



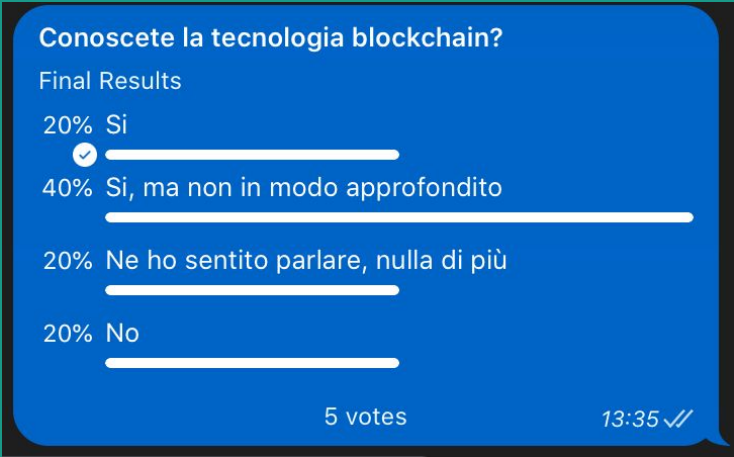
Do you trust it? No, I don't.


Part II



Your votes matter!

- Poll about the knowledge of **blockchain** technology: <https://t.me/c/1351105384/1408>





Today we talk about blockchain





But first...





Let's reverse the entropy to go back a week



Source: [giphy.com](https://www.giphy.com)



What we talked about

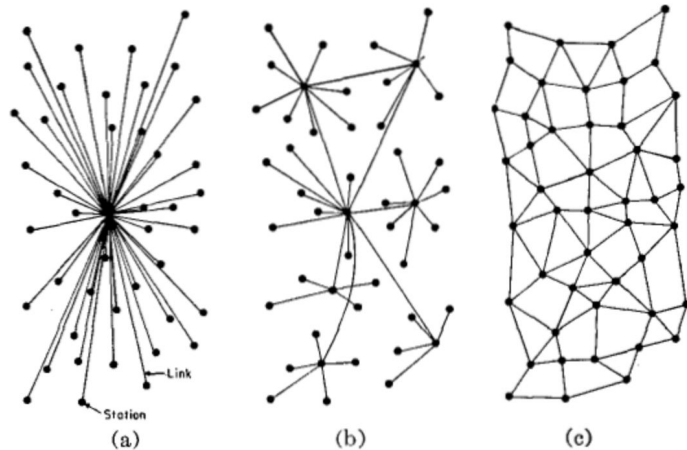


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

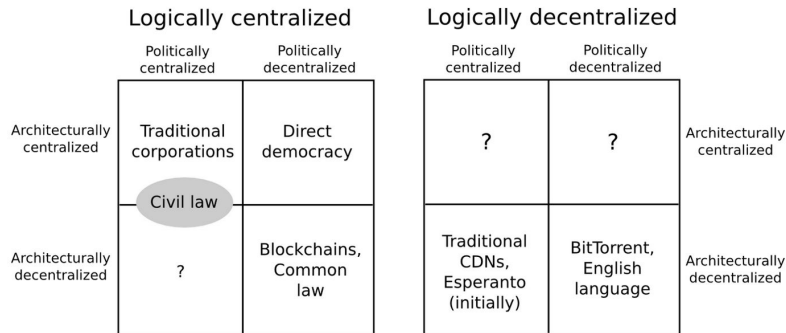
We got the difference between **centralization** and **decentralization** and the meaning of **distribution**.

[Source from which I took the screenshot](#)

[Original paper](#)



What we talked about



We got also the three main properties to classify centralized/decentralized systems:

- Architectural (de)centralization
- Political (de)centralization
- Logical (de)centralization

Source: [Buterin's article](#)



What we talked about

- We understood the power of the decentralization by focusing on the great strengths:
 - Fault tolerance
 - Attack resistance
 - Collusion resistance
- We got a better idea about decentralization strengths by doing some examples:
 - Immuni
 - League of Legends
- Today we're going to focus on another example: **blockchain**



What is a blockchain?

*“A blockchain is a technology that allows to **record** and **organize** information in **transactions** in **blocks**.*

*Each block is **linked** to the previous one via cryptography, thus forming the **block chain**.*

*The inclusion of a transaction in a block is allowed by a predefined **consensus mechanism** among the participants of the blockchain.*

*The ledger is **shared** among all blockchain participants.”*

Source: *Da Zero alla Luna*



Transactions and block



Transaction

*A transaction represents the registration of an **event** between one or more actors.*

If we talk about Bitcoin, a transaction contains the amount that was transferred between two people.



Block

A **block** is a file that contains transactions data.

If we talk about Bitcoin, a block contains:

- Transactions data
- Link to the previous block
- Timestamp



Chain



Chain

We got what is a block. But how the chain is made up?

*The chain is made up by **linking** each single block to the previous one via **cryptography**.*

Why do the blocks have to be linked?

The linking process allows you to have a ledger that is **impossible for anyone to edit**. I would change a transaction inside an old block, I have to change that block but also all the following blocks. Remember: each block contains the **hash** of the previous block.

In short words, I have to change the chain!



Consensus algorithm



Consensus algorithm

Why does a blockchain need a **consensus algorithm**? We already have the chain!

Keep in mind this concept: when we talk about blockchain, we don't just talk about the linking process of the blocks, but we mean also the **decentralized (and distributed) network** on which the blockchain is based.

In other words, the decentralized network needs a **communication protocol** to work correctly.



Consensus algorithm

Periodically, the nodes of the network accept transactions. Each transaction is insert in a block. When the “timer” has expired, the nodes **close** the block and any transaction will be insert in this block.

The network proposes a **challenge (Proof of Work, PoW)**: the **miners** have to find an hash with n zeros at the beginning of the hash string. The first miner that wins the challenge, wins a **reward**.

Challenge: find an hash string with n zero at the beginning.

Reward: a method to incentivize network participants to “play fair”.



Consensus algorithm

Nowadays, the consensus algorithms that are used are:

- *Proof of Work*
- *Proof of Stake*
- *Proof of Existence*

The most used is PoW.



Ledger



Ledger

As we said in the last speech, a blockchain keeps an **immutable ledger**.

We can say that a blockchain is **DLT (Distributed Ledger Technology)**.

In other words a blockchain is database, but not vice versa.



Ledger

- A blockchain is a database
- A DLT is a database
- A blockchain is a DLT

But

- A DLT is not necessary a blockchain
- A database is not necessary a blockchain
- A database is not necessary a DLT

Database >> DLT >> Blockchain (consider these concepts as sets)



Ledger

Every nodes of the network must contain the same content. Every nodes must **agree**.

The winner miner sends the result to the network: the network nodes **check** that the hash found is correct.



What is the purpose of the consensus algorithm?



What is the purpose of the consensus algorithm?

Before answering this question, let's talk about the history of blockchain.



History of the blockchain

Blockchain was born with Bitcoin.

At the end of 2008, **Satoshi Nakamoto** (we still don't know who is) published a *white paper*: in this document Satoshi presents [Bitcoin](#).

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



History of the blockchain

In this paper, Satoshi didn't write *blockchain*, but he talks about a **peer-to-peer electronic cash system**. He wanted to create a new way to exchange cash.

But what is the purpose?

Throughout the history of humanity, we trusted on a **third-party**.

The financial crisis in 2008 is a demonstration of the *trusted-third-party* problem.



History of the blockchain

The purpose of Satoshi was to build a *peer-to-peer* system: he wanted to erase the trusted-third-party.

The users can exchange cash **without** the need of banks (trusted-third-parties). In this way, Bitcoin deprives the banks of authority.



History of the blockchain

But without a trusted-third-party, how can we sure that a person is not cheating? This is the [Byzantine generals problem!](#)

Satoshi has solved this problem with the PoW!



History of the blockchain

- A block to validate is ready
- Miners are ready to mine the hash (they try to win the *challenge*)
- If any miner sends an incorrect hash string to the network, the network notices it and rejects the hash string
- The hash string is validate by every nodes (or many of them)

This is the purpose of the *consensus algorithm*.



What is the purpose of the consensus algorithm?

Thanks to *consensus algorithm*, the **double-spending problem** in Bitcoin is solved!

There is an attack that it could be possible: **51% attack** (never happened in Bitcoin).



**So, don't distribute the
knowledge,
but decentralize it to the
world.
It's safer.**





Bibliography

- Vitalik Buterin, [The Meaning of Decentralization](#), Medium, 2020.
- Paul Baran, [On distributed communications networks](#), 2020. The paper was written in September 1962.
- Gian Luca Comandini, *Da Zero alla Luna*, 2020.
- [Byzantine generals problem](#), Wikipedia, 2020.
- [First gif](#), 2020.
- [Second gif](#), 2020.

I suggest to read also *Mastering Bitcoin* by Andreas M. Antonopoulos.



The end.

Maybe this is the end... or it could just be the beginning.



Source: [giphy.com](https://www.giphy.com)