Bitcoin Foundation

Selecting a Wallet and Protecting your bitcoins

Education Committee of the Bitcoin Foundation

The first thing anyone will need to do in order to use bitcoins is to select a wallet. A wallet is software and there are many to choose from. Wallets maintain the private keys, and generate public keys from them as requested. The utility of wallets is primarily to process transactions, these being "send" and "recieve funds" requests. Wallets typically allow entry either of the QR code for the transaction or the actual 30 some digit public key for a send or receive transactions.

Here are the main categories:

1. Web Wallets: Just like they sound, these are online wallets where your bitcoins are stored on a web server. Very easy to setup and use, and useful for minor transactions. Often your assets are held by the wallet company, and they use their own private keys. You own a "promise to pay" from the wallet company and do not actually own bitcoins.

2. Mobile Wallets: Some mobile phones will offer mobile phone wallets. These can be quick and convenient and individuals have complete control of their bitcoins. Just like your cash wallet, however, if the phone is lost, or damaged, all of the bitcoins stored there may be permanently lost. Be sure to back up all Bitcoins to somewhere off the phone.

3. PC/Mac/Linux Wallets: These wallets are usually the fullest featured but least portable of all of the wallets. Just like mobile wallets, if the computer is subject to malware or is stolen, all of the bitcoins stored there may be permanently lost. Be sure to back up all bitcoins to somewhere OFF the computer

4. Offline/Cold Storage Wallets - These are the most secure of any but are less convenient to use. Because they are not connected to the Internet they cannot be hacked. In order to spend bitcoin from the account involves a two step process where the authorization to transfer is transported manually via thumb drive from the offline computer to an online one.

It is recommended to use more than one wallet. Bitcoins can easily be transferred between wallets so it is easy and generally safer to have your bitcoins in more than one place.

Here are a few key things to keep in mind:

1. Bitcoins, like cash, can be lost, stolen or destroyed.
2. Bitcoins, unlike cash, can be backed up or printed and stored offline.
3. Bitcoins, unlike cash, are not completely anonymous. While your identity is not disclosed, every transaction is public record.
4. The essence of "owning bitcoins" is owning the private key which can generate those public keys seen in bitcoin transactions. All of the issues concerning encryption of a wallet, moving funds to offline or cold storage wallets, not putting more funds in a wallet than one can afford to lose, have to do with maintaining the secrete of the private keys.
5. If the private key in your wallet was given to you or provided to you by someone else, it is possible an attacker with that knowledge could steal your bitcoins without hacking your wallet.
6. Several web wallets and mobile wallets do not provide users with their own private keys, but operate with pooled resources. You essentially give money to the wallet company, then as you spend it they provide bitcoins and execute the transaction with their own private keys.
7. Be clear as to whether you own your bitcoins - meaning, you have exclusive knowledge of the private keys - or you own a "promise to pay" from an exchange or wallet provider.
8. If you have a record of your private keys, no matter what wallet is used, unless an attacker has found the secret of those private keys, you can retrieve your bitcoins.

Protecting your bitcoins:

Here is a short list of items to be considered a minimum when protecting your bitcoins:

1. Encrypt with a password

2. Backup all wallets (with encryption) to another device, computer, flash drive, etc – frequently
3. Export or Print all Bitcoins to “Cold Storage” (Paper Wallet) – Keep these documents in very safe place
4. If your private keys were given to you by a wallet company, generate some of your own private keys and transfer the funds to your own keys. Keys that could potentially be in a wallet company’s database, even if printed off on a paper wallet for cold storage, may at some future point be hacked.