Virtual Currency:

the ฿itcoin manual

By Lachlan Roy

VIRTUAL CURRENCY: THE BITCOIN GUIDE

By: Lachlan Roy
http://lachlanroy.com

Edited by: Justin Pot

Cover Photo by Kushch Dmitry via Shutterstock

Table of Contents

Introduction

Cash is great.

There are no banks to worry about. No fees, no credit cards, no chance of having your identity stolen or your account frozen. You may not earn any interest, but you always have instant access to your money and you know exactly how much you have.

It's also great for when you need to give money to someone else. There's no forms to fill out or confusing account numbers. There are no fees to worry about. You don't need to deal with a middleman. You just hand over the money and that's it.

Then the Internet happened. Great services like eBay and web stores let you do your research at home and then buy exactly what you need without having to hunt for it in brick and mortar stores. All well and good, but suddenly cash isn't cutting it any more. After all, it's hard to hand someone a few notes and coins when they live on the other side of the world.

Wouldn't it be great to be able to use cash on the Internet, too? To have the ability to store your own money on your own computer? To buy what you need online without dealing with banks and middlemen?

That's where BitCoin comes in. Cash for the Internet is here.

BitCoin: The Virtual Currency

What is BitCoin?

BitCoin is a new, all-digital, *peer-to-peer* (p2p) currency, which can be used to replace cold, hard cash when buying and selling goods and services online.

Unlike most money online, which is stored in banks and transferred using payment processors like PayPal, BitCoin is completely distributed between its users and sent between users without the need for a middleman.

Why should I use BitCoin?

There are a few major advantages to using BitCoin in place of your normal currency for online transactions, most of which stem from how BitCoins are stored.

First of all, BitCoin is a global, decentralised currency. This means that there is no country to which BitCoin specifically belongs, making it a viable currency to use all over the world. This makes international transactions simple; no longer does there need to be a discussion over whether the payment should be made in the buyer's currency or the seller's, nor at which exchange rate the transaction should take place.

Another big advantage that decentralised currencies have is that a Federal Reserve or national bank does not manage the value of the currency. This means that the currency will retain its value regardless of the performance of the global economy, similar to the value of rare metals and commodities like oil. It has no single point of failure; the entire Internet would have to go down for BitCoin to fail.

Second, because transactions are made directly from one person to another, there is no middleman, and therefore no fees. In a few years time there will be a slight charge for transactions due to the way that the currency is managed, but it should be much less than the standard alternatives.

Third, because the BitCoins you own are stored in a *wallet file* on your computer, you have full control over your funds. Since the BitCoins are not stored in an "account" they cannot be frozen, meaning that you will never be left without cash. Furthermore, there is no "small print", transaction limits, forms or other limits like you would have with a bank.

Finally, while it does cost money to exchange fiat currencies to BitCoins and vice versa, it doesn't cost anything to accept them, making it a great way to be paid online for goods or services.

Some downsides to using BitCoin

Of course, like all things, there are some downsides to using BitCoins, which may mean that using them is not for you. It's worth giving it some thought before rushing in.

First of all, because you hold on to the money and don't store it in a bank, you won't earn any interest on any money stored as BitCoins. While to most people this isn't a major problem (since you're likely only using BitCoins to send to somebody else), if you're a merchant dealing in BitCoins, not collecting interest could have significant implications.

Reliability is also a major issue. While in theory its internet-wide distribution should make the currency stable, it is still potentially susceptible to shocks in supply or demand, which could cause rapid changes in its value. It's important to remember that BitCoin is a fledgling currency that has only been around for a couple of years and is one of the first of its kind, so there's no real way to tell how successful it will be.

Furthermore, while its decentralised nature can be advantageous, it does also mean that if something does go horribly wrong there's no bank or government to back it up.

Simply put: BitCoins could be worthless someday.

Another problem is the way that money is sent from peer to peer. While it is possible to create more complex transaction systems for BitCoin, the simple transfers that make up the majority of BitCoin transactions have no set securities. That basically means that all transactions are final and there are no refunds, making it great for scammers; once the money is gone, it's almost impossible to get it back without the other party returning it voluntarily. There is no bank or credit card company to appeal to.

The other main downsides to using BitCoins come down to the disadvantages it shares with physical cash - its ability to be lost or stolen. As the BitCoins are stored in a simple file called a *wallet file*, they can be at risk to hackers and viruses that can transfer the money from your wallet to theirs (which, again, is almost impossible to reverse due to the nature of transactions). However, it's a fairly simple and straightforward process to secure your wallet file - we'll touch on that later.

While it is quite difficult to "lose" the wallet file in the same way you might lose your real wallet, there are still the possible dangers of file corruption, hard drive failure

and accidental deletion. Since the only record of the BitCoins you own is the wallet file that they're stored in, losing the wallet means losing the BitCoins.

Again, this is fairly easy to safeguard against, and we'll be looking at a few different methods a bit later.

So, now you know the risks involved. There are a few, to be sure, but most are easily avoided.

How to use BitCoin

Getting a BitCoin wallet

The first step to getting started with BitCoins is to get yourself a BitCoin wallet. Just like a real wallet, this is where your BitCoins are stored. It is far more tangible than money stored in a bank account – the wallet file you create is a file just like any other document. It can be moved around and stored on different devices. You can even duplicate it to have multiple copies (obviously this doesn't duplicate the money inside, though!).

Your BitCoin wallet is comprised of two parts: the wallet file, which stores the BitCoins, and the wallet application (also called the BitCoin client), which opens those wallet files. This means that it is possible to store the wallet file on a USB drive (for example) and open it on any computer that has the wallet application installed. As there is a version for most operating systems, it's possible to open the BitCoin file pretty much anywhere.

You can download the official client from the BitCoin website (www.bitcoin.org). There you can get the right version for your operating system.

For Windows and OS X, installing the wallet application is just like installing any other application for your platform. I'll assume that you already know how to do this. Opening the application will generate the wallet file and assign you your first receiving address (more on this in a bit).

For Ubuntu, downloading the client gives you a `.tar.gz` file which contains four different versions: the main application and the windowless server in both 32-bit and 64-bit flavours. You can put this folder anywhere and then click on `bitcoin` to start the program.

Alternatively, instead of installing the BitCoin client, you can choose to use an online service such as Instawallet (www.instawallet.org). This site generates a wallet file and ties it to a specific URL which you can save as a bookmark. This allows you to access

your BitCoins from pretty much anywhere, but means that you have to trust the service with your BitCoins.

Have a look at the BitCoin client window. This is the Mac version, but like most cross platform applications it's pretty much the same for every version.
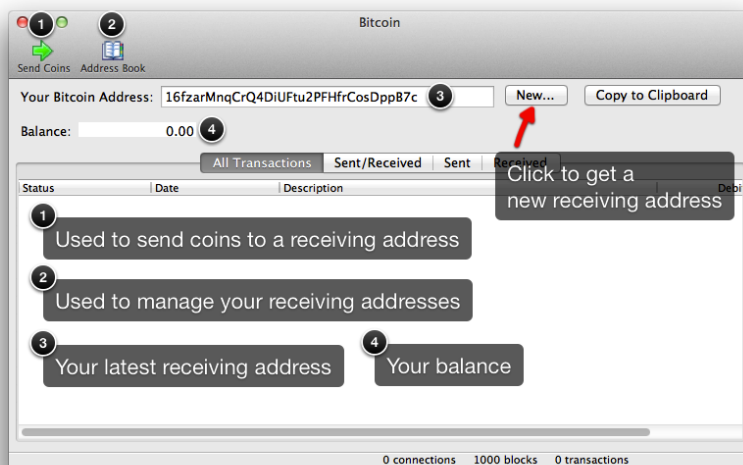

That's all there is to it. Pretty simple, right?

Filling your wallet

Now it's time to put some 'Coins' in that wallet. There are three main ways to add BitCoins to your wallet file: donations and free BitCoins, currency exchange, and BitCoin trading (or becoming a BitCoin merchant). Each one is fairly self-explanatory, but we'll go a bit more in-depth anyway.

Before that, though, it's time to introduce some new terminology. BitCoins are sent to your wallet via a *receiving address*, which is a long string of randomly generated characters that points to your wallet file. The process is similar to the sender writing a cheque for a certain amount, although the process is all automatic and the cheque doesn't need to be manually cashed in.
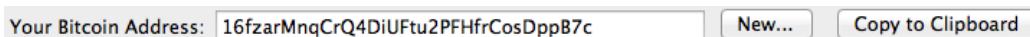
Interestingly, you don't need to use a single receiving address forever; on the contrary, it is generally recommended that you create a new receiving address for each expected transaction so that it is easier to track individual payments. All previous receiving addresses remain valid and active, so it is possible for old receiving addresses to be reused again and again.

You can also fill your wallet through BitCoin mining - we'll be dealing with this later.

Donations/Free BitCoins

As you may have guessed, this section deals with free BitCoins from websites and from other individuals. While the BitCoins you'll get for nothing are few and far between (and usually far less than a whole BitCoin), it's still something to get you started and to help you understand how BitCoin transactions work.
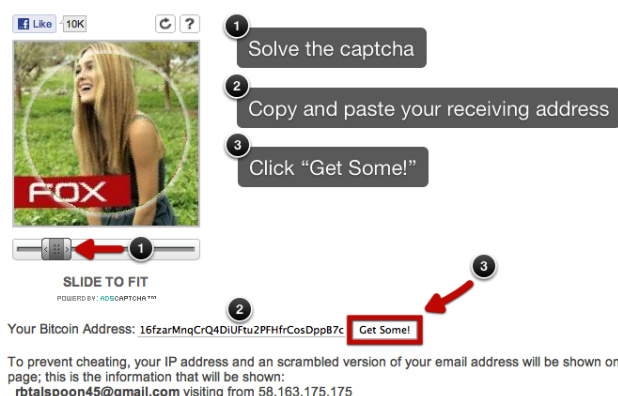
The best place to get your first free BitCoin (or a percentage thereof) is to head over to the BitCoin Faucet (https://freebitcoins.appspot.com/), which gives out 0.001BTC to new BitCoin users. You'll need a Google account of some description (typically your Google Mail or Google+ account, although you can sign up for a free Google account using a different email address) – a countermeasure put in place to prevent a few people from abusing the free money.

Once you've logged in with your Google account, you'll need to solve a captcha (a puzzle used to prove that you're not a robot), then enter your receiving address before clicking "Get Some!".

That's it! It may take up to 10 minutes for the payment to come through, as the BitCoin Faucet bundles payments together to reduce load on the network, but then you should see 0.001 BitCoins show up in your wallet.

Donations work much in the same way. You can put a receiving address pretty much anywhere; on your FaceBook or Google+ profile, on forums, in email

signatures or even in real life. That way, if somebody has some spare 'Coins and wants to thank you for something it's just a case of sending a BitCoin or so to your receiving address.

If you found my post helpful, feel free to send a tip to 1QGukeKbBQbXHtV6LgkQa977LJ3YHXXW8B
The amount doesn't matter—just getting in the habit helps us all build a healthier, friendlier, more productive web.
Please lend your support for the New BitCoin Q&A Site

A typical example of a receiving address placed in a forum signature
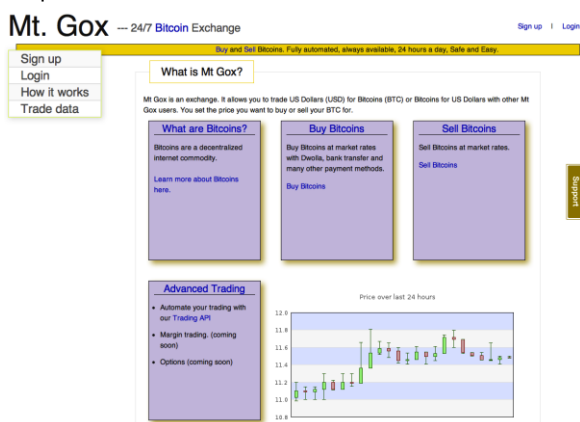
Currency Exchange

Although free BitCoins are awesome, it doesn't give you a whole lot to work with. The easiest solution is to exchange your currency for some BitCoins. There are a number of websites you can use to do this, though you'll need to make sure that the website you choose will handle your particular currency (otherwise you'll end up exchanging money twice, with transaction fees and all)!

For a list of the BitCoin exchange sites and the currencies they support, there's a page over at the BitCoin wiki (https://en.bitcoin.it/wiki/Trade).
There are two main types of currency exchange: real time and fixed-rate. Real time trading is where the buyer lists the maximum price they are willing to pay for each BitCoin, while the seller lists the minimum price they are willing to sell each BitCoin for. Trade instantly happens when these two prices overlap. In this scenario it is possible to get a great exchange rate, although this can require some patience.

Fixed-rate exchange, on the other hand, is much closer to your standard foreign exchange transaction: a company will offer a rate which is fixed for a certain period of time, and will exchange any quantity of fiat currency for BitCoins at a standard rate. While you won't get as good a deal as if you're patient in real time trading, fixed-rate exchange is more reliable and instantaneous.

The most popular exchange website by far is Mt Gox (www.mtgox.com), which is responsible for over 80% of BitCoin transactions using the real time model.

BitCoin Trading

The other main way to get BitCoins is to earn them by providing goods or services online and accepting BitCoins as payment. From obvious things like web design and app development to crazy things like ordering pizza for someone, dictating 500 words or writing a song, pretty much anything can potentially earn you BitCoins.

If you want to sell physical objects, you can use websites such as the BitCoin World Market (http://www.bitcoinworldmarket.com) which pays you in BitCoins or other currencies.

Conversely, if you already run a business online, accepting BitCoins is really easy. You can read more about this by looking at the article on the BitCoin Wiki (https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses) then post a link on the Trade page (http://en.bitcoin.it/wiki/Trade) so that people can find your website!

Finally, if you want to sell a one off item or provide a service, look no further than the site For BitCoin (http://www.forbitcoin.com), which will let you say what you'll do for BitCoins and how much you want for the trouble. It's a simple idea, but one that works really well.

Spending BitCoin

Funnily enough, finding something to spend your hard earned BitCoins on is just a case of going to the same places you can use to earn BitCoins.

The best place to start is the BitCoin Wiki's Trade Page (http://en.bitcoin.it/wiki/Trade), which provides a list of all the known websites that accept BitCoins for goods or services.

All BitCoin transactions involve a sending address and a receiving address. When you earn BitCoins you give somebody your receiving address; to spend BitCoins, you're provided a receiving address to send BitCoins to.
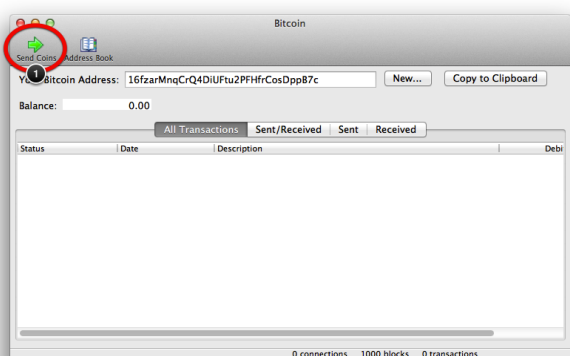
Sending BitCoins is easy. Just click on the "Send Coins" button in the client window. Then, in the resulting "Send Coins" window, enter the Receiving Address you want to send the coins to, specify an amount and click "Send". That's it!

Securely Sync Your BitCoins

Since you're looking after your money yourself, and there's no built-in backup in case something goes horribly wrong and your money is lost or stolen, it's important that you keep your BitCoin wallet locked up and backed up.

To achieve this, we'll be making use of two separate, free, cross-platform programs that we've extensively covered in the past: TrueCrypt and DropBox.

The process is largely the same regardless of platform, although each operating system does have a slightly different place that it stores the BitCoin files. We'll quickly run through each one, and I'll assume you know what you're doing with TrueCrypt and DropBox and that you already have them installed and ready to go. If you haven't come across them before, I strongly suggest that you go and read the MakeUseOf PDF guides for each.

Bear in mind, though, that some of the steps involved are quite advanced. If you're not at all confident in your abilities with a computer, I'd suggest leaving this bit alone. As a general rule, if you have no idea where or what the Terminal is, you probably shouldn't be using it.

Windows

First up, you'll want to make a Virtual Encrypted Disk using TrueCrypt. Just use the basic settings, and don't worry about making a dynamic disk – you really don't want anything going wrong with it! Ideally the VED should be around 100MB in size to accommodate any large increases in file size in the future. Save the VED file to DropBox so that it's automatically backed up!

Before we start working with the files, start up BitCoin and take note of the receiving address. We can use this to verify that it is using the data properly.

Once you've done that, it's just a case of finding the folder where the BitCoin client stores all its files (including your wallet file). You can usually find this by going to Start > Run (or by pressing `WinKey + R` and typing in the following:

```
explorer %APPDATA%\Bitcoin
```

This is the default location for BitCoin data:

```
C:\Documents and Settings\YourUserName\Application data\Bitcoin (XP)
```

```
C:\Users\YourUserName\Appdata\Roaming\Bitcoin (Vista and 7)
```

Once you've found the folder, copy the entire folder into the VED that you created earlier. Take note of the drive letter you assign to the VED – you'll be using this in a bit when you tell BitCoin where to look for its data. For this example we'll assume that the drive you have selected is the E: drive.

Once you've copied the files over, create a temporary backup of the file, then delete the original file from the `Appdata` folder. This will force the BitCoin client to use the VED as a source if everything has been done correctly, otherwise it will simply create a new folder to replace the one that was deleted.

Now that you've finished moving files around, you can create a new shortcut to start the BitCoin application. Find BitCoin in your Start Menu, right click the shortcut and choose "Send to > Desktop (create shortcut)". Then right click the shortcut you just edited and click "Properties…" and enter in the following in the "Target" field:

```
C:\Program Files\Bitcoin\bitcoin.exe -datadir=E:\Bitcoin
```

Don't forget to change `E:` to the drive letter you assigned the VED. Also, if you're using a 64-bit version of Windows, you'll need to change

```
C:\Program Files\ 
```
to `C:\Program Files (x86)\`

The first part of the Target string (starting with `C:\Program Files\`) is the location of the BitCoin client application, but not the wallet file or the files it works with. The `-datadir` switch basically tells BitCoin to load all its files from `E:\BitCoins` instead of the default file location in the `AppData` folder.

With that done, it's just a matter of double clicking that shortcut to use BitCoin from the secure Virtual Encrypted Drive. Just make sure that you've mounted the VED *before* you start the BitCoin client, and that you always mount it to the same drive letter.

At this point we can start up the BitCoin client and check to see whether we have the same receiving address as the one we started with. If we do, it's been successful. If not, don't worry! Just try going through the steps again.

Mac OS X

If you're using OS X 10.6 or 10.7 (Snow Leopard or Lion), you'll need to install a free system utility called MacFUSE first that provides the software necessary to create VEDs using TrueCrypt. It uses a standard .pkg installation process, so you shouldn't run into any problems at all. When that's installed, we can get started properly.

Create a Virtual Encrypted Disk (VED) using TrueCrypt. Just use all the default settings, enter a secure password and save it in your DropBox folder. You'll want to allocate around 100MB to the VED to make sure that you don't run out of room down the line.

After creating the VED, mount it using TrueCrypt. This will mount a volume which looks just like when you mount a .dmg file to install an application. By default this will be called `NO NAME` – right click this in the Finder sidebar and rename it to something a bit more intuitive, such as `BITCOIN` (FAT, the file system used by the VED requires the name to be in capital letters).

Before doing anything to the BitCoin files, open up BitCoin and take note of your receiving address. We can use this to verify whether the symbolic link has worked correctly.

By default, the files needed by the BitCoin client are stored in the following location:
`~/Library/Application Support/Bitcoin`

The ~ means your home folder, not the root `Library` folder – these are two different folders which contain different data. Make sure you look in the right one! When you find it, copy the entire `BitCoin` folder to the VED and then delete the folder in `Application Support`. You'll probably want to copy it to your Desktop as a failsafe in case something goes wrong, too.

Now it's time to create a *symbolic link* to trick OS X into thinking that the folder is still there in `Application Support`, even though it's now in the VED. To do this, we'll need to start up a Terminal window, and enter in the following:

```
ln -s /Volumes/BITCOIN/Bitcoin ~/Library/Application Support/Bitcoin
```

Where `BITCOIN` is the name you gave to the VED when it's mounted.

That's the last step! Now you can start up the BitCoin client and it will take its data from the VED. Make sure you mount the VED *before* starting the BitCoin client, though – if you start the client without mounting the VED, it will create a new `Bitcoin` folder in `Application Support` and remove the symbolic link. If this happens, just delete the folder in `Application Support`, mount the VED and create the symbolic link again using the same command.

Now we can start up the BitCoin client and check to see whether we have the same receiving address as the one we started with. If so, it's all done and working great.

Ubuntu

First up, create a Virtual Encrypted Disk (VED) using TrueCrypt. Just use all the default settings, use a secure password and save it in your DropBox folder. You'll want to allocate around 100MB to the VED to make sure that you don't run out of room down the line.

When you've created the VED, use TrueCrypt to mount it. When you choose a slot to mount the VED, it will mount it in `/media/truecrypt<x>`, where `<x>` is the number of the slot you chose. For this example, we'll assume you've chosen slot 1, in which case the mount point would be `/media/truecrypt1`.

Before doing anything to the BitCoin files, open up BitCoin and take note of your receiving address. We can use this to verify whether the symbolic link has worked correctly.

By default BitCoin files are stored in the folder `~/.bitcoin`, where ~ is the root of your home folder. As files starting with "." are hidden by Ubuntu, you'll need to unhide the folder by pressing `Ctrl + H`. Then move (`Ctrl + X` to cut, `Ctrl + V` to paste) the entire `.bitcoin` folder to the VED, which acts just like a memory stick.

Once the files have been moved, we just need to make a symbolic link to point the BitCoin client to the VED when it's looking for its files. We do this by opening up a Terminal window (Applications > Accessories > Terminal) and entering the following:

```
ln –s /media/truecrypt1/.bitcoin ~/.bitcoin
```

All done! If you go and start the BitCoin client again, you should notice that your receiving address is the same as before. This means that you've done everything successfully and it is ready to use.

Make sure you mount the VED *before* starting the BitCoin client, though – if you start the client without mounting the VED, it will create a new `.bitcoin` folder in your home folder and remove the symbolic link. If this happens, just delete the `.bitcoin` folder in your home folder, mount the VED and create the symbolic link again using the same command you used before.

BitCoin Mining

Before we start to talk about this, I should point out that very few people mine for BitCoins. You don't need to mine to use BitCoins; people who mine usually either do it for fun or are prepared to take a risk with a business that is very likely to make less than invested.

What is BitCoin Mining?

Although BitCoin is a distributed, peer-to-peer currency, it has to have a set capacity for it to retain its value. For this reason, there will be a total of just under 21 million BitCoins available for circulation.

However, if 21 million BitCoins were to become available all at once and there wasn't enough demand for them, the BitCoins would be essentially worthless. For this reason, the rate of new BitCoins entering circulation must be tightly controlled so that BitCoins do not flood the market, instead being introduced gradually over the next 100 years or so. This is where BitCoin mining comes in.

BitCoin mining is the process of using a computer to generate blocks, which are used to process and verify the transactions which occur between the time the block was generated and the time the previous block was generated. Blocks contain data from the previous block so as to create a block chain, which contains information about every transaction within the chain.

Creating a block requires a lot of work, which translates to a lot of time and a lot of computer processing power. So, as an incentive, anybody who successfully creates a block is given a reward (currently 50BTC, worth roughly 500 USD at the time of writing) as well as any transaction fees included in the transactions hashed in the block.

Total BitCoins over time
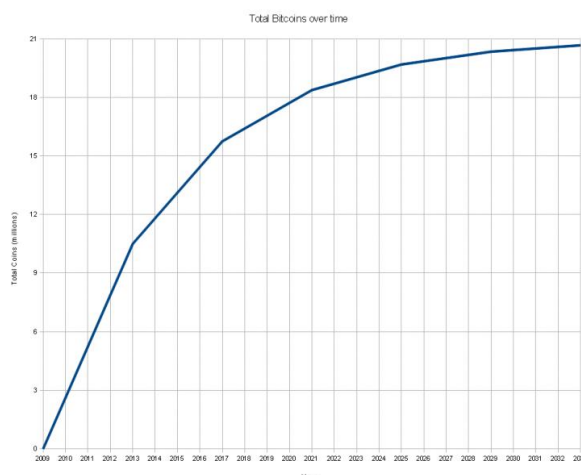
There are a few catches, though. The network is designed to maintain a block production rate of a new block every 10 minutes (or 6 blocks an hour). As more people begin to mine with more powerful computers, the difficulty is adjusted so that it takes longer for a block to be produced (making it harder for each individual to be the producer of a block).

The other catch is that the reward for each block produced is halved every 210,000 blocks. Currently there are around 142,000 blocks in existence, so it will be a while before the reward amount falls. When it does reach 210,000 blocks, though, the reward will drop to 25BTC. When 420,000 blocks have been produced, the reward will fall to 12.5BTC, and so on and so forth.

Once the 21 million BitCoins have been produced there will no longer be a reward, although the producer of the block will still receive all transaction fees for that block (which, by this point, will be significant enough to be a reward in itself).

What do I need to mine BitCoins?

At its most basic, all you need for BitCoin mining is a computer with a BitCoin mining application and an Internet connection. Having said that, there's a difference between mining BitCoins and mining BitCoins *well*. The applications used for mining BitCoins make use of your graphics card, which can carry out many calculations at the same time (far more than possible with even the best CPUs). Put simply, more powerful graphics cards can carry out more calculations at once and carry them out faster.

BitCoin mining performance is measured in *hashes per second* (hash/s), or the number of times the graphics card can convert the data supplied to it into a fixed-length string of characters. When a hash is generated with the correct value a block is created, so the higher the hash/s value of the graphics card, the faster it is likely to create a new block.

Most mid-range desktop graphics cards today (such as the AMD 6750 for $120) are capable of producing around 170Mhash/s (*Megahashes* per second) - that's 170 000 000 hashes per second.

On the flip side, some people build servers made specifically for BitCoin mining. These may have 3 or 4 of the most powerful graphics cards currently available, which working together are able to produce over 2Ghash/s (*Gigahashes* per second) - that's more than 2 000 000 000 hashes *every second*.

Having said that, you can still successfully mine by using the graphics card in your computer, although upgrading it to a more powerful graphics card to improve performance can still be beneficial.

To mine using a Mac you really want to be running Snow Leopard or later – earlier versions of OS X can't make use of the graphics card and are too slow to be worth the hassle.

How do I mine BitCoins?

Mining for BitCoins is really easy, and just needs to be set up then left to mine. First you'll need to choose how you want to mine. It boils down to two options: mining by yourself, or mining as part of a pool (where you pool your computer's work with other members and split the rewards when a block is produced).

If you mine by yourself, you'll get to keep 100% of everything you earn. Just bear in mind that there's no way of knowing if and when you'll produce a block. Conversely, working for a pool means that you'll get a steadier income (as the pool is more likely to produce more blocks than you are by yourself), but you'll sacrifice some of your earnings to the person running the mining pool.

In this guide I'll be showing you how to start mining for yourself, and also for mining in the BTC Guild mining pool. If you're using Windows or Ubuntu, Danny Stieben has written a great guide to get you started over on the main MakeUseOf site. For OS X we'll be using the *DiabloMiner.app*, a frontend for the command-line BitCoin miner *DiabloMiner*. You can download the latest version from this thread on the BitCoin Talk Forum. Make sure you select the **DiabloMiner** version, not the **RPCMiner** version (which uses the CPU instead of the GPU and is much slower as a result).

Solo Mining

Configuring the BitCoin Client

Before we can start mining, we need to set up the client to act as a server that communicates with the BitCoin network so that we can mine by ourselves. This involves editing a file called `bitcoin.conf` (or creating one if it doesn't already exist). This is stored in the `Application Support` folder, along with the other BitCoin files.

First, browse to the `Application Support` folder to see if there is already a `bitcoin.conf` file. If there is, open it with TextEdit. If it isn't, we'll open TextEdit anyway to create the file.

When we have TextEdit open, make sure that you're working in Plain Text mode (as formatting plays havoc with program files) by pressing cmd+shift+T. Then enter the following text:

```
rpcuser=username
```

```
rpcpassword=password

rpcport=8332

server=1
```

You can change the username and password if you wish; for solo mining it doesn't really matter at all either way. `rpcport` is the port which BitCoin uses for uploading and downloading new block information, and `server=1` makes BitCoin enables server functions allowing us to mine without connecting to a pool. Save the file; if you're creating it from scratch, make sure to disable "If no extension is provided, use .txt".

Now you can start BitCoin and it will automatically start up the server in the background. When this happens it will start to download all the previous blocks it can find, which can take a *very long time*. This can affect DiabloMiner, so you'll need to wait for it to finish.

Configuring DiabloMiner

When you start DiabloMiner for the first time, you'll be greeted with the set-up wizard. These are the settings you'll want to enter:

Server host name or IP address: `localhost`

Server port number: `8332`

Miner username: `username (or whatever username you chose)`

Miner password: `password (or whatever password you chose)`

Start mining automatically on log-in? `No (so you can change settings)`

That's it! DiabloMiner will take care of the rest. However, if you see an error like:

```
ERROR: Can't connect to Bitcoin: Bitcoin returned error message:
Bitcoin is downloading blocks...
```

It's because the BitCoin client hasn't finished getting set up yet. Unfortunately there's no easy way to tell when it's ready, so you'll just have to wait and try again later.

Mining Pool (BTC Guild)

Creating a BTC Guild Account

The first step to mining in a pool is creating an account with the mining pool. This is usually done through the pool's website – in this case http://www.btcguild.com.

Creating an account is just like creating an account on any website. There's a link for creating an account on the left hand side of the page under the login box. Just choose a username and password and then click "Register". You'll instantly be logged in with the username you just chose; there's no confirmation email to worry about.

Creating a Worker

The next step is to create a *worker* account – each computer used for BitCoin mining needs its own login (which allows you to set up multiple computers all mining under your one main username).

If you don't have any workers yet, red text will appear at the top of the screen telling you to set up a new worker. It's a link; click it and you will be taken to the *Worker* page which allows you to add a new worker.

Creating a new worker just involves providing a worker name (which is in the form of `yourusername_workername` where `yourusername` is your BTC Guild username) and a password for that particular worker (we'll refer to it as `worker_password`).

Configuring DiabloMiner

When you start DiabloMiner for the first time, you'll be greeted with the set-up wizard. These are the settings you'll want to enter:

Server host name or IP address: uscentral.btcguild.com

Server port number: 8332

Miner username: yourusername_workername

Miner password: worker_password

Start mining automatically on log-in? No (so you can change settings)

All done! You should see text to the effect of:

[8/23/11 2:31:08 AM] Started

[8/23/11 2:31:08 AM] Connecting to:
http://uscentral.btcguild.com:8332/

[8/23/11 2:31:08 AM] Added ATI Radeon HD 6750M (#1) (5 CU, local work size of 256)

Waiting...

```
59005/62050 khash/s
```

When you see that last number you know that you have successfully connected and you have started mining. Congratulations!

You'll want to give it a while – a few days, maybe more – before you collect any payouts. At that point you can supply your receiving address to the pool website and they will transfer your earnings straight to your wallet. Simple!

Conclusion

BitCoins are great.

There are no banks to worry about. No fees, no credit cards, no chance of having your identity stolen or your account frozen. You may not earn any interest, but you always have instant access to your money and you know exactly how much you have.

They're also great for when you need to give money to someone else. There's no forms to fill out or confusing account numbers. You don't need to deal with a middleman. You just send some BitCoins to their Receiving Address and that's it.

Then the Internet happened. Web stores let you do your research at home and then buy exactly what you need without having to hunt for it in brick and mortar stores. After all, it's easy to send someone a few BitCoins, even if they live on the other side of the world. If you're the one selling, it's even easier to receive them.

Even if you're not selling, you can still conjure BitCoins out of the cryptographic soup that is the hash, block and block-chain system that makes BitCoins tick using nothing but a computer with a discrete graphics card.

Isn't it great to be able to use cash on the Internet, too? To have the ability to store your own money on your own computer? To buy what you need online without dealing with banks and middlemen?

Yeah. It is, and BitCoin makes it possible.Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips.

Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips.

If you want more great guides like this, why not **subscribe to MakeUseOf and receive instant access to 20+ PDF Guides** like this one covering wide range of topics. Moreover, you will be able to download free Cheat Sheets, Free Giveaways and other cool things.

Subscribe to MakeUseOf : http://www.makeuseof.com/join

MakeUseOf Links:

Home:	http://www.makeuseof.com
MakeUseOf Directory:	http://www.makeuseof.com/dir
MakeUseOf Answers:	http://www.makeuseof.com/answers
Geeky Fun:	http://www.makeuseof.com/tech-fun
PDF Guides:	http://www.makeuseof.com/pages/
Tech Deals:	http://www.makeuseof.com/pages/hot-tech-deals

Follow MakeUseOf:

RSS Feed:	http://feedproxy.google.com/Makeuseof
Newsletter:	http://www.makeuseof.com/join
Facebook:	http://www.facebook.com/makeuseof
Twitter:	http://www.twitter.com/Makeuseof

Download Other MakeUseOf PDF Guides!

Like us to download: http://makeuseof.com/pages