

Bitcoin Basis 15 – Hardware wallets

A hardware wallet is a portable physical device that manages private keys, making it more secure and easier to sign transactions and keep track of your value.

It reduces the risk of human error when using your private keys and keeps them away from your computer or phone. Bitcoin exists on the blockchain, not in a wallet.

A hardware wallet therefore does not contain bitcoin, but it does contain encrypted access codes that are required to authorize transactions.

Some hardware wallets can also be used to facilitate the signing of smart contracts. Secure hardware wallets have secure chips, a good random data generator, are open-source, have no backdoors. For safety, they should also have the option to work air-gapped, without contacting a computer via a USB connection.

An important point is the seed phrase, consisting of 12 or 24 words. These are generated during installation and are used as the basis for generating your addresses and private keys. You can also use this to restore the wallet and the value on it.

It is essential to store these words securely and offline.

Whoever holds this, also holds your value.

A hardware wallet is not necessary and only increases the security of your private keys.

@avbpodcast - bitcoinbasis.be