drained, many within seconds.

Chapter 6 Conclusions

“DO NOT USE BRAINWALLETS”

[https://en.bitcoin.it/w/index.php?
title=Brainwallet&oldid=61264](https://en.bitcoin.it/w/index.php?title=Brainwallet&oldid=61264)

Chapter 6 Conclusions

“DO NOT USE BRAINWALLETS”

[https://en.bitcoin.it/w/index.php?
title=Brainwallet&oldid=61264](https://en.bitcoin.it/w/index.php?title=Brainwallet&oldid=61264)

Now... with Science!

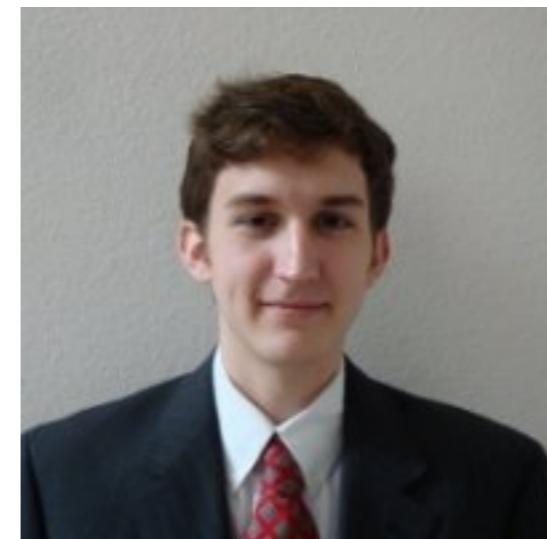
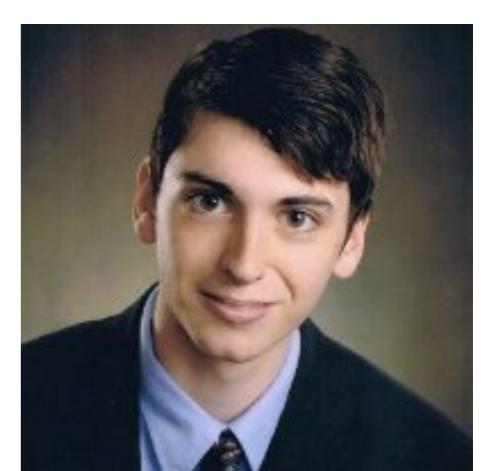
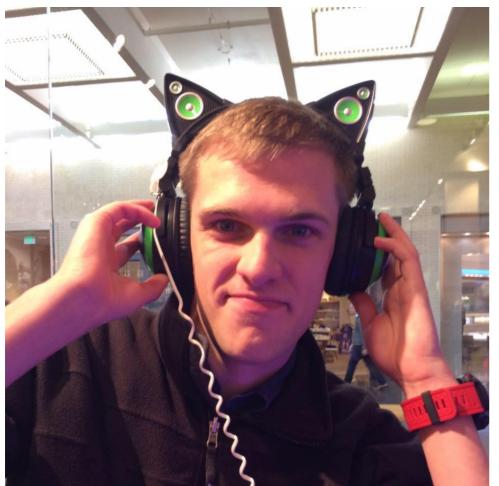
Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - Ch. 2 - Bitcoin Primer (covered in proposal)
 - Research Questions (covered in proposal)
 - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
 - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
 - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
 - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
 - **Ch. 7 - Conclusions**

Thesis Contributions

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
 - DDoS attack prevalence and impact
 - Bitcoin scam prevalence and profit
 - Brain wallet prevalence and drainer profit

Thanks!



Questions?