Hands Off My Keys! The Basics of Offline Wallets

Author	josh
Date	2020-02-13 18:00:40

Overview

In the cryptocurrency world, ownership of your money is controlled by cryptographic *private keys*. These keys are used for deriving your receiving addresses and ultimately for spending funds. For obvious reasons, secure storage of these keys is *absolutely critical* for any Bitcoin user, as anyone with the keys can control the funds at that address.

There's varying levels of key ownership and storage, and today we're going to talk about one of the most secure - offline wallets.

The What & Why of Offline Storage

How is Offline Storage Possible?

One of the interesting properties of cryptocurrencies is the ability to store funds offline in the first place. Bitcoin is digital cash after all, built on a peer-to-peer network. How can you store internet money without the internet?

It's important to understand what Bitcoin actually is fundamentally, and a bit of how transactions work. When you operate a Bitcoin wallet, you don't actually store *bitcoin* on the wallet. What you really store is *private keys that unlock bitcoin.* When you create a wallet, your wallet generates private keys. Those keys are used to generate your *receiving addresses.*

So, when someone sends you some Bitcoin, the blockchain stores a record saying that you now own some coins at that address. The blockchain is distributed around the world over the peer-to-peer bitcoin network, but the keys that *unlock* those coins for spending are stored in the wallet. When you go to spend that bitcoin at a later time, your wallet's keys sign a new transaction that says that the receiver now owns those coins.

Based on this system, it turns out that a user *doesn't have to be online* to *receive* some bitcoin at an address. If you generate a private key and its address totally offline, someone can send bitcoin to that address over the network without the wallet (keystore) having any internet connection at all. You only need to be online to *spend* the coins later, in order to sign and broadcast that transaction.

What are Offline Wallets?

Hence, the concept of offline wallets. It's possible to generate a private key completely offline, generate the associated address, and send funds to that address without this wallet having any connection at all. It's as simple as copying the generated offline address and giving it to the

person that wants to send you Bitcoin (or copying it into your online wallet to send some savings offline).

So what do these wallets look like exactly? Well, there's two common types of offline wallets, both serving the same general purpose: there's **paper wallets** and **hardware wallets**.

A paper wallet is a simple keypair, generated offline and printed out on paper or another medium for long term storage. A paper wallet doesn't have to be paper either, it could be a keypair engraved in a metal coin or metal wallet like the Coinstack. You could make a paper wallet by writing the key in icing on a cookie cake, although I wouldn't advise it - longevity is important and I'd be sure to eat that cake if it was me...

Paper wallets are simple, and fairly trivial to generate. There are several programs that one can download and run offline, and connect to their hard-wired printer. They do have several pitfalls though - longevity and reuse issues. First, it's important that the medium be preserved. Paper can be stained and ink ruined, so paper should be laminated and stored in a fireproof location. Metal wallets are better for this. As well, the address *must only be used once and funds completely spent.* Many users have lost funds by misunderstanding change addresses, thinking that they could spend small amounts from a paper wallet key. If you're going to use a paper wallet, you must import all the funds to an online wallet at once and send the change back to a *new* address. For these reasons, paper wallets have fallen out of favor.

The latest innovations are with **hardware wallets**, electronic devices that generate keys/addresses, and also sign transactions. These are small USB devices that generate keys from a single *seed phrase*, and also allow you to plug the device into a computer for signing and broadcasting transactions. Wallets such as KeepKey, Trezor, and Ledger are popular solutions. These devices will give you a seed phrase you should securely back up (also offline), and offer increased usability and security over pure paper-wallet keypair solutions.

These devices are engineered first and foremost for security. Even when they're plugged into a PC for transaction signing, they communicate with a limited protocol to the PC. They will only allow the transmission of data like signed transactions, and nothing else. So when you plug your hardware wallet into a PC to send some bitcoin, no virus or hacker can access the keys the way they could with an online wallet or full-filesystem wallet stored on a hard drive. The hardware wallet device simply won't allow it.

Why Offline Wallets?

So why do this in the first place? Well again, it's critical that private keys be kept safe. Anyone that finds or *steals* your private keys is now technically the owner of your crypto. So much like other data on your computer, keys are vulnerable to theft and corruption.

Malware can target online computers and mobile phones more easily, because malicious websites and network connections can drop viruses on the device fairly easily. As well, the network connection allows this malware to send the keys back to the thieft! Not only that, but things happen to computers and phones more often than they happen to special devices and metal/paper wallets kept in a safe. If you drop your phone in the toilet or your hard drive dies without a backup, you've lost your coins.

Offline solutions are the most secure because they provide an "airgap" between the keys and any prying eyes. A non-networked hardware wallet or metal wallet can't be hacked over a network - because they're not connected to one. For most of us, an offline device in a safe at our home or bank is much harder to steal, and much less of a target, than our online devices. This makes offline wallets by far the safest for long-term storage of cryptocurrency private keys.

Secure Long-Term Storage with Offline Wallets

Ultimately - your keys, your coins. By using offline wallet solutions, you can't prevent malicious actors from gaining access to the private keys that prove ownership of your crypto funds. Online wallets like mobile wallets and full nodes are totally fine for day-to-day spending, and you should use them for that. You don't want to have to import a paper wallet for every Bitcoin purchase. But for long-term safe keeping, offline storage provides a safe airgap between your keys and the dark parts of the internet. So if you'd like to save some of your coins for the long term, get a hardware wallet and keep those keys away from the bad guys!