

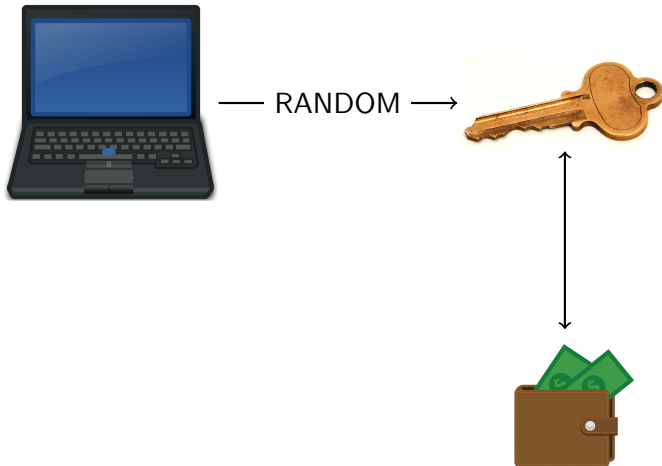
The Bitcoin Brain Drain: A Short Paper on the Use and Abuse of Bitcoin Brain Wallets

Marie Vasek*, Joseph Bonneau^o, Ryan Castellucci[†],
Cameron Keith[¶] and Tyler Moore*

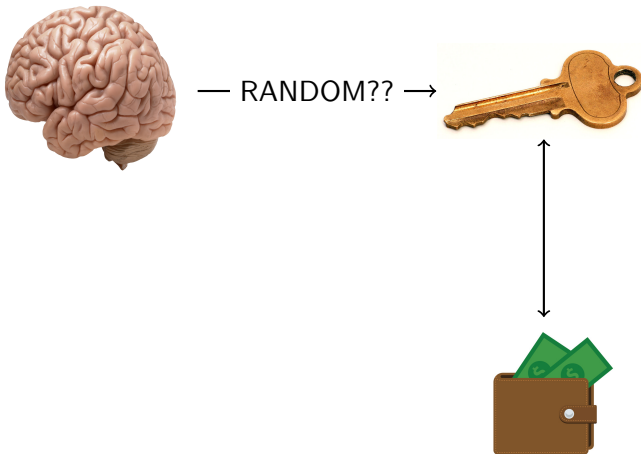
University of Tulsa*, Stanford University^o, White Ops[†],
Southern Methodist University[¶]

Financial Cryptography
February 25, 2016

What is a Brain Wallet?



What is a Brain Wallet?



... and why do we care?



comments related view images (0)



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 [shwitt](#)

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 [13w4Hn1BJQM4bjZZgYtXpyp4ciow29tKj](#)^[3] (I think the wallet passphrase was something simple like "satoshinakamoto" but I forget 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

4 of 16 That's okay. mv BTC is in correcthorsebatterystaple :)

[permalink](#)

Roadmap

- Generating Candidate Brain Wallet Passwords
- Brain Wallet Usage
- Brain Wallet Draining

Password Corpora: 300 Billion Candidate Passwords

Source	# Wallets	(non-empty)	Unique	90% # drains	Total BTC	Total USD
<i>Word lists</i>						
Urban Dictionary	296	3	2	3.00	561.95	43 120.77
Two Words	13	3	0	4.00	0.79	92.65
Eng/Slang Urban Dict.	63	14	28	2.00	0.90	124.96
Eng. Wikipedia	250	0	0	2.00	505.77	38 833.16
WikiQuotes	35	0	0	12.00	60.96	17 620.50
Phrases	283	0	0	3.00	578.69	57 376.80
xkcd	90	3	3	13.00	97.66	29 140.44
Lyrics	329	4	16	3.00	230.45	26 788.97
Blockchain.info tags	112	0	10	7.00	577.93	31 683.29
Rootkit	123	2	0	6.00	4.50	570.78
MySpace	59	0	0	3.00	1.14	210.44
RockYou	415	3	2	3.00	113.82	33 807.17
LinkedIn	213	0	0	2.00	10.11	738.52
LEET MRL	3	0	0	1.00	0.01	1.49
Prince MRL	295	4	7	3.00	88.93	21 028.02
CrackStation	640	3	37	2.00	396.09	41 326.80
Naxxatoe	388	0	2	2.00	41.56	3 389.31
Skull Security	414	3	3	2.00	71.73	20 756.32
Uniqpass	490	3	0	2.00	134.95	35 266.27

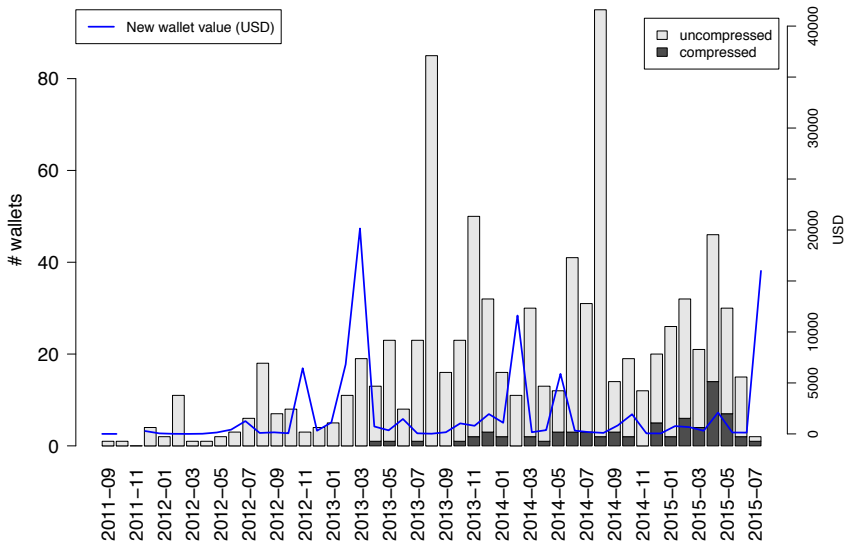
Password Corpora: 300 Billion Candidate Passwords

Source	# Wallets	(non-empty)	Unique	90% # drains	Total BTC	Total USD
<i>Non-word lists</i>						
Reddit User Challenge	1	0	1	1.00	0.01	2.62
Brute Force	200	3	3	3.00	22.47	3 895.99
Modified BW Passwords	74	1	9	2.00	2.25	209.98
Overall	884	21	139	2.00	1 806.22	103 472.13

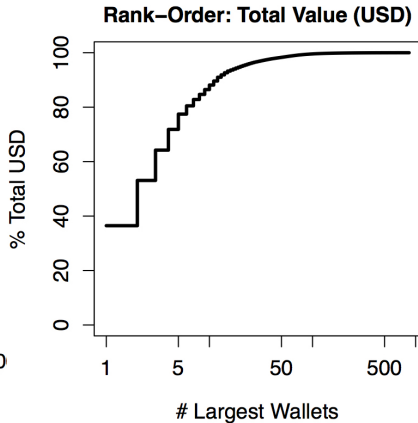
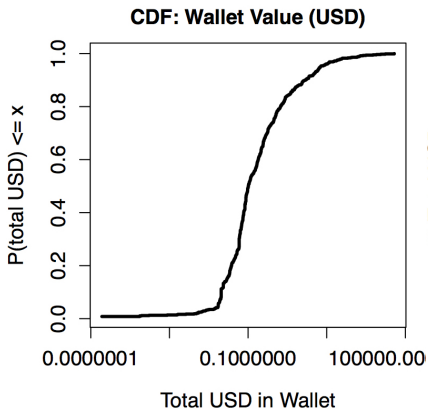
Brain Wallet Usage

- 884 distinct brain wallets
- 845 different passwords
- 1 806 BTC (approx. 103 000 USD)
- 798 uncompressed and 71 compressed
- Notable Passwords
 - one two three four five six seven
 - ""
 - how much wood could a woodchuck chuck if a woodchuck could chuck wood

New Brain Wallet Usage by Month



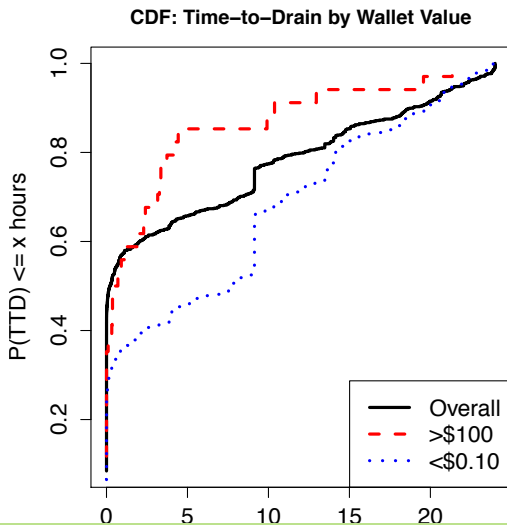
Value Stored in Brain Wallets



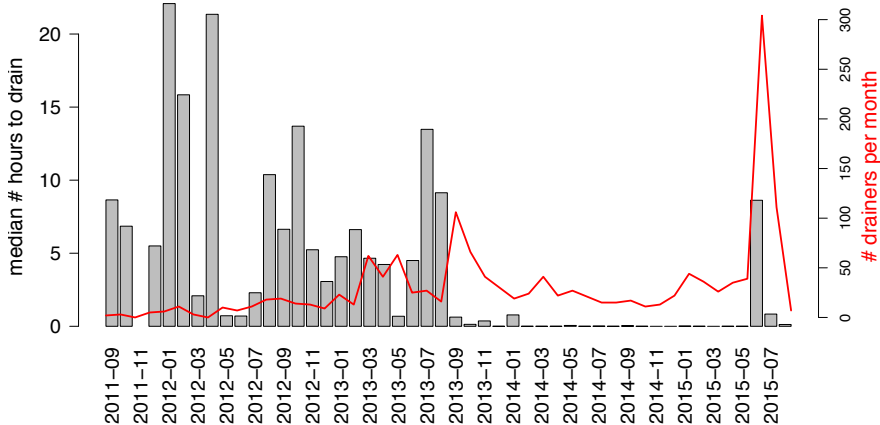
Drainers

- 1 895 drains on 884 wallets
 - 98% drained at least once
 - 69% of wallets are drained exactly once
 - 1.9% are drained more than ten times.
- 14 drainers (at least) targeting multiple brain wallets
 - Top 4 drainers netted \$35 000 between them
- \$1 – median value of drain among successful drainers

Brain Drain Time



Brain Wallet Drains over Time



Conclusion

- Tested 300 BILLION passwords through BrainFlayer
- Found only 884 used brain wallets worth 1 806.22 BTC or 103 472.13 USD
- 98% drained at least once
 - Most within minutes

Conclusion

“DO NOT USE
BRAINWALLETS”

<https://en.bitcoin.it/wiki/Brainwallet>

Conclusion

“DO NOT USE
BRAINWALLETS”

<https://en.bitcoin.it/wiki/Brainwallet>

Now... with Science!

Questions?

