



Bitcoin Starter Guide

Storing and
Securing Bitcoins





Introduction

In this guide, we explore the popular types of bitcoin wallets, offer guidance on using a wallet and pass along wallet security tips and best practices.



Table of Contents

Bitcoin Wallet Basics	3
Choosing a Wallet	
A Look at the Bitcoin Wallet Universe	4
Five Popular Wallet Types	5
Using a Bitcoin Wallet	6
Bitcoin Wallet Security	
Seven Tips to Live By	7

Bitcoin Wallet Basics

Before making purchases and payments in bitcoin, you must have a bitcoin wallet. Unlike a physical wallet, a bitcoin wallet virtually stores and secures your digital currency. The wallet holds the public and private keys associated with the bitcoins that you own and the addresses used for transactions.

Bitcoin transaction records are straightforward and typically include:

Input: Addresses used to send the original bitcoins

Amount: Number of bitcoins sent and received during the transaction

Output: Address of the recipient



A variety of wallet options exist, each holding benefits and drawbacks. Selecting the most appropriate wallet is a personal choice dependent on three key factors:



Device usage



Security preferences



Transaction speed needs

Choosing a Wallet

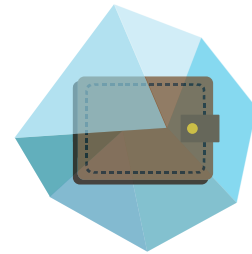
A Look at the Bitcoin Wallet Universe

Hot vs. Cold Wallets

The two most popular wallet types are “hot wallets” and “cold wallets”. A hot wallet refers to an online bitcoin storage solution that is connected to the Internet. The key benefit of using a hot wallet is the ability to instantaneously transfer funds. While these wallets provide great ease of use, they are more vulnerable to hackers and digital malfunction.



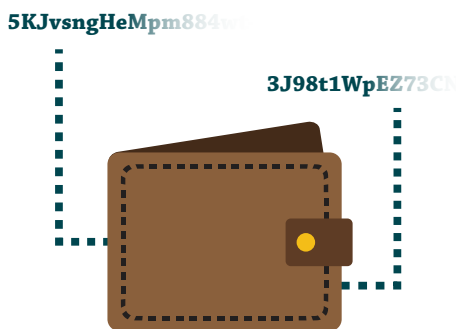
Cold wallets are not connected to the Internet thus making them considerably less vulnerable to hackers and cyber criminals. Since they are offline, there is some manual labor involved in conducting transactions using a cold wallet. Users can create unsigned transactions online, sign them offline using their cold wallet and then send the signed transaction to an online device. While more secure, the transaction process is more cumbersome when using a cold wallet.



Multi-Sig Wallets

Though not yet widely available, multi-signature wallets require more than one private key signature in order for funds within a wallet to be spent, enhancing a wallet’s security. The technology has promising implications for companies as well as individuals.

For businesses working from a shared bitcoin wallet, multi-signature technology could require a majority of those with access to the wallet to sign off on any transactions before a transaction goes forward. For individuals, requiring more than one signature will decrease the chances that a wallet can be compromised by a hacker obtaining a single private key from a device like a mobile phone.



Five Popular Wallet Types

Online Wallets



Online wallets are the prototypical “hot wallet”, giving users the ability to make instantaneous payments and transactions. Another key advantage of online wallets is that you can access them from anywhere, regardless of which device you are using. Because these wallets store your private keys online, in a database often controlled by a third-party provider, they are more vulnerable to hacking.

Mobile Wallets



If you want the ability to send bitcoin payments instantaneously but want to do it anywhere and anytime, a mobile bitcoin wallet may be the right option for you. Mobile wallets come with all the risks of online and mobile devices inherently present their own unique challenges. A stolen mobile device that is not properly secured can give unauthorized users access to your account.

Desktop Wallets



Desktop wallets, or software wallets, involve software that is downloaded onto a bitcoin user’s computer. These wallets allow for greater control over the data stored in a bitcoin wallet and greater security since access to data is not stored in the database of a third-party provider. Setting up a desktop wallet, however, is less instantaneous than an online or mobile wallet.

Hardware Wallets



Hardware wallets are often referred to as “cold storage” because these devices allow for sensitive data to be held completely offline. Hardware wallets allow users to create private keys and sign transactions offline before entering them into the online blockchain. This creates a safer storage space and reduces the threat of cyber attacks.

Paper Wallets

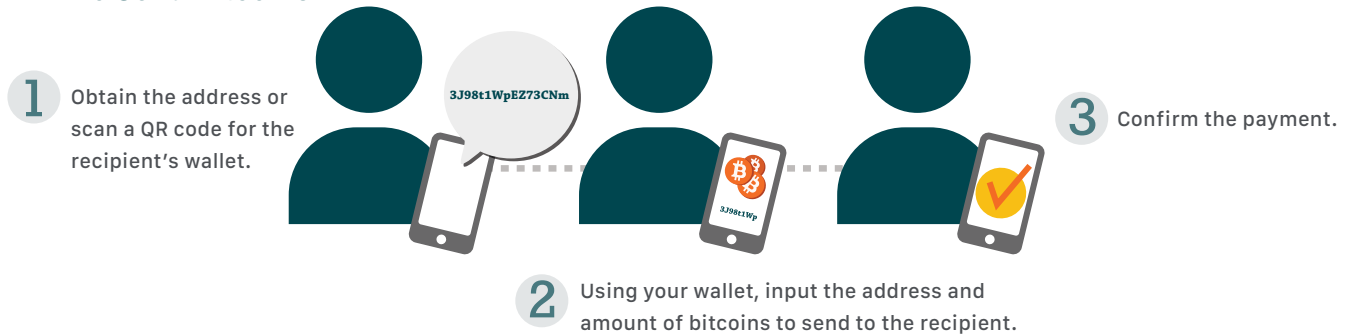


A paper wallet is the most secure wallet option for those who are concerned about online theft or data loss. A paper wallet is beneficial in that no computer malfunction or hacker can threaten your account. However, these types of wallets also require a great deal of diligence from their owners, who must update and discard of wallets after transactions. A paper wallet can be created by printing the private keys associated with each address and will often contain QR codes that users can quickly scan in order to use coins.

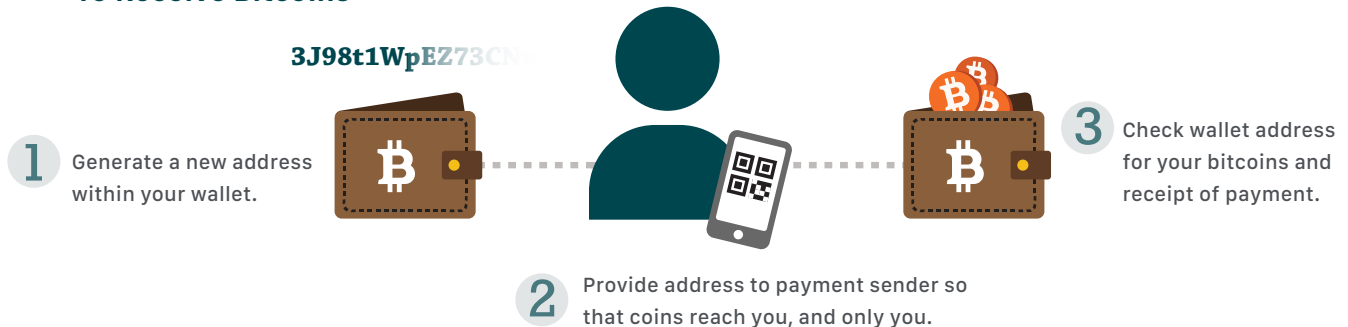
Using a Bitcoin Wallet

A bitcoin wallet is essential for creating transactions within the Bitcoin system, whether they are from an individual, purchased on an exchange or are doled out as rewards for bitcoin mining.

To Send Bitcoins



To Receive Bitcoins



Though information such as the number of bitcoins associated with each address can be publicly viewed via the blockchain, it is impossible for someone to access an address belonging to you without your private keys. While an address can be derived from a private key, those who view an address have no way of constructing the key that unlocks the bitcoins associated with an address.

Remember, because the bitcoin system does not require the transmission of personal data (name, bank accounts, social security number, etc.), your bitcoin wallet is essential to identifying you and validating the transfer of ownership of bitcoins. Unlike a bank account, the wallet provider you choose cannot see your balance or interfere with your accounts.

Bitcoin Wallet Security

Seven Tips to Live By

When using a bitcoin wallet, several risks exist including, a hacked wallet provider, loss of digital keys or passwords, loss of mobile devices connected to your wallet and computer and software malfunction. Even in the case that you opt for a hardware or paper cold wallet, the risk of theft or device loss still presents security risks. Below, we highlight seven ways to ensure you are optimizing your wallet security:

Use a Strong Password and Encryption

Though many believe that risk is inherent with use of a digital currency, there are many steps that can be taken to secure the data associated with your bitcoin wallet. Choosing a strong password is a fundamental first step. Bitcoin users should also consider encrypting data and backup data stored online to provide an additional layer of security against hackers.



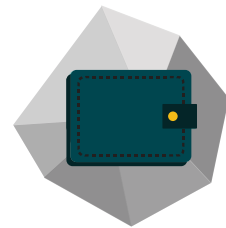
Backup Your Wallet Often

As with all things digital, backing up your wallet should be a top priority to ensure that data, and thus your bitcoins, don't go lost or missing. A quick backup of your bitcoin wallet can solve a number of problems that arise with both online glitches and user error. Diversifying backup devices by using items like cloud-based storage and USB drives can also help keep data safe and accessible in case one method of backup fails.



Use Cold Wallets

Storing some, or all, of your bitcoin wallet data offline, in cold storage, is one way to ensure the security of your digital currency. Removing data from the Internet eliminates the risk of software failure or damage that could be done by malware or hackers.



Keep Wallet Software Up-To-Date

Updating your wallet software is an important, and easy, step that can be taken to prevent future issues. This is especially important when it comes to using hot wallets, particularly mobile wallets. Simply put, when a new version of your bitcoin wallet is released, you should be sure to update your software. Software updates address glitches or bugs in the previous version and are necessary to keep your wallet working seamlessly with the ever-evolving Bitcoin system.



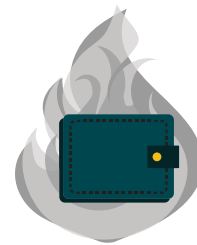
Do Not Share Private Keys or Wallet Passwords

Anyone with access to your private key codes can utilize them to spend your bitcoins. Thus it is imperative that your private keys are stored safely and remain completely private. Do not casually share this information or leave a record of this sensitive data where it can easily be found.



Treat Your Hot Wallet Like Your Cash Wallet

Only keep those bitcoins that you are ready to spend immediately in hot wallets. Having bitcoins in a wallet connected to the Internet is like having cash in your wallet -- it is easier to steal. While hot wallets make performing a transaction quick and seamless, remember that if your wallet is compromised, the bitcoins in it are gone forever. Instead of keeping all of your bitcoins in a hot wallet, transfer the bulk of your digital currency to cold storage. Then move funds to your hot wallet as needed.



Make a Succession Plan

Finally, include instructions for your bitcoin account in your succession plans. If something suddenly happens to a bitcoin user, and they have not made arrangements for their loved ones to access their private bitcoin data, access to those bitcoins could be lost forever.



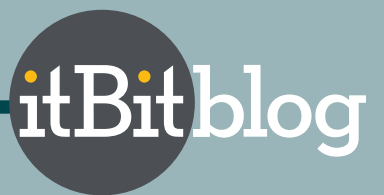


**Bitcoin
Starter Guide**
Bitcoin Basics
and Benefits

Bitcoin Starter Guide Vol. 1

**Bitcoin
Starter Guide**
Acquiring and
Using Bitcoins

Bitcoin Starter Guide Vol. 2



Visit the itBit Blog to view
our latest digital currency
articles and research.



Start trading today

Open New Account

Learn More about itBit

Connect with itBit



Legal Disclaimers: The information contained in this itBit Welcome Guide (this "Welcome Guide") provides only a general overview of itBit Pte. Ltd. ("itBit"). Accordingly, while itBit makes every attempt to ensure that the information contained in this Welcome Guide is true and accurate when made, itBit is not responsible for any errors or omissions, or for the results obtained from the use of the information contained herein. All information in this Welcome Guide is provided "as is," with no guarantee of completeness, accuracy, and timeliness or of the results obtained from the use of this information. In no event will itBit, its related entities, or the owners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information contained in this Welcome Guide or for any consequential, special or similar damages, even if advised of the possibility of such damages.

In no event shall the information contained in this Welcome Guide be construed as the rendering by itBit, its related entities, or the owners, agents or employees thereof of professional advice or services. As such, the information provided in this Welcome Guide should not be used as a substitute for consultation with professional advisors. Before making any decision or taking any action regarding trading, you should always consult with a licensed financial advisor and tax advisor to determine the suitability of any investment. Bitcoin trading involves a high degree of risk. The Bitcoin market is new and unproven and may not grow. Currently, there is relatively small use of Bitcoin in the retail and commercial marketplace in comparison to relatively large use by speculators, thus contributing to price volatility that could adversely affect an investment in Bitcoin. It should not be assumed that trading Bitcoin will be profitable or that it will not result in losses. In order to participate in the trading of Bitcoin, you should be capable of evaluating the merits and risks of the investment and you should be able to bear the economic risk of losing your entire investment. No material contained in this Welcome Guide should be considered as an offer by itBit to sell or a solicitation by itBit of any offer to buy Bitcoin.