Blockchain under the hood: How does blockchain actually work?

Hashing: a cryptographic fingerprint

A hash is like a digital fingerprint; it is unique to each piece of data on the blockchain. Users put information regarding their transaction (name of receiver and sender along with the amount transferred) into a cryptographic hashing algorithm – a complex mathematical formula – and receive a set of letters and numbers that is distinct to that transaction. The specific input, if unchanged, will always produce the same exact hash. If, however, any part of the data input is changed (for example a malicious actor changes the amount transferred), the hash would change to an entirely different set of characters and make it incompatible with the rest of the chain. Therefore, even without seeing the details of the transaction, nodes can quickly tell that the data within the block has been tampered with and reject that version of the ledger. It is this cryptographic security that makes blockchain ledgers more trustworthy and "almost" immutable.

Examples of hashes

Input	Hash output (using SHA 256 algorithm)
OECD	879D5ACDCDA51A6F1B00EBFE77513D9B19F574499C867997EE1FB6B1FA6DDBB0
OeCD	19C91C8433AC66422E8B13A468B3E96D5D7924BEB1164F8412484900C7C1EDC6

Note: Even subtle changes like upper or lower case significantly alter the hash.

Mining

For some blockchains, in order to add blocks to the ledger, transfers must go through a mining process. Mining is a way of adding transaction records, via blocks, onto a public ledger. Miners are nodes in the network that ensure the transactions in the block are valid. Specifically, they ensure that senders have not already used the funds they want to send to receivers. Once miners finish the verification, they have to ask the network for **consent** to add the new block to the ledger. In order to do so, they have to follow the **consensus mechanisms** chosen for the platform.

Consensus

One of blockchain's key characteristics is the consensus mechanisms it uses to gather consent. Agreement among nodes regarding the "state" of the ledger is essential for the function of the blockchain ledger. The bitcoin blockchain utilises a consensus model called Proof of Work, which requires the miner to compete against other miners to create and broadcast blocks for approval. If successful, they are rewarded in Bitcoin. There are other consensus mechanisms like Proof of Stake, Proof of Authority, Proof of Elapsed Time, and Proof of Burn – all of these are variations on the means for the network to agree on changes to the ledger.

What are digital financial assets?

A digital asset that works as a medium of exchange

The term **tokenisation** describes the process of transferring rights to a real world asset into a digital representation – or token – on the blockchain. Being in possession of that digital token then gives you the right to that asset and the ability to trade and track it digitally.

There are three main types:

Payment tokens Commonly known as a cryptocurrency, a payment token can be a store of value and a unit of measurement, e.g. Bitcoin.

Utility tokens A token that represents a right to a good or service, similar to a gift card, e.g. StorjCoin.

Security tokens A token that provides equity or equity like investment in a company. The holder of the token has rights to the company's future profits, e.g. tZERO.

Why is this important? What can it be used for? One example: Bitcoin

In today's financial system, banks are an essential intermediary for financial transactions and transfers. They verify the identity of the sender, the ability of the sender to make a transfer (i.e. a sufficient account balance) and accuracy of the recipient's address. In this context, the bank acts as the only trusted third party.

However given the bank stores all data on a single centralised ledger, it therefore creates a **single point of failure**, whereby hackers or malicious actors can direct all their efforts for cyberattacks or manipulation to this specific entity. These financial intermediaries also charge **fees** to process transactions. In the case of international remittances, these fees are significant compared to the overall value of the transaction.

It was in this environment that the first blockchain application, a digital currency (cryptocurrency) called **Bitcoin**, was born. It created a peer-to-peer currency that enables users to transfer value to one another without having to go through a bank. Due to Bitcoin's use of cryptographic hashing, mining, and consensus mechanisms, users are able to verify transactions without needing a central authority controlling a single ledger.

Comparing bank transfers and Bitcoin