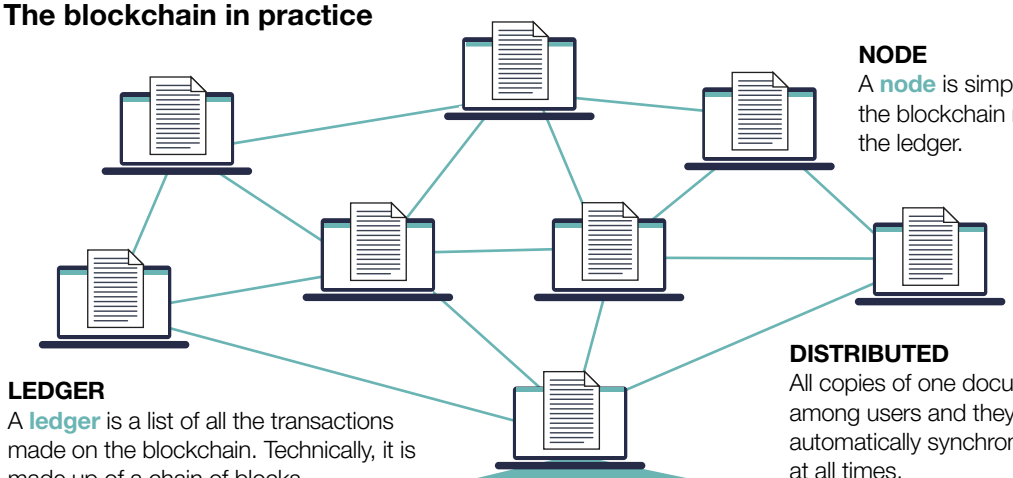
What is blockchain?

A blockchain is a shared ledger of transactions between parties in a network, not controlled by a single central authority. You can think of a ledger like a record book: it records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called nodes.

The blockchain in practice



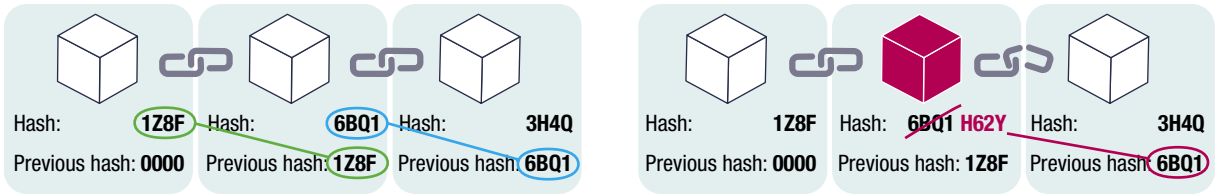
NODE
A node is simply a computer on the blockchain network that stores the ledger.

LEDGER
A ledger is a list of all the transactions made on the blockchain. Technically, it is made up of a chain of blocks.

DISTRIBUTED
All copies of one document are spread among users and they are constantly and automatically synchronised, hence identical at all times.

BLOCKCHAIN UNDER THE HOOD

A block is comprised of a group of transactions from the same time period, like a page from a record book.



Source: Savjee, (2017)

Inside each block:
Hash
Previous block's hash
Transaction data
Timestamp

Along with its own hash, each block stores the hash of the block before it.
A hash is a unique string of letters and numbers created from text using a mathematical formula. Blocks are therefore "chained" together making the ledger (almost) immutable or unable to be changed. To add a block, it may first need to be mined and then approved by a number of notes through a consensus mechanism.

Different types of blockchain

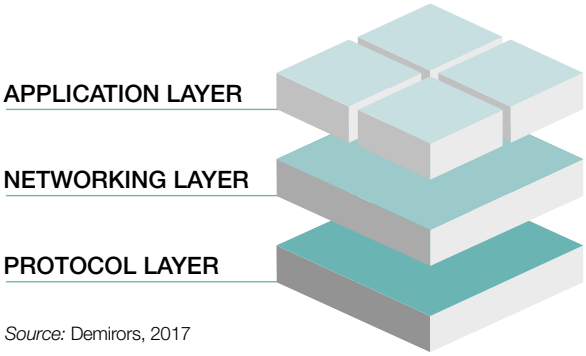
Before going further, it is important to note that not every blockchain is made the same. While there are a number of variable features, two of the most important are the **"openness" of the platform** (public or private) and the **level of permissions required to add information** to the blockchain (permissioned or permissionless). **Public** blockchains (like Bitcoin) are open for anyone to read and view, while **private** blockchains can only be viewed by a chosen group of people. Similarly, **permissioned** blockchains permit just a select group of users to write (i.e. generate transactions for the ledger to record) and commit (i.e. verify new blocks for addition to the chain). In contrast, **permissionless** blockchains allow anyone to contribute and add data to the ledger.

Table 1. The main types of blockchain segmented by permission model

			READ	WRITE	COMMIT	EXAMPLE
BLOCKCHAIN TYPES	OPEN	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Supply chain ledger for retail brand viewable by public
	CLOSED	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned "enterprise"	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	External bank ledger shared between parent company and subsidiaries

Source: Hileman & Rauchs, 2017

The layers of blockchain



Source: Demirors, 2017

Blockchain is comprised of three layers that each add different components to its development. It is not necessary to get involved in the most technical layers in order to develop an application or use a blockchain application.

The **protocol layer** lays the foundational structure of the blockchain. It determines the computing language the blockchain will be coded in and any computational rules that will be used on the blockchain.

The **networking layer** is where the rules set up on the protocol layer are actually implemented.

The **application layer** is where networks and protocol are used to build applications that users interact with.

Blockchain's key characteristics

Distributed

One of the core aspects of a blockchain is that it is a distributed ledger, meaning that the database is maintained and held by all nodes in the network. No central authority holds or updates the ledger, rather each node independently constructs its own record by processing every block (group of transactions), deciding if it is valid, then voting via the **consensus mechanism** on their conclusions. Once a change in the record is agreed, each node updates its own ledger.
In contrast, traditional databases are stored and maintained centrally, which can make them high-value targets for hackers and criminals.

Immutable

In general, once a transaction is added to a blockchain ledger, it cannot be undone.
This immutability is one of the principal aspects that contribute to the trustworthiness of blockchain transactions. A blockchain's immutability is secured through its use of cryptography (see below for an explanation of **hashing**). In a traditional, centralised database, an authorised user can connect to the server to add or modify the data without the approval or detection of other users. Because all the data is held in one place, if the security of the server or the authority that runs the server is compromised, data can be modified or permanently deleted. This may sometimes be irreversible and occur without anyone else realising it.

Agreed by consensus

No block can be added to the ledger without approval from specified **nodes** in the network. Rules regarding how this consent is collected are called **consensus mechanisms**. Consensus protocols are crucial in ensuring that every block is valid and that all participants agree and maintain the same version of the ledger. They heavily affect the incentives for nodes to act honestly and are therefore the most important variables when designing a blockchain.

Misconceptions about blockchain

Pseudonymous

Contrary to popular belief, in general, blockchain technology does not allow its users to be totally anonymous. Rather, public blockchain platforms tend to be **pseudonymous**: user identities can be anonymous but their accounts are not, as all of their transactions are visible to all other users. On these platforms, user accounts can be created without any identification or authorisation process. This allows users to use a pseudonym. **Permissioned** blockchains can require a user's identity to be verified before they are able to access or use the blockchain.

…Well "almost" immutable…

While rare, it is possible for the blockchain to be compromised if nodes pool their resources and collude to approve incorrect ledger entries. However, the larger the network, the more difficult it becomes to carry out this attack. In most systems, it would cost the attacker many more resources to carry out the attack than they would gain from the attack itself. Additionally, some private blockchains allow for central authority nodes to change information on the ledger. Advances in quantum computing (supercomputing) threaten some current cryptographic security measures, but there is equally the likelihood that blockchain's security will evolve with quantum computing capabilities.