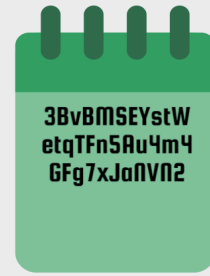
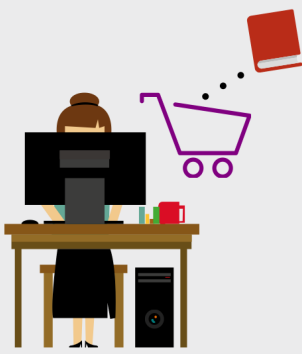


HOW THE BLOCKCHAIN WORKS

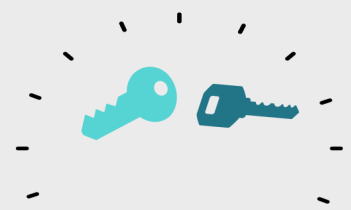
The bitcoin illustration



Anna buys a book online.

Her online book retailer accepts **bitcoin** and Anna already holds a bitcoin wallet.

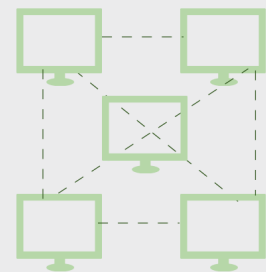
The retailer sends Anna its bitcoin **address** (a chain of 26 to 35 characters).



Anyone can **verify the transaction**, with the public key.

Anna sends her payment to the address of her retailer. She signs the transaction with the private key of her own address, created for this given transaction, and adds her own public key to the transaction.

To ensure **privacy**, addresses are usually different for each transaction. An address is linked to a private key and a public key.



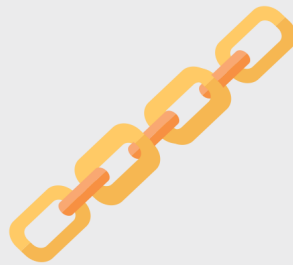
This is where the miners come into play.

Miners are techy blockchain enthusiasts, located all around the world.

Transactions are recorded in **blocks**.

The ledger is a chain of blocks. **Blockchain is the realisation of a public ledger.**

The blockchain, shared in real-time on the miners' computers, stores the record of all confirmed bitcoin transactions.



As a new block is created every 10 minutes, modifying a recorded block would require modifying all the following blocks, which is nearly impossible.

A block contains the **hashes of the previous and current blocks, and a 'nonce'** (a random number). All blocks are linked to one another. It can be viewed as a wax seal.

To store a transaction in the blockchain, miners' computers create **cryptographic hashes** (strings of letters and numbers).

81cd02ab7e569...
e320b6c2fffc8...
5572eca4d4db7d0...
0000000000008a3a41b...



A hash must look a certain way (starting with a number of zeros). **Miners must generate many hashes before finding a successful one.**

The successful miner is **rewarded** in bitcoins.



Anna's transaction is now complete and verified!