What's in Your Wallet? Understanding Private Key Control

Author	josh
Date	2018-11-29 21:34:25

Overview

Just like your cash, cards, and ID, your cryptocurrency assets live in something called a "wallet". Most all forms of digital money implement this concept in some form, and understanding wallets is critical to safely storing and using your favorite digital currency.

Much like your physical wallet, your Bitcoin, Monero, or Ethereum wallet gives you *direct* access to the funds inside. A crypto-wallet isn't like a credit card - if a stranger gets a hold of it, you can't cancel it. Much like cash, the money stolen would be theirs!

But how does this work? How can a digital asset act like cash when all other forms of digital monetary transactions (credit cards, bank transfers, PayPal) can be "cancelled" if stolen? We must first understand a bit about what a "private key" is, and why who controls it is so important to the security of your cryptocurrency funds.

A word on private keys

Without getting to far into the technical details, let's discuss a bit about what a "private key" is and why it is so important. Remember how I said that your crypto-wallet is like digital cash, and your wallet "stores" your Bitcoin or other currency? Well, that's not *quite* how that works...

In reality, the amount of Bitcoin that you own is stored on a worldwide, completely public ledger/database called the "blockchain". This ledger stores a public record of all of the Bitcoin transfers ever conducted, so anyone can see exactly who owns what. Sound scary and insecure? How can you control your digital cash if *everyone* has access to this open blockchain??

This is where private keys come in. Bitcoin (and other crypto currencies) use a form of cryptography called "elliptic curve cryptography" to generate the Bitcoin "addresses" people can use to send you money. The address is completely public; you can give it to anyone and they can send you funds. However, behind this address is a special "private key" used to access those funds on the blockchain. Your address is generated *from* this randomly generated private key by using this form of cryptography.

The cryptography used in address generation makes it so that you can't figure out the *private key* by going backwards from the *public key*, or Bitcoin address. However, the private key is used to *prove that you own the address* without ever revealing it, thanks to the magic of elliptic curve cryptography. It is critical that the private key is **always kept secret**, because anyone with the private key can access the Bitcoin at the associated address.

Levels of Private Key control in Wallets

Now that we understand the basics of private keys and their importance, we can talk a bit about how different wallets keep these keys safe from the prying eyes of crypto-thieves. All wallets must work in some way that keeps the private keys, well, *private* so that control of the funds lies with their rightful owner. There are three general approaches to private key control in wallets: a **full control** model, a **hybrid** model, and a **custodial** model.

Full control wallets

Full control wallets offer the obvious - *complete and total* control of the private keys. With a full control model, the private keys are generated and stored on the user's device, be it a desktop computer, mobile phone, or even a hardware wallet like the Trezor. With this model, the private keys never leave the user's device in any shape or form.

The advantage to this model should be fairly obvious - it is by far the most secure model. There is no trust involved with a third party; the funds are completely controlled by you. Users should still exercise care around other security parameters (ensuring a virus-free machine, for example), but generally these wallets offer the most hardened approach to keeping private keys safe.

The disadvantage here is the lack of convenience and ease of use. This wallets require the most technical savvy of these three models, although most "power users" will have no problem understanding and securing these wallets. It is extremely important that the users of these wallets understand how to *back up* their private keys. If the device is fried or lost and there is no accessible backup, all funds will be lost! Fortunately again, BIP39 mnemonic backups make this tasks easier than it was with the first few Bitcoin wallets.

Hybrid wallets

Some major players in the crypto space have created an interesting hybrid model for private key storage. Web wallets like those at blockchain.info or btc.com implement this model. With hybrid wallets, private keys are generated and then *encrypted* on the user's machine (usually in the web browser) before being stored on the company's server. With these wallets, private keys are only *known and accessible* to the user, while the company keeps an encrypted backup safe on their servers.

With this model, security is still pretty strong. Because strong encryption is done on the user's machine, no one with access to the company's servers have access to the actual private keys without the decryption passphrase, which lies safely with the user. This model requires that the user trust that the company's code (which is preferably open source) is soundly implemented and doesn't contain secret backdoors. However, if the encryption is done right no one but the user can actually access the keys. This model is slightly less secure than a full control model,

Although there is a small amount of security tradeoff here, this model comes with increased convenience to the user. Most web wallets have a more traditional username and password login interface, so the user only needs to create and remember a secure passphrase to access their funds, with the site taking care of backups for them. This may be easier for a beginner crypto-

enthusiast, and any good site will still offer mnemonic backups and private key exports for the savvy user.

Custodial wallets

The final model we'll discuss here is the custodial wallet. Many exchanges like Coinbase offer custodial wallets. Like a hybrid wallet, all you need to do is create a username and password and log into a website to access funds. However, the critical difference is that with a custodial wallet, *the user doesn't know their private keys at all!*. With custodial wallets, the website takes care of generating and storing all the private keys without revealing them to the user. No backups to manage, and no need to understand how to do much more than log in to a website to use this kind of wallet.

The security pitfalls of this model are pretty serious, in my opinion. With these wallets, the user has no way to back up their private keys. What's more, the user must *completely trust* the company or individual implementing this kind of wallet. These companies *must* have significant security measures in place to avoid attacks on their servers, and they must be trusted to mitigate the access rogue employees could have to user's money.

In fact, these types of wallets *completely break* a fundamental security principle of Bitcoin - the user controls their keys, therefore the user controls their money. Custodial wallets far more closely resemble the centralized model of traditional banks.

Don't worry though - these wallets aren't all scary! The cost of security comes with a large benefit - ease of use! These wallets have a much smaller learning curve for complete beginners. Just sign up for a wallet account just like you would a forum, email address, or social media account. For someone with little understanding of the world of cryptocurrencies, this type of wallet offers a gentle introduction

My only advice would be that given the security pitfalls of this model, only use custodial wallets to store small amounts or for buying and selling. Most custodial wallets live in currency exchanges, so use them to buy your crypto of choice and send the funds to a more secure wallet.

Know Your Keys

The most important takeaway from this discussion of private key control models is that it is important for a wallet user to know where their private keys are. Again, in Bitcoin and other cryptos, control over your private keys is control of your money. Anyone with access to the keys has access to your money and can spend it freely, so either keep them to yourself or make sure the holder is a wallet maker you trust.

By understanding these different models, users have more control over how they choose to secure their wallets and keep their funds safe. Understanding the pros and cons of full control, hybrid, and custodial wallets allows a cryptocurrency user to choose the best wallet for their needs. Ultimately, an understanding of these models allows for better security and comfort with digital money, because a person knows who truly owns their keys and is responsible for keeping them safe.