BIP39 Mnemonics Made Easy (Part 1 - Backups, Simplified!)

Author	josh
Date	2018-01-19 18:42:46

Overview

A critical component of cryptocurrency security is the ability for users to easily and efficiently backup the private keys that control access to their funds on the blockchain. Without one's private keys, any funds in a user's addresses are irrecoverably lost. However, the nature of early wallets made backing up one's private keys a regularly-scheduled necessity, unwieldy and annoying for most users. BIP39 and associated Bitcoin Improvement Proposals have thankfully simplified private key backup by introducing HD wallets and mnemonics.

Newer wallets explained

HD? So like, High Definition? No, Hierarchical Deterministic!

In the early days of Bitcoin and other cryptocurrencies, address generation was done non-deterministically. For each new address needed, a private key would be randomly generated and stored in the wallet's backup file. Most wallets would pre-generate some addresses in the initial wallet file, but every new private key/address introduced into the wallet meant a new backup would be needed. For privacy reasons, it is recommended to use a new address for each transaction. And for every new address generated since the last backup, a user would need to create a new backup to avoid losing recent funds in the event of a wallet resortation. Even for "power users", backups became an unwieldy and annoying task. Enter BIPs (Bitcoin Improvement Proposals) 32 and 44. In summary, these proposals introduce HD ("Hierarchical Deterministics Wallets"). These wallets only require one *seed* to be randomly generated. And from that seed, *all* the private keys and addresses a wallet needs can be derived in a tree structure; all associated with the initial seed. Since the private keys and addresses can be *regenerated* from the seed, one only has to back up the seed to recover all of their private keys, addresses, and transactions for a wallet. Much better!

Introducing Mnemonics - Simplifying Seed Backups

The ability to generate an entire wallet from one seed drastically simplified wallet backups, and therefore has improved the ease by which users can keep their funds safe. However, a seed is still just a random binary value. Represented in hex or Base64 encoding, it is still fairly easy to misread/miswrite a character and accidentally create a useless wallet backup. To truly simplify the task of backing up a wallet seed, some developers in the Bitcoin space proposed a system that allows the translation of the binary seed value into English words that can be more easily transcribed or even memorized to secure access to one's funds. This proposal, given the designation BIP39, was written by Marek Palatinus, Pavol Rusnak, Aarone Voisine, and Sean Bowe.

What does a mnemonic look like?

Mnemonics don't use just any set of words. These words are carefully chosen to avoid ambiguity and make transcription easy, so that a user doesn't accidentally create an incorrect backup. There are a total of 2048 words in the dictionary, and a wallet mnemonic contains 12-24 words. The last word contains a checksum validating the other words in the list, making it easy for wallets to validate a backup. Here is a sample Bitcoin or Bitcoin Cash BIP39 mnemonic:

1. army
2. van
3. defense
4. carry
5. jealous
6. true
7. garbage
8. claim
9. echo
10. media
11. make
12. crunch

WARNING, DO NOT use this seed for a wallet. A seed must remain private, and your funds will be stolen! This mnemonic is excerpted from Andreas' Antonopoulos' *Mastering Bitcoin* to further discourage its use - millions of people have access to this wallet. Now how do you get one of these fancy mnemonics for a wallet? Most modern wallet software will generate this for you when you create a wallet. Then, all you need to do is write down the phrase and store it in a secure location to backup access to your funds if your wallet device is lost or stolen. Alternatively, a mnemonic can be generated by a separate tool and imported as a backup into the wallet software. I've written a generator called MnemonicGen that produces standard phrases that can be imported into any modern HD wallet that supports BIP39. Keep in mind that this particular project is meant to be academic/experimental and may not be sufficiently secure for your needs. But other mnemonic generators like Ian Coleman's are widely used and well-vetted.

Mnemonics - Backups Made Better

With BIP39 mnemonics, Bitcoin newbies and power users alike can easily create and backup secure wallets without the need to keep a schedule or deal with unwieldy binary data encoding. This modern standard is implemented in widely-used and accessible wallets like the Bitcoin.com wallet, Electron Cash, Blockchain.info, and more. I would personally advise upgrading your cryptocurrency experience by using an HD wallet, simplifying your security practices and keeping your funds safe! In the next article, we'll discuss the technical workings of BIP39, showing how we can go from a random seed to a set of words in a few fairly straightforward steps.