Blockchain

What is blockchain?

Blockchain can be presented as an accounting ledger or shared digital register which is secure and transparent, accessible to all, and extremely difficult to alter. It is best known as the underlying technology for cryptocurrency, but its applications and potential for businesses extend far beyond this use. The main function of blockchain is to guarantee the uniqueness and immutability of information through its data structure. This is made up of a series of blocks that are linked to each other (hence the term blockchain) to ensure that each transaction or entry is unique, signed and unforgeable. Thanks to this and its decentralised nature, blockchain allows transactions to be validated and recorded across a computer network without the need for a central authority.

Blockchain allows direct transactions between parties without the need for an intermediary, such as a bank. One of the main strengths of blockchain is that it is a system where trust is intrinsic and shared, relying on the community to ensure the verification and authenticity of transactions.

To this end, blockchain relies on a consensus mechanism. This mechanism allows those in the blockchain network to agree on the validity of information or a transaction, guaranteeing the system's integrity and security without having to resort to a central authority. There are several consensus mechanisms, the best known of which are Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake (DPoS).

Security *Transparency* **Decentralisation**
Smart contracts *Transactions*
Peer-to-Peer *Economy* **Traceability** *Cryptocurrency*
Tokenisation *Storage* **Anonymisation**
Technology **Trust** *Confidentiality*
Consensus *NFT*

REPUBLIQUE ET CANTON DE GENEVE
h e g Haute école de gestion Genève
UNIVERSITÉ DE GENÈVE

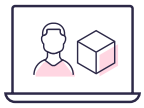
Learn more

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

How a transaction works on the blockchain (according to the POW consensus)

1 Initiating the transaction

Person A wants to make a transaction to person B, such as a cryptocurrency transfer.

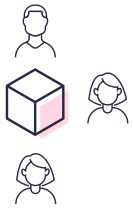


2 Creating the transaction

Person A creates a transaction. This transaction includes information such as the amount to be transferred, the recipient's address, a digital signature to prove the transaction's authenticity, and possibly a transaction fee.

3 Broadcasting the transaction

The transaction is broadcast to the blockchain network. This is a broadcast database containing the history of all the transactions carried out between users, known as a "registry". The transaction is represented online by a "block". Network nodes (computers participating in the network) receive the transaction.

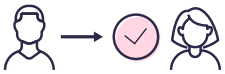


4 Verification by nodes

The network nodes verify the transaction's validity through cryptographic techniques. They examine the digital signature, the funds available in Person A's account, and ensure that the transaction does not violate the rules of the blockchain protocol. The transaction is transformed into a unique digital identifier called a "hash".

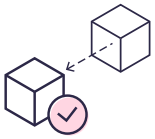
5 Validating the transaction

The validator verifies the transaction's validity by checking the digital signature, the funds available in Person A's account, and ensuring that protocol rules are followed.



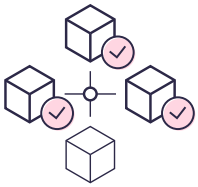
6 Creating a block

Once enough transactions have been verified and grouped together, a network node or "miner" creates a new block. All the nodes compete to register the block by solving a "mathematical puzzle" to get compensated for this work. This block contains a record of all the verified transactions and a link to the previous block.



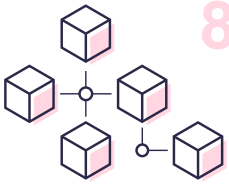
7 Reaching consensus

Once the majority of nodes in the network have accepted the validity of the new block, consensus has been reached. This ensures that all the nodes reach agreement on the state of the ledger.



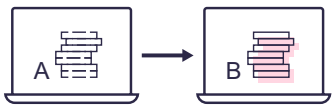
8 Adding to the blockchain

The new block is added to the existing blockchain. Each block contains a link to the previous once, forming a continuous, unalterable chain.



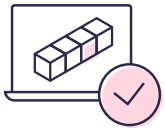
9 Updating balances

The amount is debited from Person A's account to be added to Person B's account.



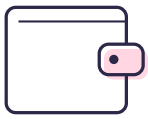
10 Confirming the transaction

Once the transaction has been confirmed and added to the chain, Person B can see the funds in their account. The transaction is then considered complete.



Fundamental concepts of blockchain

What is a blockchain wallet and how does it work?



A blockchain wallet is an application or device which allows users to store and manage their digital assets, such as cryptocurrency. Each wallet has a pair of keys: a public key (this is the wallet's address, like an IBAN code, e.g. 0xBa42BFFF-D11aF1Dd027F4DDe9E-4b75a25df3308f), which corresponds to the address that funds or digital assets to be received into the digital wallet, and a private key (password), which is kept secret and gives access to the contents of the wallet, as well as being used for authorising outgoing transactions. All transactions are recorded and verified on the blockchain. The wallet's security largely depends on the protection offered by the private key.

The benefits of cdr

In blockchains, several consensus mechanisms are used to validate and add new transactions to a given chain. The two most common types of consensus are proof of work (PoW) and proof of stake (PoS).

- **Proof of work (POW) :**
  In this process, miners solve complex mathematical problems to validate and add new transactions to the chain. Each problem solved allows a new block to be created. Miners compete to solve these problems, and whoever succeeds first earns the right to validate a transaction, add it to the blockchain, and get compensated for the work. However, solving these problems requires a lot of computing power, making the process energy intensive. This method makes the network's security robust, as forging transactions requires a prohibitive amount of energy and computing power.
- **Proof of stake (POS) :**
  In this process, validators are entrusted with validating transactions. They are selected based on the amount of cryptocurrency they are willing to pledge or "stake" as a guarantee of their honesty. The more cryptocurrency a validator puts into play, the greater their chances of being chosen to create a new block of transactions. This approach consumes less energy than PoW, because it does not involve solving complex mathematical problems. Instead, it relies on having trusted validators, because they have something to lose if they act maliciously. PoS rewards holding cryptocurrency for the long term: the more you have, the more likely you are to be chosen to validate transactions.

In summary, PoW focuses on solving complex - and therefore energy-intensive - problems to secure the blockchain, while PoS relies on a trust mechanism linked to a stake of cryptocurrency, which promotes engagement and saves energy.

Signing in blockchain

Signing is a cryptographic mechanism that allows an individual to prove their identity and guarantee the integrity of a transaction or message. Using a pair of keys (a private key for signing and a public key for verifying), the signature ensures that the transaction was initiated by the rightful holder of the private key, and was not tampered with along the way.

Blockchain's characteristics

Blockchain redefines how we store, manage and exchange information and assets, under the spectrum of digital trust. Here are some of its characteristics:

Decentralisation

Blockchain operates on a decentralised network of computers (nodes) located around the world. This eliminates the need for a centralised trusted third party and allows for greater resilience against outages and attacks.

Immutability

Data on the blockchain is immutable by design, meaning that once a piece of data has been added to the blockchain, it cannot be changed or deleted. As such, immutability guarantees the integrity and transparency of blockchain data and strengthens digital trust.

Digital uniqueness

This refers to the ability to ensure that a piece of data or digital object is unique and cannot be duplicated or reproduced without permission. Beyond blockchain, in the traditional digital world, everything is easily infinitely duplicatable, whether photos, videos, software or other types of data. However, blockchain makes it possible to create and verify the uniqueness of a digital asset, guaranteeing its authenticity, rarity and value.

Security

Blockchain uses advanced cryptographic techniques to secure data and transactions. Data is grouped into blocks, and these blocks are then cryptographically linked to form a chain, making it extremely difficult to falsify information.

Less need for a "middleman"

Blockchain simplifies processes by cutting out intermediaries (e.g. banks, solicitors, registers, etc.), as it plays the role of a single trusted third party. This helps reduce costs and speed up processes.

Transparency

Blockchain offers complete transparency by allowing all stakeholders to access transaction data recorded on the blockchain, without preventing confidentiality if necessary.

Traceability

Thanks to the transparent, immutable nature of blockchain, the full transaction history of an asset, product or information can be tracked.

Automation

Smart contracts are self-executing computer programmes that run automatically when certain conditions are met. They enable processes and transactions to be automated, increasing reliability, reducing costs and speeding up the process.

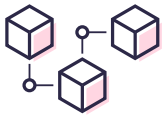
Tokenisation

Tokenisation is the process of converting a tangible asset or specific right (e.g. property, works of art, company shares, intellectual property rights) into digital tokens, symbolising a portion of the original asset within a blockchain. This allows assets such as cryptocurrencies and NFTs to be issued, exchanged and transferred securely using cryptographic protocols, without the need for intermediaries, while maintaining the transaction's authenticity.

Types of blockchain

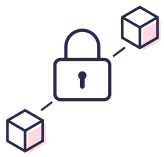
There are several types of blockchain, and each one is designed to meet specific security, privacy and governance needs. Each of these types has unique characteristics making them suitable for different use cases, and different levels of access and control.

Public blockchains



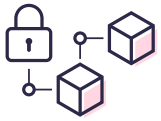
Public blockchains are open to everyone and have no access restrictions. Anyone can join the network, verify transactions, and validate blocks. The best-known examples of public blockchains are Bitcoin and Ethereum.

Private blockchains



Private or permissioned blockchains are restricted to a specific group of authorised entities or users. They are often used in companies, organisations or consortiums of participants who agree on their use to improve the efficiency and confidentiality of operations. In a private blockchain, participants are known and verified. This can enable greater transaction speed and lower transaction costs, but at the expense of decentralisation and trust.

Hybrid blockchains



Hybrid blockchains combine features from public and private blockchains. They allow levels of access and control to be customised, so that part of the blockchain can be public and accessible to everyone, while another part is private and reserved for a restricted group. Hybrid blockchains aim to reconcile the benefits of decentralisation and privacy.

What is bitcoin?

Bitcoin (BTC) is a cryptocurrency: a type of decentralised digital currency that uses blockchain to record and secure transactions. It is the first successful use case of blockchain technology. There are many other cryptocurrencies that use blockchain technology, such as Ether (ETH) and Binance Coin (BNB). Bitcoin is also the name of the platform that allows the use and circulation of the Bitcoin cryptocurrency, in the same way that Ethereum is based on the Ethereum blockchain.

What is an NFT ?

NFTs (Non-Fungible Tokens) are unique digital tokens based on blockchain technology. They are used to represent the ownership and authenticity of digital items such as artwork, videos, music, and other indivisible virtual assets. Non-fungible by definition, an asset that is considered an NFT cannot be replaced by another similar asset. Each NFT has a unique identifier and is recorded on a blockchain, guaranteeing its traceability and uniqueness.

Satoshi Nakamoto

is the pseudonym of the person(s) who developed the Bitcoin cryptocurrency. Nakamoto's work on Bitcoin made it possible to give the blockchain digital materiality.

A brief history

The history of blockchain is marked by a series of technological developments that have transformed the way we design and manage digital transactions.

1983

David Chaum introduces the concept of "blind signatures", allowing a message to be encrypted so that the recipient can decrypt and sign it without knowing the real content of the message.

2009

Satoshi Nakamoto mines the first block of the Bitcoin blockchain, marking the official beginning of the Bitcoin network and blockchain technology.

2015

Creation of the first blockchain game "Spells of Genesis" by Shaban Shaame from Geneva, marking the beginning of NFTs.

2015

Launch of Ethereum, which brings advanced programming capabilities, expanding the potential applications of blockchain well beyond simple financial transactions.

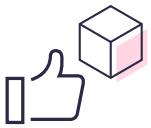
Blockchain is an ever-evolving technology, and new advances continue to be made to improve its performance, security, and potential for different applications.

Blockchain can be used in many areas:

- Trade
- Logistics
- Health
- Finance
- Games and entertainment
- Energy
- Security
- Insurance
- Property
- And many more

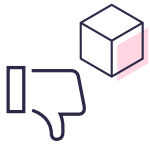
Advantages and disadvantages of blockchain

Advantages of blockchain



- **Improved security:** Data recorded on a blockchain is encrypted and cryptographically linked, making transactions and information very secure and difficult to alter.
- **Decentralisation:** Decentralization reduces the need for intermediaries and enables peer-to-peer transactions, which builds trust and reduces costs.
- **Transparency:** Transparency of transactions and data ensures that all stakeholders can verify and track operations, building trust.
- **Traceability:** Blockchain makes it possible to trace every step of a transaction or process, which is essential for supply chains, asset management and regulatory compliance.
- **Reduced errors and fraud:** The immutable nature of the data recorded on the blockchain limits the risks of human error and falsification.
- **Efficiency:** Automated processes and smart contracts reduce the need for manual processes, speeding up operations.
- **Opportunities for innovation:** Blockchain opens the door to new opportunities and offers a wide scope for innovation. New applications for the technology continue to emerge.

Disadvantages of blockchain

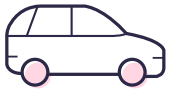


- **Energy costs:** When new blocks are registered on the blockchain, this creates varying energy costs depending on the type of consensus used. PoW is highly energy intensive, while PoS is much more economical.
- **Technical complexity:** Implementing and managing blockchain require specialist technical skills, which poses a challenge for businesses.
- **Limited reversibility:** Once a transaction is recorded on the blockchain, by design, it is intentionally made immutable and is permanently recorded.
- **Adoption and regulation:** Blockchain regulations vary greatly between countries, which affects the suitability of adopting and developing blockchain.
- **Risk of losing access:** Since blockchain operates without an intermediary (bank, solicitor, lawyer, etc.), it is your responsibility to keep your private key secure and know your public key. Losing a private key could result in permanently losing access to digital assets or data stored on the blockchain.
- **Trust level:** The level of trust depends on the number of participants in the blockchain. The more participants, the more robust the blockchain.

How can you use blockchain for your business?

Blockchain technology offers great potential for most business sectors. It paves the way for increased levels of transparency, security and efficiency by revolutionising the way data is recorded, shared and verified. The following is a non-exhaustive list of the ways in which Blockchain is being used in different sectors:

Transport and mobility



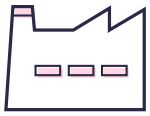
- Securely paying for public transport tickets.
- Managing public transport routes.
- Automating vehicle rental and facilitating trip sharing.
- Securing communication between driverless vehicles and infrastructure.
- Simplifying overseas parking and toll payments by automating transactions and eliminating intermediaries.
- Facilitating the management and optimisation of energy exchanges between the electrical grid and electric vehicles.
- Secure digital management of driving licenses and license plates.

Banking and insurance

- Speeding up international money transfers by cutting out intermediaries and enabling fast, cost-effective, trusted transactions.
- Simplifying verification processes for opening bank accounts and subscribing to services.
- Managing and securing digital assets (securities and bonds) by recording them transparently.
- Simplifying stock market transactions and making them secure by enabling almost instant clearing and settlement.
- Automating insurance policy claims and payment processes using blockchain-based smart contracts.
- Recording and verifying claims transparently by storing information immutably.
- Reducing fraud by storing data and transactions securely.
- Guaranteeing transaction compliance by verifying legitimacy using immutable blockchain protocols.
- Strengthening the audit and control of contractual commitments and financial activities through unique traceability and execution.

How can you use blockchain for your business?

Production



- Real-time tracking for goods shipments, ensuring supply chain transparency and security.
- Keeping real-time records of stock levels, facilitating production management and order planning.
- Facilitating tracking for sources of raw materials, components and finished products along the supply chain, ensuring traceability, transparency and compliance with quality standards.
- Automating agreements and transactions between suppliers, manufacturers and carriers, improving the efficiency of logistics processes.
- Recording conformity certification, quality labels and production standards on the blockchain, simplifying product and process control.
- Automating payments between different actors in the supply and distribution chain, thereby reducing inherent transaction risks, delays and fees associated with financial transactions.

Trade

- Tracking the origin and provenance of products along the supply chain (product traceability).
- Real-time stock level monitoring, allowing inventory and restocking to be managed and automated.
- Creating blockchain-based loyalty programmes, where points and rewards are automatically recorded and managed transparently.
- Simplifying item returns by automating records of returned product information and associated refunds.
- Certifying products.
- Managing payments between retailers, suppliers and consumers.
- Verifying the authenticity of products, thereby reducing the risk of purchasing counterfeits.

How can you use blockchain for your business?

Health

- Storing electronic patient records securely and immutably, ensuring access to relevant health information by authorised professionals.
- Secure and confidential sharing of medical data, avoiding risks associated with sharing and data misuse.
- Monitoring clinical trials, ensuring data integrity and transparency in medical research.
- Improving the traceability of medicines, reducing the risk of counterfeits and ensuring that medicines are authentic and safe.
- Recording patient authorisations and consent for medical procedures, clinical trials and information sharing.
- Automating medical bills and payments between healthcare providers, insurers and patients.
- Recording medical information (e.g. allergies, medical history) for rapid recovery in emergency situations.

Food processing

- Implementing food traceability, allowing all stakeholders to verify the origin, provenance and quality of products.
- Help identifying sources of possible food contamination by tracing products to their origin.
- Recording storage and transportation conditions for perishable products to ensure compliance with food safety standards.
- Verifying seed authenticity through registering certifications, labels and standards.
- Reducing food waste by enabling better management of the supply and production chain.
- Verifying labelling to ensure information is accurate.
- Sharing agricultural data between producers to improve practices.

Getting started with blockchain

1 Familiarise yourself with blockchain

Familiarise yourself with the basic concepts of blockchain, as well as its advantages and limitations, by participating in seminars, webinars, online courses and workshops to gain knowledge. Identify how the technology could be relevant to your project.

2 Evaluate use cases

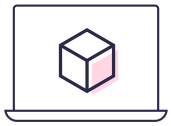
Analyse existing processes, products and services to identify areas where blockchain could add value, such as automation, traceability, transparency, transactions and cost reduction. Estimate integration costs and conduct a profitability analysis by comparing different technical solutions to achieve your desired objective. Study the different blockchain platforms available and choose the one that best suits your needs, but be aware that blockchain is not necessarily the most appropriate technical solution for your project.

3 Develop a strategy

Develop a clear strategy for integrating blockchain. Identify your objectives, resources needed, platform, deadlines and success indicators. Consult plenty of specialists to support you and help you integrate blockchain into your organisation. Develop a prototype for your project. Test it both internally and with a test group. As blockchain technology rapidly evolves, it is essential to keep your knowledge of the field up to date.

Getting started with blockchain

4 integrate blockchain with your existing systems



Integrate the blockchain solution with your existing systems. Make sure the new technology can be seamlessly integrated into your operations. Call on a specialist to help you if necessary.

Identify potential risks associated with using blockchain and mitigate them by putting measures in place. Stay informed of regulatory changes regarding blockchain.

5 Capitalise on integrating blockchain within your company

Take advantage of the increase in digital trust that blockchain creates by informing your customers, partners and other stakeholders that you have integrated blockchain into your business activities. Explain the advantages of using this technology, both for the company and for them. Always check in with your business needs and revisit how relevant it is to use any technology, including blockchain, to meet your needs.

« Blockchain goes far beyond cryptocurrencies; it is a versatile technology that reinvents transparency, trust and digital uniqueness.»

Arnaud Gaudinat, Associate Professor at Geneva Business School