

Bitcoin & Litecoin Survival Guide

Everything you need to quickly and safely
join the Bitcoin and Litecoin revolution



Table of Contents

Legal Notices	3
Introduction.....	4
How Bitcoin Works.....	8
Why Bother With Bitcoin?	16
Choosing A Wallet	22
Getting Hold Of Bitcoins.....	31
Spending Bitcoins	35
Staying Safe And Secure	38
Beyond Bitcoin & Litecoin	54
Resources	57

Legal Notices

No Warranties

This report is provided AS IS for informational purposes, without any warranties, except for any applicable refund policy. This report is not guaranteed to produce any particular result. The reader assumes all responsibility and risk for the use of the information contained herein. Nothing contained in this report shall be considered as specific legal or financial advice. You should seek legal & financial advice as appropriate for your specific situation.

No Endorsement

None of the companies or websites mentioned herein have endorsed this publication.

Trademarks

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright Notice

This publication is owned and published by Cogmentis Ltd, and all rights are reserved. You may NOT distribute this report in any form. It does NOT come with resell rights.

Published by: Cogmentis Ltd

18 Cherrywood, Northfleet, DA11 8PL, UK

Website: <http://www.cogmentis.com>

Introduction

Bitcoin is undoubtedly the hottest development in money this century, and is rapidly gaining worldwide attention.

Every day, the media is filled with stories of fortunes made (and lost) in the 'wild west' that is the world of Bitcoin.

But for all the thousands of column inches devoted to this amazing development, there is still a lot of confusion about what Bitcoin is, how it works and how to avoid becoming one of the horror stories.

This 'survival guide' will quickly give you everything you need to join in this amazing (but sometimes confusing) new frontier whilst helping you avoid the many pitfalls you may face.

This book is purposely short. That's because the aim isn't to dazzle you with the intricate details of elliptical curve cryptography or bog you down in the philosophy and politics behind an open-source currency.

Instead, we hope to give you just the right amount of detail you need to quickly 'stake your claim' and avoid the bandits in the badlands.

Throughout this guide, we'll be talking about Bitcoin, but the principles apply to Litecoin too. There are a few minor differences between the two, but these will be highlighted as we go along.

At its heart, Bitcoin is a form of digital money. But to understand why it is so revolutionary, we first have to understand why the need for it exists.

The problem with money

For centuries, money has changed hands in one form or another. Back in the 'good old days', it was usually some scarce resource, such as gold, silver, and even conch shells.

Today, money takes the form of paper, coins or electronic balances in numerous local currencies, which only have value because a government declares them legal tender (known as "fiat currency").

But regardless of the form that money takes, the problem with it has always been the amount of **trust** required to make the system work.

For example, you have to trust banks to protect your money from theft and give it back when you want it.

You have to share private information such as your passport number, mother's maiden name or first school to prove your identity and trust it will be kept safe from identity fraudsters.

And when it comes to the currency itself, you have to trust it isn't counterfeit and will deliver the expected value.

The problem is that trust has often been abused, and never more so than in our modern digital world.

For example, identity theft is on the rise and credit card fraud causes misery for customers and merchants alike.

But the banks are not much better. Fractional reserve banking rules mean that they can 'multiply' the supply of money through successive loans and deposits, creating credit bubbles and risking withdrawal

"runs" as they are only holding a fraction of customers money on deposit.

And governments and banks can debase the value of currency at an instant by printing truckloads of money (Quantitative Easing anyone?).

Yes, when it comes to money in the modern world, trust seems to be in very short supply.

How Bitcoin solves the problem

What makes Bitcoin so revolutionary is that it solves the trust problem by creating a digital currency which is impossible to counterfeit, and which can be securely transferred from one person to another without the usual risk of fraud.

Not only that, but it also operates without the need for banks or central authorities, so it can't be devalued or debased by rampant money printing.

It achieves all this through a mixture of peer-to-peer networking and military grade cryptography.

Bitcoins are very similar to fiat currency and gold in that they have no intrinsic value other than their use as money.

But unlike gold, which is hard to use day to day, and fiat currency, which is hard to trust, Bitcoin is both simple to use and trustable, because it is digital and follows the laws of mathematics.

With the trust issue sorted, the only other thing that is required for a currency like Bitcoin to hold value is the number of people using it, and adoption is increasing exponentially.

In many respects, it's just like the gold rush days of the old wild west. More and more people have heard the stories of 'gold in them thar hills', and their adoption of Bitcoin is driving an exponential rise in value as people rush in to stake their claim.

And just like the gold rushes of the past as well as the technological leaps forward of the industrial and digital revolutions, Bitcoin offers some amazing possibilities for the initiated.

We'll cover the opportunities provided by Bitcoin a little later on. Bit first, we need to understand a little more about what Bitcoin is and how it all works.

Bitcoin vs Litecoin

We've already said that Bitcoin is a form of digital currency, and whilst that's true, it's not the complete picture because it doesn't really tell us anything about how it comes to exist and what makes it unique.

In essence, Bitcoin is **a system of rules**, or protocols, agreed by everyone who wants to use the system. These rules are based on advanced mathematics, and are implemented and enforced in software known as a **'wallet'**.

The rules can change, of course, but only if the majority of people on the network agree they should. Otherwise it's not Bitcoin any more.

Litecoin is an example of where a subgroup of users decided to change some of the Bitcoin rules, creating a 'sister currency' to Bitcoin.

How Bitcoin Works

Wallets, Addresses and Keys

When you open your Bitcoin software (known as a **wallet**) for the first time, it will work its cryptographic magic to create a **public Bitcoin address** and a corresponding **private key** for you to use.

Think of a Bitcoin address as being like a numbered safety deposit dropbox in a public bank.

With Bitcoin, anyone can check the balance or deposit coins into a box if they know its public Bitcoin address, but only the holder of the private key can unlock it and take anything out.

The level of encryption used is so high that the lock on each Bitcoin address has almost as many possible combinations as there are atoms in the entire earth!

When you spend or transfer bitcoins to someone else, you effectively unlock your own safety deposit box, take out the coins and deposit them into the other person's box.

Once that's done, you can't get them back unless the person with the private key opens that box and gives them back.

The sheer brain boggling security provided by the level of encryption used in Bitcoin means that when you receive a payment, it is as good as receiving cash and can only have come from a person who had the right private key.

It also means that if you lose the private key to your Bitcoin address, the coins are locked away forever and can never be used.

Managing the transaction ledger

Traditional local currencies rely on banks to control the supply of money and the accounting of transactions (which history shows they do very poorly).

With Bitcoin, each person effectively becomes their own bank.

That's because all transactions made in the Bitcoin network are publicly recorded in a single, authoritative ledger called the **Block Chain**, which is shared and stored by everyone in the network.

As transactions are made, they are broadcast across the network, validated against the ledger (to ensure the bitcoins have not already been spent) and then batched up and cryptographically written as an entry (called a **block**) in the ledger roughly every 10 minutes.

To ensure that no-one person can control the block chain transaction ledger entirely, the right to create the next block is determined in a kind of lottery called **mining** (a nod to the gold miners of the past).

Miners have to perform billions of cryptographic calculations until they find the 'lottery ticket' which allows them to append a block of transactions to the end of the block chain ledger.

Each time a new block of transactions is added to the block chain, the lottery starts again using the updated block chain as the starting point, and the difficulty of finding a winning lottery ticket is automatically

adjusted over time by the network to ensure that, on average, a block 'winner' is found every 10 minutes.

As a reward for winning the lottery and doing all the processing needed to verify, secure and cryptographically lock the latest block of transactions onto the end of the block chain, the miner is rewarded with a certain number of newly minted bitcoins, plus, any "transaction fees" optionally donated by the sender of the coins.

This cryptographic lottery not only makes sure control of the ledger is fairly shared across the network, but also means that it is impossible for anyone to sneakily change any entry in the ledger, since this would require a cryptographic recalculation of the block the transaction is in and every block in the chain that follows it.

Rules of Bitcoin

The Bitcoin network is bound by a number of rules which all peers in the network enforce via the Bitcoin software. These rules can be only be changed if there is consensus amongst the community to adopt a new software standard.

Litecoin, which is a separate system based on Bitcoin, is an example of where this has happened.

Some of the notable rules are:

Number of bitcoins is limited

A maximum of 21 million bitcoins can ever be created, and the rate at which they are created is halved every 4 years until the limit is reached some time around 2040.

For Litecoin, the limit is 84 million, but as the block creation rate is also 4 times higher, the last coin will also be minted sometime around 2040.

As the number of newly minted coins begins to dwindle over time, it is expected that volume of people transacting on the network will generate enough "transaction fees" to encourage the ongoing processing of transactions.

Block creation rate stays constant

The difficulty of mining the next block is automatically adjusted by network consensus over time so that, on average, a miner will win the right to add an entry to the ledger and mint some new coins for themselves every 10 minutes.

For Litecoin, the difficulty is set so that a block is, on average, created every 2.5 minutes.

The block creation rate is important, because until your transaction is included in a block, there is a chance it could be rejected (e.g., because of double spend attempt).

That's why you generally have to wait up to 10 minutes for a Bitcoin transaction to be confirmed, and up to 2.5 minutes for a Litecoin transaction.

As more blocks are mined and appended to the end of the block chain, the chances of anyone editing your transaction and recalculating every block on the block chain from that point forward gets exponentially smaller, and once 6 more blocks have been added, the ledger is generally considered 'set in stone'.

For Bitcoin, this means about an hour (6 x 10 minutes), for Litecoin about 15 minutes (6 x 2.5 minutes) is all that is needed for a transaction to be considered safer than waiting 6 months on a credit card transaction.

Minimum coin divisibility

Because bitcoins are not physical, like cash or coinage, they can be split into fractions as needed. Bitcoin has a minimum allowable unit of a hundred-millionth (0.00000001), known as a "Satoshi" after the creator(s) pseudonym.

Litecoin has the same minimum unit, called a "Litoshi".

Addresses are anonymous and single use

Because there is no central authority, all transfers between Bitcoin addresses are recorded in the public transaction ledger called the block chain.

To maintain privacy, the block chain transaction ledger contains absolutely no information about ownership whatsoever.

Instead, the owner of an address is simply the person who holds the private key to unlock it. That's why Bitcoin addresses are more like numbered safety deposit boxes than bank accounts.

It's also why, if you lose your private key, there is no way to prove you are the rightful owner of the box or unlock it. Ever.

Even though there is no ownership data in the block chain, it's quite possible that anonymity could be compromised in other ways.

For example, someone can work out that a particular Bitcoin address is yours if you tell them that you own it (e.g., by publishing it on your website).

And when you send or receive funds with someone who knows your real identity, they will know the address used is yours.

Once an address can be traced to an individual, it is possible to look in the block chain ledger and 'trace' the movement of coins from address to address.

For these reasons, Bitcoin addressees are considered single use, so new one should be used for each transaction. The official Bitcoin client, for example, uses something known as 'change addresses' to ensure that each address selected is used only once.

We'll cover this more in a moment, but for now be aware that Bitcoin strips away the layers of privacy provided by the traditional centralised banking model, and puts the responsibility firmly in your hands!

Previous transaction inputs must be completely spent

When bitcoins are transferred from one address to another, for example because of a purchase, then any coins from previous transactions used to fund this new transaction (known as 'inputs') must be completely spent.

As Bitcoin addresses are considered single use, you can imagine, using our safety deposit box analogy, that when you unlock a box, you have to take out all the coins. You can't just take out a few.

If the value you wish to transfer is less than the total value of coins you remove from the deposit box, you then need to re-deposit the

difference - i.e. *your change* - back to yourself, less any (currently optional) "transaction fee" donation you decide to leave for the miner.

Depending on the wallet software you use, your change can be deposited back to the same address, or to a completely new (and often hidden) Bitcoin address.

For example, if you had received coins from three earlier transactions: 0.5 BTC, 2 BTC and 5 BTC and you wanted to send 6 BTC to someone else, you would have to empty the deposit boxes containing the 5 BTC and 2 BTC transactions and redeposit 1 BTC back as change.

Note that if you choose to use a Bitcoin address more than once - e.g. by having a Bitcoin 'tip address' posted on your website - then the deposit box analogy above breaks down a bit.

In this case, you might like to think of previous Bitcoin transactions as being a bit like individual banknotes.

So, using our previous example, you might imagine that your deposit box contains three banknotes: a 5 BTC note, a 2 BTC note and a 0.5 BTC note.

You have to hand over whole banknotes (in this example, the 5 BTC and 2 BTC), and you get to re-deposit a 1 BTC 'banknote' as change.

Choice of mining lottery

As with any lottery, the more tickets you buy the more chance of winning you have overall.

In the case of a cryptographic mining lottery, it's the person who can solve the most puzzles (known as "proof of work") who stands most chance of finding the lucky ticket in the end.

Bitcoin's choice of lottery (SHA-256) favours the miner who has the fastest hardware, which has led to an "arms race" of specialised hardware mining rigs.

This has made it almost impossible for individuals to mine any more, as the network automatically adjusts the difficulty to ensure the block creation rule still applies.

Litecoin's choice of lottery (Scrypt) is designed to level the playing field somewhat, as the ability to solve puzzles is limited by memory more than raw processing power.

Even so, with the costs of hardware and electricity, mining is a competitive business governed by the laws of supply and demand, and so sometimes it is profitable, and sometimes it is not.

Because of the level of competition, individual "hobby" miners usually now pool their resources in a kind of lottery syndicate, sharing the coins earned according to who contributed the most solved puzzles.

Why bother with Bitcoin?

As an investment

The rise of crypto-currencies has been likened to the gold prospecting days of the wild west, with people scrambling to stake their claim in this digital frontier.

The chances are that you are reading this guide because you've read stories about how people have made fortunes in the Bitcoin gold rush.

In fact, Bitcoin and gold have a lot in common.

To start with, both are scarce commodities. To date, only 171,300 tonnes of gold have been mined, and the supply of bitcoins is limited to around 21 Million.

They also have no intrinsic use or value, other than as a store of value! This makes the value totally subjective.

In other words, both gold and bitcoins are only valuable because they are a durable store of value which cannot be debased by money printing like fiat currency can.

Bit unlike gold, which is heavy, inconvenient to use and difficult to store, bitcoins can be carried around like cash, and transferred in a couple of clicks to anyone in the world.

But are bitcoins a good investment?

The truthful answer is that no-one knows. The current Bitcoin fever could turn out to be nothing more than a short term bubble or the beginning of a whole new era.

Here are some things to consider as you make up your own mind.

Mining is expensive

Every Bitcoin created must be mined in the competitive lottery, which involves computers generating thousands of cryptographic calculations every second in the hope of finding the "lucky ticket" that gives them the right to create the next block.

This means that every Bitcoin created requires not only an investment in hardware, but also a cost of electricity to mine it.

The more miners there are, the harder the lottery is to win and so the more expensive the coin is to create in terms of energy expenditure.

This gives Bitcoin an intrinsic 'cost of creation' value, which can be compared to the cost of mining an ounce of gold from the ground.

Combined with the overall scarcity of the coins, it encourages an upwards trend in Bitcoin value as miners seek to make their investment in hardware and electricity pay.

Coins lost cannot be replaced

Unlike fiat currency, which is reprinted as it wears out (and at the whim of banks and governments), the supply of bitcoins is fixed.

And although bitcoins cannot be destroyed, they can only be spent or transferred if you have the private key.

This means that if you lose your private key, the coins are effectively taken out of circulation and locked away forever.

As keys are lost and coins are locked out of use, the remaining coins in the network become more valuable by virtue of becoming more scarce.

This also creates an upward trend in the value of remaining coins over time. And because remaining coins can be divided into hundred millionths, it doesn't create any liquidity issues.

Security from interference

Leaving aside the issues from hacked wallets, which we will cover later in this guide, Bitcoin offers an unprecedented level of security against interference by companies, governments or other authorities.

The peer-to-peer nature of the network means that the block chain ledger would be near impossible to wipe out, overwrite or regulate, just as the music torrent network has survived attempts by the music industry, governments and pressure groups to control it.

Taking over the Bitcoin network would require an entity to gain control over at least 51% of the network computing power (something known as a 51% attack), which, as the popularity of Bitcoin spreads, becomes exponentially harder to achieve.

Their digital nature, ease and security of transfer, and the anonymity of the block chain ledger also makes them easier to protect against national interference too.

So unlike gold, which history shows governments have had a tendency to confiscate in difficult times (such as Roosevelt's 1933 gold raid in the USA or the UK's gold licensing of the 1960s), Bitcoin addresses cannot easily be traced to any individual or transferred without the private key.

Uptake is increasing exponentially

From the start of Bitcoin in 2009, the amount of value being pumped into Bitcoin is increasing at an exponential rate as more and more people exchange valuable goods and services for bitcoins.

Mainstream retailers are starting to take notice, drawn in by the low transaction fees and confidence that comes with irreversible transactions, and the more goods and services that are exchanged for bitcoins, the more the subjective value of the coins will increase.

At the time of last update to this guide (October 2016), a Bitcoin is worth around \$630, and there are around 16 million bitcoins in circulation. This means the total value held in the Bitcoin network is around \$10bn.

In global currency terms, that's minuscule. It's only around 10% of Amazon's 2015 annual revenue of \$107Bn. Put another way, with around 7 billion people on the planet, it represents less than \$1.50 per person.

If Bitcoin continues to grow into a global currency, the value of it will have to increase to cope with the demands of commerce. And the upside is potentially staggering.

The PayPal network, for example, holds around \$20Bn value, which would imply a Bitcoin price of nearly \$1300.

And if Bitcoin attracts just 1% of gold investors, or \$90Bn value, the value of a Bitcoin would have to be over \$5,500.

And if Bitcoin attracts 5% of gold investors, or \$450Bn value, the value of a single Bitcoin would have to be around \$28,000!

Legislation / Tax situation

Crypto-currencies like Bitcoin and litecoin are so new that most governments don't yet know how to treat them for tax and legal purposes.

This is compounded by the fact that in the early days of Bitcoin, the anonymity and easy transfer of coins made the currency attractive to underground and illegal activities.

Some governments, notably the USA and UK, have recognised that crypto-currencies such as Bitcoin are not in themselves illegal and present an innovative development.

They have not yet, however, decided to what, if any legislation is required, nor has the status as a currency been universally agreed, so the tax situation on capital gains may vary from country to country.

Volatility and longevity

For all the upsides, Bitcoin and Litecoin are still young (Bitcoin launched in 2009, Litecoin in 2011), and the volume of coins in circulation is still relatively small.

This means that whenever there is a spike in demand, such as when a Bitcoin news story breaks, the price of Bitcoin can fluctuate wildly. Not to mention the fact that the small market size makes it prone to manipulation such as "pump and dump" or "short and distort" tactics.

Plus, crypto-currency is still in its infancy, and there are already a dozen variations on the Bitcoin model (of which litecoin is the best known), so it is entirely possible that Bitcoin and/or litecoin could fade

into the background in favour of an alternative, stronger cryptocurrency.

So whilst the majority of indicators suggest that Bitcoin and litecoin are likely to appreciate over the next few years as the market goes mainstream, ***there is also a significant risk that your investment in bitcoins will be worth nothing at all.***

So you need to carefully consider the upside and downside of investing in Bitcoin and make your own decision, and only risk money you are prepared to lose.

As a currency

As we mentioned above, merchants are increasingly accepting Bitcoin as a medium of exchange because it offers unprecedented low fees, security and certainty of transactions.

Bitcoin is starting to be accepted by more and more mainstream merchants, from computer hardware suppliers to coffee shops. They have even been accepted by Virgin Galactic as payment for the first civilian trip into space.

As a customer, it can be reassuring to have an additional means to pay for goods and services, especially if your spending power has increased whilst you've been holding your coins.

You can find a list of Bitcoin friendly merchants here:

<http://usebitcoins.info/>

Choosing a Wallet

There are essentially four choices when it comes to software wallets, each with its own pros and cons.

Full Bitcoin Client

The official Bitcoin client, known as **Bitcoin Core** (formerly *Bitcoin-Qt*), is the original wallet software, and it offers the highest level of security, privacy and stability of all the wallets as long as the computer you run it on is secure.

Change Addresses

Whenever you send or receive money, the chances are that the anonymity of the address you used for the transaction will be compromised or 'tainted'.

For example, when you purchase something from a retailer, they will probably have some form of customer record or delivery address that can link your real world identity to the Bitcoin address being used.

The Bitcoin Core client helps your privacy by ensuring that Bitcoin addresses are only used once.

It does this by creating a large number of random hidden Bitcoin addresses (100 by default), to which it transfers any remaining balance (your 'change') whenever you send coins to someone else.

With the Bitcoin Core wallet, you can think of your Bitcoin addresses as behaving more like banknotes. The value being transferred is what matters, not the serial number of the bank note itself.

So, if you had two addresses, each with 5 bitcoins in your wallet (i.e. 10 coins total) and you transferred 6 bitcoins to someone else, the wallet software would automatically take all 10 coins out of the old (now tainted) addressees, sending 6 coins to the other person's address and 4 bitcoins (your change) to one or more new, untainted Bitcoin 'addresses in your wallet (your 'change addresses').

This is just like pulling two \$5 banknotes from your real wallet to pay for a \$6 item and receiving 4 dollar bills as change. It doesn't matter to you the serial number of the individual banknotes, only that the value of notes returned to your wallet adds up to \$4.

The great thing about the use of change addresses is that it quickly becomes impossible for someone tracing the chain of transactions to know which addresses you own and which you do not.

The downside to this approach is that if you make a lot of transactions, there is a significant risk that any backup of your wallet will not contain all the newly created change addresses and their private keys.

So if your computer explodes or is stolen, you may lose any money held in a change address that was created after your last backup, as you won't know either the address or its private key!

Full Block Chain Node

The Bitcoin Core wallet acts as a full node in the peer-to-peer network. What this means is that the computer you run the wallet software on will hold a full copy of the block chain transaction ledger, and be able to verify and relay transaction blocks.

The great thing about having the full client is that you are 100% independent of any third party, and your presence enhances the resilience, security and diversity of the entire network.

The downside to running the full client is that it can take over a day for your wallet to process the entire block chain ledger, and you need to have the disk space and internet bandwidth to cope with the full block chain.

The block chain is around 90Gb in size (October 2016), and currently growing exponentially each month.

Other features and portability

The Bitcoin Core wallet is not only designed for use by individuals on their computers, but also by merchants and payment service providers as a server driven utility.

It achieves this by presenting a single, simplified wallet for individuals, whilst allowing access to advanced features via special commands.

The great thing about this dual use approach is that merchants and payment service providers can do advanced things like setting up 'accounts' (essentially like a bank) for each customer, and managing the Bitcoin addresses for each account separately.

The downside is that this advanced functionality requires some advanced knowledge to use it effectively, and it effectively limits non-technical users to having a single wallet on a single computer.

Armory Add-on

At the time of writing, there is also an add-on for the Bitcoin Core client, called **Armory**, which helps you unlock some of the advanced features of the Bitcoin Core wallet, as well as helping to overcome some of the limitations.

For example, it allows you to manage multiple wallets, lets you do advanced things like signing messages and reduces the risk of losing coins from incomplete backups of your wallet.

It does this by *deterministically* creating new addresses in your wallet, rather than randomly creating them, so that in the event that you lose your wallet for any reason, all the addresses can be rediscovered using a single backup (*regardless of when it was taken*).

This makes your backups much more secure from accidental loss, but also means that your backups are even more valuable in the hands of a thief, so guard them well!

Lightweight Bitcoin Client (SPV)

To overcome the need to store the entire block chain ledger, the Bitcoin protocol makes allowances for a lightweight alternative to the full Bitcoin client, known as Simplified Payment Verification (SPV).

Lightweight clients are designed to overcome the limitations of running a full client node, favouring simplicity and speed over the added security of being a full network node.

At the time of writing, lightweight client options include **MultiBit**, **Electrum** and **Bither**.

Reliance on Full Bitcoin Nodes

Lightweight clients, such as MultiBit don't download and check the entire block chain to confirm the integrity of the ledger. Instead, they simply check how deep a block is buried as an indicator that the block has been validated by the full nodes and unlikely to be reversed.

The great thing about this approach is that you don't have to download and maintain a copy of the entire block chain to your computer, which means you not only save over 100Gb of disk space, but your wallet software synchronises quickly — usually in just a minute or so.

The downside to this approach is that you have to trust that the information you receive from the network is accurate. This leaves you open to the remote possibility of being duped by a dishonest (but technically brilliant) merchant if you were paying for something whilst using their wifi connection.

Multiple Wallets

Unlike the Bitcoin Core client, which only allows you one wallet, the Multibit wallet allows you to create as many wallets as you like. So you can have a wallet for different members of the family, for home and work, current account and savings, etc.

No Change Address Pool

To keep things simple, Multibit doesn't create a pool of change addresses like Bitcoin Core, so treats Bitcoin addresses more like bank accounts.

The great thing about this is that it keeps things simple — all change is simply sent back to your main receiving address. Or, if you have more than one, it sends it to the last address created.

The downside is that using an address more like a bank account than a single use banknote means that privacy is more likely to be compromised.

Third-party wallet

Third party wallets such as **Blockchain.info** work just like lightweight wallets, except they are tied to a particular website or service for their block chain data.

So rather than accepting the validity of a block of transactions in the Bitcoin network based on how deeply in the chain it is buried, a third party wallet relies on information provided by a third party service acting as a full network node.

The great thing about this is that, like a lightweight wallet, you don't need to download the full block chain ledger, and as long as you trust your wallet service provider, you can be sure that you are always getting correct information about the block chain.

The downside is that if your service provider gets hacked or goes down, you may be left without the ability to transact on your account and will need to fall back to manual methods.

Web Wallet

A web wallet differs from a third party wallet in that the entire wallet is web based. This means that they hold the private key to your Bitcoin address in a useable format.

Web wallets are usually used by coin exchanges and payment service providers to allow them to move coins into and out of escrow on your behalf, and transfer coins in exchange for hard currency.

Web wallets providers are considered the highest risk as an incident involving the loss or theft of your private key could result in the loss of your coins.

As such, web wallets should be used for brief transactions and never for long term storage.

Cold Storage Wallet

All of the above wallet solutions can be considered "hot" wallets, as the private keys are kept on a computer system (either yours or a web wallet providers).

As such, they are ready to use at a moment's notice, but this also means the keys are potentially vulnerable in case of hacking, virus, or loss of data.

A cold storage wallet, on the other hand, is one where the private keys are not stored on an internet connected computer.

There are two main types of cold storage wallet.

Paper Wallet

A paper wallet is simply a printed piece of paper containing a public Bitcoin address and its corresponding private key.

As soon as you fund the address by sending coins to it, you effectively have your own banknote!

Paper wallets can also be created with a password protected private key — known as BIP38 encrypting — which adds an extra layer of security to the piece of paper.

Paper wallets are the most secure form of wallet storage as a would-be thief has to acquire the piece of paper in order to steal your coins.

You can create a Bitcoin paper wallet using the **bitaddress.org** service (or **liteaddress.org** for Litecoin paper wallets).

Brain Wallet

Whereas paper wallets are created totally at random, Brain Wallets are Bitcoin addresses and keys created using a set of rules.

The idea is that rather than printing a paper wallet, you can simply remember a pass phrase and use it to create the right key/address pair at any time simply by entering that pass phrase into the brain wallet generator.

In theory, this gives you the security and deniability of having an address and key that are stored only in your head!

The problem is that as human beings, we are generally awful at generating secure passwords and pass phrases. And hackers have enormous computing resources at their disposal to guess them.

Brain wallets are therefore "easy pickings" for hackers looking for Bitcoin addresses to rob, and most of the thefts of bitcoins to date have been from brain wallets with supposedly secure pass phrases.

So, always create a random paper wallet — never, ever, ever create a brain wallet. Ever.

Getting hold of bitcoins

There are four main ways to get your hands on bitcoins.

Purchase on an exchange

For most people, this is going to be the primary way of getting hold of bitcoins as it allows you to purchase any amount, just as you would any other "foreign currency".

Because Bitcoin transactions are final and irreversible, you will generally have to pay for your bitcoins using a non-reversible payment method — usually cash or bank transfer.

PayPal and credit card purchases are not usually accepted by exchanges, as they may be subject to chargeback or fraudulent payment claims.

You can find details of exchanges in your country by visiting:

Bitcoin: <http://howtobuybitcoins.info/>

Litecoin: <https://litecoin.com/services#exchanges>

Accept them as a merchant

If you have a business, then accepting bitcoins can make a lot of sense — especially as many Bitcoin holders are currently sitting on large gains in spending power thanks to the recent rise in Bitcoin value.

As a merchant, you have two main options — either accept bitcoins directly because you want to build a position in them, or use a

merchant service provider who can convert the bitcoins to your local currency on a regular basis for you.

The advantage of using a Bitcoin merchant service provider is that you can gain access to a new customer base whilst still limiting your exposure to fluctuations in the price of Bitcoin.

The downsides of using a merchant service provider is that coins awaiting transfer to local currency are vulnerable in case the merchant provider is hacked. This is because the service, if automated, has to use the private keys to make the transfers internally and if the keys fall into the wrong hands, the coins can easily be stolen.

Whilst this sounds unlikely, the anonymity and price of Bitcoin makes merchant providers a very real target for determined hackers, and there have been a number of reports of Bitcoin merchant providers being hacked.

At the time of last update to this guide (October 2016), Bitfinex was the latest casualty, losing an estimated 120,000 BTC (more than \$75 million US dollars) worth of customer bitcoins after being hacked.

So, if using a merchant service, it is generally much safer if they will either sweep your balance to currency frequently (to limit the loss in case of a hack) or if you specify that coins are immediately forwarded to a Bitcoin address which you control (as then only you have the private key).

Earn them

In an effort to encourage uptake of Bitcoin and Litecoin, many early miners set up "faucets" which allowed people to get hold of some coins for free.

These early faucets have all but dried up, however, it is still possible to earn bitcoins in exchange for doing mundane tasks like viewing adverts or web pages.

Generally, the return in investment with these sorts of schemes is extremely low, and usually not worth your time, sanity or electricity to sit at your computer and perform the tasks requested.

Become a miner

As we discussed earlier, new bitcoins are created any time a block of transactions is written into the block chain ledger, and the person who has the right to post the next block of transactions is determined by a kind of lottery called 'mining'.

As more and more people become miners, the network automatically adjusts the chances of winning the lottery so ensure that that a new block of transactions is created, on average, every 10 minutes (2.5 minutes for Litecoin).

With Bitcoin, the choice of lottery (SHA-256) favours the miner who has the fastest hardware, which has led to an "arms race" of specialised hardware mining rigs.

This massive influx of computing power has raised the difficulty of winning the Bitcoin lottery to such a high level that it is practically

impossible for individuals to earn anything by mining any more — the electricity costs dwarf the value of coins mined and even if you have free electricity, it can take months to earn pennies.

Litecoin's choice of lottery ("script") is designed to level the playing field somewhat, as the ability to solve puzzles is limited by memory more than raw processing power.

Even so, many former Bitcoin miners using older rigs have now moved over to mining Litecoin, which means that mining has become more difficult and less profitable than before once electricity costs are taken into account.

That said, if you have free electricity available, or want to have a go at building and running a mining rig as a hobby, then we recommend the excellent tutorial by Cryptobadger.

<http://www.cryptobadger.com/build-your-own-litecoin-mining-rig/>

The rig that he suggests can be used to mine one of over a dozen different crypto-coins, and you can check the expected returns for the various currencies using the website below:

<http://www.coinwarz.com/calculators>

Spending Bitcoins

Spending bitcoins is extremely easy once you have chosen your wallet, and it involves just three simple steps

1) Get the Bitcoin address to send to

In order to send bitcoins to someone, you need one of their Bitcoin addresses. Because Bitcoin addresses are usually considered single use, the recipient will usually generate a new Bitcoin address for you.

This is especially true of merchants, who will use a new Bitcoin address for each customer not only for privacy, but also so they can link the payment back to a specific customer order.

The exception to this rule is where someone invites contributions by publishing a tips or donations address on their website or their book.

Bitcoin addresses are safe to send to others, as they can only be used to deposit coins and view the balance, so depending on the setting, they could present it either as a plaintext address, a scannable QR barcode, or a payment link you can paste into a web browser.

Here are some examples of how you might get sent a Bitcoin address:

- **Bitcoin address as a scannable QR code:**



- **Plaintext Bitcoin address:**

1PjRyiq8TSUm1TxHwfhG8nLbsFM4GHF1q7

- **Payment link:**

<bitcoin:1PjRyiq8TSUm1TxHwfhG8nLbsFM4GHF1q7?amount=0.005>


(NB: All 3 are examples using our Bitcoin 'tip' address, so please feel free to use it for spending practice if you've found this guide useful!)

2) Enter the address and amount

Once you have the address to send to, simply visit the 'Send' tab of your wallet and enter (or scan) the address and the amount of Bitcoin you wish to send.

Quick Send

Use the form below to send a payment to a bitcoin address.

To: 

Enter The Bitcoin Address of the Recipient

Amount: =

Enter The Amount of Bitcoins to send

Depending on your choice of wallet software, you may be able to enter the amount in your local currency.

Alternatively, if you had clicked a payment link, it should automatically have added the correct amount to pay on your behalf.

3) Hit send and wait for confirmation

Although your transaction is broadcast to the Bitcoin network, it can take up to 10 minutes for it to be batched up into the next available block and written into the block chain ledger.

Depending on the nature of your transaction, the person receiving the coins may wish to wait for this to occur, and for valuable transactions may wish to wait for up to 6 confirmations to be sure the transaction is all but impossible to reverse.

A 'confirmation' occurs as each successive blocks of transactions are written to the ledger, so a Bitcoin transaction can take around an hour (6 x 10 minutes) to be considered 'set in stone'.

Litecoin differences

Litecoin transactions work exactly the same way, except that Litecoin confirmations happen every 2.5 minutes, so transactions are much faster.

It therefore only takes 15 minutes (6 x 2.5 minutes) to consider a high value transaction 'set in stone'.

The only other difference is that whilst Bitcoin addresses always start with a "1", Litecoin addresses always start with an "L".

For example: LgayRkx4MJ4Q8Zs58chVZG87mz9oTDP2T1

Staying Safe and Secure

As you've probably realised, reading through this survival guide, your Bitcoin address private keys are the most important thing you have.

The person who holds the key to a Bitcoin address is considered the owner of the coins, and can spend or transfer them at any time.

If you lose the private key to a Bitcoin address, you have no way of unlocking the coins to use them or proving that you are the owner.

And with around the same number of possible key combinations as atoms in our planet, you've got more chance of the earth being wiped out by a rogue asteroid than randomly guessing your key.

The following tips will help ensure you and your money stay safe.

Use secure passwords

Password cracking techniques have come on a long way over the last few years, as has the technology. The graphics card in an average gaming PC is powerful enough to crack any 6 digit password in around 15 minutes, simply by trying all possible combinations in rapid succession!

And a specially built computer containing 8 graphics cards can break any 8 character password in around 12 hours!

What's more, password crackers are now using the predictability of human behaviour to make longer, supposedly secure passwords easily crackable too.

For example, a common pattern used by people trying to create a secure password is to start with a capital letter, use some lower case characters, symbols and numbers that usually spell out a common word, then finish with some numbers.

So if your current 'secure' password is something like Pu55yc@t123, it is easy pickings to a professional password cracker.

The problem with most passwords is the human factor — we tend to use easily recognisable patterns like the example given above, in order to make them easier to remember.

And any part of a password which isn't totally random weakens it, so a password like Pu55yc@t123 is at best only as strong as a 6 character password, once the non-random parts (pussy, cat, 123, and the common symbol substitutions) are taken into account.

So if an 11 digit password using combinations of Uppercase, lowercase, symbols and numbers isn't secure... what is?

The secret, it turns out, is to use a passphrase made up of six or more **words** chosen totally at random.

The best system for doing this, *recommended by cryptographers*, is to use the Diceware Passphrase system.

<http://www.diceware.com/>

There is also an online Diceware password generator at:

<https://entima.net/diceware/>

A six word Diceware passphrase made of truly random words would give more combinations than there are grains of sand on all the worlds beaches.

For total security, you should use a different secure password for every website and service you use, and this creates a problem for most people.

The solution is to use a secure password manager, such as keepass.info to create random passwords for all your sites, and then secure it with a Diceware master password which you can remember.

Use a cold storage wallet for savings

Just as you wouldn't carry your entire life savings around with you, neither should you keep all your bitcoins in a software ("hot") wallet.

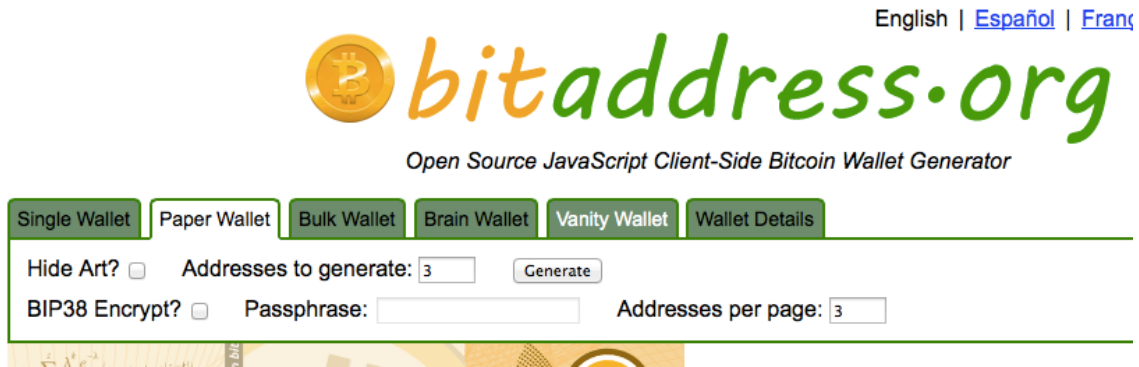
Not only is a paper wallet safe in case your computer hard drive blows up, it also gives you an added layer of physical security — in order to steal your coins, a thief has to actually get hold of the piece of paper containing your Bitcoin address and private key.

What's more, you can even encrypt the private key before you print your paper wallet, which means that not only does the thief have to get hold of your paper wallet, they also have to find the password to unlock the private key.

This is like locking the key to your main safe inside another safe. You must remember the password, however otherwise you won't be able to recover your private key!

Here's a step by step guide to securely creating a paper wallet.

1) Visit bitaddress.org (or liteaddress.org for Litecoin)



2) Click the paper wallet tab and select how many wallets you wish to create.

3) If you are going to password protect your private key, click the 'encrypt' checkbox and enter a password.

4) Click "generate" and then print the wallets.

Extra security measures

The bitaddress website is generally very safe, and all Bitcoin addresses and keys generated are created locally in your web browser, so nothing is sent over the internet.

However, it is possible that if your computer is already infected with a virus or other spyware, the private keys created could be compromised as they are created.

So, for additional security, you can take the following steps:

- Scan your PC for viruses and spyware! If you don't have dedicated anti-virus protection on your PC, then we recommend using the "Housecall" online scanner by Trend Micro.

<http://housecall.trendmicro.com/>

- Download the bitaddress creator to your computer and run it locally. The link to the GitHub repository can be found at the bottom right of the web page, and you can then click the button to 'download zip'. Here are the direct download links:

- Bitaddress download:

<https://github.com/pointbiz/bitaddress.org/archive/master.zip>

- Liteaddress Download:

<https://github.com/litecoin-project/liteaddress.org/archive/master.zip>

- Unplug your internet connection before using them!

Checking the balance of a paper wallet

You can easily check the balance of a paper wallet without weakening the security simply by looking up the Bitcoin address in the public block chain ledger.

There are a number of websites which publish the block chain ledger online, including blockexplorer.com (for Bitcoin) and ltc.blockr.io (for Litecoin).

Some software wallets, such as blockchain.info, also allow you to set up your paper wallet address as a 'watch only' address. This

means the wallet can look up the value of the coins in your paper wallet, but because you don't enter the private key, it cannot transfer them elsewhere.

Use 'hot' wallets for spending money

Of course, a paper wallet isn't very convenient for buying a coffee at Starbucks, so it makes sense to use one of the software wallets for day to day transactions.

If a paper wallet is like your savings account, a software wallet (or 'hot' wallet) is like your physical wallet — you only carry around enough cash for your day to day needs in case it is lost or stolen.

Your choice of software wallet is entirely yours, and the pros and cons of each type of wallet were detailed earlier, however Multibit is a good all round choice for desktop computers and if you use a smartphone or tablet, then Blockchain.info is an excellent choice as it is portable between your computer, tablet and phone.

Always secure your hot wallet

With a software wallet, the private keys are stored in the software ("hot") to make transactions easier. It is therefore vitally important that you secure your hot wallet with a strong password, as that is all that stands between a thief and your bitcoins!!!

The importance of this cannot be overstressed, as there are a growing number of cases where a computer virus is used to send a copy of the wallet database to the hacker. If it is unsecured, or secured with a weak password, they can use your private key to steal your coins at any time in the future!

All the software wallets have some form of encryption option and some also have what is known as '*two factor authentication*'. This is a second form of identification, such as requiring you to enter a code that is sent to a nominated email address as well as a password to unlock your wallet.

Ensure paper wallets are single use

To spend coins stored in a paper wallet, you simply need to import the private key into your software wallet, usually by scanning the QR code. You can then use it just like all the other addresses in your wallet.

However, once you have entered the private key on an internet connected device, the paper wallet address should be considered "hot" and hackable.

So, if you are doing a partial transfer from your paper wallet, it is generally safer to send the remaining coins to a brand new "cold storage" paper wallet address rather than returning them to the old paper wallet address.

Generate Bitcoin addresses randomly

We talked earlier about "Brain Wallets" being an easy target for thieves because human beings are usually hopeless at choosing truly secure passwords.

The problem with them is that the address and private key are created deterministically by the pass word/phrase used — that is, you get the *same* address and key pair returned every time you type the pass phrase into the brain wallet generator.

So whereas normally the chance of stumbling across the address/key combination of a randomly created paper wallet is 2^{160} , which is like trying to find a single atom in the entire earth, a deterministic Bitcoin key/address combination can be found immediately if the password or phrase used to determine it is known.

And usually, because we humans are pretty predictable (even when we are trying to be random), this cuts down the search required drastically.

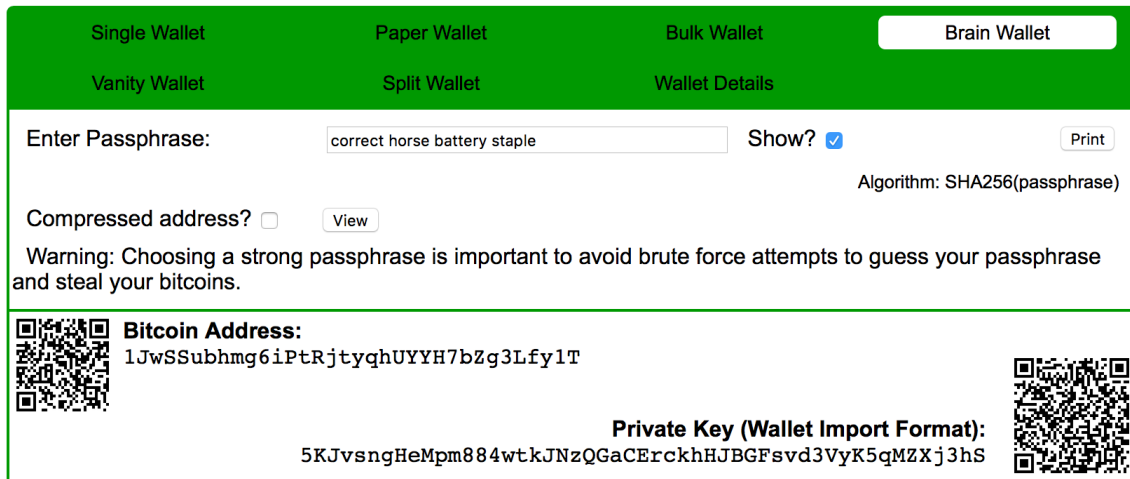
For password crackers, this is a dream come true. They can simply run all the common passwords and phrases until they find an address with coins on it. In fact, if you use any recognisable pattern in your password — or even any phrase from your favourite book or poem — it can be found.

In relative terms, having a Bitcoin address determined with a simple password is like giving someone the first 97 digits of your 100 digit combination lock or telling them the atom they want is in a particular pebble.

What's more, because the block chain ledger is public, the password crackers can simply use bot software to monitor all the Bitcoin addresses created with common passwords. So even if an address isn't being used yet, the second someone adds coins to it, they can find out and steal them.

To show you how simple it can be, here's a quick example:

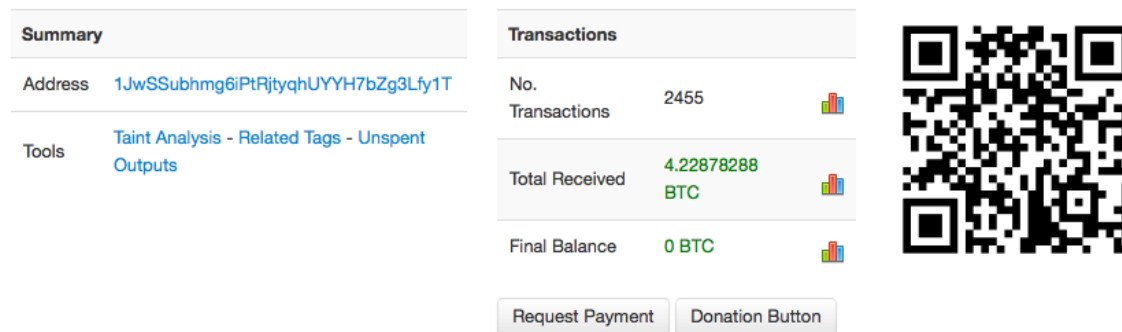
1) Visit www.bitaddress.org, click the 'Brain Wallet' tab and lookup the



address for the passphrase "correct horse battery staple". You should get:

2) View this address at blockchain.info

correct horse battery staple Addresses are identifiers which you use to send bitcoins to another person.



Summary	
Address	1JwSSubhmg6iPtRjtyqhUYyH7bZg3Lfy1T
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	2455
Total Received	4.22878288 BTC
Final Balance	0 BTC

[Request Payment](#) [Donation Button](#)

As you can see, at the time this picture was taken, this address had seen 2455 transactions, with a total of 4.228 BTC deposited and removed, leaving a zero balance. And at the time of last update to this guide (October 2016) over 4100 transactions have been processed

through this bitcoin address. If there was a positive balance at the address, you would be able to spend it with the private key:

5KJvsngHeMpm884wtkJNzQGaCErckhHJBGFsvd3VyK5qMZXj3hS

Of course, if you used a truly secure pass phrase as the brain wallet seed, such as a randomly generated 8-10 word Diceware password, a brain wallet can be as secure as a random one.

But as you are probably going to write down the passphrase somewhere anyhow, it's usually just safer to generate and print a random paper wallet instead.

Be careful what you run on your computer

Computers are always at risk of viruses and malware, but the minute you run a software Bitcoin wallet on your computer, you open yourself to the additional risk of it being compromised by malicious software.

Remember that crypto-currencies like Bitcoin and Litecoin contain the heady mix of money and technology, plus semi-anonymous, non-reversible transactions.

This makes your software wallet a rewarding challenge for malware creators, and there are already a few examples of coin stealing software out in the wild, such as the [StealthBit app for Mac OSX](#).

So before you download any software - and especially any wallet related software - make sure you double check the website is genuine.

For example, only ever download the Bitcoin Core or Litecoin Core software from the official websites. There is a list of official resources in the back of this guide.

Be careful who you allow onto your computer

Related to the last tip, the minute you add a Bitcoin wallet to your computer, you need to start being careful about who you physically allow access to it.

Remember that not everyone you meet on a community forum really has your best interests at heart, so you need to sense check any instructions you get with other people, and only allow someone access onto to your computer if you would trust them with your credit card!

Wait 6 confirmations before shipping

If you are accepting a Bitcoin or Litecoin payment for something valuable, be sure to wait for 6 confirmations before shipping.

A 'confirmation' happens whenever the next block of transactions is added to the block chain ledger.

With each confirmation , the chances of anyone editing your transaction and recalculating every block on the block chain from that point forward gets exponentially smaller, and once 6 more blocks have been added, the computing power required to revise the ledger would be so astronomically large that the ledger is generally considered 'set in stone'.

For Bitcoin, this means about an hour (6 x 10 minutes), for Litecoin about 15 minutes (6 x 2.5 minutes) is all that is needed for a transaction to be considered safer than waiting 6 months on a credit card transaction.

Of course, there is nothing to stop you shipping on fewer confirmations, or even without any, if the value and/or risk of loss is low — so if you were selling cups of coffee, you might choose to go ahead without any confirmations for speed of service.

Never delete a wallet...

...Unless you are sure you know what you are doing. When you delete a wallet, you destroy the private keys and lock yourself out of the Bitcoin addresses the wallet contained.

Here are some things to think about before you delete a wallet.

Is anyone likely to send coins to the addresses again?

Some people tend to think of Bitcoin addresses like bank accounts, rather than single use addresses. So before you delete a wallet, think hard about whether anyone is likely to send more coins to the addresses it contains.

Have you ever published any of the addresses in the wallet — e.g. as a donation or tip address? Have you given any of the addresses in the wallet to any friends, family, or customers to use?

Have you completely emptied the wallet of all coins?

It might sound obvious, but you'd be surprised the number of people who delete wallets containing coins.

The most common reason is because of the way software wallets allow you to create Bitcoin addresses on demand, and some (such as the Bitcoin Core client) create hidden addresses to use as 'change addresses', which are used to enhance your privacy by returning any unspent coins in a transaction to a new address.

A common scenario that results in loss of coins is when a person imports a Bitcoin address from a paper wallet into a software wallet so they can spend some coins, then deletes the software wallet straight afterwards "for security".

What they didn't notice was that the change from the transaction was not sent back to the paper wallet Bitcoin address, but was sent to one of the default or change addresses in the wallet... which they have now deleted.

So, before you delete a wallet, wait an hour. That way, you will give the block chain ledger time to fully and irreversibly confirm your transactions.

If your wallet is still empty after an hour, and your wallet is showing as 'in sync' with the network, you can be comfortable that the wallet is safe to delete.

Backup, Backup, Backup

It goes without saying that unless you have the private key to a Bitcoin address, you can't use any coins stored at that address. So always make sure you have multiple backups in place.

For paper wallets, this means making a few copies and keeping them in separate safe locations. That way, if your house burns down, you

don't lose them all. Also, consider keeping them in a ziplock bag to prevent them getting damp.

For software wallets, this generally means making a backup every time you create a new address or send money.

Backing up when you create an address is pretty obvious — as your old backup won't contain the new address.

But it's also important to backup when you send coins too. That's because some software wallets automatically enforce the single-use of addresses by creating hidden 'change' addresses.

For example, the main Bitcoin Core client has a pool of 100 hidden Bitcoin addresses which it sends your change any time you send coins. But because you won't know exactly when that pool has been used up and a new batch of change addresses is created, you really need to backup any time you send coins from your wallet.

If you have the Armory add-on to the Bitcoin Core client, the risk of loss from incomplete backup is avoided because all the addresses are created deterministically (i.e. they are calculated from a common random root key rather than totally random).

However, whilst this protects you from incomplete backup it makes it even more important to protect the backup, as if it falls into the wrong hands, then the private key for any address you could ever wish to create can be reproduced from that backup!

So, if you have a lot of coins in your hot wallet, consider using a 'fragmented' paper backup. These are special backups which allow you to specify the number of fragments which are needed to use it. For

example, you might specify a "2 of 3" fragmented backup, which means that at least two of three fragments are needed to use it.

Which brings us neatly to the next tip...

Beware, lightning does strike twice!

If, despite taking the precautions in this guide, you are still the victim of theft from your hot wallet, then you should assume that the Bitcoin addresses are permanently compromised and start afresh.

Never, ever, reuse a compromised address, as the thief could lull you into a false sense of security and wait years before striking again when you have all but forgotten the last theft.

So, just as you would change your locks after a break-in, always change your Bitcoin addresses if you are unlucky enough to be robbed.

And if you use a deterministic wallet, such as the Armory add-on for the Bitcoin Core client, this means totally resetting your wallet so that a new root key is created as if the thief has the root key, they can use it to determine the private key for ANY address you could create now or in the future using the old root key.

Don't keep all your eggs in one basket

It's an ancient proverb, but it stands as good advice in the digital age of Bitcoin too. Bitcoin addresses cost nothing to create, and there are no holding fees of any kind.

So, rather than putting all your savings in one paper wallet, it makes sense to spread them across a number of separate paper wallet addresses.

Not only does this limit your loss in case you lose one of the pieces of paper, but it also means that if you slip up and accidentally make the paper wallet hot by reusing it, your risk of loss is minimised.

Remember, unlike the traditional banking system, which usually offers some form of financial protection in case a bank fails, you have no such protection if one of your Bitcoin addresses is compromised.

Only invest what you are ok to lose

Finally, always remember that Bitcoin is a new and experimental currency, and that any investment in coins could as easily be worth nothing as make you a fortune.

The market for coins is currently still comparatively small, and this not only makes the 'exchange rate' extremely volatile, but also makes it prone to manipulation.

And if you are using bitcoins as a currency, you need to accept that future price fluctuations can either work in your favour or against you.

For example, the widely reported first transaction in Bitcoin, which took place on 21st May 2010, was for a Papa Johns pizza. The pizza cost 10,000 bitcoins back then, which at the time was a great deal for the person ordering as all it had cost them was a couple of dollars in electricity to mine them.

Today (October 2016), 10,000 BTC is worth in excess of \$600,000...

So only invest what you are prepared to lose, enjoy your pizzas and remember that hindsight is always "20:20".

Beyond Bitcoin & Litecoin

Although Bitcoin and Litecoin are the original 'gold and silver' cryptocurrencies, the open-source nature of the software means that there are now over 80 alternatives (known as 'altcoins') out there, most of them based on the Litecoin codebase.

And just like other currency markets, there is money to be made (and lost) by speculating on the exchange rates of these currencies.

Some of these alternatives are genuine attempts to 'build a better coin' - just as Litecoin was designed to overcome some of the perceived weaknesses of Bitcoin - but its also fair to say that many more of these other coins are simply hyped up "pump and dump" schemes designed simply to make money for their creators.

Even so, some speculators have done very well making money trading these coins on exchanges such as shapeshift.io, and many others mine them in the early days as a way to get Bitcoin and/or Litecoin more cheaply.

That's because many of these alternative coins seem to follow a classic bubble pattern: The value of the coins rises dramatically shortly after release as people pile into it on the expectation that they will be able to sell at a profit to a 'greater fool' before the hype dies out and the coin crashes.

Of course, it's possible that another coin will emerge that is genuinely better and stronger than Bitcoin and Litecoin, so here are some things to consider before deciding whether to dabble in an altcoin or avoid it like the plague.

What's the innovation?

Some of the other coins offer some genuine innovations, such as Namecoin (key/value storage), Peercoin (Proof of Stake), and Primecoin (mines prime numbers).

Many others, however, offer little more than a few tweaks in the block creation or coin mining rates.

So it pays to ask yourself whether the coin offers any significant evolution of the Bitcoin concept, or is it just a pump and dump clone?

Who are the programmers?

Although the original creator of Bitcoin is a programmer (or most likely group of programmers) going under an anonymous pseudonym, "Satoshi Nakamoto", the current programming team is a public facing group of professionals currently led by Wladimir J. van der Laan of the MIT Digital Currency Initiative.

Likewise, the creator and lead programmer of Litecoin is ex-Google employee, Charles Lee, who leads a core group of 6 developers.

Both teams routinely work hand in hand to enhance the security of the overlapping parts of the Bitcoin/Litecoin protocols and are not afraid of standing by their work publicly.

On the other hand, some of the altcoins are run by anonymous individuals who have barely even got the programming experience needed to rebrand the Litecoin code.

Can you buy anything?

As we discussed earlier in the guide, the value of an crypto-currency depends not only on its utility as a store of value, but also as a medium of exchange.

An altcoin which people are happy to accept in return for goods and services for will build real long term value in the currency faster than an altcoin which merely generates exchange speculation.

This leads on to the final key indicator..

Is there a community?

Value comes in many forms, so even if the altcoin is too new to have any substantial number of people accepting it for goods and services, it may *still* be generating value in its community.

Does the coin have a strong moral mission or purpose? Does it attract a certain kind of person? Does it create a 'feel good' factor?

Dogecoin is a great example of where the community behind an altcoin can make all the difference. This coin was started as a joke based on the Shiba Inus "Doge" meme, but its lighthearted ethos has attracted a vibrant community of supporters wanting to 'do good'.

As a result, it is now the defacto coin for 'tipping' and community fundraising sent the Jamaican bobsleigh team to the Sochi Olympics.

In summary - are people investing themselves or the results of their hard work into an altcoin, or are they simply throwing a 'hot potato' from one person to another and hoping the music doesn't stop before they pass it on?

Resources

Here are the resources mentioned in this guide, in one place for easy reference, plus some more reading if you want to disappear 'down the rabbit hole'.

Bitcoin Resources

General

- **Official Website:** <http://bitcoin.org/>
- **Buying (and Selling):** <http://howtobuybitcoins.info/>
- **Using:** <http://usebitcoins.info/>
- **Block Chain Ledger:** <http://blockexplorer.com>
- **Charts and Stats:** <https://blockchain.info/charts>
- **Accepting Bitcoins:**
https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses

Paper Wallets

- **Online:** <http://www.bitaddress.org>
- **Offline:**
<https://github.com/pointbiz/bitaddress.org/archive/master.zip>

Software Wallets

- **Official Bitcoin Core:** <http://Bitcoin.org/en/download>
- **MultiBit:** <https://multibit.org/>

- **Blockchain.info Wallet:** <https://blockchain.info/wallet/>
- **Armory:** <https://bitcoinarmory.com/download/>
- **Electrum:** <http://electrum.org>
- **Bither:** <https://bither.net>

Mining

- <http://www.bitcoinmining.com>
- <http://www.coinwarz.com/calculators>
- <http://shapeshift.io>

Litecoin Resources

General

- **Official Website:** <https://litecoin.org>
- **Buying (and Selling):** <https://litecoin.com/services#exchanges>
- **Using:** <https://litecoin.com/services#merchants>
- **Block Chain Ledger:** https://litecoin.com/services#block_explorers
- **Charts and Stats:** https://litecoin.com/services#litecoin_data
- **Accepting Litecoins:**
https://litecoin.info/Service_directory#Merchant_tools

Paper Wallets

- **Online:** <http://www.liteaddress.org>

- **Offline:**

<https://github.com/litecoin-project/liteaddress.org/archive/master.zip>

Software Wallet

- **Official Litecoin Core:** <https://litecoin.org>

- **Electrum LTC:** <https://electrum-ltc.org>

- **Litevault:** <https://www.litevault.net>

Mining

- <http://www.cryptobadger.com/build-your-own-litecoin-mining-rig/>

- <http://www.coinwarz.com/calculators>

- <http://shapeshift.io>

Security

- **Strong Password Generator:** <http://www.diceware.com/>

- **Strong Password Generator (Online):**

<https://entima.net/diceware/>

- **Password Manager:** <http://keepass.info>

- **HouseCall AntiVirus:** <http://housecall.trendmicro.com/>

- <http://arstechnica.com/security/2012/08/passwords-under-assault/>

More Info

- The Original Bitcoin White Paper: <http://bitcoin.org/bitcoin.pdf>

- <https://en.bitcoin.it>