Securing your wallet

Like in real life, your wallet must be secured. Bitcoin makes it possible to transfer value anywhere in a very easy way and it allows you to be in control of your money. Such great features also come with great security concerns. At the same time, Bitcoin can provide very high levels of security if used correctly. **Always remember that it is your responsibility to adopt good practices in order to protect your money**.

⚠ Be careful with online services

You should be wary of any service designed to store your money online. Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank. Accordingly, you might want to use other types of Bitcoin wallets. Otherwise, you should choose such services very carefully. Additionally, using two-factor authentication is recommended.

Small amounts for everyday uses

A Bitcoin wallet is like a wallet with cash. If you wouldn't keep a thousand dollars in your pocket, you might want to have the same consideration for your Bitcoin wallet. In general, it is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment.

Backup your wallet

Stored in a safe place, a backup of your wallet can protect you against computer failures and many human mistakes. It can also allow you to recover your wallet after your mobile or computer was stolen if you keep your wallet encrypted.

Backup your entire wallet

Some wallets use many hidden private keys internally. If you only have a backup of the private keys for your visible Bitcoin addresses, you might not be able to recover a great part of your funds with your backup.

Encrypt online backups

Any backup that is stored online is highly vulnerable to theft. Even a computer that is connected to the Internet is vulnerable to malicious software. As such, encrypting any backup that is exposed to the network is a good security practice.

Use many secure locations

Single points of failure are bad for security. If your backup is not dependent of a single location, it is less likely that any bad event will prevent you to recover your wallet. You might also want to consider using different medias like USB keys, papers and CDs.

Make regular backups

You need to backup your wallet on a regular basis to make sure that all recent Bitcoin change addresses and all new Bitcoin addresses you created are included in your backup. However, all applications will be soon using wallets that only need to be backed up once.

Encrypt your wallet

Encrypting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software.

Never forget your password

You should make sure you never forget the password or your funds will be permanently lost. Unlike your bank, there are very limited password recovery options with Bitcoin. In fact, you should be able to remember your password even after many years without using it. In doubt, you might want to keep a paper copy of your password in a safe place like a vault.

Use a strong password

Any password that contains only letters or recognizable words can be considered very weak and easy to break. A strong password must contain letters, numbers, punctuation marks and must be at least 16 characters long. The most secure passwords are those generated by programs designed specifically for that purpose. Strong passwords are usually harder to remember, so you should take care in memorizing it.

Offline wallet for savings

An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches.

Offline transaction signing

This approach involves having two computers sharing some parts of the same wallet. The first one must be disconnected from any network. It is the only one that holds the entire wallet and is able to sign transactions. The second computer is connected to the network and only has a watching wallet that can only create unsigned transactions. This way, you can securely issue new transactions with the following steps.

1. Create a new transaction on the online computer and save it on an USB key.
2. Sign the transaction with the offline computer.
3. Send the signed transaction with the online computer.

Because the computer that is connected to the network cannot sign transactions, it cannot be used to withdraw any funds if it is compromised. Armory can be used to do offline transaction signature.

Hardware wallets

Hardware wallets are the best balance between very high security and ease of use. These are little devices that are designed from the root to be a wallet and nothing else. No software can be installed on them, making them very secure against computer vulnerabilities and online thieves. Because they can allow backup, you can recover your funds if you lose the device.

Keep your software up to date

Using the latest version of your Bitcoin software allows you to receive important stability and security fixes. Updates can prevent problems of various severity, include new useful features and help keep your wallet safe. Installing updates for all other software on your computer or mobile is also important to keep your wallet environment safer.

Multi-signature to protect against theft

Bitcoin includes a multi-signature feature that allows a transaction to require multiple independent approvals to be spent. This can

be used by an organization to give its members access to its treasury while only allowing a withdrawal if 3 of 5 members sign the transaction. Some web wallets also provide multi-signature wallets, allowing the user to keep control over their money while preventing a thief from stealing funds by compromising a single device or server.

Think about your testament

Your bitcoins can be lost forever if you don't have a backup plan for your peers and family. If the location of your wallets or your passwords are not known by anyone when you are gone, there is no hope that your funds will ever be recovered. Taking a bit of time on these matters can make a huge difference.