

Most solutions today do not effectively guarantee that the information stored on them is not ever going to be modified or deleted. Blockchain is here to change this reality.

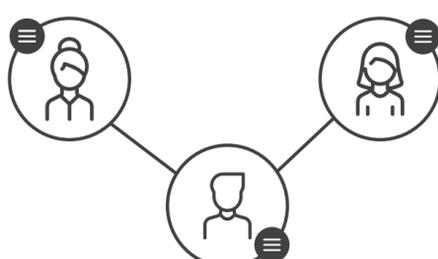


WHAT IS BLOCKCHAIN?

The Blockchain is a structure composed of a series of blocks, where each block carries information about transactions, and the identification address of its previous block. This list of transactions composes a distributed ledger. The Blockchain enables us to describe contracts or implement applications that will forever be stored in the network, where modifications are not allowed. It can securely record any exchange between two parties, disregarding the need for an intermediary and guaranteeing trust and integrity.

HOW ARE THE TRANSACTIONS MADE?

Transactions in the blockchain are commonly made by following the rules described in smart contracts, which are pieces of code deployed in the network, becoming distributed applications. Transactions referencing contracts are exposed to the business rules in it described and will only be concluded once every condition is fulfilled. After the transaction is completed, it is included into a block, which will further be permanently stored in the network.



WHY IS IT SAFE?

Cryptographic algorithms enable most of the underlying structure of a blockchain. The three main aspects where we see that are:



**PUBLIC/
PRIVATE KEY**

Each user in the blockchain is identified by two encrypted addresses: a private and a public key. A private key is used to sign transactions in a way that even one alteration to the content will completely change the signature. It is used together with a public key, which allows a party to verify that a signature was produced by another without the need to know their private key.



HASHING

Because it can be replicated, a blockchain needs a method to verify that it was not altered, guaranteeing the integrity of every block on the chain. This is done through hashing, something like a block signature. The hash is generated based on a block's content and it is included at the beginning of the next block. This means that every block's hash includes immutable information about the previous block, making it impossible to change any entry to the chain.



CONSENSUS MECHANISM

Blockchains have the inherent capacity of being distributed, so that any interested party can have its own copy to store and verify. To ensure that each copy, or node, can confirm new blocks, a consensus mechanism is needed. This mechanism, which can prevent foul play with prohibitive computational costs or based on the compromise between parties and the chain, determines the properties of the block hashing and whether a block can be recognised as part of the chain.

AVAILABLE FRAMEWORKS



Hyperledger is an open source collaborative effort initially created by the Linux Foundation to advance cross-industry blockchain technologies. Today, it is maintained by big industry parties such as J.P. Morgan, American Express, Intel and IBM.



Ethereum is an open-source blockchain platform maintained by the developer's community and guided by the Ethereum foundation. It is a distributed platform that can run smart contracts and decentralized applications using blockchain technology.



Corda is an open source blockchain project created and maintained by R3. This framework enables the creation of interoperable blockchain networks that transact with each other in strict privacy.

WHAT DO WE HAVE TODAY?

Anything that can be modeled as a transaction between two parties can be enforced by a blockchain. That goes from the classic example of exchanging currency to more advanced cases such as a government confirming identities, two people signing an apartment lease, or a website storing users' pictures. Whole distributed applications can be implemented and executed over the blockchain.

IDENTITY



uPort is an open identity system that allows users to register their own identity on Ethereum, send and request credentials, sign transactions, and securely manage keys & data.

HEALTH



MedicalChain applies blockchain technology to facilitate the storage and utilization of patient electronic records for doctors in the UK.

SUPPLY CHAIN



Everledger uses blockchain to store the data of a combination of the latest forensic approaches to give physical assets an identity, enabling items to have proof of authenticity, existence, as well as ownership. This provides confidence in the information captured and tracked through the asset's lifetime journey.

SUPPLY CHAIN



IBM Food Trust, which was built using Hyperledger, is a track-and-trace solution for food and groceries. It uses the collaborative work of growers, processors, wholesalers, distributors, manufacturers, retailers, and others, to enhance visibility and accountability across the food supply chain.

SUPPLY CHAIN



Provenance uses blockchain to provide chain-of-custody and certification of supply chains for consumer products.

ENTERTAINMENT



Spotify is working to leverage blockchain to help solve problems with artists' copyright attribution and rewarding.

FINANCE



Smart Valor facilitates the access to alternative investment opportunities and global wealth using asset tokenization and blockchain technologies.

FINANCE



Ripple is a solution that connects banks and payment providers via RippleNet to provide one frictionless experience for sending and receiving money globally.

BLOCKCHAIN AT POATEK

Here at Poatek we have dived into the Ethereum platform. Our Blockchain team has done in-depth research of the solution, understanding transactions exchanges, coding and deployment of contracts, and nodes networking. We have built our own private network and created our local cryptocurrency in order to validate our studies.