

# WHAT IS **BITCOIN?**

THE BEGINNER'S GUIDE TO CRYPTOCURRENCY

by Gavin Phillips



# What Is Bitcoin?

# The Beginner's

# Guide to

# Cryptocurrency

Written by Gavin Philips

Published May 2018.

Read the original article here: <https://www.makeuseof.com/tag/bitcoin-cryptocurrency-guide/>

This ebook is the intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this ebook is prohibited without permission from [MakeUseOf.com](https://www.makeuseof.com).

# Table of contents

<b>1. What Is Bitcoin?</b>	<b>4</b>
1.1 Who Uses Bitcoin?	4
1.2 Using Bitcoin: Pros and Cons	5
1.3 What Is the Blockchain?	6
1.4 What Is Bitcoin Mining?	8
Bitcoin Mining Difficulty	9
1.5 What Is a Bitcoin Fork?	9
<b>2. How to Buy Bitcoin</b>	<b>10</b>
2.1 Where to Buy Bitcoin?	10
Coinbase	10
LocalBitcoins	10
Gemini	11
Other Options for Buying Bitcoin	11
2.2 Bitcoin Wallet Types	11
2.3 Bitcoin Wallet Guide: Electrum	12
2.4 How to Receive Bitcoin	13
2.5 How to Send Bitcoin	14
<b>3. How to Mine Bitcoin</b>	<b>15</b>
3.1 Hardware for Mining Bitcoin	15
3.2 Bitcoin Mining Profit Calculator	15
3.3 Bitcoin Mining Pools	16
3.4 Solo Mining Bitcoin	17
<b>4. The Future of Bitcoin</b>	<b>17</b>
4.1 Bitcoin Power Consumption	18
4.2 Bitcoin “Layer 2” Protocol	19
4.3 Bitcoin Price Volatility	19
<b>That’s Everything You Need to Know About Bitcoin</b>	<b>20</b>



Bitcoin is global. During 2017, the price of a single Bitcoin rocketed from \$963 to over \$19,000. Then, as quickly as it rose, the price plummeted to less than half of that.

**Bitcoin's immense value has some people perplexed.** How is an entirely digital currency worth more than an ounce of gold? Moreover, why is there so much interest in Bitcoin?

This guide will hold your hand as you **enter the world of Bitcoin and cryptocurrencies**. Want to know what mining is? Don't understand what a wallet is? Unsure if Bitcoin is right for you? Here's everything you need to know in one convenient article.

## 1. What Is Bitcoin?

Bitcoin is a distributed digital cryptocurrency. Unlike regular fiat currency, there is no central Bitcoin bank to print and regulate the flow of currency. Bitcoin is held by users linked together by a central ledger. The ledger is a **core Bitcoin feature known as the blockchain**. The blockchain records every single transaction made using Bitcoin, validating transactions and ensuring the integrity of the network.

The idea of a distributed digital currency isn't especially new. Bitcoin concepts were discussed in cypherpunk mailing lists long ago. Then in 2009, **mysterious programmer Satoshi Nakamoto** built the peer-to-peer distributed network, making it available to the world. **Initial uptake was slow**. The first Bitcoin transaction was for two pizzas costing 10,000 BTC (a cool \$190,000,000 at the high point of 2017).

Bitcoin has since morphed from a fledgling digital currency into an asset or commodity. In fact, Bitcoin somewhat straddles the median. Its use as a currency is limited, it is too volatile to be considered a solid asset, and it is traded similarly to regular stocks and shares.

Bitcoins trade in decimal places. That means you do not have to buy an entire Bitcoin to start using the cryptocurrency. With prices for an individual Bitcoin at times reaching into the tens of thousands of dollars, there are not many who can afford to buy outright. Instead, budding users buy part of a Bitcoin.

For example, you have \$1,000 and want to buy some Bitcoin. **At the time of writing, \$1,000 nets you 0.11 BTC**. If the price of Bitcoin rises, so does the amount you have, and vice-versa when it falls.

### 1.1 Who Uses Bitcoin?

Bitcoin is a currency. Some owners use Bitcoin to pay for services. There are a number of online services that accept Bitcoin (and other cryptocurrencies) in place of regular cash. While Bitcoin started small, **some major retailers and international companies now accept it** as payment, including Microsoft, Expedia, Newegg, Overstock, and UK company CeX. Furthermore, a vast number of VPN and hosting sites accept Bitcoin.

Bitcoin has also seen heavy uptake on the so-called darknet. Because Bitcoin is decentralized and with a little effort is also fairly anonymous, some nefarious sites use the cryptocurrency instead of fiat currency. The anonymity and decentralization mean Bitcoin is ideal for places where regular banking is an issue.



For instance, during civil unrest throughout Venezuela, citizens turned to Bitcoin as their regular currency devalued because of massive inflation. Similarly, some African nations use Bitcoin instead of local currency because of the uncertainty in price, while Bitcoin is by-and-large pegged to the US dollar.

**The real answer is that anyone who wants to use Bitcoin can. They just need to buy some first.**

## 1.2 Using Bitcoin: Pros and Cons

As with most pieces of technology, there are pros and cons to using Bitcoin. I'm going to list a few of each, with some short explanations as to my reasoning.

### Pros to Using Bitcoin

- **Freedom:** Users can send and receive Bitcoin anywhere in the world, irrespective of local currency.
- **Decentralized:** There is no central bank to control new Bitcoin. As we'll explore in a moment, users mine new Bitcoin using computers, meaning the users are in control of the network.
- **Transparent:** The blockchain ledger underpinning Bitcoin is available **to anyone who wishes to download it**; it currently stands at over 145GB. There are, however, numerous sites that allow us to double-check transactions, while personal information remains hidden.
- **Privacy:** While there are ways to trace Bitcoin transactions back to their source, Bitcoin is largely anonymous. In addition to privacy, Bitcoin transactions protect against identity theft and credit/debit card fraud by using only digital wallet IDs, never your actual details.
- **Supply:** There is a finite supply of Bitcoin; only 21 million Bitcoin will ever exist. Several million are already presumed irretrievably lost, increasing demand for the rest. Meanwhile, Bitcoin is the baseline almost all other cryptocurrencies measure against.
- **Protection:** Unlike regular currency, you cannot counterfeit Bitcoin. Sure, there are scams out there to steal Bitcoins, and unscrupulous individuals will try and sell fake Bitcoin, but you cannot actually fake a Bitcoin.

### Cons to Using Bitcoin

- **Fees:** In the early days, Bitcoin transaction fees were minimal. In December 2017, the average transaction fee peaked at \$55, up from November's high of \$19. Fees could continue to rise, too. While \$55 is extremely high and likely involved a large sum of Bitcoin, many balk at general fees.
- **Instability:** Price instability makes Bitcoin difficult to use as currency. Many vendors are unwilling to risk their incoming payments decreasing in value by the time it processes. Unlike a regular U.S. dollar, the value of your Bitcoin could disappear overnight, leaving you with nothing (jibes at centralized currency, quantitative easing, and inflation aside).



- **Refunds:** One of the positives of Bitcoin is payment privacy. Unfortunately, it is also a downside. If you send money to the wrong Bitcoin address, there is no way to claim it back. Similarly, if you purchase something using Bitcoin and it never arrives, there is no charge-back function.
- **Competition:** Some argue that competition is healthy for the cryptocurrency markets, and I agree. Bitcoin holds the most value and is still the most attractive investment opportunity, but other cryptocurrencies offer more in terms of privacy, security, and functionality. They cost less, and could eventually overtake Bitcoin.
- **Unregulated:** Similar to the lack of refunds, **some Bitcoin-related scams** are essentially impossible to recover from. Law enforcement can do nothing once your coins are gone, other than commiserating and filing a report.
- **Loss:** It is possible to irretrievably lose Bitcoins, be that through destruction, encryption, or similar.
- **Uptake:** For most of the reasons above, Bitcoin has low uptake among businesses, and will continue to struggle for many years. In conjunction, Bitcoin is slow to process payments, processing a theoretical maximum of seven transactions per second (compared to regular banking systems like Visa that processes thousands every second).

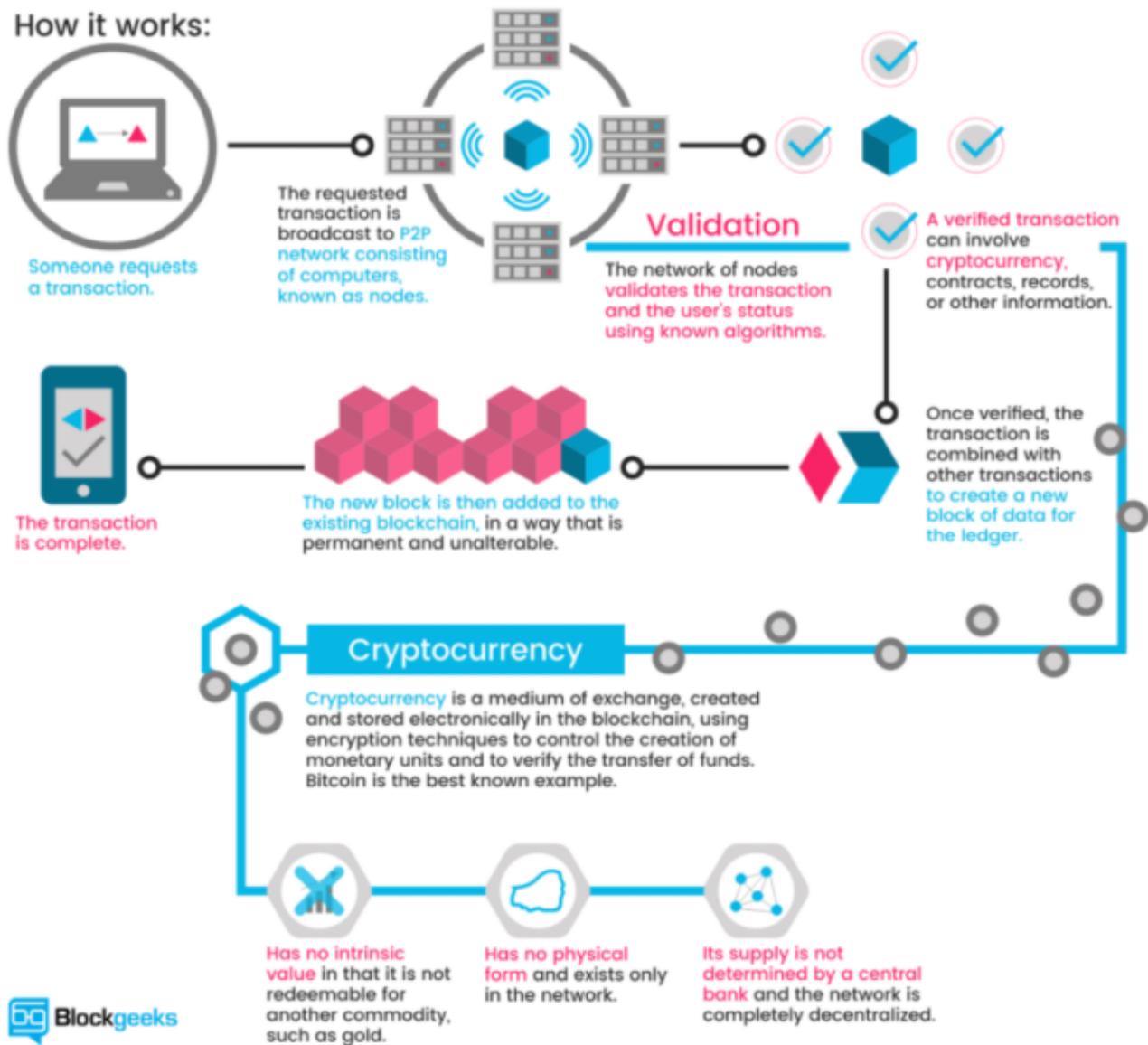
### 1.3 What Is the Blockchain?

The blockchain is the revolutionary technology behind Bitcoin and other cryptocurrencies. The Bitcoin blockchain contains details of every Bitcoin transaction, past and present, recording them as they take place. So how does it work?

Let's use an example. You want to send Bitcoin to your friend. When you hit the Send button, your transaction is added to a block.

When your block amasses enough transactions, it broadcasts to every connected node in the network. The nodes "mine" the block, verifying the transactions (as well as collecting transactions fees for their troubles). Once verified, the block adds to the chain, and your funds arrive with the recipient.

## How it works:

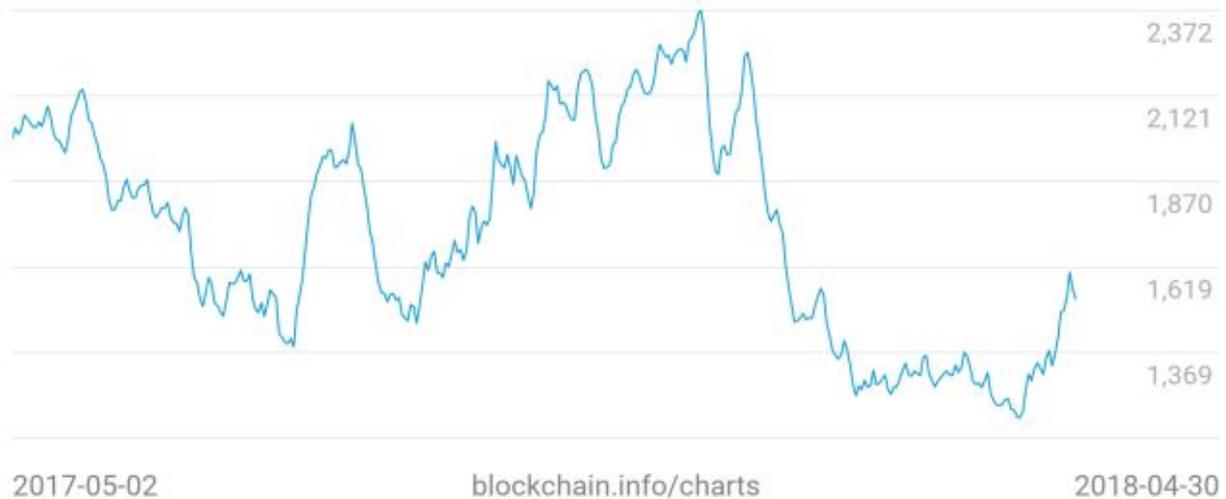


Digital currency is simply data. It is ones and zeroes. One major problem for digital currencies is double spend. That is, users attempting to dupe vendors by spending the same digital currency in two locations. Blockchain technology stops that issue by requiring that the network verifies every transaction.

Once a majority of nodes confirm that the transactions in the block are unique, it is added to the blockchain. Each new block is linked to the previous to ensure a chain of accepted transaction history, thus protecting the network, users, and vendors alike. But the nodes aren't just doing this out of the goodness of their hearts. No, there is a financial incentive to for nodes to verify the blocks.

## Average Number Of Transactions Per Block

# 1,525



Each block carries a reward. The current block reward is 12.5 BTC. In 2020, the reward will halve, dropping to 6.25 BTC. Approximately five years after that, it will halve again, to 3.125 BTC. The halving process will continue until the year 2140 when, by most estimates, the Bitcoin mining process will complete.

### 1.4 What Is Bitcoin Mining?

Mining is another way of referring to, and is intrinsic to, the block verification process. Every ten minutes or so, a block containing pending Bitcoin transactions releases to the network. The block can contain thousands of individual transactions. Miners compete to verify the transactions contained in the block.

While some people say miners “solve difficult mathematical equations,” that isn’t strictly true. Transactions are verified by matching a 64-digit hexadecimal hash. The first miner to match a hash and verify 1MB of transactions is eligible for the aforementioned block reward. This system is known as **proof of work** and, unfortunately for the vast majority of individuals, means it is simply impossible to solo mine Bitcoin.

But why?

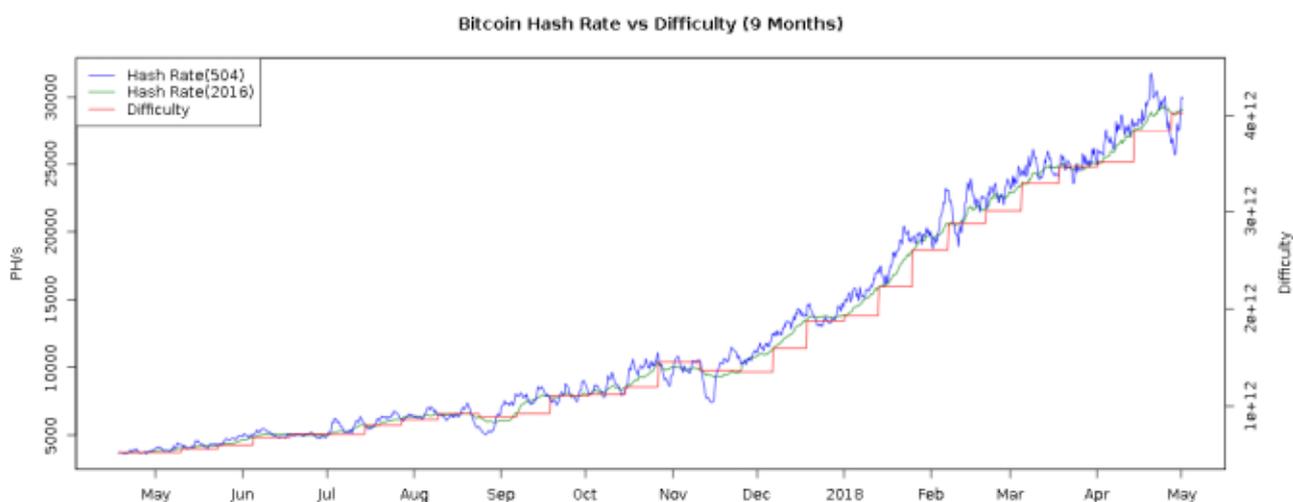
Well, it takes a staggering amount of computing power to generate hashes at a high rate. To mine successfully, you need a high hash rate, in turn requiring a huge amount of electricity. This is why there are **concerns about the overall power consumption of Bitcoin** and other cryptocurrencies. Hash rates are measured in megahashes per second (MH/s), gigahashes per second (GH/s), and terahashes per second (TH/s).

In the early days of Bitcoin, it was possible to mine using a regular CPU. Now Bitcoin mining requires specialized hardware: either high-spec GPUs contributing to a mining pool (more on this later) or an ASIC miner.

## Bitcoin Mining Difficulty

To stick to the mining algorithm and block halving timeframe, the Bitcoin network aims to release a new block every ten minutes. But if there are more miners, there is a higher chance of someone matching the correct hash in a shorter timeframe. That's where mining difficulty comes into play.

As the total hash rate power increases, so does the difficulty level of the mining process. After every 2016 blocks, the network difficulty changes. If the block discovery time is less than 10 minutes and the hash rate high, the difficulty level increases. If the block discovery process takes longer than 10 minutes, the same protocol decreases difficulty.



## 1.5 What Is a Bitcoin Fork?

Another common Bitcoin term is **fork**. Unlike the fork you eat with, **a cryptocurrency fork is more akin to a fork in the road**. Bitcoin (and other cryptocurrency) forks take place for many reasons, but usually boil down to:

- Differing ideals and approaches to the original coin implementation
- A major issue or security fault with the technology behind the coin

Forks are also soft or hard. A hard fork typically introduces a radical change to the existing protocol, usually creating an entirely new cryptocurrency in the process. Some major hard fork examples include:

- **Bitcoin XT:** One of the first notable hard forks, Bitcoin XT aimed to boost the Bitcoin network to 24 transactions per second by increasing the block size from 1MB to 8MB.
- **SegWit: Segregated Witness** reduces the size of each Bitcoin transaction, in turn allowing more transactions per block, which allows for faster and cheaper transactions. Technically a soft fork, SegWit mobilized other developers to complete their own hard forks.
- **Bitcoin Cash:** One of the most controversial hard forks, Bitcoin Cash split from the “main” branch to protect against future changes. (Indeed, Bitcoin Cash is undergoing its own hard fork in 2018.)
- **Bitcoin Gold:** Aimed to restore mining functionality to GPUs rather than specialized mining equipment.



Certain forks have seen the price of a single Bitcoin surge as investors and speculators pile in. Newly created Bitcoin-based currencies have no set initial value, either.

## 2. How to Buy Bitcoin

So now that you know the basics of Bitcoin, it is time to buy some.

### 2.1 Where to Buy Bitcoin?

There are several trusted and secure places to buy Bitcoin. There are also a vast number of places that are not trusted and are thoroughly insecure. Here are the three most secure places to purchase your first Bitcoin.

#### **Coinbase**

Coinbase is one of the biggest Bitcoin currency exchanges. It brokers the exchange of the fiat currencies of 32 countries into Bitcoin, (as well as Bitcoin Cash, Ethereum, and Litecoin). In November 2017, Coinbase reported some 13 million active users. However, this was before the price of Bitcoin soared in December, allegedly adding up to 300,000 users per day at its peak.

User numbers aside, Coinbase makes purchasing Bitcoin extremely easy. All you need is your bank account details and an account. Coinbase understandably restricts initial purchase limits until the user verifies their account using a phone number or photo identification.

Coinbase transactions are, for the most part, extremely fast. In the US and some EU countries transactions using debit or credit cards process immediately, and you'll receive your Bitcoin instantaneously.

#### **LocalBitcoins**

LocalBitcoins is a site of peer-to-peer Bitcoin vendors, spread throughout the world. Unlike the majority of other Bitcoin/fiat currency exchanges, LocalBitcoins is decentralized, like the currency itself. Prices change as the market fluctuates, and sometimes there is a chance to buy Bitcoin at slightly lower prices than usual.

The biggest bonus to LocalBitcoins is the range of available payment methods. Most other sites restrict payments to verified bank accounts and credit cards. LocalBitcoins allows payment using Amazon gift card codes, Western Union, PayPal, cash in person, Google Wallet, and more—so long as the seller has the option listed. LocalBitcoins is currently active in 249 countries around the globe.

In addition, you need very little personal information to purchase Bitcoin using LocalBitcoins. The website doesn't demand heaps of information and, depending on your payment choice, only the vendor will see your account details.

## Gemini

Gemini is one of the most secure fiat-to-cryptocurrency exchanges available to those new to Bitcoin. One of the biggest positives to using Gemini is the FDIC-insured deposit scheme. Furthermore, Gemini is licensed and registered in New York and is operated by Bitcoin billionaires Tyler and Cameron Winklevoss (AKA the Winklevoss twins).

Gemini is well-respected throughout the crypto world. Aside from offering insured holdings, digital assets are put into cold storage to maintain security and, unlike many other large exchanges, Gemini actually has decent customer support. Better still, if your order is big enough, Gemini will offer a price discount.

## Other Options for Buying Bitcoin

These three are by no means the only fiat-to-Bitcoin exchanges. Here are a few more you might consider:

- **Bitstamp**
- **Bisq**
- **Coinmama**

## 2.2 Bitcoin Wallet Types

The next step is to grab a Bitcoin wallet. Just like your regular currency, Bitcoin needs a wallet. This is, however, a digital wallet accessible through your computer. There are several cryptocurrency wallets out there. Wallets are also hot, cold, software, or hardware.

Sound confusing? Don't worry, I'm going to quickly explain what all this means:

- **Hot wallet:** A hot wallet is considered one connected to the internet. The Coinbase scenario above uses a hot wallet. If you keep your Bitcoin on the exchange where you bought it, you're using a hot wallet. A hot wallet is extremely useful for making quick payments, trading on crypto-exchanges, and so on. **Online web wallets** are also considered hot wallets, as they are only accessible via the internet.
- **Desktop wallet:** A desktop wallet is designed to be downloaded and installed on your desktop. Desktop wallets are handy for managing your cryptocurrency when you're offline. Some wallets double up as nodes in their respective blockchain networks.
- **Mobile wallet:** Like a desktop wallet, a mobile wallet is downloaded and installed on your smartphone. There are various wallets available for iOS and Android. Mobile wallets are considered hot as your smartphone is readily accessible via a data connection at most times.
- **Hardware wallet:** A hardware wallet is an offline physical device, such as the Trezor wallet. A hardware wallet works like a minute portable safe. But they can also send and receive transactions online when required. A hardware wallet is considered a cold wallet (see below).
- **Cold wallet:** A cold wallet, also referred to as cold storage, is an offline wallet. You only connect the wallet to the internet to send and receive cryptocurrency. This ensures no one can hack your Bitcoin, and so on.

**Keeping your funds in cold storage is the most secure option.** But if you plan to spend your Bitcoins or exchange them for other cryptocurrencies (commonly referred to as “altcoins”), you’ll need an easily accessible wallet. That’s where the other wallet choices step in.

If you’re buying Bitcoin as a long-term investment, I would advise checking out one of the following wallet options.

## 2.3 Bitcoin Wallet Guide: **Electrum**

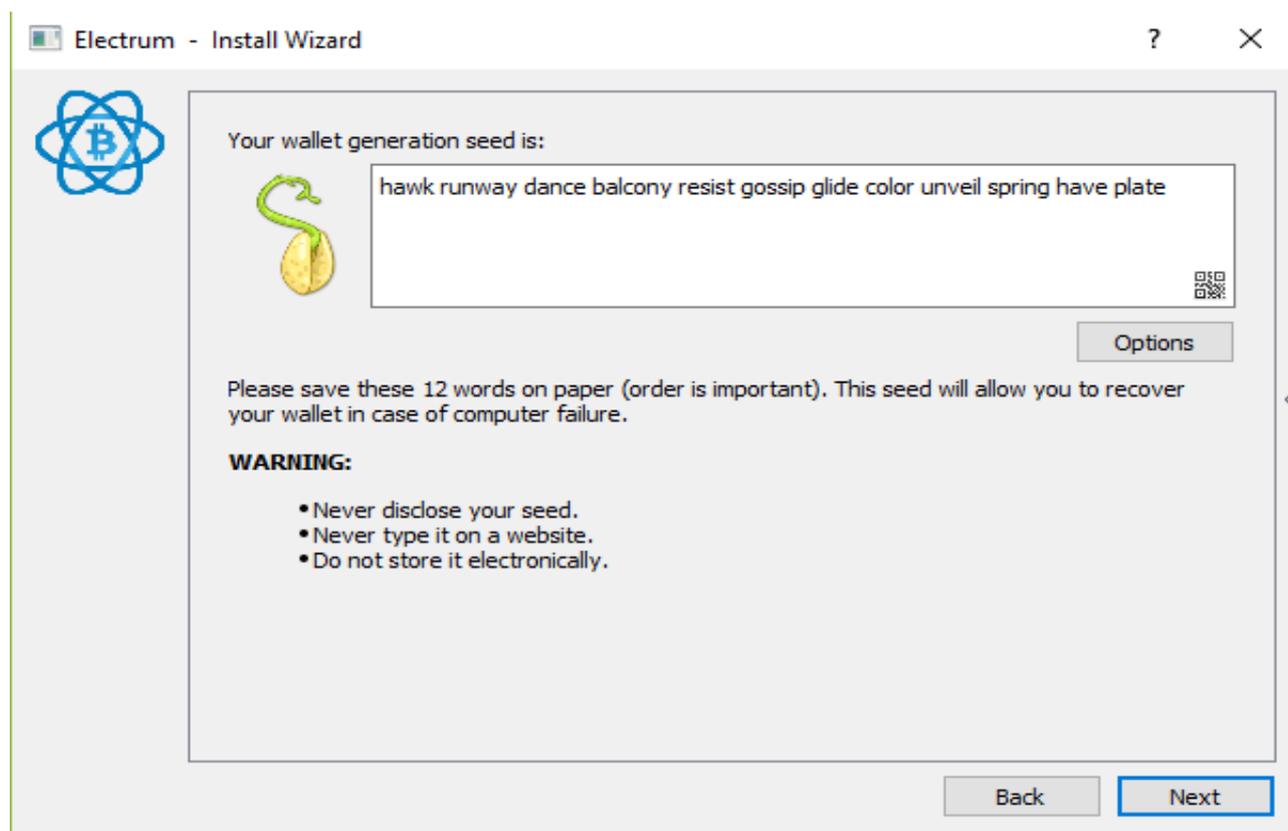
Onto the actual wallets. I’m going to show you Electrum, for holding just Bitcoin. There are other wallets available that hold more than Bitcoin.

I would advise almost every Bitcoin newcomer to check out Electrum. It is one of the best Windows desktop Bitcoin wallets around. Electrum is relatively easy to use, is secure, and has some friendly error mitigation tactics that are perfect for Bitcoin newcomers. I also really like that it is open source. That doesn’t automatically make it secure, but it certainly makes it vastly more difficult for nefarious backdoors and other vulnerabilities.

You download and install Electrum to your desktop. Once you install Electrum, it will guide you through the creation of your first wallet. Choose the **Standard Wallet** for now. Next, you must **Create a new seed**, using a **Standard** wallet. (You can head back and create a **SegWit** wallet later on.)

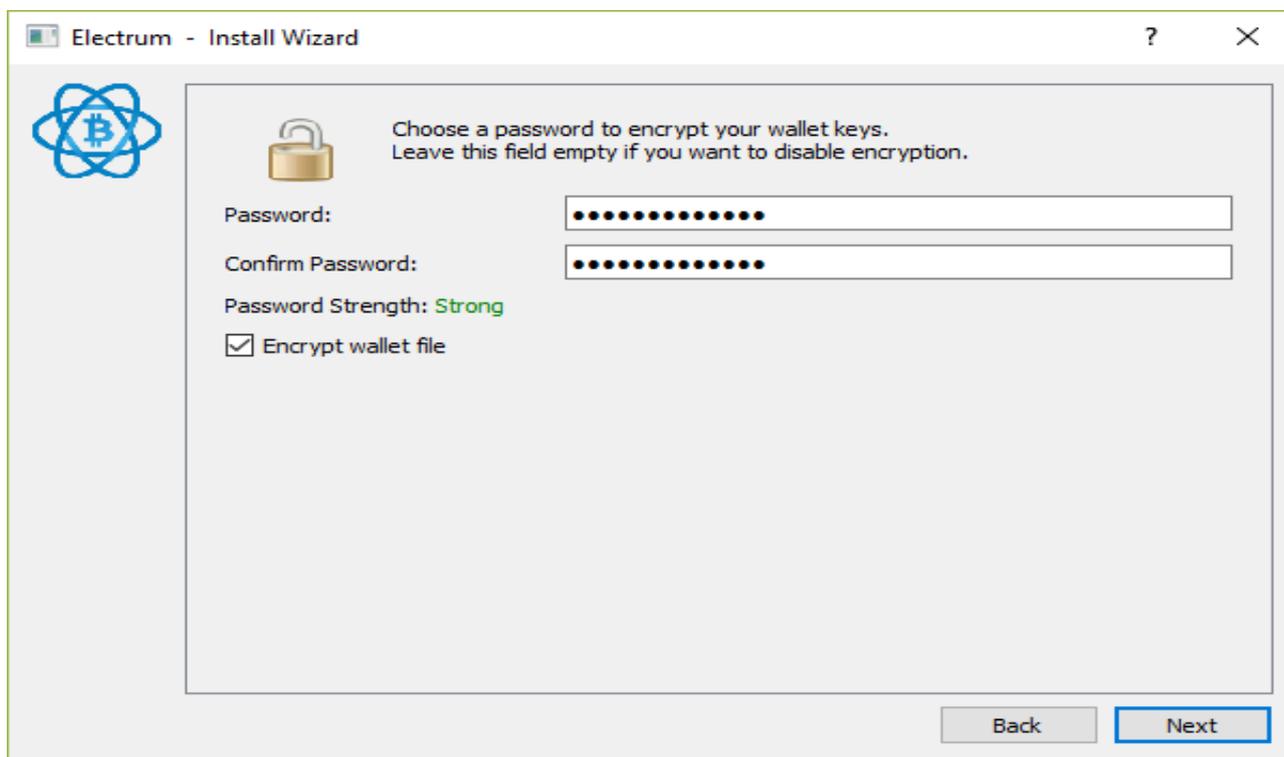
The next screen allows you to create a seed. The wallet seed allows you to recover your Bitcoin wallet from another device at a later date. As it says on the screen, never disclose your seed. If anyone else accesses your seed information, they can recover your wallet to their own device and drain your funds—without you knowing.

Unhappy with the default seed? Press **Back** and **Next** a few times until you’re happy. Then copy the seed down and press **Next**.



Now you must create a password. I suggest creating a very strong, single-use password. This password will encrypt your wallet and keep it secure. Like your seed, do not forget or lose this password; **your funds will be irretrievably lost otherwise.**

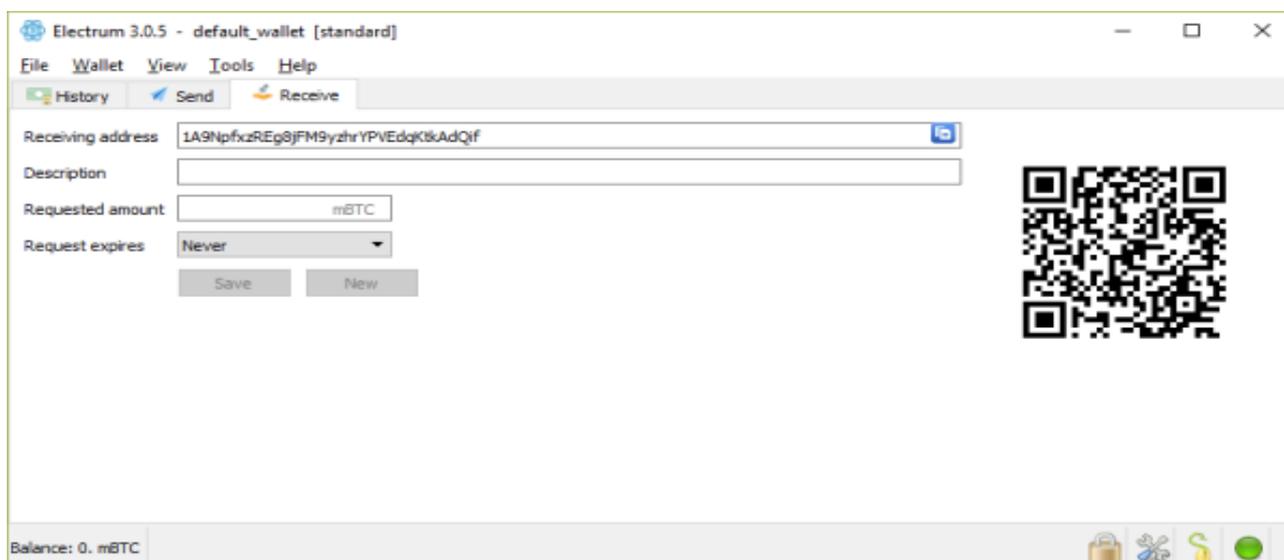
Electrum will now create your actual wallet.



## 2.4 How to Receive Bitcoin

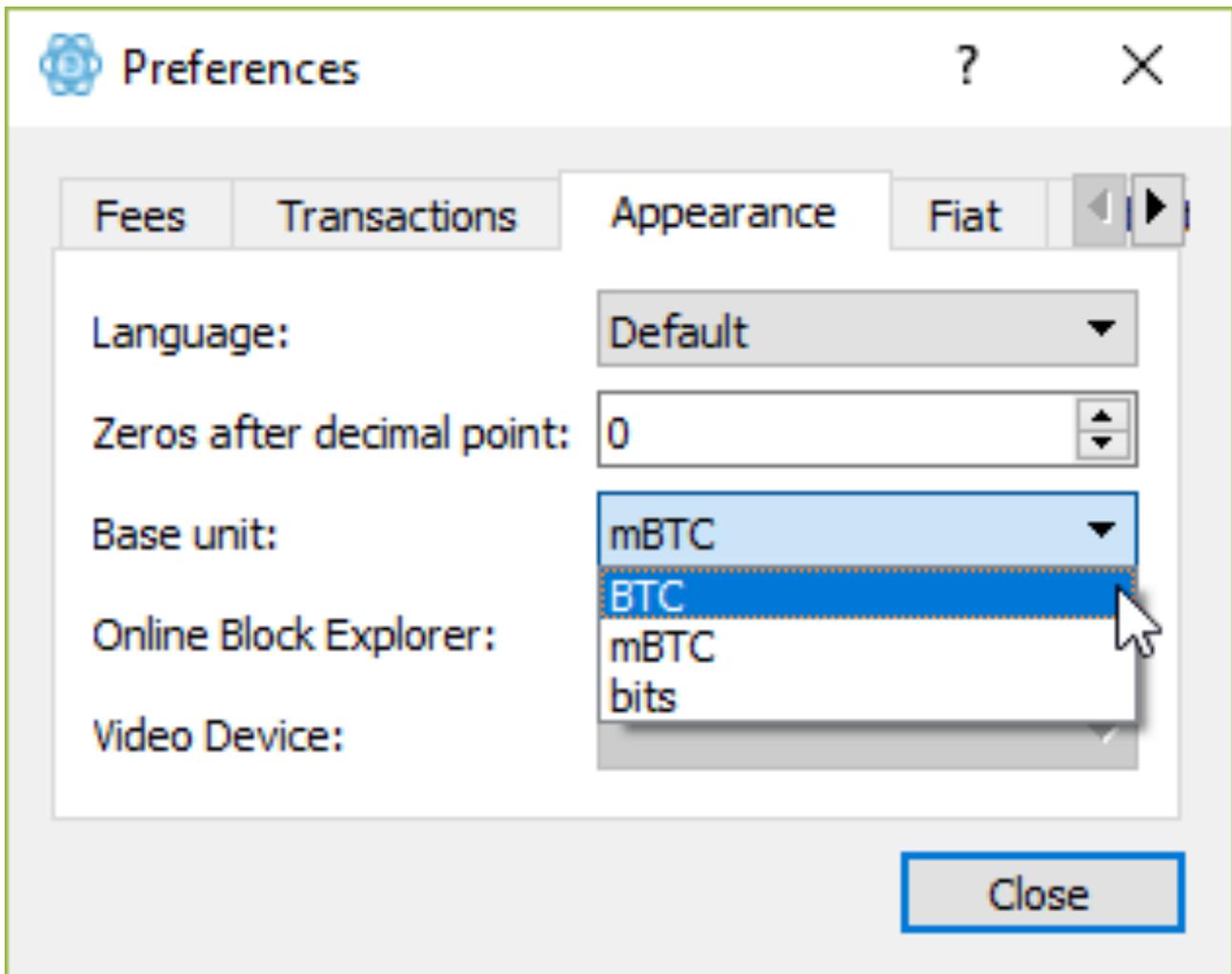
Remember the Bitcoin you bought using one of the exchanges above? You can now send that Bitcoin to this desktop wallet. The Electrum app has three tabs: **History**, **Send**, and **Receive**.

Open the **Receive** tab. Note the **Receiving address**? This is the address you should input into the Bitcoin exchange. For instance, if you bought using Coinbase, you would head to **Accounts > BTC Wallet > Send**, then enter the amount to send. As pictured in the image below, you enter the Electrum receiving address, press **Continue**, and confirm the transaction.



## 2.5 How to Send Bitcoin

If you want to send your Bitcoin to another address at a later date, you'll need the **Send** tab. Add the Bitcoin address you wish to send to in the **Pay to** box and add a description if necessary. Next, enter the amount you would like to send. Note the default Electrum denomination is in **mBTC**, or millibitcoins. One millibitcoin equals 0.001 Bitcoins. This is to allow greater control over the exact amount of Bitcoin sent at one time.



With this in mind, 1 BTC equals 1000 mBTC, and so on. Use a **Bitcoin denomination converter** before sending to ensure you have the correct amount. Alternatively, in the Electrum app, head to **Tools > Preferences > Appearance**, and change the default base unit to **BTC**.

## 3. How to Mine Bitcoin

Mining Bitcoin is a power and resource-intensive process. In the early days of Bitcoin, even a laptop CPU could happily mine the cryptocurrency. But as the number of miners attempting to validate transactions rises, so does the difficulty of matching hashes. As such, regular hardware is essentially worthless when it comes to Bitcoin mining.

Instead, many users contribute their system resources to a shared mining pool. Pooling resources gives miners a far greater chance of winning the Bitcoin block reward. However, all users then share the reward. Let's take a look at how you can solo mine, or join a mining pool instead.

### 3.1 Hardware for Mining Bitcoin

Before we consider the nuances of solo mining, we need to consider the hardware you need. If you're considering solo mining Bitcoin, you need an ASIC (Application-Specific Integrated Circuit) Bitcoin miner. Otherwise, your efforts will end up only costing you money (for electricity and the degradation of your GPU).

ASIC mining hardware specifications regularly change to provide more hash power. However, you're looking for three main ASIC specifications:

- Power Efficiency
- Hash Rate
- Price

Remember, you have to pay off any hardware costs before you start making a profit, so the price point is important. Similarly, ASIC Bitcoin mining uses electricity—a lot of it, too. Before you splurge on an ASIC Bitcoin miner, use a Bitcoin mining profit calculator to check if you will make any returns.

### 3.2 Bitcoin Mining Profit Calculator

Bitcoin mining profit calculators also vary depending on how you're mining. Some Bitcoin mining pool sites sometimes have their own site-specific calculator detailing pool payouts for certain bits of hardware.

Otherwise, the [CryptoCompare Bitcoin mining calculator](#) works well. You need the hashing power of your hardware, your electricity consumption, and cost per kilowatt hour (kWh). You should also add your mining pool fee if applicable.

Another useful site is [WhatToMine](#). WhatToMine shows your hash rate for a range of different cryptocurrency algorithms, quickly showing you where your hardware will profit.

0	470	3	480	0	570
0	1060	1	1070	0	1070Ti
CryptoNight		CryptoNightV7		Equihash	
Hash rate		Hash rate		Hash rate	
630.0	h/s	630.0	h/s	430.0	h/s
Power		Power		Power	
100.0	W	100.0	W	120.0	W
Daily cost		Daily cost		Daily cost	
\$0.02		\$0.02		\$0.03	

### 3.3 Bitcoin Mining Pools

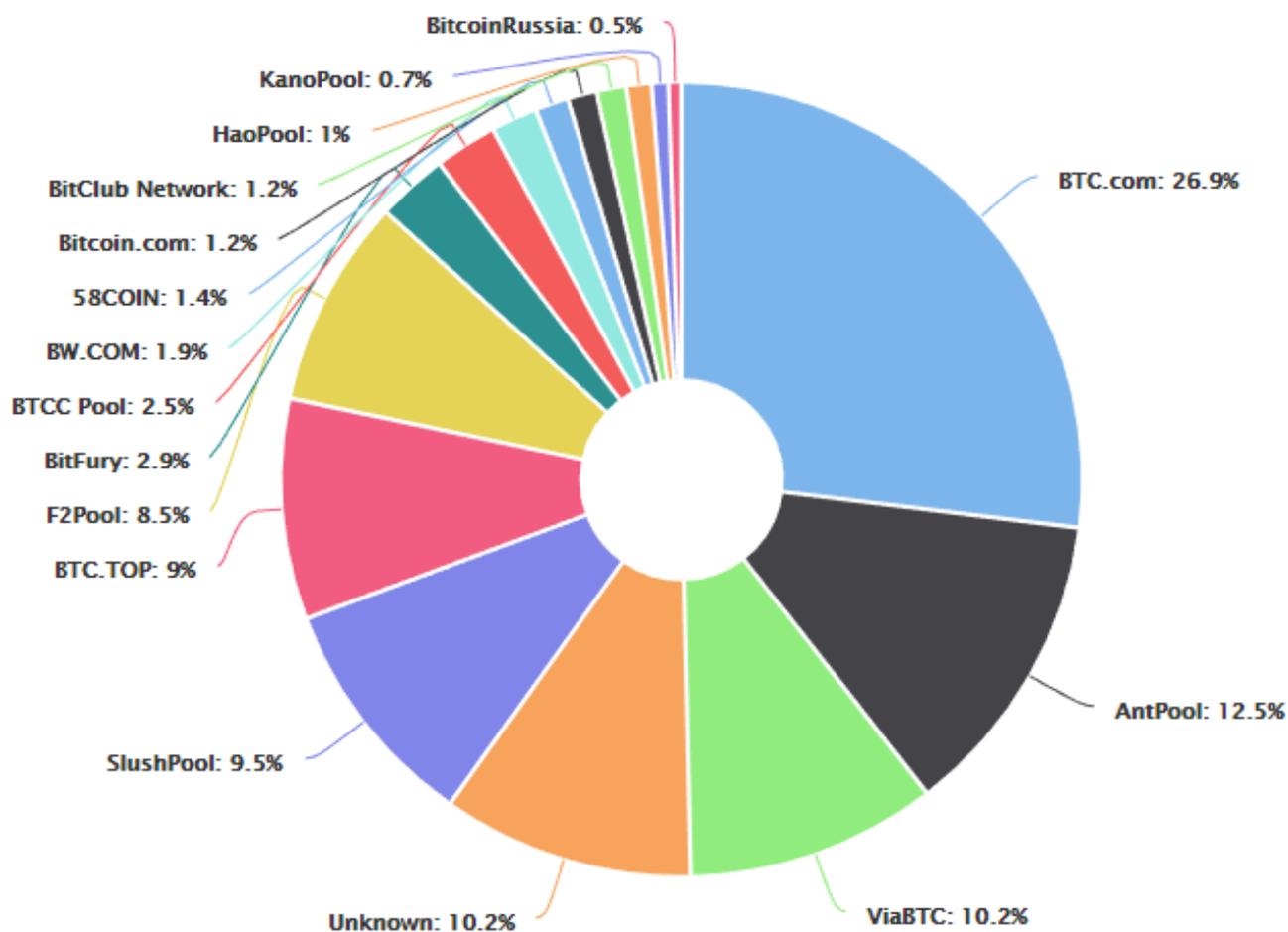
Your best bet for securing some freshly mined Bitcoin is through a mining pool. **Mining pools use combined shared resources** to boost their overall power. The boosted hash rate gives a shared Bitcoin mining pool a greater chance of finding a new block to mine. Users share the resulting block reward, usually distributed by user power contribution.

While reward sharing decreases the amount of Bitcoin you receive, it also gives you a chance of actually succeeding at Bitcoin mining. Mining pools account for the overwhelming majority of all Bitcoin mining at this point, with major pools accounting for large proportions of the total hash power in action at any one time.

Bitcoin mining pools all have their own nuances. Here are three worth checking out that are also easy for beginners:

- **AntPool:** AntPool is one of the largest Bitcoin mining pools, regularly accounting for 25 percent of the total hash power around the world. Owned by Chinese ASIC manufacturer Bitmain, AntPool has an easy-to-use interface that lets you customize your Bitcoin payouts.
- **Slush Pool:** Slush Pool is another veteran Bitcoin mining pool that is easy to use for beginners. Slush Pool holds steady between 10-15 percent of total Bitcoin mining hash power and its users see decent returns for their hardware time investment.
- **BTC.com:** Like Slush Pool and AntPool, BTC.com is one of the most well-known Bitcoin mining pools around. BTC.com regularly accounts for 20% or more of global hash power and is known for its Full Pay Per Share payout system (increasing pool payouts).

Some Bitcoin mining pools offer custom software to connect to their infrastructure. However, at other times (depending on the pool you choose) you will enter the pool mining address in a third-party mining tool, such as **CGMiner**. The below image shows the rough percentage share of each mining pool at the time of writing (May 2018).



### 3.4 Solo Mining Bitcoin

Solo mining isn't an easy task, at least regarding Bitcoin. A solo mining rig that can compete with the larger mining pools will cost a vast sum of money. That's not to say you cannot try, but your chance of finding a block to mine alone is minuscule.

## 4. The Future of Bitcoin

**The future of Bitcoin is difficult to predict.** Will the price blast to the moon once again? Or is Bitcoin set for a prolonged period of uncertainty?

At the moment, there are no solid guesses. **Overall awareness of Bitcoin is mixed at best.** Are we in an enlightenment phase, or has the Bitcoin market already capitulated for good?

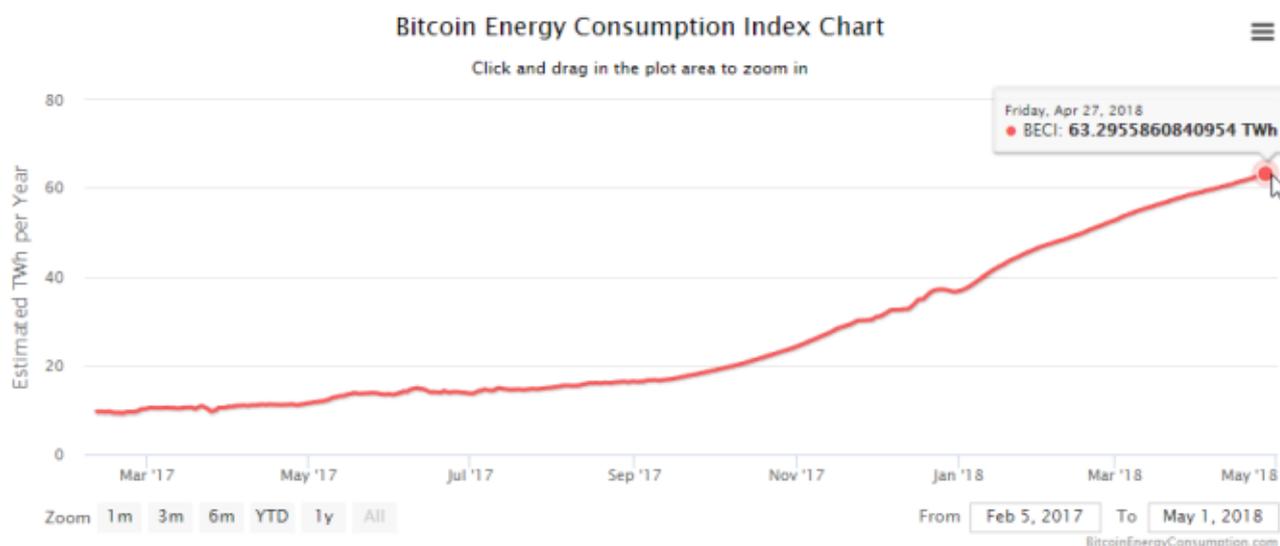
Looking at the numbers doesn't make the immediate future of Bitcoin any clearer. **Bitcoin price predictions are a dime a dozen**. Here are a handful of Bitcoin price predictions from a range of sources:

- **Saxo Bank:** \$60,000 in 2018, before crashing back to \$1,000 before 2019
- **John McAfee:** \$1,000,000 by 2020
- **James Altucher:** \$1,000,000 by 2020
- **Winklevoss twins:** \$152,000, unspecified date
- Masterluc (legendary crypto-trader): \$40,000-\$110,000 by 2019

But perhaps **the future of Bitcoin isn't price predictions and market capitalization**. The future of Bitcoin might be measured in its direct influence in the introduction of cryptocurrencies to the world. Moreover, the ongoing **value of the decentralized blockchain technology behind Bitcoin** also holds a legacy.

## 4.1 Bitcoin Power Consumption

Some aspects of Bitcoin must change, however. The global power consumption of the Bitcoin mining network is staggering. From December 2017 to April 2018 (the time of writing), Bitcoins **power consumption almost doubled**, from around 32 TWh to 63 TWh—or more than the entire country of Switzerland. Power consumption continues to rise as Bitcoin's growth is driven by the desire for profit.



Even countries like Iceland, that run almost exclusively on renewable energy, are struggling to cope with Bitcoin mining demand. Iceland has long had extensive power consumption issues through its aluminum smelting industry (using more than 70% of the country's entire power), but now Bitcoin mining is sucking up more energy than the entire population uses to power their homes for a year.

There is another downside, too. While geothermal and hydro plants have a smaller environmental impact than a fume-spewing Chinese coal plant, it isn't neutral. Furthermore, most of the Bitcoin mining requires no staff, returns very little in taxes to the Icelandic people, and isn't worthwhile to the country. To the world, yes, renewable energy for Bitcoin mining is excellent. But for the host nation? Not so much.

## 4.2 Bitcoin “Layer 2” Protocol

Another issue facing Bitcoin is sustainable growth. Simply put, the Bitcoin network cannot process enough transactions to compete with fiat currency solutions or the expansive pressure on the existing infrastructure. Several proposals would mediate this issue. One is the hard forks earlier discussed.

However, another solution lies with new “Layer 2” Bitcoin network protocols. These Layer 2 protocol solutions aim to increase network capacity and transaction speed without requiring a hard fork. Instead, a Layer 2 protocol sits atop and interacts with the existing Bitcoin network. The most notable example is the Lightning Network.

The **Lightning Network** creates user-generated private payment channels without ever directly interacting with the blockchain. Instead, the Lightning Network channel caches transactions until each party is ready to finalize. Then, when the channel closes, the Bitcoin transactions register on the blockchain. The Lightning Network has around 1,000 nodes at the time of writing and is currently used for smaller transactions.

Fiat is to gold as lightning network is to Bitcoin.

*Fiat was effectively a layer 2 solution to scaling gold. It was backed and settled to gold until that backing was removed. Unlike fiat though, LN's settlement to Bitcoin is cryptographically secured and cannot be removed!*

— Charlie Lee [LTC] (@SatoshiLite) *December 10, 2017*

There is even discussion regarding another protocol layer between the main Bitcoin network and Layer 2 protocols to further increase transaction speed.

## 4.3 Bitcoin Price Volatility

Bitcoin price volatility is of major concern for users and investors. Although the wild speculation and volatile price made some people overnight millionaires in November and December 2017, the peaks and troughs make it difficult to use as regular currency.



The introduction of Bitcoin derivative markets in January 2018 did introduce a measure of stability. Both the Chicago Mercantile Exchange and the Chicago Board Options Futures Exchange now offer Bitcoin futures trading. The period after their introduction saw a long period of Bitcoin price depression. Furthermore, the Bitcoin price per coin has struggled to rise to its previous heights.

Regardless, Bitcoin remains too volatile for most regular retailers to accept it as a serious form of payment for goods and services.

## That's Everything You Need to Know About Bitcoin

Using this guide makes buying, selling, trading, and understanding Bitcoin easy. You now know how to use the Electrum Bitcoin wallet, as well as what signing up to a Bitcoin mining pool means. And finally, you know what the immediate future of Bitcoin looks like, including how the network will evolve to cope with continual growth.

The Bitcoin journey is still in its infancy. And while Bitcoin might not last the distance, it has certainly set the cryptocurrency ball rolling.

Read more stories like this at

