**Bitcoin as Money and its History**

**Blockchain & Crypto Technology**

**Class Notes**

**Fall 2025**

[**Bitcoin: What is it? 2**](#_44yt0sus2oe8)

[Bitcoin as a digital currency 2](#_gzung9c27rx4)

[**How have bitcoins come to be seen as money? 3**](#_sy9l06ysnxui)

[What is money? 3](#_irsnwmsuz7nk)

[Forms of money 4](#_l8ugfty1avg0)

[Commodity money 4](#_lsji479bpqzu)

[Representative money 5](#_j0w714ft0423)

[Fiat money 5](#_olijkbe7t908)

[Barter 6](#_2dbmk3tj6wwl)

[Is bitcoin any of the different forms of money? 6](#_pnqss9jx0n9f)

[Features of money as per economists 10](#_zdhwfdgk51g2)

[Can bitcoin serve as a medium of exchange? 10](#_72rdjka7g9o4)

[Can bitcoin serve as a store of value? 13](#_ys1z1dnjlcmp)

[Can bitcoin serve as a unit of account? 15](#_qut6ey49csz)

[Does bitcoin possess the features of money? 16](#_ocm8wy4of6g4)

[Money as per sociologists 16](#_cvsfiujs67z7)

[Can bitcoin be seen as money as per the view of sociologists? 16](#_fniau9a7l0mc)

[**Motivation for Bitcoin 17**](#_dvpr8qji6vdn)

[Elimination of intermediaries 17](#_7uybbblv6z3i)

[Fees 17](#_n1ylwjsyxo0r)

[Censorship 18](#_z4ylvycs0rnk)

[Mistrust in fiat currencies 18](#_n87amcz8lvyg)

[**Unknown identity of Satoshi Nakamoto and disappearance 20**](#_baygr6iz8g9n)

[Avoiding conviction for criminal activity 21](#_vgx8pel4mx66)

[Avoiding the association with Silk Road 21](#_ln5e1sv9b71g)

[Protecting oneself as a wealthy person 23](#_al3xcjr6izx4)

[Protecting oneself from any retribution after moving markets 23](#_ozpfp2j4meao)

[To redirect attention to the currency and platform 24](#_9rxvgukuya1m)

[Protection from the middleman who is eliminated 24](#_cyubfvypp5st)

Chatbot for these classnotes: <https://chatgpt.com/g/g-68afaf2892b8819194d4785d94b33aa4-chatbot-for-bitcoin-as-money-its-history>

## Bitcoin: What is it?

Bitcoin is both a platform and a digital currency. When referring to it as a platform, which includes the network and the protocol that enables the digital currency, we use Bitcoin -- that is, with uppercase B -- and when referring to it as a unit of currency, we use bitcoin -- that is, with lowercase b.

In today’s class, we will largely focus on the digital currency, i.e., bitcoin. Eventually, we will get to Bitcoin as a platform.

### Bitcoin as a digital currency

Bitcoins are created using a particular software present on a network of computers worldwide. It is an [open source software available to anyone to download](https://bitcoin.org/en/download) and install. Once they do that and start using it, they become a node on the Bitcoin network that keeps the digital currency going.

* One computer with Bitcoin software is sufficient to create and keep a record of the currency. This is what happened when it started. However, when there is no one else to transact with, the currency would have no value and the record-keeping cannot be trusted. Therefore, for it to be valuable, you need more than one node on the network. These days we find over [23K nodes at any time](https://bitnodes.io/). These vary depending on the value of bitcoin. A year ago this time, we had about 19K nodes (we had about 16K two years ago this time).
* Because of the use of cryptography techniques to enable its use and to keep a record, it is also referred to as a cryptocurrency.
* The unit of currency is bitcoins or BTC. Each BTC is equal to 100M Satoshis.
* There is no entity that authorizes the currency's creation. In other words, it is not issued by any entity.
* Every 10 minutes or so, 3.125 BTCs get created. In about 4 years from April 2024, only 1.5625 BTCs will be created every 10 minutes or so. Four years after that, the number will halve, and so on.
  + The whole creation process started with the genesis block that generated 50 BTCs.
    - For unknown reasons, the next block with 50 BTCs occurred 6 days after the genesis block. Subsequently, blocks and the BTCs in them have been generated with an average gap of 10 minutes.
  + For a few days since the start (on Jan 3, 2009), it was only Satoshi Nakamoto who was running the software. Then someone else joined the network on Jan 12, 2009.
  + Since there were only a few others on the network during the initial days, those who ran the initial nodes accumulated a lot of bitcoins.   
    - Satoshi Nakamoto accumulated about 1M BTCs before disappearing in April 2011.
    - It is said that many just did not care about the BTCs they accumulated initially and have lost them.
    - It is **estimated** that about 3M to 4M BTCs have been lost forever. Of course, this figure also includes those who wanted to keep their BTCs but have forgotten or lost the passwords to be able to use them.
  + In a future class, we will learn who gets to keep the BTCs that get created (or are mined) every 10 minutes or so.
  + About 19.91 million BTCs have been ‘mined’ so far (see [graph](https://www.blockchain.com/charts/total-bitcoins)). (the number was 19.75 million a year ago this time)
* In all about 21M BTCs will be created. No additional BTCs will be created after that. This is expected to happen in 2140.
* You typically have to pay a transaction fee when you give bitcoins to anyone. It is not mandatory but in case you don’t add a transaction fee to your submitted transaction, it may not go through. We will learn more about this in a future class.

## How have bitcoins come to be seen as money?

For us to understand that, we need to first understand what money is and then examine how bitcoins relate to what we understand as money.

### What is money?

There are at least three different ways in which we can answer this question.

* One way to answer the question of ‘what is money’ is to look at forms of money over man’s history.
* The second way to answer this question is to look at features of money as described by economists.
* The third way is to look at how sociologists have attempted to understand money.

We can then see if bitcoins qualify as money from those different viewpoints.

#### Forms of money

Money has taken various forms in the history of man.

##### Commodity money

With commodity money, the terms of payment amount to something like this: I'll pay you with something that is intrinsically valuable and is valued by many.

* + That thing which is intrinsically valuable and is valued by many is considered as money. Some examples:
    - Cattle
    - Grain
    - Precious metals, such as gold and silver.
    - Rai stones – these are stone discs, some of which are human sized or even larger, in the Micronesian island of Yap. ([article](https://www.bbc.com/travel/article/20180502-the-tiny-island-with-human-sized-money))



* + The intrinsic value of the commodity arises from its usefulness for people outside of its usefulness as a medium of exchange. In other words, it is useful for purposes other than people seeing it as money.
    - Cattle may be useful for milk, meat, and for work on the farm.
    - Grains are edible.
    - Precious metals are useful as jewelry or as a manufacturing raw material.
    - Though there is a debate about whether Rai stones are commodity money or fiat money (i.e., something that is decreed by the government as legal tender), it has been argued that Rai stones have symbolic value outside their use as currency. For instance, rounder Rai stones have religious significance and are used in religious ceremonies. They were also more valuable if there was an interesting story about their extraction and transportation via canoe from the island of Palau to Yap. The more difficult and interesting their extraction and transportation, the greater was its value. Indeed, when a European explorer found a more efficient way to extract the stone, its value dropped.

##### Representative money

With representative money, the terms of payment amount to something like this: I'll pay you with something that has a claim on a thing with intrinsic value.

* You have some form of a token that has no value but it can be exchanged by the issuer for something intrinsically valuable. For instance, prior to 1971, the US dollar bill could be exchanged by a representative of the US Treasury for an equivalent amount of gold.
  + Hence, the US dollar bill (or any other US currency bill) at that time was representative money.

##### Fiat money

With fiat money, the terms of payment amount to something like this: I'll pay you with something that is not linked to anything valuable but has been decreed as a legal tender by the government.

* You have something with no intrinsic or representative value but which has been decreed by the government to be a legal form of exchange. The government expects taxes to be paid to it in fiat money.
* The US dollar is fiat money as are the currencies of Canada, China, Great Britain, Russian, India, etc.

Now that we have defined fiat currency, it is time to consider a broader (though incorrect) definition of representative money used by some. They consider a token that has a claim on something that is intrinsically valuable or decreed as fiat currency as representative money. Thus, a money order can also be considered as representative money. However, it is not a genuine representative money because it does not have a claim on something intrinsically valuable.

##### Barter

With barter, the terms of payment amount to something like this: Let us directly exchange different things of value.

For example:

* A farmer may trade a sack of rice with a carpenter in return for repairing a broken door. Neither rice nor carpentry service is “money,” but both have value, so they are directly exchanged.
* In a modern setting, two professionals might exchange services – such as a web designer creating a website for a dentist in return for free dental care. Again, no money is involved, but each party provides something the other values.

As the above terms of payment suggest, barter is not really a form of money but a substitute. We are nevertheless including it in the discussion about forms of money because such a discussion often includes barter.

Barter is often discussed in relation to money because it highlights the limitations that money can overcome. Barter requires a “double coincidence of wants”: both parties must want what the other is offering at the same time. Money eliminates this problem by providing a widely accepted medium of exchange.

##### Is bitcoin any of the different forms of money?

Let us see if it fits into any of the forms of money.

* It does not have any use outside its use as money or a financial instrument. Therefore, it cannot be commodity money.
* It is not a “genuine” representative money. It wasn’t created as a token for something intrinsically valuable. Nor is it representative money as per the broader definition of such money because it was not created as a token with a claim on fiat currency.
* In general, it is not fiat money. It was not decreed as official currency by any government when it was created.

At one point, however, two countries did decree bitcoin as fiat currency. El Salvador adopted bitcoin as legal tender on September 7, 2021, alongside the U.S. dollar. The Central African Republic followed in April 2022. In both cases, bitcoin qualified as fiat money because it was legal tender by government decree.

That is no longer the case. The [Central African Republic repealed its bitcoin legal tender law](https://www.demandsage.com/crypto-legal-countries) in March 2023 as part of alignment with a monetary union it formed with other nations. El Salvador, under pressure from the IMF, [dropped bitcoin as official currency](https://finance.yahoo.com/news/el-salvador-changes-bitcoin-rules-164742636.html) in February 2025.

Thus, today no country recognizes bitcoin as fiat money.

How well did bitcoin work as a fiat currency?

Let us examine the case of El Salvador.

* + Motivations for why El Salvador decreed bitcoins as official currency  
    - A belief that it will foster more and cheaper financial services. Specifically, it was expected to lower the cost of making remittances by El Salvadorians who are working abroad and send money to their families in El Salvador. These remittances are a major part of the El Salvadoran economy – about 25% of the GDP, and transaction fees average about 10.2% for physical transfers ([article](https://nupoliticalreview.org/2024/02/28/the-truth-behind-bitcoin-country/)). Although online bank transfers are less expensive, only about 11% of the population has mobile accounts.
      * This has not materialized. Only 1.7% of remittances in 2022 were via cryptocurrencies ([article](https://www.merit.unu.edu/el-salvador-bitcoin-policy/)), even though they promised lower transaction fees of only a few percent of the remitted amount.
    - A belief that it will lure foreign investors to develop geothermal power from volcanoes to supply the large amounts of electricity needed for mining the cryptocurrency. Geothermal power has the advantage of being green.
      * There is a potential in El Salvador to use geothermal energy to mine cryptocurrency. It has 170 volcanoes. In May 2024, [Reuters reported](https://cointelegraph.com/news/el-salvador-mines-bitcoin-volcanic-energy) that El Salvador had mined 471 bitcoins since 2021 by diverting 1.5MW from a 102MW state-owned geothermal power plant.
      * However, El Salvador has not succeeded in attracting foreign investors for using geothermal energy to mine cryptocurrency. This idea may have been doomed for failure from the get go. Only about 27% of energy generation in El Salvador makes use of geothermal sources. It requires expensive infrastructure — besides requiring water which is in short supply in El Salvador — and is less preferred to fossil fuels which end up being cheaper ([article](https://www.rollingstone.com/culture/culture-features/el-salvador-bitcoin-law-volcano-bonds-nayib-bukele-1388472/)).
      * This idea was not abandoned completely. A public-private partnership in El Salvador to build a power generation park was announced. This park was expected to harness renewable sources – solar and wind power in addition to geothermal power – and provide 241 megawatts of energy for bitcoin mining. As part of this initiative, a mining pool called Lava Pool went live in October 2023 ([article](https://bitcoinmagazine.com/business/volcano-energy-bitcoin-mining-pool-goes-live)).
    - A belief that doing so will project an image of El Salvador as a country that wants to be ahead when it comes to innovation.
      * It is not clear how El Salvador is faring on this dimension. The public-private partnership mentioned above was expected to raise $1B via a bond issue. The bond issue was meant to be a test of how people see El Salvador in terms of innovation. However, $250M were raised but not via bonds. Therefore, we don’t have clarity on how people are viewing El Salvador on the dimension of innovation.
      * However, there is also some evidence that El Salvador is being seen as an innovative country. Some time back, Argentina looked to El Salvador for guidance on bitcoin adoption, highlighting El Salvador's pioneering approach to integrating cryptocurrency into a national economy ([article](https://www.benzinga.com/markets/cryptocurrency/24/05/39036114/argentina-seeks-guidance-from-el-salvador-on-bitcoin-adoption)). Even Panama considered El Salvador as a model for cryptocurrency adoption.

There were some positive outcomes for El Salvador that, while not directly tied to the initial motivation for legalizing bitcoin, stemmed from the decision to legalize bitcoin as official currency:

* To support the adoption of bitcoin, El Salvador created bitcoin reserves. A wallet linked to the Salvadoran government has been purchasing one bitcoin daily since March 16, 2024. This steady acquisition has seen the country’s reserves rise to about $770 million as of August 2025 ([article](https://news.bit2me.com/en/770-million-in-BTC-reserves-in-El-Salvador-after-rally)). In the long run, as the value of these holdings increases, they have the potential to strengthen El Salvador’s economy and enhance its global standing.
* The initiative has also boosted tourism. A year ago, the U.S. Department of State reported that bitcoin legalization helped attract cryptocurrency enthusiasts and increased El Salvador’s international visibility. Between 2019 and 2023, the country became the fourth fastest-growing tourism destination, recording a 35% increase in visitors. In 2024 alone, tourism was projected to rise by another 22% year over year ([article](https://www.onesafe.io/blog/el-salvador-bitcoin-tourism-crime-impact)).

While there are some positives in El Salvador’s adoption of bitcoin as a legal currency, the overall sentiment is that El Salvador does not seem to have fared well in its experiment ([article1](https://www.nytimes.com/2022/07/05/world/americas/el-salvador-bitcoin-national-currency.html), [article2](https://insights.som.yale.edu/insights/el-salvador-adopted-bitcoin-as-an-official-currency-salvadorans-mostly-shrugged)). In addition to citing the above described challenges, people cite the following as evidence to make the case that the experiment has not succeeded.

Specifically, a year into the experiment,

* only 2% of its population was using the Chivo wallet, which was downloaded by about 60% of its population. Each person who downloaded the wallet had received $30 as a stipend for downloading the wallet.
* Only 14 percent of the country’s businesses had made bitcoin transactions since it was introduced.
* Only 3 percent said they perceived any business value in it.

However, the supporters of the initiative did not give up.

* They claimed that we have to be patient and give time for the experiment to bear fruit. (article [1](https://bitcoinmagazine.com/culture/these-trends-show-bitcoin-is-becoming-our-futures-money), [2](https://cointelegraph.com/news/dips-be-damned-el-salvador-is-stronger-because-of-bitcoin)).
* They engaged in measures, such as education, to increase the adoption of bitcoin. El Salvador launched Bitcoin training for 80,000 civil servants ([article](https://cryptoslate.com/el-salvador-launches-bitcoin-training-for-80000-public-servants/)). This initiative aimed to equip public sector employees with the necessary knowledge to handle bitcoin-related transactions and services. By providing this training, El Salvador hoped to streamline the use of bitcoin in various governmental functions and promote broader acceptance of the cryptocurrency among the population.

However, as part of an agreement with the IMF for a $1.4 billion loan, El Salvador amended its law that had decreed bitcoin as fiat currency. Whether the measures taken to salvage bitcoin adoption would have succeeded remains unknown.

One way to understand the overall failure of El Salvador’s push for bitcoin is by examining the nature of its initiative in light of bitcoin's underlying philosophy. El Salvador’s effort was a centralized initiative, which runs counter to bitcoin decentralized philosophy. This mismatch may well explain much of the failure.

* For example, the Chivo wallet is a custodial wallet. In other words, someone else – in this case, the government – has custody of your bitcoins. This arrangement allows the government to track transactions and even censor activity. Reports indicate that the Salvadoran government froze the wallets of individuals who had received transactions from Wasabi, a bitcoin wallet that enables users to mix their unspent coins with those of others. Such mixing is typically done to prevent transaction tracing and preserve privacy ([article](https://news.bitcoin.com/reports-claim-chivo-bitcoin-wallet-is-flagging-wasabi-transactions-in-el-salvador/)).

In sum, bitcoin remains outside the traditional categories – neither commodity, representative, nor fiat money.

#### Features of money as per economists

Economists define money as something that has the following three features:

* It is a medium of exchange
  + You can use money to exchange it for something else. Others are willing to exchange what they have for the money that you give them.
* It is a store of value
  + Money retains its value over time. You can be reasonably confident that it will retain its purchasing power over time.
* It is a unit of account
  + You can use money to count what you own or you owe to others. You can use it to calculate the value of something. To enable this, money is divisible, countable, and fungible (i.e., you can exchange a unit of money with another unit of it without losing or gaining anything).

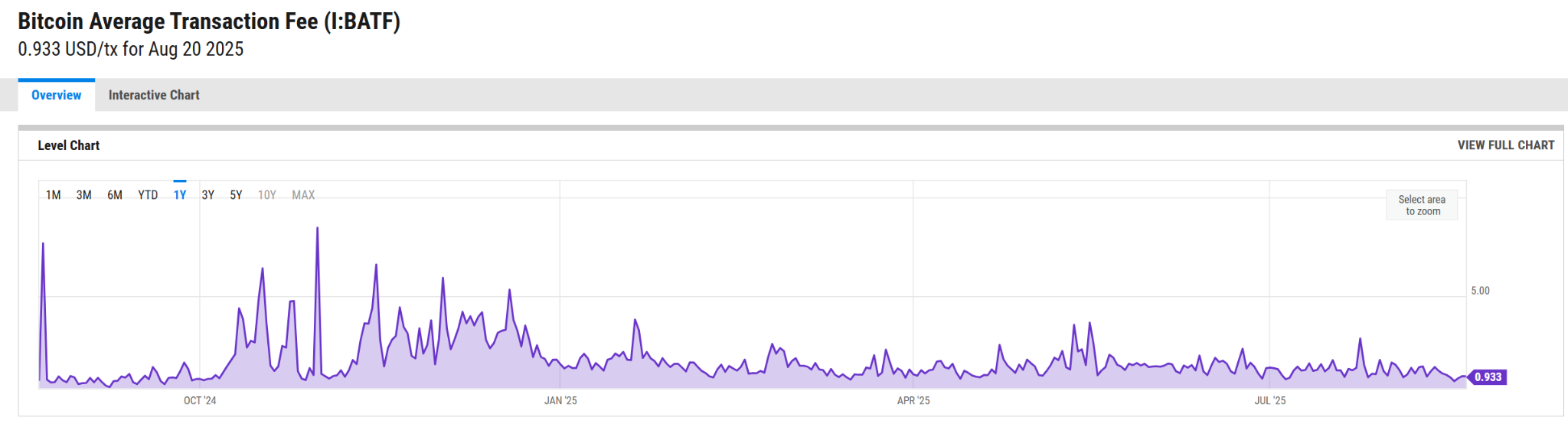
Does bitcoin qualify as money on the basis of these features? It does to some extent on at least two of them.

##### Can bitcoin serve as a medium of exchange?

It is a reasonably good medium of exchange. See [this video](https://www.youtube.com/watch?v=n9MXX6dXKPM).

What is contributing to making bitcoin as a medium of exchange? (or, what is making bitcoin attractive as a medium of exchange?)

* No intermediary or third party is involved. There are two outcomes of this.
* First, there is no one to control the fees. They are determined by supply and demand of transaction processing on the network. The advantage of market forces determining the fees is that you can expect the fees to be competitive.
  + To be sure, while the fees may be relatively low in proportion to value that is transacted, in dollar terms the fees have tended to be high in the past (e.g., in April 2024, they touched over $128). They are hovering mostly under $1 at the moment. Check out the [chart](https://ycharts.com/indicators/bitcoin_average_transaction_fee#:~:text=Bitcoin%20Average%20Transaction%20Fee%20is,61.59%25%20from%20one%20year%20ago.) for transaction fees.



However, there are ways to reduce the fees. One way to reduce transaction fees on the Bitcoin network is to use the Lightning network build on top of the Bitcoin network. It aggregates small transactions (between two parties) which are not recorded on the blockchain. Only when the aggregate amount reaches a certain level is the transaction recorded. View [video](https://www.youtube.com/watch?v=rrr_zPmEiME) about the Lightning network (there are inner details you probably won’t understand at this point in the course but you get a general idea; you will be assigned a reading in a future class to help you understand this better).

* Second, the potential for censorship is lower. When there is a third party, there is potential for censorship that can curb the currency's use. The third party can accept or reject your transaction. For example, as the video indicates, outflow of money from China is regulated and needs approval of authorities. A third party can also do other things besides restricting the types of transactions you can carry out: it can restrict who specifically you transact with, how much you can accumulate, and possibly other things too. These censorship actions don't occur on the Bitcoin network, thereby making it attractive as a medium of exchange.
* Anonymity on the Bitcoin network also makes it an attractive medium of exchange for some. To be sure, this includes bad elements but there may be others (i.e., good people) who care about their privacy and would not like to share what they do with their money with anyone.
* Another contributor to bitcoin as a medium of exchange is its increasing adoption. Adoption would be indicated by the number of holders of bitcoins. The more people there are who are willing to accept and transact in a particular currency, the better the currency is as a medium of exchange! However, it is challenging to estimate the number of holders of bitcoins because we don’t have a system of a single, unique identifier for each bitcoin holder (you will understand this challenge more easily when you learn more about the Bitcoin platform and how ownership of bitcoins is determined). We can only arrive at rough estimates, which can vary depending on how one studies this issue and the assumptions one makes during the study.
  + A Crypto.com study (thought to be among the more reliable ones) estimated that there were more than 219 million individual bitcoin holders in late 2022 compared to 183 million from a year earlier ([article](https://cryptonews.com/news/how-many-people-use-bitcoin.htm)).
    - A website called Bitbo (<https://bitbo.io/how-many-users/>) estimates that currently there are 106M bitcoin users.
  + Another way to estimate the number of users is by studying the number of wallets. The number of Blockchain.com wallets (which, by the way, are not the only way to own bitcoins) has gone up over the years (see [chart](https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users) – part of premium service and, hence, you may not be able to view it). Know that one can have an empty wallet too. Since the Blockchain.com wallet is non-custodial (i.e., a third party is not involved), we cannot know how many wallets are empty. Therefore, estimating bitcoin users by looking at the number of such wallets should be done cautiously.
    - Bitbo estimates that currently there are 200M bitcoin wallets.

One could argue that the above discussion reflects adoption in terms of holding bitcoin, which is different from adoption as a medium of exchange. On this front, there are signs that the infrastructure for spending bitcoin is expanding.

Specifically, the capacity of the Lightning Network, which we described earlier as a system built on top of Bitcoin to enable faster and cheaper payments – has steadily increased, showing more interest in using bitcoin for everyday transactions.

Major payment platforms such as PayPal, Visa, and Mastercard have also integrated bitcoin, allowing users to make purchases at millions of merchants (though these payments are usually converted to local currency at the point of sale). However, purists may argue that this undermines the very idea of Bitcoin as a medium of exchange, since it is not being transferred directly between buyer and seller but is instead routed through the fiat system.

* PayPal, Visa, and Mastercard allow bitcoin holders to pay at millions of merchants, but the cryptocurrency is instantly converted into local fiat currency (e.g., U.S. dollars) at the point of sale. The merchant receives payment in their local currency, insulating them from bitcoin’s volatility and removing the need to hold or manage it. In this sense, such payment solutions do not make bitcoin a direct medium of exchange between consumer and merchant. Rather, they act as a bridge, increasing bitcoin’s utility and liquidity for everyday spending by embedding it into traditional financial infrastructure. At the same time, this example helps clarify what it means for something to function as a medium of exchange: a currency serves this role only when it is directly accepted between transacting parties, without the need for conversion into another form of money.

##### Can bitcoin serve as a store of value?

Bitcoin has increasingly been viewed as a potential store of value for a variety of reasons, ranging from its use as a hedge against inflation, to its similarities with gold, to the growing role of institutional investment through spot ETFs.

Bitcoin as a hedge against inflation

I have come across cases where it made sense for people to use it as a store of value. For example, Argentinians were seeing bitcoin as a better store of value when compared to their country’s currency, the peso, which has tended to fluctuate more than the state of Argentina’s economy. See [this video](https://www.youtube.com/watch?v=s7tzuE9kQeQ).

* In a certain province of Argentina (Mendoza), one can pay their taxes in bitcoin! ([article](https://en.cryptonomist.ch/2022/08/30/argentina-mendoza-now-accepts-bitcoin-to-pay-taxes/)). In other words, it is also becoming a better medium of exchange in Argentina!

So, bitcoin is emerging as a store of value for some because it can act as a hedge against wild currency fluctuations.

Similarity to gold

Some argue that bitcoin is like gold on a variety of features. Since gold is a good store of value because of those features, they argue that bitcoin may also emerge as a store of value in the long run.

What features of gold contribute to it being a good store of value?

* Gold has a limited supply.   
  + Easy gold has already been mined and the level of production of gold has essentially plateaued. It is challenging to access whatever gold remains to be mined.
* Gold’s demand is steady or increasing.  
  + We also know that the demand for gold is not coming down. If anything, it is increasing. It is needed for production of many things we use in our daily lives (jewelry, electronics, and health equipment).
* Gold’s value is not under the control of any government.  
  + It is, therefore, protected from uncertainty in a government’s actions. For instance, it cannot be devalued by a government. Or a government cannot make more of it.
* Gold and its value are portable.  
  + You can carry it with you and it tends to be valuable across borders.

Bitcoin can be argued to be similar to gold on these features.

* It is scarce like gold. Only 3.125 BTCs are created every 10 minutes or so and, in all, only about 21M BTCs will be created. Like gold, most of the bitcoins have already been mined.
* Its use for transactions is expanding, supported by developments such as the Lightning Network and integration into payment platforms like PayPal, Visa, and Mastercard.
* It is not under the control of any government.
* It is portable and so is its value.

Those who adopt this line of thinking and see bitcoin and gold as similar argue that bitcoin, too, can serve as a store of value. When presented with the counter argument that unlike gold, bitcoin’s price is volatile, those who see bitcoin is similar to gold emphasize its long-term upward trajectory. In their view, volatility does not disqualify bitcoin but instead reflects the early stages of adoption. Over time, as the market matures and usage expands, bitcoin may come to function much like gold – a scarce, portable, and widely recognized store of value.

Approval of spot Bitcoin ETFs

Another important development that reinforces bitcoin’s image as a store of value is the approval of spot Bitcoin ETFs in major markets such as the U.S. Before this, investors only had access to futures-based Bitcoin ETFs, which did not hold Bitcoin directly but instead held contracts tied to its future price. These funds gave investors only indirect exposure to Bitcoin, and because the contracts expire and must be regularly replaced (“rolled over”), they often face extra costs and performance gaps compared to Bitcoin’s actual market price.

By contrast, spot Bitcoin ETFs hold bitcoin directly. This structure allows investors to track bitcoin’s price more accurately and gives institutional and retail investors a regulated, more accessible way to gain exposure without managing wallets or custody. By reducing barriers to entry and increasing demand, these ETFs strengthen the perception of bitcoin as a legitimate investment asset and potential long-term store of value.

Important clarification: The approval of spot Bitcoin ETFs did not make bitcoin itself a security.

* Bitcoin is a commodity. Like gold or oil, its value is determined by supply and demand. It is not issued by an entity that promises profits.
* A security, by contrast, is an investment contract. Under the Howey Test in U.S. law, something is a security if people invest money with the expectation of profit that comes primarily from the efforts of others (e.g., stocks in a company).
* ETF shares are securities. When you buy a share in a Bitcoin ETF (or gold ETF), you are not buying the commodity directly. Instead, you are buying a security issued by the ETF sponsor, who manages the holdings on your behalf. Your profit depends partly on the sponsor’s efforts to store, safeguard, and administer the asset.

So, the ETF itself is a security, but the underlying asset – bitcoin – remains a commodity. This is the same logic that applies to gold: gold is a commodity, but shares in a gold ETF are securities.

In sum, the above discussion suggests that bitcoin is increasingly being positioned as a store of value. Its role as a hedge in unstable economies, its frequent comparison to gold, and its growing acceptance through financial instruments like spot ETFs all point to its rising legitimacy. These developments indicate that more individuals and institutions are beginning to treat bitcoin as “digital gold.”

At the same time, there are good reasons why bitcoin has not yet proven to be a universally dependable store of value. Its price volatility is far greater than that of traditional assets, making it difficult to rely on for preserving purchasing power. Adoption as a safe-haven asset remains patchy, mostly concentrated in countries facing currency crises rather than across stable economies. Regulatory uncertainty also limits confidence, as governments continue to debate how bitcoin should be treated legally. Finally, bitcoin depends on digital infrastructure, making it more fragile than tangible assets like gold. These limitations mean that, while it is increasingly being perceived as a store of value, it is not yet universally accepted as one.

##### Can bitcoin serve as a unit of account?

Technically it can. But, in reality, it does not serve as a unit of account. Much of what we do in any country gets accounted for in that country's currency. For instance, in the US, we keep our accounts in the US dollars. Even when bitcoin was a fiat currency in El Salvador, people continued to use the US dollar as a unit of account. In fact, Article 6 of El Salvador’s Bitcoin Law stated ”For accounting purposes, the USD will be used as the reference currency.” ([article](https://www.cato.org/blog/bitcoin-law-counterfeit-free-choice-currency))

One reason bitcoin is not widely used as a unit of account is its high volatility. If a business kept its books in bitcoin, the value of revenues, costs, and profits would swing wildly with bitcoin’s price, making financial reporting unreliable.

##### Does bitcoin possess the features of money?

In sum, at this point, when one considers bitcoin vis-a-vis the features of money, it can be considered to be an emerging currency. It seems to be a reasonable medium of exchange. There are certain use cases where it can be a reasonable store of value. However, at this point there does not seem to be any evidence of bitcoin as a unit of account.

#### Money as per sociologists

For sociologists, for something to be considered as money ([article](https://journals.sagepub.com/doi/full/10.1177/02632764211049826)):

* There is a belief within the community that others would accept it for trade purposes.
* It is not necessary for it to have any usefulness besides its use for conducting business. Its value comes from the level of desire or demand for it.
* There is a wide enough economic community that uses it. The wider the economic community that uses it, the stronger is its role as money. We see that with the US dollar. It is accepted as an international currency almost everywhere.

From this perspective, money is a social institution based on belief and trust, not just a commodity with intrinsic value or a currency decreed by the state.

##### Can bitcoin be seen as money as per the view of sociologists?

Yes. Specifically, we see the following with bitcoin:

* Right from a few years after the implementation of bitcoin, there has been a community that has believed in bitcoin as money and has used it for trade. The online Silk Road marketplace made this community grow. By the time this marketplace was taken down, there were many others outside this marketplace that were believing bitcoin as money. That community has only grown.
* It does not have any usefulness outside its use as money. But that is fine as per the view of sociologists.
* Like the US dollar, the community of bitcoin users is wide as they transcend geographic borders.   
  + It is believed that Russia is skirting many of the international sanctions by making use of bitcoin. In fact, Russia approved a law allowing use of crypto for global payments as it faced sanctions ([article](https://www.cnbc.com/2024/07/30/russia-considers-legalizing-crypto-as-a-form-of-payment-amid-sanctions.html)).

Sociologists emphasize that bitcoin functions as a social institution built on belief and trust. They argue that demand for something like bitcoin is likely to grow because it was created to challenge the state’s control of money. People seek an alternative to fiat currency as trust in governments that issue it continues to erode. Moreover, as geographic borders become less relevant for global trade, the need for a currency that is seamlessly accepted across the world becomes stronger. Bitcoin fits that role well.

## Motivation for Bitcoin

Since we already had money, why did we need another form of money? What was the motivation for its creation? Our discussion since our first meeting provides some answers. We will revisit those in a more coherent way. These motivations also suggest why Satoshi Nakamoto disappeared as soon as bitcoin started to get adopted.

There are at least two reasons that are often cited as motivations for creating Bitcoin.

### Elimination of intermediaries

Many business and personal transactions involve intermediaries. Most of the time, we don't work with cash. We are using checks, credit cards, or electronic payment systems. All these involve a trusted third party such as the bank, the credit card company (e.g., Visa, MasterCard, American Express, etc), or a company such as PayPal. There are two issues that arise due to intermediaries: fees and censorship

#### Fees

The third parties have considerable market power due to which they charge significant fees which customers end up paying either directly or indirectly.

* Visa and Mastercard are among the most profitable companies in the world, with net margins in 2023 of 57% and 43% respectively

Theoretically speaking, Bitcoin was supposed to reduce fees by eliminating powerful third parties. While we do not have a few, powerful third parties, we nevertheless have other actors in the Bitcoin world (e.g., those running the nodes) who play a part in the demand and supply dynamic on the Bitcoin platform that determines transaction fees (we will learn about these actors later). There are times when the dynamic produces high prices and makes using bitcoin to pay for something inefficient compared to using a credit card. For instance, consider paying a transaction fee of around $3.65 on May 16, 2025 for a Starbucks coffee as opposed to 2.5% when using a credit card.

However, saving fees was a relatively weaker motivation in comparison to the motivations cited below.

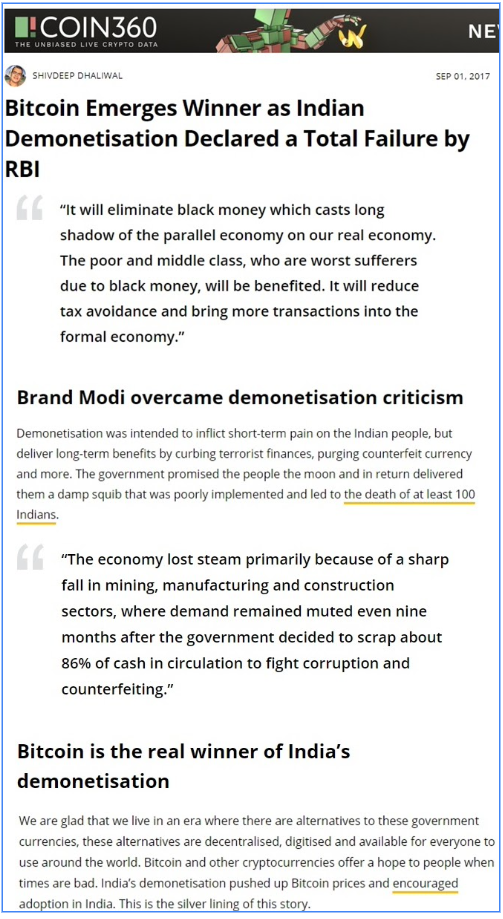
#### Censorship

As indicated earlier, having a third party implies the possibility of censorship. For instance, after Wikileaks released damaging secrets about the functioning of the US government, the government worked with third parties such as Visa, MasterCard, and PayPal to not allow Wikileaks to collect donations via credit cards or PayPal. Donations immediately dried up by 90%. With bitcoins, there is no such censorship.

### Mistrust in fiat currencies

Rulers and governments are known to debase their fiat money.

* For instance, rulers who used commodity money based on the amount of gold or silver in them have been known to reduce the amount of the precious metal used while trying to keep the value of the coins the same. That would result in people hoarding the older coins and taking money out of circulation or creating a black market for older coins.
* Governments try to improve the economy by increasing the supply of money (e.g., quantitative easing by the US in the wake of 2008 financial crisis and 2020 Covid pandemic). Many times, as in the case of the 2008 financial crisis, this may be stimulated by actions of the government to save big financial institutions that took and encouraged risky actions. While the financial institutions were almost made whole, the common man paid for their actions that were encouraged by the financial institutions’ risky behavior. Furthermore, when the supply of fiat money increases, its value goes down, which affects the buying power of the common man.
* Some governments also demonetize their currency, like it happened in 2016 when India suddenly demonetized Rs. 500 and Rs. 1000 currency bills. That not only led to drop in economic activity and hardship for many, it also led to deaths for many as they stood in lines trying to exchange demonetized bills for valid currency or they were refused medical treatment that they sought with demonetized currency (see [article](https://medium.com/rootnews/financial-genocide-how-the-demonetisation-policy-killed-105-people-899b50f2f77e) about people dying in India in the wake of demonetization; also see the following montage from an [article](https://cointelegraph.com/news/bitcoin-emerges-winner-as-indian-demonetisation-declared-a-total-failure-by-rbi) that appeared about 10 months after the demonetisation move).



Bitcoin was created to protect against actions of rulers and governments that are not good for the common man. It offers a way by which people can take matters into their own hands and not suffer as a result of government actions that are often seen as capricious and favoring a selected set of people. Offering that way was a major motivation behind its creation.

See this [video](https://www.youtube.com/watch?v=55KyJl8faNY) for how Venezuelans are using bitcoins to counter the actions of the government (another [video](https://youtu.be/X8JmdtULfwI?si=CTPnFAadr3k7bU27)).

* The highlighted video was made in 2016 but bitcoin continues to be used in Venezuela to protect against inflation and the challenges in sending remittances into Venezuela ([article](https://www.reuters.com/technology/venezuelas-economy-regresses-crypto-fills-gaps-2021-06-22/)).

## Unknown identity of Satoshi Nakamoto and disappearance

We don’t know who Satoshi Nakamoto is. We know that the entity behind the name speaks very good English -- this is evident from the discussion forums.

There have been many attempts and speculations to uncover the identity of Satoshi Nakamoto. For instance, in 2014 Newsweek had a [cover story](https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html) on who Satoshi Nakamoto might be and it caused quite a frenzy. The person who Newsweek identified as Satoshi Nakamoto released a statement saying that he is not the Satoshi Nakamoto who created Bitcoin.



Some have even claimed that they are Satoshi Nakamoto. However, at this point, it would be appropriate to say that the identity is a mystery.

Instead of coming forward to be celebrated as an inventor, why do you think Bitcoin’s inventor has chosen to remain anonymous and has disappeared?

See [video](https://www.youtube.com/watch?v=Bze53qwHS8o). The video gives us some motivations but there are additional potential motivations.

The following is a more complete (but not necessarily exhaustive) list.

### Avoiding conviction for criminal activity

When you create a new currency, it can rise to compete against a country's official currency. Governments don't like that and they outlaw the creation of any new currency. You can be convicted for criminal activity as it happened in the case of [Bernard von NotHaus](https://www.nytimes.com/2012/10/25/us/liberty-dollar-creator-awaits-his-fate-behind-bars.html) ([Wikipedia article](https://en.wikipedia.org/wiki/Bernard_von_NotHaus)) who was convicted by the US for creating Liberty Dollars. Satoshi may have feared such an action and, therefore, stayed anonymous and eventually disappeared.

Gavin Andersen, who worked closely with Satoshi Nakamoto on the development of Bitcoin software, believes that the fear of arrest by authorities may be the reason why Satoshi Nakamoto was evasive about his identity from the start. The Newsweek article referred to earlier quoted Andresen as saying the following about Satoshi Nakamoto: "Back then, it was not clear that creating Bitcoin might be a legal thing to do. He went to great lengths to protect his anonymity."

### Avoiding the association with Silk Road

Bitcoin facilitated the rise of the Silk Road marketplace (and, also, vice versa) which was launched in February 2011, a few months before Satoshi Nakamoto's disappearance. The Silk Road enabled bad elements in society to flourish. No good government would like that.

* Maybe, Satoshi Nakamoto feared that since bitcoin facilitated the Silk Road, governments were likely to go after its creator. If for nothing else, they would like to investigate if the creator is in cahoots with the bad elements because they stood to benefit from the popularity of the marketplace.
  + Such a fear would not be unfounded because we know that the US government went after the creator of Silk Road, Ross Ulbricht ([recent video about Ulbricht after his pardon](https://www.youtube.com/watch?v=mgRIo7KA848)).
  + Incidentally, someone did try to link Satoshi to the Silk Road but this [link was eventually not believed](https://www.computerworld.com/article/2486316/link-between--satoshi--bitcoin-account-and-silk-road-dissolves.html).

| **About the Silk Road marketplace (from ChatGPT)**  How was the Silk Road able to maintain anonymity?  The Silk Road marketplace, which operated on the dark web, made use of several technologies and practices to try to maintain the anonymity of its users. While these methods provided a degree of privacy, they did not make users completely immune to law enforcement actions. Here are some of the ways the Silk Road attempted to maintain user anonymity:  1. \*\*Tor Network\*\*: The Silk Road was hosted on the Tor network, which is designed to anonymize internet traffic by routing it through a series of volunteer-run servers. This makes it difficult to trace the source and destination of data, including the IP addresses of users accessing the website.  2. \*\*Bitcoin Transactions\*\*: Bitcoin was the primary currency used on the Silk Road. Bitcoin transactions are pseudonymous; they don't reveal the identities of the parties involved but are recorded on the public blockchain using alphanumeric addresses. Users could create Bitcoin wallets without providing personal information, adding a layer of anonymity.  3. \*\*Encrypted Communications\*\*: Users on the Silk Road communicated using encrypted methods such as PGP (Pretty Good Privacy) encryption. This protected the content of their messages and made it more challenging for third parties to intercept or decipher their communications.  4. \*\*User Pseudonyms\*\*: Buyers and sellers on the Silk Road used usernames or pseudonyms instead of their real names. This added an additional layer of anonymity.  5. \*\*Escrow System\*\*: The Silk Road used an escrow system, where funds from buyers were held in escrow until the buyer received the product and confirmed its quality. This reduced the risk of scams but made it more challenging for authorities to trace transactions directly to sellers.  6. \*\*Security Measures\*\*: The website employed various security measures to protect user information and transactions, making it more difficult for hackers to access sensitive data.  Despite these efforts to maintain anonymity, law enforcement eventually identified and arrested the site's creator, Ross Ulbricht, in 2013. His arrest and subsequent conviction demonstrated that even in the dark web, where anonymity is a priority, it is not foolproof, and law enforcement agencies can investigate and apprehend individuals involved in illegal activities.  It's important to note that the Silk Road was an illegal marketplace that facilitated the sale of drugs and other illegal goods and services. Engaging in such activities is against the law, and users who participated in illegal transactions on the Silk Road faced legal consequences if identified and prosecuted by law enforcement agencies.  How would users communicate their physical addresses to get the items shipped and yet maintain anonymity  Maintaining anonymity while sharing physical addresses for shipping on platforms like the Silk Road required users to take additional precautions. While it's important to note that such activities are illegal, some individuals still attempted to hide their identities. Here are some methods that were used to maintain a degree of anonymity:  1. \*\*Use a Drop Address\*\*: Many users on the Silk Road would employ what's known as a "drop address." This is typically a location that is not directly linked to the buyer's identity, such as an abandoned building or an empty house. The buyer could receive packages at this address without revealing their true location.  2. \*\*Cryptocurrency Tumbling\*\*: To further obfuscate the source of funds and maintain some level of privacy, users might employ cryptocurrency tumblers or mixers. These services mix multiple transactions together, making it difficult to trace the origin of the funds used for the purchase.  3. \*\*Encrypted Communication\*\*: Buyers and sellers may continue to use encrypted communication, such as PGP encryption, to exchange shipping details. This helps ensure that the information shared remains confidential.  4. \*\*Use of Fake Names\*\*: Buyers might use fake names or initials when receiving packages to reduce the risk of detection.  5. \*\*Parcel Mules\*\*: Some users might employ third parties, known as "parcel mules," to receive packages on their behalf. These individuals are often paid to accept deliveries and forward them to the actual buyer, adding another layer of separation.  6. \*\*Access Points or Mailboxes\*\*: Some users may rent private mailboxes or access points, which can be used as a shipping address. These services often do not require users to provide personal identification, enhancing anonymity.  It's important to emphasize that engaging in illegal activities like purchasing illegal drugs online is both unethical and against the law. Law enforcement agencies actively work to combat such activities, and individuals involved in illegal online marketplaces can face serious legal consequences if they are identified and prosecuted.  Moreover, technology and law enforcement methods have evolved over the years, making it increasingly difficult for individuals to maintain anonymity in these types of transactions. The above methods may have been used in the past, but they do not guarantee anonymity or protection from law enforcement investigations. |
| --- |

### Protecting oneself as a wealthy person

Satoshi Nakamoto also amassed about 1M BTCs. These bitcoins were gaining in value when Satoshi Nakamoto disappeared (in 2012). Today, they would be worth over $100B. Depending on where this person is located, an individual with this level of wealth will probably go the extra mile to stay secure and guard against theft, kidnapping, and, consequently, threat to life.

### Protecting oneself from any retribution after moving markets

When this individual dumps the bitcoins owned, there is likely to be a huge drop in price. That individual is likely to be sought in order to take revenge. Maybe, Satoshi Nakamoto is choosing to stay anonymous to maintain the flexibility to dump bitcoins without attracting any retribution for such an action.

### To redirect attention to the currency and platform

Some argue that Satoshi Nakamoto may have disappeared to take attention from the individual or group behind the currency because such attention would be antithetical to the idea behind Bitcoin. It is supposed to be decentralized. The pronouncements of the individual or group would have undue influence on the value of the currency. The opinions of this person or group may hold greater weight than those of the Bitcoin community at large. So, it is argued, it would be best for the creator to simply disappear.

### Protection from the middleman who is eliminated

The blockchain technology cuts out the middleman. Middlemen or intermediaries are a huge industry. Banks and electronic payment systems (e.g., Western Union, PayPal) mediate business and personal transactions. Investment banks mediate the raising of capital.

* Intermediaries stand to lose money from people who use bitcoin.
  + For instance, Western Union and others like it were assumed to lose $400M as a result of the move to legalize bitcoin in El Salvador ([article](https://www.cnbc.com/2021/09/09/el-salvador-bitcoin-move-could-cost-western-union-400-million-a-year.html)).
* Those working for intermediaries stand to lose money due to more efficient processes introduced by blockchain technology.
  + According to a [report from Accenture](https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf), blockchain technology could bring significant savings in business processes of investment banks, including: (a) 70% savings in central finance reporting, (b) 50% savings in business operations, (c) 30–50% savings in compliance, and (d) 50% savings in centralized operations. All of this implies less profits or loss of earnings for some people.

In sum, blockchain technology is likely to impact a significant number of people or entities.

Would you be happy if you were one of the middlemen or working for a middleman and your role is being cut by blockchain technology? Would you be happy with Satoshi Nakamoto? Would you or some other intermediary whose economic role has been eliminated not try to get even with Satoshi Nakamoto somehow? An industry that gets eliminated may try to drum up charges and get Satoshi Nakamoto put behind bars. People can be quite vindictive. It is not just intermediaries but even those currently involved in inefficient processes stand to see their role being cut. They can try to get even with Satoshi Nakamoto due to which this person will be motivated to go into hiding.