Everything you need to know about bitcoin

2014 Extended Edition

Everything you need to know about bitcoin

INDEX

WHAT IS A BITCOIN?

Bitcoin (BTC) is a virtual currency and peer-to-peer (P2P) network that was released in 2009. It was created by someone (or some ones) who refer to themselves as Satoshi Nakamoto.

The true identity of Nakamoto is still a mystery years after the emergence of the currency. One of the strong theories is that Nakamoto is actually a group of people who have taken great strides to make sure that they remain anonymous. Anonymous and filthy rich - the amount of ***Bitcoins*** owned by Nakamoto is estimated to be worth billions of United States dollars at current exchange rates.

Bitcoin aims to remove the trusted third party from the way that we exchange money.

When swiping a run of the mill Visa card at the grocery checkout, a customer tells Visa that they want Visa to release some money to the store (minus fees). In a Bitcoin world, Visa is taken out of the equation and is replaced with a peer-to-peer secure and ***trusted network***. The customer gives the merchant the currency immediately - just like cash.

In the Bitcoin world, those transactions are logged into a database known as a block chain, which is shared across every server participating in the Bitcoin network.

While that might sound at first glance as a pie-in-the-sky solution, many merchants are jumping on the bandwagon. Everyone from mom and pop brick and mortar stores and restaurants to major retailers like ***overstock.com*** have announced plans to accept BTC in the same way that they accept Visa and Mastercard.

GEARING UP FOR VIRTUAL GOLD MINING

Those ready to buy into the gold rush will find themselves using highly specialized machines used almost solely for churning out BTC.

It wasn't always so specialized. Even in the early months of 2013, it was reasonable to use a high-end desktop system to start mining coins. While it's still possible to do that, it's no longer profitable once you remove the cost of overhead running the system for months upon months to generate a virtual sliver of a coin.

ASIC (Application-specific integrated circuit) based systems are currently at the front of the line for aspiring Bitcoin mining operations.

Many companies have made both good and bad names for themselves entering into this highly niche market. ***Butterfly Labs*** and ***KNCMiner*** Miner lead the pack with varying degrees of reviews coming in from Internet forums. A bad review usually comes from an inability to release hardware according to their pre-order promotions. The advantage to new miners is that these track records are easily accessible when making a decision to risk a pre-order purchase.

Now is the time to jump into the pre-order lines because many of these Bitcoin retailers have pre-orders for the next-best-thing in Bitcoin mining operations that are announced as being released in February or March 2014.

What new miners need in equipment will depend on a number of factors. Available power should be a primary concern as many of the units require at least 900 watts to function. Smaller systems that are on the market today may allow for less overall power, but they will also deliver less in hashing power. More hashing power means more ***money***.

The other is technical skill, specifically with computer hardware. Some units are all-in-one solutions that require only minor computer hardware knowledge.

These systems generally require a high end power supply unit of 1200 watts or greater with multiple PCI-E power connections. Other solutions require a dedicated computer along with the requisite power. With Bitcoin mining gaining popularity a quick Google search can help anyone put together a system.

But first, you'll need to choose your weapon.

KNCMiner made news after selling over ***$18,000,000*** worth of pre-orders for their latest ASIC system. ***Neptune*** is one of many all-in-one solutions that they've released over the past year. Early purchasers snagged the 3Th/s systems for ***$7,995*** and the second batches were marked up to ***$9,995.*** The company released a statement that they have sold out on all ***Neptune*** orders, but also teases that they might be releasing upgrades and more for their previous model the Jupiter (600 gh/s). ***KNCMiner's*** products have a built in web and command line interface that allows for quick and painless administration. Their manual describes in detail how to connect their systems to a power supply that must be purchased separately. Be sure to follow their recommended power guidelines for best performance.

Butterfly Labs will release their Monarch card that is said to average 600 GH/s for $2,100. These cards require an external computer and can connect either via USB 2.0 or PCI-Express slots.

Each card utilizes 2 PCI-E slots. More experienced miners or computer savvy beginners might be comforted by the extra control that ***Butterfly Labs*** provides with choices over mining software and operating systems to run the cards.

Black Arrow Software has their Prospero X-3 rack-mountable systems available for $5,949.15 and includes 5 days of free hosting with the system.

Much like the ***KNCMiner*** systems, it is a standalone unit that comes with its own web interface for configuration and reporting. These units also come with a built in power supply, which removes one element of complication from the install. The hashing power is estimated at 2 TH/s.

Many manufacturers also offer hosting services, which eliminates the concern of power and hardware maintenance costs.

The costs varies depending on the equipment and length of contract. The benefit of hosting at the manufacturer is being able to mine during what could be a lengthy shipping process. If the unit sits in a FedEx airplane for 5 days, it's not making money. The risks are, of course, leaving a brand new system in the hands of a technician in a datacenter.

Another good way of making some quick investment money is to purchase pre-orders and sell them through conventional means. As early as November, people were selling pre-orders of their ***KNCMiner*** Neptune orders on eBay for a considerable mark-up. There is risk associated with orders not coming in on time, but most listings gave sellers plenty of wiggle room in case something goes wrong with manufacturing.

A WORD ON BITCOIN DIFFICULTY

Bitcoins have a finite supply. Many years down the road, BTC will hit its predetermined cap of around 21,000,000 BTC.

As blocks are solved, the ***Bitcoin*** network rewards miners with a certain amount of Bitcoins. Today, 25 BTC is awarded per block discovered, but over time it will decline until miners do not receive rewards at all. Many years from now miners will be ***processing blocks*** for transaction fees only. But for the time being and maybe even decades, miners work together using mining pools (see helpful links for more information) to share the work and, ultimately, the loot. It's impossible to estimate exactly how and when difficulty increases, but miners can certain that the difficulty will increase over time and overall hashing power is extremely important.

The Bitcoin network by design wants to solve 1 block every 10 minutes.

The maximum amount of a difficulty increase is 4 times the current difficulty. As difficulty gets higher, miners need more hashing power to keep their share in the pool up, which in turn generates more BTC. As new equipment is released into the wild, the ***first miners*** will pull in the most Bitcoins. Equipment can become outdated almost overnight. As the difficulty increases, miners will be forced to make a decision on whether it's the power costs incurred to keep their systems running. With next-generation ASIC systems on the way (Q1 2014) difficulty is likely to continue increasing.

To calculate Bitcoin difficulty now and into the future, use this site Bitcoin Wisdom.

BUY BITCOINS

People who bought BTC a few years ago are now basking on a beach resort somewhere with an umbrella drink in hand.

Despite missing the boat on the first $1,000 USD valuation of BTC in November, there's still money to be made hoarding BTC.

The value of Bitcoins is constantly changing. The highest point was followed by a consider drop when the Chinese government caused major confusion in their efforts to stymie Bitcoin growth. They announced that they do not want financial institutions dealing with Bitcoins. That announcement meant that people in China can own and ***trade Bitcoin***, but they can't involve the exchanges that other countries can use to transfer BTC to other currencies, like the yuan. Without exchanges, they are limited to small one-on-one type exchanges. That resulted in the largest exchange BTC China being crippled and losing reportedly at least two payment processors. The big news caused the value of the BTC to drop almost $400.

It's not clear whether the Chinese government will make revisions to their decision, but Zennon Kapron of financial advisory firm Kapronasia Shanghai told Forbes that an upcoming deadline might spell out in better detail what the Chinese government is planning.

He said, what is also confusing is that the regulators have said that ***exchanges*** can exist, yet they are cutting off the means for exchange funding and withdrawing, so they are sending very mixed signals. I believe we will see some additional comments from regulators by the end of the year.The Chinese New Year is January 31, 2014.

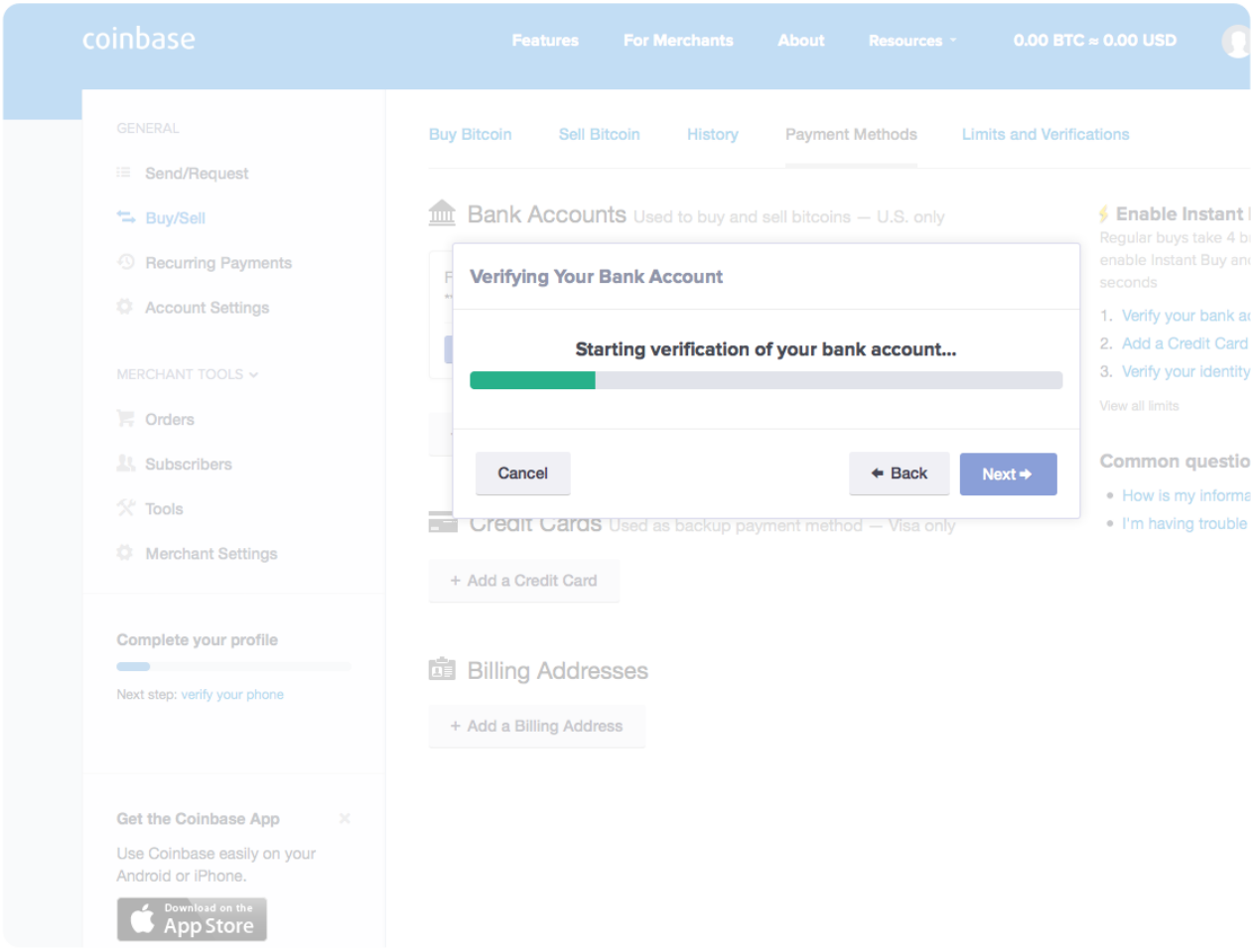
If the value drops so much overnight, why is investing in it even viable? One thing to keep in mind is that the value of BTC was just $13.51 on January 1, 2013.

The value today hovers somewhere around $850-$1,000. Most miners expect the value to go up and down, but estimates of the potential value of a Bitcoin seem to indicate that value will go up with difficulty increases.

To buy Bitcoins, you'll need a service like Coinbase to transfer from your currency to BTC.

Working with ***Coinbase***is incredibly simple. Sign up for an account using an email address and password. Then simply link your bank account and a credit card account if you want to have instant buy access. Otherwise wait for a bank transfer to go through for your BTC purchase. There are limitations in place on the account, but it's enough to get started almost instantly. To avoid some of those limitations or to avoid using your bank account at all, take a look at ***Coinmama*** for credit card transfers using Western Union and Money Gram.

Remember to protect your account with two factor authentication. The average smartphone will be able to handle the heavy lifting for the task.



WHAT'S IN YOUR VIRTUAL WALLET?

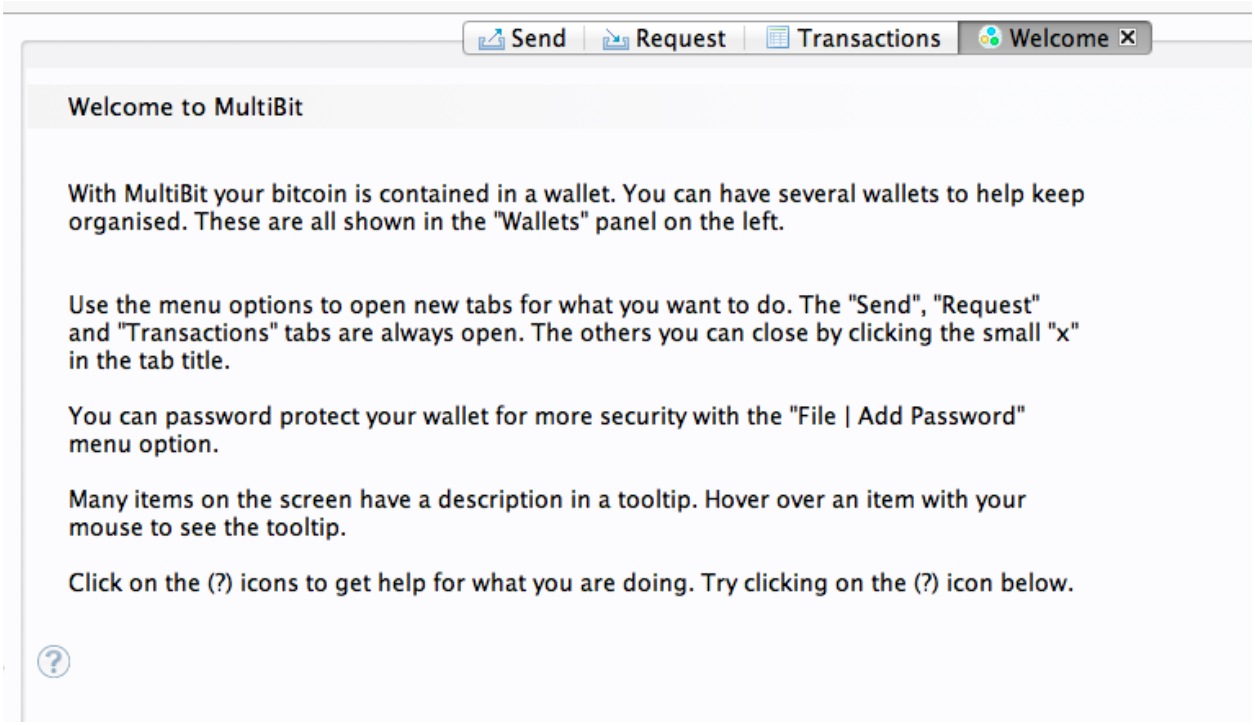
Bitcoins are stored in a virtual wallet, which is exactly how it sounds.

Services like ***Coinbase*** provides you with a web-based wallet, but when dealing with serious amounts of Bitcoin (more than 5) a real wallet is a requirement. Big investors will want locally stored private keys, paper back ups and quick syncs to the blockchain.

There are many multi-platform wallets available for free and most are even open source. The top recommended programs are Multibit and Electrum.

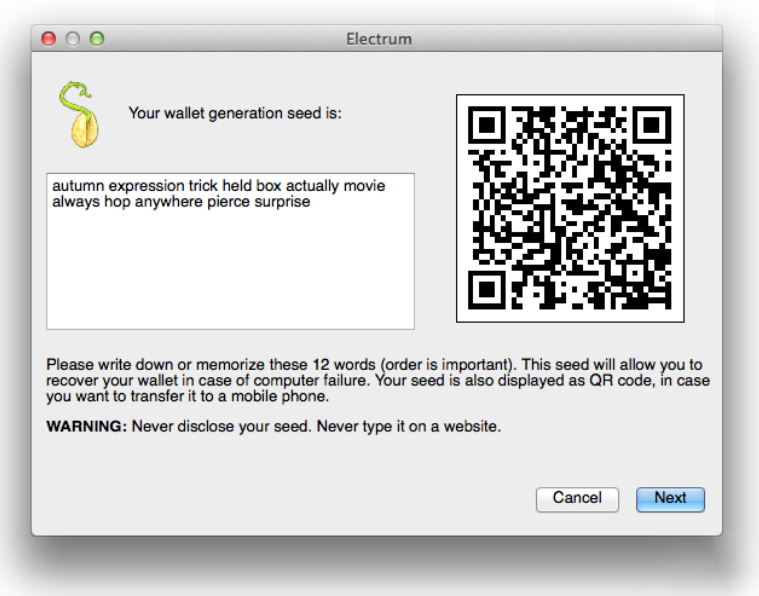
Multibit is extremely simple to get started with, but is lacking in user interface design.

What you get is a light-weight, open source wallet that will work on your PC (either Windows or Linux) or on your Mac. It's donationware and they'd like you to transfer 0.01 BTC for use of the software. It's acceptable for casual use, but beware of your backups as they can be unencrypted.



Electrum has the same base features as Multibit but comes with additional security to prevent air gaps and also the ability to store your wallet in paper form.

This is a good choice for cold storage, which means that your Bitcoins are stored either offline, on a USB drive, or encrypted to prevent quick access to the coins. For example after amassing coins, some miners have printed paper backups of their wallet and stored the wallet in a safety deposit box. With extra security and features comes extra complexity, but once the *Bitcoin* riches start flowing, it'll be worth the learning curve.



Wallet files are good targets for viruses or trojans. It's important to keep your computer safe from any outsiders that could steal your coins with a few keystrokes.

Windows users can install *KeyScrambler*, which is a good (and free) option to protect against *keylogging*. There is also a browser plug-in available for Firefox on all platforms.

See the helpful links section for more information on other wallet services.

BUY POWER TO MAKE MONEY

A relative newcomer in the Bitcoin world is cloud hashing. Members of these services purchase overall hashing power instead of purchasing hardware.

Many miners struggle to make the math work out in their favor, instead preferring to go the route of mining on their own. But some miners looking to spend hundreds of dollars instead of thousands of dollars find the low cost entry into the market appealing. Services like *CEX.IO* offer users the ability to purchase and trade hashing power. With some speculating, good traders can make a profit in the volatile market.

For even less involvement, miners can purchase equipment from co-ops like dzminercoop.comor purchasing mining contracts from places like cloudhashing.com.

Be aware of growing difficulty within the blocks when committing to long periods of time with low hash rates. 50 GH/s might be worth it today, but it's unlikely that it will be worth anything six months from now.

TURN YOUR BUSINESS IDEA INTO A BITCOIN MACHINE

Many businesses are turning toward digital currency to reach a new, unique market.

As others are investing their hard earned cash into mining technology, day trading, or ***trading for Bitcoins***, they will need a place to spend them. Mom and pop shops, both brick and mortar and online, have led the way for accepting Bitcoins in trade for their products and services.

One easy way to start a Bitcoin-based business is joining an affiliate program like The ***Bitcoin Affiliates*** and promote merchants who accept BTC for payment.

HOW BUSINESSES ARE USING BITCOINS

- ***Shopify*** announced in November 2013 that it would allow all merchant's using their pre-built service the ability to accept BTC in the same way that they integrate with credit card processors. With that one conversion, the Bitcoin market gained 75,000 retail shops.

- ***Overstock.com*** CEO and Chairman Patrick Byrne announced late December 2013 that his company would accept Bitcoins for purchases in 2014.

- Dating site ***OKCupid.com*** accepts Bitcoins for their premium subscription service

- Billionaire founder of Virgin Group Richard Branson announced that Virgin Galactic would let would-be space tourists pay for their flights using digital currency

- ***foodler.com*** allows users to have food delivered using BTC

After you've got your business online and accepting Bitcoins, head over to ***Reddit*** and get some free advertising with an announcement on ***http://reddit.com/r/bitcoin***.

GETTING IN AT THE GROUND LEVEL

The rising difficulty of Bitcoins and the specialized industry churning out ASIC machines to solve the Bitcoin puzzles are forcing the regular Joe computer user out of mining.

People interested in mining, but looking for more hobby than second career should look toward alternative coins.

Litecoin (LTC) is second only to Bitcoin in popularly and value. It uses scrypt encryption for its cryptographic puzzles.

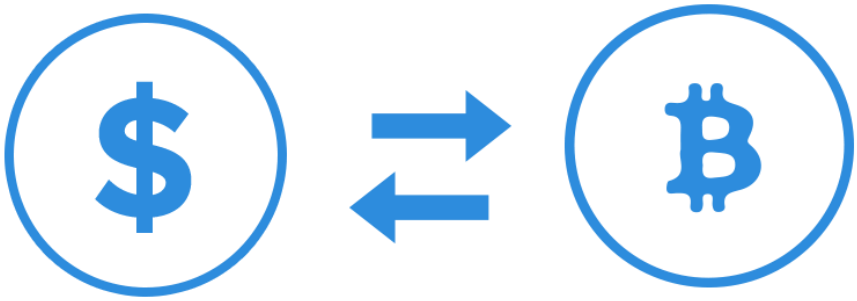
There are not specialized ASIC systems built for mining scrypt yet, so anyone with a decent video card has a good chance of making a profit mining LTC. High end systems exist using many video cards at a time can be built or purchased to handle all of the mining tasks. Miners with experience building high-end gaming or video-processing systems will have the upper hand in building a profitable rig. The more GPU (graphics processing unit) power usually means more LTC mined. It's also important to have between 4-8G of fast memory.

Quark (QRK) uses CPU mining, which means just about any computer can get involved in it.

While Bitcoin wants a 10 minute block generation, Quark's generation is 30 seconds and offers a guaranteed 1 QRK reward for each block solved.

NXT (pronounced next) calls itself a descendant of Bitcoin.

Most alternative coins use a fork of Bitcoin's source code but adjust the rules and block rewards to create a new currency. This coin takes a step away from Bitcoin and uses all new code. It's just launched in 2014 so it'd be a great time to get started on it.



HELPFUL LINKS

Wallet/ Exchange Services

CEX
Coinmama-use code 621XX276 for $7 USD discount!
Mt. Gox
Blockchain

Pools

BTCGuild
Ghash.io
Bitminter

Merchant Services

BitPay
BIPS
Bitcoin Payflow

Software

QFX Software (KeyScrambler)
Multibit
Electrum

Hardware

Butterfly Labs
KNCMiner
Black Arrow

Tech Chat/ Forums

BitcoinTalk
KNC Forums
Reddit's /r/bitcoin
StackExchange

Altcoins

Litecoin
QRK
Nextcoin
Reddit.com/r/altcoin