Module 1: Understanding Blockchain

1) What is Blockchain

Blockchain is a distributed ledger that records all the transactions that take place on the network. A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies. It allows transactions to have public "witnesses," thereby making a cyberattack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it

A **blockchain can** be either **centralized** or decentralized. It is important, however, that decentralized not be confused with **distributed**. While a **blockchain** is inherently **distributed** (meaning that many parties hold copies of the ledger), it is not inherently decentralized.

A blockchain is a way to implement a distributed ledger, but not all distributed ledgers necessarily employ blockchains. In a distributed ledger,it is not necessarily the case that all nodes either receive all the information.

By extension, a blockchain constitutes a database that contains the history of all the exchanges made between its users since its creation. This database is secure and distributed: it is shared by its different users, without intermediaries, which allows everyone to check the validity of the chain.

Advantages of Blockchain over Typical Centralized System:

- Gets rid of any intermediaries
- Verification of transactions
- High-security protocols
- Lower costs
- Transparent network system
- Immutable and decentralized

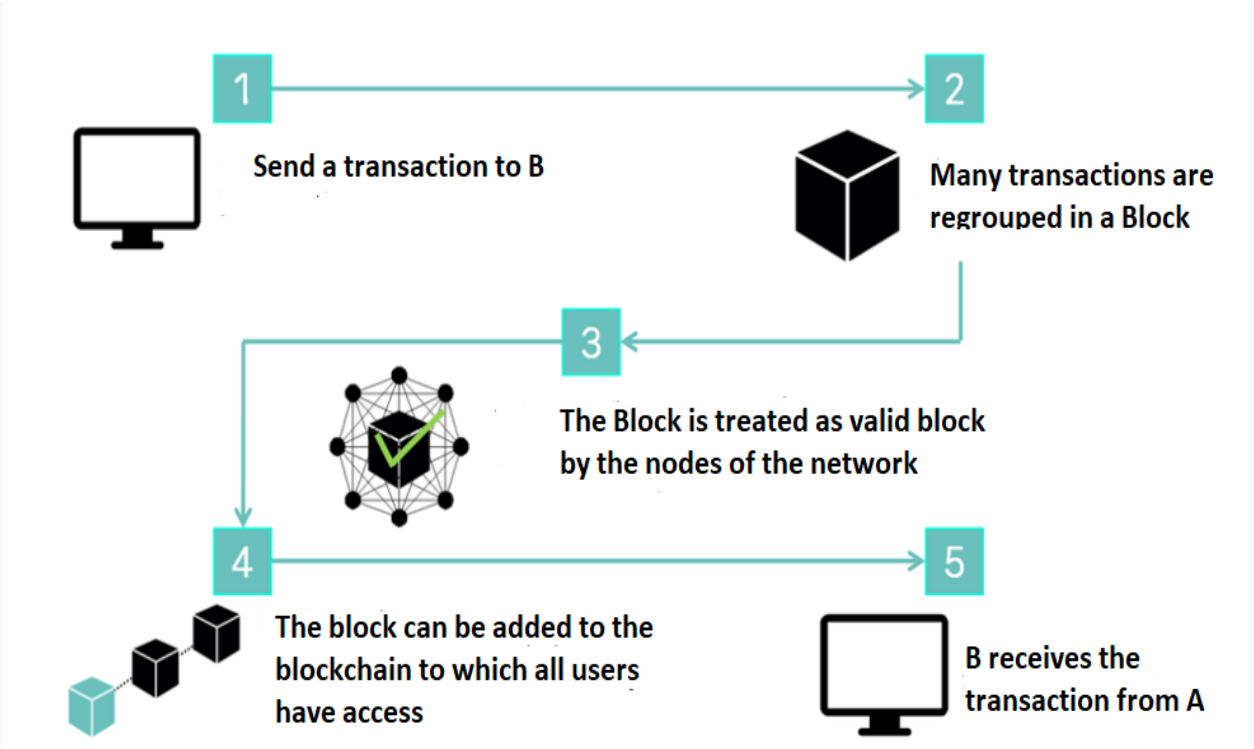
History of Blockchain Technology

1991-2008: Do you know when was the first time blockchain actually emerged? Well, back in **1991**, Stuart Haber and Scott Stornettqo started working on the first blockchain technology. At first, they wanted to create a cryptographically encrypted block of chain. Moreover, they tried to make it tamper-proof.

2) How it works?

Transactions between network users are grouped in blocks. Each block is validated by the nodes of the network called "miners", according to techniques which depend on the type of blockchain. In the bitcoin blockchain this technique is called "Proof-of-Work", proof of work, and consists in solving algorithmic problems. Once the block is validated, it is time stamped and added to the blockchain. The transaction is then visible to the receiver and the entire network.

There are public blockchains, open to all, and private blockchains, the access and use of which is limited to a certain number of actors.



This process takes a certain time depending on the blockchain we are talking about (about ten minutes for bitcoin, 15 seconds for Ethereum).

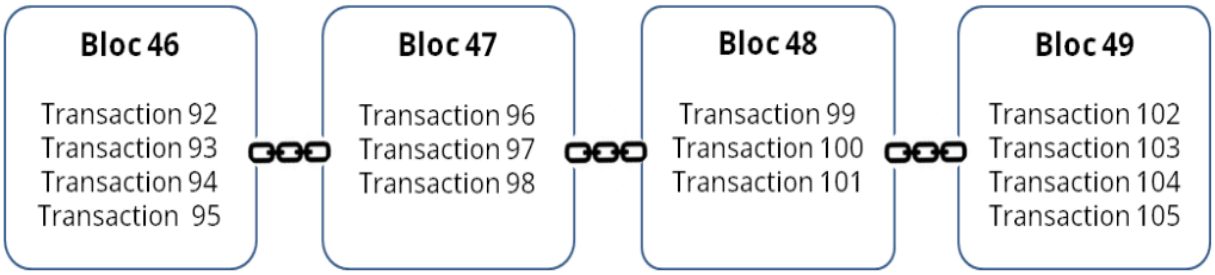
The decentralized nature of the blockchain, coupled with its security and transparency, promises much broader applications than the monetary fie.

- Blocks:

  “Blocks” on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

  - Blocks store information about transactions like the date, time, and price, etc.
  - Blocks store information about who is participating in transactions.
  - Blocks store information that distinguishes them from other blocks. each block stores a unique code called a “hash” that allows us to tell it apart from every other block.

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain.



- **Transaction**

  A **Blockchain transaction** can be **defined** as a small unit of task that is stored in public records. These records also knows as blocks. These blocks are executed, implemented and stored in **blockchain** only after the validation by all persons involved in the **blockchain** network.

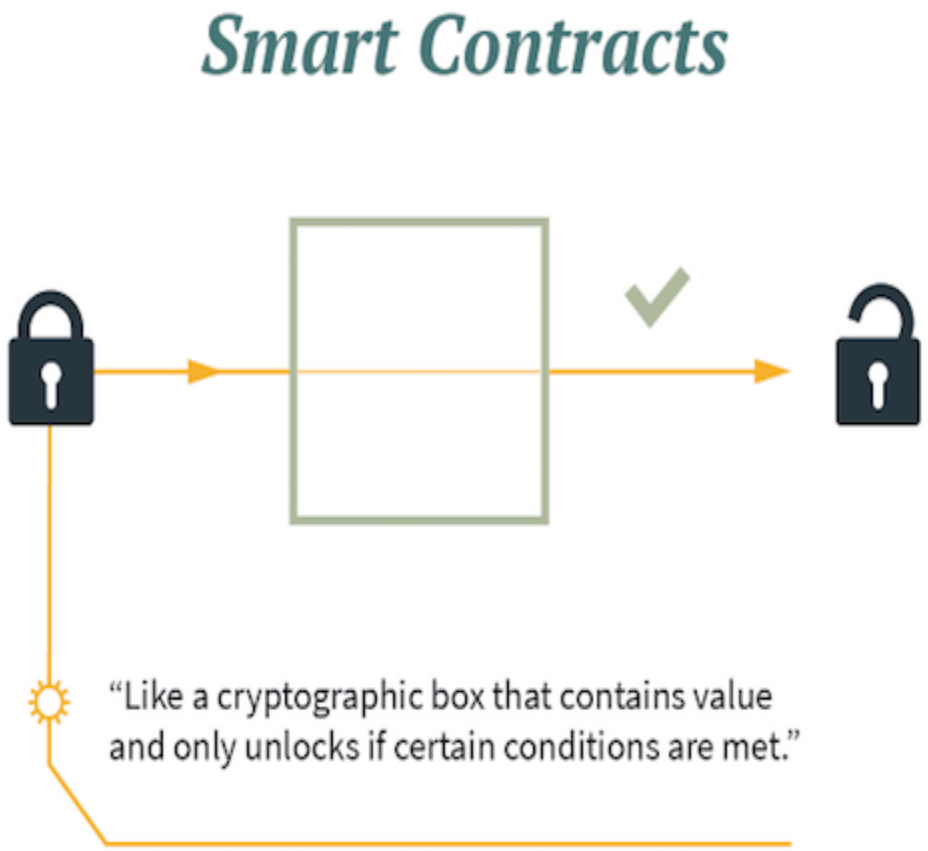
  So, when a blockchain transaction happens all the nodes in the network will have to say it’s valid or it won’t get added to the ledger.

- ## Smart contract

  In blockchain, the smart contract is a code fragment that executes the terms of a contract. The code behind a smart contract contains specific terms that are executed when triggered by specific agreed events. A blockchain network uses smart contracts to provide controlled access to the ledger.

Smart contracts are designed and implemented within blockchains, and therefore they inherit some of the blockchain's properties:

- **They're immutable**, which means a smart contract can never be changed and no one can tamper with or break a contract.
- **They're distributed**, which means that the outcome of the contract is validated by everyone in the network, just like any transaction on a blockchain. Distribution makes it impossible for an attacker to force control to release funds, as all other participants would detect such an attempt and mark it as invalid.



A. **Channel**

A channel can be defined as a sub-network for peers communication, if it is necessary to divide transactions according to different boundaries according to some service logic.

B. **Consensus**

The process of keeping the ledger transactions synchronized across the network –to ensure that ledgers update only when transactions are approved by the appropriate participants, and that when ledgers do update, the update with the same transactions in the same order – is called consensus.

3) Application domains

Trading - Governmental Services - Healthcare - Oil and Gas - Insurance -Media and Entertainment -Travel - Network Solutions Cyber Security and the Internet of Things, ect.

We can classify the use of blockchain in three categories:

- Applications for the transfer of assets (monetary use, but not only: securities, votes, stocks, bonds, etc.).

- Blockchain applications as a registry: it thus ensures better traceability of products and assets.

- Smart contracts: these are stand-alone programs that automatically execute the terms and conditions of a contract, without requiring human intervention once started.

The fields of exploitation are immense: banks, insurance, health and pharmaceutical industry, supply chain of many sectors (food industry, luxury, international trade, distribution, wines, aeronautics, automobile ...), music industry, energy, real estate, voting ...

Above all, blockchain paves the way for a new web, the decentralized web, and a new digital economy, the token economy. To understand their challenges, it is crucial to avoid caricatures about cryptoactive agents, which are at the heart of this revolution.

Obviously, these promises are not without challenges, whether economic, legal, governance, or even ecological.

3) Blockchain platforms

Many Blockchain platformscan be considered like Ethereum, Hyperledger, Multichain,Open Ledger, Chain, Bitcoin Blockchain, and Corda.


HYPERLEDGER


ethereum


Bitcoin


MultiChain


Quorum


OpenLedger