Blockchain
World Trust Revolution

Introduzione
Oggi più che mai la dinamicità della modernità all'interno di un contesto socio-economico ci spinge alla ricerca costante di **fiducia**, sicurezze sia personali che verso sistemi astratti o simbolici. In quest'ottica, la fiducia ha infatti un ruolo fondamentale nel mantenere un equilibrio fra conoscenza e ignoranza, permettendoci di agire anche laddove non vi sia una piena conoscenza delle situazioni in cui ci troviamo.

La post-modernità ci ha gradualmente condotto di fronte a una trasformazione sociale profonda, che ci ha portato a quella che viene definita «*fiducia distribuita*», un nuovo paradigma, reso possibile dalla tecnologia, che sta riscrivendo il nostro modo di vivere, lavorare e consumare.

Blockchain Technology
La **blockchain**, da un punto di vista strettamente tecnico è "*catena di blocchi*" che può essere semplificata come un processo in cui un insieme di soggetti condivide **risorse informatiche** (*memoria, CPU, banda*) per rendere disponibile alla comunità di utenti un database virtuale del quale ogni partecipante ha una copia dei dati. L'utilizzo di un *protocollo di aggiornamento* ritenuto sicuro dalla comunità degli utenti e di tecniche di validazione crittografiche genera la reciproca fiducia dei partecipanti nei dati conservati dalla blockchain.

I componenti basilari della Blockchain:
- **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 e effettuate in modo ordinato e sequenziale. Il Ledger è costituito dall'insieme dei blocchi tra loro incatenati.

Struttura del blocco
Le **transazioni** sono raggruppate nei blocchi del blockchain e il numero di transazioni all'interno di ognuno di questi blocchi varia in base alla dimensione della transazione stessa. La dimensione della transazione, invece, varia in base al ***numero di input e di output*** della stessa. Un blocco è composto da due parti principali: l'**header** e il **body**. Mentre le transazioni sono racchiuse nel body del blocco, nell'header sono presenti ***sette campi*** di gestione del blocco stesso.

Versione	02000000
Hash del blocco precedente (PrevHash)	E87C17C45768w7e1643fsd5481sd3f4131df681
Merkle root	697we168t4v1a4rv3v1e3r43c4er14ca8c4168a
Timestamp	358b0553
Bits	535f0119
Nonce	48750933
Numero di transazione	64

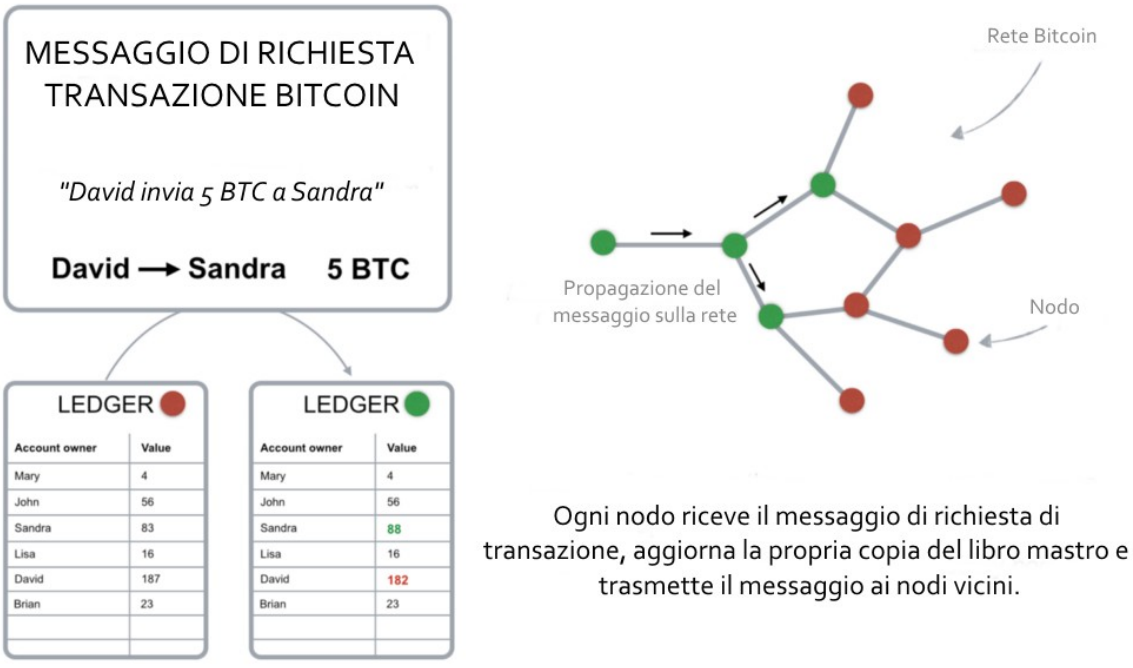
Il campo **Versione** dipende dalla versione del software utilizzato, il campo **PrevHash** è un hash (*una funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza prederminata*) di 256 bit che serve per fare riferimento al precedente blocco della catena, il **Merkle root** è l'hash di tutti gli hash di tutte le transazioni nel blocco, il campo **Timestamp** rappresenta il marcatore temporale dell'ultima transazione, il campo **Bits** rappresenta il corrente *valore target*: l'hash dell'header di un blocco dev'essere minore o al massimo uguale al corrente valore di target per essere accettato dalla rete, il campo **Nonce** è un valore a 8 byte che viene aggiunto al blocco in modo che l'output della funzione di hash vari facendo in modo che risulti inferiore al valore target, il valore viene ricalcolato finché l'hash del blocco non contiene il richiesto numero di zeri principali, ed infine, il campo **Numero di transazione** identifica il numero della transazione contenute nel blocco.

Ciascun blocco contiene dunque diverse transazioni con ***informazioni relative all'indirizzo pubblico del ricevente, le caratteristiche della transazione e la firma crittografica*** che garantisce della sicurezza e dell'autenticità della transazione.

La Blockchain è da vedere come un **registro pubblico** e **condiviso** costituito da una serie di client o di nodi, organizzata per aggiornarsi automaticamente su ciascuno dei client che partecipano al network. Ogni operazione effettuata deve essere confermata automaticamente da tutti i singoli nodi attraverso software di crittografia, che verificano un pacchetto di dati definiti a chiave privata o seme, che viene utilizzato per firmare le transazioni, garantendo l'identità digitale di chi le ha autorizzate.

Per tenere traccia della quantità di tutte le transazioni e quindi del valore posseduto da ognuno di noi, la blockchain utilizza un **ledger**, un file digitale che tiene traccia di tutte le transazioni della rete blockchain. Il file di contabilità generale non è memorizzato in un server di entità centrale ma è ***distribuito*** in tutto il mondo tramite una **rete di privati computer** che stanno memorizzando dati e eseguendo calcoli. Ciascuna di questi computer rappresentano un "nodo" della rete blockchain e hanno una copia del file del libro mastro.

Esempio transazione

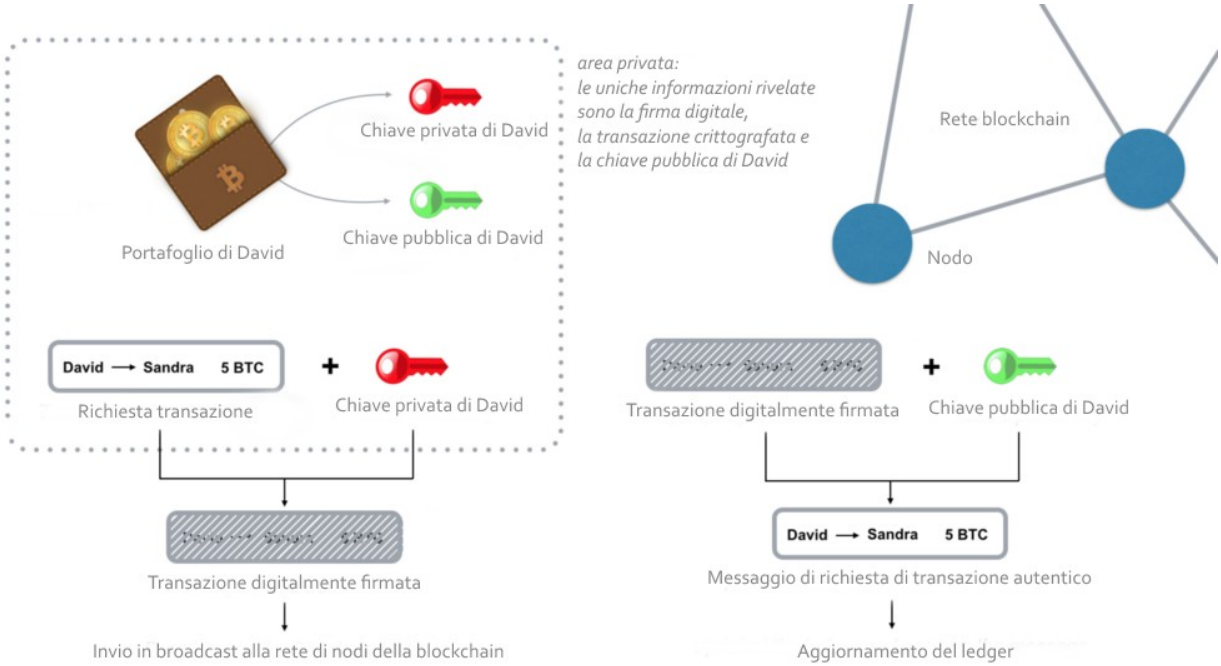


Se David vuole inviare Bitcoin a Sandra una quantità di *5 Bitcoin*, criptovaluta maggiormente diffusa oggi, ***trasmette un messaggio alla rete*** che dice che la quantità di Bitcoin nel suo

account dovrebbe scendere di 5 BTC e la quantità di account di Sandra dovrebbe aumentare della stessa quantità. Ogni nodo della rete riceverà il messaggio e *applicherà la richiesta transazione alla loro copia del libro mastro*, aggiornando così i saldi dei conti.

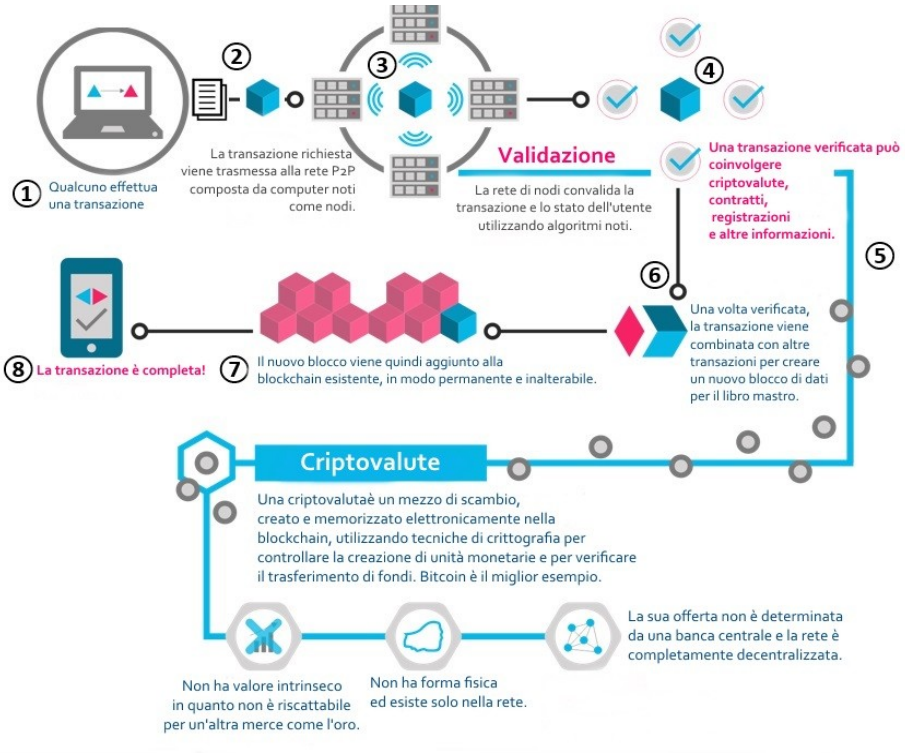
Per poter eseguire transazioni sulla blockchain, è necessario un *portafoglio* o **wallet**, un programma che consente di memorizzare e scambiare la propria moneta/valore. Ogni wallet o portafoglio è protetto da un metodo crittografico che utilizza una **coppia unica di differenti chiavi connesse**: una **chiave privata** e una **pubblica**.

Se un messaggio è crittografato con una chiave pubblica specifica, solo il proprietario della chiave privata abbinata sarà in grado di **decifrare e leggere il messaggio**. Quando David vuole inviare Bitcoin a Sandra, ha bisogno di farlo trasmettere un messaggio crittografato con la chiave privata del suo portafoglio. Ogni nodo nella rete può verifica che la richiesta di transazione provenga da David decifrando il messaggio di richiesta di transazione con la chiave pubblica del suo portafoglio.



Quando si crittografa una richiesta di transazione con la chiave privata del tuo wallet si generare una **firma digitale** che viene utilizzata dai computer blockchain per raddoppiare il controllo sulla fonte e l'autenticità della transazione. La firma digitale è una stringa di testo che è il risultato di una combinazione della ***richiesta di transazione*** e la ***chiave privata***, quindi non può essere utilizzata per altre transazioni. Se cambi un singolo carattere nel messaggio di richiesta di transazione, la firma digitale cambierà, quindi nessun potenziale attaccante può modificare le richieste di transazione o modificare la quantità di Bitcoin che stai inviando.

Ogni nodo nella blockchain sta mantenendo una copia del libro mastro. Quindi per conoscere il saldo del tuo portafoglio, devi analizzare e ***verificare tutte le transazioni che hanno mai avuto luogo sull'intera rete collegata al tuo portafoglio*** tramite i riferimenti che ha come input. Per semplificare e velocizzare il processo di verifica, i nodi di rete mantengono un record speciale di transazioni non spese. Grazie a questo controllo di sicurezza, si pone un argine al possibile problema del **double spending** ovvero del doppio utilizzo di una stessa quantità di valuta.



Validazione dei blocchi

Perché un nuovo blocco di transazioni sia aggiunto alla Blockchain è necessario appunto che sia
controllato, validato e crittografato. Solo con questo passaggio può poi diventare attivo ed essere
aggiunto alla Blockchain. Per effettuare questo passaggio è necessario che ogni volta che viene
composto un blocco venga validato ovvero vengano eseguiti **algoritmi di consenso distribuito** al fine di essere accettato da tutti i nodi di rete. Questa operazione viene definita, in base alla tipologia di algoritmo di consenso, come **mining** o **validazione** ed è svolta dai **miner** o **validatori**.
Generalmente gli algoritmi di consenso distribuito maggiormente diffusi sono il **Proof-of-Work** o **PoW** e il **Proof-of-Stake** o **PoS**.

Proof-of-Work

Hashcash (*SHA-256*) è la funzione Proof of Work utilizzata dal Bitcoin. La criptovaluta obbliga i miners a risolvere dei **problemi matematici estremamente complessi** e computazionalmente difficili per poter aggiungere blocchi alla blockchain. Tale funzione produce un tipo di dati molto specifici che vengono utilizzati per verificare che sia stata eseguita una notevole quantità di lavoro - da qui il termine ***Proof of Work***, in italiano "**prova di lavoro**".

Possiamo guardare alla Proof of Work come un lungo tentativo che alla fine produce un singolo pezzo di dati che si adatta all'interno del protocollo Bitcoin. Questo processo richiede molto tempo ed energia, ma i miners sono ampiamente ricompensati.

Proof-of-Stake

Nel modello di consenso ***Proof of Stake***, il numero di token di valuta digitale detenuti da ciascun utente, è determinante all'interno del sistema. Più grande è la partecipazione ("*stake*"), ovvero la quantità di token posseduti da un utente, maggiori sono le probabilità che non si stia violando il sistema.

I blocchi della Proof of Stake, a differenza dei blocchi della Proof of Work, non vengono estratti, ma **coniati**. I partecipanti che possiedono una **partecipazione significativa** nei sistemi Proof of Stake vengono selezionati su **base pseudocasuale** per coniare i blocchi e aggiungerli alla blockchain.

Il processo di selezione pseudocasuale entra in funzione dopo che il sistema ha analizzato diversi fattori al fine di garantire che siano selezionati solo gli individui con una quota maggiore, ma anche altri con una stake inferiore.

Nel caso in cui il processo di verifica dovesse rilevare un errore il blocco viene rifiutato e tutti hanno visibilità del fatto che la *transazione non è stata autorizzata*. Diversamente, se tutte le transazioni sono validate, il blocco viene creato e aggiunto ed entrerà a far parte della **Blockchain** (*della catena*) a tutti gli effetti come un **record permanente e immutabile**; nessun partecipante alla Blockchain potrà cambiarlo o rimuoverlo.

Esempio di manipolazione del blocco

Il blocco A contiene il numero 1, e il suo codice Hash è axf0. Il blocco successivo B contiene il numero 7 e il riferimento al blocco precedente, cioè axf0. Nel momento in cui un membro del network provasse a modificare il contenuto del blocco A (portando il valore da 1 a 2), l'Hash cambierebbe a sua volta da axf0 a, esempio, c47n. **Ma il blocco B ancora riporta axf0 come riferimento!** L'anomalia viene quindi immediatamente identificata.
Oltretutto, nel caso una parte terza volesse modificare l'intera blockchain, dovrebbe ricalcolare tutte le *Proof of Work* per evitare anomalie, azione che richiederebbe una ***potenza di calcolo al momento non disponibile*** se non tramite l'impiego, ancora teorico, della **computazione quantistica**.

È possibile, per diversi nodi, ***validare più blocchi contemporaneamente***, portando così ad una biforcazione della catena. In questo caso, i Miner lavorano per la validazione dei blocchi su entrambe le **biforcazioni** della catena ma, appena in una delle due viene validato ed aggiunto un nuovo blocco, tutti i miners che lavoravano sull'altra si spostano su quella a cui è stato aggiunto un blocco nuovo, trasformando così il blocco abbandonato in un **blocco orfano**. Questo accade perché l'obiettivo dei miner è quello di lavorare per **estendere la catena in lunghezza**.

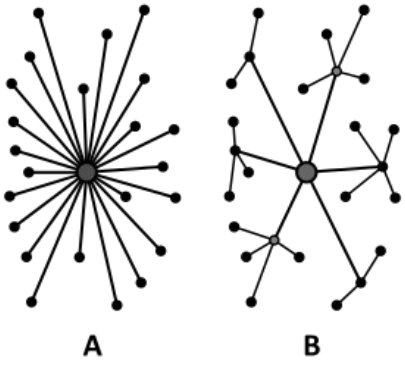
Decentralizzazione

Wikipedia riporta che con il concetto di decentralizzazione si indica il processo attraverso il quale le attività di un'organizzazione, in particolare quelle relative alla **pianificazione e al processo decisionale**, sono *distribuite* o *delegate* ***lontano*** da una posizione o **gruppo centrale di potere**.

Nella rete cripto, investitori e sviluppatori sono desiderosi di spingere per piattaforme decentralizzate di scambio; in questo modo, *nessun intermediario conduce il commercio* ma sono le comunità a poter prendere decisioni indipendenti e gestire sé stessi, **eliminando l'interferenza governativa**.

Pro

1. Apertura e trasparenza
Con un sistema decentralizzato, tutti i partecipanti interagiscono uno con l'altro. Non vi sono ***intermediari*** di media importanza per detenere fondi nel commercio. Aumenta quindi la **trasparenza** e di conseguenza i livelli di **fiducia** tra gli stessi partecipanti.



2. Maggiore sicurezza
Con **l'elevatissima integrazione** e **interazione** dei partecipanti, la possibilità di un attacco da parte di un hacker di sistema è molto bassa; l'hacker deve passare attraverso tutti i sistemi dei partecipanti per hackerare un singolo cripto-network, rendendo il tentativo più difficile di prima.

3. Consenso

Tutti i partecipanti prendono le proprie ***decisioni in accordo*** tra loro, al contrario dei sistemi centralizzati in cui ognuno è controllato da una sola parte e alcune decisioni sarebbero prese anche se non fossero necessariamente positive per tutti.

4. Velocità ed efficienza
Un partecipante al mercato che negozia direttamente tra loro in piattaforme decentrate è più **veloce** ed **efficiente**. Qui non esistono processi e protocolli intermedi che avrebbero altrimenti rallentato il processo di trading.

Contro:
1. Complesso ed elaborato
Nella loro funzionalità, i sistemi decentralizzati sono difficili da costruire e richiedono quindi un grande sforzo per comprenderli ed eventualmente utilizzarli.

2. Non completamente sviluppato
Mentre parliamo, il decentramento è una tecnologia in via di sviluppo con molte potenzialità, in contrapposizione a sistemi centralizzati già ben sviluppati.

Blockchain pubbliche e private

Blockchains pubblici
Protocolli blockchain allo stato dell'arte basati su algoritmi di consenso Proof of Work (PoW) sono *open source* e *non autorizzati*. Chiunque può partecipare, **senza permesso**. Chiunque può scaricare il codice e avviare l'esecuzione di un nodo pubblico sul proprio dispositivo locale, ***convalidare le transazioni*** nella rete, partecipando così al processo di consenso. Chiunque nel mondo può inviare transazioni attraverso la rete e aspettarsi di vederle incluse nella blockchain se sono valide. Chiunque può leggere la transazione sul blocco pubblico. Le transazioni sono *trasparenti, ma anonime / pseudonimi*.

Blockchains privati
Le autorizzazioni di scrittura vengono mantenute ***centralizzate in un'unica organizzazione***. Le autorizzazioni di lettura possono essere pubbliche o limitate a un livello arbitrario. Le applicazioni di esempio includono la gestione del database, il controllo, ecc. Le blockchain private sono un modo per sfruttare la tecnologia blockchain impostando ***gruppi e partecipanti*** che possono verificare le transazioni internamente. Questo ti *mette a rischio di violazioni della sicurezza come in un sistema centralizzato*, al contrario della blockchain pubblica garantita da meccanismi di incentivazione teorica del gioco. Tuttavia, le blockchain private hanno il loro caso d'uso, specialmente quando si parla di ***scalabilità e conformità dello stato delle regole sulla privacy dei dati e di altre questioni normative***.

Smart Contract

Nel 1994 **Nick Szabo**, crittografo ed esperto di diritto, si rese conto che il **registro decentralizzato** poteva essere utilizzato per gli **smart contract** o **self-executing contracts**, contratti blockchain o contratti digitali. In questo formato, i contratti possono essere convertiti in un ***codice informatico***, archiviati e replicati sul sistema e supervisionati dalla rete di computer collegati nella blockchain. Questo meccanismo risulta in un ***feedback continuo*** che va dal trasferimento di denaro alla ricezione del prodotto o servizio.

Lo Smart Contract ha bisogno di un supporto legale per la sua stesura, ma non ne ha bisogno per la sua verifica e per la sua attivazione. Lo **Smart Contract fa riferimento a degli standard di comportamento e di accesso a determinati servizi.** Uno Smart Contract è la "*traduzione*" o "*trasposizione*" in *codice* di un contratto in modo da verificare in automatico

l’avverarsi di ***determinate condizioni*** (*controllo di dati di base del contratto*) e di ***autoeseguire*** in automatico azioni (*o dare disposizione affinché si possano eseguire determinate azioni*) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate. In altre parole, lo Smart Contract è basato su un codice che “*legge*” sia le *clausole* che sono state concordate sia la condizioni operative nelle quali devono verificarsi le condizioni concordate e si autoesegue nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate. Esistono due tipologie di smart contract:

- **Smart Legal Contract** (*Contratti Intelligenti di tipo Legale*)
  Qui il **contenuto legale** del contratto intelligente è essenziale. Pensiamo alla certificazione notarile di un documento o al trasferimento della proprietà di un certo dominio internet al verificarsi di determinate condizioni (ad es. l’accredito di un bonifico, eseguito dalla banca del compratore, sul conto corrente del venditore).

- **Smart Code Contract** (*Contratti software privi di contenuto legale*)
  In questo caso ci troviamo di fronte ad un programma che in maniera **atecnica** viene chiamato con il nome di **contratto intelligente**. Ipotizziamo di sviluppare uno Smart Contract che gestisce, tramite l’IoT, la temperatura presente nella nostra abitazione al variare di quella esterna.

I vantaggi degli smart contract

1

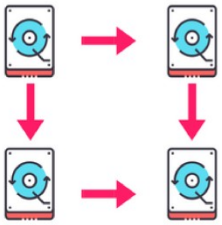
Indipendenza

Sei tu stesso a realizzare la transazione, senza dover passare da un notaio o da un avvocato

2

Fiducia

I tuoi documenti vengono criptati su un registro distrubuito



3

Sicurezza

Nella blockchain i tuoi documenti vengono duplicati molte volte

4

Risparmio

Gli smart contract aiutano a risparmiare denaro, perché annullano la necessità di intermediari

5

Precisione

Gli smart contract non solo fanno risparmiare tempo e denaro, ma evitano anche gli errori che nascono dal compilare manualmente moduli e documenti

STACCO A SISTEMI:

Alla base della fiducia vi è la possibilità di *verifica univoca*, di riconoscimento immediato: nella tecnologia implementata dalla Blockchain l'applicazione diretta di tale ***dogma*** è racchiusa nell'utilizzo di una particolare categoria di funzioni definite **funzioni di hash crittografiche**.

Si tratta di un **algoritmo matematico** che mappa dei dati di lunghezza arbitraria (messaggio) in una stringa binaria di dimensione fissa chiamata valore di hash, ma spesso viene indicata anche con il termine inglese **message digest** (o semplicemente ***digest***). Tale funzione di hash è progettata per essere unidirezionale (*one-way*), ovvero difficile da invertire.

Una funzione di **hash crittografica** è una classe speciale di funzioni hash che ha varie proprietà che lo rendono ideale per la **crittografia**. Ci sono alcune proprietà che una funzione hash crittografica deve avere per essere considerata sicura. Esaminiamole una per una:

- **Proprietà 1**: **deterministico**

  Ciò significa che non importa quante volte si passa un particolare *input attraverso una funzione di hash*: **si otterrà sempre lo stesso risultato**. Questo è fondamentale perché se ottieni diversi hash ogni volta sarà *impossibile tenere traccia dell'input*.

- **Proprietà 2**: **calcolo veloce**

  La funzione di hash dovrebbe essere in grado di ***restituire rapidamente l'hash di un input***. Se il processo non è abbastanza veloce, il sistema semplicemente non sarà efficiente.

- **Proprietà 3**: **resistenza pre-immagine**

  Quali stati di resistenza pre-immagine è che dato **H(A)** non è fattibile determinare **A**, dove A è l'input e H (A) è l'hash dell'output. Si noti l'uso della parola "***non fattibile***" anziché "*impossibile*". Sappiamo già che non è impossibile determinare l'input originale dal suo valore hash. Facciamo un esempio:

  Supponiamo che stai tirando un dado e che l'uscita sia l'hash del *numero* che esce dai dadi. Per determinare il numero generato originariamente è necessario scoprire gli **hash di tutti i numeri da 1 a 6 e confrontarli**. Poiché le funzioni di hash sono ***deterministiche***, l'hash di un input particolare sarà sempre lo stesso, quindi puoi semplicemente confrontare gli hash e scoprire l'input originale.

  Ma funziona solo quando la quantità data di dati è molto inferiore. Con *un*'***enorme quantità di dati***, come ad esempio un **hash a 128 bit**, l'unico metodo che devi trovare l'input originale è usando il "**metodo di forza bruta**" ovvero prendere un input casuale e confrontare l'output con l'hash di destinazione e ripetere fino a trovare una corrispondenza.

  Quindi, è possibile identificare **tre casi tempistici** di forza bruta:

  - **Scenario migliore**: ottieni la tua risposta al primo tentativo. Le probabilità che ciò accada sono *astronomiche*.
  - **Scenario peggiore**: ottieni la tua risposta dopo $\mathbf{2^{128} - 1}$ **volte**. Fondamentalmente, significa che troverai la tua risposta alla fine di tutti i dati.
  - **Scenario medio**: lo troverai da qualche parte nel mezzo quindi fondamentalmente dopo $2^{128}/2$ = **2127 volte**. Per metterlo in prospettiva, 2127 = 1,7 x 10^{38}. Quindi è possibile interrompere la *resistenza pre-immagine* tramite il metodo della forza bruta, ci vuole così ***tanto tempo*** che non ha importanza.

- **Proprietà 4: modifiche nell'input modifica l'hash**

  Anche se fai un piccolo cambiamento nel tuo input, ***le modifiche che si rifletteranno nell'hash saranno enormi***. Questa è una funzione critica perché questa proprietà dell'hash porta a una delle più grandi qualità della blockchain, la sua immutabilità.

- **Proprietà 5: resistenza alla collisione**

  Dati due diversi input **A** e **B** dove **H(A)** e **H(B)** sono i loro rispettivi hash, è **impossibile** che ***H(A)*** sia uguale a ***H(B***). Ciò significa che per la maggior parte, ogni input avrà il proprio hash unico. Perché abbiamo detto "per la maggior parte"? Parliamo di un concetto interessante chiamato "***The Birthday Paradox - Il paradosso del compleanno***".

  Cos'è il paradosso del compleanno?
  Se incontri uno sconosciuto per caso nelle strade, è **molto improbabile** che entrambi abbiate lo **stesso compleanno**. Infatti, supponendo che tutti i giorni dell'anno abbiano la stessa probabilità di avere un compleanno, le probabilità che un'altra persona condivida il tuo compleanno è **1/365**, che è dello **0,27%.**

  Tuttavia, se si riuniscono ***20-30 persone in una stanza***, le probabilità di due persone che condividono lo stesso compleanno risalgono astronomicamente. In effetti, c'è una probabilità **50-50** per 2 persone di condividere lo stesso compleanno in questo scenario.

  È a causa di una ***semplice regola in probabilità*** che va come segue: supponiamo che ci siano **N diverse possibilità** che qualcosa accada, quindi ***la radice quadrata di N elementi casuali calcolerà una probabilità del 50% di collisione***.

  Quindi, applicando questa teoria per i compleanni, si hanno 365 diverse possibilità di compleanni, quindi la radice di 365 restituisce 23, il numero di persone da scegliere a caso per il 50% di possibilità che due persone condividano i compleanni.

  Qual è l'applicazione dell'hashing?

  Supponiamo di avere un **hash a 128** bit che ha 2^{128} possibilità diverse. Usando il paradosso del compleanno, si ha una probabilità del 50% di rompere la resistenza di collisione su sqrt (2^{128}) = 264esima istanza.

  Come si può vedere, è molto più facile **spezzare la resistenza alle collisioni** che non rompere la resistenza alla pre-immagine. Nessuna funzione hash è *esente da collisioni*, ma di solito impiega tanto tempo a trovare una collisione. Quindi, se si usa una funzione come SHA-256, è sicuro assumere che se ***H(A) = H(B)*** allora A = B.

- **Proprietà 6: Puzzle amichevole**

  Per ogni uscita "**Y**", se k viene scelto da una distribuzione con **alta entropia minima** non è possibile trovare un input **x** tale che **H (k | x) = Y**.

  Con il termine ***alta entropia minima*** si indica che la distribuzione da cui viene scelto il valore è enormemente distribuita al punto che scegliere un valore casuale ha una *probabilità trascurabile*. Fondamentalmente, se ti è stato detto di scegliere un numero compreso tra 1 e 5, questa è una **distribuzione a bassa entropia minima**. Tuttavia, se dovessi scegliere un numero compreso tra 1 e un miliardo, si tratta di una ***distribuzione ad alta entropia minima***. Il segno "|" indica la **concatenazione** quindi la definizione

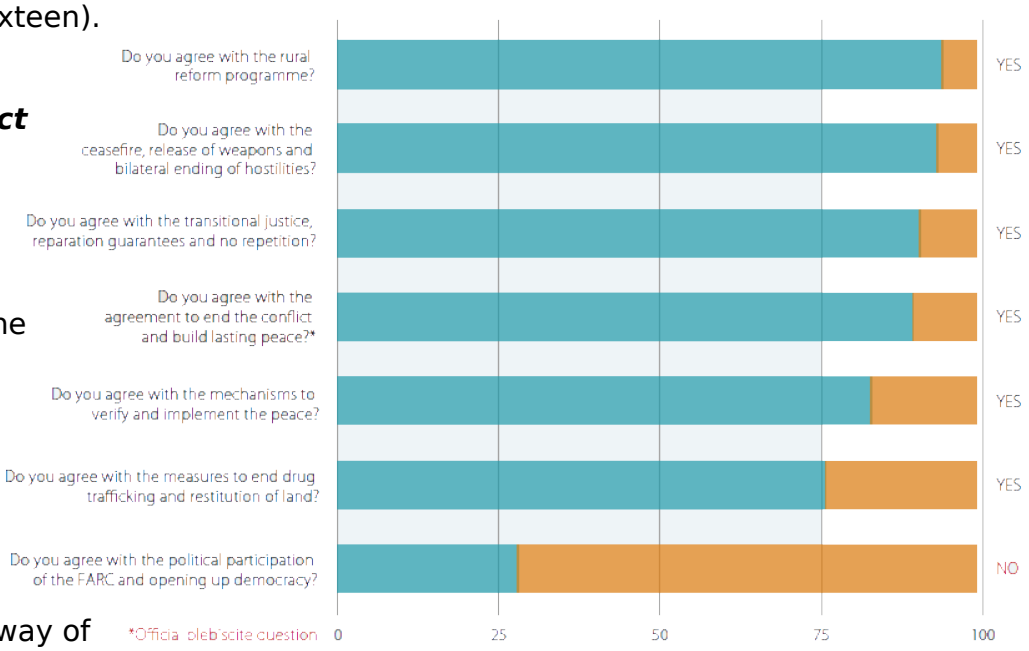
indicherà che se si sceglie un valore casuale "k" da una vasta distribuzione, non è possibile trovare un valore X tale che l'hash della concatenazione di k e x darà l'output Y.

STACCO AD INGLESE: As our societies grew more complex and our trade routes grew more distant, we **built up more formal institutions** like banks for currency, governments, corporations, etc.

These institutions helped us manage our trade as the complexity grew, and **our personal control was much lower**. With the internet, we put these same institutions online.
We are now entering in a **radical evolution** of how we interact and trade, because for the first time, we can lower uncertainty not just with political and economic institutions but we can do it with technology.

CASE STUDY: Blockchain Voting for Peace in Colombia
In order to give Colombian expatriates a voice in a **2016 (two thousand and sixteen) Peace plebiscite** and test the potential of Blockchain technology in electoral processes, the tech non-profit *Democracy Earth Foundation* set up a digital process that allowed Colombian expats, who were unable to vote through the official process, an opportunity to participate in a plebiscite to approve the peace treaty. This process raised interesting questions for governments about the future use of blockchain in electoral processes and could potentially lead to new ways to ensure the integrity of the election process.

THE PROBLEM
Only *six hundred thousand* of the 6 million Colombians living abroad had the right to vote at the consulate of their countries of residence, because they voted there during previous elections.
This ***could limit the ability of Colombians living abroad*** to vote in the historic plebiscite on the peace treaty between the **Colombian Government** and **FARC**, held on 2 October 2016 (two thousand and sixteen).
The FARC was a guerrilla movement involved in the ***Colombian armed conflict*** from 1964 (nineteen sixty-four)



AN INNOVATIVE SOLUTION
Against this background, the tech non-profit Democracy Earth Foundation launched the digital **voting platform Plebiscito Digital** (*Digital Plebiscite*). The Digital Plebiscite was powered by blockchain technology, testing a new way of validating and authenticating electoral votes. **Blockchain** is a database that enables the transfer of value within computer networks.

Democracy Earth also wanted to experiment with a **different concept of democracy**: *liquid democracy*. Instead of giving citizens the choice between voting “Yes” or “No” to support the peace treaty, each voter could vote on **sub-themes** of the proposed peace treaty and indicate the relative importance of each one.

IMPACT AND RESULTS

The pilot has launched a discussion in the Colombian media about the potential of blockchain technology for voting and the value of the concept of liquid democracy.
Additionally, the initiative has been adopted by "***The Net Party***" (*Partido de la Red Colombia*), which is now promoting the idea of blockchain voting through social media.
Blockchain could disrupt voting, just as it has currency, and could apply to any democratic government, bringing the expression of democracy in the entire world to a new level of representation.

STACCO A STORIA: La crescita esponenziale di Bitcoin, legata strettamente alle tecnologie *blockchain-based*, resta la più repentina delle **espansioni tecnologico-economiche** dell'ultimo secolo. Resta da capire se i bitcoin sono una bolla oppure no. Peccato che anche su questo aspetto gli esperti siano divisi: chi ritiene che siano solo un ***bene speculativo*** che non ha un vero utilizzo nel mondo (oppure estremamente limitato) e chi invece pensa che diventeranno uno ***strumento economico*** sempre più frequentemente utilizzato, magari per gli scambi internazionali.

Uno degli economisti più critici nei confronti dei bitcoin è **Paul Krugman**, *premio Nobel nel 2008*. È dal 2013 che Krugman sminuisce l'importanza dei bitcoin, considerati una "*fantasia libertariana e antigovernativa*".

In molti paragona la "bolla Bitcoin" al ***crash di Wall Street del 1929*** identificando l'ottimismo spregiudicato e incosciente in tale tecnologia lo stesso degli anni venti del *tracollo finanziari di Wall Street*, nel rapido aumento dell'interesse per i mercati e la loro relativa, poi giunta all'apice, **attività speculatrice**. Per comprenderne il paragona è necessario approfondire l'ambiente economico durante il corso degli anni Venti.

Situazione economica degli anni venti
Negli anni venti l'economia statunitense, uscita dalla ***recessione post-bellica del 1920-1921***, entrò in una fase di **prosperità ed espansione**. La produzione e l'occupazione aumentarono in maniera consistente, mentre i salari crescevano poco ed i prezzi si mantenevano stabili, consentendo alle imprese di aumentare i loro profitti.

Proprio gli aumentati profitti delle imprese statunitensi e le prospettive di un loro ulteriore aumento diedero il via alla **speculazione in borsa** della seconda metà del decennio, in un clima di forte ottimismo e fiducia, indispensabile affinché si sviluppi un boom. I crescenti investimenti in borsa furono facilitati dal ***credito facile***.

In quel periodo, i capitali da investire negli USA erano abbondanti. La causa remota è fatta risalire al 1925 quando la Gran Bretagna decise di **tornare al sistema aureo**, un cambio ampiamente sopravvalutato. Ciò rese la Gran Bretagna un luogo conveniente per le esportazioni, mentre era conveniente investire negli Stati Uniti. Così un ***crescente flusso di denaro si diresse verso gli USA***, investito prevalentemente in **titoli pubblici** (titoli di stato emessi per finanziare il debito pubblico), lasciando grosse somme di denaro nelle mani delle banche e dei risparmiatori che li vendettero.

Infine, occorre sottolineare che il basso **tasso di sconto** rendeva conveniente per le banche statunitensi prendere denaro in prestito dal **Federal Reserve System**, il sistema bancario statunitense, per prestarlo a loro volta a chi desiderasse investire in borsa. Fu così che a partire dal secondo semestre del 1924 la **Borsa di New York** cominciò a crescere, trend che continuò per tutto l'anno successivo. Alla fine del 1927 il valore dell'indice industriale del **New York Times** era quasi raddoppiato.

La speculazione del 1928-29

La natura del boom cambiò nel 1928 quando ***l'andamento del mercato azionario si staccò da quello dell'economia reale*** e dalle plausibili prospettive di aumento degli utili societari. Il mercato assunse anche un **andamento spettacolare**, con un andamento altalenante all'interno di una tendenza fortemente crescente.

Tuttavia, il normale investimento azionario aveva lasciato il posto alla **speculazione**: si acquistavano azioni per ***rivenderle quando il loro prezzo fosse sufficientemente salito***, non per detenerne la proprietà e godere dei dividendi. Ciò era particolarmente evidente dal modo con il quale le azioni venivano acquistate.

Si trattava di **acquisiti su margine**. L'investitore prendeva il denaro necessario all'acquisto in prestito dalle banche a tassi dell'8-10% e forniva in garanzia una percentuale in contante e il valore dei titoli stessi, con la clausola che se il loro valore fosse sceso *sotto un certo margine* avrebbe dovuto versare **nuovo contante**. Poi l'investitore affidava i titoli all'agente di cambio che si occupava di rivenderli a prezzi aumentati in modo da pagare il prestito e lasciare un guadagno consistente nelle tasche dell'investitore.

Poiché il tasso di sconto della Federal Reserve era del 5%, le banche ***trovavano conveniente prestare denaro agli speculatori***, perché in una situazione di mercato crescente si trattava di un *tipo di prestito molto garantito*. Persino le imprese statunitensi trovavano conveniente investire i propri residui attivi in questi prestiti *piuttosto che effettuare investimenti in beni capitale*. Indice di ciò è l'enorme **aumento dei prestiti ai borsisti**, che passarono da 1 miliardo di dollari nel 1920 ai 6 miliardi alla fine del 1928, ***arrivando fino a* 7 miliardi *nell'autunno del crollo***.

All'inizio del 1929, in pochi si rendevano conto che la fine del boom era vicina. A tale proposito è ***significativo il discorso sullo Stato dell'Unione*** pronunciato il 4 dicembre 1928 dal **Presidente uscente Coolidge** elogiativo della condizione economica del Paese, rimarcando gli sforzi e l'intelletto della popolazione Statunitense e del diffuso benessere che questi avevano creato per la formazione di una società libera e giusta.

Il nervosismo iniziò a manifestarsi sul mercato a marzo. Intorno alla metà del mese, si apprese che il **Federal Reserve Board** teneva riunioni quotidiane a **Washington D.C**. *senza rilasciare alcuna dichiarazione*. Così, il lunedì 25 marzo impauriti dal silenzio della Banca centrale gli **investitori iniziarono a vendere**. Il giorno dopo le cose peggiorarono ulteriormente, con tassi di interesse fino al 20%. Fu allora che intervenne a salvare la situazione **Charles Mitchell**, *uno dei direttori della Federal Reserve Bank of New York*. Egli dichiarò che la sua banca avrebbe prestato agli investitori il denaro necessario a fermare la crisi, anche ***ricorrendo a fondi presi in prestito dalla Federal Reserve***. Poiché il Federal Reserve Board di Washington non prese posizione, il mercato si rassicurò e nei giorni successivi tornò a crescere.

Dopo questa crisi, il mercato crebbe costantemente per tutta l'estate. Nelle parole dei politici, dei banchieri, degli studiosi, della stampa e della gente l'ottimismo era evidente. Solo alcuni accademici, il New York Times e le agenzie **Standard Statistics e Poor's** (*oggi note come Standard & Poor's*) **rimanevano scettici**, ma essi erano inascoltati. La borsa veniva considerata sempre meno come un registro a lunga scadenza delle prospettive aziendali e sempre più come il **prodotto di manovre speculative e artificiose**.

Le holding e gli investment trust

In quegli anni, viste le potenzialità offerte dal mercato finanziario, vi fu **un'emissione enorme di nuovi titoli azionari**, con la fondazione di moltissime nuove società. Una parte di queste emissioni serviva a finanziare una nuova ondata di **fusioni**. Veniva costituita una holding che emetteva azioni per raccogliere il denaro necessario ad acquisire le compagnie di gestione locali. Spesso, però, finì con il crearsi un ***complesso sistema piramidale di holding che a loro volta controllavano altre holding***. Altro caso, riguardante la vendita di beni di consumo al dettaglio, i cinema, i grandi magazzini, consisteva nel creare grandi catene. L'emissione di azioni era necessaria per costituire nuove ramificazioni territoriali.

Un'altra struttura societaria che si diffuse molto nei tardi anni venti negli Stati Uniti fu **l'investment trust**. Esso era l'equivalente di una moderna società di investimento, che ***raccoglieva il denaro*** mediante la vendita delle proprie azioni e obbligazioni per ***poi***

investirlo nell'acquisto di un portafoglio di azioni di altre società già esistenti. Nel 1921 ne esistevano solo una *quarantina* per poi arrivare a 751 nell'ottobre del 1929.

L'inizio della fine
Il **3 settembre 1929** fu il giorno in cui finì la grande corsa al rialzo. Dopo il 3 settembre il mercato prese un andamento irregolare, a volte sostenuto a volte fiacco, con una **tendenza discontinua ma nel complesso decrescente**.

La prima flessione si verificò il 5 settembre e fu definita ***flessione Babson*** perché fece seguito alle dichiarazioni dello statistico americano **Roger Babson** che *la crescita del marcato azionario non poteva continuare e prima o poi si sarebbe avuto un crollo*. Il giorno successivo il mercato si riprese, ma la tendenza era segnata.

Negli anni successivi al crollo si indicarono solitamente **due fatti** come **scatenanti il disastro dell'ottobre 1929.** Il *primo* fu il ***fallimento***, il 20 settembre *dell'impero industriale dall'americano Clarence Hatry*, in seguito alla scoperta che egli ***aveva alterato la consistenza patrimoniale delle sue società falsificando i certificati azionari***. Il *secondo* fu il ***rifiuto*** da parte del Dipartimento dei servizi pubblici del Massachusetts di autorizzare la *divisione in quattro delle azioni della compagnia locale dell'elettricità*, la Boston Edison, ***dichiarando anche che il titolo aveva un prezzo troppo elevato rispetto alle reali condizioni dell'impresa***.

Il lunedì ci furono ***forti ribassi*** e si scambiarono oltre 6 milioni di azioni. Martedì ci fu un lieve recupero, anche in seguito a dichiarazioni di Mitchell nelle quali si affermava che le perdite si erano spinte troppo oltre. Mercoledì, tuttavia, vi furono **grandi perdite**.

Si giunse così a **giovedì 24**, il cosiddetto **Giovedì nero**, non tanto per l'entità delle perdite quanto per le ***scene di panico che caratterizzarono la giornata***. Furono 12 milioni le azioni che cambiarono di mano, a prezzi via via più bassi, gettando nella disperazione molti risparmiatori e investitori. Mezz'ora dopo il mercato era in preda alla psicosi, si verificarono vere e proprie **vendite da panico** (*panic selling*), negli ambienti dello **Stock Exchange**, sede della borsa valori, si respirava un'aria di profondo nervosismo, *mentre già si diffondeva la voce che undici noti speculatori si fossero tolti la vita*.

Al termine di una riunione negli uffici della **J.P. Morgan & Chase** in cui si erano riuniti tra i più importanti banchieri newyorkesi, **Thomas W. Lamont**, numero uno della Morgan dichiarò che i grandi banchieri sarebbero intervenuti per ***calmierare la discesa dei prezzi***.

Dopo una lieve ripresa nel fine settimana, si giungerà così al **martedì 29 ottobre**, *il giorno più rovinoso di tutta la storia dei mercati azionari*.
Il "**Martedì nero**", **29 ottobre 1929**, furono scambiate 16,4 milioni di azioni. La ***famiglia Rockefeller*** e ad altri giganti finanziari ***si unirono per comprare grosse quantità di azioni*** in modo da dimostrare al pubblico la loro fiducia nel mercato, *ma i loro sforzi non riuscirono a fermare la discesa*. Il **Dow Jones** perse un altro 12% quel giorno. L'orologio finanziario non si fermò sino alle 19:45 in quella sera, il mercato perse 14 miliardi di dollari di valore, portando la **perdita della settimana a 30 miliardi**, ***dieci volte di più del budget annuale del governo federale degli Stati Uniti***, molto più di quanto gli stessi spesero in tutta la prima guerra mondiale.

Come si verifica in tutte le situazioni di "***bolla finanziaria***", basate su speculazione ed euforia, il mercato prima o poi torna in equilibrio e questo accade con una spinta emotiva alle vendite incontrollate pari d'intensità, ma di *segno opposto*, a quella che ne sorregge gli acquisti in precedenza; in poche parole, l'euforia che origina la bolla viene ad essere seguita da **fenomeni di panico** che ne decretano lo ***scoppio***.

L'economia statunitense si risollevò totalmente da tale crisi unicamente con la ***crescita della produzione industriale*** dovuto allo scoppio della **Seconda Guerra Mondiale** e all'aumento della produzione bellica.

STACCO AD ITALIANO: In ambito letterario, testimonianza dell'avversione per la crescente complessità tecnologica del proprio tempo e per il crescente degrado morale che questa ha portato in ogni ambito delle attività umane, è dato dall'espressione della poesia montaliana e dai suoi diari risalenti al '71 e al '72.

Eugenio Montale nasce a **Genova** il ***12 ottobre 1896*** da una famiglia di *agiati commercianti*. Dopo aver iniziato l'istituto tecnico è costretto a interrompere la scuola per ***problematiche di salute***, studiando da autodidatta e diplomandosi nel 1915. Durante il periodo scolastico si forma una solida cultura grazie a letture approfondite ed eterogenee di ***romanzi inglesi*** oltre che di *Leopardi, Baudelaire* e altri poeti liguri contemporanei.
Nel 1917 frequenta il corso per allievi ufficiali a Parma divenendo sottotenente e combattendo come volontario in **Vallarsa**, nel Trentino. Congedato nel luglio del 1919 torna a Genova, trascorrendo le stagioni estive nella villa di famiglia a *Monterosso*, un paese delle ***Cinque Terre***, in Liguria.

Il periodo fiorentino
Nel 1927 Montale si trasferisce a Firenze divenendo nel '29 direttore del *Gabinetto letterario Vieusseux*, importante istituzione culturale fiorentina dalla quale verrà espulso nel 1938 per il ***rifiuto di iscrizione*** al Partito fascista. A Firenze Montale si avvicina ai poeti ermetici e scrittori quali *Vittorini, Gadda e Contini* che lo inducono ad approfondire lo studio della **letteratura dantesca**.

A partire dal 1933 si lega sentimentalmente alla *giovane ebrea americana* **Irma Brandeis**, costretta poi nel 1938 alla fuga negli Stati Uniti a causa *dell'emanazione delle leggi razziali*. A lei il poeta dedica la sua seconda raccolta **Le Occasioni** (1939).

La guerra, il periodo milanese e l'ultimo Montale
Nel 1939 Montale va a vivere con **Drusilla Tanzi** (detta **Mosca**), che tuttavia sposerà solo nel 1962. Nel 1948 su trasferisce a Milano, dove diventa redattore del "*Corriere della Sera*".

La crescente fama dell'autore consegue a ***riconoscimenti pubblici*** quali *lauree ad honorem* presso le università di Milano, Roma e Cambridge oltre al premio Feltrinelli presso l'Accademia dei Lincei. Alla maggiore dimensione pubblica dell'autore si accompagna un ***progressivo silenzio poetico***. Negli anni del boom economico Montale è ***scettico*** sull'utilità della poesia in una società dominata dal potere del denaro e dei media. Pausa terminata negli anni Sessanta con la pubblicazione di ***Xenia***, composta in memoria della moglie Drusilla Tanzi.

Nel 1975 la fama dell'autore raggiungere il suo **apice** grazie al conferimento del **premio Nobel per la letteratura** valsogli «*per la sua poetica distinta che, con grande sensibilità artistica, ha interpretato i valori umani sotto il simbolo di una visione della vita priva di illusioni*». Eugenio Montale muore a Milano la sera del **12 settembre 1981**.

Pensiero e poetica
La ***produzione montaliana*** copre un ampio arco cronologico - *dal 1920 al 1980* - e attraversa tutte le *principali correnti poetiche del Novecento* pur senza identificarsi in modo esclusivo con nessuna di esse.

Il male di vivere
La visione del mondo di Montale è caratterizzata da un **lucido disincanto**, che si traduce in **forme di radicale pessimismo**. Interprete di una sensibilità prettamente novecentesca, il poeta guarda al mondo come a un insieme di eventi casuali e insensati, non sorretti da alcun principio unificante e **dominati dal dolore e dalla sofferenza**. Di fronte a questa realtà, l'uomo avverte una profonda **inadeguatezza** e una *sensazione di disarmonia*, un angoscioso "male di vivere" che nasce dalla *consapevolezza di un'esistenza priva di senso e finalità*, non lenita neppure dalla fede religiosa.

La funzione poetica e il "varco"

A tale visione negativa si accompagna una **nuova concezione del compito della poesia**. Il poeta non è in grado di offrire soluzioni positive o dissimulare il disagio individuale e collettivo; egli ha invece il compito di ***registrare il male di vivere e farsi testimone della dignità umana nel suo sforzo di sopravvivere al caos universale***. La sua è una poesia scabra ed essenziale, che trasferisce il dolore in oggetti e situazioni concrete attraverso immagini asciutte e antiretoriche.

Nonostante tale visione pessimistica, tuttavia, Montale non approda mai ad un vero ***nichilismo*** poiché, pur constatando l'insensatezza dell'esistenza, resiste in lui una ***fiducia residua nella possibilità di cogliere il senso della realtà***, attingendo all'autenticità della vita. Montale si nutre quindi della speranza di individuare, tramite un evento "***miracoloso***" e casuale, il "**varco**", permettendo di cogliere una **verità definitiva**. Tale tensione è destinata a rimanere frustrata poiché il *significato ultimo della realtà sfugge sempre, rendendo più cocente la sconfitta e amaro il pessimismo.*

La poetica degli oggetti

La visione dell'autore si esprime tramite una poetica fondata su elementi concreti e quotidiani, definita "**correlativo oggettivo**" e rielaborata dal *poeta anglo-americano* **Thomas S. Eliot**. Montale si propone di rappresentare oggetti e situazioni concrete non con uno scopo descrittivo o realistico, ma come ***equivalenti di precisi stati d'animo e sentimenti***, che assumono una valenza universale. Tale tecnica conferisce ai versi di Montale una concretezza che tuttavia *non esclude l'oscurità*. Il poeta, infatti, non rende esplicito il legame tra l'oggetto e la sensazione che vi si collega ma *lascia al lettore il compito di decifrarne il significato*.

Evoluzione dello stile

Montale delinea un ***originalissimo percorso stilistico***, in aperta opposizione all'estetica del poeta-vate. L'autore sceglie un *linguaggio volutamente dissonante*, che si colloca nel solco della tradizione dantesca (il Dante petroso e le rime infernali). Il registro è quello di una **quotidianità ricercata ed essenziale**, che sa accogliere anche *termini aulici o specialistici*.

Sulla spiaggia

Composta il **30 agosto 1972**, la poesia fu inserita nella raccolta *Diario del ’71 e del ’72*. Su una spiaggia della Versilia, il poeta si gode la tranquillità delle prime luci del mattino: nella pace dell’alba l’unica figura umana assume una valenza quasi metafisica, ma è un’illusione destinata a svanire con l’arrivo della ***moltitudine caotica dei bagnanti***.

Ora il chiarore si fa più diffuso.
Ancora chiusi gli ultimi ombrelloni.
Poi appare qualcuno che trascina
il suo gommone.
La venditrice d'erbe viene e affonda
sulla rena la sua mole, un groviglio
di vene varicose. È un monolito
diroccato dai picchi di Lunigiana[3].
Quando mi parla resto senza fiato,
le sue parole sono la Verità.
Ma tra poco sarà qui il cafarnao
delle carni, dei gesti e delle barbe.
Tutti i lemuri umani avranno al collo
croci e catene. Quanta religione.
E c'è chi s'era illuso di ripetere
l'exploit di Crusoe![4]

3. Lunigiana: regione della Toscana compresa tra la Versilia e le Alpi Apuane.

4. exploit di Crusoe: in riferimento all'impresa di Robinson Crusoe, protagonista del romanzo di Daniel Defoe che naufraga su un'isola deserta.

L'atmosfera iniziale della lirica sembra preludere a un'improvvisa epifania, come accade in molte liriche precedenti del Montale, anche se la poetica del componimento vira decisamente verso tematiche quotidiane. In pochi versi la ***situazione spazio-temporale indefinita*** si popola di ***ombrelloni e gommoni***, preludio dell'imminente giornata di mare, ma l'attenzione è catturata da una figura femminile: la donna occupa interamente la scena non solo senso fisico ma anche in senso **metafisico**, poiché le sue parole, paragonate alla "Verità", riscuotono il poeta dalla sua tranquillità, lasciandolo senza fiato.

Sembra che il varco si presenti in **modo inaspettato agli occhi del poeta**: si tratta tuttavia solo di un momento, perché l'arrivo della folla lo riporta bruscamente alla realtà e gli fa pronunciare un'ironica considerazione sull'affollamento delle spiagge.

Proprio nei versi finale emerge con chiarezza l'atteggiamento di superiorità e disprezzo per i nuovi miti della contemporaneità. In un **disprezzo per la società contemporanea**, l'invasione dei bagnanti, indicati dispregiativamente come carni, gesti e barbe, allude alla spersonalizzazione dell'individuo nella società massificata. I gitanti sono ***paragonati a creare ultraterrene***, lemuri, che vagano nel mondo per tormentare i vivi, compreso, ovviamente, il poeta, che si era illuso di trovare un angolo tranquillo in cui attendere l'arrivo del giorno.

Il tono generale del componimento è *colloquiale e ricco di termini ed espressioni* tratte dal linguaggio quotidiano, ma inaspettatamente i versi sono impreziositi da un raro termine, cafarnao, in riferimento alla città ebraica di ***Kefar Nahum***, centro della predicazione di Gesù in cui avvennero i primi scontri tra giudei e sostenitori della nuova dottrina, indicante dunque calca e grande confusione, acuendo ancora di più la distanza tra la folla e il desiderio di pace e solitudine reclamato dall'io lirico.

STACCO EDUCAZIONE FISICA:

Già agli albori degli **anni Venti** l'ideologia fascista cominciò a plasmare le strutture economiche, politiche e sociali del paese, attuando una serie di mutamenti sia sociali quanto giuridici. Nell'ottobre del 1922 **Mussolini** consolidò il proprio potere con la ***marcia su Roma***, ottenendo il potere in Italia. Il consolidamento del potere fascista si ebbe nel 1925 anche con l'aiuto di innovazioni in ambito sportivo e disciplinare nell'educazione fisica.

Mussolini introdusse un **ordinamento monopolistico** non solo in ambito politico dunque, ma anche in ambito educativo, facendo presa sulle masse di giovani, "fascistizzando" gli ordinamenti educativi preesistenti e creandone di nuovi mirati alla formazione della *nuova generazione fascista*. Vennero soppresse le organizzazioni scoutistiche e sostituite dall'Opera Nazionale Balilla e dagli GUF (*Gruppi Universitari Fascisti*).

Il 3 aprile 1926 venne creata **l'Opera Nazionale Fascista** la quale dall'anno successivo avrebbe provveduto all'insegnamento dell'educazione fisica nelle scuole medie ed elementari. **Renato Ricci**, presidente dell'ONB, si batté per un'attività fisica più formativa che agonistica, in netto contrasto con la filosofia del CONI, fautori di campionismo e olimpismo. L'istituzione si basata sull'antico *concetto greco-romano* della sana educazione fisica legata all'esercizio intellettuale, aggiungendovi un carattere militaresco strettamente legato all'ideologia fascista.

Parallelamente al rinnovamento di tali strutture educative, lo sport durante il ventennio assunse un ruolo sempre più rilevante, venendo considerata al pari delle altre discipline scolastiche, e gli insegnati di ginnastica e iniziarono a far parte del consiglio dei professori: l'educazione fisica tuttavia nell'ottica fascista non doveva limitarsi solo alle strutture scolastiche ma doveva ***espandersi in tutta la società*** sotto forma di **strutture**

organizzative e militanti esterne. Nelle scuole vennero dedicate due ore settimanali all'insegnamento dell'educazione fisica e i programmi d'insegnamento prevedevano:

- **attività ginnica** a carattere ricreativo per le classi minori;
- **saluto romano**, saluto collettivo in classe e fuori, l'attenti, riposo e marcia di gruppo per le classi superiori;
- per i giovani tra i 16 e 18 anni inoltre erano previsti **esercizi a corpo libero e attrezzi**, lanci, corse piane ad ostacoli e marce non superiori ai 20 KM. Di fondamentale importanza era l'alternare all'allenamento individuale anche l'allenamento collettivo e l'utilizzo di **forme sportive mirate all'addestramento tattico-militare** (come i lanci, i quali avevano come fine ultimo testare l'ipotetico lancio di granate).

Gli sport di maggior successo durante il Ventennio furono prevalentemente mirati all'addestramento militare, tra cui:

- **Tiro a segno**, utile per l'addestramento alle armi dei giovani
- **Ginnastico**, sport di educazione e miglioramento fisico della razza
- **Scherma**, nella versione riavvicinata al combattimento romano
- **Atletica leggera**, basilare per la preparazione civica e militare dei giovani
- **Canottaggio**, per una maggiore capacità polmonare
- **Alpinismo**
- **Motorismo**, tra cui motociclismo, motonautica e aviazione, in grado di formare il carattere e dotare di conoscenze tecniche e di sopravvivenza in caso di vita o di morte.

Periodicamente si tenevano dei **saggi collettivi** che riunivano giovani da tutta Italia: l'obiettivo era puramente **propagandistico** ed esaltativo dei valori fondanti degli ideali fascisti di patria. Venivano svolti esercizi a corpo libero e di atletica, oltre che tennis o sci. Tali eventi si concludevano solitamente con un **discorso finale del Duce**. Dal 1929 venne poi istituito il **concorso Dux**, manifestazione di saggi ginnici svolta nei **campi Dux**.

La **Scuola fascista di educazione fisica**, erede degli Istituti di Magistero di Roma, Torino e Napoli chiusi nel 1923 a seguito della Riforma Gentile, iniziò i propri corsi il 7 febbraio 1928. Ospitato sin dall'inaugurazione presso **l'Accademia militare di educazione fisica della Farnesina**, l'istituto si trasferì nella sua sede definitiva al foro Mussolini nel novembre 1932. L'istituto avrebbe dovuto svolgere una funzione essenziale: formare gli insegnanti di educazione fisica delle scuole e gli *istruttori ginnico-sportivi dell'Opera nazionale balilla* (ONB). Le necessità contingenti però, ovvero la mancanza di dirigenti per l'organizzazione giovanile, spinsero il presidente Renato Ricci, a compiere delle scelte diverse. La Scuola assunse, infatti, il ruolo di centro per la **formazione della dirigenza maschile** delle organizzazioni giovanili fasciste.

A un anno dalla sua fondazione la scuola modificò nome diventando l'«Accademia fascista di educazione fisica». Ricci voleva che essa fosse il «più gigantesco esperimento di educazione di Stato» mai tentato sino ad allora per la formazione «in senso patriottico e unitario, cioè fascista», delle «classi più giovani di un popolo». L'istituto doveva garantire all'organizzazione giovanile fascista la **classe di educatori-dirigenti** di cui aveva bisogno.

Dal 1929 si evidenziò una maggiore politicizzazione della struttura, dei corsi e delle finalità. Si stabilì che l'iscrizione al partito fosse un requisito essenziale per poter fare domanda d'ammissione, che gli anni di «***anzianità fascista***», compresi quelli trascorsi nell'ONB, e l'aver rivestito cariche dirigenziali locali fossero un importante criterio di valutazione nella scelta finale dei candidati. Anche i programmi subirono delle modifiche. Venne dato, infatti, ***maggiore spazio all'educazione politico-sociale***, alla pedagogia e a tutte le materie

letterarie, filosofiche, storiche e giuridiche ritenute necessarie per formare dal punto di vista politico-ideologico i futuri capi giovanili fascisti.

Le materie all'interno dell'Accademia maschile, oltre allo studio di una lingua straniera, divenuta obbligatoriamente *tedesco* nell'ottobre 1940, vennero organizzate in **quattro sezioni**: **politica, militare, biologico-scientifica e ginnico-sportiva**. A differenza di tutti gli altri istituti superiori, il diploma dell'Accademia non veniva rilasciato in nome del Re Imperatore, ma **in nome del Duce**.

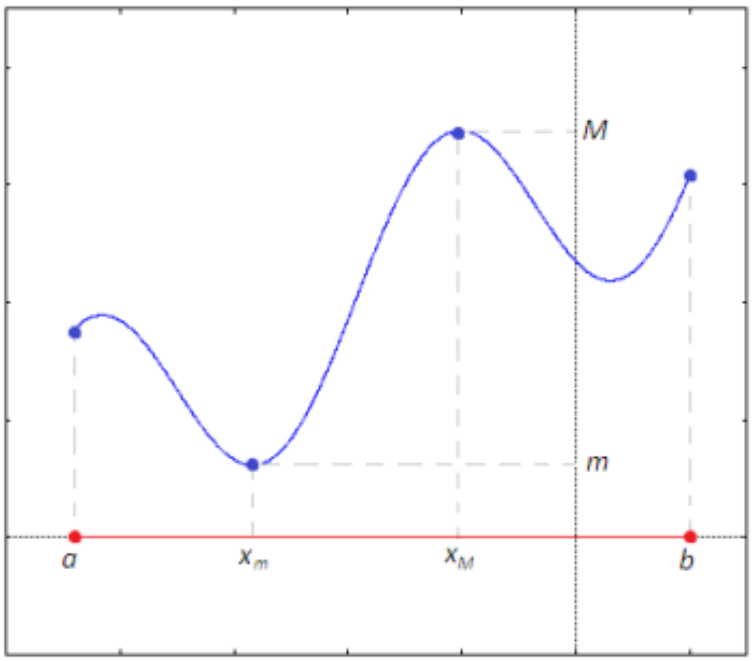
STACCO A MATEMATICA:
E' innegabile che oggi non parleremmo di progresso ed evoluzione senza uno dei principi cardine che da sempre regolano, più o meno evidentemente, le leggi della natura e della scienza: la matematica, nocciolo della società industrializzata ed evoluta. Intorno alla fine del Settecento la necessità di introdurre un nuovo metodo che consentisse il calcolo dell'area di superfici che non rientrassero nella categoria di figure note già dalla Geometria elementare riuscì ad apportare un incommensurabile apporto, arrivando a noi oggi sotto forma di strumento matematico.

Integrale definito secondo Riemann

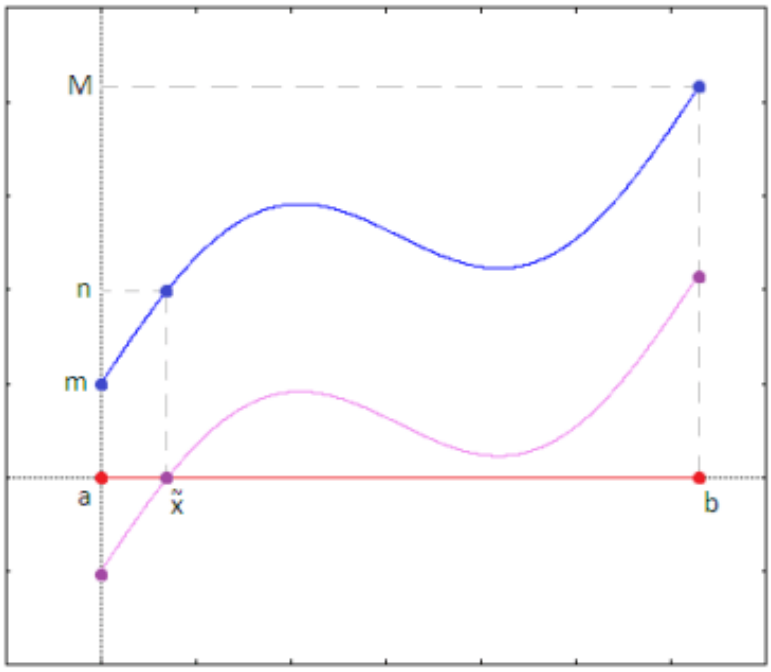
L'**integrale definito secondo Riemann** si basa sulla risoluzione del problema delle aree; in pratica si tratta di trovare l'area di una regione di piano compresa tra la curva, l'asse x e tra le rette x = a x = b, fra gli antichi il matematico che più si avvicinò alla soluzione fu Archimede da Siracusa.

Data una funzione **y = f(x)** definita e continua in **[a,b]** (intervallo a,b chiuso) e per comodità supposta positiva, 2 teoremi assumono considerazione nel contestualizzare la teoria in esame:

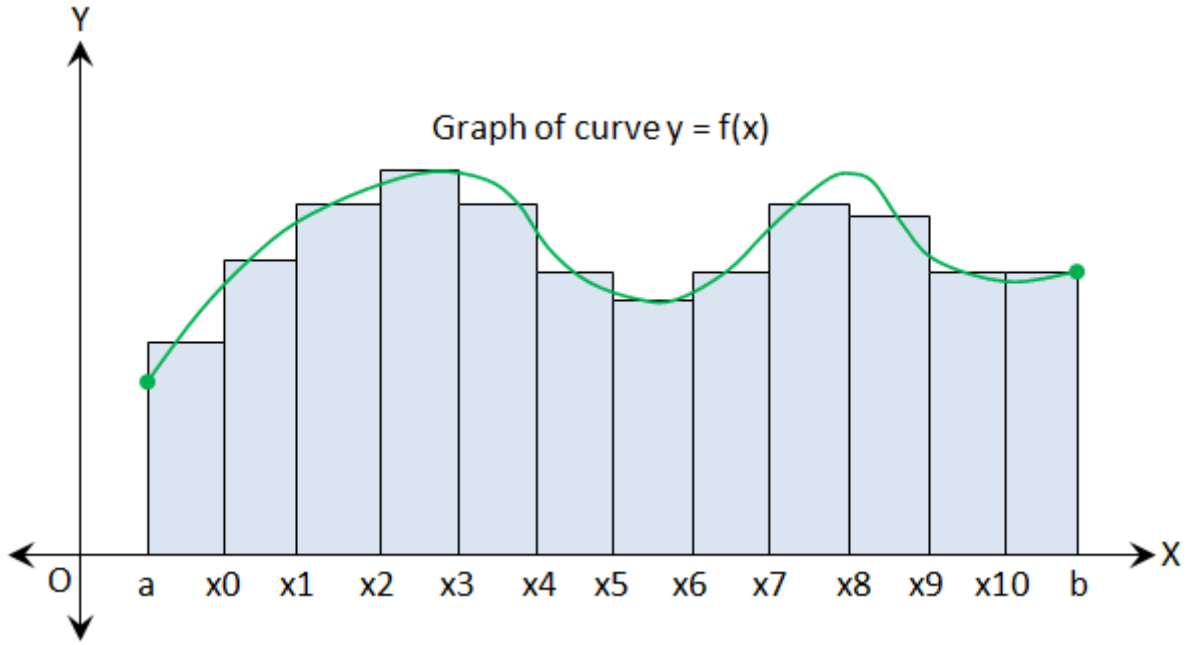
- **Teorema di Weierstrass**
  Se y = f(x) definita e continua in [a,b] allora f(x) ammette in [a,b] massimi e minimi assoluti.



- **Teorema dei valori intermedi** o **Bolzano-Darboux**
  Se y = f(x) definita e continua in [a,b] allora f(x) ***assumerà tutti i valori*** compresi tra il massimo e il minimo assoluto al **variare di x in [a,b].**

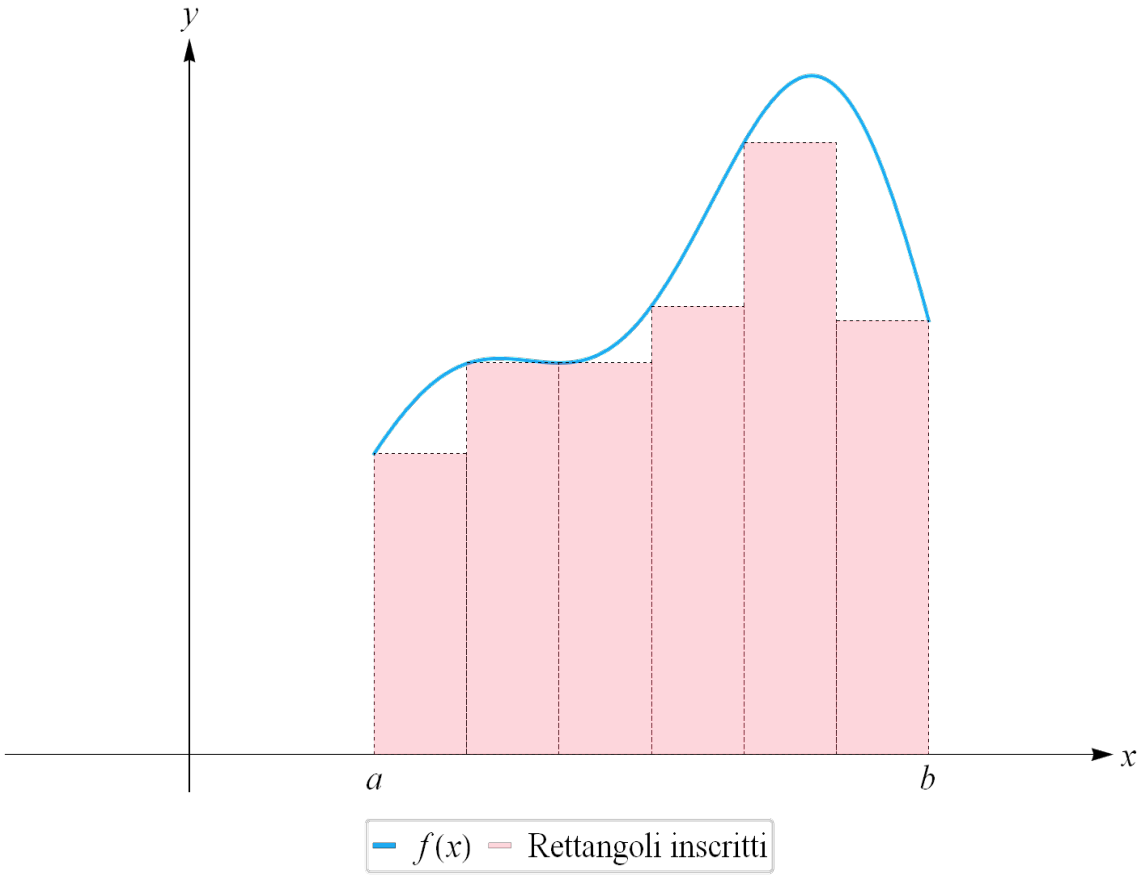


Problema delle aree



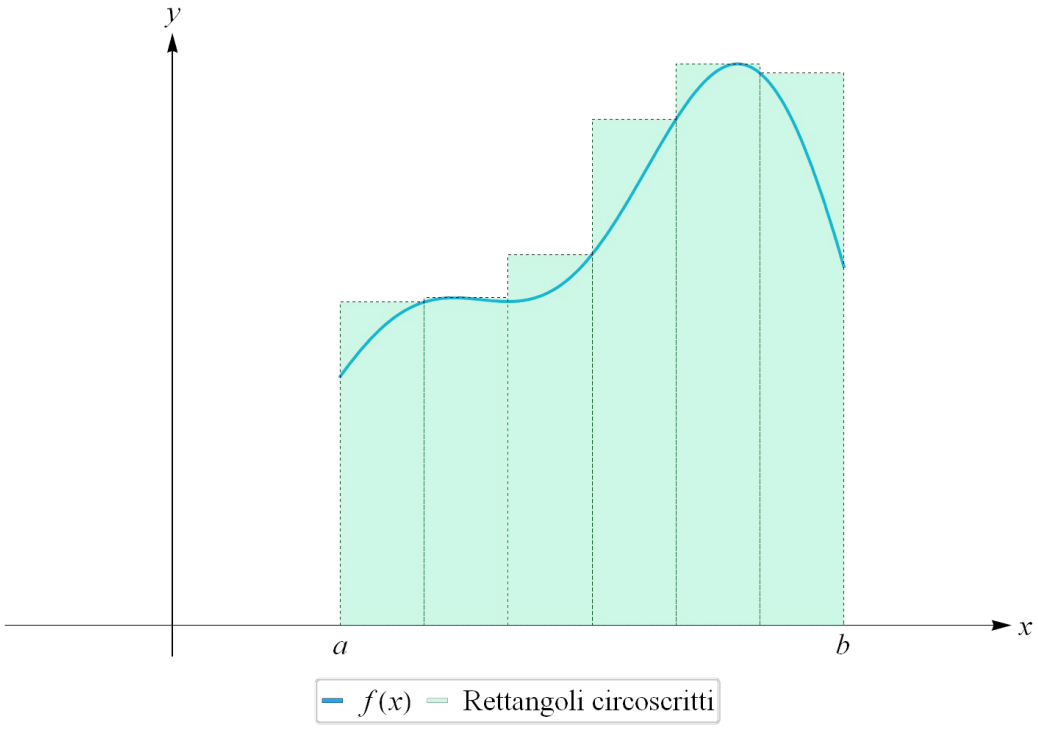
Dividendo l'intervallo [a,b] in **intervalli minori di uguale dimensione** $h=\frac{b-a}{n}$ si ottengono intervalli in cui valgono le teorie precedentemente esposte in quanto per ipotesi la funzione è continua nell'intervallo chiuso.

Considerando **tutti i rettangoli** che hanno per base h e per altezza i minimi assoluti della funzione in ciascun intervallo, la ***somma delle aree di questi rettangoli*** è una figura



chiamata **rettangoloide inscritto**.

Considerando **tutti i rettangoli** che hanno per base h e per altezza i massimi assoluti della funzione in ciascun intervallo, la ***somma delle aree di questi rettangoli*** è una figura chiamata **rettangoloide circoscritto**.



Definendo **s** ed **S** rispettivamente la **somma delle aree dei rettangoloidi inscritti e circoscritti** è possibile scriverli in forma contratta nel modo seguente:

$$s_n = h_1 \cdot m_1 + h_2 \cdot m_2 + \ldots + h_n \cdot m_n = \sum_{i=1}^{n} h_i \cdot m_i$$

$$S_n = h_1 \cdot M_1 + h_2 \cdot M_2 + \ldots + h_n \cdot M_n = \sum_{i=1}^{n} h_i \cdot M_i$$

All'aumentare del numero degli intervalli ***le aree dei triangoli inscritti aumentano***, mentre ***le aree dei triangoli circoscritti diminuiscono***. Un esempio classico precedentemente analizzato a lezione è l'espandersi e il contrarsi delle aree di due palloncini uno dentro l'altro, i quali ***tendono*** ad avvicinarsi ad **un'area comune**.

T = Area del trapezoide

Rettangoloidi inscritti $s_1 \leq s_2 \leq \ldots \leq s_n \leq T$
Rettangoloidi circo scritti $S_1 \geq S_2 \geq \ldots \geq S_n \geq T$ } L'uguale nella relazione vale quando f(x) è una funzione costante

Dal tendere a T di tali aree è possibile definire tale relazione **tramite le relazioni**

$$\lim_{n \to \infty} \sum_{i=1}^{n} h_i \cdot m_i = T = ¿ \lim_{n \to \infty} \sum_{i=1}^{n} h_i \cdot M_i ¿$$

Nel corso dell'anno non abbiamo svolto esercizi di tale tipologia per la difficoltà oggettiva di esprimere i massimi ed i minimi assoluti in funzione di n.
Il limite delle due successioni si chiama area del rettangoloide, esso viene indicato con il simbolo:

$$T = \int_a^b f(x)\,dx$$

Considerando adesso z_n un punto intermedio all'interno di ciascun intervallo di suddivisione all'intervallo [a,b], valutiamo i rettangoli con altezza il valore della funzione in tale punto opportuno ottenendo :

$$\sum_{i=1}^{n} h_i \cdot m_i \leq \sum_{i=1}^{n} h_i \cdot f(Z ¿¿ i) \leq \sum_{i=1}^{n} h_i \cdot M_i ¿$$

Tende a Tende a Tende a

Per i principi del teorema del confronto e della maggiorabilità e dell'inferiorità.

Dunque, è possibile affermare che **l'integrale definito** **è il limite comune a cui tendono le aree dei rettangoloidi inscritti, circoscritti e intermedi quando il numero di suddivisioni dell'intervallo [a,b] tende a infinito.** **Geometricamente** è rappresentabile, come osservato, dall'*area di un trapezoide*.

Teorema della media integrale

Se y = f(x) definita e continua in [a,b] allora esiste almeno un punto $C \in [a,b]$ in cui risulta:

$$f(c) = \frac{\int_a^b f(x)\,dx}{b-a}$$

Dimostrazione

Per il **teorema di Weierstrass** la f(x) ammette m e M. Consideriamo adesso i rettangoli di base l'ampiezza [a,b] e altezza M e m.

$r \leq T \leq R$

$$(b-a) \cdot m \leq \int_a^b f(x)\,dx \leq (b-a) \cdot M$$

Dividiamo per (b- a) tutti i termini della disuguaglianza che osserviamo essere **strettamente positiva** in quanto b>a ottenendo:

$$m \leq \frac{\int_a^b f(x)\,dx}{b-a} \leq M$$

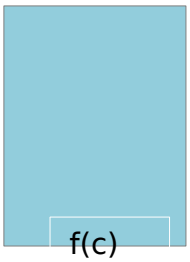
Da cui: $m \leq n \leq M$

Per il **teorema di Bolzano-Darboux** o dei valori intermedi esiste almeno un punto c appartenente all'intervallo [a,b] in cui risulta:

$$f(c) = \frac{\int_a^b f(x)\,dx}{b-a}$$

Il significato geometrico del teorema della media è dimostrabile:

$f(c) = \frac{\int_a^b f(x)\,dx}{b-a}$ moltiplicando per (b – a) otterremo $f(c)\cdot(b-a) = \int_a^b f(x)\,dx$ da cui:



(b – a) = **Area trapezoide** = $\int_a^b f(x)\,dx$

L'**area del trapezoide** è uguale all'area di un rettangolo che ha come lati **l'ampiezza dell'intervallo [a,b]** e il valore della f(x) in **opportuni punti** c dell'intervallo [a,b].