



**A Look At Blockchain Technology**

**What is Blockchain?**

The Blockchain is a decentralized ledger of all transactions across a peer to peer network. Using this technology, participants can confirm transactions without the need of central certifying authority. And it is the technology that enables the existence of cryptocurrency (among other things) Potential applications include fund transfers, selling trade, voting, and many other uses.

**What is Cryptocurrency?**

A cryptocurrency is a medium of exchange which is created and stored electronically in Blockchain using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin and Ethereum are the best-known examples of cryptocurrency.

**Traits of Cryptocurrency:**

1. It has no physical form and exists only in the network.  
2. It has no intrinsic value i.e it is not redeemable for other currencies  
3. Its supply is not determined by a bank and the network is completely decentralized.

**How Blockchain Works?**

The technology idea behind the Blockchain is similar to that of a database, except the way you interact with the database is different. So, let’s understand the concept how it works:

Someone requests a transaction.  
*1. The requested transaction is broadcasted to P2P network consisted of computers known as nodes.*  
*2. Validation: The network of nodes validates the transaction and user’s status using known algorithms.*  
*3. A verified transaction can include cryptocurrency, contracts, records or other information.*  
*4. Once verified, the transaction is linked to other transactions to create a new block of data for the ledger.*  
*5. The new block is then appended to the existing Blockchain, in a way that is permanent and unalterable.*   
*6. The transaction is finally complete.*

**Why is it so revolutionary?**

Blockchain technology can operate for almost every type of transaction including money, goods, and property. Its potential uses are virtually endless: from managing taxes to enabling migrants to send money to their families in countries where the banking system is terrible.

Blockchain can also help to lessen frauds every transaction is recorded and distributed on a public ledger for anyone to see.

**Potential Applications:**

Blockchain also has potential applications far behind Bitcoin and other cryptocurrencies. Let’s have a look  
1. Automotive: Consumers can use the Blockchain to manage fractional ownership in autonomous cars.  
2. Financial Services: Faster and cheaper settlements can save the billions of dollars from transaction costs while improving transparency.  
3. Voting: Using Blockchain codes, a constituent can cast votes via smartphone, tablet or computer, resulting in immediately verifiable results.  
4. HealthCare: Patients encrypted health information can be shared with multiple providers without the risk of privacy breaches.

**Who is Using it?**

In theory, if Blockchain goes mainstream, anyone with access to the internet would be able to use it to make transactions. Currently, only a tiny proportion of global GDP (around 0.025%, or $20 billion) is held in the Blockchain, according to a [survey](http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf): by the World Economic Forum’s Global Agenda Council.

The Forum’s research suggests this will increase significantly over the next decade, as banks, insurers and tech firms perceive the technology as a means to speed up contracts and cut costs.  
Companies pursuing to adapt Blockchain include UBS, Microsoft, IBM, etc. The Bank of Canada is also exploring the technology.

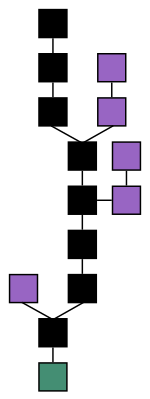
**Wrapping Up:**

Overall, the Blockchain technology has the potential to transform several industries from advertising to energy distribution. The main innovation is that the technology enables market participants to transfer assets across the internet without the requirement for a centralized third party.

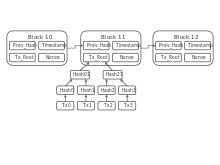
From a marketing perspective, it’s helpful to consider Blockchain technology as a type of next-generation business process of improving the software. Collaborative technology, such as Blockchain, promises the ability to enhance the business processes that happen between the companies, radically lowering the “cost of trust.”

And that’s all about Blockchain technology. If you have any queries or feeling something left behind, please comment below now. We will be happy to answer all of your questions related to it.

# Blockchain

[](https://en.wikipedia.org/wiki/File:Blockchain.svg)

Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

[](https://en.wikipedia.org/wiki/File:Bitcoin_Block_Data.svg)

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

A **blockchain**, originally **block chain**, is a continuously growing list of [records](https://en.wikipedia.org/wiki/Record_%28computer_science%29), called *blocks*, which are linked and secured using [cryptography](https://en.wikipedia.org/wiki/Cryptography). Each block typically contains a [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash_function) of the previous block, a [timestamp](https://en.wikipedia.org/wiki/Trusted_timestamping) and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed [ledger](https://en.wikipedia.org/wiki/Ledger), a blockchain is typically managed by a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are [secure by design](https://en.wikipedia.org/wiki/Secure_by_design) and exemplify a distributed computing system with high [Byzantine fault tolerance](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance). [Decentralized](https://en.wikipedia.org/wiki/Decentralized) consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other [records management](https://en.wikipedia.org/wiki/Records_management) activities, such as [identity management](https://en.wikipedia.org/wiki/Identity_management),[transaction processing](https://en.wikipedia.org/wiki/Transaction_processing), documenting [provenance](https://en.wikipedia.org/wiki/Provenance), [food traceability](https://en.wikipedia.org/wiki/Traceability#Food_processing) or voting.

Blockchain was invented by [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) in 2008 for use in the [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) [bitcoin](https://en.wikipedia.org/wiki/Bitcoin), as its public transaction [ledger](https://en.wikipedia.org/wiki/Ledger). The invention of the blockchain for bitcoin made it the first digital currency to solve the [double spending](https://en.wikipedia.org/wiki/Double-spending) problem without the need of a trusted authority or central [server](https://en.wikipedia.org/wiki/Server_%28computing%29). The bitcoin design has been the inspiration for other applications.

## Contents

* [1 History](https://en.wikipedia.org/wiki/Blockchain#History)
* [2 Structure](https://en.wikipedia.org/wiki/Blockchain#Structure)
  + [2.1 Blocks](https://en.wikipedia.org/wiki/Blockchain#Blocks)
  + [2.2 Decentralization](https://en.wikipedia.org/wiki/Blockchain#Decentralization)
  + [2.3 Openness](https://en.wikipedia.org/wiki/Blockchain#Openness)
* [3 Uses](https://en.wikipedia.org/wiki/Blockchain#Uses)
  + [3.1 General potentials](https://en.wikipedia.org/wiki/Blockchain#General_potentials)
  + [3.2 Land registration](https://en.wikipedia.org/wiki/Blockchain#Land_registration)
  + [3.3 The Big Four](https://en.wikipedia.org/wiki/Blockchain#The_Big_Four)
  + [3.4 Smart contracts](https://en.wikipedia.org/wiki/Blockchain#Smart_contracts)
  + [3.5 Nonprofit organizations](https://en.wikipedia.org/wiki/Blockchain#Nonprofit_organizations)
  + [3.6 Decentralized networks](https://en.wikipedia.org/wiki/Blockchain#Decentralized_networks)
  + [3.7 Governments and national currencies](https://en.wikipedia.org/wiki/Blockchain#Governments_and_national_currencies)
  + [3.8 Banks](https://en.wikipedia.org/wiki/Blockchain#Banks)
  + [3.9 Other financial companies](https://en.wikipedia.org/wiki/Blockchain#Other_financial_companies)
  + [3.10 Other uses](https://en.wikipedia.org/wiki/Blockchain#Other_uses)
* [4 Academic research](https://en.wikipedia.org/wiki/Blockchain#Academic_research)
  + [4.1 Journals](https://en.wikipedia.org/wiki/Blockchain#Journals)
* [5 Predictions](https://en.wikipedia.org/wiki/Blockchain#Predictions)
* [6 Working](https://en.wikipedia.org/wiki/Blockchain#Working)
  + [6.1 Ownership integrity](https://en.wikipedia.org/wiki/Blockchain#Ownership_integrity)
  + [6.2 Transaction integrity](https://en.wikipedia.org/wiki/Blockchain#Transaction_integrity)
  + [6.3 Order integrity](https://en.wikipedia.org/wiki/Blockchain#Order_integrity)
* [7 See also](https://en.wikipedia.org/wiki/Blockchain#See_also)
* [8 References](https://en.wikipedia.org/wiki/Blockchain#References)
* [9 Further reading](https://en.wikipedia.org/wiki/Blockchain#Further_reading)
* [10 External links](https://en.wikipedia.org/wiki/Blockchain#External_links)

## History

[](https://en.wikipedia.org/wiki/File:Confirmed_Transactions_Per_Day.png)

Bitcoin transactions (January 2009 – September 2017)

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. In 1992, Bayer, Haber and Stornetta incorporated [Merkle trees](https://en.wikipedia.org/wiki/Merkle_tree) to the design, which improved its efficiency by allowing several documents to be collected into one block.

The first blockchain was conceptualized by a person (or group of people) known as [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) in 2008. It was implemented the following year by Nakamoto as a core component of the [cryptocurrency bitcoin](https://en.wikipedia.org/wiki/Bitcoin), where it serves as the public [ledger](https://en.wikipedia.org/wiki/Ledger) for all transactions on the network. Through the use of a blockchain, bitcoin became the first digital currency to solve the [double spending](https://en.wikipedia.org/wiki/Double_spending) problem without requiring a trusted authority and has been the inspiration for many additional applications.

In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20GB ([gigabytes](https://en.wikipedia.org/wiki/Gigabyte)). In January 2015, the size had grown to almost 30GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50GB to 100GB in size. The words *block* and *chain* were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, *blockchain,* by 2016.

The term *blockchain 2.0* refers to new applications of the distributed blockchain database, first emerging in 2014. [*The Economist*](https://en.wikipedia.org/wiki/The_Economist) described one implementation of this second-generation programmable blockchain as coming with "a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level." Blockchain 2.0 technologies go beyond transactions and enable "exchange of value without powerful intermediaries acting as arbiters of money and information." They are expected to enable excluded people to enter the global economy, protect the privacy of participants, allow people to "monetize their own information," and provide the capability to ensure creators are compensated for their [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property). Second-generation blockchain technology makes it possible to store an individual's "persistent digital ID and persona" and provides an avenue to help solve the problem of [social inequality](https://en.wikipedia.org/wiki/Social_inequality) by "potentially changing the way wealth is distributed". As of 2016, blockchain 2.0 implementations continue to require an off-chain [oracle](https://en.wikipedia.org/wiki/Oracle_%28computer_science%29) to access any "external data or events based on time or market conditions [that need] to interact with the blockchain."

In 2016, the central securities depository of the Russian Federation ([NSD](https://en.wikipedia.org/wiki/National_Settlement_Depository_%28Russia%29)) announced a pilot project, based on the [Nxt](https://en.wikipedia.org/wiki/Nxt) blockchain 2.0 platform, that would explore the use of blockchain-based automated voting systems. IBM opened a blockchain innovation research center in Singapore in July 2016. A working group for the [World Economic Forum](https://en.wikipedia.org/wiki/World_Economic_Forum) met in November 2016 to discuss the development of [governance models](https://en.wikipedia.org/wiki/Multistakeholder_governance_model) related to blockchain. According to [Accenture](https://en.wikipedia.org/wiki/Accenture), an application of the [diffusion of innovations](https://en.wikipedia.org/wiki/Diffusion_of_innovations) theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the [early adopters](https://en.wikipedia.org/wiki/Early_adopter) phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the [Chamber of Digital Commerce](https://en.wikipedia.org/wiki/Chamber_of_Digital_Commerce).

## Structure

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network and a distributed timestamping server. They are [authenticated](https://en.wikipedia.org/wiki/Authentication) by [mass collaboration](https://en.wikipedia.org/wiki/Mass_collaboration) powered by [collective](https://en.wikipedia.org/wiki/Collective) [self-interests](https://en.wikipedia.org/wiki/Self-interest). The result is a [robust](https://en.wikipedia.org/wiki/Robustness_%28computer_science%29) [workflow](https://en.wikipedia.org/wiki/Workflow) where participants' [uncertainty](https://en.wikipedia.org/wiki/Uncertainty) regarding data security is marginal. The use of a blockchain removes the characteristic of infinite [reproducibility](https://en.wikipedia.org/wiki/Reproduction_%28economics%29) from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of [double spending](https://en.wikipedia.org/wiki/Double_spending). Blockchains have been described as a [value](https://en.wikipedia.org/wiki/Value_%28economics%29)-exchange [protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol). This blockchain-based exchange of value can be completed more quickly, more safely and more cheaply than with traditional systems. A blockchain can assign [title](https://en.wikipedia.org/wiki/Title_%28property%29) rights because it provides a record that compels [offer and acceptance](https://en.wikipedia.org/wiki/Offer_and_acceptance).

### Blocks

Blocks hold batches of valid [transactions](https://en.wikipedia.org/wiki/Transaction_processing) that are hashed and encoded into a [Merkle tree](https://en.wikipedia.org/wiki/Merkle_tree). Each block includes the [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash) of the prior block in the blockchain, linking the two. The linked blocks form a chain. This [iterative](https://en.wikipedia.org/wiki/Iteration) process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They only keep the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Because blockchains are typically built to add the score of new blocks onto old blocks and because there are incentives to work only on extending with new blocks rather than overwriting old blocks, the probability of an entry becoming superseded goes down exponentiallyas more blocks are built on top of it, eventually becoming very low. For example, in a blockchain using the [proof-of-work system](https://en.wikipedia.org/wiki/Proof-of-work_system), the chain with the most cumulative proof-of-work is always considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of [computation](https://en.wikipedia.org/wiki/Computation). Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and [parallel](https://en.wikipedia.org/wiki/Parallel_computing) manner.

#### Block time

The *block time* is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency), this is practically when the money transaction takes place, so a shorter block time means faster transactions. The block time for [Ethereum](https://en.wikipedia.org/wiki/Ethereum) is set to between 14 and 15 seconds, while for [bitcoin](https://en.wikipedia.org/wiki/Bitcoin) it is 10 minutes.

#### Hard forks

This section is [transcluded](https://en.wikipedia.org/wiki/Transclusion) from [Fork (blockchain)](https://en.wikipedia.org/wiki/Fork_%28blockchain%29). ([edit](https://en.wikipedia.org/w/index.php?title=Fork_%28blockchain%29&action=edit) | [history](https://en.wikipedia.org/w/index.php?title=Fork_%28blockchain%29&action=history))

A *hard fork* is a rule change such that the software enforcing the old rules will see the blocks adhering to the new rules as invalid. To prevent a blockchain split, all nodes running the old software shall upgrade to new rules. Alternatively, all nodes using the new software shall return to the old rules as was the case of bitcoin split on 12 March 2013.

[Ethereum](https://en.wikipedia.org/wiki/Ethereum) has hard-forked to "make whole" the investors in [The DAO](https://en.wikipedia.org/wiki/The_DAO_%28organization%29), which had been hacked by exploiting a vulnerability in its code. In this case, the fork resulted in a split creating [Ethereum](https://en.wikipedia.org/wiki/Ethereum) and [Ethereum Classic](https://en.wikipedia.org/wiki/Ethereum_Classic) chains. In 2014 the [Nxt](https://en.wikipedia.org/wiki/Nxt) community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment.

### Decentralization

By storing data across its network, the blockchain eliminates the risks that come with data being held centrally. The decentralized blockchain may use [ad-hoc](https://en.wikipedia.org/wiki/Ad-hoc) [message passing](https://en.wikipedia.org/wiki/Message_passing) and [distributed networking](https://en.wikipedia.org/wiki/Distributed_networking).

Its network lacks centralized points of vulnerability that [computer crackers](https://en.wikipedia.org/wiki/Security_hacker) can exploit; likewise, it has no central point of [failure](https://en.wikipedia.org/wiki/Failure). Blockchain security methods include the use of [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography).[[4]](https://en.wikipedia.org/wiki/Blockchain#cite_note-primer-4):5 A *public key* (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A *private key* is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

This is where blockchain has its advantage. While centralized data is more controllable, information and data manipulation are common. By decentralizing it, blockchain makes data transparent to everyone involved.

Every [node](https://en.wikipedia.org/wiki/Node_%28networking%29) in a decentralized system has a copy of the blockchain. [Data quality](https://en.wikipedia.org/wiki/Data_quality) is maintained by massive database [replication](https://en.wikipedia.org/wiki/Replication_%28computing%29) and [computational trust](https://en.wikipedia.org/wiki/Computational_trust). No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using software. Messages are delivered on a [best-effort](https://en.wikipedia.org/wiki/Best-effort_delivery) basis. Mining nodes validate transactions, add them to the block they are building, and then [broadcast](https://en.wikipedia.org/wiki/Broadcasting_%28networking%29) the completed block to other nodes. Blockchains use various time-stamping schemes, such as proof-of-work, to serialize changes. Alternate consensus methods include [proof-of-stake](https://en.wikipedia.org/wiki/Proof-of-stake). Growth of a decentralized blockchain is accompanied by the risk of node centralization because the computer resources required to process larger amounts of data become more expensive.

### Openness

Open blockchains are more [user-friendly](https://en.wikipedia.org/wiki/Usability) than some traditional ownership records, which, while open to the public, still require physical access to view. Because all early blockchains were permissionless, controversy has arisen over the blockchain definition. An issue in this ongoing debate is whether a private system with verifiers tasked and authorized (permissioned) by a central authority should be considered a blockchain. Proponents of permissioned or private chains argue that the term "blockchain" may be applied to any data structure that batches data into time-stamped blocks. These blockchains serve as a distributed version of [multiversion concurrency control](https://en.wikipedia.org/wiki/Multiversion_concurrency_control) (MVCC) in databases. Just as MVCC prevents two transactions from concurrently modifying a single object in a database, blockchains prevent two transactions from spending the same single output in a blockchain. Opponents say that permissioned systems resemble traditional corporate databases, not supporting decentralized data verification, and that such systems are not hardened against operator tampering and revision. Nikolai Hampton of [*Computerworld*](https://en.wikipedia.org/wiki/Computerworld) said that "many in-house blockchain solutions will be nothing more than cumbersome databases." Business analysts [Don Tapscott](https://en.wikipedia.org/wiki/Don_Tapscott) and [Alex Tapscott](https://en.wikipedia.org/wiki/Alex_Tapscott) define blockchain as a distributed ledger or database open to anyone.

#### Permissionless

The great advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no [access control](https://en.wikipedia.org/wiki/Access_control) is needed. This means that applications can be added to the network without the approval or trust of others, using the blockchain as a [transport layer](https://en.wikipedia.org/wiki/Transport_layer).

[Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) and other cryptocurrencies currently secure their blockchain by requiring new entries to include a proof of work. To prolong the blockchain, bitcoin uses [Hashcash](https://en.wikipedia.org/wiki/Hashcash) puzzles developed by [Adam Back](https://en.wikipedia.org/wiki/Adam_Back) in the 1990s.

Financial companies have not prioritised decentralized blockchains. In 2016, [venture capital](https://en.wikipedia.org/wiki/Venture_capital) investment for blockchain related projects was weakening in the USA but increasing in China. [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) and many other cryptocurrencies use open (public) blockchains. As of January 2018, bitcoin has the highest market capitalization.

#### Permissioned (private) blockchain

Main article: [Distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger)

Permissioned blockchains use an access control layer to govern who has access to the network. In contrast to public blockchain networks, validators on private blockchain networks are vetted by the network owner. They do not rely on anonymous nodes to validate transactions nor do they benefit from the [network effect](https://en.wikipedia.org/wiki/Network_effect). Permissioned blockchains can also go by the name of 'consortium' or 'hybrid' blockchains.

The [*New York Times*](https://en.wikipedia.org/wiki/New_York_Times) noted in both 2016 and 2017 that many corporations are using blockchain networks "with private blockchains, independent of the public systems.

#### Disadvantages

Nikolai Hampton pointed out in [*Computerworld*](https://en.wikipedia.org/wiki/Computerworld) that "There is also no need for a "51 percent" attack on a private blockchain, as the private blockchain (most likely) already controls 100 percent of all block creation resources. If you could attack or damage the blockchain creation tools on a private corporate server, you could effectively control 100 percent of their network and alter transactions however you wished." This has a set of particularly profound adverse implications during a [financial crisis](https://en.wikipedia.org/wiki/Financial_crisis) or [debt crisis](https://en.wikipedia.org/wiki/Debt_crisis) like the [financial crisis of 2007–08](https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%9308), where politically powerful actors may make decisions that favor some groups at the expense of others. and "the bitcoin blockchain is protected by the massive group mining effort. It's unlikely that any private blockchain will try to protect records using gigawatts of computing power — it's time consuming and expensive." He also said, "Within a private blockchain there is also no 'race'; there's no incentive to use more power or discover blocks faster than competitors. This means that many in-house blockchain solutions will be nothing more than cumbersome databases."

## Uses

Blockchain technology can be integrated into multiple areas. The primary use of blockchains today is as a distributed ledger for [cryptocurrencies](https://en.wikipedia.org/wiki/Cryptocurrency), most notably [bitcoin](https://en.wikipedia.org/wiki/Bitcoin). While a few [central banks](https://en.wikipedia.org/wiki/Central_banks), in countries such as [India](https://en.wikipedia.org/wiki/India), [China](https://en.wikipedia.org/wiki/China), [United States](https://en.wikipedia.org/wiki/United_States), [Sweden](https://en.wikipedia.org/wiki/Sweden), [Singapore](https://en.wikipedia.org/wiki/Singapore), [South Africa](https://en.wikipedia.org/wiki/South_Africa) and [United Kingdom](https://en.wikipedia.org/wiki/United_Kingdom) are studying issuance of a Central Bank Issued Cryptocurrency (CICC), none have done so thus far.

### General potentials

Blockchain technology has a large potential to transform business [operating models](https://en.wikipedia.org/wiki/Operating_model) in the long term. Blockchain distributed ledger technology is more a [foundational technology](https://en.wikipedia.org/wiki/Foundational_innovation)—with the potential to create new foundations for global economic and social systems—than a [disruptive technology](https://en.wikipedia.org/wiki/Disruptive_technology), which typically "attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly". Even so, there are a few operational products maturing from [proof of concept](https://en.wikipedia.org/wiki/Proof_of_concept) by late 2016. The use of blockchains promises to bring significant efficiencies to global [supply chains](https://en.wikipedia.org/wiki/Supply_chain), financial transactions, asset ledgers and decentralized social networking.

As of 2016, some observers remain skeptical. Steve Wilson, of Constellation Research, believes the technology has been [hyped](https://en.wikipedia.org/wiki/Media_circus) with unrealistic claims. To mitigate [risk](https://en.wikipedia.org/wiki/Risk_management) businesses are reluctant to place blockchain at the core of the business structure.

This means specific blockchain applications may be a disruptive innovation, because substantially lower-cost solutions can be instantiated, which can disrupt existing business models. Blockchain protocols facilitate businesses to use new methods of processing digital transactions. Examples include a payment system and [digital currency](https://en.wikipedia.org/wiki/Digital_currency), facilitating [crowdsales](https://en.wikipedia.org/wiki/Crowdfunding), or implementing [prediction markets](https://en.wikipedia.org/wiki/Prediction_market) and generic [governance](https://en.wikipedia.org/wiki/Governance) tools.

Blockchains alleviate the need for a [trust service provider](https://en.wikipedia.org/wiki/Trust_service_provider) and are predicted to result in less [capital](https://en.wikipedia.org/wiki/Capital_%28economics%29) being tied up in disputes. Blockchains have the potential to reduce [systemic risk](https://en.wikipedia.org/wiki/Systemic_risk) and financial [fraud](https://en.wikipedia.org/wiki/Fraud). They automate processes that were previously time-consuming and done manually, such as the [incorporation](https://en.wikipedia.org/wiki/Incorporation_%28business%29) of businesses. In theory, it would be possible to collect taxes, conduct conveyancing and provide risk management with blockchains.

As a distributed ledger, blockchain reduces the costs involved in verifying transactions, and by removing the need for trusted "third-parties" such as banks to complete transactions, the technology also lowers the cost of networking, therefore allowing several applications.

Starting with a strong focus on financial applications, blockchain technology is extending to activities including decentralized applications and collaborative organizations that eliminate a middleman.

### Land registration

"Land is a financial source, if people can prove they own it, they can borrow against it."

Emmanuel Noah, CEO of [*Ghanaian*](https://en.wikipedia.org/wiki/Ghana) startup BenBen, New York Observer

Frameworks and trials such as the one at the Sweden Land Registry aim to demonstrate the effectiveness of the blockchain at speeding land sale deals. The Republic of Georgia is piloting a blockchain-based property registry.

The Government of India is fighting land fraud with the help of a blockchain.

In October 2017, one of the first international property transactions was completed successfully using a blockchain-based [smart contract](https://en.wikipedia.org/wiki/Smart_contract).

In the first half of 2018, an experiment will be conducted on the use of blocking technology to monitor the reliability of the Unified State Real Estate Register (USRER) data in the territory of Moscow.

### The Big Four

Each of the [Big Four accounting firms](https://en.wikipedia.org/wiki/Big_Four_accounting_firms) is testing blockchain technologies in various formats. [Ernst & Young](https://en.wikipedia.org/wiki/Ernst_%26_Young) has provided [cryptocurrency wallets](https://en.wikipedia.org/wiki/Cryptocurrency_wallets) to all (Swiss) employees, has installed a bitcoin ATM in their office in Switzerland, and accepts bitcoin as payment for all its consulting services. Marcel Stalder, CEO of Ernst & Young Switzerland, stated, "We don't only want to talk about digitalization, but also actively drive this process together with our employees and our clients. It is important to us that everybody gets on board and prepares themselves for the revolution set to take place in the business world through blockchains, [to] smart contracts and digital currencies." [PwC](https://en.wikipedia.org/wiki/PwC), [Deloitte](https://en.wikipedia.org/wiki/Deloitte), and [KPMG](https://en.wikipedia.org/wiki/KPMG) have taken a different path from Ernst & Young and are all testing private blockchains.

### Smart contracts

Blockchain-based [smart contracts](https://en.wikipedia.org/wiki/Smart_contract) are contracts that can be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is [automated](https://en.wikipedia.org/wiki/Automation) [escrow](https://en.wikipedia.org/wiki/Escrow). The [IMF](https://en.wikipedia.org/wiki/International_Monetary_Fund) believes blockchains could reduce [moral hazards](https://en.wikipedia.org/wiki/Moral_hazard) and optimize the use of contracts in general. Due to the lack of widespread use their legal status is unclear.

Some blockchain implementations could enable the coding of contracts that will execute when specified conditions are met. A blockchain smart contract would be enabled by [extensible](https://en.wikipedia.org/wiki/Extensible_programming) programming instructions that define and execute an agreement. For example, [Ethereum Solidity](https://en.wikipedia.org/wiki/Solidity) is an open-source blockchain project that was built specifically to realize this possibility by implementing a [Turing-complete](https://en.wikipedia.org/wiki/Turing_complete) programming language capability to implement such contracts.

### Nonprofit organizations

* Level One Project from the [Bill & Melinda Gates Foundation](https://en.wikipedia.org/wiki/Bill_%26_Melinda_Gates_Foundation) aims to use blockchain technology to help the two billion people worldwide who lack bank accounts.
* Building Blocks project from the [U.N.](https://en.wikipedia.org/wiki/U.N.)'s [World Food Programme](https://en.wikipedia.org/wiki/World_Food_Programme) (WFP) aims to make WFP's growing cash-based transfer operations faster, cheaper, and more secure. Building Blocks commenced field pilots in Pakistan in January 2017 that will continue throughout spring.
* [Publiq](https://en.wikipedia.org/wiki/Publiq), a platform for authors founded in 2017, aims to use blockchain technology to guarantee authenticity of texts, avoid [censorship](https://en.wikipedia.org/wiki/Censorship), and combat [fake news](https://en.wikipedia.org/wiki/Fake_news).

### Decentralized networks

* The Backfeed project develops a distributed governance system for blockchain-based applications allowing for the collaborative creation and distribution of value in spontaneously emerging networks of peers.
* The Alexandria project is a blockchain-based Decentralized Library.
* Tezos is a blockchain project that governs itself by voting of its token holders.[Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) blockchain performs as a cryptocurrency and payment system. [Ethereum](https://en.wikipedia.org/wiki/Ethereum) blockchain added [smart contract](https://en.wikipedia.org/wiki/Smart_contract) system on top of a blockchain. Tezos blockchain will add an autonomy system – a decentralized code Development function on top of both bitcoin and Ethereum blockchains.

### Governments and national currencies

* The director of the Office of IT Schedule Contract Operations at the US General Services Administration, Mr. Jose Arrieta, disclosed at the 20 Sep ACT-IAC (American Council for Technology and Industry Advisory Council) Forum that its organization is using blockchain distributed ledger technology to speed up the FASt Lane process for IT Schedule 70 contracts through automation. Two companies, United Solutions (prime contractor) and Sapient Consulting (subcontractor) are developing for FASt Lane a prototype to automate and shorten the time required to perform the contract review process.
* The Commercial Customs Operations Advisory Committee, a subcommittee of the [U.S. Customs and Border Protection](https://en.wikipedia.org/wiki/U.S._Customs_and_Border_Protection), is working on finding practical ways Blockchain could be implemented in its duties.

Companies have supposedly been suggesting blockchain-based currency solutions in the following two countries:

* e-Dinar, [Tunisia](https://en.wikipedia.org/wiki/Tunisia)'s national currency, was the first state currency using blockchain technology.
* eCFA is [Senegal](https://en.wikipedia.org/wiki/Senegal)'s blockchain-based national digital currency.

Some countries, especially Australia, are providing keynote participation in identify the various technical issues associated with developing, governing and using blockchains:

In April 2016 Standards Australia submitted a New Field of Technical Activity (NFTA) proposal on behalf of Australia for the International Organization for Standardization (ISO) to consider developing standards to support blockchain technology. The proposal for an NFTA to the ISO was intended to establish a new ISO technical committee for blockchain. The new committee would be responsible for supporting innovation and competition by covering blockchain standards topics including interoperability, terminology, privacy, security and auditing. There have been several media releases supporting blockchain integration to Australian businesses.

### Banks

[Don Tapscott](https://en.wikipedia.org/wiki/Don_Tapscott) conducted a two-year research project exploring how blockchain technology can securely move and store host "money, titles, deeds, music, art, scientific discoveries, intellectual property, and even votes". Furthermore, major portions of the [financial industry](https://en.wikipedia.org/wiki/Financial_industry) are implementing [distributed ledgers](https://en.wikipedia.org/wiki/Distributed_ledger) for use in [banking](https://en.wikipedia.org/wiki/Banking), and according to a September 2016 [IBM](https://en.wikipedia.org/wiki/IBM) study, this is occurring faster than expected.

Banks are interested in this technology because it has potential to speed up [back office](https://en.wikipedia.org/wiki/Back_office) settlement systems.

[Banks](https://en.wikipedia.org/wiki/Bank) such as [UBS](https://en.wikipedia.org/wiki/UBS) are opening new research labs dedicated to blockchain technology in order to explore how blockchain can be used in financial services to increase efficiency and reduce costs.

Russia has officially completed its first government-level blockchain implementation. The state-run bank [Sberbank](https://en.wikipedia.org/wiki/Sberbank) announced 20 December 2017 that it is partnering with Russia's Federal Antimonopoly Service (FAS) to implement document transfer and storage via blockchain.

[Deloitte](https://en.wikipedia.org/wiki/Deloitte) and [ConsenSys](https://en.wikipedia.org/wiki/ConsenSys) announced plans in 2016 to create a digital bank called Project ConsenSys.

[R3](https://en.wikipedia.org/wiki/R3_%28company%29) connects 42 banks to distributed ledgers built by [Ethereum](https://en.wikipedia.org/wiki/Ethereum), Chain.com, [Intel](https://en.wikipedia.org/wiki/Intel), [IBM](https://en.wikipedia.org/wiki/IBM) and [Monax](https://en.wikipedia.org/wiki/Monax).

A Swiss industry consortium, including [Swisscom](https://en.wikipedia.org/wiki/Swisscom), the [Zurich Cantonal Bank](https://en.wikipedia.org/wiki/Zurich_Cantonal_Bank) and the Swiss stock exchange, is prototyping [over-the-counter](https://en.wikipedia.org/wiki/Over-the-counter_%28finance%29) asset trading on a blockchain-based Ethereum technology.

### Other financial companies

The credit and debits payments company [MasterCard](https://en.wikipedia.org/wiki/MasterCard) has added three blockchain-based [APIs](https://en.wikipedia.org/wiki/API) for programmers to use in developing both person-to-person (P2P) and [business-to-business](https://en.wikipedia.org/wiki/Business-to-business) (B2B) payment systems.

[CLS Group](https://en.wikipedia.org/wiki/CLS_Group) is using blockchain technology to expand the number of currency trade deals it can settle.

VISA payment systems, Mastercard, Unionpay and SWIFT have announced the development and plans for using blockchain technology.

Prime Shipping Foundation is using blockchain technology to address issues related to the payments in the shipping industry, seeking 150 million USD to develop their proprietary PRIME Token.

### Other uses

Blockchain technology can be used to create a permanent, public, transparent ledger system for compiling data on sales, storing rights data by authenticating [copyright registration](https://en.wikipedia.org/wiki/Copyright_registration), and tracking digital use and payments to content creators, such as wireless users or musicians. In 2017, IBM partnered with [ASCAP](https://en.wikipedia.org/wiki/ASCAP) and [PRS for Music](https://en.wikipedia.org/wiki/PRS_for_Music) to adopt blockchain technology in music distribution. [Imogen Heap](https://en.wikipedia.org/wiki/Imogen_Heap)'s Mycelia service, which allows managers to use a blockchain for tracking high-value parts moving through a [supply chain](https://en.wikipedia.org/wiki/Supply_chain), was launched as a concept in July 2016. Everledger is one of the inaugural clients of IBM's blockchain-based tracking service.

Kodak announced plans in 2018 to launch a digital token system for photograph copyright recording.

Another example where smart contracts are used is in the music industry. Every time a dj mix is played, the [smart contracts](https://en.wikipedia.org/wiki/Smart_contract) attached to the dj mix pays the artists almost instantly.

An application has been suggested for securing the spectrum sharing for wireless networks.

New distribution methods are available for the [insurance](https://en.wikipedia.org/wiki/Insurance) industry such as [peer-to-peer insurance](https://en.wikipedia.org/wiki/Peer-to-peer_insurance), [parametric insurance](https://en.wikipedia.org/wiki/Parametric_insurance) and [microinsurance](https://en.wikipedia.org/wiki/Microinsurance) following the adoption of blockchain. The [sharing economy](https://en.wikipedia.org/wiki/Sharing_economy) and [IoT](https://en.wikipedia.org/wiki/Internet_of_Things) are also set to benefit from blockchains because they involve many collaborating peers. [Online voting](https://en.wikipedia.org/wiki/Online_voting) is another application of the blockchain. Blockchains are being used to develop information systems for [medical records](https://en.wikipedia.org/wiki/Medical_record), which increases [interoperability](https://en.wikipedia.org/wiki/Interoperability). In theory, legacy [disparate systems](https://en.wikipedia.org/wiki/Disparate_system) can be completely replaced by blockchains. Blockchains are being developed for [data storage](https://en.wikipedia.org/wiki/Computer_data_storage), publishing texts and identifying the origin of [digital art](https://en.wikipedia.org/wiki/Digital_art). Blockchains facilitate users could take ownership of game assets ([digital assets](https://en.wikipedia.org/wiki/Digital_asset)),an example of this is [Cryptokitties](https://en.wikipedia.org/wiki/Cryptokitties).

Notable non-cryptocurrency designs include:

* [Steemit](https://en.wikipedia.org/wiki/Steemit) – a blogging/social networking website and a cryptocurrency
* [Hyperledger](https://en.wikipedia.org/wiki/Hyperledger) – a cross-industry collaborative effort from the [Linux Foundation](https://en.wikipedia.org/wiki/Linux_Foundation) to support blockchain-based distributed ledgers, with projects under this initiative including Hyperledger Burrow (by Monax) and Hyperledger Fabric (spearheaded by IBM)[[131]](https://en.wikipedia.org/wiki/Blockchain#cite_note-131)
* [Counterparty](https://en.wikipedia.org/wiki/Counterparty_%28technology%29) – an open source financial platform for creating peer-to-peer financial applications on the bitcoin blockchain
* Quorum – a permissionable private blockchain by [JPMorgan Chase](https://en.wikipedia.org/wiki/JPMorgan_Chase) with private storage, used for contract applications
* [Bitnation](https://en.wikipedia.org/wiki/Bitnation) – a decentralized borderless "voluntary nation" establishing a jurisdiction of contracts and rules, based on Ethereum
* [Factom](https://en.wikipedia.org/wiki/Factom), a distributed registry
* Tezos, decentralized voting.

[Microsoft Visual Studio](https://en.wikipedia.org/wiki/Microsoft_Visual_Studio) is making the Ethereum Solidity language available to application developers.

IBM offers a cloud blockchain service based on the open source [Hyperledger Fabric](https://en.wikipedia.org/wiki/Hyperledger_Fabric) project

Oracle Cloud offers Blockchain Cloud Service based on [Hyperledger Fabric](https://en.wikipedia.org/wiki/Hyperledger_Fabric). Oracle has joined the Hyperledger consortium.

In August 2016, a research team at the [Technical University of Munich](https://en.wikipedia.org/wiki/Technical_University_of_Munich) published a research document about how blockchains may disrupt industries. They analyzed the [venture funding](https://en.wikipedia.org/wiki/Venture_funding) that went into blockchain ventures. Their research shows that $1.55 billion went into [startups](https://en.wikipedia.org/wiki/Startup_company) with an industry focus on finance and insurance, information and communication, and professional services. High startup density was found in the USA, UK and Canada.

[ABN Amro](https://en.wikipedia.org/wiki/ABN_Amro) announced a project in real estate to facilitate the sharing and recording of real estate transactions, and a second project in partnership with the [Port of Rotterdam](https://en.wikipedia.org/wiki/Port_of_Rotterdam) to develop logistics tools.

## Academic research

[](https://en.wikipedia.org/wiki/File:BlockchainPanelDiscussionAtIEEETechIgnite2017.jpg)

Blockchain panel discussion at the first [IEEE Computer Society](https://en.wikipedia.org/wiki/IEEE_Computer_Society) TechIgnite conference

In October 2014, the MIT Bitcoin Club, with funding from MIT alumni, provided undergraduate students at the [Massachusetts Institute of Technology](https://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology) access to $100 of bitcoin. The adoption rates, as studied by Catalini and Tucker (2016), revealed that when people who typically adopt technologies early are given delayed access, they tend to reject the technology.

### Journals

In September 2015, the first peer-reviewed academic journal dedicated to [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) and blockchain technology research, *Ledger*, was announced. The inaugural issue was published in December 2016. The journal covers aspects of [mathematics](https://en.wikipedia.org/wiki/Mathematics), [computer science](https://en.wikipedia.org/wiki/Computer_science), [engineering](https://en.wikipedia.org/wiki/Engineering), [law](https://en.wikipedia.org/wiki/Law), [economics](https://en.wikipedia.org/wiki/Economics) and [philosophy](https://en.wikipedia.org/wiki/Philosophy) that relate to cryptocurrencies such as [bitcoin](https://en.wikipedia.org/wiki/Bitcoin).[[143]](https://en.wikipedia.org/wiki/Blockchain#cite_note-143)[[144]](https://en.wikipedia.org/wiki/Blockchain#cite_note-Hertig2015-144) There are also research platforms like Strategic coin that offer research for the blockchain and crypto space.

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. Authors are also asked to include a personal bitcoin address in the first page of their papers.

## Predictions

A [World Economic Forum](https://en.wikipedia.org/wiki/World_Economic_Forum) report from September 2015 predicted that by 2025 ten percent of global GDP would be stored on blockchains technology.

In early 2017, [Harvard Business School](https://en.wikipedia.org/wiki/Harvard_Business_School) professors [Marco Iansiti](https://en.wikipedia.org/wiki/Marco_Iansiti) and [Karim R. Lakhani](https://en.wikipedia.org/wiki/Karim_R._Lakhani) said the blockchain is not a [disruptive technology](https://en.wikipedia.org/wiki/Disruptive_technology) that undercuts the cost of an existing business model, but is a [foundational technology](https://en.wikipedia.org/wiki/Foundational_innovation) that "has the potential to create new foundations for our economic and social systems". They further predicted that, while foundational innovations can have enormous impact, "It will take decades for blockchain to seep into our economic and social infrastructure."

## Working

|  |  |
| --- | --- |
|  |  |

In order for a community maintained ledger to work one needs a way to ensure three types of integrity. Hereunder each of those is treated separately.

### Ownership integrity

To make sure only the owner of an account is able draw from it, one needs a way to verify ownership using only the ledger itself. To this end a transaction in the ledger consists of three things. A public key of the account from which money is drawn, a public key of the account to which money is sent and an encoded message approving the transaction. This encoded message is encoded by the private key of the account owner and can be decoded by anyone using the public key that was registered as the sender in the ledger. This verification procedure is called a [digital signature](https://en.wikipedia.org/wiki/Digital_signature) and is comparable to the authentication step of the [https](https://en.wikipedia.org/wiki/Https) protocol. Note that the public key plays a dual role, it is both the account number itself as well as a way to verify the digital signature.

Due to the fact that encoding can only be done by the owner with his/her private key and decoding can be done by anyone using the public key everyone can check for him or herself that the one who drew upon an account with a certain public key has the corresponding private key.

### Transaction integrity

One must only be able to draw from an account if there is a positive balance in it. To this end each payment from an account must reference an unspent payment to that account in the past. As we are considering a 'zero trust' system it is instrumental that everyone has his or her own copy of the entire ledger in order to verify whether this reference payment indeed exists.

This way of safeguarding the integrity of transactions is called the [transaction chain](https://en.wikipedia.org/w/index.php?title=Transaction_chain&action=edit&redlink=1).

### Order integrity

Even with the transaction chain and [digital signature](https://en.wikipedia.org/wiki/Digital_signature) in place there is still no way of telling what the ordering of all transaction is. This makes the system vulnerable to the following attack:

*Eve can send money to Bob making use of a past transaction she got from Alice. She can send this to Bob's ledger who will in response send her the product or service they had agreed upon. Once she has received the product or service she can spend that same past transaction from Alice again, this time sending it to her own account. If she now starts broadcasting this new payment to the rest of the network, claiming she had made this transaction first, then there is no way for the rest of the network to tell which transaction occurred first. In case the network accepts the payment of Eve to herself the payment of Eve to Bob becomes invalid as it references an already spent transaction.*

In order to prevent this kind of attack there must be some way of safeguarding the ordering of transactions. This is where the blockchain comes in. In the blockchain transactions are grouped into blocks that are thought of as having happened at the same time. The chain of blocks then provides you with a chronology of the transactions.

In order to add a new block to the chain one needs to solve the following problem.

*Let f be a function computing a number based on two inputs in a highly disorderly fashion. Further consider a* [*hash*](https://en.wikipedia.org/wiki/Hash_function) *function h that can hash the content of a block b. Now find a number n such that*

f ( n , h ( b ) ) < t h r e s h o l d {\displaystyle f(n,h(b))<threshold}where the threshold is chosen in such a way that the network takes typically about 10 minutes to find a correct number.

When a party within the network has found a solution it broadcasts the block that it wants to add to the chain together with the found solution of the previous block. The rest of the network verifies this solution and adds the block. Multiple branches in the chain can occur due to the fact that parts of the network may have been isolated for a while. Each party in this case the parties in the network will choose the longest chain available and work further on that branch only.

The fraudulent tactic applied by Eve above is now prevented due to three things:

* The content of a block consists of the new transactions as well as the hash of the previous block and the previous solution. This means that altering one block implicates altering the hash of all blocks coming after it.
* Only the longest chain is adopted by the rest of the network.
* Calculating the solution of a block is very time and resource consuming.

Suppose Eve wants to alter a block that lies, say 6 blocks deep in the chain. Due to bullet point one she will need to recalculate all 5 blocks coming after. After that, due to bullet point two, she will need to catch up with the rest of the network producing more blocks than the entire community combined had produced thus far. Due to bullet point three this is not feasible.

The blockchain is secured by the amount of work it takes to add a block. There are many participants competing to add the next block making a single party extremely unlikely to be able to outrun all other parties for a longer period time. This means that blocks that lie deeper in the chain are very safe. Only blocks at the very rear can be tempered with.

For a blockchain to be effective it needs to have many participants, preventing one party from getting too much relative computing power and with that influence over the chain itself. To this end there needs to be an incentive for people to calculate solutions and add new blocks. In bitcoin this is currently taken care of by awarding the party that added a block with some bitcoin.

*When one joins the block chain, the very first step is to download and verify the integrity of the entire ledger.*

* *Do all public keys correspond with the encoded message?*
* *Do all transactions reference past transactions?*
* *Does each block provide a solution to the previous block?*

*Once this is done one only needs to verify each new block making sure the three rules above are observed.*

* [Changelog](https://en.wikipedia.org/wiki/Changelog) – a record of all notable changes made to a project
* [Checklist](https://en.wikipedia.org/wiki/Checklist) – an informational aid used to reduce failure
* [Economics of digitization](https://en.wikipedia.org/wiki/Economics_of_digitization)
* [List of cryptocurrencies](https://en.wikipedia.org/wiki/List_of_cryptocurrencies)
* [List of emerging technologies](https://en.wikipedia.org/wiki/List_of_emerging_technologies)
* [Blockchain game](https://en.wikipedia.org/wiki/Blockchain_game)
* [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin)
* [Cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency)
* [Types of blockchain](https://en.wikipedia.org/wiki/Types_of_blockchain)