

Blockchain

A **blockchain**^{[1][2][3]} — originally **block chain**^{[4][5]} — is a **distributed database** that maintains a continuously-growing list of ordered **records** called *blocks*. Each block contains a **timestamp** and a link to a previous block.^{[6]:6} By design blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively.

Blockchains are **secure by design** and an example of a distributed computing system with high **byzantine fault tolerance**. **Decentralised consensus** can therefore be achieved with a blockchain.^[7] This makes blockchains suitable for the recording of events, title, medical records and other records management activities, identity management, transaction processing and proving provenance. This offers the potential of mass **disintermediation** and vast repercussions for how **global trade** is conducted.

The first blockchain was conceptualised by **Satoshi Nakamoto** in 2008 and implemented the following year as a core component of the digital currency **bitcoin**, where it serves as the public **ledger** for all transactions.^[1] Through the use of a **peer-to-peer** network and a distributed timestamping server, a blockchain database is managed autonomously. The invention of the blockchain for bitcoin made it the first digital currency to solve the **double spending** problem, without the use of a trusted authority or central **server**. The bitcoin design has been the inspiration for other applications.^{[1][3]}

1 History

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta, followed by publications in 1996 by **Ross J. Anderson** and 1998 by **Bruce Schneier** and **John Kelsey**.^[8] In parallel, **Nick Szabo** was working in 1998 on a mechanism for a decentralized digital currency that he called *bit gold*.^[9] In 2000 Stefan Konst published a general theory for cryptographic secured chains and suggested a set of solutions for implementation.^[8]

The first blockchain was then conceptualised by **Satoshi Nakamoto** in 2008 and implemented the following year as a core component of the digital currency **bitcoin**, where it serves as the public **ledger** for all transactions.^[1] Through the use of a **peer-to-peer** network and a distributed timestamping server, a blockchain database is managed autonomously. The invention of the blockchain for bitcoin made it the first digital currency to solve the **double spending** problem. The bitcoin design has been the inspiration for other applications.^{[1][3]}

The blockchain format was first used for **bitcoin**, as a solution to the problem of making a database both secure and not requiring a trusted administrator.^[4] The words *block* and *chain* were used separately in Satoshi Nakamoto's original paper in October 2008,^[10] and when the term moved into wider use it was originally *block chain*,^{[4][5]} before becoming a single word, *blockchain*, by 2016. In August 2014, the bitcoin blockchain file size reached 20 **gigabytes** in size.^[11]

By 2014, “Blockchain 2.0” was a term referring to new applications of the distributed blockchain database.^[12] *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.”^[1] Blockchain 2.0 technologies go beyond transactions and “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, enable the protection of privacy and people to “monetize their own information”, and provide the capability to ensure creators are compensated for their **intellectual property**. Second-generation blockchain technology makes it possible to store an individual's “persistent digital ID and persona” and are providing an avenue to help solve the problem of **social inequality** by “[potentially changing] the way wealth is distributed.”^{[13]:14–15} As of 2016, Blockchain 2.0 implementations continue to require an off-chain **oracle** to access any “external data or events based on time or market conditions [that need] to interact with the blockchain.”^[14]

In 2016, the central securities depository of the Russian Federation (NSD) announced a pilot project based on blockchain technology.^[15] Various regulatory bodies in the music industry have started testing models that use blockchain technology for royalty collection and management of copyrights around the world.^[16] IBM opened a blockchain innovation research centre in Singapore in July 2016.^[17] A working group for the World Economic Forum met in November 2016 to discuss the development of governance models related to blockchain.^[18] According to Accenture, an application of the diffusion of innovations theory suggests that in 2016 blockchains attained a 13.5% adoption rate within financial services, therefore reaching the early adopters phase.^[19] In 2016, industry trade groups joined to create the Global Blockchain Forum, an initiative of the Chamber of Digital Commerce.^[20]

2 Description

A blockchain facilitates secure online transactions.^[21] A blockchain is a decentralized digital ledger that records transactions on thousands of computers globally in such a way that the registered transactions cannot be altered retrospectively.^{[22][1]} They are authenticated by mass collaboration powered by collective self-interests.^[23] The result is a robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of digital cash was spent only once, solving the long-standing problem of double spending. Blockchains have been described as a value-exchange protocol.^[12] This exchange of value can be completed more quickly, more safely and more cheaply with a blockchain.^[24] A blockchain can assign title rights because it provides a record that compels offer and acceptance.^[1] From the technical point of view a blockchain is a hashchain inside another hashchain.^[25]

A blockchain database consists of two kinds of records: transactions and blocks.^[1] Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree.^[1] Each block includes the hash of the prior block in the blockchain, linking the two. Variants of this format were used previously, for example in Git, and it is not by itself sufficient to qualify as a blockchain.^[26] The linked blocks form a chain.^[1] This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.^[27] Some blockchains create a new block as frequently as every five seconds.^[28] As blockchains age they are said to grow in height. Blocks are structured by division into layers.

Sometimes separate blocks can be validated 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 which are not selected for inclusion in the chain are called orphan blocks.^[27] Peers supporting the database don't have exactly the same version of the history at all times, rather they keep the highest scoring version of the database that they currently know of. 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, but because blockchains are typically built to add the score of new blocks onto old blocks and there are incentives to only work on extending with new blocks rather than overwriting old blocks, the probability of an entry becoming superseded goes down exponentially^[29] as more blocks are built on top of it, eventually becoming very low.^{[1][30]:ch. 08[31]} For example, in a blockchain using the proof-of-work system, the chain with the most cumulative proof-of-work is always considered the valid one by the network. In practice there are a number of methods that can demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.^[32]

The blockchain is parsed by software to extract relevant information.^[33] The Nxt cryptocurrency community considered and dismissed a blockchain rollback in 2014 after a theft at a major exchange.^[34]

2.1 Decentralization

By storing data across its network, the blockchain eliminates the risks that come with data being held centrally.^[1] Decentralised blockchains may use ad-hoc message passing and distributed networking. Its network lacks centralized points of vulnerability that computer hackers can exploit or any central point of failure. Blockchain security methods include the use of public-key cryptography.^{[4]:5} A public key (a long, randomly-generated string of numbers) is an address on the blockchain. Bitcoins 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 otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.^[1]

Every node or miner in a decentralized system has a copy of the blockchain. Data quality is maintained by massive

database replication^[7] and computational trust. No centralized “official” copy exists and no user is “trusted” more than any other.^[4] Transactions are broadcast to the network using software. Messages are delivered on a best effort basis. Mining nodes validate transactions,^[27] add them to the block they’re creating, and then broadcast the completed block to other nodes.^{[30]:ch. 08} Blockchains use various time-stamping schemes, such as proof-of-work to serialize changes.^[35] Alternate consensus methods include proof-of-stake and proof of burn.^[27] Growth of a decentralized blockchain is accompanied by the risk of node centralization because computer resources required to operate bigger data become more expensive.^[36]

2.1.1 Forks

If two groups of users disagree about a proposed change to the blockchain protocol or algorithms, the two groups are free to each run their own versions of the blockchain software, which creates two descendant blockchains with their own separate histories from that point forward.

There are two types of forks - soft forks, which are forward-compatible, and hard forks, which are not.

For example, Ethereum has hard-forked multiple times. One of the first Ethereum hard forks was an ad-hoc fork to “make whole” the investors in The DAO, which had been hacked by exploiting a vulnerability in its code.

2.2 Openness

Open blockchains are more user friendly 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.^{[37][38][39][40][41]} 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 (MVCC) in databases.^[42] 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.^{[13]:30–31} 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.^{[37][39]} The *Harvard Business Review* defines blockchain as a distributed ledger or database open to anyone,^[43] and *Computerworld* claims that “much of [permissioned blockchain hype] is nothing more than snake oil and spin”.^[44]

2.2.1 Permissionless

The great advantage to an open, permissionless network is that guarding against bad actors is not required and no access control is needed.^[29] This means that applications can be added to the edge of the network without the approval or trust of others, using the blockchain as a transport layer.^[29] This openness allows researchers to examine real-time transaction data in a closed economic system.

Bitcoin and Ethereum currently secure their blockchain by requiring new entries including a proof of work. To prolong the blockchain, bitcoin uses Hashcash puzzles developed by Adam Back in the 1990s.^[45] Ethereum plans to switch to a proof-of-stake system in the future.^[46]

Financial companies have not prioritised decentralized blockchains.^[47] In 2016, venture capital investment for blockchain related projects was weakening in the USA but increasing in China.^[48] Bitcoin and Ethereum use open (public) blockchains. As of September 2016, bitcoin has the highest market capitalization while Ethereum is second.^[49]

2.2.2 Permissioned

Main article: Distributed ledger

Permissioned blockchains are emerging as open source protocols where openness and collaboration are encouraged.^[50] These will always have the ability to restrict who can participate in the consensus processes as well as who can transact.^[32] These private blockchains lack transparency. They do not rely on anonymous miners to validate transactions nor do they benefit from the network effect.^[51] Miners are vetted. The *New York Times* notes that many corporations are using blockchain networks “with private blockchains, independent of the public system.”^[3]

2.2.3 Disadvantages

Nikolai Hampton pointed out in *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.”^[44] This has a set of particularly profound adverse implications during a financial crisis or debt crisis like the financial crisis of 2007–08, 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.”^[44] 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.”^[44]

2.3 Applications

While there is potential to transform business operating models there are few operational products maturing from proof of concept.^[48] The use of blockchains promises to be able to bring significant efficiencies to global supply chains although many observers remain skeptical. Some analysts, such as Steve Wilson from Constellation Research, believe the technology has been hyped with unrealistic claims.^[52] In order to mitigate risk businesses are reluctant to place blockchain at the core of the business structure.^[53] Blockchains are a technology that may be integrated into multiple areas. It is a disruptive innovation because it allows businesses to use new methods of processing digital transactions.^[54] Examples include a payment system and digital currency, facilitating crowdsales, or implementing prediction markets and generic governance tools. Blockchains are expected to disrupt the cloud computing industry although practical technical issues remain as obstacles.^[55]

Blockchains can be thought of as an automatically notarised ledger. They alleviate the need for a trust service provider and are predicted to result in less capital being tied up in disputes. Blockchains have the potential to reduce systemic risk and financial fraud. They automate processes which were previously time-consuming and done manually such as the incorporation of businesses.^[56] In theory, it would be possible to collect taxes, conduct conveyancing and provide risk management with blockchains.

Major applications of blockchain include cryptocurrencies—including bitcoin, BlackCoin, Dash, and NXT—and blockchain platforms—Factom as a distributed registry, Gems for decentralized messaging, MaidSafe for decentralized applications, Storj for a distributed cloud, and Tezos for decentralized voting.^{[13]:94} 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.^[57] The Republic of Georgia is piloting a blockchain-based property registry.^[58] The Ethical and Fair Creators Association uses blockchain to help startups protect their authentic ideas.^[59]

New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and microinsurance following the adoption of blockchain.^[54] Banks are interested in this technology because it has potential to speed up back office settlement systems.^[60] The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers.^[61] Online voting is another application of the blockchain.^[62] Blockchains are being used to develop information systems for medical records which increases interoperability. In theory, legacy disparate systems can be completely replaced by blockchains.^[63] Blockchains are being developed for data storage, publishing texts and identifying the origin of digital art.

2.3.1 The Big Four

Each of the Big Four accounting firms are testing blockchain technologies in various formats. Ernst and Young has provided digital wallets to all employees, has installed a bitcoin ATM in their office in Switzerland, and accepts bitcoin as payment for all its consulting services.^[64] Mark Stalder, CEO of Ernst and 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.”^[64] PWC, Deloitte, and KPMG have taken a different path from Ernst & Young and are all testing private blockchains.^[64]

2.3.2 Smart contracts

Blockchain-based **smart contracts** are contracts that can be partially or fully executed or enforced without human interaction.^[65] One of the main objectives of a smart contract is **automated escrow**. The IMF believes blockchains could reduce **moral hazards** and optimize the use of contracts in general.^[66] Due to the lack of widespread use their legal status is unclear.^[66]

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** programming instructions which both define and execute an agreement.^[67] For example, **Ethereum** is an open source blockchain project that was built specifically to realize this possibility by implementing a **Turing-complete** programming language capability to implement such contracts.^{[13]:ch. 11} As of January 2016, smart contract systems are not being used for ether.^[68]

3 Applications

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.^[69] The primary use of blockchains today is for the creation of **cryptocurrencies**, such as bitcoin.^[70] While a few **central banks**, in countries such as **China, United States, Sweden, Singapore, South Africa, & England** are studying issuance of a Central Bank Issued Cryptocurrency (CICC), none have done so thus far.^[70]

In October 2014, the MIT Bitcoin Club, with funding from MIT alumni, provided undergraduate students at the **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.^[71]

The *Harvard Business Review* 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”.^[43] Furthermore, major portions of the **financial industry** are implementing **distributed ledgers** for use in **banking**^{[72][73]}, and according to a September 2016 IBM study, this is occurring faster than expected.^[74] The credit and debits payments company **MasterCard** has added three blockchain-based **APIs** for programmers to use in developing both **P2P** and **B2B** payment systems.^[75]

CLS Group is using blockchain technology to expand the number of currency trade deals it can settle.^[53]

A recent **World Economic Forum** report predicts that by 2025 10% of GDP will be stored on blockchains or blockchain related technology.^[76]

3.1 Alternative blockchains

Alternative blockchains, also known as altchains, are based on bitcoin technology in concept and/or code.^[6] The term encompasses all blockchains but bitcoin’s main chain. Compared to bitcoin, these designs generally add functionality to the blockchain design. Altchains can provide solutions including other digital currencies, although tokens used in these designs are not always considered to be such. Altchains target performance, anonymity, storage and applications such as **smart contracts**.^[77] Starting with a strong focus on financial applications, blockchain technology is extending to activities including decentralized applications and collaborative organizations that eliminate a middleman.^[78]

Notable non-cryptocurrency designs include:

- LaZooz – decentralized **real-time ride sharing**^[79]
- Swarm and Koinify – decentralized **crowdfunding**^[80]
- Synereo – synchronous and asynchronous **communication**^[81]
- Steemit combines a blogging site/social networking website and a cryptocurrency
- **DECENT Network content distribution platform**
- **Hyperledger** — cross-industry collaborative effort to support blockchain-based distributed ledgers

- **Counterparty** — open source financial platform for creating peer-to-peer financial applications on the bitcoin blockchain
- **Bitcache**
- **Bitnation** is the world's first operational Decentralized Borderless Voluntary Nation, a Blockchain Powered Jurisdiction.

For a list of cryptocurrencies, see *List of cryptocurrencies*.

3.2 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**,^[82] and tracking digital use and payments to content creators, such as musicians.^[83] **Imogen Heap's Mycelia**^[84] service, which allows managers to use a blockchain for tracking high-value parts moving through a **supply chain**, was launched as a concept in July 2016. Everledger, “building systems to record the movement of diamonds from mines to jewelry stores”, is one of the inaugural clients of IBM's blockchain-based tracking service.^[85]

3.2.1 Commercial offerings

Distributed ledgers and other blockchain-inspired software are being developed by commercial organizations for various applications:

- **Deloitte** and **ConsenSys** announced plans in 2016 to create a digital bank called Project ConsenSys.^[86]
- **R3 (company)** connects 42 banks to distributed ledgers built by **Ethereum**, **Chain.com**, **Intel**, **IBM** and **Monax.io**.^[87]
- **Microsoft Visual Studio** is making the **Ethereum Solidity** language available to application developers.^[88]
- **SafeShare Insurance** offers blockchain-based insurance for the **sharing economy**, underwritten by **Lloyd's of London**.^[89]
- A Swiss industry consortium, including **Swisscom**, the **Zurich Cantonal Bank** and the Swiss stock exchange, is prototyping over-the-counter asset trading on a blockchain based on **Ethereum** technology.^[90]
- **Context Labs**, a company developing blockchain enabled platforms
- **Digital Asset Holdings**, led by CEO **Blythe Masters**
- **Satoshi Citadel Industries**

In August 2016 a research team at the **Technical University of Munich** published a research document about how blockchains may disrupt industries. They analyzed the **venture funding** that went into blockchain ventures. Their research shows that \$1.55 billion went into **startups** 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.^[91]

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** to develop logistics tools.^[92]

4 Academic research

4.1 Journals

Main article: **Ledger (journal)**

In September 2015, the first peer-reviewed academic journal dedicated to **cryptocurrency** and blockchain technology research, *Ledger*, was announced. The inaugural issue was published in December 2016.^{[93][94]} The journal covers aspects of **mathematics**, **computer science**, **engineering**, **law**, **economics** and **philosophy** that relates to cryptocurrencies such as **bitcoin**.^{[95][96]}

The journal encourages authors to **digitally sign** a **file hash** of submitted papers, which will then be **timestamped** into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address in the first page of their papers.^[97]

5 See also

- **Changelog** a record of all notable changes made to a project
- **Checklist** an informational aid used to reduce failure
- **Economics of digitization**
- **History of money**
- **List of cryptocurrencies** currency based blockchains
- **List of emerging technologies**

6 References

- [1] Economist Staff (2015-10-31). "Blockchains: The great chain of being sure about things". *The Economist*. Retrieved 18 June 2016. [Subtitle] The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.
- [2] Morris, David Z. (2016-05-15). "Leaderless, Blockchain-Based Venture Capital Fund Raises \$100 Million, And Counting". *Fortune (magazine)*. Retrieved 2016-05-23.
- [3] Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". *New York Times*. Retrieved 2016-05-23.
- [4] Brito, Jerry & Castillo, Andrea (2013). "Bitcoin: A Primer for Policymakers" (PDF). Fairfax, VA: Mercatus Center, George Mason University. Retrieved 22 October 2013.
- [5] Trottier, Leo (2016-06-18). "original-bitcoin" (self-published code collection). github. Retrieved 2016-06-18. This is a historical repository of Satoshi Nakamoto's original bit coin sourcecode
- [6] "Blockchain". *Investopedia*. Retrieved 19 March 2016. Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system.
- [7] Raval, Siraj (2016). *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc. pp. 1, 2. ISBN 1491924527. Retrieved 6 November 2016.
- [8] Konst, Stefan (2000-08-09). "Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge" (PDF). *konst.de* (in German). Retrieved 2016-11-29.
- [9] POPPER, NATHANIEL (2015-05-15). "Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin". *ny-times.com*. New York Times. Retrieved 2016-11-29.
- [10] "Mail To News And Back Again". Gmane. 2008-10-31. Retrieved 2016-12-09.
- [11] Chuen, David Lee Kuo (2015). *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press. p. 319. ISBN 9780128023518. Retrieved 6 November 2016.
- [12] Kariappa Bheemaiah (January 2015). "Block Chain 2.0: The Renaissance of Money". *Wired*. Retrieved 13 November 2016.
- [13] Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. ISBN 978-0670069972.
- [14] Project Bletchley Whitepaper, Microsoft, 2016-09-19, accessed 2016-12-24.

- [15] Yakovlev, Alexander [interviewee] & Kovlyagina, Tatiana [interviewer] (2016-04-15). "НРД проголосовал за блокчейн" [NSD blockchain vote]. *Bankir.ru* (in Russian). Retrieved 18 June 2016. "Национальный расчетный депозитарий запустил пилотный проект на основе технологии распределенного реестра. Создание прототипа системы электронного голосования владельцев облигаций на блокчейне анонсировал на Биржевом форуме председатель правления НРД Эдди Астанин [The National Settlement Depository started the pilot project based on the technology of the distributed register. Creation of the prototype system of electronic voting for owners of bonds based on blockchain was announced at the Exchange forum by the chairman of the board of NSD, Eddie Astanin.]
- [16] Aitken, Roger. "MUSE: Leveraging Blockchain Technology To Revolutionize Music Industry". *forbes.com*. Retrieved 18 June 2016.
- [17] Ann Williams (12 July 2016). "IBM to open first blockchain innovation centre in Singapore, to create applications and grow new markets in finance and trade". *The Straits Times*. Singapore Press Holdings Ltd. Co. Retrieved 13 November 2016.
- [18] Stan Higgins (9 November 2016). "Former Estonian President to Lead World Economic Forum Blockchain Group". *Coindesk*. Retrieved 13 November 2016.
- [19] "The future of blockchain in 8 charts". *Raconteur*. Raconteur Media. 27 June 2016. Retrieved 3 December 2016.
- [20] Lestor Coleman (12 April 2016). "Global Blockchain Forum Launched to Coordinate Regulatory Interoperability and Best Practices". *cryptocoinsnews*. Retrieved 4 December 2016.
- [21] "Blockchain - Secured way of transaction". iFour Technolab Pvt. Ltd. Retrieved 2016-11-15.
- [22] Armstrong, Stephen (2016-11-07). "Move over Bitcoin, the blockchain is only just getting started". *Wired (magazine)*. Retrieved 2016-11-09.
- [23] Don Tapscott; Alex Tapscott (8 May 2016). "Here's Why Blockchains Will Change the World". *Fortune*. Retrieved 16 November 2016.
- [24] Michele Tucci (29 November 2015). "Can blockchain help the cards and payments industry?". *TechinAsia*. Retrieved 16 November 2016.
- [25] Mazonka, Oleg. "Blockchain: Simple Explanation" (PDF). Journal of Refence.
- [26] Linus Torvalds (2007-05-03). *Google tech talk: Linus Torvalds on git*. Event occurs at 02:30. Retrieved 2007-05-16.
- [27] Bhaskar, Nirupama Devi; David LEE Kuo Chuen (2015). "3 – Bitcoin Mining Technology". *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press. pp. 47–51. ISBN 978-0-12-802117-0. Retrieved 2 December 2016.
- [28] Jamie Redman (25 October 2016). "Disney Reveals Dragonchain, an Interoperable Ledger". *Bitcoin.com*. Retrieved 4 December 2016.
- [29] Andreas Antonopoulos (20 February 2014). "Bitcoin security model: trust by computation". *Radar*. O'Reilly. Retrieved 19 November 2016.
- [30] Antonopoulos, Andreas M. (2014). *Mastering Bitcoin. Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media. ISBN 1449374034. Retrieved 3 November 2015.
- [31] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). *bitcoin.org*. Retrieved 28 April 2014.
- [32] "Permissioned Blockchains". *Explainer*. Monax. Retrieved 20 November 2016.
- [33] Franco, Pedro (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons. p. 95. ISBN 9781119019145. Retrieved 6 November 2016.
- [34] Clay Michael Gillespie (15 August 2014). "Official NXT Decision: No Blockchain Rollback". *cryptocoin news*. Retrieved 13 November 2016.
- [35] Kopstein, Joshua (2013-12-12). "The Mission to Decentralize the Internet". *The New Yorker*. Retrieved 30 December 2014. The network's 'nodes'—users running the bitcoin software on their computers—collectively check the integrity of other nodes to ensure that no one spends the same coins twice. All transactions are published on a shared public ledger, called the 'block chain'
- [36] Gervais, Arthur; Karame, Ghassan O.; Capkun, Vedran; Capkun, Srdjan. "Is Bitcoin a Decentralized Currency?". *InfoQ*. InfoQ & IEEE computer society. Retrieved 11 October 2016.

- [37] Voorhees, Erik (2015-10-30). "It's All About the Blockchain". *Money and State*. Retrieved 2015-11-02.
- [38] Reutzel, Bailey (2015-07-13). "A Very Public Conflict Over Private Blockchains". *PaymentsSource*. New York, NY: SourceMedia, Inc. Retrieved 18 June 2016.
- [39] Casey, Michael J. (2015-04-15). "Moneybeat/BitBeat: Blockchains Without Coins Stir Tensions in Bitcoin Community". *The Wall Street Journal*. Retrieved 18 June 2016.
- [40] dinbits Staff (2015-11-03). "The "Blockchain Technology" Bandwagon Has A Lesson Left To Learn". *dinbits.com*. Retrieved 2016-06-18.
- [41] DeRose, Chris (2015-06-26). "Why the Bitcoin Blockchain Beats Out Competitors". *American Banker*. Retrieved 18 June 2016.
- [42] Greenspan, Gideon (2015-07-19). "Ending the bitcoin vs blockchain debate". *multichain.com*. Retrieved 2016-06-18.
- [43] Tapscott, Don (10 May 2016). "The Impact of the Blockchain Goes Beyond Financial Services". *Harvard Business Review*. Retrieved 16 May 2016.
- [44] Hampton, Nikolai (2016-09-05). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". *Computerworld*. IDG. Retrieved 2016-09-05.
- [45] Blocki, Jeremiah Blocki (2016-08-24). "Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond*" (PDF). *iacr.org*. International Association for Cryptologic Research (IACR). Retrieved 2016-11-20.
- [46] "Ethereum's Gold Rush is Drawing Bitcoin Miners to Ethereum". *Bitcoin Mining*. 2016-06-20. Retrieved 2016-09-17.
- [47] JP Buntinx (May 1, 2016). "The Road To Bitcoin Adoption Passes Through Many Stages". *NewsBTC*. Retrieved 4 December 2016.
- [48] James Ovenden. "Blockchain Top Trends In 2017". The Innovation Enterprise. Retrieved 4 December 2016.
- [49] "Crypto-Currency Market Capitalizations". *CoinMarketCap*. Retrieved 2016-09-17.
- [50] "Will Open Source Drive Blockchain Interoperability?". *American Banker*. SourceMedia. 23 November 2016. Retrieved 4 December 2016.
- [51] Giulio Prisco (25 August 2016). "Sandia National Laboratories Joins the War on Bitcoin Anonymity". *Bitcoin Magazine*. BTC Inc. Retrieved 21 November 2016.
- [52] Steve Wilson (3 May 2016). "Blockchain: Almost Everything You Read Is Wrong". Constellation Research Inc. Retrieved 13 November 2016.
- [53] Katie Martin (27 September 2016). "CLS dips into blockchain to net new currencies". *The Financial Times*. Retrieved 7 November 2016.
- [54] Kevin Wang, Ali Safavi (29 October 2016). "Blockchain is empowering the future of insurance". *Tech Crunch*. AOL Inc. Retrieved 7 November 2016.
- [55] Joe McKendrick (22 July 2016). "Cloud Vendors, The Great Disruptors, Face Disruption From Blockchain". *forbes.com*. Retrieved 13 November 2016.
- [56] Giulio Prisco (9 May 2016). "Delaware Blockchain Initiative to Streamline Record-Keeping for Private Companies". *Bitcoin Magazine*. BTC Inc. Retrieved 5 December 2016.
- [57] Gertrude Chavez-Dreyfuss (16 June 2016). "Sweden tests blockchain technology for land registry". Reuters. Retrieved 7 November 2016.
- [58] Laura Shin (21 April 2016). "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury". *forbes.com*. Retrieved 13 November 2016.
- [59] "The Ethical and Fair Creators Association". Retrieved 2 December 2016.
- [60] Martin Arnold (23 September 2013). "IBM in blockchain project with China UnionPay". *The Financial Times*. Retrieved 7 November 2016.
- [61] "Blockchain reaction: Tech companies plan for critical mass" (PDF). EYGM. p. 5. Retrieved 13 November 2016.
- [62] "Online Voting Platform FAQ's". Follow My Vote. Retrieved 7 December 2016.
- [63] Meg Bryant (5 May 2016). "Blockchain may be healthcare's answer to interoperability, data security". *Health Care Dive*. Industry Dive. Retrieved 4 December 2016.

- [64] Joesph Young (15 December 2016). "Ernst & Young Is Going Bitcoin While PwC, Deloitte and KPMG Push Permissioned Blockchains". *CoinTelegraph.com*. Retrieved 17 December 2016.
- [65] Franco, Pedro (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons. p. 9. ISBN 1119019168. Retrieved 4 January 2017.
- [66] International Monetary Fund (2016). *Virtual Currencies and Beyond: Initial Considerations IMF Discussion Note*. International Monetary Fund. p. 23. ISBN 9781513552972. Retrieved 12 November 2016.
- [67] Swan, Melanie (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc. p. 16. ISBN 1491920475. Retrieved 12 November 2016.
- [68] <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> Retrieved November-2016
- [69] Catalini, Christian; Gans, Joshua S. (2016-11-23). "Some Simple Economics of the Blockchain". Rochester, NY: Social Science Research Network. doi:10.2139/ssrn.2874598.
- [70] Ehsani, Farzam (22 December 2016). "Blockchain in Finance: From Buzzword to Watchword in 2016". *CoinDesk (News)*. Retrieved 22 December 2016.
- [71] Catalini, Christian; Tucker, Catherine E. (2016-08-11). "Seeding the S-Curve? The Role of Early Adopters in Diffusion". Rochester, NY: Social Science Research Network. doi:10.2139/ssrn.2822729.
- [72] Epstein, Jim (2016-05-06). "Is Blockchain Technology a Trojan Horse Behind Wall Street's Walled Garden?". *Reason*. Retrieved 2016-06-29. *mainstream misgivings about working with a system that's open for anyone to use. Many banks are partnering with companies building so-called private blockchains that mimic some aspects of Bitcoin's architecture except they're designed to be closed off and accessible only to chosen parties. ... [but some believe] that open and permission-less blockchains will ultimately prevail even in the banking sector simply because they're more efficient.*
- [73] Redrup, Yolanda (2016-06-29). "ANZ backs private blockchain, but won't go public". *Australia Financial Review*. Retrieved 2016-07-07. *Blockchain networks can be either public or private. Public blockchains have many users and there are no controls over who can read, upload or delete the data and there are an unknown number of pseudonymous participants. In comparison, private blockchains also have multiple data sets, but there are controls in place over who can edit data and there are a known number of participants.*
- [74] Kelly, Jemima (2016-09-28). "Banks adopting blockchain 'dramatically faster' than expected: IBM". Reuters. Retrieved 2016-09-28.
- [75] "MasterCard pushes ahead into blockchain tech". *Business Insider*. 2016-11-02. Retrieved 2016-11-04.
- [76] Marr, Bernard. "How Blockchain Technology Could Change The World". *Forbes*. Retrieved 2017-01-06.
- [77] "Why Bitcoin may herald a new era in finance". *www.economistinsights.com*. The Economist Group. Retrieved 9 June 2015.
- [78] De Filippi, Primavera. *From competition to cooperation*. TEDxCambridge. Retrieved 8 October 2015.
- [79] Coppola, Gabrielle & Benmeleh, Yaacov. "This Israeli Ride-Sharing App Is the Utopian, Hippie Uber". *Bloomberg*. Retrieved 27 January 2016.
- [80] Ayral, Sandrine. "Bitcoin 2.0 Crowdfunding Is Real Crowdfunding". *Techcrunch*. Retrieved 27 January 2016.
- [81] Miller, Carl. "In 2015 social media companies strengthened their rule. In 2016 they will face rebellion". *The Telegraph*. Retrieved 27 January 2016.
- [82] Jean-Pierre Buntinx (4 August 2015). "Future Use Cases for Blockchain Technology: Copyright Registration". *bitcoin.com*. Saint Bitts. Retrieved 5 November 2016.
- [83] "Blockchain Could Be Music's Next Disruptor". 22 September 2016.
- [84] Bartlett, Jamie (6 September 2015). "Imogen Heap: saviour of the music industry?". *theguardian.com*. Retrieved 18 June 2016.
- [85] Nash, Kim S. (2016-07-14). "IBM Pushes Blockchain into the Supply Chain". *Wall Street Journal*. Retrieved 2016-07-24.
- [86] Allison, Ian (2016-05-03). "Deloitte to build Ethereum-based 'digital bank' with New York City's ConsenSys". *International Business Times*.
- [87] Allison, Ian (2016-01-20). "R3 completes trial of five cloud-based blockchain technologies at 40 banks". *International Business Times*.

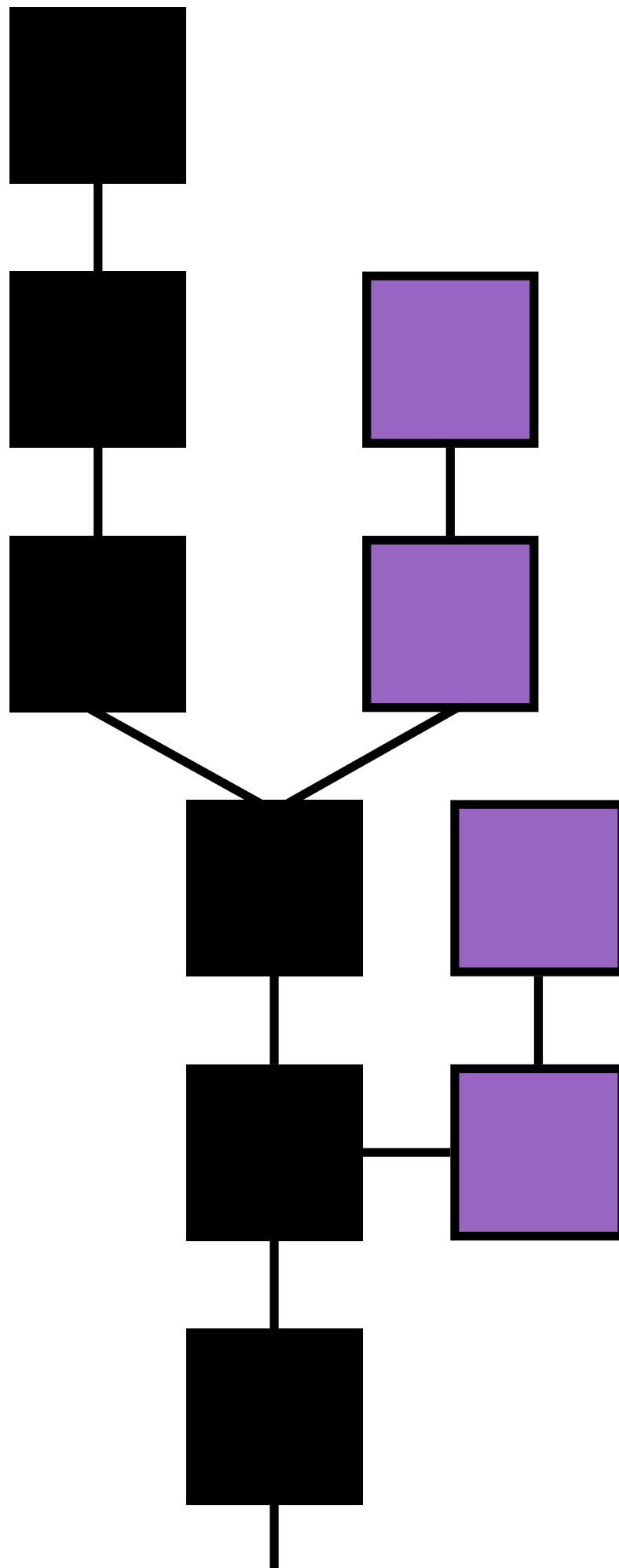
- [88] “Hyperledger blockchain code almost comes together for IoT”. *rethink-iot.com*. 1 April 2016. Retrieved 18 June 2016.
- [89] “SafeShare Releases First Blockchain Insurance Solution For Sharing Economy”. *EconoTimes*. 2016-03-18. Retrieved 2016-06-15.
- [90] Andrew Quentson (11 September 2016). *Swiss Industry Consortium to Use Ethereum’s Blockchain*. *cryptocoins news*. Retrieved 6 November 2016.
- [91] Friedlmaier, Maximilian; Tumasjan, Andranik; Welp, Isabell (2016-08-26). “Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures”. Retrieved 2016-11-29.
- [92] Higgins, Stan (2016-12-16). “ABN Amro Tests Blockchain for Real Estate Transactions”. *CoinDesk.com*. Retrieved 2016-12-18.
- [93] Exant, Andy (2015). “The future of cryptocurrencies: Bitcoin and beyond”. *Nature*. **526** (7571): 21–23. doi:10.1038/526021a. ISSN 0028-0836. OCLC 421716612.
- [94] del Castillo, Michael (22 December 2016). “Ledger Publishes First Volume of Peer-Reviewed Blockchain Research”. *coindesk.com*. Archived from the original on 10 January 2017. Retrieved 10 January 2017.
- [95] “Ledger”. *worldcat.org*. Archived from the original on 11 January 2017. Retrieved 11 January 2017.
- [96] Hertig, Alyssa (15 September 2015). “Introducing Ledger, the First Bitcoin-Only Academic Journal”. *motherboard.vice.com*. Vice Media. Archived from the original on 10 January 2017. Retrieved 10 January 2017.
- [97] Rizun, Peter R.; Wilmer, Christopher E.; Burley, Richard Ford; Miller, Andrew (2015). “How to Write and Format an Article for Ledger” (PDF). *Ledger*. doi:10.5195/LEDGER.2015.1. ISSN 2379-5980. OCLC 910895894. Retrieved 11 January 2017.

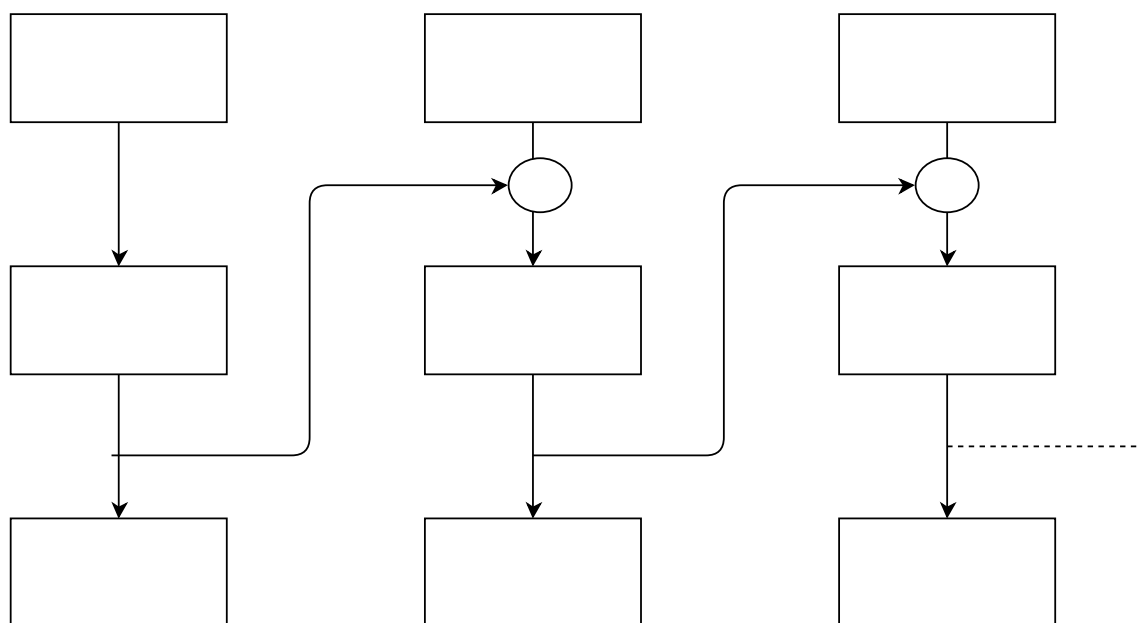
7 Further reading

- Higgins, Stan (2016-03-03). “40 Banks Trial Commercial Paper Trading in Latest R3 Blockchain Test”. *CoinDesk*. Retrieved 2016-03-21.
- Richard Gardner. “a ledger of digital transactions shared by many different computers to arrive at a consensus”. *Modulusfe*.

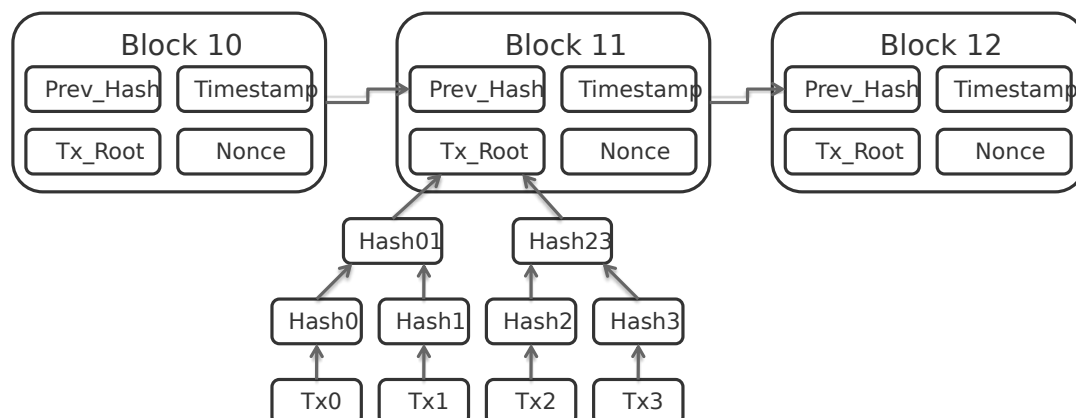
8 External links

- *Ledger*, a peer-reviewed scholarly journal.

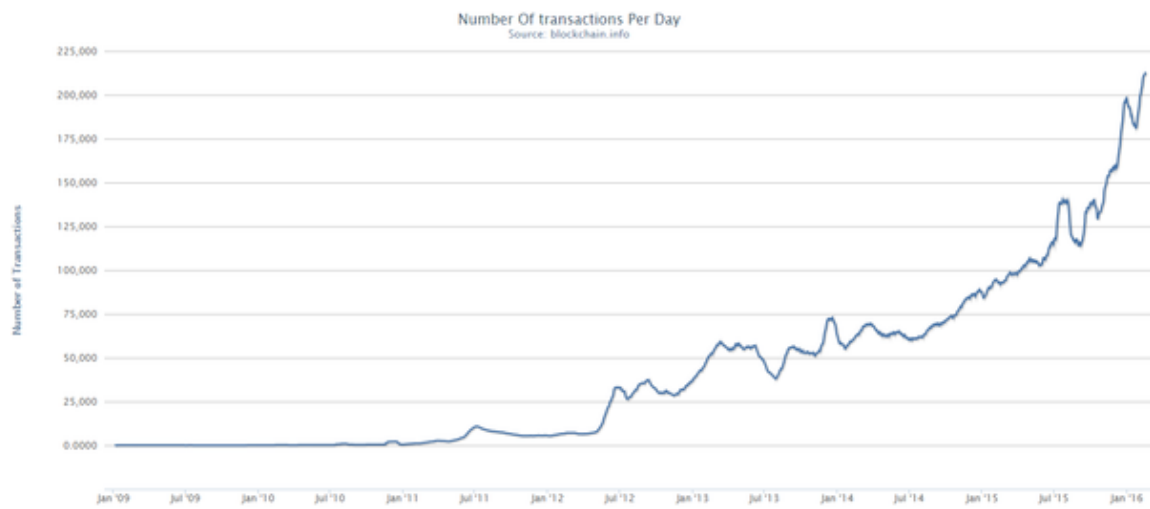




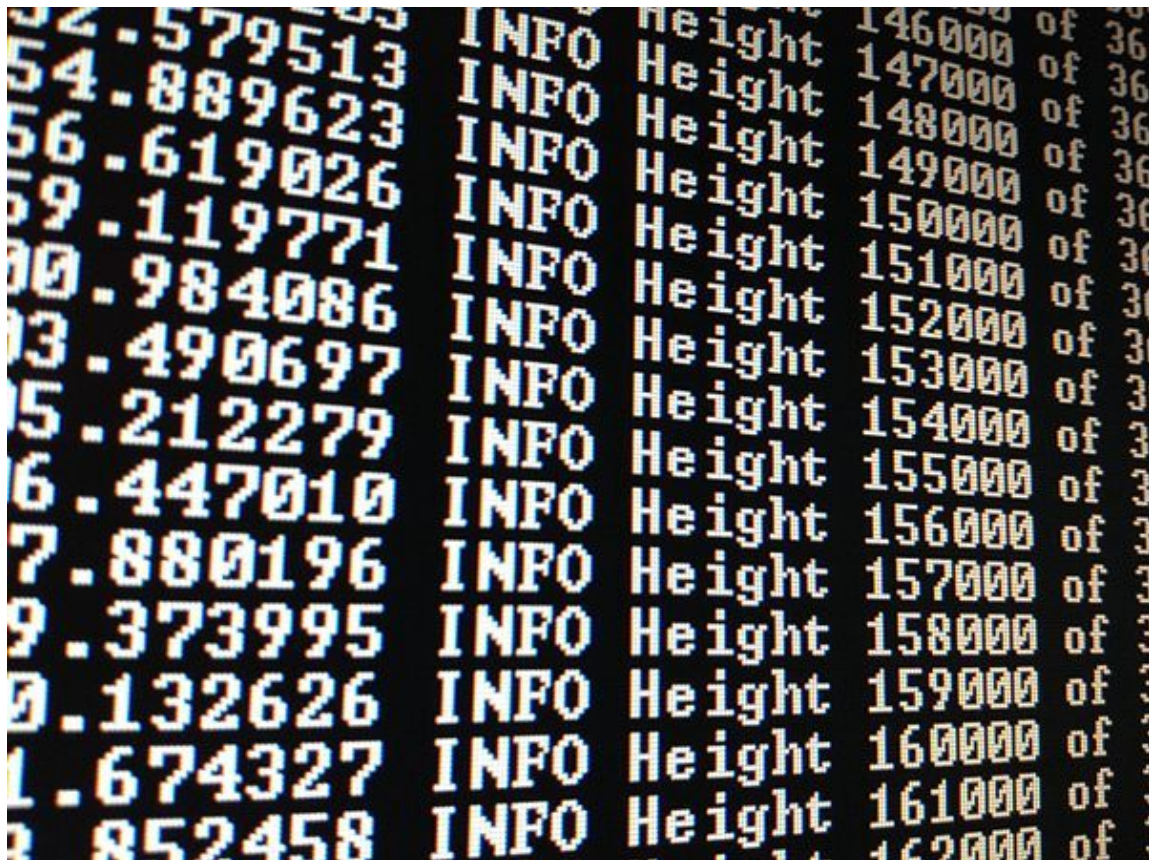
Cipher-block chaining operations



Bitcoin network data



Bitcoin transactions (January 2009 - September 2015)



Blockchain data

9 Text and image sources, contributors, and licenses

9.1 Text

- **Blockchain (database)** *Source:* [https://en.wikipedia.org/wiki/Blockchain_\(database\)?oldid=760005853](https://en.wikipedia.org/wiki/Blockchain_(database)?oldid=760005853) *Contributors:* The Anome, Edward, Nealmcb, 5ko, Grin, Apegrl, Greenrd, Jleedev, David Gerard, DavidCary, Bkonrad, Rchandra, Khalid hassani, Beland, Nerdfiles, Shiftchange, Pmetzger, Stesmo, DrummondReed, Danhash, Clotho, LjL, GünniX, Intgr, Bgwhite, Tunafizzle, Sneak, William Caputo, Deku-shrub, Eclipsed, Abune, Ladislav Mecir, Jtbobwaysf, Aldaron, Hockeyshooter, Kencf0618, Jfayel, Philippschaumann, Chris55, N2e, Krauss, Kdevans, Medovina, Grubbiv, PamD, Headbomb, Marek69, Mmortal03, Silver seren, Lfstevens, NapoliRoma, TAnthony, Magioladitis, Dulciana, Snowded, StephenJennings, AlexandreQuessy, Ontarioboy, Baldusi, Xilehence, Poltair, Laoris, Zxsmt, Afernand74, Plastikspork, Trivialist, Rhododendrites, MasterOfHisOwnDomain, Alex Zivoder, Mrcatzilla, Yobot, AnomieBOT, DerPaul, Jim1138, MaterialsScientist, Citation bot, Elninopanza, Control.valve, Dpinna85, Meldaravaniel, Sanpitch, LittleWink, Jonesey95, Serols, Trappist the monk, Eeik, Ivanvector, Dewritech, Dcirovic, Humanist09, Jonpatterns, Casascius, FeatherPluma, ClueBot NG, Irishstones, Frietjes, BG19bot, Esoteric10, Kwetal1, Hamez0, Hotgardener, Earl King Jr., Alloy020, Me, Myself, and I are Here, Ratha K, RaphaelQS, Tedsanders, FockeWulf FW 190, Claw of Slime, Mr. Smart LION, Powerful Lomax, Nikolaiho, Vwm3nelson, Amber62, Kancer89, Liance, Oxfff, Underr.ua, JefKay, Shreyasgm, Oluwa2Chainz, Wikihelpful, Ethernomad, Drjohncavazos, Thereisnous, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Webnator, Rt665j4, Jpkabin, Kapten grogg, OnePercent, AdWomanMan, Abrrr5583, Singleissuevoter, McGucket, Sam0225, Jornfranke, Satoshlong, Fouetté rond de jambe en tournant, Alpacahats, Brian1337johnson, AlexM202020, 127herudo31, LouYu2016, Carlynoelle, Bender the Bot, Earl King, Bramcohen, Sparkyscience, Villei, Wkzkwz, Ameersoric, W w smith, FPouliot, AhmedAlMallah, Preetypmr, MartinRits, HGR334, Malviyaop, Blockchainster, Alice2017 and Anonymous: 122

9.2 Images

- **File:Bitcoin.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/4/46/Bitcoin.svg> *License:* CC0 *Contributors:* This file was derived from: Bitcoin logo.svg
Original artist: Bitboy
- **File:BitcoinSign.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/b/ba/BitcoinSign.svg> *License:* Public domain *Contributors:* <http://bitcoin.org> *Original artist:* Satoshi Nakamoto
- **File:Bitcoin_Block_Data.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/55/Bitcoin_Block_Data.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Matthäus Wander
- **File:Bitcoin_transactions_per_day.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1a/Bitcoin_transactions_per_day.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Ster3oPro
- **File:Blockchain.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/5/50/Blockchain.jpg> *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* deavmi
- **File:Blockchain.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/9/98/Blockchain.svg> *License:* CC BY 3.0 *Contributors:* Bitcoin Wiki: <https://en.bitcoin.it/wiki/File:Blockchain.png> *Original artist:*
 - original file: Theymos from Bitcoin wiki
 - vectorization: Own work
- **File:Cipher-block_chaining_(CBC).svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/75/Cipher-block_chaining_%28CBC%29.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* יובל מדר
- **File:Commons-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg> *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Crypto_key.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/65/Crypto_key.svg *License:* CC-BY-SA-3.0 *Contributors:* Own work based on image:Key-crypto-sideways.png by MisterMatt originally from English Wikipedia *Original artist:* MesserWoland
- **File:Desktop_computer_clipart_-_Yellow_theme.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d7/Desktop_computer_clipart_-_Yellow_theme.svg *License:* CC0 *Contributors:* <https://openclipart.org/detail/17924/computer> *Original artist:* AJ from openclipart.org
- **File:Emblem-money.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/f3/Emblem-money.svg> *License:* GPL *Contributors:* <http://www.gnome-look.org/content/show.php/GNOME-colors?content=82562> *Original artist:* perfectska04
- **File:Folder_Hexagonal_Icon.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/48/Folder_Hexagonal_Icon.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Internet_map_1024.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg *License:* CC BY 2.5 *Contributors:* Originally from the English Wikipedia; description page is/was here. *Original artist:* The Opte Project
- **File:Nuvola_apps_kaboodle.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1b/Nuvola_apps_kaboodle.svg *License:* LGPL *Contributors:* <http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz> *Original artist:* David Vignoni / ICON KING
- **File:Symbol_book_class2.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/89/Symbol_book_class2.svg *License:* CC BY-SA 2.5 *Contributors:* Mad by Lokal_Profil by combining: *Original artist:* Lokal_Profil
- **File:Symbol_list_class.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/d/db/Symbol_list_class.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Wiki_letter_w_cropped.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1c/Wiki_letter_w_cropped.svg *License:* CC-BY-SA-3.0 *Contributors:* This file was derived from Wiki letter w.svg: ``
Original artist: Derivative work by Thumperward

9.3 Content license

- Creative Commons Attribution-Share Alike 3.0