
YouCode
POWERED BY SIMPLON
Blockchain
An Overview
Public vs
Private Keys
About me
How does it work?
BLOCKCHAIN
Hash Function
Consensus
Mechanism
Public
Private
Types
Use Cases
Blockchain Technology
101

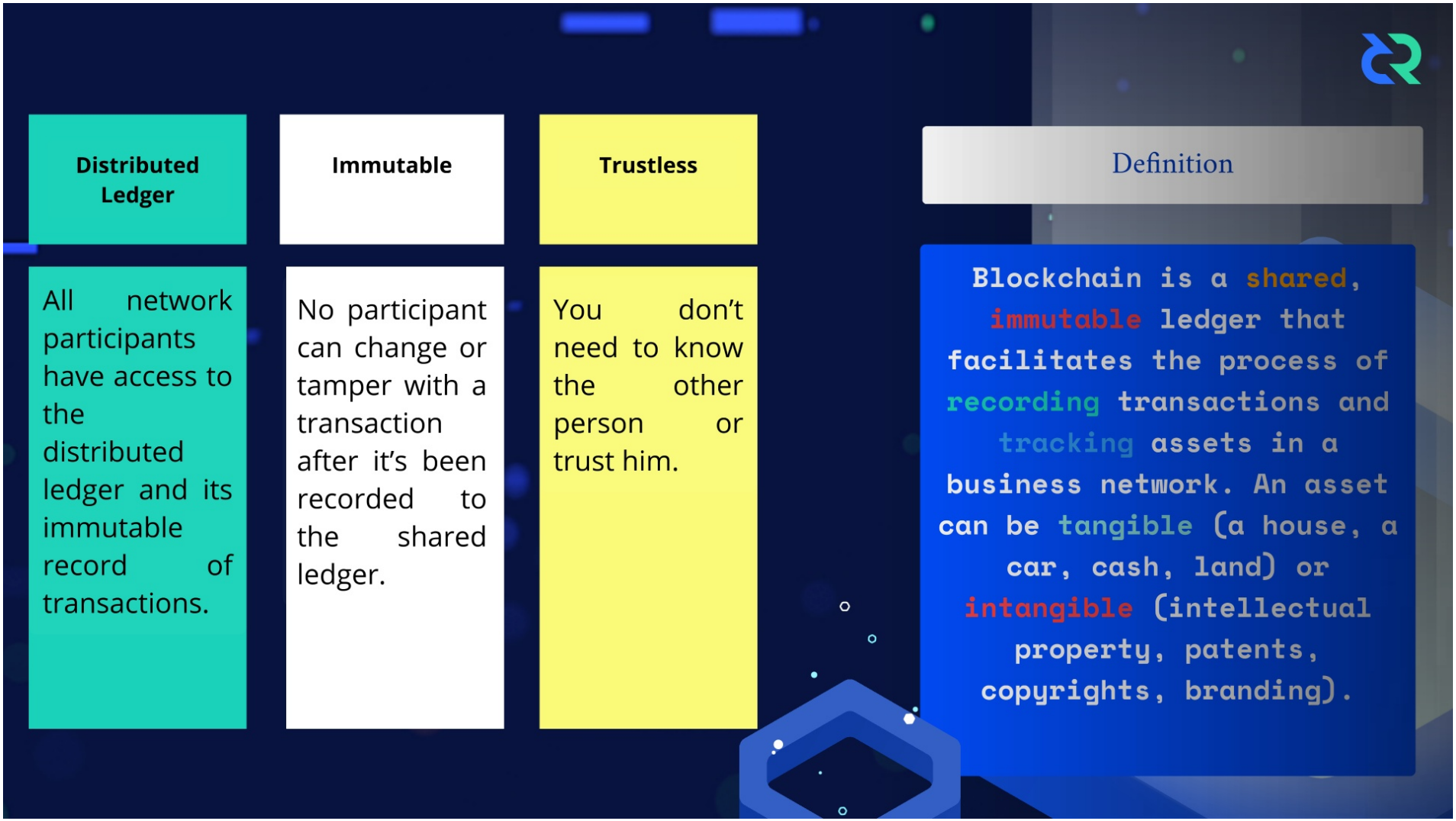
Insaf NORI

Decred Group

Community Manager

MENA

PhD Student at ENSA

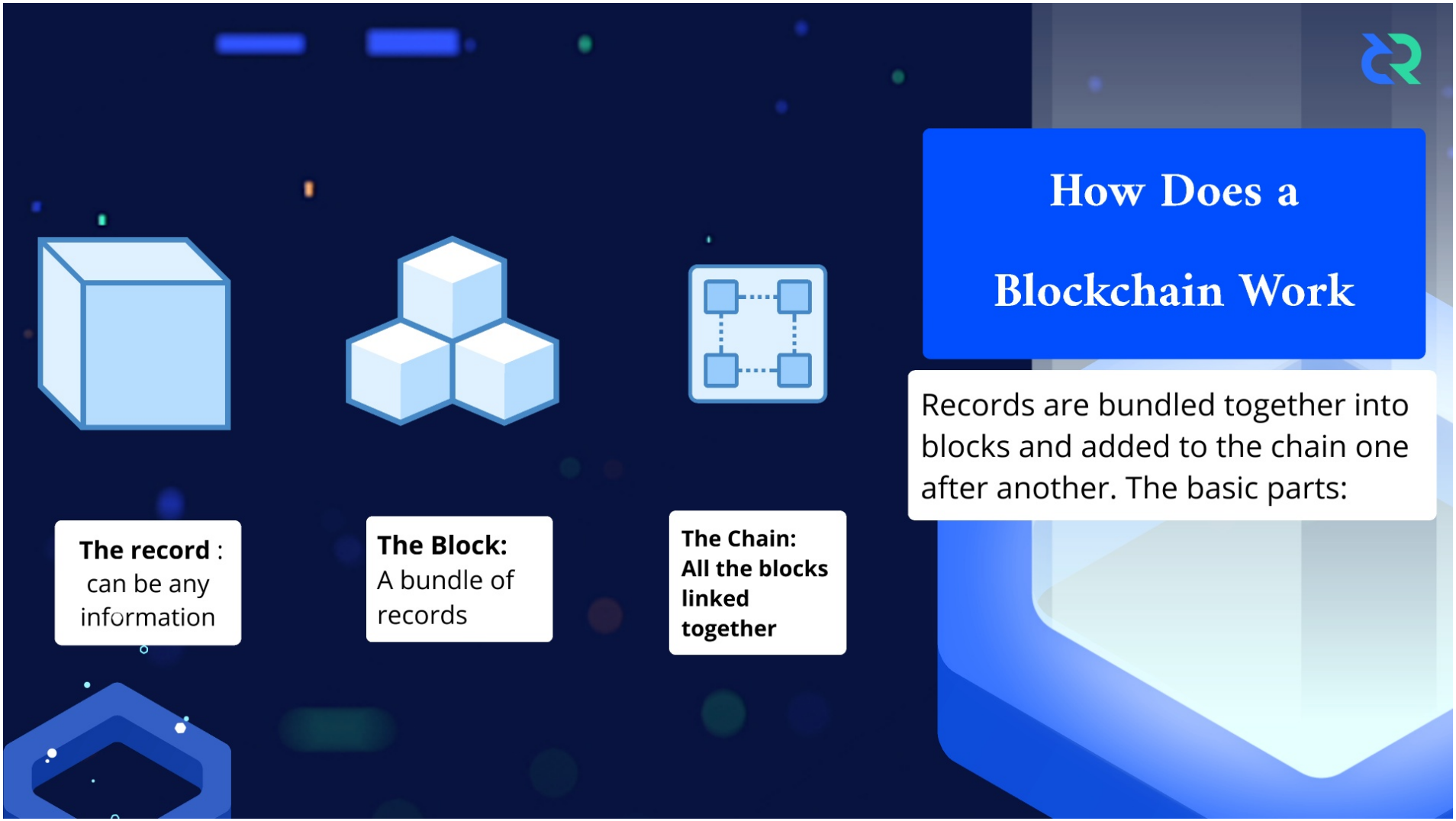

Distributed Ledger
Immutable
Trustless
Definition
All network participants have access to the distributed ledger and its immutable record of transactions.
No participant can change or tamper with a transaction after it's been recorded to the shared ledger.
You don't need to know the other person or trust him.
Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

History of Blockchain Technology

The history of Blockchain starts before 2008 white paper by Satoshi Nakamoto.

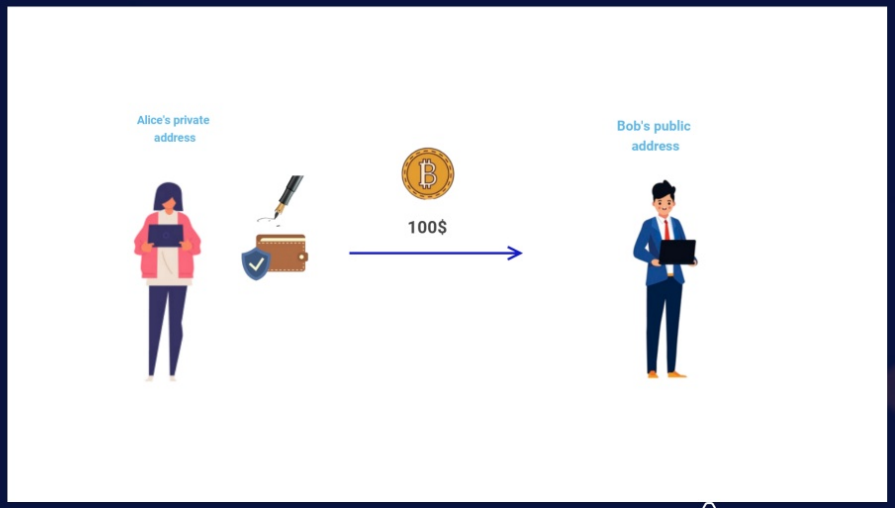
https://prezi.com/i/view/0PZt4EDlzuox15eo7DwP

How does a Blockchain Work


How Does a
Blockchain Work
Records are bundled together into blocks and added to the chain one after another. The basic parts:
The record : can be any information
The Block: A bundle of records
The Chain: All the blocks linked together

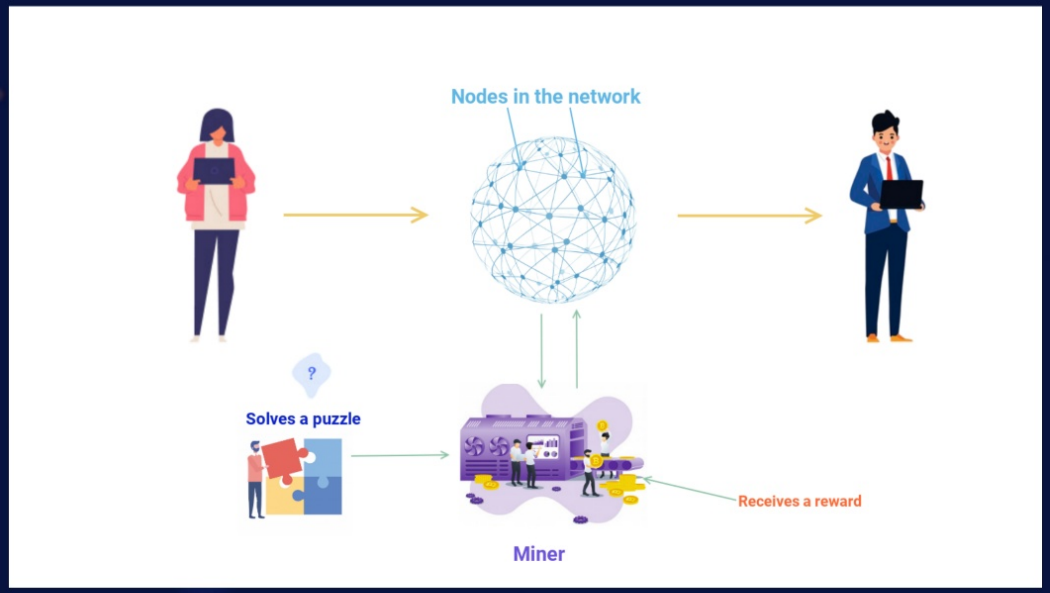
Here's how a deal gets included in a Blockchain:

Step One



A trade is recorded. For example, let's say Alice is sending to Bob $100 in crypto. The record lists the details, including a digital signature from each party.

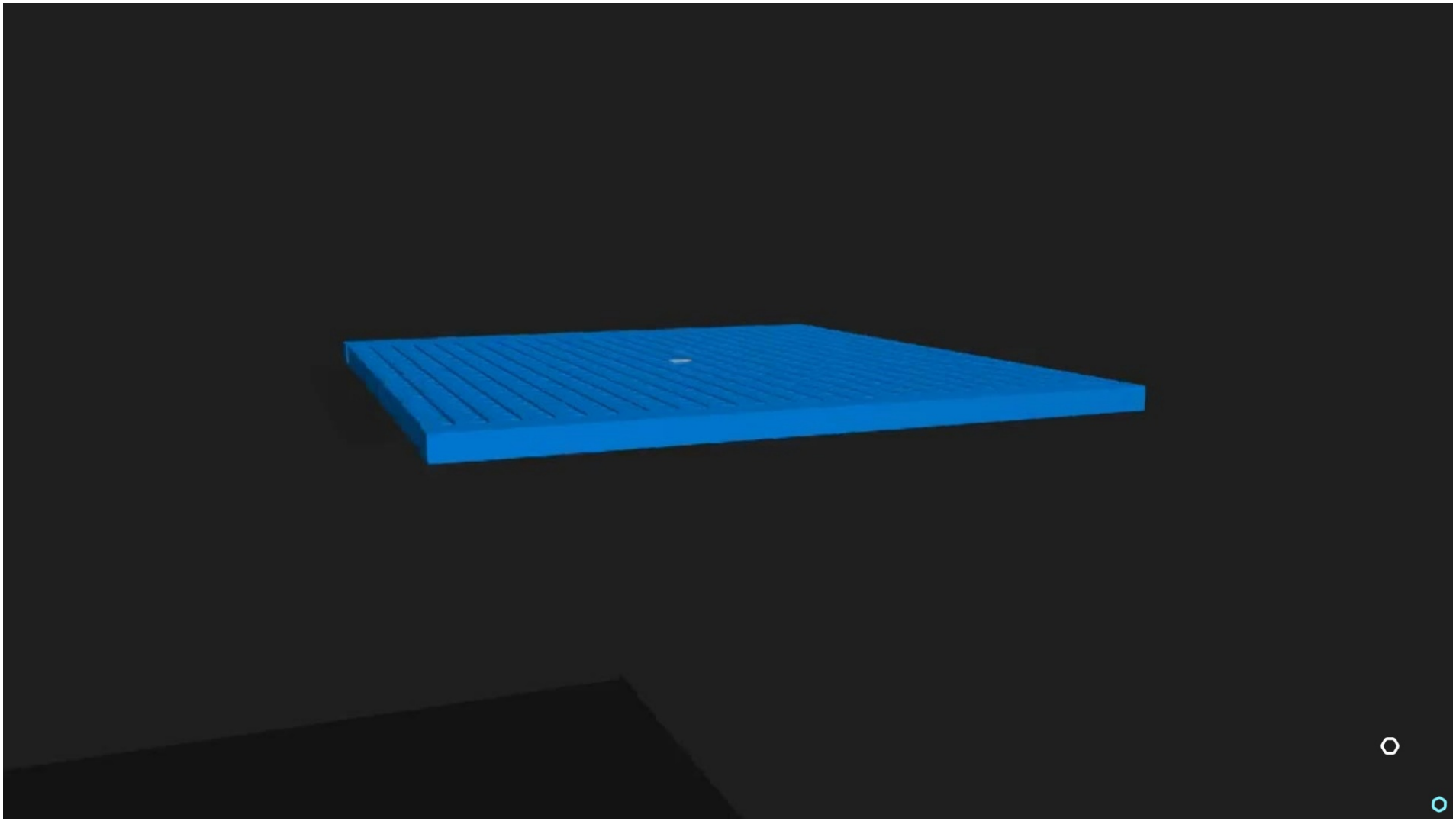
1. She enters Bob's account address as the recipient.
2. She specifies that she wants to send 100$ in crypto to Bob.
3. She signs the transaction in order to make it official with her private keys.

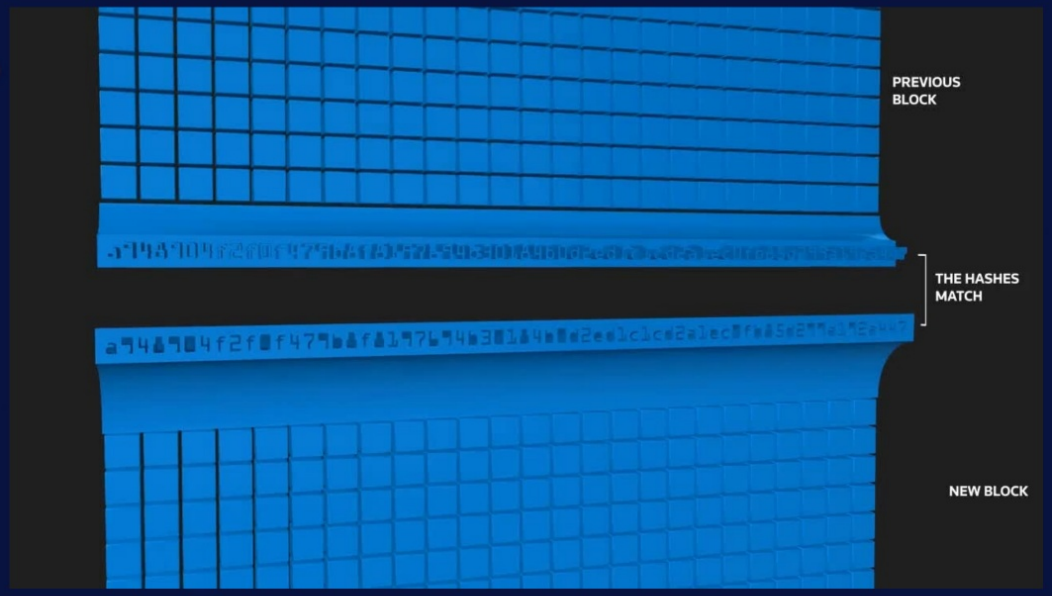


Step Two

STEP TWO
The record is checked by the network. The computers in the network, called 'Nodes', check the details of the trade to make sure it is valid.


Step Three
STEP THREE
The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain.

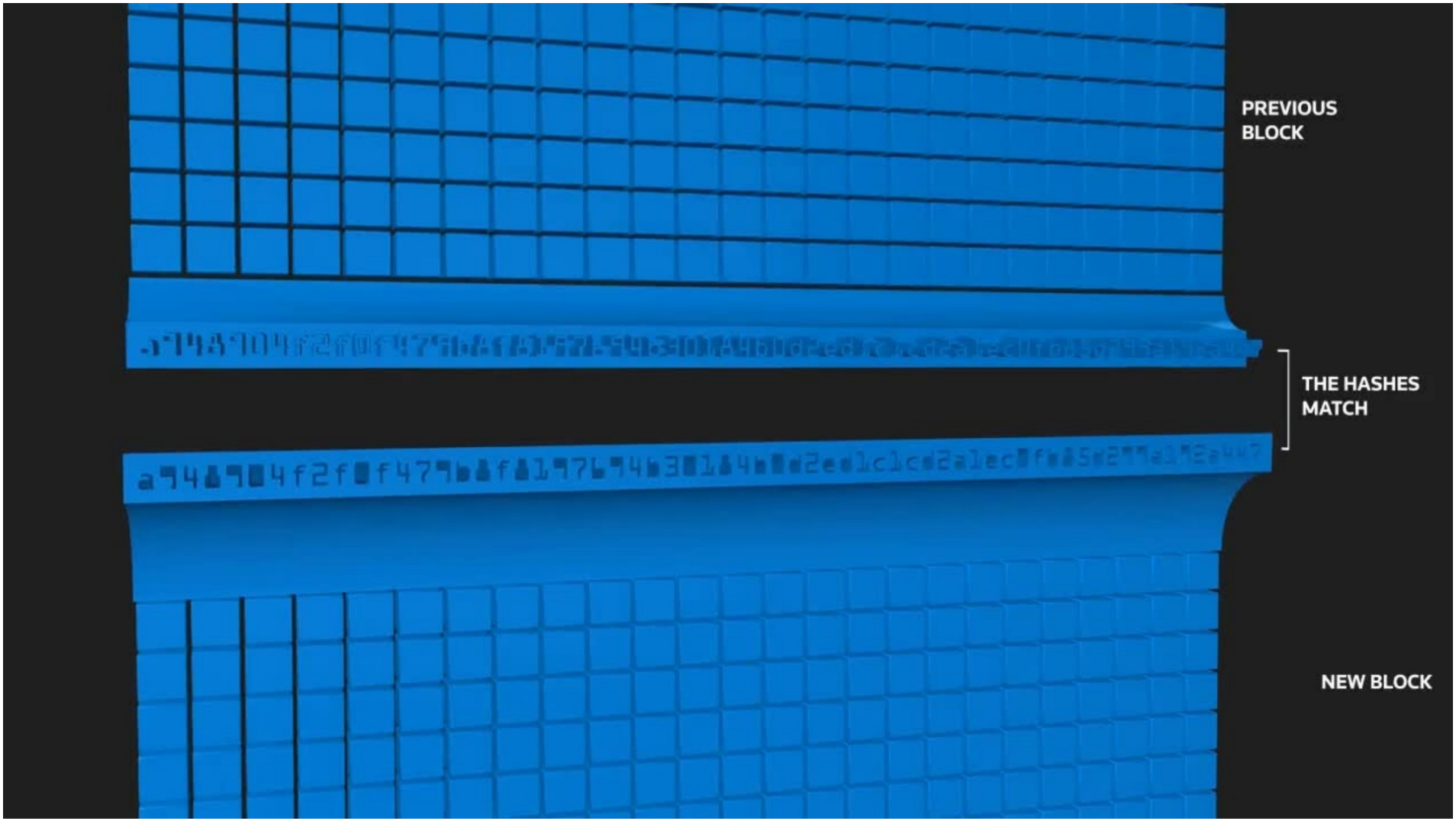




Step Four

STEP FOUR

The block is added to the blockchain. The hash codes connect the blocks together in a specific order.


PREVIOUS
BLOCK
THE HASHES
MATCH
NEW BLOCK

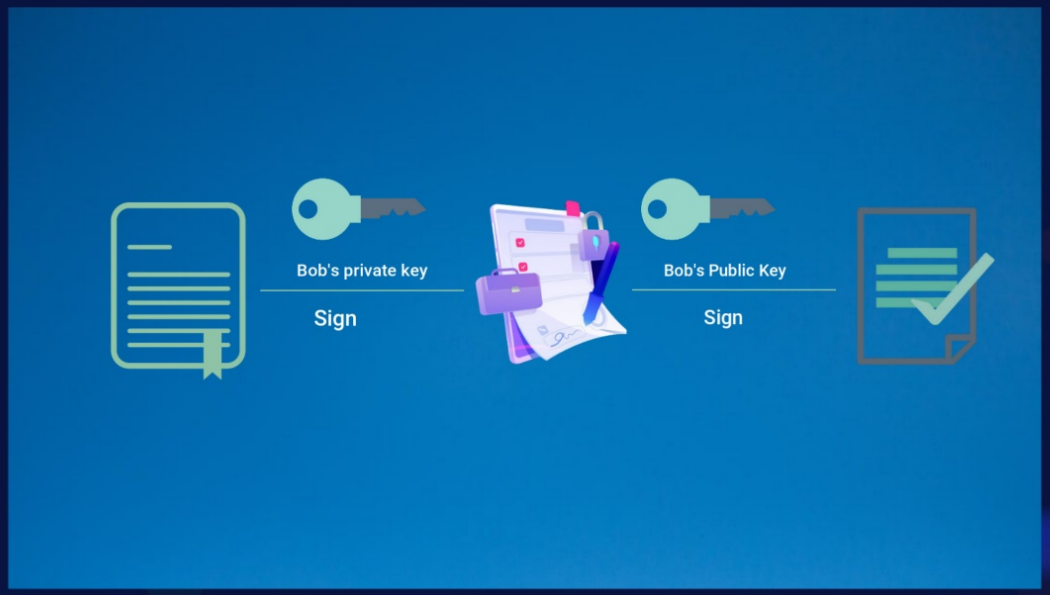
Hash Function

A hash code is created by a math function that takes digital information and generates a string of letters and numbers from it. Let's take a closer look at two important characteristics of hash codes:

First, no matter what the size of the original file, a hash function will always generate a code of the same length.

Second, any change to the original input will generate a new hash.

Example: https://andersbrownworth.com/blockchain/hash

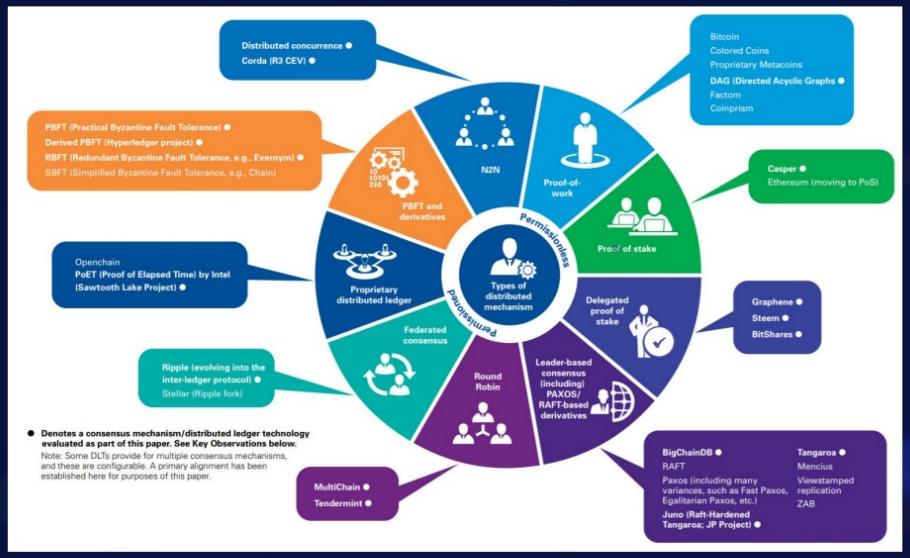


Public vs. Private Key

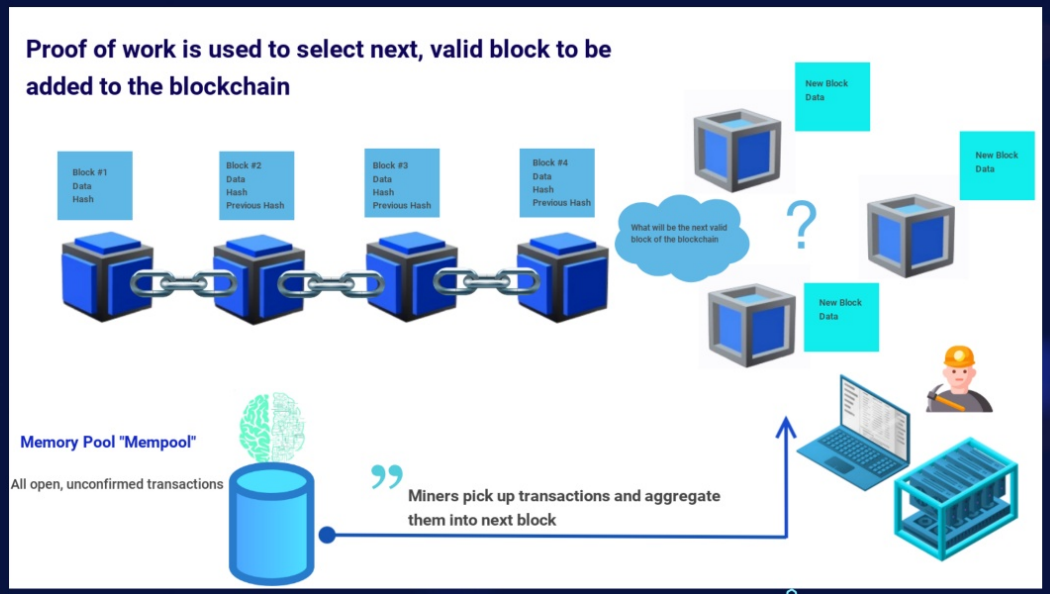
- Public key cryptography uses a pair of a public key and a private key to perform different tasks. Public keys are widely distributed, while private keys are kept secret.
- The goal of public and private keys is to prove that a spent transaction was indeed signed by the owner of the funds, and was not forged.
- When you own cryptocurrencies, what you really own is a “private key.”

Example: https://andersbrownworth.com/blockchain/public-private-keys/keys

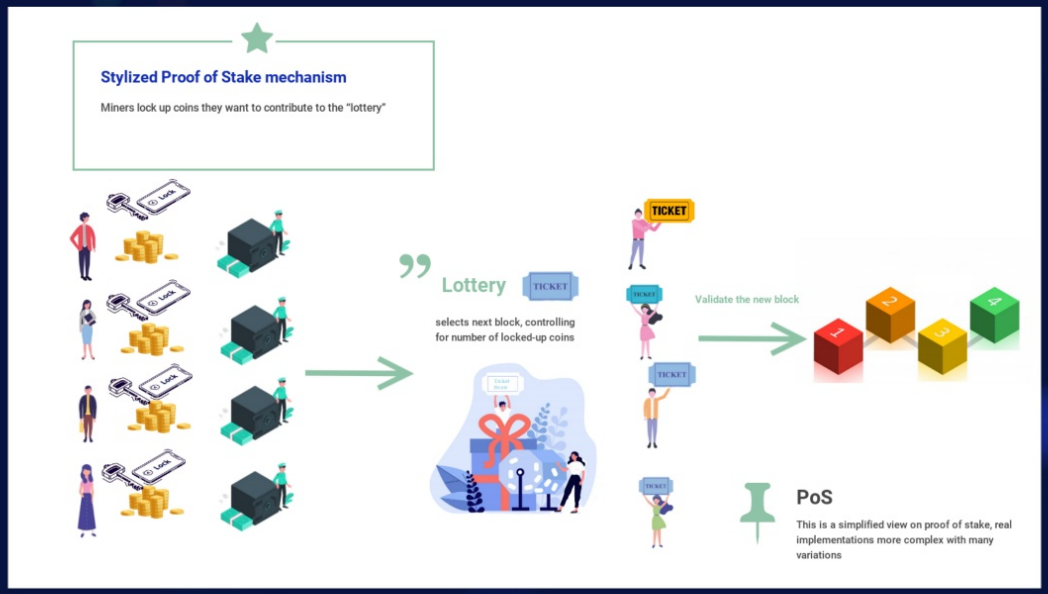
Consensus Mechanism



Proof of Work



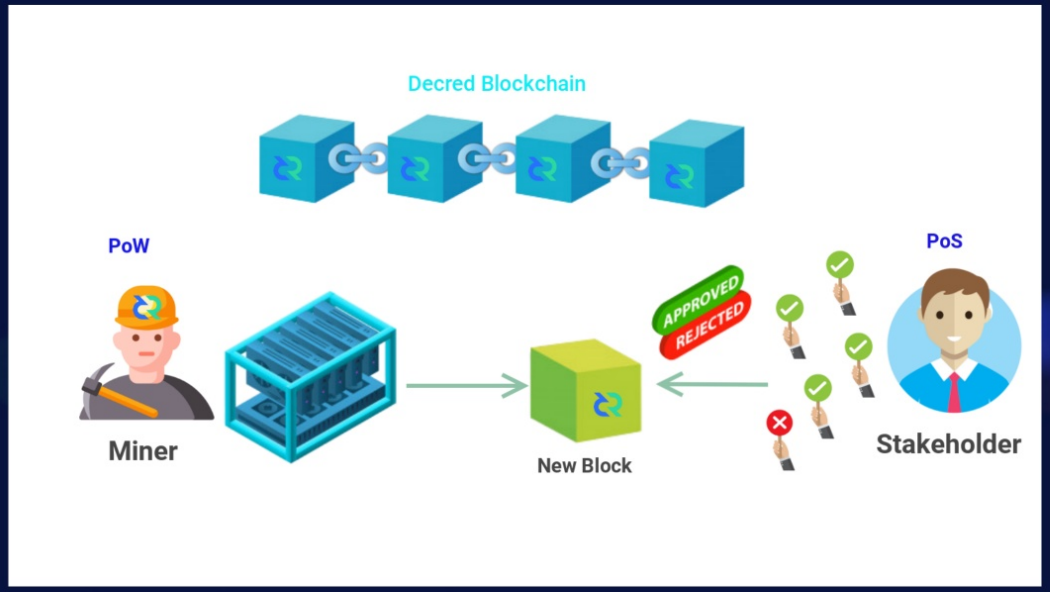
To add a block to the chain, nodes must demonstrate that they have done ‘work’ by solving an increasingly difficult computational puzzle. This process, called mining, uses a lot of computing power. In return for their work, members can receive rewards - tokens for instance, or bitcoins.



Proof of Stake

Participants buy tokens which allow them to join the network. The more tokens they have, the more they can mine.

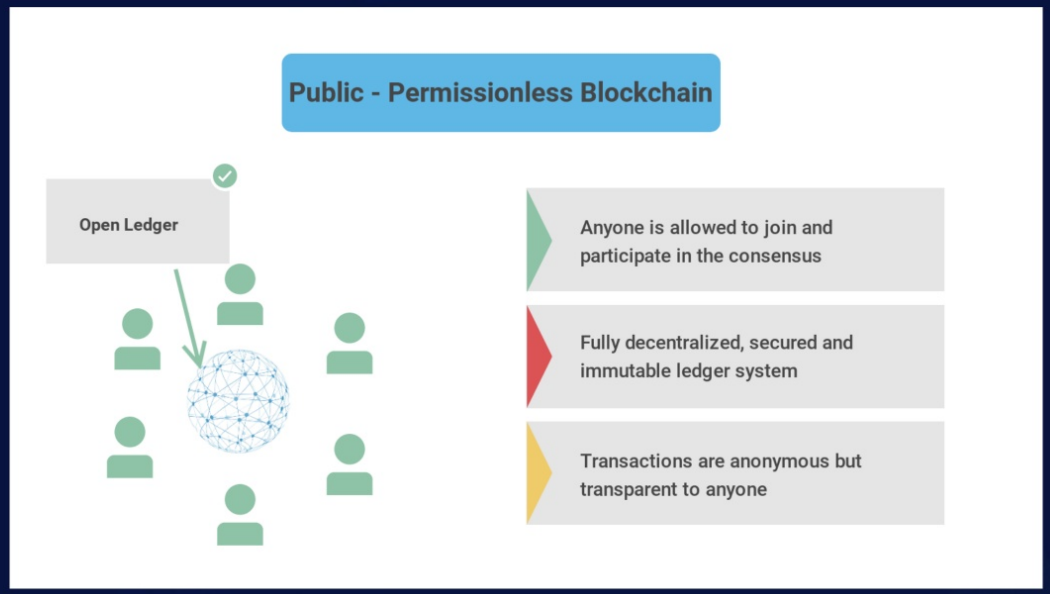
Hybrid PoW/PoS



Hybrid Proof of Work/Proof of Stake consensus mechanisms utilize elements of both PoW and PoS models when determining transaction validation rights. In doing so, they aim to mitigate the respective weaknesses of each. While the exact mechanisms of individual hybrid consensus algorithms vary, the following explanation is based on **Decred**, perhaps the most notable project using a hybrid system.

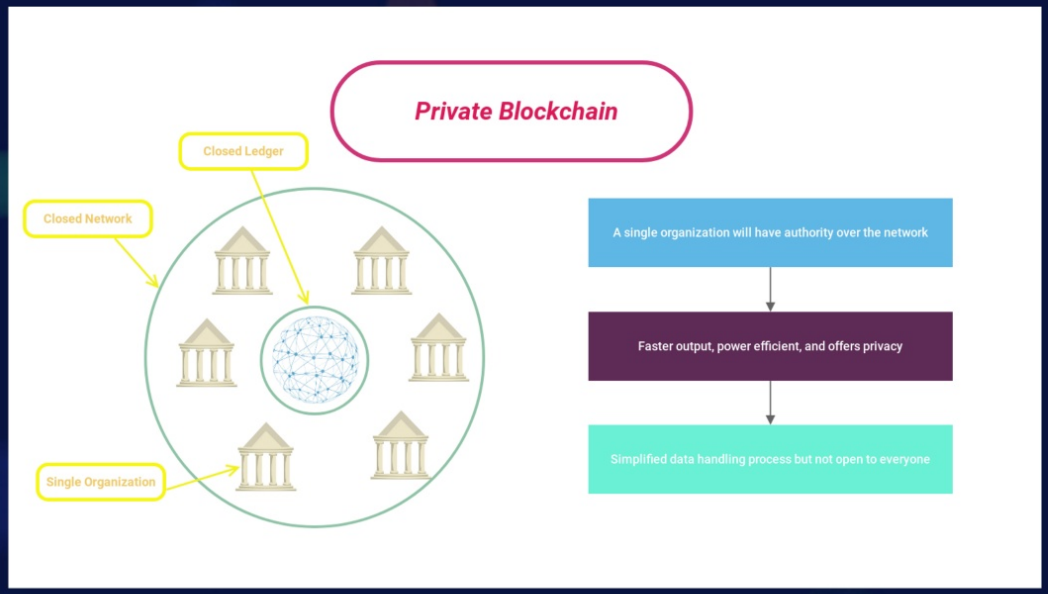

Public
Private
Types of Blockchain
Consortium
CONSORTIUM
hybrid
Hybrid Blockchain

Public-Permissionless Blockchain

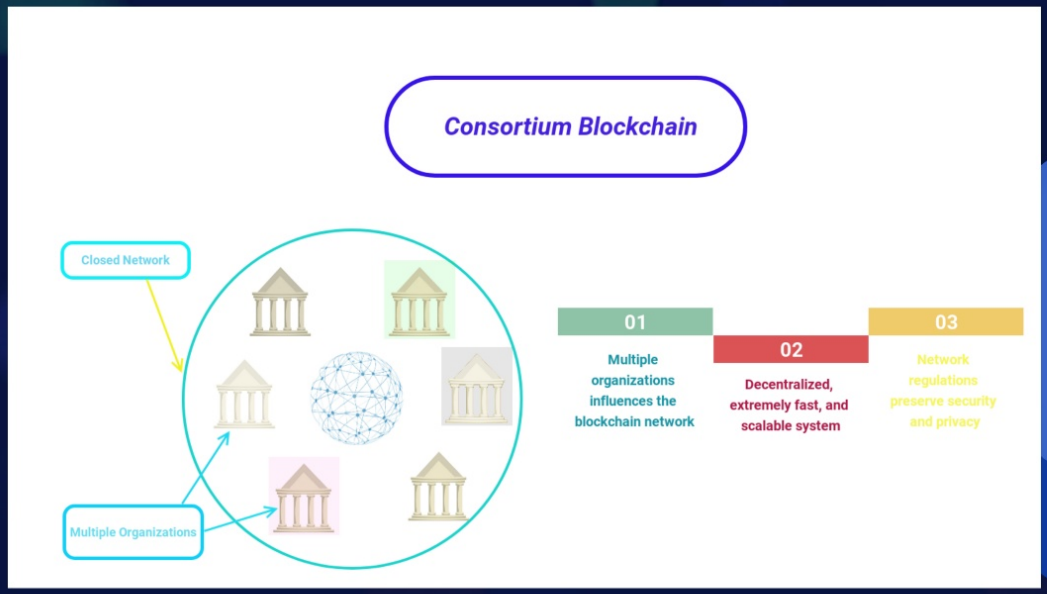


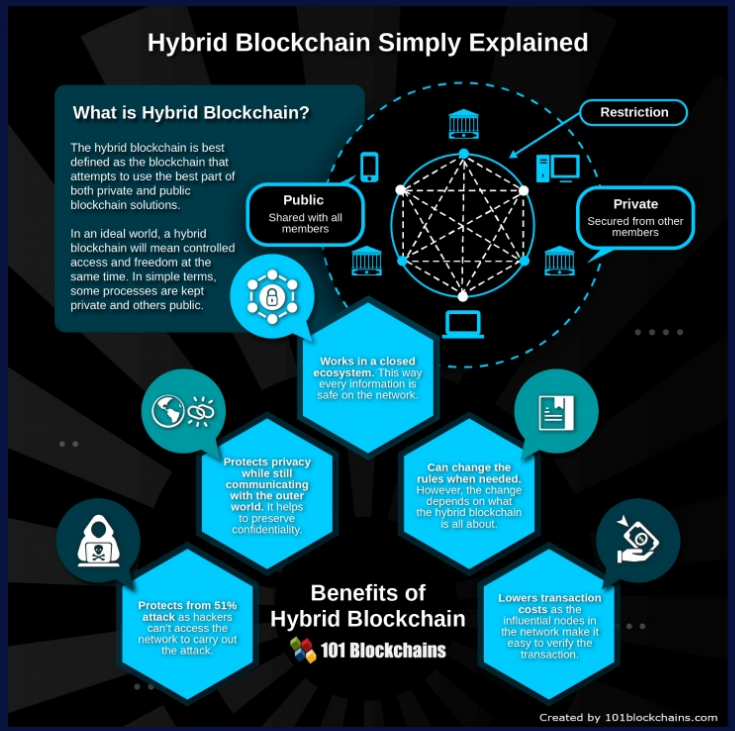
A **public blockchain** is a blockchain that anyone in the world can **read**, **send** transactions too and expect to see them included if they are valid, and anyone can participate in the consensus process.

Private Blockchain

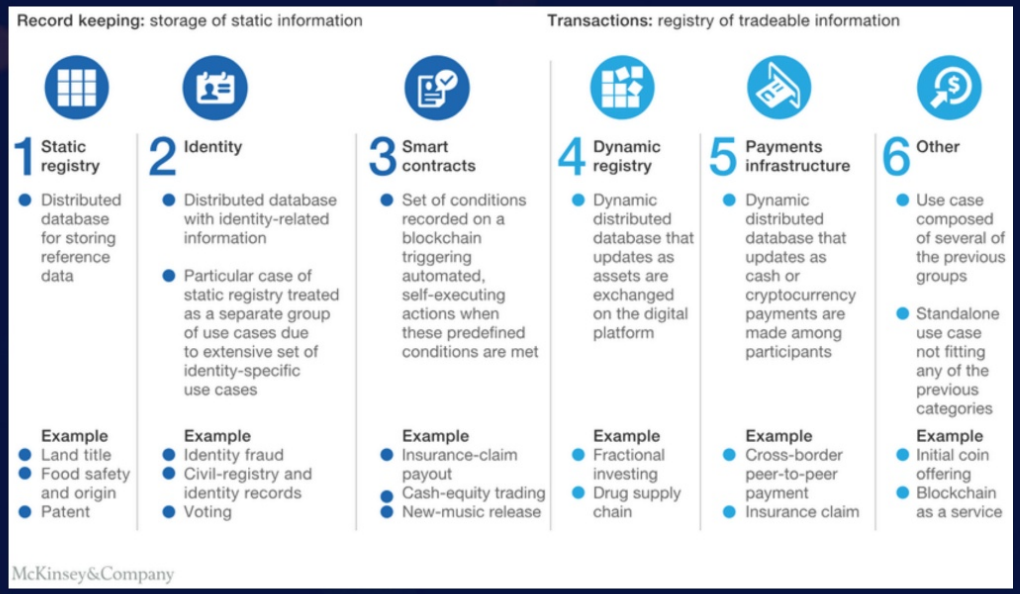


Consortium Blockchain





Hybrid Blockchain



Use Cases

Energy: https://www.energyweb.org
Healthcare: https://www.burstiq.com
Politeia: https://proposals.decred.org
https://timestamp.decred.org
Voting: https://votolegal.com.br
Estonia: https://youtu.be/OEXPF2_SbQM


Thank You


YouCode
POWERED BY SIMPLON
Blockchain
An Overview
Public vs
Private Keys
About me
How does it work?
BLOCKCHAIN
Hash Function
Consensus
Mechanism
Public
Private
Types
Use Cases
Blockchain Technology
101