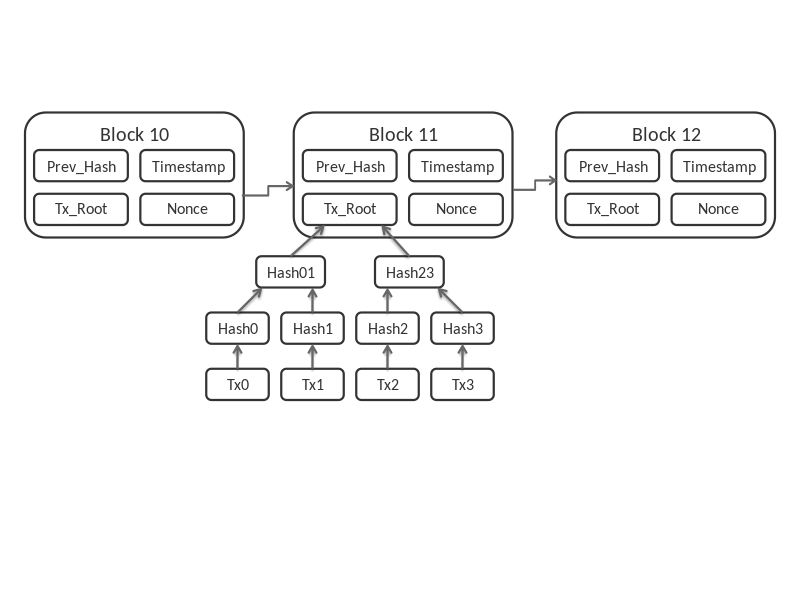
**Blockchain Introduction and development**

According to Wikipedia the clearest definition of Blockchain is a growing list of [records](https://en.wikipedia.org/wiki/Record_(computer_science)), called *blocks*, that are linked together using [cryptography](https://en.wikipedia.org/wiki/Cryptography). Each block contains a [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash_function) of the previous block, a [timestamp](https://en.wikipedia.org/wiki/Trusted_timestamping), and transaction data (generally represented as a [Merkle tree](https://en.wikipedia.org/wiki/Merkle_tree)). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks[[1]](#endnote-852).Blockchains are typically managed by a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network for use as a publicly [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) The Bitcoin blockchain protocol introduced a mechanism of making it expensive to copy digital values. A copy of the ledger is stored on multiple devices of a cryptographically secured P2P network. The ledger is a le, also called blockchain. It maintains a continuously growing list of transaction data records, chained in blocks that are cryptographically secured from tampering and revision. In order to change the contents of that ledger, network users need to reach a **mutual agreement**, also referred to as consensus. Blockchain can, therefore, be described as a shared, trusted, public ledger of transactions, that everyone can inspect, but which no single user controls. The ledger is built as a linked list – or chain of blocks – where each block contains a certain number of transactions that were validated by the network in a given timespan.[[2]](#endnote-27588)

A cryptographically secured chain of blocks is described for the first time by Stuart Haber and W Scott Stornetta in **1991**, in **1998** a computer scientist Nick Szabo works on ‘bit gold’, a decentralized digital currency and in **2000** Stefan Konst publishes his theory of cryptographic secured chains, plus ideas for implementation, later on in 2008 Developer(s) working under the pseudonym Satoshi Nakamoto release a white paper establishing the model for a blockchain.

The first blockchain as the public ledger for transactions made using bitcoin was implemented in 2009 by Nakamoto.

Blockchain technology is separated from the currency and its potential for other financial, interorganisational transactions is explored. Blockchain 2.0 is born, referring to applications beyond currency.

The Ethereum blockchain system introduces computer programs into the blocks, representing financial instruments such as bonds. These become known as smart contracts.

1. https://en.wikipedia.org/wiki/Blockchain [↑](#endnote-ref-852)
2. https://blockchainhub.net/blockchain-intro/ [↑](#endnote-ref-27588)