## What is the fuss about?

A discussion about blockchain is hard to avoid during 2020 and for good reason.

When Bitcoin rose from $5000 to $20000 in a matter of months, it gained massive coverage, thanks to the outlandish financial gains it bestowed upon its holders. And Bitcoin (cryptocurrencies[[1]](#footnote-0) in general) would not be possible without Distributed Ledgers and underlying technology. Let’s examine piece by piece.

## Ledger

| *A ledger[[2]](#footnote-1) is the principal book or computer file for recording and totaling economic transactions measured in terms of a monetary unit of account by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.* |
| --- |

Ledgers in general have been invented as soon as commerce was a reality. They were used to record an array of things, like money, property, crop. Their primitive form was that of clay tablets and papyrus, while the modern-day form is that of a vast database.

In their primitive form, the safe-keeping of ledgers was delegated to institutions of authority, such as temples and the palace. This was later replaced by the invention of double-entry book-keeping, which gave birth to the banking sector of today.

Let’s assume a paradigm for ledgers.

### The Village Paradigm

Suppose we are living in Paradigm Village, a small community of roughly 10 people. Everyone participates in the economy and has similar responsibilities. Alice is a farmer. Bob is a fisherman. Others are builders, cooks, and several other first-line professions. There is no currency in Paradigm Village and everything is accomplished through service and goods exchange.

Then one day, Alice would trade fruit for fish as per usual but realized her crop was not ripe to harvest, so she suggested completing the trade and keeping a record of that. Bob agrees and Alice will repay the favor when the fruit is ripe. As days pass, they have amassed a lot of favors, which is hard to track. And that is without adding the whole of the village to the paradigm.

So, Alice and Bob agree to appoint Cedric as the keeper of a village ledger. Cedric keeps track of favors and repayments and writes all records down on a paper that only he can access. The issues start appearing when Cedric realizes he has power in his hands, compared to other villagers.

Cedric is partial to people and bribes, which he accommodates by adding or erasing records from the ledger and that will go unnoticed, until one day the villagers congregate to discuss the faults in this system. They move for a Distributed Ledger, giving everyone access to the same pen and paper. The ledger is kept in the village center for all to record favors and repayments. Community votes settle any disputes that occur. The new system is transparent and less prone to corruption and Cedric is out of the picture.

| [[3]](#footnote-2) Alice and Bob are about to revoke trust from Cedric and move to a Distributed Ledger. |
| --- |

Distributed Ledgers of today, are an attempt to solve an ancient problem with a modern approach. They must be more complex and more powerful than a pen and paper ledger, to be scalable for a population of 10 or 10 million.

## Distributed Ledger

In essence, Distributed Ledgers are databases existing and shared across a network of multiple points (nodes). They are shared, replicated, and synchronized among the members of this network. However, Distributed Ledgers are a subset of the set of shared ledgers.

All members of the network have their copy of the ledger and any changes are applied and reflected in all copies within minutes or less. However, there is security in place to govern who and how can modify records through cryptography and signatures.

#### Distributed Ledgers can further be divided as

* Permissionless - nodes require permission to make changes
* Permissioned - nodes do require need permission
* Public - access to ledger is public to participating nodes
* Private - access to ledger is reserved to certain nodes

| [[4]](#footnote-3) [[5]](#footnote-4)A peer-to-peer network example and a Centralized VS Decentralized Network Visualization |
| --- |

## Distributed Ledger Technology - a big deal?

| *[...] Distributed Ledger Technology (or DLT) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.* |
| --- |

Some disambiguation comes first. Blockchain technology has been used as a synonym of Distributed Ledger Technology (also found as DLT) although they are not identical concepts.

A blockchain uses several technological layers, including Distributed Ledger Technology, to enable applications.

| [[6]](#footnote-5)Blockchain is a subset of Distributed Ledger Technology,  not all Distributed Ledger Technologies are blockchain |
| --- |

#### Distributed Ledger Technologies can

* Fasten transactions by removing a central authority
* Reduce transaction cost, for the same reason
* Enhance information CIA (Confidentiality, Integrity, and Availability) triad, a well-known security model. Several network nodes hold a record copy, thus manipulation and/or attack is more difficult
* Offer transparent record handling via sharing of information across network nodes

One of the first areas of application was financial transactions. Bitcoin gained worldwide fame and usage while proving that Distributed Ledger Technologies can work. Banks and financial institutions started innovating, giving birth to the term ‘Fintech’.

#### Other Areas where Distributed Ledger Technologies have or will be applied include:

* Management/sharing of public and personal information
  + Personal medical records
  + Art and commodities ownership for
  + Deed transfers
  + Tracking intellectual property for music, film, and more.
* Government and Business processes
  + Business supply chains
  + Tax collection
  + Benefits distribution
  + Handling of legal documents
  + Voting procedures

## Blockchain

| *Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority. At its most basic level, they enable a community of users to record transactions in a ledger public to that community such that no transaction can be changed once published [[7]](#footnote-6)* |
| --- |

Blockchains are a small subset of the Distributed Ledger Technology sector. They store and transmit data in packages called blocks that are connected in a chain. They employ cryptography to sync data across nodes, in an secure and immutable manner.

### 

| [[8]](#footnote-7)Blocks in a blockchain |
| --- |

#### Blocks on the blockchain consist of the following:

1. Block name and identifier
2. Numerical index to signify its place in the chain
3. A timestamp
4. The main set of data like Information about transactions, participants, etc
5. Hash. Hashes are cryptographic codes
6. The previous hash for verification purposes

### How blockchain Works

A transaction on the blockchain will generally work as follows. First, someone will ask to transact. Then the transaction request will be broadcasted to the network of nodes that will validate it once it is completed. Then, a block is added to the chain and is made publicly available to view.

| [[9]](#footnote-8)A transaction in a blockchain |
| --- |

#### Blockchain benefits

Organizing and storing information in a blockchain encompasses certain benefits, such as:

* Security
  + Records are encrypted individually and spread throughout the network
  + Resilience of data
* Immutability
  + Copies of a blockchain are kept across a peer-to-peer network, alteration requires tremendous resources thus almost impossible.
* Transparency and Verifiability
  + Through unanimous validation of records
  + Timestamped transactions
* Anonymity
  + Network nodes are both identifiable yet anonymous

| [[10]](#footnote-9) Blockchain benefits visualization |
| --- |

| [[11]](#footnote-10) Distributed Layer Technology in a blockchain, used for supply chain management |
| --- |

##### 

| [[12]](#footnote-11)Distributed Layer Technology in a blockchain, used for smart contracts |
| --- |

#### 

#### Key Takeaways

* A ledger is the principal book or computer file for recording and totaling transactions
* A Distributed Ledger is a ledger of transactions maintained in a distributed form across locations and people.
* Distributed Ledger Technology is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.
* Blockchain is a type of data structure that stores and transmits data in packages called blocks that are connected in a chain.
* Distributed Ledger Technology is a layer of blockchain.

## 

## Conclusion and the future

Distributed Ledgers are disruptive. They can process information in real-time, safeguard it and keep it tamper-proof while scaling to any size. The industries that can see wide-spread Distributed Ledger Technologies’ adaption are finance, real estate, health care, and identity management. They can facilitate smart contracts and the Internet of Things while they massively innovate fields such as democratic elections thanks to the concepts of distributed consensus, open-source, and transparency that they encompass.

As with any real revolution in a field, the threat comes with the intermediaries in a position of control in the current hierarchy and any such field. For example, the banks and government agencies aren’t yet ready for the next step. And while some may be innovated, some others might be made redundant so they are sure to protest that change of status-quo.

1. *A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership.* Andy Greenberg (20 April 2011). ["Crypto Currency"](https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html). *Forbes*. [Archived](https://web.archive.org/web/20140831001109/http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html) from the original on 31 August 2014. Retrieved 8 August 2014. <https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-crypto_currency-1> [↑](#footnote-ref-0)
2. Definition by <https://en.wikipedia.org/wiki/Ledger#cite_note-1> [↑](#footnote-ref-1)
3. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-2)
4. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-3)
5. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-4)
6. Taken from [https://miro.medium.com/](https://miro.medium.com/max/700/1*JAyPfYJznuoi6vDwncBTOA.png) [↑](#footnote-ref-5)
7. NIST blockchain Technology Overview Draft NISTIR8202, January 23, 2018 <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> [↑](#footnote-ref-6)
8. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-7)
9. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-8)
10. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-9)
11. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-10)
12. Taken from <https://blockgeeks.com/blockchain-infographics/> [↑](#footnote-ref-11)