* **Bitcoin** is a [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) and worldwide [payment system](https://en.wikipedia.org/wiki/Payment_system). It is the first decentralized [digital currency](https://en.wikipedia.org/wiki/Digital_currency), as the system works without a [central bank](https://en.wikipedia.org/wiki/Central_bank) or single administrator. The network is [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) and transactions take place between users directly, without an intermediary. These transactions are verified by network [nodes](https://en.wikipedia.org/wiki/Node_%28networking%29) through the use of [cryptography](https://en.wikipedia.org/wiki/Cryptography) and recorded in a public [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) called a [blockchain](https://en.wikipedia.org/wiki/Bitcoin#Blockchain). Bitcoin was invented by an unknown person or group of people under the name [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) and released as [open-source software](https://en.wikipedia.org/wiki/Open-source_software) in 2009.
* Bitcoins are created as a reward for a process known as [mining](https://en.wikipedia.org/wiki/Bitcoin#Mining). They can be exchanged for other currencies, products, and services. As of February 2015, over 100,000 merchants and vendors accepted bitcoin as payment. Research produced by the [University of Cambridge](https://en.wikipedia.org/wiki/University_of_Cambridge) estimates that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.

|  |
| --- |
| **Denominations** |
| [**Plural**](https://en.wikipedia.org/wiki/Plural) | bitcoins |
| [**Symbol**](https://en.wikipedia.org/wiki/Currency_symbol) | ₿ |
| [**Ticker symbol**](https://en.wikipedia.org/wiki/Ticker_symbol) | BTC, XBT |
| **Subunits** |  |
|  ​1⁄1000 | millibitcoin |
|  ​1⁄1000000 | bit  |
|  ​1⁄100000000 | satoshi |
| **Coins** | [Unspent outputs of transactions](https://en.wikipedia.org/wiki/Unspent_outputs_of_transactions) (in multiples of a satoshi)  |
| **Development** |
| [**Original author(s)**](https://en.wikipedia.org/wiki/Software_developer) | [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) |
| [**White paper**](https://en.wikipedia.org/wiki/White_paper) | [Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf) |
| **Implementation(s)** | [Bitcoin Core](https://en.wikipedia.org/wiki/Bitcoin_Core) |
| **Initial release** | 0.1.0 / 9 January 2009 (9 years ago) |
| [**Latest release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 0.16.0 / 26 February 2018 (14 days ago) |
| **Website** | [bitcoin.org](http://bitcoin.org) |
| **Ledger** |
| **Ledger start** | 3 January 2009 (9 years ago) |
| [**Timestamping scheme**](https://en.wikipedia.org/wiki/Trusted_timestamping) | [Proof-of-work](https://en.wikipedia.org/wiki/Proof-of-work_system) (partial hash inversion) |
| [**Hash function**](https://en.wikipedia.org/wiki/Hash_function) | [SHA-256](https://en.wikipedia.org/wiki/SHA-256) |
| **Issuance** | Decentralized, block reward  |
| **Block reward** | ₿12.5 |
| **Block time** | 10 minutes |
| **Block explorer** | [blockchain.info](http://blockchain.info) |
| **Circulating supply** | ₿16,858,762 (as of 11 February 2018) |
| **Supply limit** | ₿21,000,000 |
| **Valuation** |
| [**Exchange rate**](https://en.wikipedia.org/wiki/Exchange_rate) | Increase[US$](https://en.wikipedia.org/wiki/United_States_dollar)10,710 (as of 17 February 2018)  |
| [**Market cap**](https://en.wikipedia.org/wiki/Market_capitalization) | IncreaseUS$181 billion (as of 17 February 2018)  |
|  |

 The symbol was encoded in [Unicode](https://en.wikipedia.org/wiki/Unicode) version 10.0 at position U+20BF ₿ BITCOIN SIGN in the [Currency Symbols block](https://en.wikipedia.org/wiki/Currency_Symbols_%28Unicode_block%29) in June 2017.

  Compatible with ISO 4217.

 July 2016 to approximately June 2020, halved approximately every four years

**Contents**

* [1 Etymology](https://en.wikipedia.org/wiki/Bitcoin#Etymology)
	+ [1.1 Units](https://en.wikipedia.org/wiki/Bitcoin#Units)
* [2 History](https://en.wikipedia.org/wiki/Bitcoin#History)
* [3 Design](https://en.wikipedia.org/wiki/Bitcoin#Design)
	+ [3.1 Blockchain](https://en.wikipedia.org/wiki/Bitcoin#Blockchain)
	+ [3.2 Transactions](https://en.wikipedia.org/wiki/Bitcoin#Transactions)
	+ [3.3 Transaction fees](https://en.wikipedia.org/wiki/Bitcoin#Transaction_fees)
	+ [3.4 Ownership](https://en.wikipedia.org/wiki/Bitcoin#Ownership)
	+ [3.5 Mining](https://en.wikipedia.org/wiki/Bitcoin#Mining)
		- [3.5.1 Pooled mining](https://en.wikipedia.org/wiki/Bitcoin#Pooled_mining)
	+ [3.6 Supply](https://en.wikipedia.org/wiki/Bitcoin#Supply)
	+ [3.7 Wallets](https://en.wikipedia.org/wiki/Bitcoin#Wallets)
	+ [3.8 Reference implementation](https://en.wikipedia.org/wiki/Bitcoin#Reference_implementation)
	+ [3.9 Decentralization](https://en.wikipedia.org/wiki/Bitcoin#Decentralization)
	+ [3.10 Privacy](https://en.wikipedia.org/wiki/Bitcoin#Privacy)
	+ [3.11 Fungibility](https://en.wikipedia.org/wiki/Bitcoin#Fungibility)
	+ [3.12 Scalability](https://en.wikipedia.org/wiki/Bitcoin#Scalability)
* [4 Economics](https://en.wikipedia.org/wiki/Bitcoin#Economics)
	+ [4.1 Classification](https://en.wikipedia.org/wiki/Bitcoin#Classification)
	+ [4.2 General use](https://en.wikipedia.org/wiki/Bitcoin#General_use)
	+ [4.3 Acceptance by merchants](https://en.wikipedia.org/wiki/Bitcoin#Acceptance_by_merchants)
	+ [4.4 Payment service providers](https://en.wikipedia.org/wiki/Bitcoin#Payment_service_providers)
	+ [4.5 Financial institutions](https://en.wikipedia.org/wiki/Bitcoin#Financial_institutions)
	+ [4.6 As an investment](https://en.wikipedia.org/wiki/Bitcoin#As_an_investment)
	+ [4.7 Venture capital](https://en.wikipedia.org/wiki/Bitcoin#Venture_capital)
	+ [4.8 Price and volatility](https://en.wikipedia.org/wiki/Bitcoin#Price_and_volatility)
	+ [4.9 Ponzi scheme and pyramid scheme concerns](https://en.wikipedia.org/wiki/Bitcoin#Ponzi_scheme_and_pyramid_scheme_concerns)
	+ [4.10 Speculative bubble dispute](https://en.wikipedia.org/wiki/Bitcoin#Speculative_bubble_dispute)
* [5 Legal status, tax and regulation](https://en.wikipedia.org/wiki/Bitcoin#Legal_status,_tax_and_regulation)
* [6 Energy consumption](https://en.wikipedia.org/wiki/Bitcoin#Energy_consumption)
* [7 Criminal activity](https://en.wikipedia.org/wiki/Bitcoin#Criminal_activity)
* [8 In popular culture](https://en.wikipedia.org/wiki/Bitcoin#In_popular_culture)
	+ [8.1 Academia](https://en.wikipedia.org/wiki/Bitcoin#Academia)
	+ [8.2 Film](https://en.wikipedia.org/wiki/Bitcoin#Film)
	+ [8.3 Literature](https://en.wikipedia.org/wiki/Bitcoin#Literature)
	+ [8.4 Television](https://en.wikipedia.org/wiki/Bitcoin#Television)
* [9 See also](https://en.wikipedia.org/wiki/Bitcoin#See_also)
* [10 Notes](https://en.wikipedia.org/wiki/Bitcoin#Notes)
* [11 References](https://en.wikipedia.org/wiki/Bitcoin#References)
* [12 External links](https://en.wikipedia.org/wiki/Bitcoin#External_links)

**Etymology**

The word *bitcoin* first occurred and was defined in the [white paper](https://en.wikipedia.org/wiki/White_paper) that was published on 31 October 2008. It is a [compound](https://en.wikipedia.org/wiki/Compound_%28linguistics%29) of the words [*bit*](https://en.wikipedia.org/wiki/Bit) and [*coin*](https://en.wikipedia.org/wiki/Coin). The white paper frequently uses the shorter *coin*.

There is no uniform convention for *bitcoin* capitalization. Some sources use *Bitcoin*, capitalized, to refer to the technology and [network](https://en.wikipedia.org/wiki/Computer_network) and *bitcoin*, lowercase, to refer to the unit of account. [*The Wall Street Journal*](https://en.wikipedia.org/wiki/The_Wall_Street_Journal),[*The Chronicle of Higher Education*](https://en.wikipedia.org/wiki/The_Chronicle_of_Higher_Education), and the [*Oxford English Dictionary*](https://en.wikipedia.org/wiki/Oxford_English_Dictionary)advocate use of lowercase *bitcoin* in all cases, a convention followed throughout this article.

**Units**

The unit of account of the bitcoin system is *bitcoin*. [Ticker symbols](https://en.wikipedia.org/wiki/Ticker_symbol) used to represent bitcoin are BTC and XBT. Its [Unicode](https://en.wikipedia.org/wiki/Unicode) character is Small amounts of bitcoin used as alternative units are millibitcoin (mBTC), bit (ƀ) and satoshi (sat). Named in homage to bitcoin's creator, a *satoshi* is the smallest amount within bitcoin representing 0.00000001 bitcoins, one hundred millionth of a bitcoin. A *bit* equals 0.000001 bitcoins, one millionth of a bitcoin or 100 satoshis. A *millibitcoin* equals 0.001 bitcoins, one thousandth of a bitcoin or 100,000 satoshis.

**History**

Main article: [History of bitcoin](https://en.wikipedia.org/wiki/History_of_bitcoin)

On 18 August 2008, the domain name "bitcoin.org" was registered. In November that year, a link to a paper authored by [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) titled *Bitcoin: A Peer-to-Peer Electronic Cash System* was posted to a cryptography mailing list. Nakamoto implemented the bitcoin software as [open source code](https://en.wikipedia.org/wiki/Open_source_code) and released it in January 2009 on [SourceForge](https://en.wikipedia.org/wiki/SourceForge). The identity of Nakamoto remains unknown.

In January 2009, the bitcoin network came into existence after Satoshi Nakamoto mined the first ever block on the chain, known as the *genesis block*. Embedded in the coinbase of this block was the following text:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

This note has been interpreted as both a timestamp of the genesis date and a derisive comment on the instability caused by [fractional-reserve banking](https://en.wikipedia.org/wiki/Fractional-reserve_banking).

The receiver of the first bitcoin transaction was [cypherpunk](https://en.wikipedia.org/wiki/Cypherpunk) [Hal Finney](https://en.wikipedia.org/wiki/Hal_Finney_%28cypherpunk%29), who created the first [reusable proof-of-work](https://en.wikipedia.org/wiki/Proof-of-work_system#Reusable_proof-of-work_as_e-money) system (RPOW) in 2004. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto. Other early cypherpunk supporters were Wei Dai, creator of bitcoin predecessor *b-money*, and [Nick Szabo](https://en.wikipedia.org/wiki/Nick_Szabo), creator of bitcoin predecessor [*bit gold*](https://en.wikipedia.org/wiki/Bit_gold).

In the early days, Nakamoto is estimated to have mined 1 million bitcoins. In 2010, Nakamoto handed the network alert key and control of the [Bitcoin Core](https://en.wikipedia.org/wiki/Bitcoin_Core) code repository over to [Gavin Andresen](https://en.wikipedia.org/wiki/Gavin_Andresen), who later became lead developer at the [Bitcoin Foundation](https://en.wikipedia.org/wiki/Bitcoin_Foundation). Nakamoto subsequently disappeared from any involvement in bitcoin. Andresen stated he then sought to decentralize control, saying: "As soon as Satoshi stepped back and threw the project onto my shoulders, one of the first things I did was try to decentralize that. So, if I get hit by a bus, it would be clear that the project would go on." This left opportunity for controversy to develop over the future development path of bitcoin.

On 1 August 2017, a [hard fork](https://en.wikipedia.org/wiki/Fork_%28blockchain%29#Hard_fork) of bitcoin was created, known as [Bitcoin Cash](https://en.wikipedia.org/wiki/Bitcoin_Cash). Bitcoin Cash has a larger block size limit and had an identical blockchain at the time of fork. On 12 November another hard fork, [Bitcoin Gold](https://en.wikipedia.org/wiki/Bitcoin_Gold), was created. Bitcoin Gold changes the proof-of-work algorithm used in mining.

**Design**

**Blockchain**

For a broader coverage related to this topic, see [Blockchain](https://en.wikipedia.org/wiki/Blockchain).



Number of [unspent transaction outputs](https://en.wikipedia.org/wiki/Unspent_transaction_outputs)

The *blockchain* is a public [ledger](https://en.wikipedia.org/wiki/Ledger) that records bitcoin transactions. A novel solution accomplishes this without any trusted central authority: the maintenance of the blockchain is performed by a [network](https://en.wikipedia.org/wiki/Computer_network) of communicating [nodes](https://en.wikipedia.org/wiki/Node_%28networking%29) running bitcoin software. Transactions of the form *payer X sends Y bitcoins to payee Z* are [broadcast](https://en.wikipedia.org/wiki/Broadcasting_%28networking%29) to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The blockchain is a [distributed database](https://en.wikipedia.org/wiki/Distributed_database) – to achieve independent verification of the chain of ownership of any and every bitcoin amount, each network node stores its own copy of the blockchain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the blockchain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent [double-spending](https://en.wikipedia.org/wiki/Double-spending) in an environment without central oversight. Whereas a conventional ledger records the transfers of actual [bills](https://en.wikipedia.org/wiki/Banknote) or [promissory notes](https://en.wikipedia.org/wiki/Promissory_note) that exist apart from it, the blockchain is the only place that bitcoins can be said to exist in the form of [unspent outputs of transactions](https://en.wikipedia.org/wiki/Unspent_outputs_of_transactions).

**Transactions**



Number of bitcoin transactions per month (logarithmic scale)

See also: [Bitcoin network](https://en.wikipedia.org/wiki/Bitcoin_network)

Transactions are defined using a [Forth](https://en.wikipedia.org/wiki/Forth_%28programming_language%29)-like scripting language. Transactions consist of one or more *inputs* and one or more *outputs*. When a user sends bitcoins, the user designates each address and the amount of bitcoin being sent to that address in an output. To prevent double spending, each input must refer to a previous unspent output in the blockchain. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. Since transactions can have multiple outputs, users can send bitcoins to multiple recipients in one transaction. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such a case, an additional output is used, returning the change back to the payer. Any input satoshis not accounted for in the transaction outputs become the transaction fee.

**Transaction fees**

An actual bitcoin transaction including the fee from a webbased [cryptocurrency exchange](https://en.wikipedia.org/wiki/Cryptocurrency_exchange) to a hardware wallet.

Paying a transaction fee is optional. Miners can choose which transactions to process, and they are incentivised to prioritize those that pay higher fees.

Because the size of mined blocks is capped by the network, miners choose transactions based on the fee paid relative to their storage size, not the absolute amount of money paid as a fee. Thus, fees are generally measured in *satoshis per byte*, or *sat/b*. The size of transactions is dependent on the number of inputs used to create the transaction, and the number of outputs.

**Ownership**



Simplified chain of ownership. In reality, a transaction can have more than one input and more than one output.

In the blockchain, bitcoins are registered to bitcoin addresses. Creating a bitcoin address is nothing more than picking a random valid private key and computing the corresponding bitcoin address. This computation can be done in a split second. But the reverse (computing the private key of a given bitcoin address) is mathematically unfeasible and so users can tell others and make public a bitcoin address without compromising its corresponding private key. Moreover, the number of valid private keys is so vast that it is extremely unlikely someone will compute a key-pair that is already in use and has funds. The vast number of valid private keys makes it unfeasible that brute force could be used for that. To be able to spend the bitcoins, the owner must know the corresponding [private key](https://en.wikipedia.org/wiki/Private_key) and [digitally sign](https://en.wikipedia.org/wiki/Digital_signature) the transaction. The network verifies the signature using the [public key](https://en.wikipedia.org/wiki/Public_key).

If the private key is lost, the [bitcoin network](https://en.wikipedia.org/wiki/Bitcoin_network) will not recognize any other evidence of ownership; the coins are then unusable, and effectively lost. For example, in 2013 one user claimed to have lost 7,500 bitcoins, worth $7.5 million at the time, when he accidentally discarded a hard drive containing his private key. A backup of his key(s) would have prevented this.

**Mining**



[Semi-log plot](https://en.wikipedia.org/wiki/Semi-log_plot) of relative mining difficulty

*Mining* is a record-keeping service done through the use of computer [processing power](https://en.wikipedia.org/wiki/Processing_power). Miners keep the blockchain consistent, complete, and unalterable by repeatedly grouping newly broadcast transactions into a *block*, which is then broadcast to the network and verified by recipient nodes. Each block contains a [SHA-256](https://en.wikipedia.org/wiki/SHA-256) [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash) of the previous block, thus linking it to the previous block and giving the blockchain its name.

To be accepted by the rest of the network, a new block must contain a so-called [*proof-of-work*](https://en.wikipedia.org/wiki/Proof-of-work_system#Bitcoin-type_proof-of-work). The system used is based on [Adam Back](https://en.wikipedia.org/wiki/Adam_Back)'s 1997 anti-[spam](https://en.wikipedia.org/wiki/Email_spam) scheme, [Hashcash](https://en.wikipedia.org/wiki/Hashcash). The PoW requires miners to find a number called a [*nonce*](https://en.wikipedia.org/wiki/Cryptographic_nonce), such that when the block content is [hashed](https://en.wikipedia.org/wiki/Cryptographic_hash) along with the nonce, the result is numerically smaller than the network's *difficulty target*. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce values (usually the sequence of tested values is the ascending natural numbers: 0, 1, 2, 3, ...) before meeting the difficulty target.

Every 2,016 blocks (approximately 14 days at roughly 10 min per block), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network. Between 1 March 2014 and 1 March 2015, the average number of nonces miners had to try before creating a new block increased from 16.4 quintillion to 200.5 quintillion.

The proof-of-work system, alongside the chaining of blocks, makes modifications of the blockchain extremely hard, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called *confirmations* of the given block) increases.

**Pooled mining**

Main article: [Mining pool](https://en.wikipedia.org/wiki/Mining_pool)

Computing power is often bundled together or "pooled" to reduce variance in miner income. Individual mining rigs often have to wait for long periods to confirm a block of transactions and receive payment. In a pool, all participating miners get paid every time a participating server solves a block. This payment depends on the amount of work an individual miner contributed to help find that block.

**Supply**



Total bitcoins in circulation.

 The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees. of 9 July 2016, the reward amounted to 12.5 newly created bitcoins per block added to the blockchain. To claim the reward, a special transaction called a *coinbase* is included with the processed payments. All bitcoins in existence have been created in such coinbase transactions. The [bitcoin protocol](https://en.wikipedia.org/wiki/Bitcoin_protocol) specifies that the reward for adding a block will be halved every 210,000 blocks (approximately every four years). Eventually, the reward will decrease to zero, and the limit of 21 million bitcoins[[e]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-69) will be reached [c.](https://en.wikipedia.org/wiki/Circa) 2140; the record keeping will then be rewarded by transaction fees solely.

In other words, bitcoin's inventor Nakamoto set a [monetary policy](https://en.wikipedia.org/wiki/Monetary_policy) based on [artificial scarcity](https://en.wikipedia.org/wiki/Artificial_scarcity) at bitcoin's inception that there would only ever be 21 million bitcoins in total. Their numbers are being released roughly every ten minutes and the rate at which they are generated would drop by half every four years until all were in [circulation](https://en.wikipedia.org/wiki/Circulation_%28currency%29).

**Wallets**

For a broader coverage related to this topic, see [Cryptocurrency wallet](https://en.wikipedia.org/wiki/Cryptocurrency_wallet).



Electrum bitcoin wallet



Bitcoin paper wallet generated at bitaddress.org



Trezor hardware wallet

A *wallet* stores the information necessary to transact bitcoins. While wallets are often described as a place to hold or store bitcoins, due to the nature of the system, bitcoins are inseparable from the blockchain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. Bitcoin uses [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography), in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys.

There are three modes which wallets can operate in. They have an inverse relationship with regards to trustlessness and computational requirements.

* *Full clients* verify transactions directly on a local copy of the blockchain (over 150 GB As of January 2018). They are the most secure and reliable way of using the network, as trust in external parties is not required. Full clients check the validity of mined blocks, preventing them from transacting on a chain that breaks or alters network rules. Because of its size and complexity, storing the entire blockchain is not suitable for all computing devices.
* *Pruning clients* store only the set of transactions that have not been spent (the "UTXO set"), thereby reducing the size of data they need to store, while simultaneously allowing them to validate new transactions. However, if miners alter the blockchain at a point suitably far back in time (a "reorg"), the pruning client must re-validate the entire blockchain from its genesis.
* *Lightweight clients* consult full clients to send and receive transactions without requiring a local copy of the entire blockchain (see [simplified payment verification](https://en.wikipedia.org/wiki/Bitcoin_network#Payment_verification) – SPV). This makes lightweight clients much faster to set up and allows them to be used on low-power, low-bandwidth devices such as smartphones. When using a lightweight wallet, however, the user must trust the server to a certain degree, as it can report faulty values back to the user. Lightweight clients follow the longest blockchain and do not ensure it is valid, requiring trust in miners.

Third-party internet services called *online wallets* offer similar functionality but may be easier to use. In this case, credentials to access funds are stored with the online wallet provider rather than on the user's hardware. As a result, the user must have complete trust in the wallet provider. A malicious provider or a breach in server security may cause entrusted bitcoins to be stolen. An example of such a security breach occurred with [Mt. Gox](https://en.wikipedia.org/wiki/Mt._Gox) in 2011. This has led to the often-repeated meme "Not your keys, not your bitcoin".

*Physical wallets* store offline the credentials necessary to spend bitcoins. One notable example was a novelty coin with these credentials printed on the reverse side. *Paper wallets* are simply paper printouts.

Another type of wallet called a *hardware wallet* keeps credentials offline while facilitating transactions.

**Reference implementation**

Further information: [Bitcoin Core](https://en.wikipedia.org/wiki/Bitcoin_Core)

The first wallet program – simply named "Bitcoin" – was released in 2009 by [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) as [open-source](https://en.wikipedia.org/wiki/Open_source) code. In version 0.5 the client moved from the [wxWidgets](https://en.wikipedia.org/wiki/WxWidgets) user interface toolkit to [Qt](https://en.wikipedia.org/wiki/Qt_%28software%29), and the whole bundle was referred to as "Bitcoin-Qt". After the release of version 0.9, the software bundle was renamed "Bitcoin Core" to distinguish itself from the underlying network. It is sometimes referred to as the "Satoshi client".

While a decentralized system cannot have an "official" implementation, Bitcoin Core is considered to be bitcoin's [reference client](https://en.wikipedia.org/wiki/Reference_implementation). As such, it serves to define the bitcoin protocol and acts as a standard for other implementations. Today, other alternative clients ([forks](https://en.wikipedia.org/wiki/Fork_%28software_development%29) of Bitcoin Core) exist, such as [Bitcoin XT](https://en.wikipedia.org/wiki/Bitcoin_XT), [Bitcoin Unlimited](https://en.wikipedia.org/wiki/Bitcoin_Unlimited), and Parity Bitcoin.

**Decentralization**

Bitcoin was designed not to need a central authority and the bitcoin network is considered to be decentralized. However, researchers have pointed out a visible "trend towards centralization" by the means of miners joining large [mining pools](https://en.wikipedia.org/wiki/Mining_pool) to minimise the variance of their income. According to researchers, other parts of the ecosystem are also "controlled by a small set of entities", notably online wallets and simplified payment verification (SPV) clients.

Because transactions on the network are confirmed by miners, decentralization of the network requires that no single miner or mining pool obtains 51% of the hashing power, which would allow them to [double-spend](https://en.wikipedia.org/wiki/Double-spending) coins, prevent certain transactions from being verified and prevent other miners from earning income. As of 2013 just six mining pools controlled 75% of overall bitcoin hashing power.

In 2014 mining pool [Ghash.io](https://en.wikipedia.org/wiki/Ghash.io) obtained 51% hashing power which raised significant controversies about the safety of the network. The pool has voluntarily capped their hashing power at 39.99% and requested other pools to act responsibly for the benefit of the whole network.

**Privacy**

Bitcoin is [pseudonymous](https://en.wikipedia.org/wiki/Pseudonymous), meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information.

To heighten financial privacy, a new bitcoin address can be generated for each transaction. For example, hierarchical deterministic wallets generate [pseudorandom](https://en.wikipedia.org/wiki/Pseudorandom) "rolling addresses" for every transaction from a single [seed](https://en.wikipedia.org/wiki/Random_seed), while only requiring a single passphrase to be remembered to recover all corresponding private keys. Researchers at [Stanford University](https://en.wikipedia.org/wiki/Stanford_University) and [Concordia University](https://en.wikipedia.org/wiki/Concordia_University) have also shown that bitcoin exchanges and other entities can prove assets, [liabilities](https://en.wikipedia.org/wiki/Liability_%28financial_accounting%29), and [solvency](https://en.wikipedia.org/wiki/Solvency) without revealing their addresses using [zero-knowledge proofs](https://en.wikipedia.org/wiki/Zero-knowledge_proof). "Bulletproofs," a version of Confidential Transactions proposed by Greg Maxwell, have been tested by Professor [Dan Boneh](https://en.wikipedia.org/wiki/Dan_Boneh) of Stanford. Other solutions such Merkelized Abstract Syntax Trees (MAST), pay-to-script-hash (P2SH) with MERKLE-BRANCH-VERIFY, and "Tail Call Execution Semantics, have also been proposed to support private smart contracts.

**Fungibility**

Wallets and similar software technically handle all bitcoins as equivalent, establishing the basic level of [fungibility](https://en.wikipedia.org/wiki/Fungibility). Researchers have pointed out that the history of each bitcoin is registered and publicly available in the blockchain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin's fungibility. Projects such as [CryptoNote](https://en.wikipedia.org/wiki/CryptoNote), [Zerocoin](https://en.wikipedia.org/wiki/Zerocoin), and [Dark Wallet](https://en.wikipedia.org/wiki/Dark_Wallet) aim to address these privacy and fungibility issues.

**Scalability**

Main article: [Bitcoin scalability problem](https://en.wikipedia.org/wiki/Bitcoin_scalability_problem)

The blocks in the blockchain were not limited originally. The block size limit of one [megabyte](https://en.wikipedia.org/wiki/Megabyte) was introduced by Satoshi Nakamoto in 2010, as an anti-spam measure. Eventually the block size limit of one megabyte created problems for transaction processing, such as increasing transaction fees and delayed processing of transactions that cannot be fit into a block.

On 24 August 2017 (at block 481,824), [Segregated Witness](https://en.wikipedia.org/wiki/Segregated_Witness) (SegWit) went live, introducing a new transaction format where signature data is separated and known as the *witness*. The upgrade replaced the block size limit with a limit on a new measure called *block weight*, which counts non-witness data four times as much as witness data, and allows a maximum weight of 4 megabytes. Thus, per computer scientist Jochen Hoenicke, the actual block capacity depends on the ratio of SegWit transactions in the block, and on the ratio of signature data. Based on his estimate, if the ratio of SegWit transactions is 50%, the block capacity may be 1.25 megabytes. According to Hoenicke, if native SegWit addresses from Bitcoin Core version 0.16.0 are used, and SegWit adoption reaches 90 to 95%, a block size of up to 1.8 megabytes is possible.

**Economics**

**Classification**

Bitcoin is a [digital asset](https://en.wikipedia.org/wiki/Digital_asset) designed by its inventor, Satoshi Nakamoto, to work as a currency. It is commonly referred to with terms like digital currency, [digital cash](https://en.wikipedia.org/wiki/Digital_cash), [virtual currency](https://en.wikipedia.org/wiki/Virtual_currency),[[4]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-satoshi_unit-6) [electronic currency](https://en.wikipedia.org/wiki/Electronic_currency), or cryptocurrency.

The question whether bitcoin is a [currency](https://en.wikipedia.org/wiki/Currency) or not is still disputed. Bitcoins have three useful qualities in a currency, according to *The Economist* in January 2015: they are "hard to earn, limited in supply and easy to verify". Economists define money as a [store of value](https://en.wikipedia.org/wiki/Store_of_value), a [medium of exchange](https://en.wikipedia.org/wiki/Medium_of_exchange), and a [unit of account](https://en.wikipedia.org/wiki/Unit_of_account) and agree that bitcoin has some way to go to meet all these criteria. It does best as a medium of exchange; as of February 2015 the number of merchants accepting bitcoin had passed 100,000. As of March 2014, the bitcoin market suffered from [volatility](https://en.wikipedia.org/wiki/Volatility_%28finance%29), limiting the ability of bitcoin to act as a stable store of value, and retailers accepting bitcoin use other currencies as their principal unit of account.

**General use**



Liquidity (estimated, USD/year, logarithmic scale).

According to research produced by [Cambridge University](https://en.wikipedia.org/wiki/Cambridge_University), there were between 2.9 million and 5.8 million unique users using a cryptocurrency wallet, as of 2017, most of them using bitcoin. The number of users has grown significantly since 2013, when there were 300,000 to 1.3 million users.

**Acceptance by merchants**

In 2015, the number of merchants accepting bitcoin exceeded 100,000. Instead of 2–3% typically imposed by [credit card](https://en.wikipedia.org/wiki/Credit_card) processors, merchants accepting bitcoins often pay fees under 2%, down to 0%. Firms that accepted payments in bitcoin as of December 2014 included [PayPal](https://en.wikipedia.org/wiki/PayPal)[Microsoft](https://en.wikipedia.org/wiki/Microsoft)[Dell](https://en.wikipedia.org/wiki/Dell), and [Newegg](https://en.wikipedia.org/wiki/Newegg). In 2017 bitcoin's acceptance among major online retailers included three out of the top 500 online merchants, down from five in 2016. Reasons for this fall include high transaction fees due to bitcoin's scalability issues, long transaction times and a rise in value making consumers unwilling to spend it. In November 2017 [PwC](https://en.wikipedia.org/wiki/PwC) accepted bitcoin at its Hong Kong office in exchange for providing advisory services to local companies who are specialists in blockchain technology and cryptocurrencies, the first time any Big Four accounting firm accepted the cryptocurrency as payment.

**Payment service providers**

Merchants accepting bitcoin ordinarily use the services of bitcoin payment service providers such as [BitPay](https://en.wikipedia.org/wiki/BitPay) or [Coinbase](https://en.wikipedia.org/wiki/Coinbase). When a customer pays in bitcoin, the payment service provider accepts the bitcoin on behalf of the merchant, converts it to the local currency, and sends the obtained amount to merchant's bank account, charging a fee for the service.

**Financial institutions**

Bitcoins can be bought on [digital currency exchanges](https://en.wikipedia.org/wiki/Digital_currency_exchange). According to [Tony Gallippi](https://en.wikipedia.org/wiki/Tony_Gallippi), a co-founder of [BitPay](https://en.wikipedia.org/wiki/BitPay), "banks are scared to deal with bitcoin companies, even if they really want to". In 2014, the [National Australia Bank](https://en.wikipedia.org/wiki/National_Australia_Bank) closed accounts of businesses with ties to bitcoin, and [HSBC](https://en.wikipedia.org/wiki/HSBC) refused to serve a hedge fund with links to bitcoin. Australian banks in general have been reported as closing down bank accounts of operators of businesses involving the currency;[[121]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-afr.com-129) this has become the subject of an investigation by the [Australian Competition and Consumer Commission](https://en.wikipedia.org/wiki/Australian_Competition_and_Consumer_Commission). Nonetheless, Australian banks have trialled trading between each other using the blockchain technology on which bitcoin is based.

In a 2013 report, Bank of America Merrill Lynch stated that "we believe bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers." In June 2014, the first bank that converts deposits in currencies instantly to bitcoin without any fees was opened in Boston.

Plans were announced to include a bitcoin futures option on the [Chicago Mercantile Exchange](https://en.wikipedia.org/wiki/Chicago_Mercantile_Exchange) in 2017. Trading in bitcoin futures was announced to begin on 10 December 2017.

**As an investment**

Some Argentinians have bought bitcoins to protect their savings against high inflation or the possibility that governments could confiscate savings accounts. During the [2012–2013 Cypriot financial crisis](https://en.wikipedia.org/wiki/2012%E2%80%932013_Cypriot_financial_crisis), bitcoin purchases in Cyprus rose due to fears that savings accounts would be confiscated or taxed.

The [Winklevoss twins](https://en.wikipedia.org/wiki/Winklevoss_twins) have invested into bitcoins. In 2013 *The Washington Post* claimed that they owned 1% of all the bitcoins in existence at the time.

Other methods of investment are bitcoin funds. The first regulated bitcoin fund was established in Jersey in July 2014 and approved by the Jersey Financial Services Commission. *Forbes* started publishing arguments in favor of investing in December 2015.

In 2013 and 2014, the [European Banking Authority](https://en.wikipedia.org/wiki/European_Banking_Authority) and the [Financial Industry Regulatory Authority](https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority) (FINRA), a United States [self-regulatory organization](https://en.wikipedia.org/wiki/Self-regulatory_organization), warned that investing in bitcoins carries significant risks. Forbes named bitcoin the best investment of 2013. In 2014, Bloomberg named bitcoin one of its worst investments of the year. In 2015, bitcoin topped Bloomberg's currency tables.

According to bitinfocharts.com, in 2017 there are 9,272 bitcoin wallets with more than $1 million worth of bitcoins. The exact number of bitcoin millionaires is uncertain as a single person can have more than one bitcoin wallet.

**Venture capital**

[Venture capitalists](https://en.wikipedia.org/wiki/Venture_capital), such as [Peter Thiel](https://en.wikipedia.org/wiki/Peter_Thiel)'s [Founders Fund](https://en.wikipedia.org/wiki/Founders_Fund), which invested [US$](https://en.wikipedia.org/wiki/United_States_dollar)3 million in [BitPay](https://en.wikipedia.org/wiki/BitPay), do not purchase bitcoins themselves, instead funding bitcoin infrastructure like [companies](https://en.wikipedia.org/wiki/List_of_bitcoin_companies) that provide payment systems to merchants, exchanges, wallet services, etc. In 2012, an incubator for bitcoin-focused start-ups was founded by Adam Draper, with financing help from his father, venture capitalist [Tim Draper](https://en.wikipedia.org/wiki/Timothy_C._Draper), one of the largest bitcoin holders after winning an auction of 30,000 bitcoins, at the time called 'mystery buyer'. The company's goal is to fund 100 bitcoin businesses within 2–3 years with $10,000 to $20,000 for a 6% stake. Investors also invest in bitcoin mining. According to a 2015 study by [Paolo Tasca](https://en.wikipedia.org/wiki/Paolo_Tasca), bitcoin startups raised almost $1 billion in three years (Q1 2012 – Q1 2015).

**Price and volatility**



Price[[f]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-BTCinUSD-150) *(left y-axis, logarithmic scale)* and volatility[[g]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-151) *(right y-axis)*.

The price of bitcoins has gone through various cycles of appreciation and depreciation referred to by some as [bubbles](https://en.wikipedia.org/wiki/Economic_bubble) and busts. In 2011, the value of one bitcoin rapidly rose from about US$0.30 to US$32 before returning to US$2. In the latter half of 2012 and during the [2012–13 Cypriot financial crisis](https://en.wikipedia.org/wiki/2012%E2%80%9313_Cypriot_financial_crisis), the bitcoin price began to rise, reaching a high of US$266 on 10 April 2013, before crashing to around US$50. On 29 November 2013, the cost of one bitcoin rose to a peak of US$1,242. In 2014, the price fell sharply, and as of April remained depressed at little more than half 2013 prices. As of August 2014 it was under US$600.

According to [Mark T. Williams](https://en.wikipedia.org/wiki/Mark_T._Williams), as of 2014, bitcoin has [volatility](https://en.wikipedia.org/wiki/Volatility_%28finance%29) seven times greater than gold, eight times greater than the [S&P 500](https://en.wikipedia.org/wiki/S%26P_500), and 18 times greater than the US dollar. According to *Forbes*, there are uses where volatility does not matter, such as online gambling, tipping, and international remittances.

According to an article in *The Wall Street Journal*, as of 19 April 2016, bitcoin had been more stable than gold for the preceding 24 days, and it was suggested that its value might be more stable in the future. On 3 March 2017, the price of a bitcoin surpassed the market value of an ounce of [gold](https://en.wikipedia.org/wiki/Gold_as_an_investment) for the first time as its price surged to an all-time high of $1,268. A study in *Electronic Commerce Research and Applications*, going back through the network's historical data, showed the value of the bitcoin network as measured by the price of bitcoins, to be roughly proportional to the square of the number of daily unique users participating on the network, i.e. that the network is "fairly well modeled by the [Metcalfe's law](https://en.wikipedia.org/wiki/Metcalfe%27s_law)".

**Ponzi scheme and pyramid scheme concerns**

Various journalists, economists, and the central bank of Estonia have voiced concerns that bitcoin is a [Ponzi scheme](https://en.wikipedia.org/wiki/Ponzi_scheme). In 2013, [Eric Posner](https://en.wikipedia.org/wiki/Eric_Posner), a law professor at the University of Chicago, stated that "a real Ponzi scheme takes fraud; bitcoin, by contrast, seems more like a collective delusion." A 2014 report by the [World Bank](https://en.wikipedia.org/wiki/World_Bank) concluded that bitcoin was not a deliberate Ponzi scheme. The Swiss [Federal Council](https://en.wikipedia.org/wiki/Federal_Council_%28Switzerland%29) examined the concerns that bitcoin might be a pyramid scheme; it concluded that "Since in the case of bitcoin the typical promises of profits are lacking, it cannot be assumed that bitcoin is a pyramid scheme." In July 2017, billionaire [Howard Marks](https://en.wikipedia.org/wiki/Howard_Marks_%28investor%29) referred to bitcoin as a [pyramid scheme](https://en.wikipedia.org/wiki/Pyramid_scheme).

On 12 September 2017, [Jamie Dimon](https://en.wikipedia.org/wiki/Jamie_Dimon), CEO of [JP Morgan Chase](https://en.wikipedia.org/wiki/JP_Morgan_Chase), called bitcoin a "fraud" and said he would fire anyone in his firm caught trading it. [Zero Hedge](https://en.wikipedia.org/wiki/Zero_Hedge) claimed that the same day Dimon made his statement, JP Morgan also purchased a large amount of bitcoins for its clients. In a January 2018 interview Dimon voiced regrets about his earlier remarks, and said "The blockchain is real. You can have cryptodollars in yen and stuff like that. [ICOs](https://en.wikipedia.org/wiki/Initial_coin_offering) ... you got to look at every one individually."

**Speculative bubble dispute**

Main article: [Cryptocurrency bubble](https://en.wikipedia.org/wiki/Cryptocurrency_bubble)

Bitcoin has been labelled a [*speculative bubble*](https://en.wikipedia.org/wiki/Speculative_bubble) by many including former [Fed Chairman](https://en.wikipedia.org/wiki/Federal_Reserve_Chairman) [Alan Greenspan](https://en.wikipedia.org/wiki/Alan_Greenspan)and economist [John Quiggin](https://en.wikipedia.org/wiki/John_Quiggin).[[166]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-BMH-176) [Nobel Memorial Prize](https://en.wikipedia.org/wiki/Nobel_Memorial_Prize_in_Economic_Sciences) laureate [Robert Shiller](https://en.wikipedia.org/wiki/Robert_Shiller) said that bitcoin "exhibited many of the characteristics of a speculative bubble". Journalist Matthew Boesler in 2013 rejected the speculative bubble label and saw bitcoin's quick rise in price as nothing more than normal economic forces at work. Timothy B. Lee, in a 2013 piece for *The Washington Post* pointed out that the observed cycles of appreciation and depreciation don't correspond to the definition of speculative bubble. On 14 March 2014, the American business magnate [Warren Buffett](https://en.wikipedia.org/wiki/Warren_Buffett) said, "Stay away from it. It's a mirage, basically." During their time as bitcoin developers, Gavin Andresen and Mike Hearn warned that bubbles may occur.

**Legal status, tax and regulation**

Main article: [Legality of bitcoin by country or territory](https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory)

Because of bitcoin's decentralized nature, nation-states cannot shut down the network or alter its technical rules. However, the use of bitcoin can be criminalized, and shutting down exchanges and the peer-to-peer economy in a given country would constitute a "de facto ban". The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.

**Energy consumption**

Bitcoin has been criticized for the amounts of electricity consumed by mining. As of 2015, *The Economist* estimated that even if all miners used modern facilities, the combined electricity consumption would be 166.7 megawatts (1.46 terawatt-hours per year). At the end of 2017, the global bitcoin mining activity was estimated to consume between 1 and 4 gigawatts of electricity (between 9 and 35 TWh a year), with 1.2 GW as the theoretical lower bound assuming that everyone is using the most energy-efficient mining hardware available.

To lower the costs, bitcoin miners have set up in places like Iceland where [geothermal energy](https://en.wikipedia.org/wiki/Geothermal_energy) is cheap and cooling [Arctic](https://en.wikipedia.org/wiki/Arctic) air is free. Bitcoin miners are known to use [hydroelectric power](https://en.wikipedia.org/wiki/Hydroelectric_power) in [Tibet](https://en.wikipedia.org/wiki/Tibet), [Quebec](https://en.wikipedia.org/wiki/Quebec), and [Austria](https://en.wikipedia.org/wiki/Austria) to reduce electricity costs. Miners are attracted to suppliers such as [Hydro Quebec](https://en.wikipedia.org/wiki/Hydro_Quebec) that have energy surpluses. According to a [University of Cambridge](https://en.wikipedia.org/wiki/University_of_Cambridge) study, much of bitcoin mining is done in China, where electricity is subsidized by the government. **Criminal activity**

See also: [Bitcoin network § Criminal activity](https://en.wikipedia.org/wiki/Bitcoin_network#Criminal_activity)

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media. In the United States, the [FBI](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) prepared an intelligence assessment, the [SEC](https://en.wikipedia.org/wiki/U.S._Securities_and_Exchange_Commission) issued a pointed warning about investment schemes using virtual currencies, and the [U.S. Senate](https://en.wikipedia.org/wiki/U.S._Senate) held a hearing on virtual currencies in November 2013.

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods. In 2014, researchers at the [University of Kentucky](https://en.wikipedia.org/wiki/University_of_Kentucky) found "robust evidence that computer programming enthusiasts and illegal activity drive interest in bitcoin, and find limited or no support for political and investment motives".

**In popular culture**

**Academia**

In September 2015, the establishment of the [peer-reviewed](https://en.wikipedia.org/wiki/Peer-reviewed) [academic journal](https://en.wikipedia.org/wiki/Academic_journal) [*Ledger*](https://en.wikipedia.org/wiki/Ledger_%28journal%29) ([ISSN](https://en.wikipedia.org/wiki/International_Standard_Serial_Number) [2379-5980](https://www.worldcat.org/search?fq=x0:jrnl&q=n2:2379-5980)) was announced. It will cover studies of cryptocurrencies and related technologies, and is published by the [University of Pittsburgh](https://en.wikipedia.org/wiki/University_of_Pittsburgh).[[186]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-196)[[187]](https://en.wikipedia.org/wiki/Bitcoin#cite_note-197) The journal encourages authors to [digitally sign](https://en.wikipedia.org/wiki/Digital_signature) a [file hash](https://en.wikipedia.org/wiki/Hash_function) of submitted papers, which will then be [timestamped](https://en.wikipedia.org/wiki/Trusted_timestamping) into the bitcoin [blockchain](https://en.wikipedia.org/wiki/Blockchain). Authors are also asked to include a personal bitcoin address in the first page of their papers.

**Film**

The documentary film, [*The Rise and Rise of Bitcoin*](https://en.wikipedia.org/wiki/The_Rise_and_Rise_of_Bitcoin) (late 2014), features interviews with people who use bitcoin, such as a computer programmer and a drug dealer.

**Literature**

In [Charles Stross](https://en.wikipedia.org/wiki/Charles_Stross)' science fiction novel, [*Neptune's Brood*](https://en.wikipedia.org/wiki/Neptune%27s_Brood), "bitcoin" (a modified version) is used as the universal [interstellar](https://en.wikipedia.org/wiki/Interstellar_travel) payment system.

**Television**

In November 2017, the American sitcom, [*The Big Bang Theory*](https://en.wikipedia.org/wiki/The_Big_Bang_Theory), dedicated an episode on bitcoins called "[The Bitcoin Entanglement](https://en.wikipedia.org/wiki/The_Bitcoin_Entanglement)". In the episode, after hearing the price of a bitcoin had risen to $5,000, friends try to track down bitcoins they mined seven years earlier.