Everything You Ever Wanted to Know About Bitcoin

avgjoefinance.com/bitcoin-comprehensive-guide

Joe December 12, 2017

Bitcoin has been in the news quite a lot recently. I'm sure you've heard how bitcoin's price has been increasing thousands of dollars a day. Maybe you've even invested or have been thinking about investing in it.

But how much do you really know about Bitcoin?

A friend recently asked me what I thought of the cryptocurrency and while I had an initial response (my overall thoughts on bitcoin as an investment are toward the end of this post) It called to my attention how little I knew. Sure, I've seen all the posts on social media (link) and heard of terms like Bitcoin wallet, blockchain, and Bitcoin mining, but I really didn't understand them.

In an effort to learn more about the digital currency, I went down an internet rabbit hole to really determine what Bitcoin is all about. When I finally climbed back out I had a much greater understanding of how Bitcoin works and it's both simpler and more complicated than I had previously thought.

The comprehensive guide below is a result of that research.

A note on the word bitcoin and capitalization. Bitcoin is both the name of a software/community and a currency. When talking about the software Bitcoin is supposed to be capitalized, while the currency is lowercase. I'll do my must to use the correct capitalization throughout this article, but I'll probably mess up a few times, so I apologize in advance!

What is Bitcoin and Cryptocurrency?

Bitcoin is a cryptocurrency that was created in 2009 by someone under the name of Satoshi Nakamato. Originally outlined in an article about a peer-to-peer electronic cash system, Nakamato released the open-source software in January 2009.

The idea behind the system was that there wouldn't be a need for a central bank or clearinghouse to process the transactions. Using the blockchain technology, users would be able to process payments directly without the use of a middleman.

Because of the peer-to-peer processing, transactions costs are significantly lower and can also be anonymous.

Limited Supply

According to the source code, there is a finite number of bitcoins that can be mined. Currently, the number stands at 21 million (unless a change to the code is made). As of December 2017, approximately 16 million have been mined.

The limited supply of bitcoin is what causes many to believe it is valuable. Most people that invest liken it to gold since both are mined and have a finite supply. However, gold has the advantage of being a physical commodity, unlike bitcoin which is completely digital.

Crypto What?

As I mentioned earlier, **bitcoin is a type of cryptocurrency**. And it is, in fact, one of many. Others include Iota and Ethereum.

While the prefix, crypto may carry a negative connotation, that's not the case. The crypto in cryptocurrency simply refers to the fact that it uses encryption techniques to regulate its ownership and transfer. So, a cryptocurrency is simply a digital currency that uses encryption.

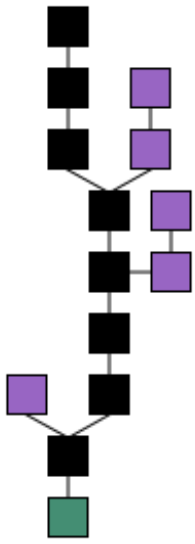
What is Blockchain Technology?

While Bitcoin uses the blockchain technology, it was not invented solely for the digital currency. The idea of blockchain has been around since the early 90s.

Blockchain is a list of records, called blocks, that are linked together, using encryption, into a

chain.

All of these blocks are kept in a public ledger across a distributed network (this means that every computer on the network has a copy of the ledger). Since the ledger is public and continually verified by the network, there is no need for a central authority.



An example of a blockchain

Blockchain Security

In simple terms, blockchain security works in two ways. One, anyone who wants to perform a transaction using bitcoin must have a public and private key.

The public key is a long string of numbers that is an address on the blockchain. The address relates to the value of bitcoin you have. The private key is the password the owner uses to access their digital assets. Put another way, the public key is your home address and the private key is what you use to unlock your door.

It is this private key that unlocks the encryption and allows the transaction to take place. If you were to lose your private key or have it stolen then all of your bitcoin would be lost.

The second security feature is the fact that every user on the network has a copy of the ledger. This means that when a new block is added it is impossible for one person to go back and manipulate it without changing that block on every computer in the network.

This transparency and security is why many people believe bitcoin has a future as a legitimate currency. While bitcoin may or may not make it long-term, banks and other institutions have started implementing blockchain technology.

How Does Bitcoin Mining Work?

When I first heard about mining bitcoin, I imagined that you had to find it, similar to how you mine for gold. The truth is that Bitcoin mining is a bit of a misnomer. Instead of directly searching for bitcoin, you search for the correct solution to a mathematical proof and are given bitcoin as a reward.

More Like Block Mining

As I mentioned earlier, Bitcoin uses a blockchain. All digital transactions are recorded in blocks which are verified by the network and then added to the chain.

Miners are the people that make this process happen. In order for a block to be added to the chain, it must contain a proof-of-work. This proof requires miners to find a number, called a nonce and encrypt it along with all of the information in the existing chain.

The result is then compared to the network's difficulty target. If the result is less than the target, then the block is added to the chain. If it doesn't meet the threshold than the miner must try a different nonce until the difficulty target is met.

The network's difficulty target is constantly being adjusted based on the total computing power in the network. Bitcoin adjusts the target so that a new block is added around every 10 minutes. The higher the difficulty the more nonces an individual user on the network must try in order to solve the proof.

You can calculate the possible combinations by taking the network target times 2^{48} divided by 65,535. Based on the current difficulty target of 1,590,896,927,258 the average number of attempts it takes to solve the proof-of-work and add a block is **6.8 sextillion**. That's a 6 with 21 zeros after it!

The volume of combinations means that only high powered, extremely expensive computers can solve the proof. Yet while it is difficult to find the correct nonce, it is relatively easy for the other computers on the network to verify the result.

The Value in Mining

However, in order for this to work, there has to be people on network willing to constantly update and verify the chain.

In order to incentivize people to continue to mine and add new blocks, each user who solves the proof-of-work is **paid a bitcoin reward** and a transaction fee.

In 2009, the reward was 50 bitcoins for each block. The program was created to halve that reward after every 210,000 blocks. Eight years later, the reward has been halved twice to 12.5 bitcoins per block. Once all 21 million bitcoins have been awarded, users verifying new blocks will continue to receive a transaction fee.

Where Do You Store Bitcoin?

One of the biggest differences between digital and paper currency is that you don't actually store digital currency. While you can own bitcoin, **you never actually receive possession of it**.

Bitcoin stays on the blockchain. The only thing an owner has is their private key. This key is the credentials needed to access the bitcoin on the chain. That is why keeping your private key safe is so important.

When you hear about bitcoin being stolen, hackers are not actually stealing bitcoin from someone's account, like they would a bank account, but rather just stealing their private key. Because the key is all you need to process a transaction.

Bitcoin Wallets

Users' private keys are stored in wallets. There a few different versions of wallets available.

Desktop and mobile wallets have the private key saved directly on them. The only real difference is mobility. With a desktop wallet, a user can only process transactions from the desktop the private key is stored on. Mobile wallets allow users to process transactions anywhere they have their mobile device.

Another option, that has become more popular as Bitcoin has grown, is online wallets. Some popular online wallets include Coinbase and Blockchain (confusing, I know, but blockchain is both the technology Bitcoin uses and a company that offers a wallet).

While online wallets provide the easiest access, they are also the least secure. Since your private key is stored directly with the online providers, if they are hacked you will lose access to all of your bitcoin. Plus, many of these sites are having issues keeping up with the increased number of transactions, making it difficult to complete buy and sell orders.

Off the Grid

The most secure way to store your private key is with cold storage. This means that the private key is stored on a desktop or even just a hard drive that is not attached to a network. By doing so, you can ensure that hackers won't be able to steal your key. The only time you would need to bring the private key online would be to complete a transaction. But this would only be for a limited amount of time, making it difficult for anyone to steal.

How Do You Buy & Sell Bitcoin?

In order to buy or sell bitcoin, you first need a Bitcoin wallet. Since these wallets contain a user's private key, they are needed by the blockchain encryption to confirm ownership before any transaction can occur. Once you have a wallet, you can purchase bitcoin on any number of exchanges.

Bitcoin Exchanges

As of today, there are a handful of exchanges devoted to bitcoin. One of the popular wallet sites, Coinbase also has its own exchange.

Making a purchase or sale on one of these exchanges is similar to buying and selling stock. Each exchange lists the current bitcoin price and you can enter orders for processing. However, unlike stocks, bitcoin is much more illiquid and the transactions aren't immediate.

Due to the high transaction volume, many of these exchanges have beenexperiencing significant downtime. Also, because the blockchain requires new blocks to be verified, there is a limit to the volume that can be processed each day. Because of this, it can sometimes take several days for a transaction to be completed.

Remember once you complete a purchase, you don't actually receive any bitcoin. Everything stays on the blockchain, all you have is your private key. So, if you lose that key, there is no way to access your bitcoin again.

Another issue with the exchanges is that they can list widely different values. While stock exchanges like the NYSE or NASDAQ are fairly in sync on price, Bitcoin exchanges don't have that level of interaction. Recently two different exchanges had a price difference of $4,000. This level of price discrepancy makes it difficult to determine if you are getting the best purchase or sale price.

What are Bitcoin Futures?

While I'm writing this post, trading of bitcoin futures is expecting to go live December 18th. So, while I'm not sure of the ultimate impact these futures will have, I can give you an overview of what it means for the digital currency.

A Golden Opportunity

Leave it to Wall Street to pounce on any opportunity it sees. The spike in bitcoin's value made it a question of when not if Wall Street would get involved. Since the supply of bitcoin is limited and there are issues over the liquidity, Wall Street has stepped in and created bitcoin futures trading.

Essentially, bitcoin futures will work similar to other currency futures. Traders will be able to

purchase contracts that will be settled at a future date. These contracts will be made up of five bitcoin each and priced in $25 increments ($5 per bitcoin).

However, the settlement of these contracts is in cash, not bitcoin. So, buying them does not entitle you to receive any bitcoin. This cash settlement means that individuals can use the futures to speculate on the price of bitcoin without having to actually buy or sell any.

While some believe this trading will bring more liquidity to bitcoin, others are concerned it will cause a major price drop. Before futures trading, there was no direct way to bet on the value of bitcoin going down. The only option you had was to bet on an increase in value by buying bitcoin itself. With these futures contracts, you will now be able to bet on a decline, similar to shorting a stock.

With this ability, the argument is these 'short-sellers' will drive down the price of bitcoin in order to earn a profit on their futures contracts. While this is a certainly a possibility, the overall impact of trading bitcoin futures remains to be seen.

Should You Invest in Bitcoin?

Now that you (hopefully) have a better understanding of what Bitcoin is and how it works, comes the question of whether you should buy any.

This has been a pretty hot-button debate (just look at any Facebook group or Reddit thread). Even professional investors and financers are split on the topic.

Shark Tank investor Kevin O'Leary doesn't "consider it a currency." While Cameron Winklevoss (one half of the Winklevoss twins and major bitcoin investor) believes that "long term, directionally, it is a multitrillion-dollar asset."

Richard Branson has even entered this space by investing in the bitcoin wallet, Blockchain.

Yet, out of all the quotes I've read, I like self-help guru, Tony Robbins' the best. He said, "I look at [bitcoin] as it's like going to Vegas."

Investment Maybe, Not Quite a Currency

From all my research, I don't think bitcoin is ready to become a functional currency like the dollar or euro. There is just too much volatility in its price and not enough people have faith in its value.

I can't remember where I read this, but one person noted that they tried to make a purchase with an international company using bitcoin. However, the company wanted them to ensure the value because they weren't willing to take a few minutes risk as to the change in its

value. The mark of a currency is faith in its value for longer than such a short period of time. Until bitcoin or some other cryptocurrency stabilizes, I don't see it as a true equal to paper currency.

As an investment, Bitcoin is purely speculation. The massive swings in value don't make it a prudent investment option. However, a lot of people are aware of the risks and still invest. Maybe you want to be able to say you own bitcoin. Just don't think it's going to make you rich.

If you do decide to buy some, assume you're going to lose your entire investment. That way you won't be tempted to use the money you can't afford to lose.