Bitcoin: Definition, origin and risks

Bitcoin is a virtual 'cryptocurrency' traded much like real money.

bitcoin representation

Bitcoin is a virtual currency known as a 'cryptocurrency that can be traded between buyers and sellers much like "real" money is.

One of the very first and most high-profile [cryptocurrencies](https://www.livescience.com/65089-cryptocurrency-blockchain.html) launched, Bitcoin is also the most well-known of this virtual money. Bitcoin first emerged in 2009 and its creator is allegedly called Satoshi Nakamoto, though several theories exist as to Nakamoto's real identity, according to [Business Insider](https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?r=US&IR=T)(opens in new tab).

A bitcoin is essentially a digital computer file that is stored in something called a digital wallet, which can be accessed by software and apps.

You can send a whole bitcoin, or a portion of one, to someone else's digital wallet in exchange for goods and services. These transactions are recorded on a blockchain: a distributed ledger that is like a database, which everyone can see. The blockchain is stored on linked [computers](https://www.livescience.com/20718-computer-history.html) known as 'nodes'.

Because everyone can see that data stored on the blockchain, it means the transactions are extremely difficult to falsify, making it super secure.

Although there are now thousands of cryptocurrencies, Bitcoin is still the most valuable and sought after currently available.

WHY IS BITCOIN USED?

While ordinary currency requires government backing and financial institutions to give them value, bitcoin has inherent value because there are only a finite supply of 21 million , according to [NASDAQ.com](https://www.nasdaq.com/articles/90-of-all-21-million-bitcoin-have-now-been-mined)(opens in new tab).

Bitcoin is not controlled by any one organisation or country, which means the performance of a nation's economy has little impact on its  truly international and able to withstand geopolitical and localized economic shocks.

This means that Bitcoin is decentralized, and operates on a peer-to-peer (P2P) it can be passed directly between individuals without the need for a bank, or even a national economy.

The movement of bitcoin is overseen by a network of 'miners', who process the transactions on the blockchain and are rewarded with new bitcoin.

Because the process is virtual, it is also much easier to use in digital transactions in a way that makes it largely untraceable by banks and the authorities. This has led to it gaining a reputation for use by criminals such as hackers, who will often demand bitcoin as a means of payment from their victim, [CNBC reported](https://www.cnbc.com/2021/11/09/bitcoin-atms-criminals-target-cryptocurrency-transactions.html#:~:text=As%20the%20number%20of%20bitcoin,to%20abuses%20of%20the%20ATMs.)(opens in new tab).

HOW ARE BITCOINS PRODUCED?

There are a number of ways that bitcoins can be produced. They can be bought using real-world currency, or you can receive them from someone else as part of a transaction. They can also be produced virtually, in a process known as crypto mining.

Crypto mining is really difficult to achieve and needs lots of computer memory. It involves computers having to decipher equations and when one is completed a new block is added to the blockchain. The crypto miner then receives an amount of bitcoin units in exchange. There are places in the world with vast stacks of computers linked together to mine bitcoin in this way.

An engineer runs diagnostics on mining rigs at the Evobits crypto farm in Cluj-Napoca, Romania. (Image credit: Getty Images / Bloomberg)

IS BITCOIN SAFE?

The 'crypto' in cryptocurrency refers to [cryptography](https://www.livescience.com/65648-cryptography.html), a type of encryption. In bitcoin's case that encryption is based on the SHA-256 algorithm designed by the US National Security Agency. It is regarded as virtually impossible to crack, according to [IBM](https://www.ibm.com/docs/en/ibm-mq/9.2?topic=tls-national-security-agency-nsa-suite-b-cryptography)(opens in new tab)*.*

Despite this, there have been incidents of Bitcoin exchanges being hacked, but this has involved attacks on the places where the digital currency was stored, such as on websites, but not the Bitcoin network itself. To achieve the latter, a hacker would have to own more than half of all nodes around the world.

PROBLEMS WITH BITCOIN

It is fair to say that not everyone is sold on the idea of Bitcoin. Tech moguls such as Elon Musk have professed their belief in them, but those with a more traditional outlook, such as the Head of the [Bank of England](https://www.bankofengland.co.uk/speech/2021/october/jon-cunliffe-swifts-sibos-2021)(opens in new tab), have expressed concerns. This is why their value tends to fluctuate from time to time, sometimes quite wildly.

It is for this reason that, although some nations like El Salvador have controversially adopted bitcoin as legal tender, as the [Financial Times](https://www.ft.com/content/fbf9aef0-453f-4e61-bd83-ff2b2bc92221)(opens in new tab) reported, it still presently tends to be traded in certain circles well beyond the mainstreams of society.

A man is seen in a store where bitcoins are accepted in El Zonte, La Libertad, El Salvador on September 4, 2021. (Image credit: Getty Images / MARVIN RECINOS)

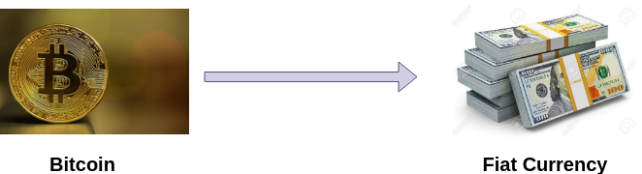
There are also environmental concerns around bitcoin due to the huge computational power required to mine it. At the beginning of last year, experts at the University of Cambridge estimated it accounted for more than 100 terawatt hours annually. This was almost a third of what the entire U.K. used.

Converting Bitcoins to Fiat Currency

In this section, we are going first to understand the meaning of **Fiat** or **Fiat Currency**.

Fiat currency is a currency which is issued by a government to be legal tender in the territories controlled by it. Fiat money that has value only because of government regulation or law is not backed by a physical commodity, such as gold or silver. The value of fiat money is derived from the relationship between **supply** and **demand** and the stability of the issuing government rather than the worth of a commodity backing it. It is based on the faith and credit of the economy. Most modern paper currencies are fiat currencies.

Every [cryptocurrency](https://www.javatpoint.com/blockchain-cryptocurrency) newcomers want to know how to cash out *bitcoin* or *withdraw* from bitcoins into fiat currency(USD, EUR, INR) which will be acceptable in their native countries. There are some easy ways to convert BTC into USD, INR, EUR or GBP, some of them are listed below. Before picking any of the listed methods, you need to find out how you want to receive your fiat currency. You can sell Bitcoins in person for cash or can sell it on exchanges and get the money directly into your bank account. You can also spend your [Bitcoin](https://www.javatpoint.com/bitcoin) to buy stuff from Amazon.



Cryptocurrency Exchange

The first one is to use a cryptocurrency exchange. Whenever you want to go on a business trip or other countries, the first thing you need to do is that you have to go to a currency exchange centre. The exchange centre switches your local currency with the currency of that country where you are visiting. It's the same thing with bitcoin. There are cryptocurrency exchanges that will convert your cryptocurrency into your local currency such as US dollars, euros or yen. There are many options available to do the exchanges of your currencies, such as Coinbase. The Coinbase is available in over 30 different countries, which can easily convert your bitcoins into currency and deposit it directly into your bank account. There are other alternatives available such as Kraken, Gemini, BitStamp.

Bitcoin Debit Card

It is also used to convert your bitcoin into fiat currency. The bitcoin debit cards allow their users to deposit their crypto coins via an online website which automatically converts them into a fiat currency such as Dollar or Euro. There are multiple options available for this. **For example,** Coinbase offers a Visa Bitcoin debit card. This card enables you to keep your holdings in bitcoin, and you can be paying anywhere that accepts Visa using your Bitcoin debit card.



Selling Bitcoins

The next option is to sell your bitcoins to someone else. As we know that, you can *transfer bitcoin directly* to another person without involving the services of a **third-party** such as a bank or a credit card. So you simply need to find out somebody who wants to buy your Bitcoins. When the buyer is available, you can transfer your bitcoins directly into their wallet and can get paid for that. In this type of transfer, there are some **security risks** involved because when you do a transfer of bitcoin to someone else, that transaction is **irreversible**. So if you send your bitcoins to someone else and that person does not pay you for the bitcoins, then there is no way to retrieve your bitcoins back. So whenever you are going to sell bitcoins to someone else whether it's a family member, a friend, or some other person, make sure that you can trust on this person, and you are going to get paid for the bitcoins that you send.

Bitcoin ATMs

Bitcoin ATM is also known as **BTMs** or **Bitcoin Teller Machines**. It is a machine where you can buy bitcoins or can sell your bitcoins. Bitcoin ATMs are available in most major cities around the world. The bitcoin **ATMs** provides a relatively fast and easiest way to quickly withdraw funds in your local fiat currency against your bitcoin holdings. Many Bitcoin ATMs also allow users to buy Bitcoin with money in much the same way as someone deposit money into their bank account at a regular ATM.

Bitcoin is basically a cryptocurrency that is stored in a virtual wallet. It is basically a digital currency that is currently used as a form of payment. The transactions related to bitcoins take place in the blockchain network. Every bitcoin is stored in a virtual wallet and the transaction involves the transfer of bitcoin from one wallet to another. Bitcoins can be sent from peer to peer irrespective of geographical location without any intermediator in between. It works in a decentralized way, meaning nobody can interfere with the digital money, only the concerned person is responsible for the bitcoins.

Fiat currency is the currency that is issued by the government. in other terms. It is the cash, coins we generally have, that is the physical form of currency. Fiat currency ranges from USD, EUR, INR, GBP, etc.

**There are lots of reasons why one might want to exchange one Bitcoin for fiat currency:**

* To get a profit from the favorable market conditions like bull run on bitcoins price.
* Get more flexibility with the money.
* Fiat currency is the most common form of currency worldwide.
* Pay a bill.
* The decision to profit from favorable marketplace conditions like a bull run on  Bitcoins price

**Converting Bitcoin To Fiat Currency**

There are many ways to convert bitcoin to fiat currency. The methods are listed below-

1. **Cryptocurrency Exchanges:**This is the most widely used method to convert bitcoin to fiat currency. It is similar to a money exchange center which is needed when a person moves from one country to another. Cryptocurrency exchanges basically convert your cryptocurrency that is bitcoin into your local currency such as rupees, US dollars, euros. The main disadvantage of this method is the delay in withdrawing fiat currency even after completing the transaction.   
   Cryptocurrency Exchanges have an inbuilt crypto converter feature that displays how much fiat currency one could get with the bitcoins that person has. There are multiple exchanges available like Gemini, coinbase, binance, etc. This has a user-friendly interface that eases the whole process of bitcoin conversion. During bull run time, these exchanges are affected negatively and face technical difficulties. Coinbase seems a suitable option as it has improved over its downtime problem by increasing the infrastructure capability. Coinbase exchange sends the converted fiat money directly into your bank account without much hassle.
2. **Bitcoin Debit Card:**Possessing a Bitcoin Debit Card is the fastest way to convert bitcoin to cash or fiat currency.  The online website is provided as a user interface where the user deposits the bitcoins and the website automatically converts those into required fiat currency. Bitcoin debit cards are used wherever debit cards are accepted, the only difference being, funds are transferred from a crypto wallet rather than from a bank account. The main disadvantage is the providers of Bitcoin debit cards takes transaction charge on every purchase and also limits the total amount of transaction per debit card.in order to register for the Bitcoin debit cards, one needs to go to the bank and do KYC.
3. **Peer-to-Peer Exchanges:** It is known that bitcoin doesn’t have any centralized authority, therefore any fund can be transferred from one peer to another. This basically involves finding a buyer who will buy your bitcoins and in return, would give cash for that. But one thing to be noted is that transactions in bitcoins are irreversible. So, choose a trustworthy buyer on whom you are sure of getting the cash after a bitcoin transaction.
4. **Bitcoin ATMs:**It is also known as a Bitcoin Teller Machine (similar to ATM). BTM acts similar to an ATM, allowing to withdraw cash. QR code and added security features like text messages are there to ensure smooth and secure transactions. BTMs allow you to buy as well as sell bitcoins.it provides a very fast and convenient way to take cash out of a bitcoin wallet. BTMs are available in developed cities of the world and more are under construction after the boom of the digital currency era. The drawback of BTMs is they charge a heavy amount on conversion and also sets a maximum transaction limit.
5. **Metal Pay:** It is a money transfer app that allows cryptocurrency holders to cash out. The need for this app is to complete KYC before filling up the bank details. After filling in bank details, the customer can buy, sell, send, receive as well as convert cryptocurrencies. Metal pay has the capability to convert at least 24 cryptocurrencies including bitcoins.

**Top Fiat Currencies For Foreign Trade**

Bitcoin trading is generally done in the following fiat currencies. These are by far the most widely used fiat currency.

* **US Dollar:**It holds more than 80% market share making it the most widely used fiat currency used in bitcoin trading. The reason behind its popularity is the huge userbase in the blockchain-based bitcoin network. While the other countries are yet to develop in the bitcoin field, the USA is already far ahead in this race.
* **Japanese Yen:** Although it has almost 7% of the total market share, it is the second most widely used fiat currency used in bitcoin trading. Japanese regulators were also some of the earliest adopters and among the most accommodating of the virtual currency.
* **Euro:**The currency of Europe, the Euro, ranks third on the list of fiat currencies with approx 5% market share in trading Bitcoins into fiat currency. But Europeans are confined to certain regions only while buying bitcoins. Slowly Europe is becoming a cryptocurrency hub with some of the nations accepting cryptocurrencies.

**Cryptocurrency Exchanges**

Platforms that facilitate the trading of cryptocurrencies for other assets, including digital and fiat currencies.

**What are Cryptocurrency Exchanges?**

In order to start buying and selling cryptocurrencies and other digital assets, the most common way is to transact with Crypto Exchanges. Cryptocurrency exchanges are privately-owned platforms that facilitate the trading of cryptocurrencies for other crypto assets, including digital and fiat currencies and NFTs.



**Key Highlights**

* The most common way of transacting in cryptocurrencies and other digital assets is via a Cryptocurrency Exchange.
* There are Centralized and Decentralized Cryptocurrency Exchanges, and each offers advantages and disadvantages.

**Centralized Cryptocurrency Exchanges (“CEX”)**

Centralized cryptocurrency exchanges act as an intermediary between a buyer and a seller and make money through commissions and transaction fees. You can imagine a CEX to be similar to a stock exchange but for digital assets.

Popular Crypto Exchanges are Binance, Coinbase Exchange, Kraken and KuCoin. Much like stock trading websites or apps, these exchanges allow cryptocurrency investors to buy and sell digital assets at the prevailing price, called spot, or to leave orders that get executed when the asset gets to the investor’s desired price target, called limit orders.

CEXs operate using an order book system, which means that buy and sell orders are listed and sorted by the intended buy or sell price. The matching engine of the exchange then matches buyers and sellers based on the best executable price given the desired lot size. Hence, a digital asset’s price will depend on the supply and demand of that asset versus another, whether it be fiat currency or cryptocurrency.

CEXs decide which digital asset it will allow trading in, which provides a small measure of comfort that unscrupulous digital assets may be excluded from the CEX.

**Decentralized Cryptocurrency Exchanges (“DEX”)**

A decentralized exchange is another type of exchange that allows peer-to-peer transactions directly from your digital wallet without going through an intermediary. Examples of DEXs include Uniswap, PancakeSwap, dYdX, and Kyber.

These decentralized exchanges rely on smart contracts, self-executing pieces of code on a blockchain. These smart contracts allow for more privacy and less slippage (another term for transaction costs) than a centralized cryptocurrency exchange.

On the other hand, even though smart contracts are rules-based, the lack of an intermediary third party means that the user is left to their own, so DEXs are meant for sophisticated investors.

**Advantages of Centralized Cryptocurrency Exchanges**

**1. User-friendly**

Centralized exchanges offer beginner investors a familiar, friendly way of trading and investing in cryptocurrencies. As opposed to using crypto wallets and peer-to-peer transactions, which can be complex, users of centralized exchanges can log into their accounts, view their [account balances](https://corporatefinanceinstitute.com/resources/knowledge/finance/account-balance/), and make transactions through applications and websites.

**2. Reliable**

Centralized exchanges offer an extra layer of security and reliability when it comes to transactions and trading. By facilitating the transaction through a developed, centralized platform, centralized exchanges offer higher levels of comfort.

**3. Leverage**

One of the other benefits of certain CEXs is the option to leverage your investments using borrowed money from the exchange, called margin trading. It allows investors to reap higher returns, but losses can also be amplified.

**Disadvantages of Centralized Cryptocurrency Exchanges**

**1. Hacking risk**

Centralized exchanges are operated by companies that are responsible for the holdings of their customers. Large exchanges usually hold billions of dollars worth of bitcoin, making them a target for hackers and theft.

An example of such an incident is Mt.Gox, which was once the world’s largest cryptocurrency exchange company before it reported the theft of 850,000 bitcoins, leading to its collapse.

**2. Transaction fees**

Unlike peer-to-peer transactions, centralized exchanges often charge high transaction fees for their services and convenience, which can be especially high when trading in large amounts.

**3. Custody of digital assets and risk of fraud**

Lastly and most importantly, most CEXs will hold your digital asset as a custodian in their own digital wallet rather than allow you to store your private keys on your own digital wallet. While more convenient when you want to trade, there are drawbacks, namely the risk of the centralized cryptocurrency exchange failing and fraud.

Recent examples include the failure of the 50 USD billion algorithmic stablecoin [TerraUSD](https://corporatefinanceinstitute.com/resources/cryptocurrency/what-happened-to-terra/) and sister token Luna, the bankruptcies of hedge fund Three Arrows Capital, lender Celsius Network, broker Voyager Digital and the sudden collapse of FTX and Alameda Research.

**Advantages of Decentralized Cryptocurrency Exchanges**

**1. Custody**

Users of decentralized exchanges do not need to transfer their assets to a third party. Therefore, there is no risk of a company or organization being hacked, and users are assured of greater safety from hacking, failure, fraud, or theft.

**2. Preventing market manipulation**

Due to their nature of allowing for the peer-to-peer exchange of cryptocurrencies, decentralized exchanges prevent market manipulation, protecting users from fake trading and [wash trading](https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/wash-trading/).

**3. Less censorship**

Decentralized exchanges do not require customers to fill out know-your-customer (KYC) forms, offering privacy and anonymity to users. Since DEXs don’t exercise censorship, more cryptocurrencies and digital assets are available than through a CEX. As a matter of fact, many Altcoins are only available on DEXs.

**Disadvantages of Decentralized Cryptocurrency Exchanges**

**1. Complexity**

Users of decentralized exchanges must remember the keys and passwords to their crypto wallets, or their assets are lost forever and cannot be recovered. They require the user to learn and get familiar with the platform and the process, unlike centralized exchanges, which offer a more convenient and user-friendly process.

**2. Lack of fiat payments**

DEXs are best for investors looking to switch from one digital asset to another and not well suited for someone looking to buy or sell digital assets with fiat currency, called on and off-ramping. It makes them less convenient for users that do not already hold cryptocurrencies.

**3. Liquidity struggles**

Some 99% of crypto transactions are facilitated by centralized exchanges, which suggests that they are accountable for the majority of the [trading volume](https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/volume-of-trade/). Due to the lack of volume, decentralized exchanges often lack liquidity, and it can be difficult to find buyers and sellers when trading volumes are low.

**The 10 Top Cryptocurrency Exchanges, Ranked by Volume (as of Nov. 2022)**

**Top Centralized Exchanges**[[1]](https://corporatefinanceinstitute.com/resources/cryptocurrency/cryptocurrency-exchanges/#citation-exchanges)

The following are the top centralized cryptocurrency exchanges, according to traffic, liquidity, and trading volumes.

1. [Binance](https://www.binance.com/en/markets)
2. Coinbase Exchange
3. Kraken
4. KuCoin
5. Binance.US
6. Bitfinex
7. Gemini
8. Coincheck
9. Bitstamp
10. Bybit

**Top Decentralized Exchanges**[[2]](https://corporatefinanceinstitute.com/resources/cryptocurrency/cryptocurrency-exchanges/#citation-dex)

Below are the highest-ranked decentralized cryptocurrency exchanges, according to traffic, liquidity, and trading volumes:

1. Uniswap (v3)
2. dYdX
3. Curve Finance
4. Kine Protocol
5. PancakeSwap (v2)
6. DODO (Ethereum)
7. Sun.io
8. ApolloX DEX
9. Uniswap (V2)
10. Perpetual Protocol

**The Legal Aspects of Cryptocurrency in India**

With the unique developments and advancements in the technology sector in India, especially during the challenges posed by the rapid spread of COVID-19, the fintech sector has shown promising results. There has been a growth, fuelled largely by curiosity and popularity, amongst the citizens of India in cryptocurrency such as Bitcoin, Ripple, Dogecoin, etc., based on which a large number of people have started investing a noticeable part of their time and money in these virtual currencies.

In India, the apex financial authority i.e., the Reserve Bank of India (“RBI”), recognised cryptocurrency, more specifically defined as a form of digital/ virtual currency created through a series of written computer codes based on cryptography /encryption and is thus free of any central issuing authority per se. Cryptocurrency is assisted through blockchain technology, that establishes a person-to-person issuance system that utilises private and public keys allowing authentication and encryption for secure and safe transactions.

**Growing Popularity of Cryptocurrency**

Being an untouched, unregulated market with a potential of over a trillion dollars, India also witnessed a huge surge of cryptocurrency exchanges.

Witnessing the increasing popularity of the use of cryptocurrency within a short span of a year and the potential revenue loss to the Government of India; the regulators and authorities started to take notice and as a consequence, in 2013 the RBI issued a press release, warning the public against dealing in virtual/digital currencies

**Restrictions Imposed by RBI**

In November 2017 the Government of India established a high-level Inter-Ministerial Committee to report on various issues related to the use of virtual currency and subsequently, in July 2019, this Committee presented its report suggesting a blanket ban on private cryptocurrencies in India.

The threat of revenue loss was so eminent to RBI, that it is interesting to note that even prior to submission of the report from the Inter-Ministerial Committee, in April 2018 the RBI had issued a circular restricting all commercial and co-operative banks, small finance banks, payment banks and NBFC from not only dealing in virtual/digital currencies themselves but also instructing them to stop providing services to all entities which deal with virtual/digital currencies.

This stalled the rise of the crypto industry in India, as exchanges required banking services for sending and receiving the money. The banking service is essential for the conversion into cryptocurrency and in turn for paying salaries, vendors, office space etc. However, the situation prevailing around cryptocurrencies and their usage completely changed on 4th March 2020, when the Hon’ble Supreme Court of India, in a well-conceived judgment quashed the earlier ban imposed by the RBI.

The Hon’ble Supreme Court of India chiefly examined the matter from the perspective of Article 19(1)(g) of the Indian Constitution, which talks about the freedom to practice any profession or to carry on any occupation, trade or business, and the doctrine of proportionality.

The Apex Court noted that there is unanimity of opinion among all regulators and governments of other countries that though virtual currencies have not acquired the status of legal tender, but they do display digital representations of value and are capable of functioning as medium of exchange, unit of account and/or store of value.

While the court recognized the RBI’s power to take a pre-emptive action, it held that the proportionality of such a measure was not there in the case, since there wasn’t any damage/loss suffered directly or indirectly, by RBI’s regulated entities as a result of VC trading. Therefore, among other reasons, on the grounds of proportionality the impugned Circular dated 06-04-2018 was set aside.

**Developments in the Crypto-World**

The Government of India is now considering the introduction of a new bill titled “Cryptocurrency and Regulation of Official Digital Currency Bill, 2021” (“**New Bill**”) which is similar in spirit to its earlier versions. However, the New Bill seeks to ban private cryptocurrencies in India with some exceptions, to encourage the underlying technology and trading of cryptocurrency but facilitated within a framework for the creation of an official digital currency which will be issued by the RBI.

The New Bill has approached the difficulty of the lack of cryptocurrency laws and suggests banning all the private cryptocurrencies in their entirety. The dichotomy in the New Bill’s suggestion arises since the RBI is still in the grey about which kinds of cryptocurrency will fall under the purview of private cryptocurrency.

If the New Bill imposes a complete ban on private cryptocurrencies, it shall lead the cryptocurrency investors to invest and deal in cryptocurrency in a completely unregulated market. Further, the aim of introducing a law related to cryptocurrency is to ease the process of trading and holding, in a safer technological environment.

However, even with the introduction of state-owned cryptocurrency which shall be monitored by the RBI, the risk in investment and holding of cryptocurrency shall remain the same.

**Current Situation of Cryptocurrency in India**

Towards the end of March 2021, according to the latest amendments to the Schedule III of the Companies Act, 2013, the Government of India instructed that from the beginning of the new financial year, companies have to disclose their investments in cryptocurrencies.

In simple words, companies now have to disclose profit or loss on transactions involving cryptocurrency, the amount of holding, and details about the deposits or advances from any person trading or investing in cryptocurrency. This move has been greatly appreciated by the people dealing in the crypto sector, as this will open the door for all Indian companies to have Crypto on their balance sheets.

Based on the inference that can be drawn from the **aforementioned facts and current scenario around the world dealing with matters of cryptocurrencies, it is noticeable that there is a complete lack of clarity concerning cryptocurrency regulation in India.**

Well-structured, clear regulations dealing with crypto trading exchanges, blockchain technology, investors, and the people employed in such sector should be made the priority given that the world of cryptocurrency is here to stay and demands more attention.

It is fascinating to note that in the Draft National Strategy on Blockchain, 2021, published by the Ministry of Electronics and Information Technology highlighted the benefits of cryptocurrency. Therefore, banning a virtual currency that has created an impact in many countries, will not be the ideal thing to do for the development of our nation.

The government needs to take an effective step towards the positive regulation and enforcement of cryptocurrency as a way forward to earn the confidence of investors and the general public in developing the nation. It was announced by the Union Finance Minister Nirmala Sitharam on 16th March 2021 that there shall not be a complete ban on cryptocurrency – “we will allow a certain amount of window for people to experiment on blockchain, bitcoins and cryptocurrency.”.

Though It would be wiser to pause, sit back and wait for the Government to formulate clear regulations concerning cryptocurrencies before running in the grey.

**Why Cryptocurrencies Need To Be Regulated? Here Are 5 Reasons**

The virtual assets need to be regulated to protect the interest of investors

The Indian government is planning to introduce a bill during the ongoing winter session of Parliament to classify cryptocurrencies as financial assets while protecting the interests of small investors. In all likelihood, the bill may set a minimum amount to invest in cryptocurrencies, while prohibiting their use as legal tender or currency substitutes. The bill also proposes to lay the groundwork for the creation of the official digital currency to be issued by the Reserve Bank of India (RBI) and regulated under the RBI act, according to a [report](https://www.ndtv.com/business/crypto-asset-bill-proposes-to-prohibit-use-of-crypto-as-currency-2635707#:~:text=The%20crypto%20bill%20which%20will,framework%20of%20crypto's%20evolving%20space&text=The%20Crypto%20Asset%20Bill%20proposes,as%20payment%20systems%20for%20remittances.) in NDTV.

From the standpoint of investors, cryptocurrency regulation is quite important. With the right kind of regulations in place, the government can make the cryptocurrency market a safer environment for investors.

**Here are 5 reasons why cryptocurrencies need to be regulated:**

**1) Prevent market manipulation and protect investors:**Market manipulation and price volatility are common in cryptocurrencies. Take, for example, Bitcoin, the world's oldest and most popular cryptocurrency, which rose to all-time highs since the beginning of 2021, before plummeting and losing a huge amount of its value. So, the lack of authorised information on these digital assets and the technological complexities associated with them makes it imperative to put regulations in place for safeguarding investors.

**2) Allow select cryptocurrencies:** Thousands of cryptocurrencies exist around the world. Most investors, however, are only familiar with a few of those, such as Bitcoin, Ether, Ripple, and Dogecoin among others. They hardly have any knowledge about the thousands of other virtual assets. So, to protect customers, a regulatory authority clearing cryptocurrency is required, which can disclose all information about the performance of the digital assets, their risks, and potential.

**3) Understanding risks associated with technology:**Technology is advancing at a breakneck pace. This carries a significant danger, as such changes have the potential to render technology, including blockchain, outdated in the future. Given the rapid rate of technological change, information infrastructure and professional financial advisors skilled in cryptocurrency are required. That way, investors can understand the technological risks of cryptocurrencies and make informed decisions.

**4) Online fraud and cyber security risks:**Investing in cryptocurrencies comes with another risk — online fraud. Hacking is a major threat worldwide, and cyber-attacks have become common. One cyber-attack could result in losses for investors who have put their savings in cryptocurrencies. Through regulations, the authorities can implement measures to help cryptocurrency investors protect their assets. Also, investors can address concerns or reclaim their investments in case they lose them.

**5) Money laundering:**Any unregulated system has the ability to fund criminal acts. As a result, a client due diligence process akin to that of a bank is required. This can help in keeping track of investors' real identities and verifying their locations when they are buying or selling cryptocurrencies. Any infringement of such norms should be met with severe sanctions.

**Cryptocurrency- a new dimension in the global economy**

***The original concept of a digital currency based on cryptography as is perceived in the present form was initiated in 2008 by “Satoshi Nakamoto” through a pseudo name.***

Cryptocurrency is a digital currency based on use of cryptography to secure transactions, control creation of additional units and also verify transfer of assets. Each “cryptocurrency” has a unique set of features and cannot be analyzed or understood by making general observations. The term is used as a generic representation of all such tokens which are generated through cryptography. In current parlance convertible, decentralized virtual currencies are referred as “cryptocurrencies”.

One estimate puts the number of cryptocurrencies at around 6700, with a total market capitalization of an astonishing 2.5 trillion USD as of Oct 25, 2021. Bitcoin, Ethereum, Binance Coin, Cardano, Solana, Ripple, Polkadot are amongst the leading names as of 2021. There is a large variation in characteristics of the cryptocurrencies which are also evolving over time due to evolution of unique features of each such instrument.

**History and Background**

Haber and Stornetta were the first to propose the concept of block-chain in 1991.Block-chain is a distributed ledger technology and consists of subsets of data, in the form of blocks. Each block or coin is mined on the basis of intense calculations and cryptography, through intense “work” or arriving at the matching result to be accepted in the block-chain. Mining of a new block or “coin” is therefore a very intense and arduous job and the successful miner is rewarded in terms of a new “coin”. Advanced hardware and large amounts of energy are needed to “work” and generate or “mine” a crypto currency.

The original concept of a digital currency based on cryptography as is perceived in the present form was initiated in 2008 by “Satoshi Nakamoto” through a pseudo name.

Evolution of cryptocurrencies has been facilitated by development of crypto exchanges over a period of time. A new ecosystem is in the offing through such exchanges, which if properly regulated can facilitate smooth participation of larger numbers of population in cryptocurrencies.

Cryptocurrencies are not backed by conventional assets such as gold reserves. They derive value from democratic and decentralized utility, market acceptance and belief. Many crypto “coins” or “tokens” are in fact backed by state-of-the-art block-chain projects. Ripple (XRP) has helped Europe’s 4 th largest bank, Banco Santander develop its One Pay FX service.

**Advantages and Drawbacks**

There are certain advantages as well as loopholes in the use of cryptocurrencies. While there are widespread apprehensions of use of cryptocurrencies for dubious activities, there may be possibilities to control and regulate this through regulated crypto exchanges and introducing KYC norms. This is by no means an easy task. However, considering that wishing away the existence of cryptocurrency does not appear to be realistic, perhaps the best way would be to develop superior regulatory norms and plug the illegal use of this new concept.

The concept of block-chain has its advantages in terms of offering true equality, i.e. each participant is equally important and there are no middlemen or Central Authorities. While anonymity or privacy is also considered an advantage, it also comes with the risk of no support or guarantee in case of any loss or hacking of the system. It might help in easier access to credit and funding at a global level even for the small and medium business persons. These are contentious policy issues which call for careful analysis for ensuring overall welfare and security of financial systems and also check misuse of technology driven financial instruments.

**Currency or Asset**

Cryptocurrency was initially conceived as a medium of payment. Lately, it has developed into a form of asset, whose value keeps on fluctuating as it gets traded in the markets or exchanges. There is an element of both a currency and an asset in this new financial instrument. As an asset, it also has the feature of very rapid fluctuation in a short duration. The sensitivity to any apprehension even by a handful of “owners” results in major dips or jumps in the prices of these cryptocurrencies/crypto-assets. Market information and crypto-exchanges do play a very critical role in the value of crypto-assets.

**Classes of Cryptocurrencies**

There are a variety of crypto instruments which have different characteristics, some as a currency and some as an asset. Cryptocurrencies have been grouped into 7 broad classes by Wolfgang et al (2019).

Transaction mechanism – eg. Bitcoin (BTC)  
Distributed computation token – eg. Ethereum (ETH)  
Utility token – eg. Golem (GLM)  
Security token (in stocks, financial instruments) – eg.ArCoin  
Fungible tokens – eg. ERC-20  
Non fungible token – eg.SAND, DEGO  
Stablecoins – eg.USD Tether (USDT), LBS Peg.

All cryptocurrencies cannot be put in any class. The fundamental technology of crypto is so dynamic; it is difficult to classify them into watertight compartments. They have many uses and characteristics. This emphasizes the difficulty in treating them as an asset or a currency at any one point of time. Cryptography and mathematical calculations form the basis of mining cryptocurrencies, which do have dynamic characteristics and also multiple variants over time. New crypto instruments are being generated on a real time basis.

**Challenges for Economies**

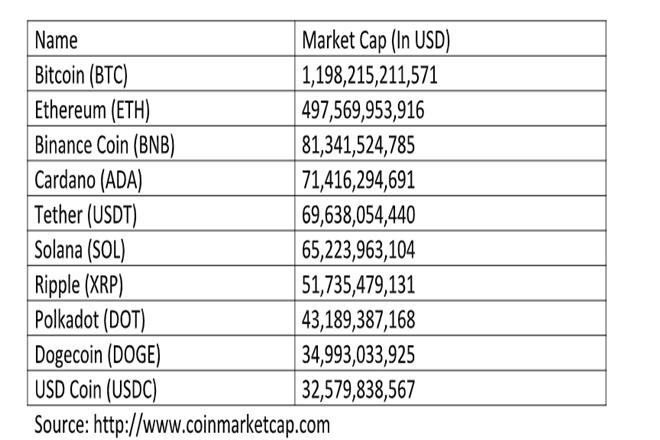
The threat to the monetary system, fear of misuse for dubious activities and no control over the private crypto-exchanges enabling sale purchase of cryptocurrencies are some real challenges faced by the individual countries, as the cryptocurrencies increase their presence and influence over the global economy. Another crucial aspect relates to taxing such transactions both domestically and internationally.

Cryptocurrencies are being considered in different perspectives by various countries. First are the Crypto-friendly countries like Malta and Singapore and Switzerland, which promote use of cryptocurrency.Second category of countries restrict cryptocurrencies. These include China, which has largely banned cryptocurrencies. South Korea, Bangladesh, Bolivia, Taiwan, Lebanon have also banned use of crypto currencies. The third category regulates use of cryptocurrencies. These countries seek to balance encouraging the use of cryptocurrencies and balancing the risks attached in use of cryptocurrencies, such as the USA.

There are variations in the manner cryptocurrencies are considered for various taxes like VAT, Capital gains or Property Tax. There is no dispute that fair and transparent taxation mechanism which is also robust and dynamic must be put in place by all economies of the world. Due to lack of clarity, there is possibility of tax gaps increasing in this area in the medium and long run. While there are bigger challenges in allowing crypto-instruments to be used as currency and mode of payments, perhaps treating it as some form of asset might be feasible. Capital gains taxation might yield more pragmatic solutions, with restrictions on claiming losses and establishing a regulatory authority in each economy for issuing instructions and regulations from time to time. Analysis of classes of cryptocurrency and also defining the nature of these assets can be a starting point for adapting this instrument into the financial system in a phased manner. A global consensus is however needed in view of the digital nature and the technology involved.

**Market share**

The top 10 cryptocurrencies based on their market capitalization as on 25 th October 2021 as reported by coinmarketcap.com are depicted in the following chart:



The importance of cryptocurrencies in the global economy has been increasing rapidly not only in terms of valuation but also in terms of holdings by the population in different countries. Cryptocurrencies are finding support from new quarters with passage of time.

**Way Ahead**

The emergence and acceptance of cryptocurrencies in different parts of the world cannot be ignored or sidelined. Block-chain technology is also here to stay. Crypto instruments have their advantages and shortcomings. It poses a challenge to the financial systems in different economies and has potential to misuse with high risk of hacking and anonymity. Perhaps more transparency and clarity is possible by considering the following issues on top priority:

1. Establishing norms and rules for use of crypto instruments in countries and at a global level.  
2. Capturing transactions through KYC and developing norms for taxing transactions.  
3. Developing and regulating Crypto Exchanges.  
4. Collecting data and conducting research to find and plug avenues for money laundering.  
5. Finding out a balance between regulation and checking crypto instruments for different purposes. Using crypto as a currency is complicated but treating it as an asset could be considered.

Research on the subject is ongoing. A more active role by governments and global institutions will help in finding pragmatic and acceptable solutions. Pragmatic regulations and transparency in treatment of this newly discovered instrument will certainly benefit in the long run.

***(The author is an IRS Officer and also an ex- Visiting Researcher at Georgetown University, USA. The views are strictly personal and do not reflect the official position or policy of Financial Express Online. Reproducing this content without permission is prohibited).)***

**How do I create a Bitcoin wallet?**

Creating a Bitcoin wallet is as easy as installing

software on your mobile device or laptop/desktop.  
  
When you install the app, your Bitcoin wallet is automatically created. You can then receive bitcoin to your wallet immediately, store it safely, and use it as you please.



**Which Bitcoin wallet should I choose?**

There are a number of wallet apps on the market from a variety of vendors and with different features to choose from. We welcome you to try the [**Bitcoin.com Wallet**](https://wallet.bitcoin.com/), the fully [**self-custodial**](https://www.bitcoin.com/get-started/custodial-non-custodial-bitcoin-wallets/) crypto wallet trusted by millions.

The [**Bitcoin.com Wallet**](https://wallet.bitcoin.com/) is what's known as a '*software wallet*'. Quality software wallets provide an excellent combination of security and ease-of-use. Depending on how you're using your bitcoin though, you may want to consider another wallet type. Here's a rundown on the different types of Bitcoin wallets and their respective pros & cons:

**Software wallets: convenient buying, selling, storing, trading, and using**

* Software wallets take the form of an app which is downloaded for free to your phone or desktop. You simply open up the app and can start making Bitcoin transactions almost immediately.
* Since software wallets connect to the Internet, there's a very small risk of hacking. Therefore, it is generally recommended to not store large amounts of bitcoin in your software wallet. That being said, if you follow [**password management best practices**](https://www.bitcoin.com/get-started/digital-asset-security/), it's safe to store bitcoin in a software wallet.
* While there have been a few isolated cases of software wallets being hacked, by far the greater risk is that you lose your 'private key,' which is like the password to your wallet. Therefore, it's critical to [**back up your wallet**](https://www.bitcoin.com/get-started/digital-asset-security/) and store the password somewhere safe.

**Tip: Make sure the software wallet you’re using is fully self-custodial like the**[**Bitcoin.com Wallet**](https://wallet.bitcoin.com/)**, meaning only you can access your crypto — *not* the wallet provider. This protects you from the risk of fraud or bankruptcy by the wallet provider.**

Read more: [**What features to look for in a Bitcoin software wallet**](https://www.bitcoin.com/get-started/how-to-choose-the-right-bitcoin-wallet/).

**Hardware wallets: long-term storage for larger amounts of bitcoin**

* Hardware wallets, also known as cold wallets, are physical devices created specifically for the purpose of storing cryptocurrencies. They offer the best security for your digital assets because they insulate you from the Internet, making it effectively impossible for hackers to infiltrate your wallet.
* Since they take more time to access, hardware wallets aren’t ideal for making frequent Bitcoin transactions. Use them for long-term storage instead.
* As with software wallets, you need to [**back up your private key**](https://www.bitcoin.com/get-started/digital-asset-security/#1) and adhere to [**password management best practices**](https://www.bitcoin.com/get-started/digital-asset-security/#2).

**Tip: Hardware wallets are well worth the initial cost — especially if you own a lot of bitcoin. To make sure the device isn't compromised, only buy one from a company you can trust.**

**Centralized exchange wallets: convenient buying, selling, and trading**

* Centralized exchanges (CEXs) have traditionally been a popular place for many newcomers to buy their first bitcoin because they make the buying process very simple. It's like opening a trading account.
* However, the CEX itself retains control over the funds in your account. Not only does this expose you to the risk of the exchange getting hacked or going bankrupt, it also means you have to ask for permission to withdraw your bitcoin, wait longer to withdraw, and usually pay higher transaction fees for withdrawals.
* We recommend using centralized exchanges only for trading (not for storing your bitcoin).

**Tip: CEXs are not a secure place to store digital assets. Once you’ve bought your bitcoin, you're advised to move it to your software or hardware wallet if you don't plan on trading it immediately.**

**Paper wallets: alternative to hardware wallets, unique method for gifting bitcoin**

Paper wallets are created by downloading a software package, then running the software (for security, preferably in an offline environment) to generate a public/private key pair which you print out on a piece of paper. Having created a paper wallet, you can send any amount of bitcoin to the wallet address. To spend it, you use the private key written on the paper to sign the spend transaction.

Like hardware wallets, paper wallets allow you to store bitcoin completely offline. This makes them a lower-cost alternative to hardware wallets.

Since the public/private key pair is written on the paper, handing over the paper to another person is similar to handing over a cash note. This makes paper wallets a novel way to exchange bitcoin face-to-face.

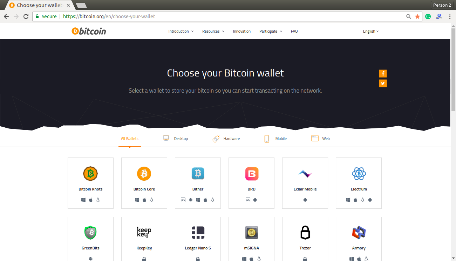
You can create your own Bitcoin Cash paper wallets at [**Bitcoin.com Paper Wallet**](https://paperwallet.bitcoin.com/?_gl=1*1o62pq9*_ga*NTA5NTkzMDAyLjE2Njk4Nzg4NjQ.*_ga_ERLPF60ZDD*MTY3MDU2NDQ0Mi4zLjAuMTY3MDU2NDQ0Mi4wLjAuMA..)

How to Choose Bitcoin Wallet

In this section, we are going to learn the process of choosing the bitcoin wallet. If you want to involve in bitcoin, you need to have a wallet. A wallet allows you to *receive bitcoins*, *send bitcoins*, *store bitcoins*. Here, I will take an example of a page called **bitcoin.org** to choose the wallet.

*Bitcoin.org* is a website that was developed by **Satoshi Nakamoto** and **Martti Malmi**. Now, Martti's is no longer an active developer, but he maintains the *Bitcoin.org* websites. He is not involved in developing bitcoin. Bitcoin.org website is not tied into any specific core developers. It's an open-source project which is handled by a global community.

Bitcoin.org is a very good starting point to explain how to choose your wallet because there is a lot of options available. In this page, we will go to an option called **Choose your wallet**. We can see this in the below image.



In the above image, we can see that there are different types of wallets that you can choose, like **Desktop wallet**, **Mobile wallet**, **Web wallet**, **Hardware wallet**, etc.

**Mobile wallet**

In the mobile wallet, you can run any type of application, whether it is on Android, iOS, Windows, or even on Blackberry. They are significantly smaller and simpler and serve as a convenient on-the-go wallet for daily usage.

Popular Mobile wallets are Bitpay, BTC.com, Edge, Electrum, Mycelium, Bitcoin Wallet, etc.

**Desktop wallet**

In the desktop wallet, you can run it on your desktop or laptop computer for Windows, Mac, and Linux. Generally, they are secure, but sometimes they are vulnerable to various malware and computer viruses.

Popular Desktop wallets are Bitcoin Core, Bitcoin Knots, mSIGNA, Armory, etc.

**Hardware wallet**

In a hardware wallet, there are devices which contain your private keys. The hardware wallets are the most secure wallets, but it will also cost money.

Popular hardware wallets are BitBox, Keepkey, Trezor, Ledger Nano S, etc.

**Web wallet**

The web wallets are online wallets that are considered less secure than other types of wallets, yet they can be highly convenient.

Popular web wallets are Guarda, Coinbase, GreenAddress, Binance, etc.

There are multiple different wallet options available which you can have and install on your mobile device, or on your computer or a web one. There is not necessary to have only one wallet. You can have multiple wallets for different needs. It helps you to spread the risk by not keeping all of your personal crypto's in one location but across different locations(wallets). You can create a wallet in any of these options that you find. If you wish, you can open up another wallet elsewhere and can send coins to a different wallet.

If you want to get started fast, select one of the wallet options that are available here. I would recommend you to try one of the web wallet options that are presented here. In the wallet, open up an account and try to send bitcoin to someone, buy bitcoin from someone, and store bitcoin into your wallet.

**To select a reliable Bitcoin wallet, one should judge it based on the following criteria:**

* **Hot/Cold Wallet:** Whether a wallet is a hot(Online storage) or cold(offline storage).
* **Control private keys:** A wallet where you own and control your keys.
* **Backup & security features:** Here, you can seed backup keys and pin codes.
* **Developer community:** It is an active development community for maintenance.
* **Compatibility:** It can be compatible with different operating systems.
* **HD Wallet:** It is a wallet that generates new addresses itself.
* **KYC:** A wallet that doesn't require KYC.

**How does IoT work with blockchain?**

IoT enables devices across the Internet to send data to private blockchain networks to create tamper-resistant records of shared transactions. IBM Blockchain enables your business partners to share and access IoT data with you — but without the need for central control and management. Each transaction can be verified to prevent disputes and build trust among all permissioned network members.

What is blockchain?

**Benefits of IoT and blockchain**

Build trust in your IoT data

Each transaction is recorded, put into a data block, and added to a secure, immutable data chain that cannot be changed — only added to.

**Rely on added security**

With the **Watson IoT® Platform** you can select the data to be managed, analyzed, customized, and shared among permissioned clients and partners.

**Gain greater flexibility**

**The IBM Blockchain Platform** is open, interoperable and is built for your multicloud world, using the latest version of the leading Hyperledger Fabric platform, optimized for Red Hat® OpenShift®.

**Generate new efficiencies**

IBM Blockchain streamlines processes and creates new business value across your ecosystem by drawing on the data supplied by IoT devices and sensors.

**Applications of IoT and blockchain**

**Freight transportation**

Moving freight is a complex process involving different parties with different priorities. An IoT-enabled blockchain can store the temperatures, position, arrival times, and status of shipping containers as they move. Immutable blockchain transactions help ensure that all parties can trust the data and take action to move products quickly and efficiently.

**Component tracking and compliance**

The ability to track components that go into an aircraft, automobile, or other products is critical for both safety and regulatory compliance. IoT data stored in shared blockchain ledgers enables all parties to see component provenance throughout a product’s life. Sharing this information with regulatory agencies, shippers, and manufacturers is secure, easy, and cost-effective.

**Log operational maintenance data**

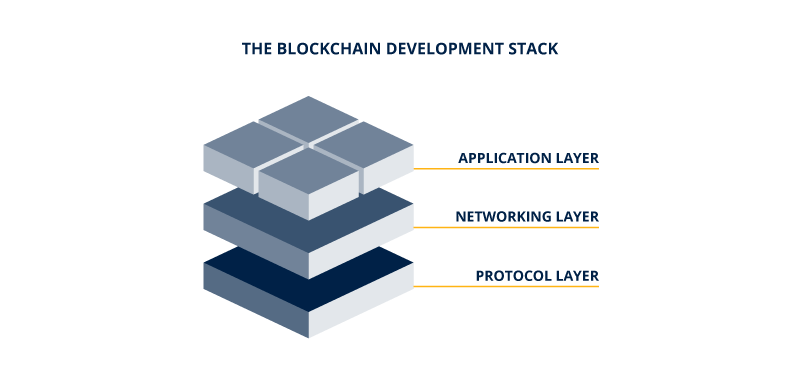
IoT devices track the state of safety for critical machines and their maintenance. From engines to elevators, blockchain provides for a tamper-free ledger of operational data and the resulting maintenance. Third-party repair partners can monitor the blockchain for preventive maintenance and record their work back on the blockchain. Operational records can also be shared with government entities to verify compliance.

**Who is involved in the blockchain network?**

Many working professionals were initially skeptical about blockchain technology’s real-world applications when it was first implemented in 2009. However, the technology has become far more widespread in recent years and is now impacting a vast range of industries. Increasingly, business leaders and other professionals are incorporating the technology and its applications into their strategies.

Blockchain technology can be viewed as a collection of components or layers. There are different ideas around the number and organization of these layers, but for the purpose of this article, we’ll examine the following:

* **Protocol layer**: This includes fundamental architecture as well as the consensus layer, activating layer, contract layer, and application layer.1
* **Networking layer**: This relates to how the protocols (software) are implemented.2
* **Application layer**: This layer acts as a user interface with the blockchain and includes smart contracts, decentralized apps, and chaincode.3



These layers involve various stakeholders at each developmental stage who are involved in infrastructure development, building services and products, funding, or education.

**Stakeholders from the protocol layer**

**1) Developers**

Developers create and optimize the blockchain protocols that serve networks and design the architecture of blockchain systems.4 These professionals must be proficient in data structures and cryptography, as these elements are crucial to the functioning of a blockchain. The protocol layer is mostly concerned with cryptographic keys that will interact with the networks, either public or private.

In public blockchain networks, anyone can see the digital ledger, edit and audit it, and participate in consensus.5 Private blockchain networks are accessible only to verified participants. The developer can override, edit, or delete entries on the chain.6

**2) Researchers and academia**

Blockchain research helps to educate others on blockchain technology’s impact, especially considering the wide-ranging applications it already has on business and society. Major research focuses include market efficiency and economics, asset pricing and valuation, transactions and anonymity, monetary theory and policy, and principles and applications of the technology.7

**Stakeholders from the networking layer**

**1) Miners**

Miners help build consensus among untrusted nodes in a public blockchain, like Bitcoin. They add transactions, bundled into blocks, to the network by solving complex mathematical problems and require considerable computing power and electricity.8

**2) Industry bodies**

Various industry bodies exist to bridge the gaps between researchers, private entities, and public institutions to advocate for the technology and to establish standards. Blockchain’s increasing ubiquity has spurred the adoption of new regulations, concerns around the use of cryptocurrencies for illegal activities, and the need to protect the users of related platforms that offer cryptocurrency-related financial services.9

**3) Traders**

These stakeholders are entities that distrust fiat currency or are motivated to drive a financial profit, and will give others access to the blockchain protocols. This is provided via tokens in the form of cryptocurrency.

**Cryptocurrency trading can occur in two ways:**

* Via leveraged derivatives. You speculate on the price movements without actually buying coins.
* Trading cryptocurrency coins via an exchange. With this method, you open a position by putting up the full asset value. Subsequently, you store the coins in a wallet.

**Stakeholders from the application layer**

For more insight into the workings of blockchain, the online short course from MIT Sloan School of Management offers an in-depth view into the technology and its applications in business.

1) Entrepreneurs

These people create the applications, products, or services that utilize blockchain protocols and networks. Entrepreneurs and start-ups will have an end goal of making a profit, but blockchain entrepreneurs – particularly in the cryptocurrency sphere – are often motivated by an anti-establishment approach to, and distrust of, traditional systems.

2) End-user

End-users utilize blockchain applications, products, or services. These stakeholders are critical to the entire blockchain strategy system, as what they deem valuable affects other stakeholders’ decision-making. The end-user’s response will significantly impact business strategy in the blockchain strategy system.

3) Corporations

These stakeholders are on a mission to utilize blockchain technology to solve business problems or develop new strategies. Many corporations recognize the value of blockchain in building trust and transparency around recruitment, certification, commercial transactions, and data security, as well as increasingly important factors like sustainability and ethical sourcing.13

Below are two examples of how blockchain can benefit corporations:

**Insurance**

The insurance sector is primed for blockchain integration. Utilizing the distributed ledger’s inimitable authentication ability, insurers can independently verify information contained in contracts to enable a simplified process at every stage. From minimizing fraud to developing a system where some claims can be verified and handled with great speed, blockchain technology’s computational power could significantly alter the industry.14

**Forecasting**

Gnosis is an example of an open-source prediction market platform, where users trade cryptocurrencies that represent outcomes of events on an open market. The idea is that aggregating uncensored public opinion on future events can provide a more reliable forecasting tool.15

4) Venture capitalists or investors

These are the individuals or organizations that provide capital to create the blockchain infrastructure. Their opportunities are broadly divided into two sets:16

* **Cryptonetworks**: Investors gain exposure to blockchain protocols via equity, simple agreement for future tokens, or tokens themselves.
* **Ecosystem, picks and shovels, or infrastructure**: These are more conventional venture capital investments in companies with predictable cash flows.

Where do you come in?

If you’re involved in the blockchain ecosystem, it’s likely you fall into one of these stakeholder categories that intersect with the blockchain strategy system.

If you do, you’ll want to keep abreast of the latest blockchain developments. The MIT Sloan School of Management’s six-week [Blockchain Technologies: Business Innovation and Application](https://www.getsmarter.com/products/mit-sloan-blockchain-technologies-business-innovation-and-application-online-program) online short course examines how blockchain is fundamentally changing business and economics. If you join the course, you’ll walk away with tools to help you leverage the technology to drive business innovation and efficiency. Learn more about what you can expect from the program [here](https://www.getsmarter.com/blog/career-advice/what-you-can-look-forward-to-on-the-mit-sloan-blockchain-program/).

The University of Cape Town (UCT), in turn, offers a cryptocurrency focus in the [Blockchain and Digital Currency: The Future of Money](https://www.getsmarter.com/products/uct-blockchain-and-digital-currency-online-short-course) online short course. This six-week online course will expand your working knowledge of blockchain and cryptocurrency assets, and reveal how crypto assets are already shaping the financial industry.

Similarly, the SDA Bocconi School of Management offers a five-week [Bitcoin and Blockchain Program](https://www.getsmarter.com/products/sda-bocconi-school-of-management-bitcoin-and-blockchain-program). This program cuts through the hype around Bitcoin and blockchain by exploring the technical pillars that underpin these powerful technologies.

**What Is Cryptocurrency: Types, Benefits, History**

<https://www.youtube.com/watch?v=8NgVGnX4KOw>

among two or more people. For instance, someone might exchange seven apples for seven oranges. The barter system fell out of popular use because it had some glaring flaws:

* People’s requirements have to coincide—if you have something to trade, someone else has to want it, and you have to want what the other person is offering.
* There’s no common measure of value—you have to decide how many of your items you are willing to trade for other items, and not all items can be divided. For example, you cannot divide a live animal into smaller units.
* The goods cannot be transported easily, unlike our modern currency, which fits in a wallet or is stored on a mobile phone.

After people realized the barter system didn’t work very well, the currency went through a few iterations: In 110 B.C., an official currency was minted; in A.D. 1250, gold-plated florins were introduced and used across Europe; and from 1600 to 1900, the paper currency gained widespread popularity and ended up being used around the world. This is how modern currency as we know it came into existence.

Modern currency includes paper currency, coins, credit cards, and digital wallets—for example, Apple Pay, Amazon Pay, Paytm, PayPal, and so on. All of it is controlled by banks and governments, meaning that there is a centralized regulatory authority that limits how paper currency and credit cards work.

**Traditional Currencies vs. Cryptocurrencies**

Imagine a scenario in which you want to repay a friend who bought you lunch, by sending money online to his or her account. There are several ways in which this could go wrong, including:

* The financial institution could have a technical issue, such as its systems are down or the machines aren’t working properly.
* Your or your friend’s account could have been hacked—for example, there could be a denial-of-service attack or identity theft.
* The transfer limits for your or your friend’s account could have been exceeded.

There is a central point of failure: the bank.

This is why the future of currency lies with cryptocurrency. Now imagine a similar transaction between two people using the bitcoin app. A notification appears asking whether the person is sure he or she is ready to transfer bitcoins. If yes, processing takes place: The system authenticates the user’s identity, checks whether the user has the required balance to make that transaction, and so on. After that’s done, the payment is transferred and the money lands in the receiver’s account. All of this happens in a matter of minutes.

Cryptocurrency, then, removes all the problems of modern banking: There are no limits to the funds you can transfer, your accounts cannot be hacked, and there is no central point of failure. As mentioned above, as of 2018 there are more than 1,600 cryptocurrencies available; some popular ones are Bitcoin, Litecoin, Ethereum, and Zcash. And a new cryptocurrency crops up every single day. Considering how much growth they’re experiencing at the moment, there’s a good chance that there are plenty more to come!

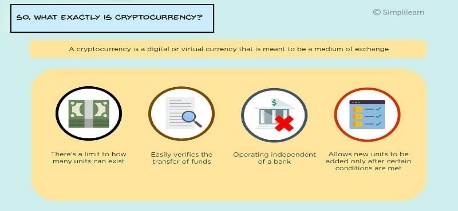
Moving forward, let us discuss what is cryptocurrency.

**What is Cryptocurrency?**

A cryptocurrency is a coded string of data representing a currency unit. Peer-to-peer networks called blockchains monitor and organize cryptocurrency transactions, such as buying, selling, and transferring, and also serve as secure ledgers of transactions. By utilizing encryption technology, cryptocurrencies can serve as both a currency and an accounting system.

A cryptocurrency is a digital or virtual currency that is meant to be a medium of exchange. It is quite similar to real-world currency, except it does not have any physical embodiment, and it uses cryptography to work.

Because cryptocurrencies operate independently and in a decentralized manner, without a bank or a central authority, new units can be added only after certain conditions are met. For example, with Bitcoin, only after a block has been added to the blockchain will the miner be rewarded with bitcoins, and this is the only way new bitcoins can be generated. The limit for bitcoins is 21 million; after this, no more bitcoins will be produced.



**Benefits of Cryptocurrency**

With cryptocurrency, the transaction cost is low to nothing at all—unlike, for example, the fee for [transferring money from a digital wallet](https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-wallet) to a bank account. You can make transactions at any time of the day or night, and there are no limits on purchases and withdrawals. And anyone is free to use cryptocurrency, unlike setting up a bank account, which requires documentation and other paperwork.

International cryptocurrency transactions are faster than wire transfers too. Wire transfers take about half a day for the money to be moved from one place to another. With cryptocurrencies, transactions take only a matter of minutes or even seconds.



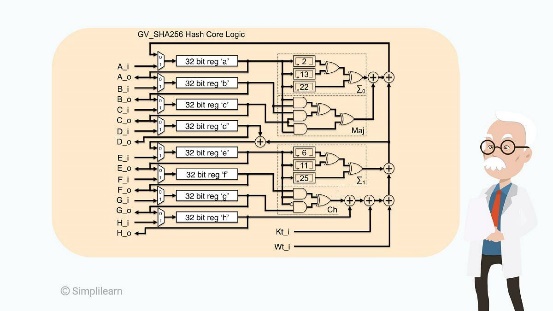
**What is Cryptography?**

Cryptography is a method of using encryption and decryption to secure communication in the presence of third parties with ill intent—that is, third parties who want to steal your data or eavesdrop on your conversation. Cryptography uses computational algorithms such as SHA-256, which is the hashing algorithm that Bitcoin uses; a public key, which is like a digital identity of the user shared with everyone; and a private key, which is a digital signature of the user that is kept hidden.

**Cryptography in Bitcoin Transactions**

In a normal bitcoin transaction, first, there are the transaction details: whom you want to send the bitcoins to and how many bitcoins you want to send. Then the information is passed through a hashing algorithm. [Bitcoin uses the SHA-256 algorithm](https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm). The output is then passed through a signature algorithm with the user’s private key, used to uniquely identify the user. The digitally signed output is then distributed across the network for other users to verify. This is done by using the sender’s public key.

The users who check the transaction to see whether it’s valid or not are known as miners. After this is done, the transaction and several others are added to the blockchain, where the details cannot be changed. The SHA-256 algorithm looks something like in the image below.



You can see how complicated it is, meaning it’s safe to say that the encryption is very difficult to hack.

**Bitcoin vs. Ethereum**

You now know that [Bitcoin is a digital currency](https://www.simplilearn.com/bitcoin-digital-currency-article) that is decentralized and works on the blockchain technology and that it uses a peer-to-peer network to perform transactions. Ether is another popular digital currency, and it’s accepted in the [Ethereum network](https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-ethereum). The Ethereum network uses [blockchain technology to create an open-source platform](https://www.simplilearn.com/decoding-the-blockchain-technology-article) for building and deploying decentralized applications.

Similarities

[Bitcoin and ether](https://www.simplilearn.com/tutorials/blockchain-tutorial/ethereum-vs-bitcoin) are the biggest and most valuable cryptocurrencies right now. Both of them use blockchain technology, in which transactions are added to a container called a block, and a chain of blocks is created in which data cannot be altered. For both, the currency is mined using a method called proof of work, involving a mathematical puzzle that needs to be solved before a block can be added to the blockchain. Finally, both bitcoin and ether are widely used around the world.

**Differences**

Bitcoin is used to send money to someone. The way it works is very similar to the way real-life currency works. Ether is used as a currency within the Ethereum network, although it can be used for real-life transactions as well. Bitcoin transactions are done manually, which means you have to personally perform these transactions when you want them done. With ether, you have the option to make transactions manual or automatic—they are programmable, which means the transactions take place when certain conditions have been met. As for timing, it takes about 10 minutes to perform a bitcoin transaction—this is the time it takes for a block to be added to the blockchain. With ether, it takes about 20 seconds to do a transaction.

There is a limit to how many bitcoins can exist: 21 million. This number is supposed to be reached by the year 2140. Ether is expected to be around for a while and is not to exceed 100 million units. Bitcoin is used for transactions involving goods and services, and ether uses blockchain technology to create a ledger to trigger a transaction when a certain condition is met. Finally, Bitcoin uses the SHA-256 algorithm, and Ethereum uses the ethash algorithm.

As of May 2020, 1 bitcoin equals $8741.81 dollars, and 1 ether equals $190.00.

**The Future of Cryptocurrency**

The world is clearly divided when it comes to cryptocurrencies. On one side are supporters such as Bill Gates, Al Gore and Richard Branson, who say that cryptocurrencies are better than regular currencies. On the other side are people such as Warren Buffet, Paul Krugman, and Robert Shiller, who are against it. Krugman and Shiller, who are both Nobel Prize winners in the field of economics, call it a Ponzi scheme and a means for criminal activities.

In the future, there’s going to be a conflict between regulation and anonymity. Since several cryptocurrencies have been linked with terrorist attacks, governments would want to regulate how cryptocurrencies work. On the other hand, the main emphasis of cryptocurrencies is to ensure that users remain anonymous.

Futurists believe that by the year 2030, cryptocurrencies will occupy 25 percent of national currencies, which means a significant chunk of the world would start believing in cryptocurrency as a mode of transaction. It’s going to be increasingly accepted by merchants and customers, and it will continue to have a volatile nature, which means prices will continue to fluctuate, as they have been doing for the past few years.

That wraps up our cryptocurrency tutorial. If you’d like to learn more about blockchain (the underlying technology of cryptocurrencies such as bitcoin), check out [Simplilearn’s Blockchain Basics Course](https://www.simplilearn.com/introduction-to-blockchain-basics-course). To learn even more and get a blockchain certification to boost your résumé, take the [Blockchain Certification Course](https://www.simplilearn.com/blockchain-certification-training-course).

If you have any questions in the article “what is cryptocurrency”, please ask your questions in the comment section below. Our experts will get back to you at the earliest.

FAQs

1. How Do You Buy Cryptocurrencies?

Bitcoin may be traded on exchanges, which provide investors with a safe and secure platform. The future has here with cryptocurrencies. To begin investing, you must first choose a reputable cryptocurrency exchange where you may buy, sell, and trade cryptocurrencies like Bitcoin, Ethereum, Tron, and others. Select a Broker or a Crypto Exchange. You must first select a broker or cryptocurrency exchange to purchase bitcoin. Then you must create and validate Your Account. Make a cash deposit to begin investing, and then place your cryptocurrency order. Choose a Storage Method.

2. What Is the Point of Cryptocurrency?

Anyone can send and receive money anywhere, using the peer-to-peer payment system. In the real world, cryptocurrency transactions are not carried around and exchanged as tangible money but as digital entries to an online database that identifies specific transactions. The benefits of cryptocurrencies include cheaper and quicker money transactions and decentralized systems that do not fail at a single point.

3. Can You Generate Cryptocurrency?

Anyone may establish a cryptocurrency, but it takes time, money, and other resources, as well as extensive technical skills. The primary possibilities are creating your own blockchain, modifying an existing one, creating a coin on an existing one, or hiring a blockchain engineer. The cost of bitcoin production ranges from $10,000 to $30,000, depending on the chosen option.

4. What Are the Most Popular Cryptocurrencies?

Consider Ravencoin, Ethereum, and Bitcoin to purchase today and retain forever. Due to their volatility, cryptocurrencies are best suited for those that can tolerate risk. For these investors, investing in the leading cryptocurrencies now, while the market is unreliable, may pay off in the long term. One of the biggest cryptocurrency exchanges in the world, Binance, has its own coin called BNB. Although Binance Coin was first designed as a token to pay for reduced transactions, it is now being used to make payments and buy a variety of goods and services.

5. Are Cryptocurrencies Securities?

On the Chicago Mercantile Exchange, the world's largest and most complex financial market, crypto derivatives like Bitcoin futures are offered. According to the Securities and Exchange Commission (SEC), Ethereum and Bitcoin are not securities.

6. How do cryptocurrencies work?

A digital currency, or cryptocurrency, is an alternative payment method developed utilizing encryption methods. By utilizing encryption technology, cryptocurrencies may act as both a medium of exchange and a virtual accounting system. You need a cryptocurrency wallet in order to utilize cryptocurrencies. Blockchain networks power cryptocurrencies. A blockchain is simply a growing collection of digital blocks that serve as a ledger. The distributed ledger of a blockchain allows for the storage of data across several computers in a network. The nodes are the individual computers that validate and store the data.

7. How to invest in cryptocurrency?

Opt for the bitcoin exchange of your choice. Create an account with the bitcoin exchange after that. Spend fiat money to fill your account. Choose the cryptocurrency that you wish to purchase. Put up a purchase order for the cryptocurrency of your choice.

8. What are the key steps to buy cryptocurrency?

Step 1: Pick the best cryptocurrency exchange.

Step 2: Open a trading account and confirm your email. Connect your phone now.

Step 3: Verify your identification in step three. Fund Your Account next.

Step 4: Purchasing and Investing in Cryptocurrency.

Step 5: Store your cryptocurrency.

Step 6: Choose a strategy in the last step.

9. What is the minimum amount you can invest in cryptocurrencies?

You may buy or sell digital money for as low as $2.00 ($2 or €2) that is denominated in your home currency.

10. Can cryptocurrencies be used to make online purchases?

Definitely, despite the fact that cryptocurrencies are not a commonly utilized payment option, a number of businesses have started to accept them in return for their goods and services. Online purchases are increasingly being made using cryptocurrencies. According to Wagner, a number of merchants now accept Bitcoin. You may shop on Overstock.com to buy furniture for your home with cryptocurrency. You may even embark on a spending spree at Nordstrom, which also accepts Bitcoin from clients.

11. How Many Cryptocurrencies Are There?

There are already more than 12,000 cryptocurrencies, and the growth rate is simply astounding. Cryptocurrencies have more than doubled in number between 2021 and 2022. Toward the end of 2021, the market added approximately 1,000 new cryptocurrencies per month.

12. What Are the Different Types of Crypto?

Bitcoin (BTC), Ethereum (ETH), Tether (USDT), USD Coin (USDC), and Binance Coin (BNB)  are some of the popular ones.

**Types of Cryptocurrency**

Presently, there are thousands of cryptocurrencies out there, with many more being started daily. While they all rely on the same premise of a consensus-based, decentralized, and immutable ledger in order to transfer value digitally between trustless parties, there are subtle and not-so-subtle differences between them.

This article will make sense of the landscape and look to help categorize cryptocurrencies into four broad types:

1. Payment cryptocurrency
2. Utility Tokens
3. Stablecoins
4. Central Bank Digital Currencies (CBDC)



**Key Highlights**

* There are thousands of cryptocurrencies out there, with many more being started daily, so how can we classify them?
* They all depend on blockchain technology, but there are many differences.
* Broadly speaking, we will classify them into four categories: Payment Cryptocurrencies, Tokens, Stablecoins, and Central Bank Digital Currencies.

**Payment Cryptocurrency**

The first major type of cryptocurrency is payment cryptocurrency. [Bitcoin](https://corporatefinanceinstitute.com/resources/knowledge/other/bitcoin/), perhaps the most famous cryptocurrency, was the first successful example of a digital payment cryptocurrency. The purpose of a payment cryptocurrency, as the name implies, is not only as a medium of exchange but also as a purely peer-to-peer electronic cash to facilitate transactions.

Broadly speaking, since this type of cryptocurrency is meant to be a general-purpose currency, it has a dedicated blockchain that only supports that purpose. It means that smart contracts and decentralized applications (Dapps) cannot be run on these blockchains.

These payment cryptocurrencies also tend to have a limited number of digital coins that can ever be created, which makes them naturally deflationary. With less and less of these digital coins can be mined, the value of the digital currency is expected to rise.

Examples of payment cryptocurrencies include Bitcoin, Litecoin, Monero, [Dogecoin](https://corporatefinanceinstitute.com/resources/knowledge/other/dogecoin/), and Bitcoin Cash.

**Utility Tokens**

The second major type of cryptocurrency is the Utility Token. Tokens are any cryptographic asset that runs on top of another blockchain. Ethereum network was the first to incorporate the concept of allowing other crypto assets to piggyback on its blockchain.

As a matter of fact, Vitalik Buterin, the founder of Ethereum, envisioned his cryptocurrency as an open-sourced programmable money that could allow smart contracts and decentralized apps to disintermediate legacy financial and legal entities.

Another key difference between tokens and payment cryptocurrency is that tokens, like Ether on the Ethereum network, are not capped. These cryptocurrencies are, therefore, inflationary – meaning that since more and more of these tokens are created, the value of this digital asset should be expected to fall, like a [fiat currency](https://corporatefinanceinstitute.com/resources/knowledge/economics/fiat-money-currency/) in a country that is constantly running its cash printing press.

A Utility Token serves a specific purpose or function on the blockchain, called a use case.

Ether’s use case, as an example, is for paying transaction fees to write something to the Ethereum blockchain or building and purchasing Dapps on the platform. In fact, the Ethereum network was changed in 2021 to expend, or burn off, some of the Ether used in each transaction to align the use case. You will hear these sorts of tokens referred to as Infrastructure Tokens.

**Service Tokens**

Some cryptocurrency projects issue Service Tokens that grant the holder access to or allow them to perform something on a network. One such type of this service token is Storj, an alternative to [Google Drive](https://www.google.com/drive/), Dropbox, or Microsoft Onedrive. The platform rents unused hard drive space to those looking to store data in the Cloud.

These users would pay for the service in Storj’s native utility token. To earn these tokens, those who are storing the data must pass random file verification cryptographically every hour to ensure that the data is still in their possession.

**Finance Tokens**

Another example of a token is Binance’s [Binance Coin (BNB)](https://corporatefinanceinstitute.com/resources/knowledge/other/binance-coin-bnb/), which was created to give the holder discounted trading fees. As this type of token grants access to a cryptocurrency exchange, you will sometimes hear it referred to as an Exchange Token.

Tokens are most commonly sold by Initial Coin Offerings (ICO), which connects early-stage cryptocurrency projects to investors. The ones that represent ownership or other rights to another security or asset are called Security Tokens, a type of fractional ownership. More broadly speaking, exchange and security tokens belong to a larger class of Financial Tokens related to financial transactions, such as borrowing, lending, trading, crowdfunding, and betting.

**Governance Tokens**

Another interesting use of tokens is for governance purposes.  These tokens give its holders a right to vote on certain things within a cryptocurrency network.  Generally, these tend to bigger and more significant changes or decisions and is necessary to maintain the decentralized nature of the network.  This allows the community, through their votes, to decide on proposals, rather than focus the decision-making power in a small group.

An example would be a DAO (Decentralized Autonomous Organizations), which are a type of virtual cooperatives.  The most famous of these is the Genesis DAO.  More currently, the MakerDAO has a separate governance token, called the MKR.  Holders of MKR get to vote on decisions pertaining to MakerDAOs stablecoin, called Dai.

**Media and Entertainment Tokens**

Lastly, there are also Media and Entertainment Tokens, which are used for content, games, and online gambling. An example is Basic Attention Token (BAT), which awards tokens to users who opt-in to view advertisements, which then can be used to top content creators.

**Non-Fungible Tokens (NFTs)**

You might wonder why another commonly heard token hasn’t been mentioned. Non-Fungible Tokens (NFTs) are certainly one of the hottest topics in the Decentralized Finance (DeFI) space. However, NFTs are not a cryptocurrency as cryptocurrencies are fungible – meaning one unit of a particular cryptocurrency is identical to the next.

A holder of one BTC should be completely indifferent if another person offers them another unit of BTC. Same for any cryptocurrency. However, for NFTs, each one is unique and non-fungible, so we don’t include them as a cryptocurrency.

**Stablecoins**

Given the volatility experienced in many digital assets, stablecoins are designed to provide a store of value. They maintain their value because while they are built on a blockchain, this type of cryptocurrency can be exchanged for one or more fiat currencies. So stablecoins are actually pegged to a physical currency, most commonly the U.S. dollar or the Euro.

The company that manages the peg is expected to maintain reserves in order to guarantee the cryptocurrency’s value. This stability, in turn, is attractive to investors who might use stablecoins as a savings vehicle or as a medium of exchange that allows for regular transfers of value free from price swings.

The highest profile stablecoin is Tether’s USDT, which is the third-largest cryptocurrency by market capitalization behind Bitcoin and Ether. The USDT is pegged to the US dollar, meaning its value is supposed to remain stable at 1 USD each. It achieves this by backing every USDT with one US dollar worth of reserve assets in cash or cash equivalents.

Holders can deposit their fiat currency for USDT or redeem their USDT directly with [Tether Limited](https://tether.to/) at the redemption price of $1, less fees that Tether charges. Tether also lends out cash to companies to make money.

However, stablecoins aren’t subject to any government regulation or oversight. In May 2022, another high-profile stablecoin, TerraUSD, and its sibling coin, Luna, collapsed. TerraUSD went from $1 to just 11 cents.

The problem with TerraUSD was that instead of investing reserves into cash or other safe assets, it was backed by its own currency, Luna. During its crash in May, Luna went from over $80 to a fraction of a cent. As holders of TerraUSD clamored to redeem their stablecoins, TerraUSD lost its peg to the dollar.

The lesson here again is to do your due diligence before even buying stablecoins by looking at the whitepaper and understanding how the stablecoin maintains its reserves.

**Central Bank Digital Currencies (CBDC)**

Central Bank Digital Currency is a form of cryptocurrency issued by the central banks of various countries. CBDCs are issued by central banks in token form or with an electronic record associated with the currency and pegged to the domestic currency of the issuing country or region.

Since this digital currency is issued by central banks, the central banks maintain full authority and regulation over the CBDC. The implementation of a CBDC into the financial system and monetary policy is still in the early stages for many countries; however, over time it may become more widely adopted.

Like cryptocurrencies, CBDCs are built upon blockchain technology that should increase payment efficiency and potentially lower transaction costs. While the use of CBDCs is still in the early stages of development for many central banks across the world, several CBDCs are based upon the same principles and technology as cryptocurrencies, such as Bitcoin.

The characteristic of the currency being issued in token form or with electronic records to prove ownership makes it similar to other established cryptocurrencies. However, as CBDCs are effectively monitored and controlled by the issuing government, holders of this cryptocurrency give up the advantage of decentralization, pseudonymity, and lack of censorship.

CBDCs maintain a “paper trail” of transactions for the government, which can lead to taxation and other economic rents to be levied by governments. On the plus side, in a stable political and inflationary environment, CBDCs can be reasonably expected to maintain their value over time or at least track the pegged physical currency.

In addition to having the full faith and credit of the issuing country, buyers of CDBCs would also not have to worry about fraud and abuse that has plagued many other cryptocurrencies.