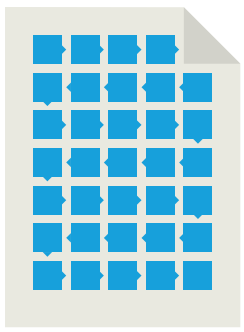
Blockchain Infographic

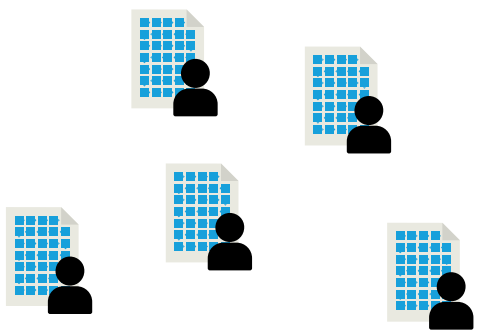
The key aspects of Blockchain technology, briefly summarised in one infographic.

Principles

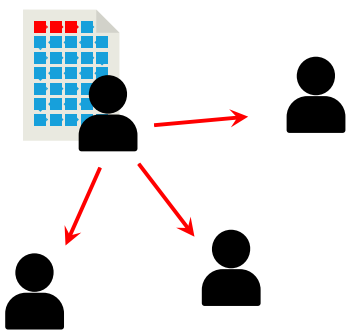


The Blockchain is a huge file containing a sequence of ‘blocks’ of data.

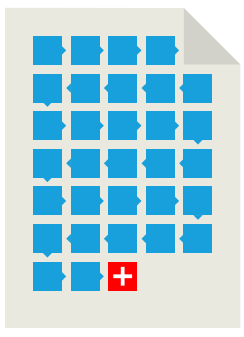
Each block of data additionally contains a fingerprint of the previous block, thus forming a “chain”.



No central storage – every participant has a local copy.



Changes are broadcast to all other participants.



Only allowed operation: append data.

Data blocks are cryptographically signed by their respective creators for authenticity.

clusil/
INFORMATION / SECURITY / LUXEMBOURG

Consensus algorithms

Due to the distributed nature of the Blockchain, different users may have a different (e.g. outdated) copy of the Blockchain. The consensus algorithm determines which of these shall be retained or discarded. Many different such algorithms exist among the available Blockchain applications.

Consensus based on challenge

The first participant who wins a particular challenge gets the privilege to append a block to the Blockchain.

Proof of work: A computationally hard task needs to be solved. The long computation time prevents malicious users from forging many invalid blocks.

Proof of capacity: A task needs to be solved that requires huge disk space. The principle is the same than for the proof of work, except that it requires storage rather than computation power.

Consensus based on stake

The privilege to append a block to the Blockchain is determined based on the stake of the participants.

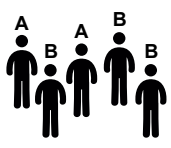
Proof of stake: A randomly chosen (but predictable) participant is chosen for appending the next block. Chances to be selected are higher if the participant owns more coins. The algorithm suffers from the 'nothing at stake' problem: participants have nothing to lose when they behave malicious.

Proof of burn: Participants needs to burn (destroy) coins to be eligible for appending the next block. Among all such participants, one is selected randomly (but in a predictable fashion).

Consensus decided by a trusted third party

A third party decides who obtains the privilege to append a block to the Blockchain.

Proof of elapsed time: A device issued by a trusted third party waits for a random time. The first participant who finished waiting can append the next block.



Consensus by voting

A newly appended block is accepted only if the majority of participants consider it legitimate.

Byzantine Fault Tolerance (BFT) algorithms: One participant is elected as leader and proposes a new block. That block is sent to all other participants, who append it to the Blockchain. They then send a fingerprint of the thus obtained (local) Blockchain to all other participants. The final version of the Blockchain is the one that has been obtained by the majority of the participants.

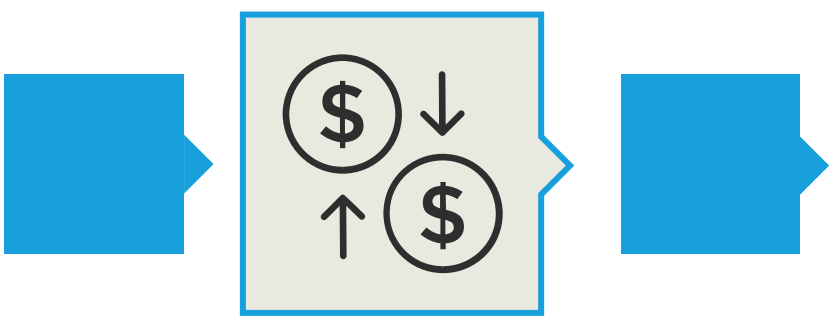
Hybrid approaches

The consensus algorithm is a mix of some of the algorithms above.

Proof of activity: First a computationally hard problem needs to be solved (as for proof-of-work strategies). The participant who may append the next block is then derived from the solution of the latter problem. This approach aims at preventing the 51% attack.

Proof of checkpoint: Proceeds like proof of stake, but periodically a 'checkpoint' needs to be obtained via a proof of work. This is to mitigate the 'nothing at stake' issue leading to coins be double-spent in a proof-of-stake setting.

Applications



Digital assets

Each block encodes a transaction of assets from one participant to another.

Examples: cryptocurrency, stock exchange

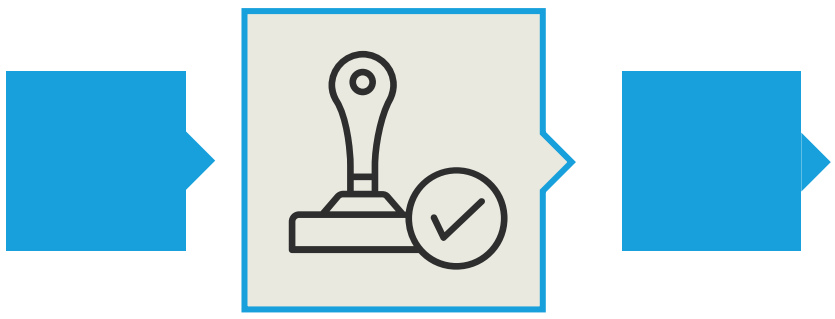
Smart contracts

Each block encodes a contract set up by one participant, or a commitment (signature) thereof by another participant.

Identity

Each block encodes the identity of a person, or an action that s/he has provably committed.

Examples: e-identity, e-voting

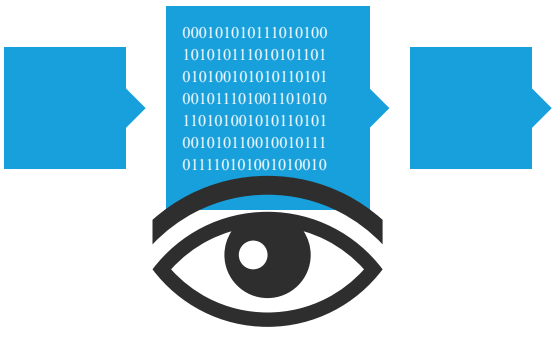


Storage

Each block encodes information the integrity of which is guaranteed to other participants.

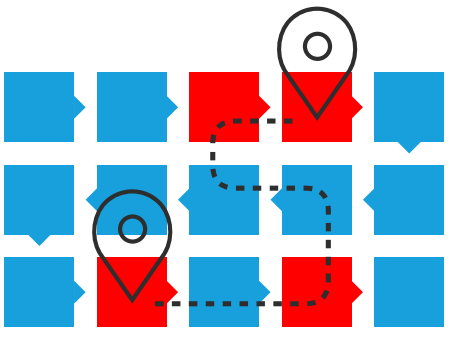
Examples: proof of authorship, ownership, originality (patents, notary)

Security aspects



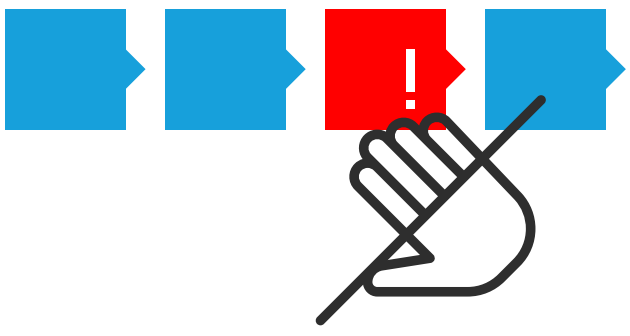
Confidentiality

Everything stored in the Blockchain is public and can be seen by everyone.



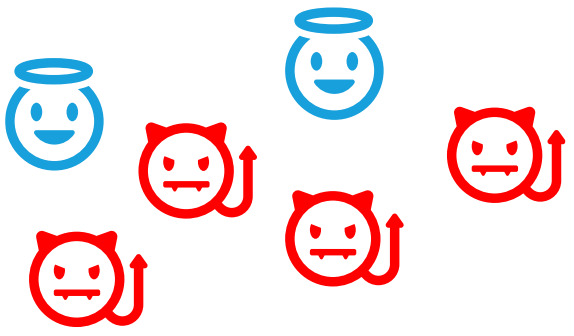
Privacy

People can be tracked, transactions can be traced back.



Persistence

Errors mistakenly introduced into the Blockchain cannot be undone.



Control

A large portion of dishonest participants can compromise the integrity of the Blockchain.

Governance

Developers control the consensus algorithm used by the Blockchain app, and can thus cause (hard) forks.