

Public Key:

Used to receive Bitcoins

Share this with anyone you wish

Private Key:

Used to spend Bitcoins

Never share this with anyone



HOW TO MAKE A PAPER BITCOIN WALLET

HOW TO MAKE A PAPER BITCOIN WALLET

A bitcoin paper wallet is simply a public and private key printed together. It is an offline wallet, and is usually regarded as a type of “cold storage” (extra-secure storage that does not make contact with the hackable internet), although it has some important differences that make its presence in that category debatable (more on this further down).

As the name suggests, paper wallets are usually made out of paper, although technically they could also be made of plastic or any other substance on which information can be durably printed.

via bitaddress.org

What is printed on the paper wallet are the private and public keys, usually in QR form, with the latter also serving as the address. You could just copy and paste the keys onto a text document and print that out (erasing the copy on the computer afterwards). Or you could use one of the free web services that generate the printable wallet for you. The key generation is usually done in your browser, so they are never transmitted on the internet. To be safe, you should clear your browser after printing. And never store an image of the paper wallet on your computer or phone.

Some paper wallet services have a nifty design that you can cut, fold and seal, making them a lightweight and relatively secure form of storing bitcoin offline. You send your bitcoin to the public address displayed on the wallet, and then store it in a secure place.

What makes paper wallets secure is that they are totally offline (generally known as “cold storage”). They are not within the reach of hackers, and your bitcoin are never trusted to a third party. As long as the paper wallet is secure, your holdings are secure.

But, therein lies the relative lack of security. Someone could find your hiding place, take your printout, spend all the bitcoin associated with those keys, and return the paper, so you would never know.

A more secure version would involve folding the paper so that the private key is hidden from sight, taping the fold with a seal that can't be broken and replaced (just search for “tamper evident seals,” there are many different providers and models), and making sure that the private key cannot be seen even if the folded paper is held up to the light.

via bitcoinpaperwallet.com

Even that is not particularly secure. What if the folder, drawer or box that you keep it in floods?

Sure, it's unlikely, but when you're securing a lot of bitcoin, it pays to think of worst case scenarios (and hey, what with climate change and all...). So, a tightly-sealed plastic bag would help.

How do you protect a paper wallet from fire? I have no idea. Keep it in the freezer? (That definitely would be "cold storage," he he.)

Also, paper itself is not the most durable of substances. Apart from the obvious risks of fire or water damage, the ink could fade with time, making the keys unreadable. No readable keys, no bitcoin.

Even with paper wallets, you can check your balance at any time using blockchain.info (just type your public key into the search box). And most online wallets allow you to import your paper wallet data. To spend those bitcoin, you will be asked to type in the private key information, or scan the private key QR code (sometimes called the "spend" QR code).



SOME GOOD PAPER WALLET GENERATORS

Bitaddress.org and Walletgenerator.net are open-source random address and key generators that uses your browser's JavaScript engine, so no keys are sent over the internet. And moving your mouse around to create entropy and mix up the characters even more is fun. That random sequence is then used to generate your public and private keys, which are displayed on the next screen for printing.

Bitcoinpaperwallet.org will create a printout of a colourful paper wallet, with the appropriate fold lines, and will sell you tamper-evident stickers for sealing it shut.

Mycelium offers an original and even more secure way to generate paper wallets, with a USB dongle that you plug directly into your printer. The device generates a paper wallet that automatically gets printed out, without ever having touched your computer.



