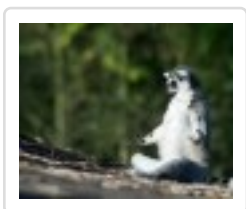


[Alternative Blockchains](#)[Bitcoin](#)[Business](#)[DApps & DAOs](#)[Editor's Choice](#)[Internet & Deep Web](#)[Privacy](#)[Reviews](#)[Trading & Investment](#)

Bitcoin Wallets Explained: How to Choose the Best Wallet for You

[Article Search](#)

Dean March 14, 2015 Bitcoin, Editor's Choice 2 Comments

**Dean**

Owner, Editor, and lead writer for Cryptorials.



[Cryptocurrency](#) writer and trader since 2014.

AMA Anytime: 21.co/cryptorials

**Make Money Online
Without Investment**

Get Free Money Now.

www.paidonlinesites.com

Wallets are one of the first things that you will need to learn about when you first get started with [Bitcoin](#). They are also one of the most important. Your choice of [wallet](#) will determine how safe and secure your coins are. It may determine how much you pay in transaction fees and whether you get any choice in the matter (you can actually submit transactions with no fee at all, it's just that they will take ages to get

processed by miners and may even be ignored forever in extreme circumstances). It will determine whether you can access your coins from anywhere or just your home computer. Because your wallet is the place you go to whenever you want to use Bitcoin, it will also be the biggest factor in your day-to-day experience – whether using Bitcoin is easy or hard, fun or unpleasant. And of course there are also many wallets which will offer you extra bonuses and advanced features which you won't get elsewhere. As a result, getting the best wallet – or more accurately the right wallet for you – should almost certainly be your highest priority once you've decided to start using Bitcoin.

Unfortunately, it isn't always easy to choose the best wallet if you are a beginner. This is because there are loads of different types out there, and the differences between them may not be immediately obvious or easily understandable if you don't know much about how Bitcoin works.

Bitcoin Explained: What is a Wallet & How Does it Work?

There is a great deal of misunderstanding, even amongst people who consider themselves quite experienced and knowledgeable Bitcoiners, about what a wallet actual is. The analogy with a physical wallet which you may use to carry your banknotes and credit cards around is useful. You open up your wallet software, it tells you how many coins you have, and you can then take coins out and give them to somebody else by just choosing an amount and clicking send. It appears, for all practical purposes, as if your coins are stored inside your wallet. In actual fact that is not exactly true, and understanding why will make you an instant expert on this subject – and will make it a lot easier to choose which software is best for your needs.

Your coins are not stored in any single location. They are stored inside the [blockchain](#) – a shared record which every part of the network uses. That is why you don't need to have your wallet open to receive coins –

**MAKE ANY INTI
CONNECTION S**



Avoid the Dangers of Pu

START NOW

Tags

anonymous
beginner's guide
Bitshares blogging bounties
cards Counterparty
crowdfunding dark
markets DECENT
decentralized alternatives
decentralized apps decentralized
exchange decentralized
markets
decentralized media
deep web earn
bitcoin earn

because they aren't actually sent to you, the shared record of ownership is simply updated to reflect the fact that you own them. This shared record, called the blockchain, is constantly updated with every transaction and therefore the balance of coins held by each address. In order to be able to spend your coins, all you need is to broadcast your wish to other people on the network, where it will be passed on and spread to everyone on the network. But to prove that you are the person who really owns that address and has the right to spend those coins you need to 'sign' the transaction with a kind of strong password called your '[private key](#)' or 'secret key'. Every address has a private key which is created at the same time as the address itself. It is this private key, which would be difficult to remember and awkward to type, which may be stored inside your wallet.

A wallet is therefore a piece of software, sometimes called client software, which at least provides the following basic functions:

- Creates new addresses with their corresponding private key
- Tells you how many coins are held by your addresses
- Uses your private keys to sign transactions so that you can spend your coins

Any particular piece of client software may create and control multiple different addresses. This is useful as you can have, for example, an address for business and another for personal. Even if you do have multiple addresses, however, you can often take coins from multiple addresses to make a single payment. You can choose how many coins to take from each of your addresses using a feature called 'coin control' – something not every wallet will support.

cryptocurrency

ecommerce email

Ethereum
exchanges FoldingCoin

gambling games hardware

how to buy bitcoins ICO

investment jobs

maidsafe margin trading

mining NXT publishing

security shopping

smart contracts social

networking Syscoin TOR

trading VPN

wallets website

publishing

Subscribe To Blog Via Email

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Join 317 other subscribers

85% Profit per Trade?

Trade NOW



bitplutos

Bitcoin Wallet Types Explained

There are various different types of Bitcoin wallet, each of which has its own advantages and disadvantages. If you read the section above, even if you only vaguely followed it, you should now be able to easily understand these different types and how to choose between them.

Desktop Computer Wallets

This section includes any software which you download and install on a PC or laptop. Desktop software gives you complete control over your coins, meaning that you don't have to trust a third-party not to lose or steal them. If you follow [good security practices](#) then this option should be safer too, as it is easier and more rewarding for hackers to target central servers to steal many people's coins than to target each individual's computer one by one. But, on the other hand, you have full responsibility for securing your own coins against hackers and computer malfunctions.

Bitcoin Core – Running a 'Full Node'

A [node](#) is simply a point on a network – in this case your computer. Running a [full node](#) just means that you have the whole blockchain downloaded on your computer and kept it up to date for you to reference when making a transaction. The blockchain has already grown very large, and just keeps getting bigger, so it takes ages to download and can be a hassle to keep update or 'synched' (synchronized) with the rest of the network. Because of this most regular users don't want to run a full node. Miners, developers and service providers need to, but you probably don't – if you choose to, however, you will be making a contribution to maintaining the decentralized Bitcoin network and its [distributed consensus](#).

You can go here to [download Bitcoin Core](#)



[Advertise with Anonymous Ads](#)

Lightweight Desktop Wallets

Using software which runs on your own computer but doesn't need the whole blockchain means that you get all of the advantages of a desktop wallet without the hassle of running a full node. Your private key is held on your computer, meaning that you retain complete control. Most desktop wallets today fall into this category so there is a lot of variety here. Popular choices include [Electrum](#) and [Multibit](#).

Wallet Apps

Installing your wallet as an app on your mobile phone or tablet has many advantages. If you are going to use it for shopping in bricks & mortar stores, for example, then it is a must. What some people don't realize, however, is that these apps fall into two categories just like the ones you might use from a desktop: locally run apps, where the whole software is downloaded (the equivalent of the lightweight client above) and web services where the app is just another way to access the same service you would access by visiting the website.

Running an app locally on a mobile device is actually even more secure than running it on a desktop computer, because mobile devices are less susceptible to viruses.

One popular choice for Android is [Bitcoin Wallet](#), whilst Apple users may want to take a look at [Breadwallet](#)

Browser Wallets with Client Side Key Generation.

A browser wallet is designed to give you the advantages of both the desktop wallet and a web wallet.

When you first sign up to a service like this it uses a password you provide (pick a strong one!) and runs it through a cryptographic program to generate your public and private keys. You can then log in to your wallet anywhere, from any device which has a browser. But

rather than logging you into a server which stores your private key, you are effectively re-generating your private key cryptographically every time you log in. This private key is then used to sign transactions within your browser – but never actually leaves your browser. This offers a good balance between the security of a desktop wallet and the convenience of a web wallet.

A good example of this type is [The Browser Bank](#)

Web Wallets

Web wallets store your key for you on their servers. You can then log in to your account with them to access your coins. This means that you can access your coins from any device and you don't need to take responsibility for security yourself. On the other hand, you are trusting a company not to disappear with your coins, and to be able to keep them safe on your behalf. You will usually, though not always, be able to choose between using an app on your mobile device, or using your browser on a personal computer.

Popular choices include [Coinbase](#) and [XAPO](#)

Multi-Sig Wallets

Multi-Signature is kind of like a joint bank account – two people need to sign a transaction before it is sent out. You can use this yourself to secure your savings by requiring both you and your partner to sign, or in a business to protect against employee theft. It can also be used by service providers to offer you increased security for your account by giving you your own private key, but also setting up 2 factor authentication and signing with their key.

One example of the use of [multi-sig](#) for improved security is [GreenAddress](#)

Hardware Wallets

For large amounts of savings some people like to use a piece of hardware which was custom designed for keeping Bitcoins safe, rather than their phone or computer. These are simply called hardware wallets and are often used for ‘cold storage’, which means long term savings which you don’t need regular access to.

Popular examples include [Trezor](#) and [Ledger](#).

Paper Wallets

As I explained in the first section of this post, your coins are not actually stored inside your wallet. The wallet software itself is just used to sign transactions, whilst the coins themselves are stored inside the blockchain which is the shared record used by all Bitcoiners. This means that you don’t actually need to use any kind of electronics or software to store your coins – all you need is your private key. When you want to spend your coins, you can then ‘import’ this private key into the kind of software described above in order to be able to use it.

A paper wallet is therefore just a piece of paper with your private key written or printed on it. The advantage of this is that somebody would have to physically break into your property (and perhaps then your safe or lockbox) in order to steal your coins – they can’t be stolen by hackers.

There are various online services which help you to key pairs and print them out in an attractive design, such as [BitAddress](#).

Brain Wallet

Brain wallets use a similar principle to paper wallets, but try to take it to the next level – so that there is not record of your private key or how to access it anywhere apart from in your own brain. A cryptographic program is used to generate your private key from a passphrase (usually at least 12 words) or mnemonic which you can remember. This same passphrase can then be used to re-generate your private key to

import into a wallet program, but in the intervening time there would be no electronic or written record of your private key anywhere.

Check out this Cryptorials article on [How to Make and Use a Bitcoin Brain Wallet](#)

For a comparison of different service providers in each section with their main features, please take a look at our [Comparison of the best Bitcoin wallets](#).

Related



[Bitcoin Brain Wallets Explained: What They Are and How to Make One](#)

April 8, 2015
In "Bitcoin"



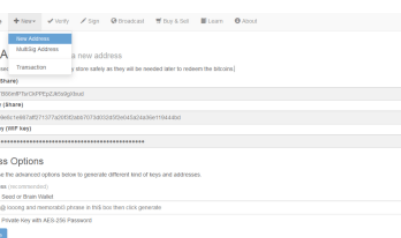
[How To Use Bitcoin Anonymously](#)

May 22, 2015
In "Bitcoin"



[Anonymous Bitcoin Wallets Explained](#)

February 28, 2017
In "Bitcoin"



[Bitcoin Brain Wallets Explained: What They Are and How to Make One](#)

April 8, 2015
In "Bitcoin"



[How To Use Bitcoin Anonymously](#)

May 22, 2015
In "Bitcoin"

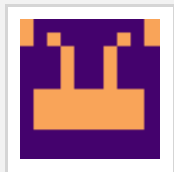


[Anonymous Bitcoin Wallets Explained](#)

February 28, 2017
In "Bitcoin"

bitcoin explained, wallets

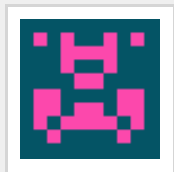
2 Comments Already



here it is - February 26th, 2017 at 5:31 am

We can always appreciate a good paper wallet. They'll last forever in a secure physical location.

[Reply](#)



CoinFunda - March 18th, 2017 at 2:29 am

Hi,

Thanks for the info. really nice post. which one is more secure paper wallet or hardware wallet.?

[Reply](#)

Leave a Reply

[« A Beginner's Guide to Smart Contracts](#)

[How To Make Money Trading Bitcoin »](#)

Partners



[Advertise with Anonymous Ads](#)

Latest Posts

Cryptocurrency combines with forex trading technology in Compcoin ICO

e-Government: Blockchain vs Traditional information systems

Tips For Staying Safe

Top Posts



The best cryptocurrency investments for 2017



How To Access The Deep Web or DarkNet - A Beginner's Guide



Dark Markets: How to Buy Things from the Deep Web's Black



When You Gamble With
Cryptocurrency

My Long Awaited
Altcoin Trading Article:
STOP BUYING
ALTCOINS THEY ARE IN
A MASSIVE BUBBLE

Orocrypt ICO: Own a
share of a gold backed
cryptocurrency network

Wagerr Decentralized
Sportsbook: ICO
Crowdsale; 'Be The
House' Oracle
Opportunities

Biggest Bitcoin Casino
Jackpot Winner



Markets
How To Earn
Bitcoin Playing
Fun Games (No
Deposit Needed)
How Anyone Can
Make Their Own
Digital Currency
Cryptocurrency
combines with
forex trading
technology in
Compcoin ICO
How To Mine
Cryptocurrency
on a Normal
Computer

How
Bit
& 1



All Content is Available as Creative Commons - Attribution
Required.

FROM **3%** TO **6%**
DAILY INTEREST