Store your bitcoins properly...

This article is going to discuss the many ways of storing your bitcoin. There are many ways of bitcoin storage and many different types of wallet software. Storing bitcoins does not involve storage of actual bitcoins per se, but involves the safe storage of the private key to the wallet addresses.

Bitcoin works based on public/private key pairs, the public key being the public address for receiving payments, the private key is used to sign the transaction to send coins from that address. Storage of the private key is stored in a 'wallet' and there are many different ways in which to do it, each with varying levels of security. The first wallet to be discussed is the bitcoin QT wallet which is also the reference wallet from the bitcoin core developers.

Bitcoin QT Wallet

The bitcoin QT wallet, or bitcoin core is the reference client. This wallet is the original wallet, created by the bitcoin core developers. This wallet is designed for use on desktop and laptop computers and stores the private keys in a file on your machine. It has many features, as well as being a wallet is acts as a node on the bitcoin network. As a result, it must store a full copy of the blockchain.

It can send/receive coins, save lists of sending and receiving addresses that are known, and also offers wallet encryption. This scrambles the private keys with a password which must be used when you want to send coins. Loss of the password means the coins are forever lost unless you have a backup of the private keys. The next section will discuss the advantages and disadvantages of the bitcoin QT wallet.

Advantages

Easy to use and intuitive.

Supported by the bitcoin core developers.

Reliable software.

Disadvantages

- Must store a full copy of the blockchain. This is 60+GB in size as of August 2016.
- Risk of coin theft if computer is infected with malware. Even if the wallet is encrypted due to loading of private keys in system memory.
- Lacking Multi-Signature support.
- Must wait for blockchain to synchronize which can take hours or days before using the wallet.

Summary

The bitcoin QT wallet and other desktop wallets are good wallets for starters, but a good specification of machine is needed to use it and it must download the entire blockchain. For limited bandwidth internet connections and machines with a small hard drive this is not a good option. It should not be used to store large amounts of funds due to the security implications, and backups of the wallet file should be taken.

Web Wallet

Another way to store bitcoins is on a Web Wallet. This is a wallet which is hosted by an external provider who also stores the private keys and has a web front-end for you to send coins. An example of this is blockchain.info. They are designed for ease of use and convenience in mind. This section includes exchange wallets.

Web wallets are easy to use and many allow import of your own private keys. This is handy for novice users and some also have mobile applications to allow mobile payments. There are security implications, some of which can be negated, but others are a serious risk. Theft of your login details through hacking can be negated by enabling 2FA or two-factor Authentication. This is where an SMS is sent to your mobile phone or similar, requiring the compromising of two devices.

However, a good rule of thumb is to assume you are not in ownership of even your own coins if you do not exclusively control the private keys. The wallet provider could steal your coins, or be compromised which can result in coin theft as shown here.

There is however an exception to this rule, which will be discussed in the next section.

Advantages

- Easy to use, with plenty of choice of providers.
- Good for small amounts of coins and everyday transaction.
- Accessible from anywhere with an internet connection.
- Secure partially against malware on the user's system if 2FA is enabled.

Disadvantages

- Security Implications and risk of coin theft.
- Lack of control with some providers.
- Lack of system transparency.

Summary

The web-based wallets are easy to use for beginners and are good for storing everyday amounts of coins. This also includes exchange wallets, which if a large amount is to be transferred / exchanged it should be done in smaller blocks and never stored in it long term, $1000s of coins can be stolen/vanished in an instant in the event of the wallet provider being hacked. It is therefore one of the least secure ways to store coins, along with desktop wallets.

Coinbase Multi-Sig Online Wallet

A multi signature online wallet is a type of online wallet that uses more than one private key. I will use the coinbase multi-signature vault as an example. These work by storing three keys typically. The design is one of the best balances between convenience and security, and protects you if the wallet provider is hacked/becomes insolvent in the case of coinbase.

These wallets work by having three keys. One is held by coinbase themselves. A second is created on your machine, encrypted with a passphrase that is not sent to coinbase and then transmitted and stored on their system, this is the ‘shared’ key. The third key or ‘user’ key is held by you only and along with the encrypted shared key printed out by the user as a backup.

This wallet works on a 2-of-3 system, to withdraw coins you log into your coinbase online account and it sends the encrypted key to you (behind the scenes) and you simply enter your passphrase to withdraw it. If coinbase becomes insolvent, you can recover your coins by your passphrase and the third ‘user’ key. If you forget your passphrase, you can supply coinbase with the user key and recover your coins that way. It allows for convenience and high levels of security, provided the wallet is set up on a non-compromised machine it is the safest online wallet present and is in a class of its own in terms of security for an online wallet. This is safe for long term coin storage.

Advantages

- Reasonably easy to use.
- Convenient, yet highly secure.
- Funds can be transferred and moved without coinbase.

Disadvantages

- The user must store the user key and / or remember their passphrase. Losing the user key and forgetting their passphrase would mean the funds are lost. Multiple copies should be stored safely.

Requires trust that coinbase does not modify the front-end software to transmit the passphrase.

Moving the funds without coinbase must be done on a secure machine.

Summary

This is the most secure online wallet on the internet for bitcoins and is recommended if you wish to store coins online with the convenience of an online wallet, yet with security close to hardware or paper wallets. It is immune to government seizure of coinbase, and hacks to coinbase, as even if the coinbase key is stolen, it is useless on its own, and the key held by both you and coinbase is encrypted and never decrypted on their servers.

The next section is going to discuss hardware wallets.

Hardware Wallets

Hardware Wallets are a type of wallet which are an external piece of hardware to your computer. Some resemble a USB memory stick, others resemble a little device, but nearly all of them use USB. This section will discuss and compare two different brands of hardware wallets. Hardware wallets have a security advantage that transaction signing only occurs inside the machine, meaning malware cannot snatch the private keys from system memory. They are as secure as paper wallets in many ways. The two brands which will be compared are LEDGER and TREZOR.

LEDGER

Ledger is a brand of hardware wallet which resembles a USB stick. Ledger works through its own application which is a chrome browser plugin or online plugin. It works by sending the transaction to be signed inside the device which is secured with a PIN which after 3 incorrect attempts wipes the wallet. The device is like a smart card. It also sends a challenge with a visual indication of the address you are trying to send coins to, on an external device such as a mobile phone or uses a security card, to verify that malware has not changed the address you are sending coins to.

The ledger much be set up on a secure machine as it displays it’s recover seed which can be used to rebuild the wallets private keys if the wallet is lost or damaged. This should be printed out, never saved on any machine that is connected to the internet and stored safely. The ledger is a high security solution and is many times more secure than generic online wallets and the bitcoin QT client and can be carried and used on a set of keys. The ledger wallet application does not need administrator privileges to install and can be used safely on an untrusted machine. The ledger can have multiple ledger wallets in a multi-signature configuration for further security.

TREZOR

A TREZOR Wallet is similar to LEDGER, but it is a bit larger and connects to the USB port via a cable. It works in a similar way but has a screen and two buttons on the device, the screen shows the wallet address you are sending coins to and you press the buttons to confirm/cancel the coins, this is a security measure to ensure you are sending the coins to the intended address. This is a high security option and the TREZOR can also use a longer password.

The security of the TREZOR is possibly the highest of any hardware based wallet solution, and uses the same recovery seed method as the LEDGER.

Advantages

> Very high degree of security, very hard to attack and in the case of using them in a multi signature configuration, almost impervious even to theft through the users themselves without all parties consenting.
>
> The most secure ways to store coins, even more secure than paper wallets as paper wallets are vulnerable to theft of the raw private keys when it is entered.

Portable, the same private keys can be loaded onto multiple hardware wallets via the recovery seed.

Disadvantages

Upfront cost, ledger starts at £20 GBP, the TREZOR at £90 GBP.

If used without multi signature, does not stop employee theft within a company, this can be negated.

The physical device is needed to send/receive coins, although the seed can be imported into many desktop wallets such as electrum.

No protection against forced sending of coins, for example at gunpoint. LEDGER is working on plausible deniability features by use of a second password which takes the user to a dummy wallet.

Summary

The hardware based wallet solutions are practically impervious to all methods of attack. There is a small vulnerability in LEDGER, where use of the ledger with the security card on an infected machines many times over can potentially get enough information to decipher what is on the security card. This can be negated by using the mobile device authentication. With this in mind, and especially when used in a multi-signature configuration hardware wallets are impervious to nearly all types of attack. Use of any hardware wallet other than these two should be researched as vulnerabilities in the random number generators used for the private key generation used in any type of wallet can be a risk if it is not truly random.

They still must be set up on a secure machine, provided this is done they are the best method of storing coins long term and are impervious to attack from nearly all vectors. To avoid the risk of damage by fire/flood or other disaster the seed should be saved in multiple locations. There is an option on TREZOR to encrypt this seed with a passphrase. Provided these precautions are followed your risk of theft or loss is almost zero, minus being forced at gunpoint to send coins. This can be negated by splitting your holdings to multiple wallets, or use of multi-signature.

The next wallet to be discussed is mobile wallets.

Mobile Wallets

Mobile wallets are bitcoin wallets stored on your mobile phone, tablet, iPod touch or another portable device. They can be used when out and about for shopping and paying for coffee, among other things if a merchant accepts bitcoin. They typically scan the receiving address as a QR code. These are typically protected with a PIN. They can be further secured by encryption of your phones device memory. Android can enable this feature. They are good for everyday amounts of coins, but backups of the wallet file should be taken. Due to their weak PIN that is often used they should be stored offline. They are reasonably secure, unless your device is rooted and at risk of malware, or your device is lost without a backup.

Due to the weak PIN often used, encrypting your device with a password and ensuring the wallet is on the device or the SD card is also encrypted, but have a lower chance of infection than a Microsoft windows desktop wallet. There have been known instances of many mobile wallets being emptied due to a weakness in the random number generator, resulting in many private keys being cracked by an external hacker by testing every possible combination of a random number generator which was not truly random, article shown here.

Advantages

- Portable, and most people have their phones with them at all times.
- Simple to use.
- Wallet can be moved to another device easily if need be.
- Can be used when out an about at merchants which accept bitcoin.

Disadvantages

- If device encryption is not used, has security risks.
- Less secure than hardware or coinbase multi-signature wallets.
- Known weaknesses in android’s random number generator left many mobile wallets vulnerable, although this problem can occur with any type of wallet.

Summary

A mobile wallet is good for a small amount of coins. They have their advantages for sending and receiving small amounts, and with their QR code scanner they can easily be used to pay for coffee and the likes at merchants which accept bitcoin, for example. They have security implications but can be used for every day sending of coins in a reasonably secure way. They are no less secure than the average online wallet if a backup is taken and your phone is not rooted/jail broken and malware free.

The final wallet to be discussed here is a paper wallet.

Paper Wallet

A Paper Wallet is a secure way to store bitcoins offline. It involves printing out the private public key pairs in plain text and as a QR code for easy scanning later. They should never be generated online but instead generated on a secure machine using local software. The receiving address can safely be stored on your machine to top it up at any time but the private key should only be stored on paper. The paper wallet can be printed multiple times and should be stored in multiple locations in trusted places.

A paper wallet has a very high security margin, and can be further secured against theft by storing the private keys encrypted with a passphrase on the paper. These wallets however can be at risk from theft if an insecure computer is used to import the private key when you want to use the funds, so care should be taken here. In the event of a plain text paper wallet, theft of the paper wallet can result in coins being stolen if you do not move them before the thief does. The wallet can be disguised as something else if need be.

Advantages

> Secure, versatile and safe from most sorts of digital disasters, including EMP explosions which can damage any electronic devices in the vicinity.

- Easy to copy, store and distribute.
- Can be used as a gift of bitcoin.
- More secure than most wallets.
- In the event of death of the coin holder, plaintext wallets can be recovered by surviving family easily.

Disadvantages

- Multiple copies should be stored, to secure against fire and flood.
- Not as secure as LEDGER and TREZOR wallets due to the risk of theft upon import on an insecure machine.
- Research on generation software should be done, flaws in the random number generator can render the wallet unsafe. The wallet should always be generated on an offline or secure machine.
- Can be more inconvenient to import.

Summary

Paper wallets are among the most secure forms of wallet, alongside hardware wallets. Their security is almost tied, but the hardware wallets are more secure after initial setup due to their ability to be used on even a compromised machine safely. Paper wallets could be set up in a multi signature configuration which would bring their security on par with hardware wallets. For long term storage of coins, they are a great option and one of the best on par with hardware wallets, but for large sums should be encrypted with an easy to remember passphrase or disguised. If the coin holder dies provider family members know where to find the wallet these can be the easiest to recover. They are the most reliable way of storing coins if multiple copies are saved, although hardware wallets can be recovered with their seed.

Security tips

Security tips when using any kind of bitcoin wallet are below:

Use well-known audited software, and do your research.

Never store large sums of coins on an exchange or online wallet, apart from the coinbase multi signature option. Large thefts and losses have occurred, as shown here.

Store paper wallets safely. Backup wallet files and/or seeds.

For long term storage of large sums of money, use only hardware or paper wallets.

Exchange your funds in blocks rather than all at once.

Store funds in multiple wallets if you have large holdings.

Never store large amounts of funds in unencrypted wallets or store private keys on your desktop, for this reason.

Remember, if you are not in exclusive possession of the private keys, you do not own your coins, even if they are your own coins. This is a good rule of thumb to remember.

Conclusion

There are many different ways to store bitcoins, each with its advantages and disadvantages. For people with small holdings, or who store small quantities at a time, mobile or desktop wallets such as bitcoin QT or electrum are good enough along with online wallets. For more serious users and users with large holdings, hardware wallets such as TREZOR or LEDGER or a Multi-Signature solution is advisable. For long term storage and infrequent access, paper wallets are ideal, or

a well stored hardware wallet and storing its seed well. For gift purposes, a paper wallet is an ideal presentation. There is a wallet for every type of user, after doing your research choose the right wallet for you.