



Receive all Bitcoinist news in Telegram!

JOIN

▼ \$19002

▼ \$728

▼ \$1071

KNOWLEDGE BASE

What is Bitcoin?

Bitcoin is an open source, p2p form of digital currency. What exactly does that mean? With Bitcoin, we have a “people’s currency” for the first time with no government or central figure controlling things like interest rates or inflation. Bitcoin transactions can’t be reversed, so users can receive payments without having to worry about chargebacks and the fees associated with them. At the same time, this feature means that you need to be careful with your coins; if you lose them, you can’t get them back. Because Bitcoin is peer to peer, fees for transactions are extremely minimal or even free.

Bitcoin takes a deflationary model. Only 21 million bitcoins are ever going to exist. There are no replacements, so lost coins are gone forever, making the supply even more scarce. This means that bitcoins will actually increase in value over time, unlike fiat currency that lose more and more value every year.

What is Blockchain?

Arguably more important than Bitcoin is the blockchain. The blockchain is the public ledger for Bitcoin, and keeps track of every transaction made. This is publicly available, and anyone can view it.

Many things can be built on top of the Bitcoin blockchain, such as colored coins. These still have the security and basic features of Bitcoin, but they can represent



Receive all Bitcoinist news in Telegram!

JOIN

completely different things. Blockchain technology is still being explored by both software developers and entrepreneurs looking to build on the protocol and establish new products and services. Blockchain technology has the ability to shape the financial industry going forward and will pave the way for new applications which empower individual users.

Bitcoin's network is maintained in a decentralized manner, with everyone pitching in. The ability for a single entity to control the network is discouraged, with someone needing 51% or more of the mining power to attempt this. There is little to no incentive for trying to control the network due to the huge cost of attempting to stage such an attack, and the fact that there would be no benefit for the attacker.

Bitcoin is also pseudo-anonymous. Using bitcoins keeps your transactions safe as it's more difficult to track transactions going from a string of digits to a different string of digits (addresses). You can even use mixers or other services to make your transactions harder to track. Bitcoin isn't designed to be a completely anonymous technology, but rather one that empowers individuals and allows them to take control of their own finances.

Why use Bitcoin?

Bitcoin saves on fees. Merchants will sometimes pass these discounts onto their customers. One good example of this is Gyft, where you have a 3% discount when using Bitcoin to purchase gift cards.

Another excellent example of enticing customers to use Bitcoin is purse.io. Purse.io allows you to purchase anything off of Amazon, and set a discount of your choosing that is between 10% to 30%. 10% discounts on orders are guaranteed to be filled within 24 hours, and other amount discounts should be filled in relatively quickly.

You can find bitcoin accepting shops in directory sites for example here: [Find bitcoin shops, markets and links](#)

Besides saving money with merchants, sending money has never been easier. With the ability to send Bitcoin quickly and cheaply around the world, remittance services are running for their money.

Bitcoin also allows you to do many things that you couldn't do conventionally. Because of the blockchain's features, such as recording transactions permanently, you could for example sign documents proving that it is indeed yours.

You can also use multi signature wallets, with multiple people having to agree to a transaction before a transaction is made. This allows for small businesses to keep



Receive all Bitcoinist news in Telegram!

JOIN

their money more secure. Multi signature wallets are ideal for companies that store their bitcoin and want to prevent someone from stealing funds. While they are typically more clunky to use, multisig wallets offer the security needed to prevent bad actors from harming the organization.

With Bitcoin you can implement a brain wallet. A brain wallet consists of a long phrase of letters that you have memorized. With this phrase you can access your Bitcoin from anywhere. It really is quite impressive that you can store money with essentially nothing but your brain.

Many people see Bitcoin as an investment vehicle. Bitcoin is essentially a high risk-high reward investment, on a scale like no other. Bitcoin's value can fluctuate by over 30% on a daily basis, making a good target for day traders seeking a quick profit. All investing, however, involves risk.

How to Use Bitcoin?

Before you can use Bitcoin, there are two things you need. First is a wallet. A wallet is an application that runs on your computer, in the web, or on your phone. Wallets store your private keys and addresses. These are two fundamental parts of what makes a bitcoin transaction work, so make sure you have a working and up to date wallet before proceeding.

The second part you will need is bitcoin itself. There are a multitude of ways to get bitcoin, from buying them outright at exchanges to receiving them from selling goods or services.

Instead of using names for payment, addresses are used which are long chains of characters used to identify a public key that is tied to a private key used to spend funds.

Where to buy bitcoin?

Unless you have a job that pays in bitcoin, you probably have to purchase your coins. There are generally three ways to buy bitcoin. You can buy them on a bitcoin exchange, you can use a bitcoin ATM, or you can purchase them in person using a service like LocalBitcoins.

Bitcoin exchanges are the most common method of buying bitcoin. There are a lot of exchanges to choose from, but some of them are more reliable than others. Here are a few exchanges recommended by Bitcoinist:

Buy directly from the [Bitcoinist website](http://bitcoinist.com).

How to keep your bitcoin safe?



Receive all Bitcoinist news in Telegram!

JOIN

There are several ways to store your bitcoin, whether it's in a lightweight wallet for easy transactions or better wallets with advanced features and extra security.

There are even dedicated hardware wallets that sign transactions and keep your private keys secure, even on a compromised computer.

Then there are cold storage wallets, or offline wallets. These are used primarily for long-term storage, and are only brought online when you need to pull funds from them. These are normally printed out, and kept in a secure location so you can, at a later time, access the wallet.

Keeping offline on something more durable than paper is highly recommended, perhaps a laminated QR code or even a metal card. This insures accurate QR scanning and deters etching or other marks that could make reading the inscribed keys or QR codes difficult.

You can also send and receive bitcoins on a mobile device. QR codes, as well as NFC in the foreseeable future may be implemented to allow for even easier sending and receiving of Bitcoin than QR codes.

Lastly, there are online wallets. Most of them require you to trust a company because they are holding your bitcoins, with blockchain being a major exemption in that you store your private keys even though it's online. Some people see this tradeoff just fine, as you're able to access your wallet anywhere, assuming you have an internet connection. Some people don't however, and believe trusting other people is against the principle of decentralization and what Bitcoin stands for. In the end, it's all about what you value more. Convenience or security.

There is a difference between a hot wallet and online wallet, while online hosted wallets require trust in a third party, hot wallets can be user controlled yet the wallet is still actively connected to the network and ready to send Bitcoin on a moment's notice.

What is 2FA?

2FA, or Two-factor Authentication, is a popular option for securing sensitive information. 2FA was originally created for use outside of cryptocurrency, and has recently been adopted by cryptocurrency services.

2FA adds a second layer of security to online accounts, making users prove that they are the real owners of the accounts they are trying to access. With 2FA, a second



Receive all Bitcoinist news in Telegram!

JOIN

password or one-time code is used. This 2FA code is usually sent via SMS, email, or mobile app.

For 2FA to be effective, your cell phone should also be encrypted. This ensures that even if hackers obtain your password, they would have to physically steal and access your cell phone as well to get into your account.

Many exchanges and mining pools use 2FA — and they should. Security and privacy are two factors which must be balanced by companies to meet consumer demands.

Security doesn't stop at 2 factors of authentication. It's possible to add extra factors of security, whether that's using many people in implementations like multi signature wallets, or biometric features such as fingerprint scanners. The possibilities are endless, and each consecutive factor increases security.

There are many phone apps that allow you to easily enable 2FA on supported accounts. The process is usually done by enabling 2FA, scanning the QR code, and then finally confirming the code.

After it's setup, you will have to enter a code that the app provides every time you login to your account. This is an excellent deterrent against hackers and other infiltrators trying to access your sensitive information. The extra 15 seconds or so to check your phone for the code is definitely worth the added peace of mind 2FA can offer.

How to calculate mining profitability?

The easiest way to calculate mining profitability is with a mining calculator. Calculators include several factors; a good mining calculator should have the ability to input power rates, power usage, hash rates, difficulty increments, price of hardware, and price of Bitcoin just to name a couple.

Another easy way to calculate if mining is profitable is asking one simple question. Let say for example that you have \$X. With \$X you can buy Y BTC.

To calculate if it's profitable to mine instead of buying, you have to ask yourself if XXX mining hardware can generate more BTC than it costs to purchase the hardware. If not, then mining is not profitable and it would be better to buy Y Bitcoin instead of purchasing hardware.

To even have a slight chance in making profit as a miner now, joining a multipool is almost a requirement. A multipool is a mining pool that mines the profitable coins



Receive all Bitcoinist news in Telegram!

JOIN

based on difficulty, selling price, etc. and then dumps xxxx coin in exchange for payouts in BTC

If you are mining for profit, a key element of making a profit is reselling. If you can resell your mining hardware at the right time, you only have to make partial ROI from mining, and let the reselling take care of the rest.

Another easy way to make profit from mining is renting your miner out to people. People are willing to pay a premium for not having to pay electricity or put up with the noise and heat outputted from a miner, so it's easy to make a profit from here.

How to understand bitcoin price charts?

Speculating on Bitcoin's price through trend analysis is very risky, and no trader will be right 100% of the time. As a general rule of investing, only invest what you can afford to lose and never put all of your eggs into one basket.

Bitcoin price charts are commonly portrayed as either a simple line graph or as a candlestick model. While the line graph presents information simply and quickly, the candlestick chart is the preferred infographic of Bitcoin traders.

When reading a simple line chart, match the time on the X-axis with the value on the Y-axis. Line charts show accurate price information over time in a way that is simple to read.

Candlestick charts use a more complicated method of presenting data. The green candle is called a bullish candle, meaning the value of the asset increased throughout the trading day, and the red candle is a bearish candle, meaning the value of Bitcoin decreased throughout the session. The open price is the price the asset traded for at the start of the trading session, and the close price is the price in which the asset was traded for at the end of the session. The open and close are presented by the colored rectangle in the candlestick icon on the chart. The high and low prices on the chart are marked by the vertical lines that project from the rectangle on the graph. The spread is the difference between the high and low prices. Skilled traders can buy at the low price and sell at the high price or close to it if the margin remains close in scope, this is one of the primary methods of profiting from Bitcoin and is known as day trading. Like all investing methods, day trading involves risk of loss, so only trade what you can afford to lose.

When you get into Bitcoin, you will eventually look at how Bitcoin is doing market-wise — and you might even keep track of other cryptocurrencies. There are several tools that are in every trader's arsenal.



Receive all Bitcoinist news in Telegram!

JOIN

A good place to start looking is at market capitalizations, which is found by multiplying the price of each coin by its total supply. A good website for just doing this is <http://coinmarketcap.com/>. Besides showing market capitalizations, it also shows volume in USD of the last 24 hours, as well as 7 day graphs showing how the coin has been trending, whether positively or negatively.

If you click on the coin's name, it will link to a block explorer, discussion thread, and a website. It also shows more in depth graphs, up to 30 days out.

There are typically two kind of graphs that you will come across, a normal price graph and a candlestick graph. While a price graph is simpler, many traders prefer the candlestick graph as it shows more information.

Below is an example of a candlestick graph. Each candlestick is either green or red, with green indicating upward market movement and red indicating downward movement trends otherwise known as bullish and bearish respectively. Each individual candlestick also shows the lowest, median, and highest price within a time period compared to a regular price graph just showing the closing price.

Above is an example of a regular price graph that shows the closing price of the specific time period. While it's not detailed enough for most traders' analyses, it does show a trend and where a coin is heading. For example, this is a graph of Bitcoin over the last 2 months. While you couldn't make some day trading predictions, even a casual glance could accurately state that Bitcoin has been on a downward trend over the last couple of months, but that's about as much as you can deduce.

What does zero confirmation transaction mean?

A zero confirmation transaction is when a company or a merchant accepts a bitcoin transaction when it gets broadcasted to the network instead of when it is confirmed.

Some companies already allow instant transactions for their customers and increase the spending utility of Bitcoin for customers looking to shop in brick and mortar stores.

Exchanges benefit from instant transactions as traders are able to move more volume in less time and quickly trade at the price they want.

Instant transaction acceptance gives more utility to shoppers at an increased risk of fraudulent transactions. Some people may be concerned with this method as it's technically less secure and could be susceptible to 51% attacks, but with Bitcoins network hashrate, a 51% attack is highly unlikely.



Receive all Bitcoinist news in Telegram!

Since there are no chargebacks in Bitcoin, it is relatively safe to accept zero confirmation transactions, but if you want to be extra cautious, wait for the first confirmation for added security.

▼ \$19002

▼ \$728

▼ \$1071

If you don't want to wait that long, waiting a couple seconds for the transaction to broadcast to several nodes will also increase security. The more nodes that accept the transaction as legitimate, the less likely that it's a double spending attempt.

JOIN

ADVERTISING



FOLLOW US



18.3K

LIKE



27.9K

FOLLOWER



209

FOLLOWER

ADVERTISING



**NEWSLETTER SUBSCRIBE**

Receive all Bitcoinist news in Telegram!

JOIN

▼ \$19002 ▼ \$728 ▼ \$1071
For updates and exclusive offers
enter your email below.

SUBSCRIBE**ADVERTISING**

aventus

**The Smarter Way
To Buy & Sell
Tickets**

FOLLOW US HERE



.COM



Receive all Bitcoinist news in Telegram!

[ABOUT US](#)

JOIN

[CONTACT US](#)

▼ \$19002

▼ \$728

▼ \$1071

[EDITORIAL POLICY](#)

[SITEMAP](#)

[JOBS](#)

[FORUM](#)

[ADVERTISE](#)



© 2017 Bitcoinist.com. All Rights Reserved.