[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/how-to-store-your-bitcoin-with-proper-wallet

How to Store Your Bitcoin with Proper Wallet

Bitcoin wallets **store the private keys you need to access a bitcoin address and spend your money. But which one is best for you? Read this article to find it out.**

Just like with your bank account or physical wallet, you need a place to store your bitcoins after you buy them.

Bitcoin is stored in digital wallets – a type of computer software that connects to the Bitcoin network. Just like bank cards have account numbers, digital wallets feature a unique address that can be shared with others when you make transactions.

This unique address is a shorter, more usable version of your public key. It consists of between 26 and 35 random alphanumeric characters and typically appears in this form: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

It is worth stating that every letter and number in this address is important. Always double-check a Bitcoin address before sending or receiving funds.

Absolute Confidentiality of Your Bitcoin Private Keys

In addition to the public key, a Bitcoin address also has a private key. And as the name suggests, this key should not be shared with anyone. Anyone with access to your private key can easily access your wallet and steal your funds. Similarly, if you fail to securely store your private key and you lose it, chances are that you may never be able to recover your bitcoin.

An easy way to understand public and private keys is to think of your public key like your home address. Anyone can see it and use it to send deliveries to your house, or in this case, transactions. Your private key is like the key to your front door. It is something that only you want to be in possession of, and it is what keeps other people from being able to access the contents of your digital wallet.

A private key is used to verify that you own the public key. It allows you to access your wallet and to sign off on transactions. Some wallets automatically generate a secure seed phrase; a set of words that allow you to unlock your wallet if you lose your keys. Print out this phrase or write it on a piece of paper and keep it in a safe place. Never take a photo of or take a screenshot of your seed words.

Bitcoin Wallets Options

Also, as with bank accounts, there are different types of wallets for storing your bitcoin, each offering its own set of pros and cons. In a broad sense, there are two main categories of bitcoin wallets:

Hot wallets: These types of bitcoin wallets are connected to the internet and are typically available online or on your smartphone.

Cold wallets: These types of bitcoin wallets cannot be accessed through the internet. They often involve physical devices (like a USB stick), where bitcoin and other cryptocurrencies can be stored securely offline.

Hot Wallets

Although relatively less secure, hot wallets are the most popular in the crypto world because of their convenience. Because hot wallets are already connected to the internet, it means people can access and exchange funds quickly – something that's important if you want to make quick trades when the crypto market is moving. Some popular examples in this category include mobile wallets (for example, BitPay), web or online wallets (for example, Coinbase) and desktop wallets (for example, Bitcoin Core).

When you register on a cryptocurrency trading platform, a web wallet will be automatically created for you to store your bitcoin. One of the downsides of using web wallets on exchange platforms is your private keys are being held by a third party. Remember the front door key analogy? Now, imagine someone else owning the key to your house. If they wanted to, the owner of the key could decide to lock you out or someone could break in without your knowledge if the owner lets the key slip into the wrong hands.

To put things in perspective, in 2019, the New Zealand-based exchange Cryptopia was hacked, and more than $17 million in ether and other cryptocurrencies was stolen, forcing the exchange to shut down. A former employee of the exchange was also convicted for stealing $170,000 in crypto by creating copies of Cryptopia's private keys and saving them to a USB. This gave him access to over $100 million in crypto.

On the flip side, an online exchange wallet is arguably the easiest to set up and use, and some leading exchanges now have insurance funds to compensate users in the event of a hack. It is worth noting, though, that this should not be exclusively relied upon.

As earlier mentioned, there are also mobile and desktop wallets (otherwise known as software wallets) that give you a greater level of control and security. Unlike the wallets created by crypto exchanges, most mobile and desktop wallets do give you access to your private keys. But that also means if your mobile phone is hacked or stolen, the thief might be able to get a copy of your wallet and your bitcoin. Software wallets, therefore, require greater security precautions. Electrum and Exodus are examples of software wallets.

Before downloading any software wallet, ensure you conduct your own due diligence and read the reviews of other customers. Also, confirm you are downloading a legitimate copy of a real wallet. Some shady programmers create clones of various crypto websites and offer downloads for free, leading to the possibility of a hack.

Cold Wallets

Cold wallets such as hardware wallets or paper wallets are the safest options when it comes to storing your bitcoin. These are completely offline products and cannot be accessed by the internet; meaning someone would have to be in the same physical location as the wallet to steal it. When you use an online paper wallet generator, however, it's important to note some can pose a security risk because you are trusting the website with key generation. If you do use one, be sure to verify the code has no backdoors (ways for the website developers to see your keys).

These are recommended if you plan to hold your bitcoin for a long time and don't plan to trade it frequently. But, once again, if you lose the hardware wallet, your bitcoin may be lost unless you have kept reliable backups of the keys. Some large investors keep their hardware wallets in secure locations such as bank vaults. Trezor and Ledger are notable examples of leading hardware wallet providers.

If you can't decide which wallet to use, don't worry. Many serious bitcoin investors use a hybrid approach, keeping most of their crypto wealth offline in a cold wallet while keeping a smaller

spending balance on a web or online wallet. This is the best of both worlds and ensures that your bitcoins are stored safely.