# Why Brainwallets are a Bad Idea

| | |
|---|---|
| **Author** | josh |
| **Date** | 2020-04-02 00:00:00 |

# Overview

Private keys are the most critical aspect of Bitcoin ownership - without them, you don't truly own your Bitcoin! But in their raw form, private keys are a bit unwieldy. A bunch of random bits (256 to be exact) are not easy to remember or write down without error. Due to this problem, users have been looking for ways to more easily write down and remember their keys since Bitcoin's inception. And one of those (misguided) methods is the brainwallet. Let's discuss what a brainwallet is, and why using one is a *terrible* idea.

# Bits and Brains

## What is a Wallet, and What is a *Brainwallet?*

First, let's discuss what a Bitcoin wallet actually is. A cryptocurrency wallet is simply a collection of *private keys* used to unlock coins for spending, and the associated *addresses* that are derived from those keys. A private key is actually a 256 bit, *randomly generated* number. As I've discussed in previous tutorials, the amount of numbers that can be stored in 256 bit integers is *astronomically huge.* 0-2^256 (2^256-1, technically speaking). That 2^256 is a number thought to be about as large as the number of atoms in the observable universe. We'll get to why that is important in just a bit.

Now this private key is used to generate a public key and address using a *one way* process. Private key -> Public Key -> Address. Using elliptic curve cryptography, one can prove they are the rightful owner of Bitcoins sent to their address by providing the public key and a digital signature, all while keeping the private key secret! That's why private keys are so important - they are used to prove you own Bitcoins, allowing you to spend them.

Now what exactly is a *brainwallet?* A brainwallet uses some of the cryptography used in Bitcoin to derive a public key from a passphrase. For example, one might use the passphrase "abc123". By running this phrase through the SHA-256 hash algorithm, you get a 256 bit number that can serve as a Bitcoin private key! This is useful because a passphrase is much easier write down correctly or remember than a 256 bit integer. Running the phrase through SHA-256 always gives the same output, so one can simply remember the passphrase without having to remember the key!

## The Problem...

Seems like a great idea, right? Well, this idea turns out to actually be a huge problem in practice. The problem is that human beings are *really, really* bad at randomness. We think we can be random, but we're really not in the cryptographic sense. Remember how I mentioned how big the 256 bit keyspace is? 2^256-1? It turns out that given *proper randomness (entropy),* it's pretty much impossible to brute force guess a key. However, keys that are not generated with a proper level of entropy are *significantly* easier to crack - and brainwallets do not have sufficient entropy to be safe!

I was turned on to the nature of this problem by security researcher Ryan Castelluci's 2014 Defcon talk entitled "Cracking Cryptocurrency Brainwallets". Ryan's excellent talk discusses just how easy it is to break these wallets, including examples from his own research tool called Brainflayer. Ryan found that a significant number of these brainwallets are easily cracked using common wordlists, and that hackers have sophisticated tools to compete and steal brainwallet funds. For example, the empty string's address has received (and lost) 59 Bitcoin! Even seemingly random, strong passphrases like "Interior Crocodile Alligator" have lost coins to these attackers.

### The Solution!

Thankfully, not all hope is lost for easy-to-store private keys. In terms of brainwallets, the solution is simple. DO NOT USE THEM! EVER! You *will* have funds stolen in a matter of time. The Bitcoin blockchain is like a permanent password database, with a juicy monetary reward for cracking!

Instead, much safer solutions have been developed and put into practice in the cryptocurrency space. You may be family with *mnemonic seed phrases*. Most wallets will now give you a 12-24 English word backup phrase you can easily write down or even memorize. This is *not* a brainwallet. Rather, a seed is generated using a cryptographically secure random number generator, and then encoded in an easy-to-use format. The seed is truly random and safe against brute-force attacks, given a properly implemented wallet.

## Brainwallets - Bad Move!

Brainwallets are fundamentally insecure. Low entropy private keys are always a recipe for disaster when it comes to cryptography, and especially so when the disaster is you losing precious coins. Instead, use modern cryptographically secure methods like BIP39 mnemonics to easily backup your funds.

If you're curious about this topic and want to experiment, check out my code project PwnedWallet. This project is a simple React web application that allows you to enter a brainwallet passphrase and see if the funds in that wallet have been stolen. The tool takes the phrase and generates the private key, public key, and address for you to see. It will then fetch balance data from a public API and show you if that wallet has ever had coins in it and if it has been emptied.

Stay safe with those keys!