[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/crypto-wallet-public-vs-private-keys

Crypto Wallet: Public vs. Private Keys

When you first start using cryptocurrencies, you will hear a lot about “your keys” of crypto wallet. But there are two kinds: public key and private key. Read on to figure them out.

If you’re considering getting a crypto wallet, you’ve probably heard that it comes with a key. In fact, it comes with two keys: a public key and a private key. They are both essential, doing different and complementary jobs.

Public Key

The public key is used to send cryptocurrency into a wallet. The private key is used to verify transactions and prove ownership of a blockchain address. If someone sends you, say one bitcoin (BTC), a private key will be required to “unlock” that transaction and prove that you are now the owner of that bitcoin.

Think of your public key as your mailing address. Anyone can look it up and send things, in this case cryptocurrency, to that address. It’s similar to providing your checking account number and routing number to set up a direct deposit – you can tell that information to anyone, but it doesn’t allow them to withdraw money or otherwise log in to your account.

Crypto Wallet: Private Key

The private key on the other hand is for the wallet owner only. The private key functions as a password to your crypto wallet and should be kept secret. The thing you must understand is that if someone discovers your private key, they will have access to all the crypto in that wallet and can do whatever they want with it.

Private keys are numerical codes – but you may never see your actual private key. To make things more user-friendly, many wallet providers often encode your private key in a way that you can more easily record and remember.

Many wallets use a “seed phrase,” also known as a “secret recovery phrase,” to unlock your wallet. If you open a crypto wallet with MetaMask, you will be assigned a string of random words that you use to unlock your funds. Your private key is hidden inside the software behind this user-friendly string of words.

However, if you keep your crypto in an exchange wallet (such as Coinbase or Binance) or with a custodian, then that company holds your private key for you. Strictly speaking, it would control your funds on your behalf.

The function of the private key, technically speaking, is to “sign” transactions that use your funds. Transactions using your funds cannot be validated by the network without your private key attached. The public key encrypts transactions, which can be decrypted only by the corresponding private key. The technology is called public-key cryptography, sometimes abbreviated PKC, or asymmetric cryptography.

How Can You Store Private Keys

The last thing that cannot be stressed enough is that you must keep your private key or seed phrase or both safe and secret. Write it down and store it in several places because if you lose it or it falls into the wrong hands, there is no way to recover it. Don’t take screenshots of it or take pictures of it with your phone because these digital copies are often targets of hackers.