

If you've been on the internet within the last five years, you'll have heard of blockchain, but may still be unsure of exactly what one is, or what it does. Essentially, a blockchain is a way of storing information in a decentralised network in a way that prevents the data from being altered or tampered with.

Everyone from disruptive startups to blue chip banks are interested. But is blockchain truly a technology that could change our lives as completely as the introduction of the internet, or a solution in search of a problem?

What IS a blockchain exactly?

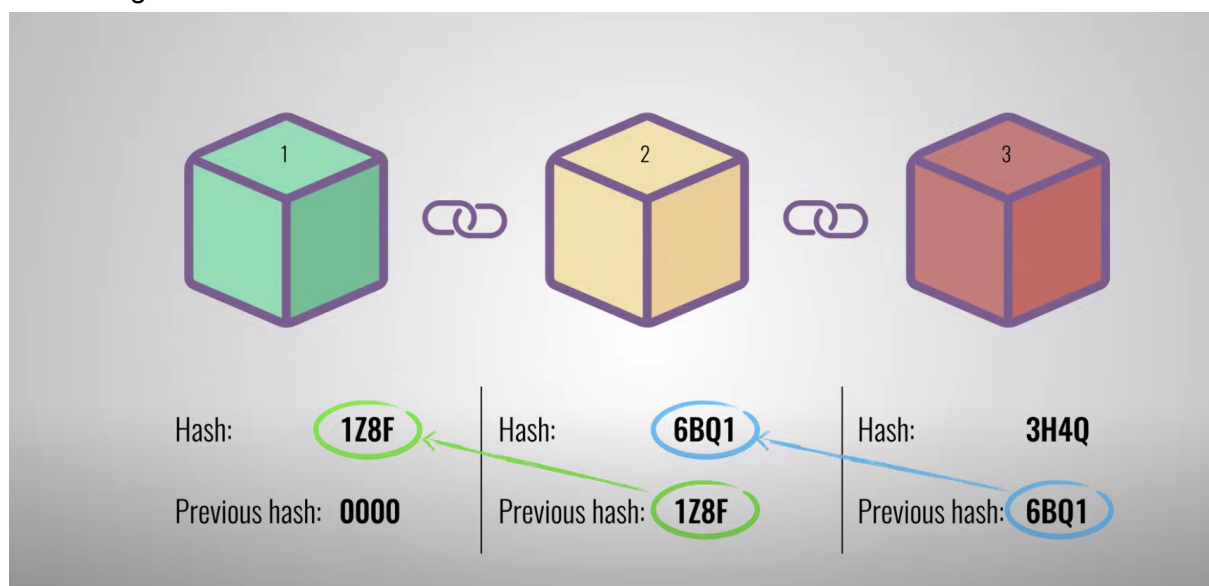
A blockchain is, unimaginatively, 'blocks' of data which are linked together in a chain. Each block refers to the previous block in the chain right back to the first, or 'genesis' block. The way the blocks are linked together makes it very difficult – close to impossible – to tamper with each block's data.

Each block contains three types of information:

- **Data:** The data will depend on the blockchain. For example, blocks on Bitcoin's blockchain contain data of the sender, receiver, and amount of each transaction.
- **Hash:** A unique identifier, like a fingerprint, for each block. A hash is calculated computationally from the block's data content.
- **Hash of the previous block:** Each block contains the unique identifier of the previous block. This is the 'chain' that links each block together.

Step 1: A chain of fingerprints

Changing a block's data causes the hash, the unique identifier, the block's 'fingerprint', to also change.



[\(Source\)](#)

As each block contains the hash or identifier of the previous block, we can compare adjacent blocks to see if the hashes match. If the hashes don't match, we can assume that the data of the block has been tampered with – this invalidates all of the following blocks in the chain. This is the first way that the blockchain secures each block's data.

Unfortunately, comparing a chain of hashes is not enough to keep a blockchain free from interference. Today's computers are so fast, they can calculate millions of hashes per minute. It is entirely possible to change a block, recalculate the hash, and then recalculate hashes for the whole chain before someone notices.

Step 2: Proof-of-Work

The second way a blockchain maintains security is through **Proof-of-Work**. Proof-of-Work is a mechanism which imposes a cost on block creation, which slows down the creation of new blocks. Before a block can be added to a blockchain, one of the nodes of the blockchain must expend a certain amount of computational power or work.

Tampering with one block means not only carrying out the proof-of-work for the tampered block, but for all of the following blocks in the chain. This makes the cost of tampering with a blockchain inefficient compared with the potential upside of accessing or changing the data. With enough computational power (and money to run it), however, re-calculating the whole chain is still possible – and could be worth it for a big enough reward.

Step 3: Decentralised network

The final – and most important – way a blockchain stays secure is by decentralising where it is stored. A blockchain is not stored or managed by a central network, instead, it uses a P2P network of multiple users and nodes.

Each node of the network owns a full copy of the blockchain. Every node in the network can add a new block to the blockchain, but cannot alter any of the existing blocks. Whenever a new block is calculated, it is sent to every node in the network. Each node checks if the new block's hash matches the hash of the previous block (and thus has not been tampered with).

If the nodes of the network verify that the new block is valid, the node adds the new block to its copy of the blockchain. Blocks that have been tampered with will not match, and will be rejected.

With a decentralised network, it's not IMPOSSIBLE to tamper with the chain – but you would need to tamper with the blocks on each node, redo the proof of work for all tampered blocks on each node, and control more than 50% of the network in order for your altered chain to be accepted. This is what makes a blockchain very secure.

History of Blockchain

The technique behind the blockchain was developed by a group of researchers in 1991, with the intention of timestamping digital documents in such a way that the document and timestamp could not be altered or backdated – a sort of digital notary.

The discovery went mostly ignored and unused until 2009, when the mysterious figure ‘Satoshi Nakamoto’ adapted the technique to create the cryptocurrency Bitcoin – the most famous example of a blockchain – and made the open-source software available so everyone could be part of Bitcoin’s decentralised network. Today, Bitcoin’s network contains tens of thousands of nodes, making it virtually impossible to tamper with its blockchain.

While Bitcoin is the most widely used and well-known blockchain, the idea of a decentralised, tamper-proof network has caught the attention of innovators in many industries.

Where could blockchains be used?

So we’ve established that the technology is a secure way of storing information that changes over time. However, where could this be used in the real world?

- **Cryptocurrencies**
- **Intellectual property and patents**
- **Digital voting**
- **Supply chain tracing**
- **Land records**

Walmart and IBM are working on a blockchain to [track Walmart’s supply chain](#) and make contaminated food recalls faster, while Swiss company Agora [are working on making digital voting via blockchain a reality](#). 15-20% of a container’s shipping cost is down to paperwork. By partnering with IBM to create a blockchain network of shippers, freight forwarders, ports, and customs authorities, Mersk estimates going fully digital with this technology could [save \\$38 billion every year](#).

Nevertheless, blockchain is not without its limitations. Several high profile incidents of hackers making off with million-dollar hauls of crypto show that 100% secure is a myth – [\\$292 million was stolen in 2019 alone via just 12 hacks](#). Another major issue facing the technology is just how much energy is needed to keep a blockchain going. Bitcoin, the largest example, is estimated to [consume more energy than the entire country of Switzerland](#). If every blockchain consumes a similar amount, we will need to get the energy from somewhere – and would it even be worth it?

Some have called blockchain ‘a solution in search of a problem’ – for example, a Walmart blockchain. If Walmart controls all of the nodes of the network, is a blockchain really necessary? Is there a better way of making the data secure and transparent without the energy intensive proof-of-work requirements?

It will take some time – and some solutions to these problems – before blockchain ideas make the full leap from the drawing board to the general population, but it looks like the technology is here to stay.