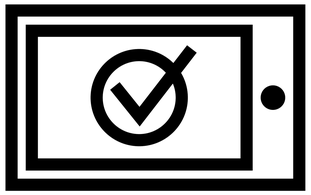
WHAT IS BLOCKCHAIN?

1.

LEDGER

The core of a blockchain is one large ledger that registers all transactions of all partners connected to a network, including the corresponding balances. All connected computers have their own identical copies of the ledger, so that it can only be changed if all partners approve.

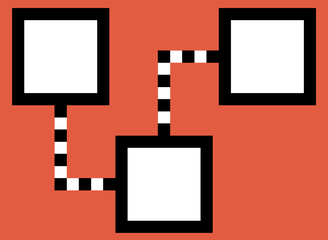
2.



TRANSACTIONS

A party that wants to do a transaction, sends it into the blockchain network. Next, every computer connected checks the ledger to determine whether or not the transaction is possible and legit. Only if a transaction gets approved by all peers, it will be registered in the ledger – which will then be updated on all computers involved.

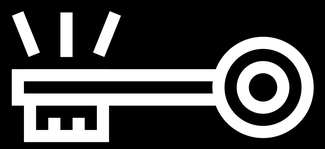
3.



BLOCKS AND CHAINS

A block is a mini set of data that holds multiple transactions – each item at least including the amount, the time, the sender and the receiver and both their balances. If the block gets approved by the network, it will be added to the ledger, a chain of blocks, hence the blockchain.

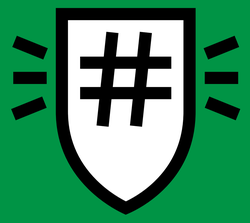
4.



HASHES

A hash is a code that mathematically encrypts the contents of a a block (cryptography). For example, the hash 66a0...45b45 could mean '1.5 bitcoin gets transferred from user X, whose balance after that is A, to user Y, whose balance after that is B. This happens on this date, at this time. This block directly follows the block with hash a2c0...64616.' This way the ledger gets represented in a long series of hashes, enabling the system to compare data very quickly.

5.



SECURITY MECHANISMS

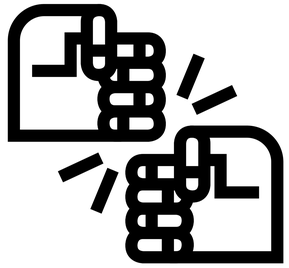
Using hashes makes it impossible to change blocks once registered. For instance, in a paper ledger it's possible to take out page 30 and replace it with a fraudulent version, but in a blockchain it's not. Page 30 now holds an encrypted referral to page 29; and page 31 holds an encrypted referral to number 30. Offering a fraudulent block afterwards will therefore never pass the test of the blockchain algorithm. And because the test is not executed by one central (potentially corrupt) party, but needs the approval of 50% +1 of the computers involved, it is also impossible to cover up any deviations.

6.

SMART CONTRACTS

A basic blockchain 'only' accommodates safer and quicker transactions. Smart contracts open up way more possibilities. Contracts are captured in codes and, when approved by all users, are able to execute themselves on the blockchain. In fact, any 'if...., then....' statement can be programmed and added to your money. For example: 'if it's January 1, if investor X did not go bankrupt and if the balance has increased more than Y since January 1 of last year, transfer 25% of the increase to X'.

7.



MACHINE TO MACHINE

As the execution of contracts, the handling of transactions and the checks on authenticity get fully automated, not only humans and businesses but also machines can actively join the blockchain network. A charged electric vehicle will now take care of the payment itself and it will warn its owner when its balance drops.

BlockLab

BLOCKLAB.NL