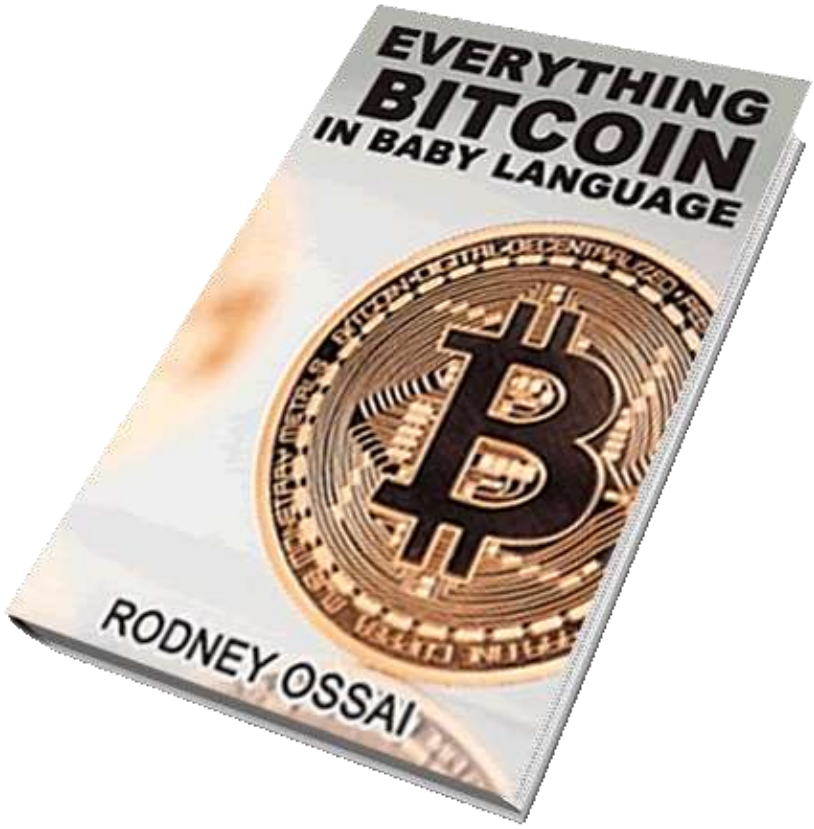
EVERYTHING
BITCOIN
IN BABY LANGUAGE

By the administrator **figurehowto.com**



What Is Bitcoin

Most Bit-coiners suck a lot when it comes to explaining bitcoin; they start with "**Bitcoin is a cryptographic**", "**Bitcoin is a decentralized**" WTF!! Is that what the layman wants to hear?

Bitcoin is a new kind of currency that isn't regulated by any government.

Bitcoin is **gold** that resides on the internet. The value of 1bitcoin will depend on how much people need bitcoins. So just as the scarcity of gold and the difficulty involved in mining gold makes it very valuable, the scarcity of bitcoin and the difficulty to mine bitcoin it also makes it very valuable.

I describe bitcoin as "**a digital version of gold**." eGold.

BITCOIN AS A CURRENCY

Currency is a medium of exchange for goods and services, and nothing more .When something is scarce and people want it, it can automatically be used as money. In the past, before Paper Money was born gold was cut into flat chips and used as money (Again scarcity of gold).

Bitcoin is an electronic currency (eCurrency) as people have begun to accept it as a form of exchange for goods and services. Unlike any other normal modern day currency; USD, EUR, GBP etc. where there is a central authority that controls the printing of these currencies and inflation rate bitcoin is de-centralized (there is no central authority/bank/server) Again, just like gold. There is a fixed amount of gold in this world (Planet earth) we just keep mining maybe we can find all. Also there is a fixed amount of bitcoins that can exist. We just keep mining maybe we can reach the limit.

What has really made bitcoin attractive is the fact that there is no server, there is no central bank you have full control over your funds. The question many people ask now is how the bitcoins are generated or created. How are they are minted since there is no central bank.

HOW DOES BITCOIN MINING WORK AS THERE IS NO SOIL TO DIG ON THE INTERNET.

Bitcoin Miners are like **the Central Bank of bitcoins**. BITCOINS are mined with software called **Bitcoin Miners**, it sounds funny right? One of the most common points of confusion for new Bitcoiners is the concept of mining. Well there are a lot of technical terms you need to understand before you can understand bitcoin mining but i will try to make this explanation as simple as possible.

BITCOIN MINING is the process by which some users put their computers to work verifying transactions in the bitcoin network. These users are rewarded with **new bitcoins** when they successfully complete the work of verification. These miners are like **the Central Bank of bitcoins** because they are the one who release more bitcoins into the economy by distributing the coins they mined by spending it.

The miner's computer solves very very complex calculations that have the ability to overheat your computer processor. The result of this calculation is called **HASH.** A hash cannot be reversed. These calculations to confirm transactions that happen on the network is called mining **because it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground.**

Some Computer Processing Units or external processing unit can perform these computer calculations (HAS HING) faster than others and this speed is rated in **HASHRATES** e.g. 1H/s means the processor performs one hash in one second 1KH/s means the processor performs 1000 hashes in one second, 1 MH/s means that the processor performs 1,000,000 hashes in one second.

Once again is the hashing term is beginning to cloud your brain and make you feel dizzy?. A hash is the solution to a complex mathematical puzzle solved by a processor to verify transactions that happened on the bitcoin network. Some processors are faster than other processors when it comes to solving the math and this is measured in hash-rates. A higher hash-rate means the processor computes more hashes in less time. These types of processors are better for mining as you will be rewarded with more bitcoins.

How Bitcoin Mining works to Mint new coins

People are sending coins to each other over the bitcoin network every second, but someone keeps a record of all these transactions right? Yes, this happens so that we know who had paid what? The bitcoin network handles this by bundling all of the transactions made during a short period (10 minutes) into a chunk of data, called a **BLOCK**

These blocks (or grouped transactions) are linked such that each new block proves that older blocks were valid. Linked blocks are called **BLOCK-CHAIN**

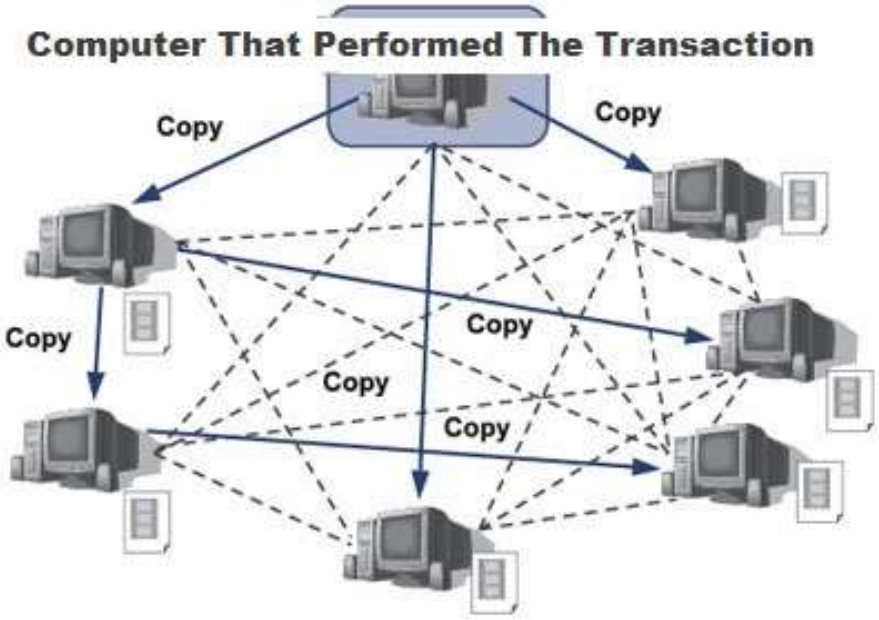
The Bitcoin network was designed in a way that only 6 blocks will be solved in 60 minutes(1hr) Which means that in every 10 minute interval a new block is created for processors to HASH(verify transactions contained in the block)

The first transaction in a block is a special transaction that produces new bitcoins (25) owned by the creator of the block.

The creator of the block is the miner or the computer that bundled the transactions together, verified them and put them in the block chain (where older blocks were kept.)

Block Chain

The block chain is simply a database where records of all the transactions that ever happened on the bitcoin network are kept. Since there is no central server on the bitcoin system, where exactly is this block chain stored. Every user on the bitcoin network is a server and a client. The bitcoin network is a **peer-to-peer network.**



PEER-TO-PEER NETWORK

When bitcoins are sent from one address to another the transaction is broadcasted (sent out) to all other nodes directly connected to the node that performed the transaction those other nodes still broadcast what they receive and in no time everybody on the network hears about the transaction.

Because of the blockchain that everybody on the network has a copy of, now everybody knows about every transaction that has ever happened on the network so everybody will know what every other persons account balance should be by simple plus and minus. Example bitcoin account 1FdPFc6bWdPiz2UP18jorvbuP6sZZ31LU2 has received only 3 bitcoins in his entire history and has sent out 1 bitcoin in his entire history so his balance must be 2 bitcoins. Everyone on the bitcoin network knows this. So your bitcoins are not stored on your PC as per say but on the network.

So the basic concept on mining is once a transaction (true or false) happens on bitcoin network, the terminal that performed that transaction broadcasts that transaction is to all other nodes (computers) on the bitcoin network connected to him. Each Miner node or computer involved in bitcoin mining bundles these transactions into a block. Each block will contain some meaningless data and false transactions like double-spend attempts. The mining computers now put this block through a hash (complex math) and an output will be gotten normally it's just a sequence of numbers and alphabets.

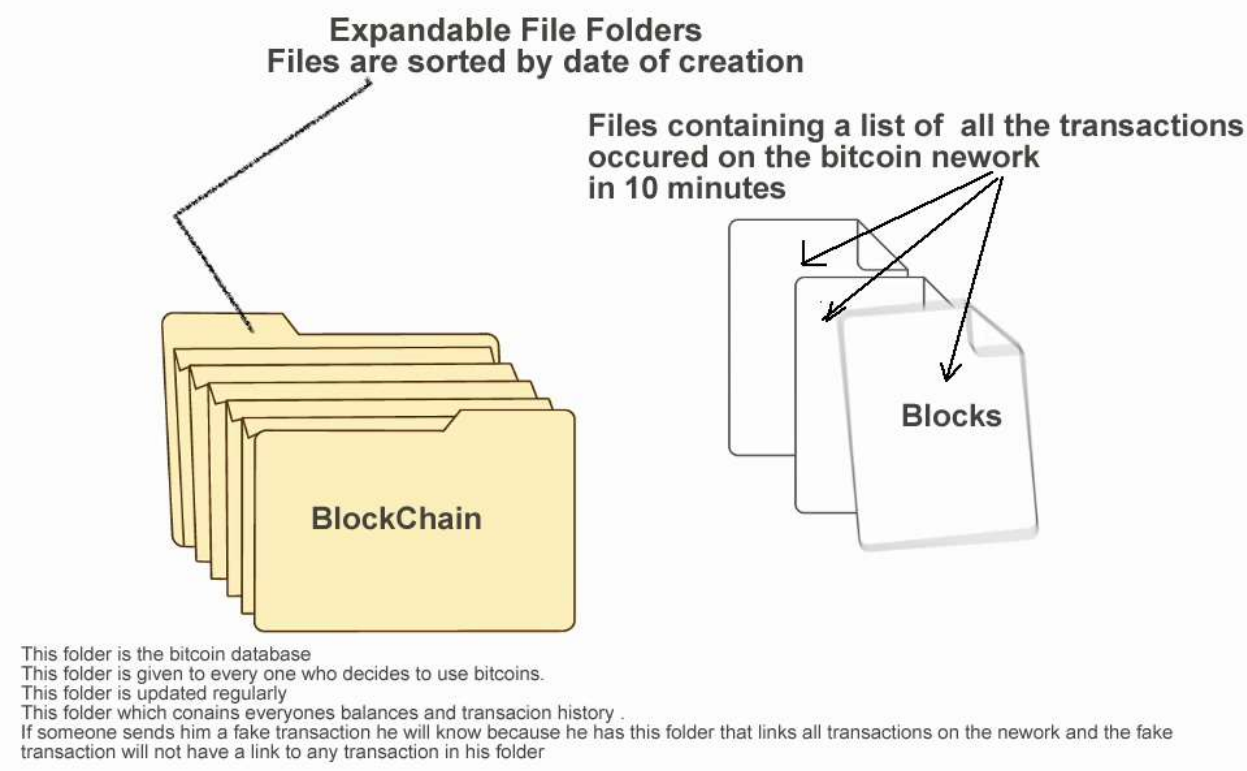
Example of a hash **b666f26b0f364886b8fe9127920fd9202315e9fe** but what makes the bitcoin network unique and difficult is that the bitcoin network will not just accept any hash value the network demands that a block's hash has to look a certain way; **it must have a certain number of zeroes at the start** so the processors involved in mining bitcoins have to work that out. When a miner

finds out correct hash value, it immediately broadcasts the new block. Also every computer on the network has its own copy of the block chain (record of transactions) so he simply adds the newly found block to the block chain.

The first transaction in a block is a special transaction that produces new bitcoins (25) owned by miner that discovered the block by solving it. The owner of these new coins distributes his new coins into the bitcoin economy by spending.

If a Mining pool was used the members of the pool share the new bitcoins in ratio of the hash power he/she donated to the pool. If you are a solo-miner you keep all 25 bitcoins to yourself.

In other words a block is a list of transactions written on an A4 sheet; the BlockChain is these A4 Sheets arranged in a file folder according to the order in which they were received.



Mining Pool

With a lot of **powerful processors** on the bitcoin network having the ability to perform millions of hashes in one second, it will mean that blocks will get resolved before 10 min and this will go against the Bitcoin network design that specifies that a block is released every 10 min. If more than one block is released in 10 minute period it means more than 25 bitcoins are minted in 10 minutes. If this continues there will be excess bitcoins in circulation and as a result the value of bitcoin will decline because it is no longer scarce.

Any way the bitcoin network automatically addresses this issue by increasing the **network difficulty** as more powerful devices begin to hash. This is achieved in such a way that the processors are made to perform more hashes to verify a single transaction.

*Say for example normally **4096** hashes verifies a **1 block of transactions** as the devices on the network become more powerful, in order to ensure that only 6 blocks are calculated in an hour the network then adjusts the difficulty to ensure that **12288** hashes verify **1 block of transactions.***

Common software's that can help you begin mining are **BFG miner**, **CG Miner**. and a host of others.

If you wish to begin mining it is usually advised that you start with a mining Pool

What is a Mining Pool.

As the network difficulty continues to increase it becomes impossible for you to use your CPU to mine because it may take your months of none stop hashing to find a block. People came together, formed a team and used the collective computing power of their CPU for mining.

We can simply say a mining pool is a group of people who decide to bring their processors together (they form a team) so they use the combined **HASHING POWER** (calculating power) of their CPU, GPU, ASIC to mine new BITCOINS.

The new bitcoins are shared according to the HashPower you contributed to the pool (Pool members with greater hash-rates get more Bitcoin when bitcoins are minted)

To rephrase, the newly generated 25 bitcoins are shared among pool members based on their contribution to solving a block. The larger your contribution, the more returns you'll receive.

When all the bitcoins are mined, miner rewards will come from transaction fees.

Common Bitcoin Terminologies

There are a lot of terms you hear when you get into **bitcoin.** I mean a whole lot of terms. We will start with the most common terms.

1) Hash: - is the output of a hash function. A hash function is simply defined as complex math performed by processors but that definition will be misleading so a hash function is a mathematical function that takes an input of any possible length of characters and transforms it into an output of a fixed length of characters. A hash output is normally it's just a sequence of numbers and alphabets like this **b666f26b0f364886b8fe9127920fd9202315e9fe .** The bitcoin network demands that the hash output of a block must resemble **00000febfe912ca920** because it increases the network difficulty by increasing or reducing the number of zeros it demands at the start there by increasing or decreasing the number of times a processor will have to solve the complex math.

2) Address: - A bitcoin address is similar to bank account number. It is the only information you need to provide if you wish to receive bitcoins. It is like the reference number to the container where your bitcoins are stored which makes it your bank account number inside the bitcoin economy.

It is not a wallet. Every bitcoin address is directly linked to a private key. You can calculate the bitcoin address if you have the private key. You can transfer money from an address if you have the private key.

Example of a bitcoin address: ***1FdPFc6bWdPiz2UP18jorvbuP6sZZ31LU2.***

3) Wallet: - A bitcoin wallet can contain one or more bitcoin addresses. When you download the bitcoin client for your PC or Android then your PC or Android device it becomes a wallet. A wallet holds your private key. Simply the wallet is a program which stores the private keys.

Websites like **blockchain.info** provides a free and very secure wallet service (An Online Wallet.) which makes it easy to send and receive Bitcoins without needing to download a Bitcoin client.

4) Private Keys: - Every Bitcoin address (account) has a unique private key attached to it. This key is what allows you to maintain control of those bitcoins inside the Bitcoin address. A private key must always be kept secret. **Anyone with your private keys can spend your Bitcoins!!! .** The private key is a secret code which allows the user to prove his ownership of his bitcoins. It is like your ATM CARD PIN or Online Banking account Password.

E.g. of a private key: **5JZB4ewYsbJhej6Psb5gL1h5BL26EoA49EzwoLSSXB8rtEDX8su**

5) Bitcoin (BTC): - Simply put is a new kind of currency that is not regulated by any government. A difference exists between the terms **'Bitcoin'** and **'bitcoin'**. Bitcoin written with capital 'B' refers to the entire system; the bitcoin economy while Bitcoin written with small 'b' is used to describe the unit of account, the currency itself. eg: 0.001, 0.01, 1.00. As at Feb 6th 2015 a person will give you $223 for 1.0BTC.

6) Block & BlockChain: - All of the transactions that happen on the bitcoin network at the same time span are bundled into one chunk of data, called a block. These blocks are linked such that each new block proves that older blocks were valid; they have reference to the previous block. These linked blocks are called **BLOCK-CHAIN**.

The blockchain is a database that has records of all the transactions that ever happened in the bitcoin economy. Every bitcoin client PC has its own copy of the blockchain.

Genesis Block is the very first block that was created and the beginning of the blockchain.

7)Confirmation:- When bitcoins are sent from one address to another the transaction is broadcasted(sent out) to all other nodes directly connected to the node that performed the transaction those other nodes still broadcast what they receive and in no time everybody on the network hears about the transaction. Within each transaction that happens there is a mathematical relationship between the ID of the coins involved, the ID of the address involved, and the ID of the transaction.

All transactions that occur are bundled into a chunk of data called block and **MINERS** process each block to verify transactions by hashing to verify that a mathematical relationship exists between the coins, address and transaction that occurred.

A confirmed transaction, is simply a transaction has been put into a block and validated by the network (By Miners).

8) Miners and Mining: - Miners are people who put their computers or any other processing unit like ASIC and FGPA into work to verify transactions that happen on the bitcoin network. Mining is the term used to describe what miners do because every 10 minutes a new block is created and difficult calculations are performed to verify transactions. The first transaction in a block is a special transaction that manufactures 25 bitcoins. This new 25 bitcoins belongs to the people (computers) that created the block.

Anyone on the bitcoin network can opt-in and become a miner by just grouping a set of unordered transactions it received from other nodes into a block, and broadcast the block to the network as a suggestion for the next block. It also tries to verify the transactions by verifying that the mathematical relationship that exists between the ID of the coins involved the ID of the address involved, is consistent with the ID of the previous transactions that the coin has been involved in.

Before a miner broadcast's a block, he must hash it and make sure that the output of the hash starts with a certain number of zeros.

9) FPGA: - Field Programmable Gate Array, An FPGA is an integrated circuit whose function can be changed as it can be reprogrammed. FGPAs used in bitcoin mining are specifically modified to perform hash calculations and produce new bitcoins from mining.

10) GPU: - Graphical Processing Unit, a GPU (or commonly just referred to as a graphics card) was previously the dominant way of Bitcoin mining. It's far more efficient than a CPU. With the increase in the difficulty CPUs became obsolete for mining but it has recently become inefficient too. FGPAs and ASIC chips are used.

11) Hash (Rate):- is simply the speed at which a processor can perform hashing but as it relates to Bitcoin, the Hash Rate is the speed at which a processing unit is completing an operation in the Bitcoin code. Example-1H/s means the processor performs one hash in one second 1KH/s means the processor performs 1000 hashes in one second, 1 MH/s means that the processor performs 1,000,000 hashes in one second.

Five Common Bitcoin Questions.

1) How do I get started?

To get started in the bitcoin economy what you need is an account number (Wallet Address). To get a bitcoin wallet address you need to download and install bitcoin client software on your PC or install Android wallet on your phone.

In order to operate a bitcoin wallet yourself you must have a significant knowledge of computers and internet however for ease and convenience, coinbase.com offers a very secure online wallet where you can just register and get a bitcoin wallet.

Registering on coinbase.com as easy as opening a Facebook account. Just register on coinbase.com and you be given a bitcoin address immediately. Think of coinbase.com as PayPal.com.

2) How do I acquire bitcoins?

You can accept Bitcoins for goods and services or seek them out via Bitcoin Exchanges; you can start mining bitcoins yourself.

Accepting bitcoins for goods and services

Do you have an existing business; well the world is now going bitcoins so your business needs to start accepting bitcoins and fortunately it is not as difficult as accepting PayPal. You can also use coinbase.com to start accepting bitcoin payments on your website. Bitpay.com as also a perfect alternative.

Buying Bitcoins on exchanges

Well if you live in the USA, coinbase is your best option although you can buy bitcoins from many other websites like CoinMama they accept **Western Union** and **Credit Card**. People in the UK can buy bitcoins from bitbargain.co.uk. BitCoin is really popular and you can buy them from anywhere really. Just make sure to trust who you are dealing with before you give your cash to get the coins transferred to your bank account.

Mining bitcoins

If you have the hardware you can acquire bitcoins by mining. You cannot mine Bitcoins with your normal PC because the network difficulty is very high, you need to use special processing units like ASIC, FPGA and High End GPU,s . There are lots of reliable mining pools out there. You can also decide to be a solominer if you have powerful enough hardware.

Some reliable mining platforms include ghash.io, bitminter.com. Some other websites like hashop.io will lend you their powerful hardware for a fee.

Earning bitcoins

There are a lot of websites that pay you in bitcoins for carrying out small tasks but seriously, a lot of them are crap. The best I can recommend for now is cointasker.com.

3) What are bitcoins worth

Bitcoins are like any other currency: they fluctuate in value relative to other currencies. The value of a bitcoin is constantly changes. There is no 'fixed' price. Usually what determines the value of bitcoins is how many people need bitcoins to how many bitcoins are available. The value of bitcoin fluctuates through supply and demand. The present worth of bitcoins can be found on Preev.com

4) How do I transfer bitcoins to my bank account?

Typically you can transfer bitcoins to your bank account with the help of an exchanger. There are exchangers in every country just do a search on Google like this **"bitcoin exchangers in "your-*country-name*"** To avoid been defrauded its best to use exchange companies not individuals.

It works like this - Transfer your bitcoins to the address (bitcoin account) of the exchanger and the exchanger will pay in the equivalent value into your bank account. Example- As at 06 Feb 2015 the value in 1.00BTC equals $223 so if you transfer 1btc to the exchanger he will transfer $223 to your bank account.

5) How difficult is it to use bitcoin

Using bitcoins is easier than using credit or debit cards and PayPal. To open an account just go to **coinbase.com, blockchain.info** or download the Android or windows app. You can make payment by simply entering the recipient's address, the payment amount, and pressing send.

You can prove that a payment was sent or received by checking http://blockchain.info/address/YOURADDRESS you will be able to see the records of the coins that were sent to or from your address.

There are Over 9,000 Places to Spend Your Bitcoins go to http://www.spendbitcoins.com

How to set-up BFGminer to begin mining bitcoins.

Typically 70% of people who mine bitcoins today do so with a mining pool and it is nearly impossible to mine bitcoins with your CPU no matter how powerful it is so for this tutorial we will assume you have an external mining device.

Before you begin

Download Latest version of BFGminer from this link 64bit here http://uploaded.net/file/vhhhezr6

Download Latest version of BFGminer from this link 32bit here http://uploaded.net/file/8p4vc4wj

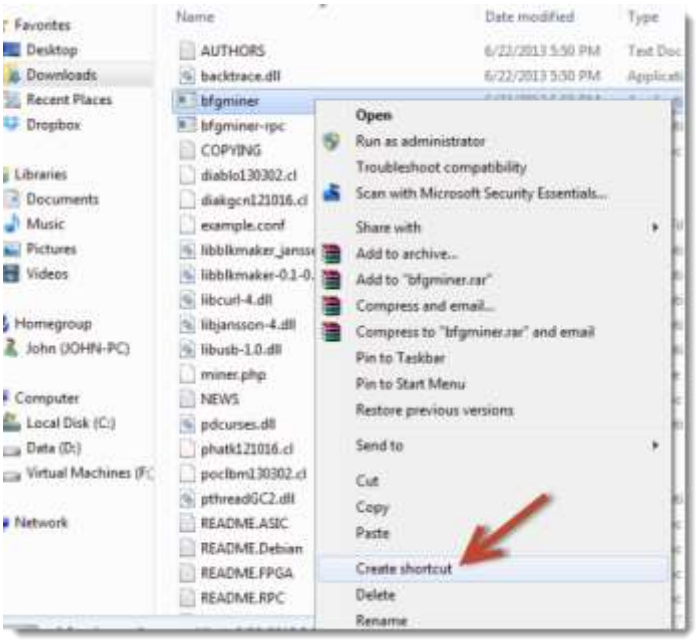
It is assumed that you should have the drivers of your external mining hardware

READY TO BEGIN

1. Plug in your USB miners to your USB port

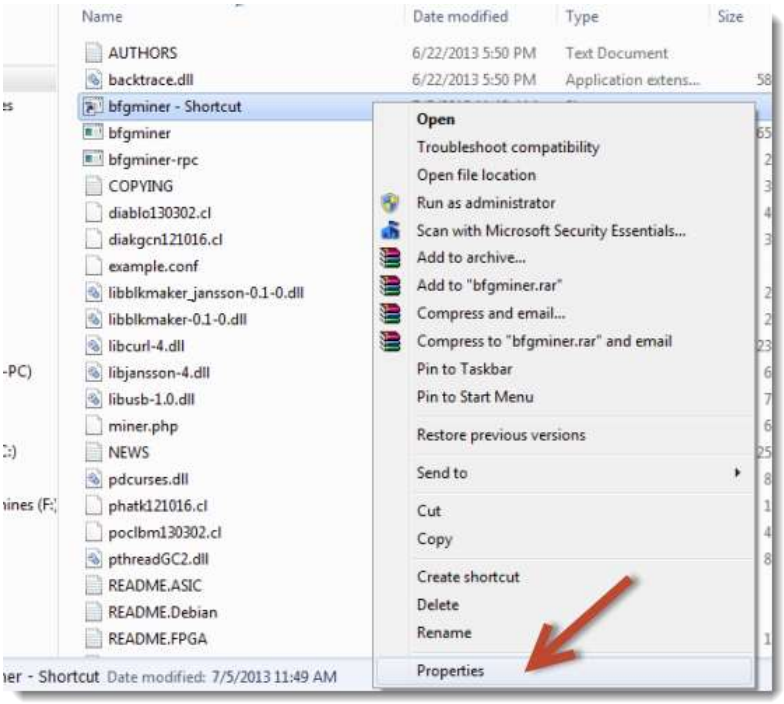
RED FURY

2. Find the folder where you save BFGMiner and unzip the file



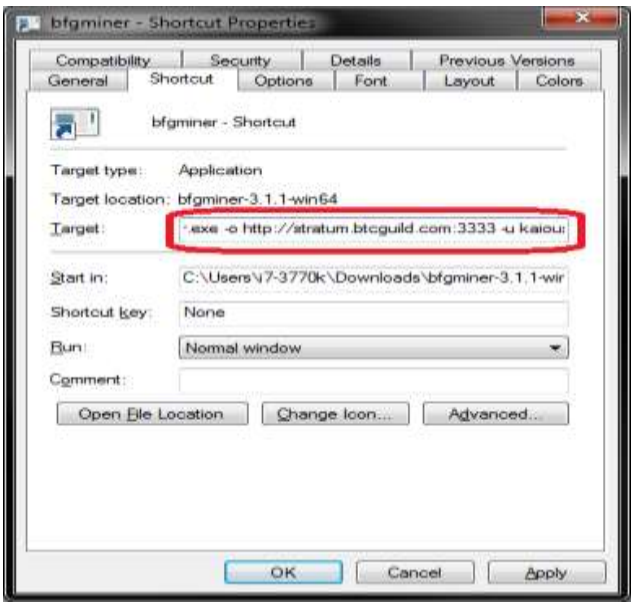
3. Right-click bfgminer.exe and Create Shortcut

4. Right click the shortcut to bfgminer-shortcut and click on Properties



6. Find the “target” box, and add the following information:

- -o YOUR POOL MINING ADDRESS
- -u YOUR USERNAME
- -p YOUR PASSWORD
- -G (if not using a graphics card on the same machine)
- -S all
- –icarus-options 115200:1:1 –icarus-timing 3.0=100



The actual values you put in should look like this

-o http://stratum.btcguild.com:3333 -u username_workername -p 123 -G -S all –icarus options 115200:1:1 --icarus-timing 3.0=100

You can then move the shortcut to your desktop for easier access. To access your BFGMiner, double click on the shortcut you made and your miner should start.

You should read though the README.TXT file that came with the BFGMiner zip file to get to know how the miner works and it's functions if you're not familiar with BFGMiner program.

PLEASE NOTE

The bitcoins are not actually stored in the address; they are still on the web. In fact, the address is just the bank account number and the private key is the bank login.

The bitcoins are not stored on your computer's hard disk or on your phone storage; the private key is stored on your computer hard disk so if your PC crashes and you know your private key maybe because you have copied it out, you have no problem you can still access your coins.

Your Bitcoins are stored on the internet inside the blockchain and every computer on the bitcoin network has a copy of the blockchain or database of records.
PrivateKeys(bank logins) are tied to every address(Bank Account Number) and the private keys now help you prove that you are the owner if the bitcoins tied to an address.

All bitcoins in the system are stored in the blockchain and a copy of the blockchain is stored on every PC on the bitcoin network.
If you install the Bitcoin PC application [Windows or Mac] your private keys are saved inside the wallet.dat file.

Creating a secure bitcoin wallet

While some people will tell you that the best place to store your bitcoins is with yourself, they say instead of using online wallets like **blockhain.info** and **coinbase.com** is best you download the bitcoin client for your PC and store your bitcoins yourself. They stated that what if one day blockcchain.info website goes down with all your coins inside your online wallet stored in their system you lose all your bitcoins.

Well, installing the PC bitcoin client and storing your bitcoins yourself is not also safer you could also loose all your bitcoins in one day.

HOW?

When you install the bitcoin client, a wallet.dat file is created and that file contains some information about your wallet; the information the wallet.dat file contains includes your private keys and remember that anyone with your private keys can steal all your bitcoins. What if your PC is hacked and the hacker gets access to your wallet.dat file and extracts your private key from it, what if a close friend or family whom you trust accesses your PC and steals your wallet.dat file. What if your hard disk crashes, what if your PC is lost or stolen. Here some people recommend copying your wallet.dat file into a flash/thumb drive and keeping the flash/thumb drive in a safe location in case your PC gets lost or stolen. You never know what if the flash/thumb drive gets damaged or missing.

There is a popular way most people recommend creating a secure bitcoin wallet that method involves installing a Linux operating system on a usb drive or hard disk to eliminate the risk of viruses and now they boot into the Linux OS and install the bitcoin client app for Linux. Any time they need to access their wallet they plug in the usb drive or hard drive into their PC, boot into linux and use it. When they are through they disconnect the flash/thumb drive and take it back to their safe secure and undisclosed location. Some even keep backups of their wallet.dat file in 3 – 4 different drives the length you go to secure your wallet depends on how much bitcoins you have to protect. This method explained above is really safe but what if there is a fire? Okay i am being ridiculous.

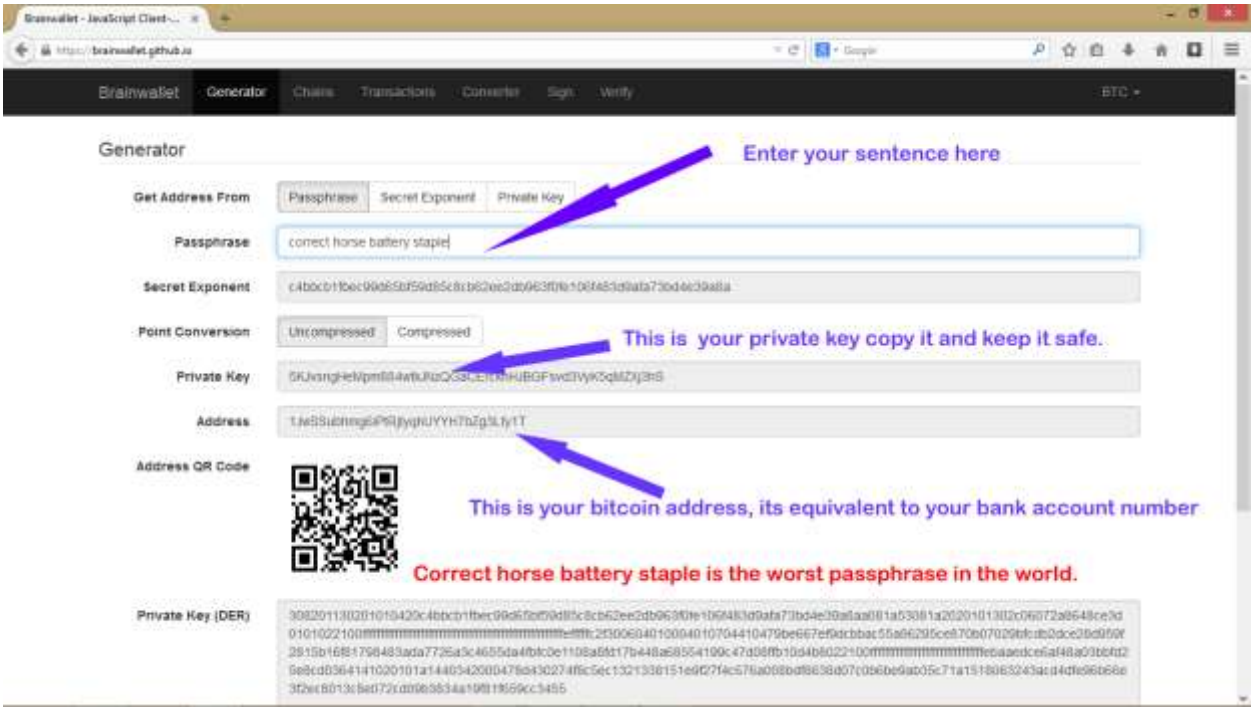
I recommend brain wallets. Wallets that is stored in your head. As at the time I wrote this article 75% of the bitcoin world is against using brain wallets to store large amounts of bitcoins because brain wallets is about thinking of a set of words and these words are run through a certain algorithm to generate your private key and wallet address. They say that if someone can guess the exact words that you used, he can generate your private key and seal all your bitcoins.

This is true and this highlights the a very big danger with brainwallets which in turn highlights' the importance of not using simple words to generate brain wallets

- ✓ Don't use words like "fuck you"
- ✓ Don't use Keyword generators as they always repeat phrases for example "correct horse battery staple"
- ✓ Think up your own words but make sure that **it is a sentence**.
- ✓ Don't use sentences' like "This is my secret brain wallet"
- ✓ You can write the names of your children together and spice It up with something at the end example ----- "AshleyTomPeytonBradley%%%China" people don't easily guess this.

How to create a Secure Bitcoin Wallet using brain wallets

1) Choose your keywords or passphrase(Use a sentence) in your mind, for example, I chose **correct horse battery staple**
   a. Go to brainwallet.github.io, https://www.bitaddress.org
2) Put in your keywords and it will calculate your PrivateKey and bitcoin address for you.



3) Give out your bitcoin address or mine into it and copy your private key and keep it safe or better still copy your keywords and keep it safe in different locations ;it will mean nothing to someone else unless you tell them that it is your brainwallet keyword.
4) Anytime you need to retrieve the private key you can simply go back to http://brainwallet.github.io and put in those keywords again.