INFORMATICA

Prof. Giorgio Poletti
giorgio.poletti@unife.it

Laurea Triennale in Economia
a.a. 2018 – 2019

Sviluppo del corso

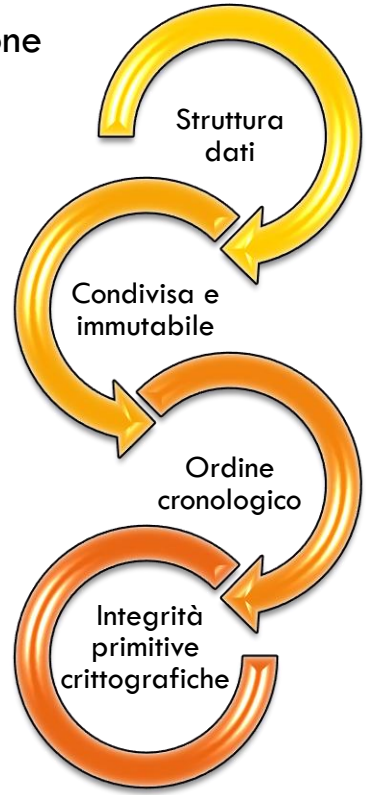
Modulo II e Modulo III

> L'invenzione della blockchain dà ancora più potere alle persone e sfida l'insidiosa cultura della proprietà e del controllo. La tecnologia alla base del bitcoin spezza la 'massima' di Orwell.
>
> Julian Assange (WikiLeaks)

- Modulo II
  - Dato e informazione: capire per comprendere – le relazioni
  - IoT (Internet Of Things), BYOB e BYOT
  - Data WareHouse e Big Data
  - Tecnologia: cambiamenti organizzativi e sociali
- Modulo III
  - Algoritmi di ricerca e posizionamento
  - Distribuzione e ricerca di Informazioni
  - Posizionarsi in Rete, Rete e i Social come luogo di Marketing
  - Blockchain: significato, importanza e rischi

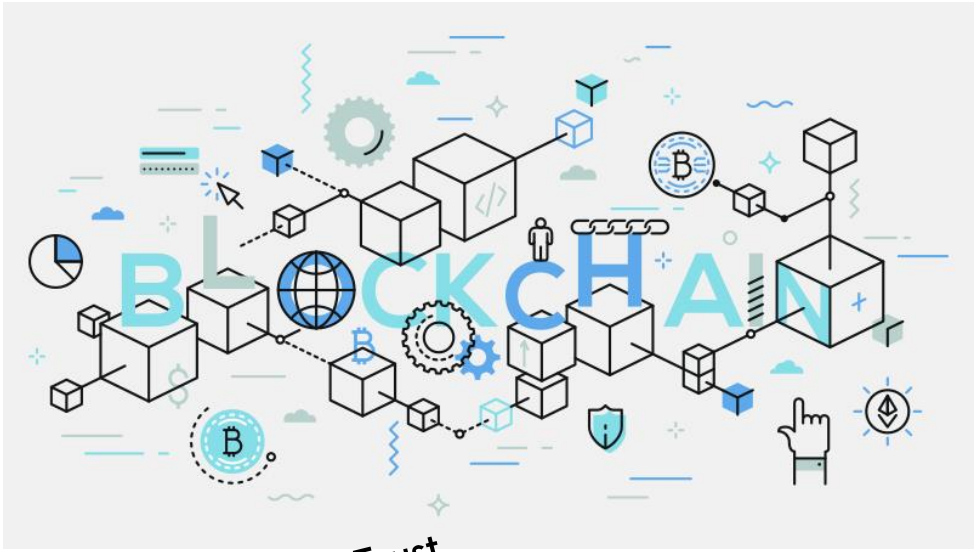
Blockchain

Storia e definizione



Internet delle Transizioni o
Internet del Valore

- decentralizzazione
- trasparenza
- sicurezza
- immutabilità



Nuovo concetto di Trust

Blockchain NON = Bitcoin

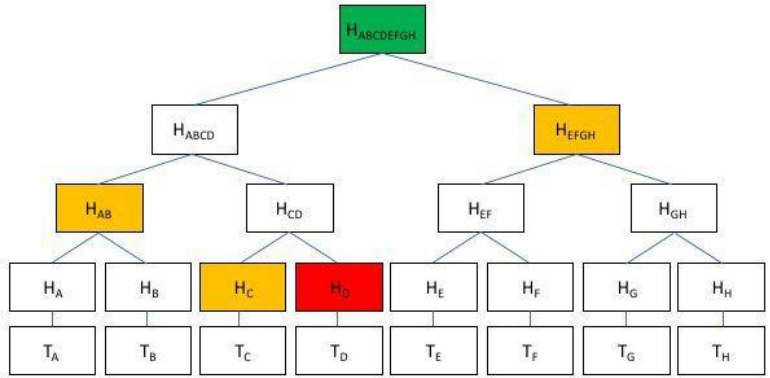
Blockchain

Storia e definizione

1991- Blockchain protetto da crittografia ***Stuart Haber e Scott Stornetta***

(*Journal of Cryptology*)

1992 – Introduzione nel Blockchain introducono i merkle tree
Haber, Stornetta e Bayer



ALBERO HASH o **ALBERO MERKLE** *è un albero in cui ogni nodo foglia è etichettato con l'hash di un blocco dati e ogni nodo non foglia è etichettato con l'hash crittografico delle etichette dei suoi nodi figli.*
EFFICIENZA e raccogliere più documenti in un blocco.

Blockchain

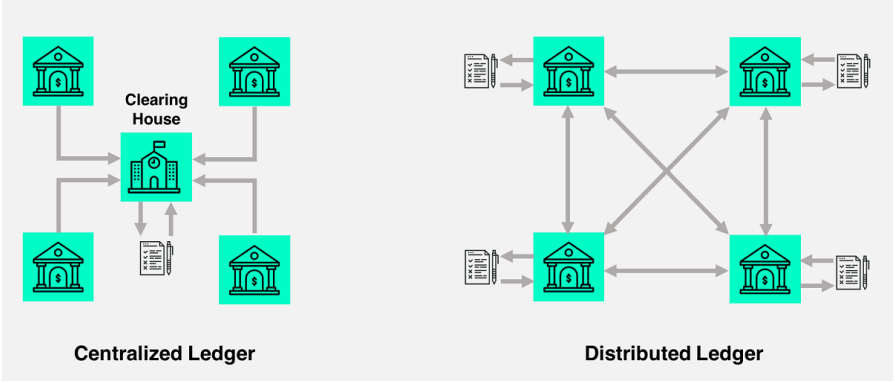
Tecnologia per ***Distributed Ledger***

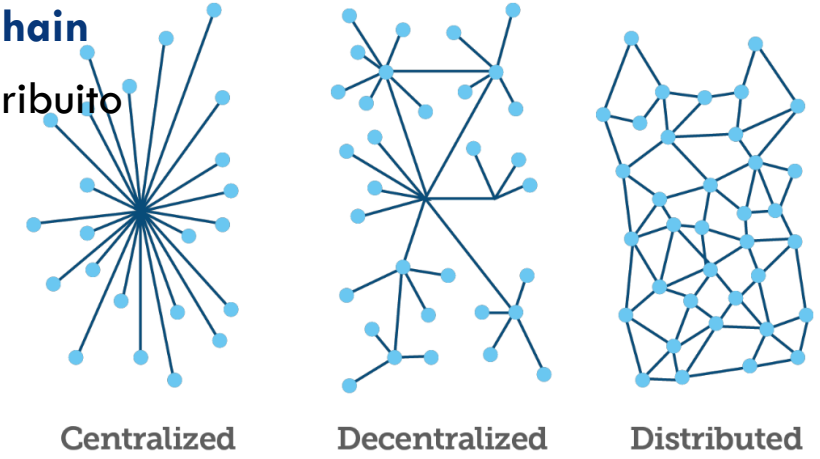
Distributed Ledger → **Blockchain**

DLT (Distributed Ledger Tecnology) - Registro distribuito

- Accesso
- Modifica

→ *da più punti della rete*



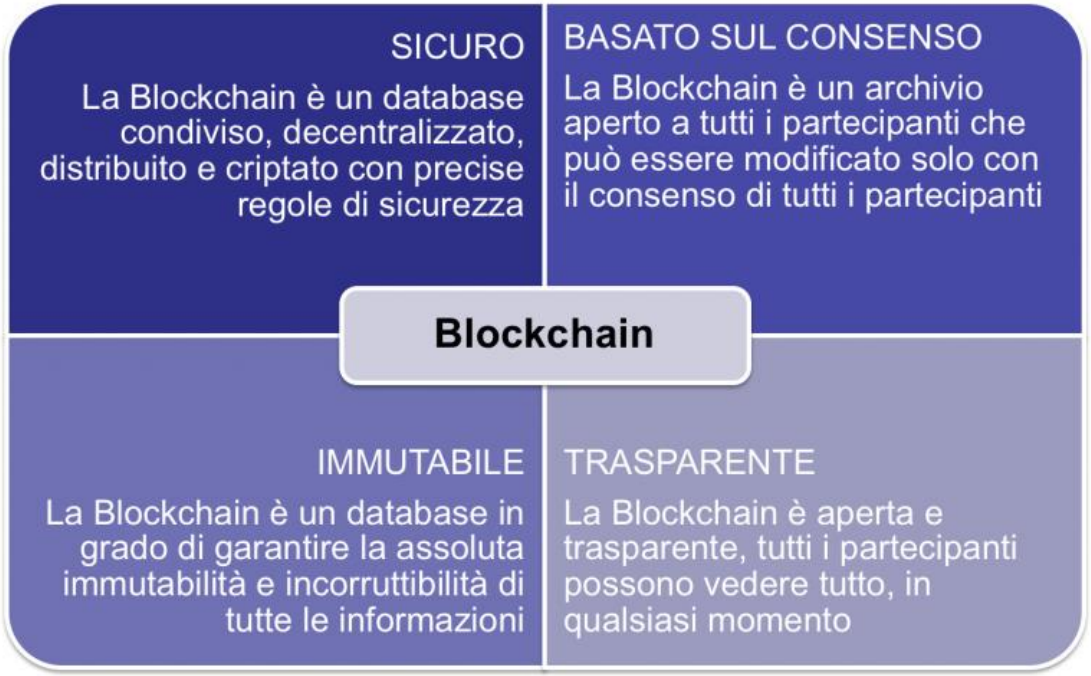


Blockchain *è quindi paragonabile alle banche dati e ai registri gestiti in maniera centralizzata da autorità riconosciute e regolamentate.*

Blockchain

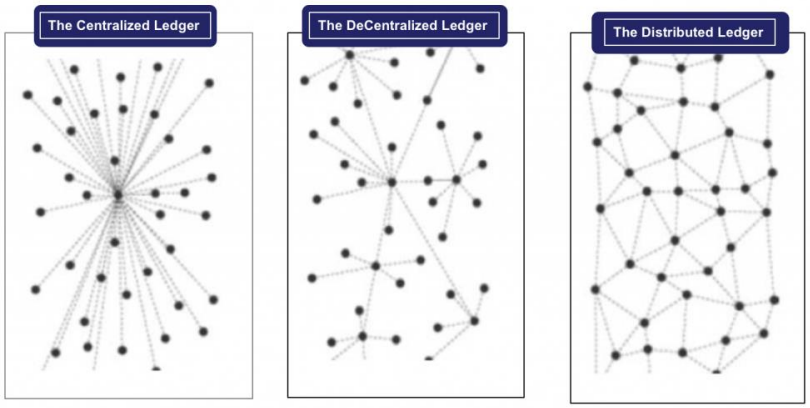
Paradigma più che tecnologia. Keywords: **decentralizzazione** e **partecipazione**

Definizioni per caratteristiche



Blockchain

Evoluzione di **Ledger** = **Libro Mastro**



Centralized Ledger

Rapporto rigorosamente centralizzato Uno-A-Molti, (presenza di una struttura o autorità o sistema centralizzato.

Fiducia nell'autorità, nell'autorevolezza del soggetto "Centro" dell'organizzazione.

Decentralized Ledger

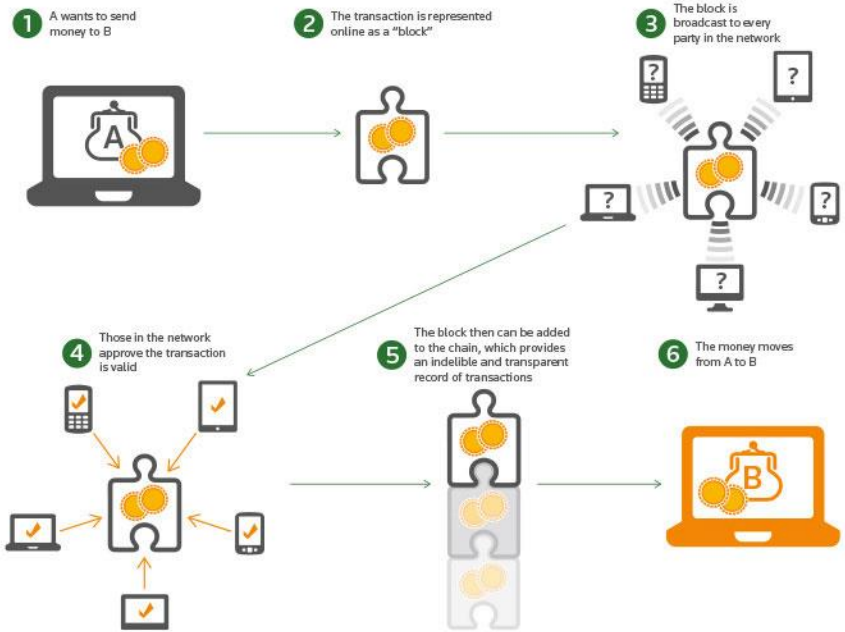
Centralizzazione a livello "**locale**", Uno-A-Molti (ripetuto), tanti "*soggetti centrali*". Fiducia delegata a un soggetto centrale, logicamente più vicino, ma comunque centralizzato.

Distributed Ledger

Novità: ***Distributed Ledger***, non esiste più nessun centro e dove la logica di ***governance*** è costruita attorno a un nuovo concetto di fiducia tra tutti i soggetti. NON si può prevalere (dati) e il processo decisionale passa ***rigorosamente*** attraverso un rigoroso processo di **costruzione del Consenso**.

Blockchain

Protocollo di comunicazione (logica del Data Base *Distribuito*)



Serie di blocchi archiviano un insieme di transazioni validate e correlate da un Marcatore Temporale (Timestamp).
Con hash (una funzione algoritmica *non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita*) per identificare il blocco in modo univoco e che permette il collegamento con il blocco precedente tramite identificazione del blocco precedente.

Blockchain

Componenti basi

Nodo: sono i partecipanti alla Blockchain e sono costituiti fisicamente dai server di ciascun partecipante

Transazione: è costituita dai dati che rappresentano i valori oggetto di "scambio" e che necessitano di essere verificate, approvate e poi archiviate

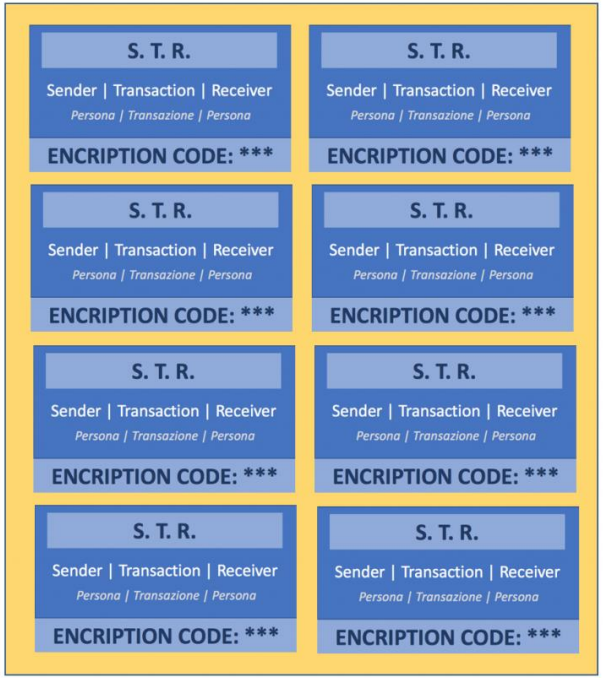
Blocco: è rappresentato dal raggruppamento di un insieme di transazioni che sono unite per essere verificate, approvate e poi archiviate dai partecipanti alla Blockchain

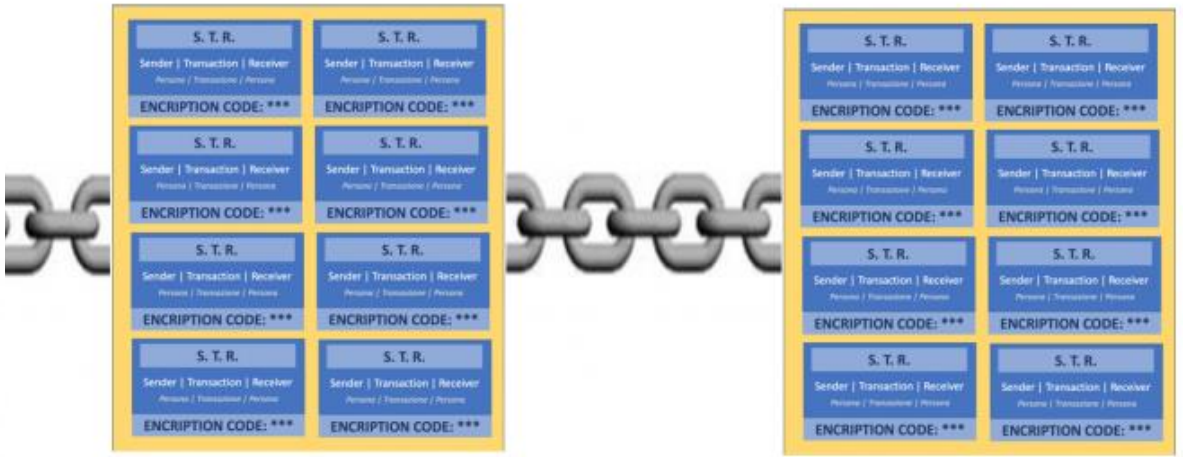
Ledger: è il registro pubblico nel quale vengono "annotate" con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo ordinato e sequenziale.

Hash: è una operazione (Non Invertibile) che permette di mappare una stringa di testo e/o numerica di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata.

Blockchain

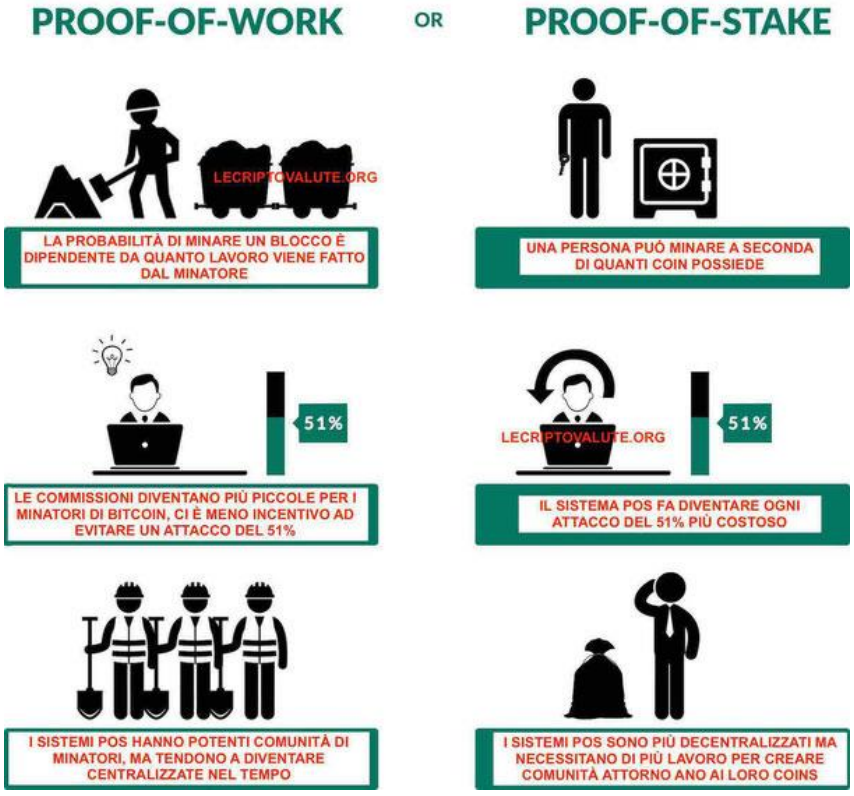
Il Blocco che raggruppa diverse transazioni





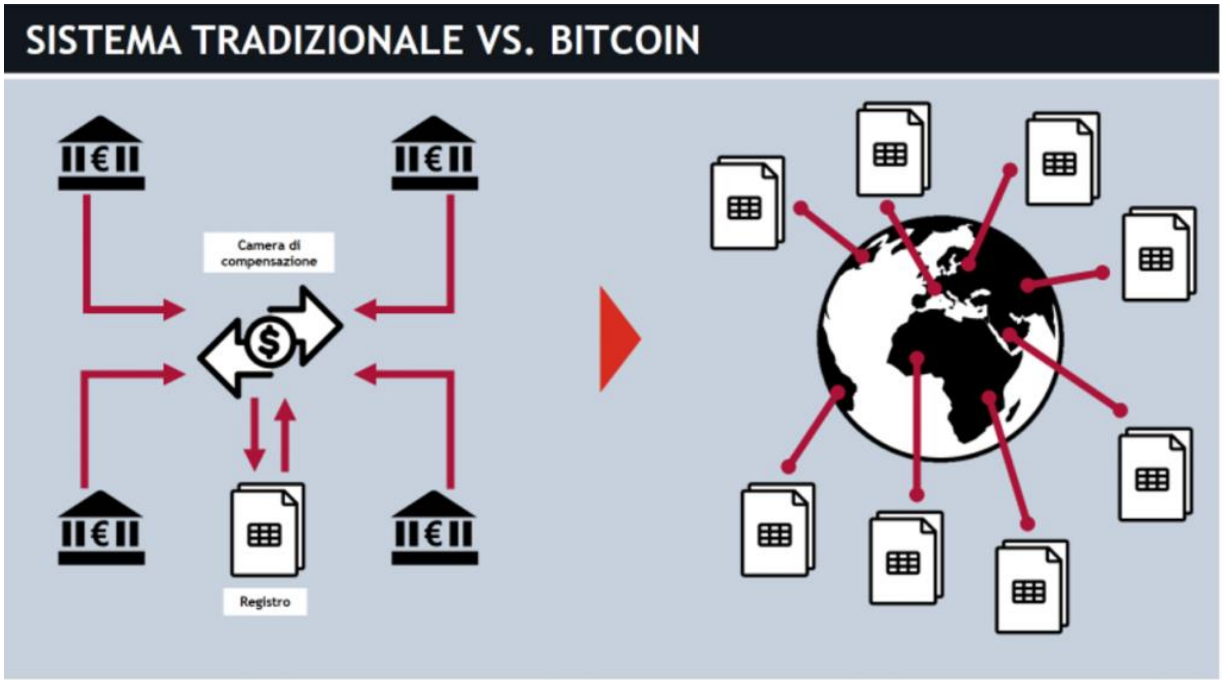
Blockchain e Criptomonete

Una **criptomoneta (criptovaluta**) è una valuta paritaria, decentralizzata e digitale la cui implementazione si basa sui principi della crittografia per convalidare le transazioni e la generazione di moneta in sé.
Si basa sul **proof-of-work**



Il **Proof of work**: è un protocollo che ha l'obiettivo principale di dissuadere gli attacchi informatici come un attacco denial-of-service (DDoS) che ha lo scopo di esaurire le risorse di un sistema informatico inviando più false richieste.

Criptomonete: come funzionano i bitcoin



The trust machine

- Coinbase
- Indacoin
- Bitpanda
- Coinmama
- Localbitcoins
- WeSellCrypto

Con il termine Blockchain s'intende il paradigma tecnologico che permette di sviluppare applicazioni Cryptocurrency-like: il protocollo Bitcoin rappresenta solo una – la prima – delle possibili realizzazioni.

Esistono 3 ere delle monete: quelle basate sulle materie prime, quelle basate su criteri politici e ora quelle basate sulla matematica.
(Chris Dixon, co-fondatore di Hunch e SiteAdvisor)