MANGEAT

Blockchain simply explained

Written by Fabien Aepli & Nurith Cohen, 27 April 2017

Blockchain is one of the symbols of the digitalisation era we live in. Blockchain, as other new technologies, is viewed as disruptive for existing business models and will likely impact our society in various manners.

This article aims at providing the reader with a simple and synthetic understanding of the concept of blockchain (intentionally, without getting into details of the underlying technological issues). *If you still have not grasped what blockchain is, here is your chance*.

What is a blockchain?

Blockchain is a secured and reliable technology, operating on a peer-to-peer basis (i.e. with connected computer systems), which is used to confidently stock and share data or list transactions. It enables to perform transactions in a relatively fast and cost-effective manner.

It is a **distributed**, **transparent** (but pseudo-anonymous) **cryptographic ledger**, deemed unforgeable, that keeps records of all transactions, **without involvement of a central intermediary**, each transaction being verified by the network participants.

When verified, the transaction is added to a ***block*** of other verified transactions. The block is then immutably added to the distributed ledger in a **linear and chronological order**. This is where the term "***chain***" comes from. The chain may be public (e.g. bitcoin blockchain) or private (i.e. access limited to members of a private network).

Said transactions may concern cryptocurrencies (e.g. bitcoin) or any other kind of digital assets or digital representations of a physical asset, so-called "***tokens***".

While traditional ledgers are centralised, meaning that the ledger holder (the central intermediary) controls the system and mediates every transaction, with the blockchain technology, **each network participant holds a copy of the ledger and participates to the approval of the transactions**. Consequently, while corrupting a "traditional" ledger implies getting to the central ledger holder (the centralised intermediary), corrupting a blockchain would imply attacking all copies of the ledger simultaneously because of the distributed nature of the ledger. The biggest "added" value of the blockchain technology may well refer to *trust*. Rather than helping you building trust, *blockchain technology makes trust irrelevant*.

How does a blockchain basically work?

New transactions (*e.g. A would like to send ten bitcoins to B*) are grouped within blocks. Each block is **verified and validated** by the "***nodes***" (network participants) or so-called "***miners***" using complex cryptotechnics which will depend on the type of blockchain (in our bitcoin transaction example: the miners will verify that A is indeed owner of ten bitcoins and once this is confirmed, the transaction is validated and visible for B and the other network participants; B thus becomes the owner of said ten bitcoins). Blockchain security methods use encryption technology.

Network participants are incentivised to perform the verification and approval tasks, mostly by receiving fees or new cryptocurrencies. If a discrepancy is found, the block is rejected. Otherwise validated transactions (in the block) are time-stamped and added to the chain, in a linear and chronological order, making a chain of transactions (or a chain of blocks) that shows every and all transactions in the history of that blockchain.

What are possible uses of a blockchain?

Originally, the blockchain technology has been used for cryptocurrency transactions. The potential of the blockchain technology goes, however, far beyond cryptocurrencies. This technology may basically be used for any types of transaction involving value (money, goods, real estate, etc.) or for unforgeable databases or registers. Blockchain technology may be applied to any transaction or operation where traceability and visibility is required (e.g. casting votes in election, proving that a document existed at a certain time or that a person is the legitimate owner of an asset, proving origin of a product within a supply chain, etc.).

It may also be used for contracts that will be automatically executed, without human intervention (so-called "*smart contracts*"). Not fully clear what that is? Follow us on our Linkedin Page and **stay tuned for the next episode: *Smart Contracts simply explained***.