[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/the-basics-of-bitcoin-wallet

The Basics of Bitcoin Wallet

Bitcoin Wallet

Bitcoin wallets are similar to their fiat counterparts — but there are specifics to using BTC wallets that make them totally different.

Traditional fiat wallets have a simple use case: to carry your personal items such as cash, bank cards, and other gift cards. Bitcoin (BTC) is undoubtedly nothing like traditional currency due to its characteristics as a censorship-resistant and peer-to-peer electronic cash system, which is secured using public-key cryptography and does not require intermediaries to process transactions, but developers still use the terms that we associate with cash to help users to navigate the new world of cryptocurrencies. For this reason, a key piece of infrastructure that users use to transact Bitcoin and other blockchain-based cryptocurrencies is referred to as a "wallet."

It is in fact a device, program or service that generates and stores a master file containing the digital "credentials" that users need in order to access, send and receive cryptocurrency via blockchain transactions. The minimum "credentials" which a user needs to interact with the public Bitcoin blockchain are a pair of public and private cryptographic keys and a public Bitcoin wallet address. These credentials are used to digitally sign and authenticate valid Bitcoin transactions on the public blockchain. The most sensitive of these credentials, the private cryptographic key, must be kept, as the name suggests, absolutely private — much like a PIN or security code for a bank account. It consists of a unique, alphanumeric string of characters and is necessary for a user to access, spend or transfer their cryptocurrency.

The public key is mathematically derived from the private key and enables a user to receive cryptocurrency from others. Like the private key, it also consists of a very long (256 bits) alphanumeric string of characters. A Bitcoin wallet is used to generate a corresponding public wallet address that serves as a public identifier for transactions. The address is a shortened — "hashed" — version of the public key (160 bits), making it easier to share with others. Note that Bitcoin wallets can be used to generate an unlimited number of public addresses, all of which are linked back to the same user wallet.

It is critically important for users not to forget or misplace the record of their private key. As Bitcoin is a disintermediated, peer-to-peer system, users do not have recourse to a third-party to help them to recover their lost public key, meaning they risk losing access to their funds forever.

There are three main types of Bitcoin wallets — software, hardware and paper — which differ in their characteristics and security levels. Depending on whether or not a Bitcoin wallet is connected to the internet, it is also further categorized as either a “hot” or “cold” wallet.

Differences Between Hot And Cold Wallets

Just as hardware and software refer to physical and nonphysical computer parts, they refer to in what way you store your cryptocurrencies.

Hardware wallets, or cold wallets, store your seed phrase and private keys in a secure physical device and protect you against cyber attacks by air gaping your private key from the internet. While the software counterpart for your cold wallet acts as a safe, still allowing your Bitcoin to exist on the blockchain and be staked, your physical device acts as a key for this safe. Each transaction requires your key, the physical device, to respond to the transaction, and your device has a pin for an additional layer of safety. Hardware wallets are almost always the safest solution against security threats.

Hot wallets refer to virtual wallets that are online and facilitate the sending of cryptocurrencies to other users or exchanges. Being virtual means that your seed phrases and private keys are stored online and in your wallet’s browser or application, making them more susceptible to cybersecurity threats, where cold wallets use physical hardware like secure elements to protect this information. Hot wallets are “hot” because they are always connected to the internet. This makes them more flexible and convenient to support a wider array of assets since there’s no hardware to deal with for integration purposes.

Cryptocurrency Wallets

Bitcoin is just one type of cryptocurrency in a world of thousands of cryptocurrencies, with new types being developed every day. Aside from Bitcoin-specific wallets, there are a number of crypto wallet apps available to secure and hold your crypto assets. Some wallets may only support a single kind of currency, while other wallets are compatible with a number of cryptocurrencies and altcoins. These are known as multi-cryptocurrency wallets.

Each crypto wallet has a unique wallet address. Depending on which cryptocurrency you are

receiving, your wallet address may or may not change. For example, with Bitcoin, your wallet address changes after every transaction, but with Ethereum your address stays the same.

If you are looking to expand your portfolio and purchase a variation of currencies, it is often recommended to split up your holdings among several crypto wallets to better secure your assets. While there is nothing wrong with holding all of your assets in a single wallet, some may say that a single wallet with a large amount of coins can draw unwanted attention and be attractive to hackers or other cyber criminals. Moreover, with multiple wallets, you are less likely to lose access to your funds. For example, imagine keeping all of your crypto in one place and then forgetting your private key. You could lose access to everything. With multiple wallets, you can mitigate some of these risks.