My Drift

Title: What is Bitcoin?

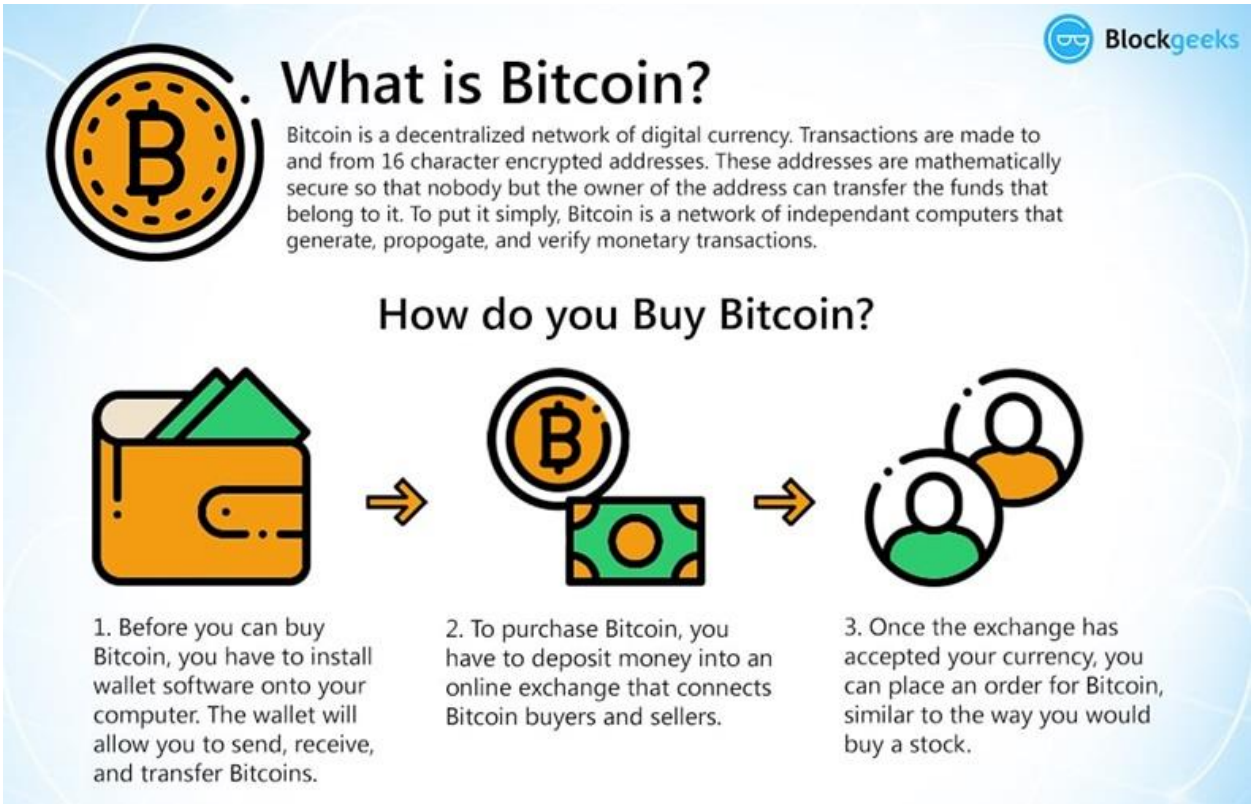
Written By: Jerry D. Petersen
Date: 15 Mar 2024
Article Number: (450-2024-9)

I have no clue what's a Bitcoin!

However, my son is thinking about investing a few bucks each pay day on bitcoins. He asked me to do a little research and maybe write an article to see if I thought this was a good idea.

What is Bitcoin?

In 2008, a pseudonymous programmer named Satoshi Nakamoto published a 9-page document outlining a new decentralized, digital currency. They called it Bitcoin.



What is Bitcoin

bitcoin

What is Bitcoin

The world's most popular digital currency, or cryptocurrency. There are no bitcoin bills or coins: all transactions happen online.

Who controls Bitcoin

Unlike regular currencies controlled by the government, Bitcoin is a decentralized currency that is not controlled by any central authority.

What is Bitcoin used for

Bitcoin can be used for payments. but most people use Bitcoin as an investment with an intent of making a profit.

How are Bitcoins created

New Bitcoins are created through a process called mining, where computers solve mathematical equations and generate Bitcoin.

How can you get Bitcoins

Buying at a Bitcoin exchange, special retail locations or Bitcoin ATMs; or earning through mining, playing some online games, etc.

Is Bitcoin a good invetment

Being a very volatile currency, there is a huge risk involved with trading Bitcoins. So it is not the best investment for small individual investors.

Bitcoin is the world's first successful decentralized cryptocurrency and payment system, launched in 2009 by a mysterious creator known only as Satoshi Nakamoto. The word "cryptocurrency" refers to a group of digital assets where transactions are secured and verified using cryptography – a scientific practice of encoding and decoding data. Those transactions are often stored on computers distributed all over the world via a distributed ledger technology called blockchain (see below.)

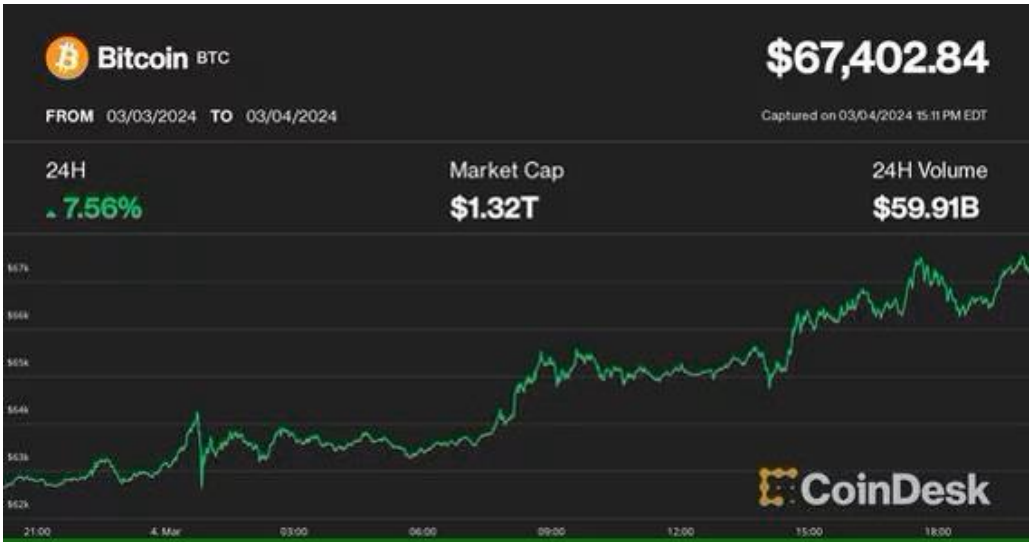
Bitcoin can be divided into smaller units known as "satoshis" (up to 8 decimal places) and used for payments, but it's also considered a store of value like gold. This is because the price of a single bitcoin has increased considerably since its inception – from less than a cent to tens of thousands of dollars. When discussed as a market asset, bitcoin is represented by the ticker symbol BTC-USD.

The term "decentralized" is used often when discussing cryptocurrency, and simply means something that is widely distributed and has no single, centralized location or controlling authority. In the case of bitcoin, and indeed many other cryptocurrencies, the technology and infrastructure that govern the creation, supply, and security of it do not rely on centralized entities, like banks and governments, to manage it.

Instead, Bitcoin is designed in such a way that users can exchange value with one another directly through a peer-to-peer network; a type of network where all users have equal power and are connected directly to each other without a central server or intermediary company acting in the middle. This allows data to be shared and stored, or bitcoin payments to be sent and received seamlessly between parties.

The Bitcoin network (capital "B", when referring to the network and technology, lower-case "b" when referring to the actual currency, bitcoin) is completely public, meaning anyone in the world with an internet connection and a device that can connect to it can participate without restriction. It's also open-source, meaning anyone can view or share the source code Bitcoin was built upon.

Perhaps the easiest way to understand bitcoin is to think of it like the internet for money. The internet is purely digital, no single person owns or controls it, it's borderless (meaning anyone with electricity and a device can connect to it), it runs 24/7, and people who use it can easily share data between one another. Now imagine if there was an 'internet currency' where everyone who used the internet could help to secure it, issue it and pay each other directly with it without having to involve a bank. That's what bitcoin essentially is.



Bitcoin Value Chart

An alternative to fiat currency

Nakamoto originally designed bitcoin as an alternative to traditional money, with the goal for it to eventually become a globally accepted legal tender so people could use it to purchase goods and services.

However, bitcoin's utility for payments has been stymied somewhat by its price volatility. Volatility is a word used to describe how much an asset's price changes over a period of time. In the case of bitcoin, its price can change dramatically day to day – and even minute to minute – making it a less than ideal payment option. For example, you wouldn't want to pay $3.50 for a cup of coffee and 5 minutes later it's worth $4.30. Conversely, it doesn't work out

great for merchants either if bitcoin's price falls dramatically after the coffee's handed over.

In many ways, bitcoin works in the opposite way as traditional money: It is not controlled or issued by a central bank, it has a fixed supply (which means new bitcoins cannot be created at will) and its price is not predictable. Understanding these differences is the key to understanding bitcoin.

Basic Components of Bitcoin

Basic Terms

Encryption: **Encrypting data means hiding it in such a way that if the user has a password or code, then only that data can be interpreted. Ciphering serves a similar role in cryptography.**

Cryptocurrency: **Cryptocurrency is like physical money, is a medium of exchange, although a digital one.**

Wallet: **A secure digital wallet used to store, send, and receive digital currencies is known as a crypto wallet.**

Blockchain: **Blockchain is a public ledger that is distributed and decentralized. The blockchain is a database that is validated by a large group of people rather than a single authority.**

Nodes: **The machines that make up the blockchain network are known as nodes. They are in charge of preserving and disseminating updated copies of the transactions that are carried out in real-time. When a new block is created and added to the general ledger, a copy is sent to all of the network's nodes.**

Private Key: **A wallet (essentially an address), and a private key are the two entities that are needed to complete a transaction. A private key is a series of random digits that, unlike an address, must be kept private.**

Bid Price: **The bid price is the price at which someone is attempting to sell an asset.**

Ask Price: **The price at which people are attempting to purchase an asset.**

Components Of Bitcoin

There are four basic components of bitcoin:

- **Software**
- **Cryptography**
- **Hardware**
- **Miners(Gaming Theory)**

1. Software: **Bitcoin is, at its heart, a piece of software that defines what a bitcoin is and how it is transmitted. Checking of validity or who is allowed or**

not allowed to be within bitcoin etc. Type of the regulations of a legitimate bitcoin is established via it. Everything is run by software, which in this case is the bitcoin program. The bitcoin program is always available 24 hours a day, seven days a week.

2 Cryptography: Cryptography and bitcoin as a cryptocurrency are at the heart of the software. Bitcoin regulates both the transfer of bitcoin between parties and the production of new bitcoin units using encryption. Bitcoin would not be conceivable without cryptography. So, we've established that this software use cryptography to regulate bitcoin transfers across the internet. Cryptography is a mathematical approach that can only be solved by machines, not people. Cryptography is required to safeguard the data.

3. Hardware: Cryptography demands a lot of hardware to run and solve. This gear has been created specifically for mining, i.e. detecting Nonce to validate blocks and hashes. To accomplish a simple activity on the bitcoin blockchain, a lot of CPU power is required. If one tries to mine bitcoin with a smartphone or home computer right now, you'll lose your computer and rack up a large electric bill.

4. Miners (Gaming Theory): Game theory studies rational decision-making behavior in humans. Game theory allows interactions between two or more players in a system where the participant's outcome is based on the actions of the others. Every participant's aim is to maximize his gain. The game theory is used by bitcoin to ensure that rational individuals align their interests in a certain way. They impact the network's miners' interactions and behavior in particular.

Miners are individuals who participate in a gaming theory, as bitcoin is essentially a game that is played by miners all over the world. The first component, as mentioned above, is bitcoin software that issues a cryptography challenge every 10 minutes. The cryptography task entails locating a Nonce that will allow the hash of a certain block to be legitimate

How does Bitcoin work?

It's important to understand how the separate components to Bitcoin work - all of which combine together to create a decentralized payment system:

The Bitcoin Network

The native cryptocurrency of the Bitcoin network, called Bitcoin (BTC)

The Bitcoin Blockchain

Bitcoin runs on a peer-to-peer network where users — typically individuals or entities who want to exchange bitcoin with others on the network — do not require the help of intermediaries to execute and validate transactions. Users can choose to connect their computer directly to this network and download its public ledger in which all the historical bitcoin transactions are recorded.

This public ledger uses a technology known as "blockchain," also referred to as "distributed ledger technology." Blockchain technology is what allows cryptocurrency transactions to be verified, stored, and ordered in an immutable, transparent way. Immutability and transparency are vitally important credentials for a payment system that relies on zero trust.

Whenever new transactions are confirmed and added to the ledger, the network updates every user's copy of the ledger to reflect the latest changes. Think of it as an open Google document that updates automatically when anyone with access edits its content.

As its name implies, the Bitcoin blockchain is a digital string of chronologically ordered "blocks" — chunks of code that contain bitcoin transaction data. However, it is important to mention that validating transactions and bitcoin mining are separate processes. Mining can still occur whether transactions are added to the blockchain or not. Likewise, an explosion in Bitcoin transactions does not necessarily increase the rate at which miners find new blocks.

Irrespective of the volume of transactions waiting to be confirmed, the Bitcoin is programmed to allow new blocks to be added to the blockchain approximately once every 10 minutes.

Due to the public nature of the blockchain, all network participants can track and assess bitcoin transactions in real-time. This infrastructure reduces the possibility of an online payment issue known as double-spending. Double spending occurs when a user tries to spend the same cryptocurrency twice.

Bob, who has 1 bitcoin, might try to send it to both Rishi and Eliza at the same time and hope the system doesn't spot it.

Double spending is prevented in the traditional banking system because reconciliation is performed by a central authority. It also isn't a problem with physical cash because you can't hand two people the same single dollar bill.

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending"
Satoshi Nakamoto

Bitcoin, however, has thousands of copies of the same ledger and so it requires the entire network of users to unanimously agree on the validity of each and every bitcoin transaction that takes place. This agreement between all parties is what's known as "consensus."

Just as banks constantly update the balances of their users, everyone that has a copy of the Bitcoin ledger is responsible for confirming and updating the balances of all bitcoin holders. So, the question is: How does the Bitcoin network ensure that consensus is achieved, even though there are countless copies of the public ledger stored all over the world? This is done through a process known as "proof-of-work."

What is proof-of-work?

Computers in the Bitcoin network use a process called proof-of-work (PoW) to validate transactions and secure the network. Proof-of-work is the Bitcoin blockchain's "consensus mechanism."

While Proof-of-Work was the first and is generally the most common type of consensus mechanism for cryptocurrencies that run on blockchains, there are others — most notably proof-of-stake (PoS), which tends to consume less overall computing power (and therefore less energy).

Proof-of-work elevates certain network contributors to the role of "validators" – more commonly known as "miners" – only after they have proven their commitment to the network by dedicating an immense amount of computing power to discovering new blocks — a process that typically takes approximately 10 minutes.

When a new block is discovered, the successful miner who found it through the mining process gets to fill it with 1 megabyte's worth of validated transactions. This new block is then added to the chain and everyone's copy of the ledger is updated to reflect the new data. In exchange for their efforts, the miner is allowed to keep any fees attached to the transactions they add, plus they're given an amount of newly minted bitcoin. The new bitcoin created and handed to successful miners is known as a "block reward."

All Bitcoin users have to pay a network fee each time they send a transaction (usually based on the size of it) before the payment can be queued for validation. Think of it like buying a stamp to post a letter.

The goal when adding a transaction fee is to match or exceed the average fee paid by other network participants so your transaction is processed in a timely manner. Miners have to cover their own electricity and maintenance costs when running their machines all day to validate the bitcoin network, so they prioritize transactions with the highest fees attached to make the most money possible when filling new blocks.

You can view the average fees on the Bitcoin mempool, which can be likened to a waiting room where unconfirmed transactions are held until they are selected and added to the blockchain by miners.

How is bitcoin created?

The Bitcoin network automatically releases newly minted bitcoin to miners when they find and add new blocks to the blockchain. The total supply of bitcoin has a cap of 21 million coins, meaning once the number of coins in circulation reaches 21 million, the protocol will stop minting new coins. In a way, Bitcoin mining doubles as both the transaction validation and the bitcoin issuance process (until all the coins are mined, then it will only function as the transaction validation process.)

Importantly, increasing the amount of computing power dedicated to bitcoin mining will not mean more bitcoins are mined. Miners with more computing power only increase their chances of being rewarded with the next block, so the amount of bitcoin mined remains relatively stable over time.

The Bitcoin network uses a coin distribution strategy known as "bitcoin halving" that ensures the amount of bitcoin distributed to miners reduces over time. By gradually decreasing the supply of new bitcoin entering circulation, the idea is it will help support the asset's price (based on the fundamental principles of supply and demand.)

A bitcoin halving (sometimes called a "halvenings") happens every 210,000 blocks or roughly four years. When the bitcoin protocol first launched in 2009, each successful miner received 50 bitcoin (BTC) as a block reward. Fast forward to 2021: Block rewards are now 6.25 BTC, a reduction from 12.5 BTC prior to the bitcoin halving in May 2020.

The next halving is expected to take place sometime in 2024 and will see block rewards drop again, to 3.125 BTC. This process will continue until eventually there are no more coins left to be mined.

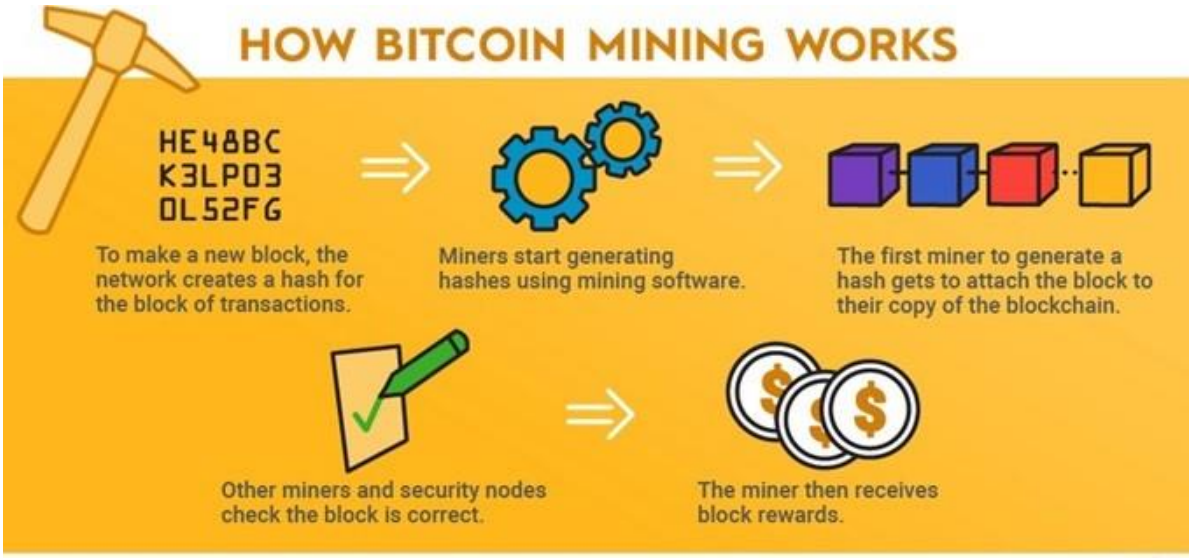
Today, there are over 18.7 million BTC in circulation meaning there are just 2.25 million BTC left to enter circulation. However, taking into consideration the halving principle and other network factors like mining difficulty, it's estimated the last bitcoin will be mined sometime around the year 2140.

"As computers get faster and the total computing proof-of-worker applied to creating bitcoins increases, the difficulty increases proportionally to keep the total new production constant. Thus, it is known in advance how many new bitcoins will be created every year in the future."
Satoshi Nakamoto

How to mine bitcoin

Bitcoin mining is a process that adds transactions to the blockchain and mints new Bitcoin. It involves solving complex mathematical problems using powerful, specialized computer hardware. There was a time in history when it was reasonable to mine bitcoin from your own home, but as the computational hardware requirements have grown, most people entering the space will typically join a mining pool, which is a group of miners pooling resources for greater efficiency.

Miners utilize hardware—often Application-Specific Integrated Circuits (ASICs)—to solve these problems. This process is competitive; the first to solve the problem adds the next block to the blockchain and receives a Bitcoin reward.



Bitcoin mining is not easy. It's extremely energy-intensive, leading to high electricity costs and substantial heat generation so cooling solutions are a must-have for mining hardware. There's also a substantial upfront investment in equipment, and profitability isn't guaranteed due to the volatile nature of Bitcoin's price and the ever-increasing mining difficulty. Lastly, regulatory scrutiny or bans in certain regions due to environmental or other concerns can

pose challenges, so always check local laws before starting. Despite the risks, Bitcoin mining can be potentially profitable for those with the right setup and understanding of the risks.

What is a bitcoin wallet?

A bitcoin wallet is a software program that runs on a computer or a dedicated device that provides the functionality required to secure, send and receive bitcoin. Counterintuitively, the bitcoin itself is not stored in a wallet. Instead, the wallet secures the cryptographic keys — essentially a very specialized type of password — that proves the ownership of a specific amount of bitcoin on the Bitcoin network.

Anytime a bitcoin transaction is executed, ownership of the bitcoin transfers from the sender to the recipient, with the network designating the recipient's keys as the new "password" for accessing the bitcoin.

Bitcoin uses a system called public-key cryptography (PKC) to preserve the integrity of its blockchain. Originally used to encrypt and decrypt messages, PKC is now commonly used on blockchains to secure transactions. This system allows only individuals with the right set of keys to access specific coins.

There are two types of keys required to own and execute bitcoin transactions: A private key and a public key. Both keys are strings of randomly generated alphanumeric characters used to encrypt and decrypt transactions. On the

bitcoin network, PKC implements one-way mathematical functions that are easy to solve in one way and almost impossible to reverse.

The blockchain uses the one-way mathematical algorithm to create a public key from the private key. With this, it is practically impossible to regenerate the private key from the public key, meaning you'd better not lose your keys (or forget your password to access them). Also, you will receive a public address, which is simply the hashed or shorter form of your public key.
This address functions similarly to a house address and is shared to receive bitcoin. On the other hand, the private key must be kept hidden from prying eyes, just as your debit card's PIN is meant for your eyes alone.

To execute transactions, you are required to use your private key and public key to encrypt and sign your Bitcoin transactions. Also, you have to include the public address of the recipient. With this, only the recipient with the right private key can unlock or claim the transferred bitcoin.

What are Bitcoin ATMs and how do they work?

Like standard ATMs, Bitcoin ATMs are a type of electronic kiosk where customers can make financial transactions, but they're designed for cryptocurrency rather than cash. There are over 63,000 of these Bitcoin ATMs across the United States, according to research group How Many Bitcoin ATMs. Here's what you should know about them if you've ever considered using one.

What are Bitcoin ATMs?

Bitcoin ATMs, sometimes referred to as BTMs, are kiosks where customers can buy and sometimes also sell Bitcoin, a type of cryptocurrency. Bitcoin ATMs are owned and operated by third-party companies — two with the largest networks are Bitcoin Depot and Coinme.

To use a Bitcoin ATM, customers can insert cash or a debit card to exchange their traditional currency for Bitcoin currency. While Bitcoin ATMs are generally accessible to everyone, they may require that the customer have an existing account with the Bitcoin ATM operator.

Cryptocurrency (including Bitcoin) is not connected to a bank account and is entirely virtual, utilizing blockchain technology. That means that when currency is exchanged at a Bitcoin ATM, it does not appear in a bank account or as cash, but rather it is transferred into a separate, digital Bitcoin wallet.

Bitcoin ATMs can be located using the Bitcoin website.

How to use a Bitcoin ATM

What's common to all Bitcoin ATMs is that you can use them to purchase Bitcoin by exchanging traditional currency for it. You'll need a cryptocurrency wallet, which is where the Bitcoin is stored, since the digital currency is not tied to a bank account. Once the amount of cash you want to exchange for Bitcoin is inserted into the ATM, you can enter your wallet's address or QR code into the machine. The cash will be exchanged for Bitcoin at the current market rate and sent to your digital wallet.

Some Bitcoin ATMs are bidirectional, meaning you can both purchase and sell Bitcoin at them. In the latter case, you can enter the amount of Bitcoin you'd like to exchange for cash and collect the cash or have it deposited onto your debit card.

Bitcoin ATMs can also be used to send Bitcoin to another person. Instead of entering your crypto wallet address, you enter the wallet address of the person you'd like to send the Bitcoin to, and then the Bitcoin you purchase will be deposited into their wallet.

In some cases, and depending on the purchase amount, you may need to provide a form of ID by scanning or taking a picture of it at the machine before completing the currency exchange.

Bitcoin ATM fees

Bitcoin ATMs have gotten some flak recently for charging high transaction fees. Truthout, a nonprofit organization, reports that Bitcoin Depot ATMs may charge up to 20 percent in exchange fees and don't disclose the total cost to customers.

Most Bitcoin ATM transaction fees fall between 5 and 15 percent of the total amount. By contrast, it's easy to find online cryptocurrency exchanges with transaction fees of less than 1 percent.

In addition to transaction fees, some Bitcoin ATM operators may charge a variable miner fee. This fee is used to pay Bitcoin miners, who add Bitcoin transactions to the blockchain to validate them.

Before using a Bitcoin ATM, make sure to research potential fees charged and look for the lowest fees.

Benefits and risks of Bitcoin ATMs

Benefits:

Ease of access: Because cryptocurrency isn't tied to a central system, anyone can buy or trade it, regardless of whether they have a bank account. The widespread availability of Bitcoin ATMs make it easy to buy (or sell) Bitcoin by trading in cash.

Privacy: Bitcoin ATMs often don't involve sharing your personal information, though in some cases they require you to scan an ID before completing a transaction.

Ability to sell Bitcoin: Some Bitcoin ATMs come with bi-directional functionality, so customers can also use them to sell Bitcoin.

Risks:

High transaction fees: The transaction fee for exchanging currency at a Bitcoin ATM can range anywhere from 5 to 20 percent. Meanwhile, there are online cryptocurrency exchanges charging less than 1 percent in transaction fees.

Lack of cryptocurrency options: Typically, Bitcoin ATMs only allow you to trade cash in for Bitcoin. If you're looking to buy other types of cryptocurrency, you'll likely need to go to an online crypto exchange.

Frequent target for scams: One of the downsides to the anonymity and accessibility of Bitcoin ATMs is that they can easily be taken advantage of by scammers and fraudsters. In 2021, the FBI noted an increase in scammers that directed victims to retrieve or send money through Bitcoin ATMs under false pretenses. If someone falls for a scam using a Bitcoin ATM, it's especially difficult to track down the scammer and recover funds.

Lack of protection: Bitcoin and other cryptocurrencies are not regulated by the federal government. That means that when you get Bitcoin from a Bitcoin ATM and add it to your digital wallet, it's not insured by the FDIC, as it would be in a bank account, to protect against theft or loss of funds.

Bottom line

If you're interested in trading in cash to buy Bitcoin — or in selling Bitcoin you already have — Bitcoin ATMs could be a convenient way to do so. They can be found all around the U.S., and you don't need to share any bank account information to use them. All that's needed is a cryptocurrency wallet.

Look out for the fees these ATMs charge, though, which can be high. It's also important to be wary of scammers, who often take advantage of the decentralized nature of Bitcoin ATMs. Make sure you only send money to those you know and trust.

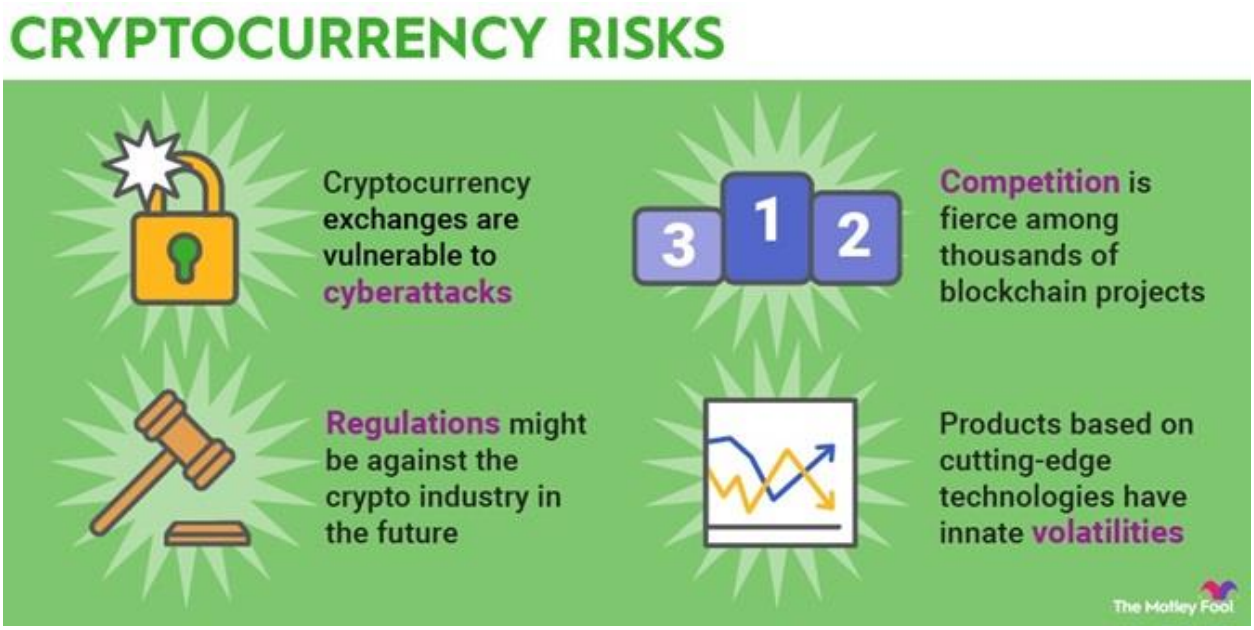
So, after researching bitcoins, do I think it is a good idea to invest money in bitcoins?

Well, I would not invest in bitcoins for the following reasons:

- **Too risky! See Cryptocurrency Risks Chart on next page.**
- **From what I can tell, buying bitcoins is more like gambling than investing.**
- **Best investing advice I could find is Index Funds.**

However, what do I know? I don't have any stocks.

You may make a lot of money buying bitcoins or you may lose it all. Each person must decide for themselves.



Reference

The best bitcoin reference I could find is a book titled "The Only Bitcoin Investing Book You'll Ever Need".

Bigdrifter44@gmail.com

Bigdrifter.com