Politecnico di Torino

Corso di laure magistrale in Ingegneria Gestionale

Tesi Laurea Magistrale

Implementazione della Twin Transition all'interno delle PMI

Candidato:

Stefano Berardi S275818

Relatore:

Luca Settineri

Anno Accademico 2021/2022

Introduzione

"*Implementazione della Twin Transition all'interno delle PMI*" tratta lo sviluppo della piattaforma digitale che mira a sostenere l'adozione dell'Economia Circolare nel settore delle Piccole e Medie imprese di tutta Europa, attraverso processi di digitalizzazione.

Ad oggi in Europa, come in tutto il mondo, si sta facendo sempre più improrogabile il tema dell'inquinamento e su come diminuire le emissioni di carbonio nelle nazioni. Molti sforzi ed iniziative sono stati messi in atto per incentivare la transizione verso processi e prodotti in linea con le tematiche dell'economia circolare.

La scelta delle PMI come target è estremamente rilevante rispetto al raggiungimento di una Europa più green in quanto "Nel 2020, erano circa 22 milioni di unità, di cui 21 milioni con meno di 10 dipendenti. Ciò significa che il 93% delle PMI sono microimprese. La quantità di aziende più grandi è marginale in confronto, perché sono circa 41.000 unità, pari allo 0,2% del totale" (Relazione annuale sulle PMI europee 2020-2021 - Commissione europea - EASME).

Le PMI sono anche le Organizzazioni più colpite dall'attuale crisi pandemica, con maggiori difficoltà ad innovare i propri processi; l'implementazione di processi digitali uniti all'Economia Circolare è ciò che permetterebbe loro di uscire da questa emergenza globale.

Pertanto, l'obiettivo della piattaforma è identificare, sviluppare e implementare soluzioni e strumenti digitali innovativi per PMI al fine di sostenere e guidare le organizzazioni attraverso processi di miglioramento rivolti all'Economia Circolare.

Questi strumenti digitali sono basati su due tecnologie: l'Intelligenza Artificiale e la Blockchain. La prima rende la piattaforma capace di interpretare quali siano le necessità delle PMI dando indicazioni su quali processi modificare, mentre la seconda garantisce un trattamento dei dati sicuro per tutte le organizzazioni che utilizzeranno questo servizio.

In questo documento si analizzeranno le principali soluzioni esistenti in tema di Intelligenza Artificiale e Blockchain specificando quali sono state scelte per il progetto.

Sommario

1. Twin Transition

I governi di tutto il mondo esortano il settore industriale, ma anche i consumatori, per ridurre l'utilizzo di materie prime. l'Europa punta sull'innovazione come forza trainante nel raggiungimento della Twin Transition (ovvero transizione verde e digitale congiuntamente) verso un'economia a zero emissioni di carbonio e zero rifiuti.

Il Green Deal vuole separare la crescita economica dallo sfruttamento delle risorse entro il 2050 e trasformare le catene di valore industriali "take-make-discard", nota anche come Linear Economy, in modelli virtuosi che escludano i rifiuti e l'inquinamento dai processi, mantenendo prodotti e materiali in utilizzo più a lungo e contribuendo a rigenerare gli ecosistemi. Questo modello prende il nome di Circular Economy, la cui trattazione è presente nel capitolo successivo.

l'applicazione di questo nuovo modello permetterà di risolvere, o almeno di ridurre, tutti i problemi legati all'inquinamento e dei rifiuti.

L'elettronica di consumo (e-waste) è un primo esempio di come sia necessario intervenire utilizzando logiche circolari. Meno del 40% dei 9 milioni di tonnellate (2017) di rifiuti elettronici nell'UE è attualmente riciclato. Essendo una miscela complessa di materiali e componenti, molti dei quali sono pericolosi e difficili da gestire, i rifiuti elettronici possono causare gravi problemi ambientali e sanitari.

Anche sul fronte dei rifiuti plastici sono necessari interventi importanti per i quali l'Europa ha sia raddoppiato le tasse su di essi che finanziato vari progetti.
Ad esempio, il progetto ReCircE vuole migliorare lo smistamento dei rifiuti di plastica utilizzando l'intelligenza artificiale (AI) abbinata all'utilizzo di un Digital Product Passport[1] per sostenere la trasparenza informativa nella catena dei materiali riciclati, rendendo più semplice ri-utilizzare granulati di plastica da prodotti complessi come bollitori elettrici e giocattoli.

I ricercatori hanno studiato come la digitalizzazione nell'industria (Industria 4.0) si stia rapidamente evolvendo per soddisfare le richieste dei consumatori e del governo nel campo della gestione dei rifiuti, quello che chiamano ReWaste4.0, e su sistemi robotici che selezionano i rifiuti misti.

Prevenire è meglio che curare, quindi la prima priorità è quella di ridurre, riutilizzare e riciclare i materiali per evitare che i rifiuti arrivino in discarica. Ciò richiede processi di selezione complessi per i quali sono già state sviluppate tecnologie con sensori per il rilevamento dei materiali, nuove tecniche di

[1] L'Iniziativa Prodotti Sostenibili, inclusa nel nuovo Circular Economy Action Plan e tra gli obiettivi del Green Deal, prevede di istituire un passaporto digitale dei prodotti (DPP) che raccolga i dati sulla catena del valore dei prodotti. L'obiettivo del DPP è promuovere la produzione sostenibile, consentire la transizione all'economia circolare, offrire nuove opportunità commerciali agli attori economici, aiutare i consumatori a compiere scelte sostenibili e consentire alle autorità di verificare il rispetto degli obblighi di legge.

Digital imaging [2] e modelli di business innovativi, e si prevede che i dati saranno un fattore critico per determinare gli impianti di gestione dei rifiuti'.

Un esempio di questa tecnologia sono gli Smart Bins che sono in grado di rilevare il proprio stato di riempimento, la frequenza e l'orario di utilizzo attraverso una scansione costante effettuata da un sensore e successivo invio dei dati raccolti ad un software di back-end, tramite rete wireless low cost.
Il cestino invia misurazioni relative al suo stato di riempimento (vuoto, pieno a metà o completamento pieno) ed occlusione (occluso o non occluso). Le informazioni fornite consentono di ottimizzare il processo di raccolta dei rifiuti conferiti nei contenitori stradali, riducendo l'impiego di risorse e mezzi pianificati e contribuiscono inoltre al miglioramento qualitativo del servizio, garantendo tempestività d'intervento per le situazioni critiche, evitando così il manifestarsi di situazioni con accumulo di rifiuti sopra il contenitore.

La soluzione si basa su tecnologie particolarmente efficienti dal punto di vista energetico che permettono al contenitore intelligente di operare per anni, senza bisogno di collegarlo alla rete elettrica, grazie a batterie di lunga durata ed a software di controllo ottimizzati.

L'Europa sta chiaramente facendo progressi, ma la direttiva europea sui rifiuti e il piano d'azione CE sono più ambiziosi. I nuclei familiari nel l'UE-27 generano attualmente circa l'8,2% dei rifiuti totali, mentre l'edilizia (36%), l'estrazione mineraria/estrattiva (26,2%) e l'industria manifatturiera (10,6%) costituiscono la stragrande maggioranza (fonte Eurostat, Waste Generation 2018).

Al fine di accelerare questi miglioramenti si stanno finanziando e promuovendo innumerevoli progetti, come:

- Il progetto ReCircE mira a migliorare l'efficienza dei cicli dei materiali. Questo obiettivo viene raggiunto combinando una descrizione digitale del prodotto con tecnologie di selezione intelligenti supportate dall'intelligenza artificiale (AI). Le informazioni sul prodotto e sul ciclo di vita del prodotto sono memorizzate nel record del ciclo di vita. Ciò include, ad esempio, i materiali utilizzati nei processi di fabbricazione e le loro proprietà. Queste informazioni sono rese disponibili per il recupero del materiale - ad es. per la selezione, il riciclaggio e il successivo riutilizzo. In questo modo, i dati possono essere ottenuti dal file del ciclo di vita e utilizzati per migliorare l'ordinamento. I dati sui prodotti e sui materiali sono resi disponibili ai processi di apprendimento automatico per consentire decisioni di ordinamento basate sull'IA. Allo stesso tempo, i dati provenienti dallo smistamento confluiscono nel record del ciclo di vita e rappresentano una fonte supplementare di informazioni per i successivi processi di riciclaggio.

- Attraverso ReWaste4.0 la trasformazione dell'industria del trattamento dei rifiuti urbani e commerciali misti non pericolosi verso un'economia circolare è iniziata studiando e applicando i nuovi approcci dell'Industria 4.0. La visione del ReWaste4.0 è, tra l'altro, lo sviluppo di impianti

[2] Digital imaging o acquisizione di immagini digitali è la creazione di una rappresentazione digitale delle caratteristiche visive di un oggetto, come una scena fisica o la struttura interna di un oggetto. Il termine viene spesso assunto per implicare o includere l'elaborazione, la compressione, l'archiviazione, la stampa e la visualizzazione di tali immagini. Un vantaggio chiave di un'immagine digitale, rispetto a un'immagine analogica come una fotografia cinematografica, è la capacità di propagare digitalmente copie del soggetto originale indefinitamente senza alcuna perdita di qualità dell'immagine.

di trattamento per i rifiuti non pericolosi in una "Smart Waste Factory" in cui viene raggiunta una comunicazione digitale e l'interconnessione tra qualità dei materiali e delle macchine, nonché le prestazioni dell'impianto.

- TOMRA Recycling in Norvegia è uno dei primi utilizzatori di Intelligenza Artificiale che utilizza modelli matematici, basati sulle informazioni raccolte dal campionamento di materiali su larga scala.
  La finlandese ZenRobotics[3] vede il machine learning e la robotica come "un nuovo standard industriale". Il suo impianto di recupero basato sull'intelligenza artificiale estrae materiali preziosi dal flusso di rifiuti e intensifica i tassi di riciclaggio.
  I robot creano un ambiente di smistamento più strutturato e prevedibile che aiuta a mitigare i rischi per la salute e la sicurezza associati alla selezione manuale, e quindi creare condizioni di lavoro più sicure attraverso maggiori possibilità di distanziamento sociale", nota ZenRobotics.

- Il progetto OECD RE-CIRCLE fornisce orientamenti politici sull'efficienza delle risorse e la transizione verso un'Economia Circolare e mira a identificare e quantificare l'impatto delle politiche per guidare una serie di parti interessate nei paesi membri dell'OECD e nelle economie di mercato emergenti attraverso analisi qualitativa. Il lavoro di Resource Efficiency and Circular Economy si concentra sulle interconnessioni tra l'uso dei materiali e: attività economica, mercato del lavoro, commercio internazionale, cambiamento climatico, innovazione digitale, sicurezza alimentare, modelli di business circolari, catene del valore globali, rifiuti di plastica.

Secondo la Ellen Macarthur Foundation, l'intelligenza artificiale sosterrà la transizione verso la Circular Economy, tenendo conto delle informazioni relative all'impatto ambientale già in fase di progettazione ottimizzando i modelli di business e razionalizzando le infrastrutture necessarie per mantenere i prodotti ei materiali in uso.

Ma l'innovazione digitale appena descritta richiede ingenti investimenti sia in tecnologie che nella formazione del personale per avvicinarli ai temi dell'Economia Circolare.

Il settore industriale Europee è spesso un mosaico di piccole e grandi imprese, molte delle quali lottano per giustificare investimenti in avanzate tecnologie green che non sempre hanno un impatto economico rilevante nel breve termine. I costi di capitale (CAPEX) devono essere compensati da incrementi di efficienza che riducano i costi operativi tipici (OPEX) come il lavoro. E quando non lo fanno, questo favorisce le organizzazioni di grandi dimensioni che sono maggiormente facilitate ad accedere ai capitali necessari per gli investimenti.

L'OECD[4] valuta questa e altre sfide con il suo progetto RE-CIRCLE per aiutare i paesi membri e i mercati emergenti a identificare e quantificare la loro efficacia in tema di Economia Circolare in diversi

---

[3] ZenRobotics Ltd., fondata nel 2007, è un leader globale nel riciclaggio robotico intelligente e la prima azienda ad applicare robot di smistamento basati su AI in un ambiente complesso di smistamento dei rifiuti.

[4] L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD) è un'organizzazione internazionale che lavora per costruire politiche migliori per una vita migliore, con l'obbiettivo di plasmare politiche che promuovano prosperità, uguaglianza, opportunità e benessere per tutti. Insieme ai governi, ai responsabili politici e ai cittadini, lavorano per stabilire

settori, dall'innovazione digitale, ai rifiuti di plastica e alla sicurezza alimentare al commercio internazionale e ai mercati del lavoro.

La forte enfasi sull'innovazione verde e sulle nuove tecnologie sia nella produzione di beni che nel consumo di prodotti e servizi corre il rischio di lasciarsi alle spalle segmenti della società. Ben 80 milioni di europei non usano né hanno accesso a Internet.
Affinché la Twin Transition in Europa sia raggiunta sul piano tecnico quanto su quello sociale ed etico, sono necessari nuovi posti di lavoro qualificati passando attraverso un training specifico della risorse.

Secondo il rapporto FORENV sulle innovazioni economiche, imprenditoriali, tecnologiche e sociali emergenti nell'Economia Circolare, le comunità locali e le imprese sociali che cercano di garantire benefici per le persone e l'ambiente svolgono un ruolo importante in una Economia Circolare inclusiva. Questo è anche il motivo per cui l'agenda europea sulle competenze ha fissato misure ambiziose per riqualificare milioni di europei entro il 2025.

"Ci si aspetta che nuovi modelli di business basati sulla tecnologia che sostituiscano molti posti di lavoro poco qualificati nel l'economia circolare (ad es. trasporti senza conducente, robotica, ecc.), mentre verranno creati altri posti di lavoro tecnici", sostiene la relazione FORENV, aggiungendo che la sostituzione della manodopera o l'aumento delle tecnologie introdotto dal Green Deal offre una soluzione per una diminuzione della forza lavoro europea man mano che le popolazioni continuano ad invecchiare. "Questo potrebbe costringere le imprese ad adattare i posti di lavoro alle competenze disponibili come ogni dipendente sarebbe più prezioso nel mercato del lavoro".

Mentre i paesi sono ancora alle prese con le incertezze del Covid-19, la digitalizzazione, l'intelligenza artificiale e la robotica sono viste da molti come un'opportunità di miglioramento piuttosto che di regressione per l'implementazione della Circular Economy, creando ambienti operativi più sicuri e più puliti

In particolare, i progressi nell'intelligenza artificiale (AI) sono destinati a trasformare il modo in cui tutte le industrie si approcciano al loro business, dall'ottimizzazione della produzione e dei sistemi energetici, al modo in cui gli scienziati analizzano e utilizzano i dati, dalla previsione del cambiamento climatico alla mancata comprensione degli ecosistemi.

L'ottimismo circa il potenziale di questa tecnologia è elevato, come sottolineato da uno studio Intel[5], il quale ha rilevato che il 74% dei leader tecnologici ritiene che l'intelligenza artificiale possa aiutare a

---

standard internazionali basati su prove e trovare soluzioni a una serie di sfide sociali, economiche e ambientali: dal miglioramento delle prestazioni economiche alla creazione di posti di lavoro, alla promozione di un'istruzione forte e alla lotta all'evasione fiscale internazionale.

risolvere le sfide ambientali di lunga data; e il 92% pensa che l'analisi predittiva aiuterà le organizzazioni a rilevare i problemi e sviluppare nuove soluzioni, fornire costi e ostacoli normativi possono essere superati. In un altro studio di Microsoft sull'Intelligenza Artificiale in Europa, l'89% delle aziende intervistate si aspetta che essa produca benefici per il business ottimizzando le proprie operazioni e aumentando l'efficienza delle risorse.

Consapevole delle questioni normative e delle implicazioni etiche, l'UE sta conducendo una politica industriale globale sull'Intelligenza Artificiale e la robotica. L'intelligenza artificiale può aiutare i fornitori di energia a passare dalla gestione preventiva a quella predittiva degli asset, e aiutare i settori ad alta intensità energetica a identificare e migliorare le loro prestazioni. Può aprire la strada a reti di trasporto più verdi e intelligenti e veicoli autonomi. Può affrontare i problemi di sicurezza alimentare, prevedere le malattie di origine alimentare e la carestia, nonché migliorare la gestione sostenibile della terra, dell'acqua e di altre risorse ambientali fondamentali per la salute più ampia dell'ecosistema.

L'Europa è una forza trainante nella ricerca in Intelligenza Artificiale ospitando il 32% degli istituti di ricerca in tutto il mondo. Il sostegno dell'UE alle iniziative in materia di Intelligenza Artificiale è in costante crescita con ogni programma di finanziamento della ricerca a lungo termine. Per il prossimo bilancio di Horizon Europe (2021-2027), l'UE ha proposto di investire almeno 7 miliardi di euro nella ricerca su questa tecnologia.

Un’altra tecnologia che può contribuire alla digitalizzazione e alla transizione verde è rappresentata dalla Distributed Ledger Technology.

Nonostante, Bitcoin, la prima applicazione Blockchain, è ampiamente nota come una tecnologia ad alto impatto ambientale, che consuma enormi quantità di energia ed emette grandi quantità di CO2 al fine di convalidare le transazioni e sostenere la rete, esistono soluzioni che utilizzano architetture di rete e protocolli differenti, consentendo di raggiungere soluzioni più efficienti dal punto di vista energetico. Ad esempio, le Blockchain private che utilizzano algoritmi basati sulla Proof-of-Authority (PoA) non consumano più energia di un tradizionale database.

La tecnologia Blockchain potrebbe sbloccare nuove fonti di finanziamento e mobilitare i mercati per la riduzione delle emissioni di carbonio attraverso la creazione di nuove piattaforme di finanziamento volte alla riduzione del costo del capitale per i progetti infrastrutturali, insieme a una maggiore liquidità, trasparenza e maggiore accesso ai fondi.

In secondo luogo, questa tecnologia potrebbe dare visibilità agli obiettivi di sostenibilità consentendo ai paesi e agli stakeholders di tenere traccia dei dati e delle informazioni sui progetti che vengono attuati. Le piattaforme Blockchain sono un modo per standardizzare i dati, valutare le performance degli asset e migliorarne la conformità (standard di sostenibilità o ESG[6]), che possono essere ulteriormente

[6] ESG (Environmental Social Governance) è utilizzato per indicare le attività legate all’investimento responsabile, che perseguono cioè gli obiettivi tipici della gestione finanziaria tenendo però in considerazione anche aspetti di natura

enfatizzate quando sono integrate con sensori remoti (internet of things) o collegati ad applicazioni di intelligenza artificiale.

In terzo luogo, può aumentare la consapevolezza e l'accesso agendo come un'infrastruttura che consente di effettuare transazioni di nuovi modelli di mercato. Ciò può incentivare e aumentare la volontà e la capacità delle istituzioni e dei consumatori di contribuire a costruire la sostenibilità a lungo termine, favorendo anche i cambiamenti all'interno delle industrie per adattarsi alle mutevoli richieste dei consumatori.

Il ruolo della Blockchain nel contesto dell'infrastruttura sostenibile è considerato molto al di là dell'abilitazione di servizi efficienti di raccolta dati, monitoraggio, reporting e steering. La tecnologia può potenzialmente affrontare anche le sfide e le opportunità principali nel sostenere le attività connesse alla mitigazione e all'adattamento, in particolare nei settori dell'energia, dei trasporti e manifatturiero.

---

ambientale, sociale e di governance. Aziende e investimenti vengono dunque analizzati, oltre che sotto il profilo economico, anche in base ai tre criteri che ne definiscono la sostenibilità.

1.1 Economia Circolare

L'Economia Circolare è un'alternativa al modello di business aperto e lineare, che viene sostituito da un circuito chiuso di flussi di materiali. La crescente popolarità del concetto dell'Economia Circolare deriva dal deterioramento del l'ambiente e, di conseguenza, dalla necessità di ricercare metodi di produzione e di consumo meno dipendenti dal l'esaurimento delle risorse naturali e dalle fonti energetiche riducendo l'impatto ambientale.

Tra il numero crescente di studi sul l'attuazione del concetto dell'Economia Circolare, si possono identificare due approcci: top-down e bottom-up.
L'approccio top-down sottolinea il ruolo preponderante delle iniziative politiche e sociali (come, ad esempio, i programmi Horizon e Interreg) che conferiscono linee guida e finanziano i progetti.
L'approccio bottom-up prevede che le aziende e le organizzazioni, in modo proattivo, sostengano direttamente questa transizione coinvolgendo la società, spinte da un spiccato senso etico e di responsabilità sociale dell'ambiente e del suo sfruttamento e dalla possibilità di aumentare i profitti aumentando il valore del prodotto, accedendo a nuovi mercati e fonti di finanziamento.

In Figura 1, tratta dallo studio di Legambiente, è riportato il dettaglio delle principali motivazioni che spingono le organizzazioni a porsi come promotore di questo cambiamento:

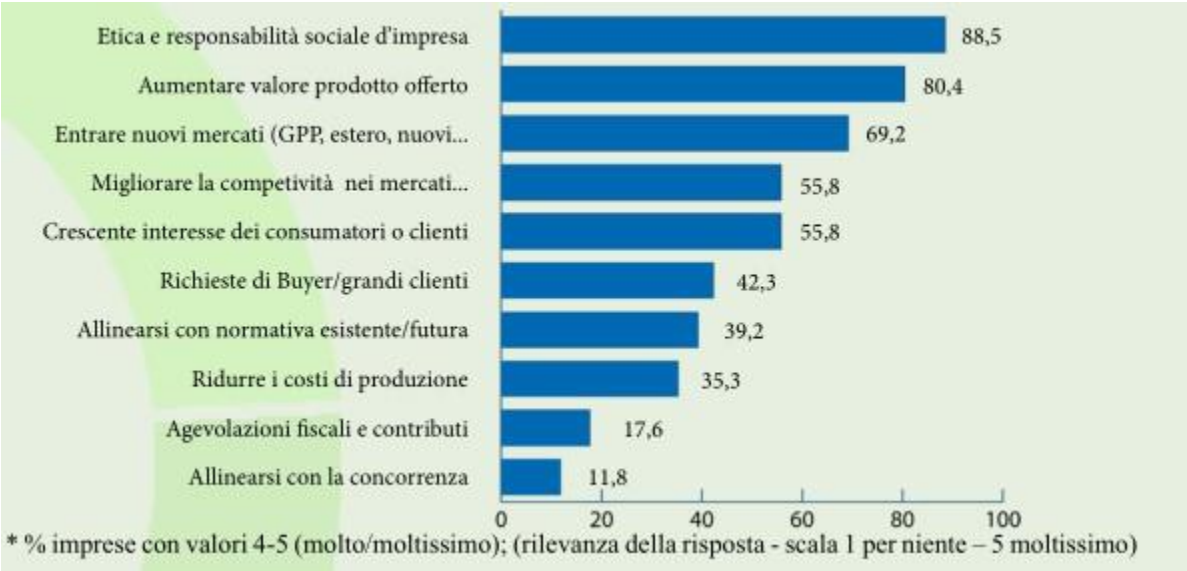


Figura 1 Motivazioni che hanno spinto ad adottare un modello di business circolare

La grande sfida da superare invece è rappresentata dalla mancanza di conoscenza ed istruzione sul tema dell'Economia Circolare che porta con sé: scetticismo sul ritorno economico di investimenti ingenti (lato Produttore), diffidenza sull'aumento di prezzo dei prodotti di cui può essere difficile apprezzarne le motivazioni (lato Cliente) e manca di supporto attraverso linee guida o normative (lato Pubblica Amministrazione) come evidenziato nella figura 2.

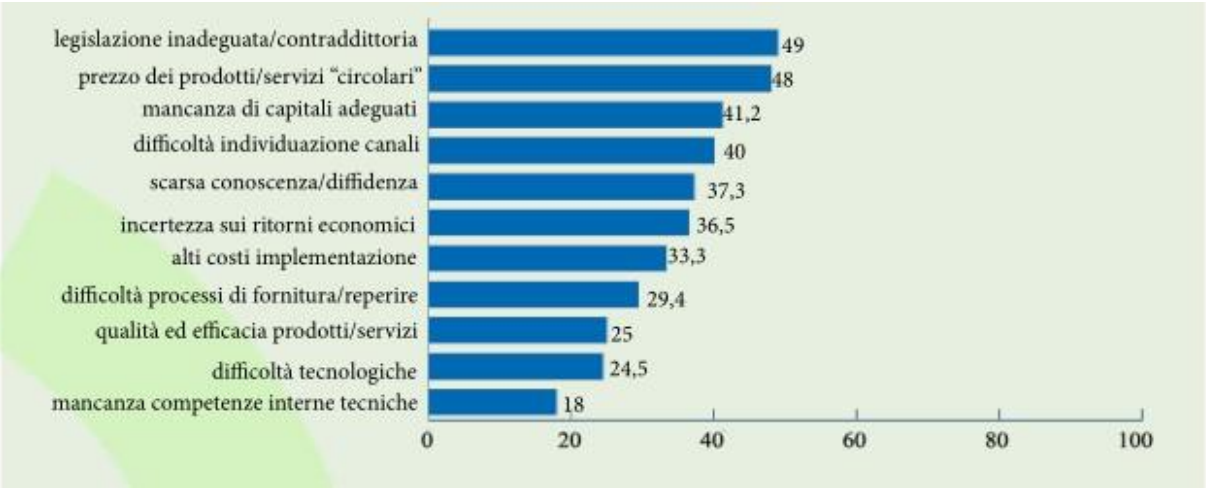
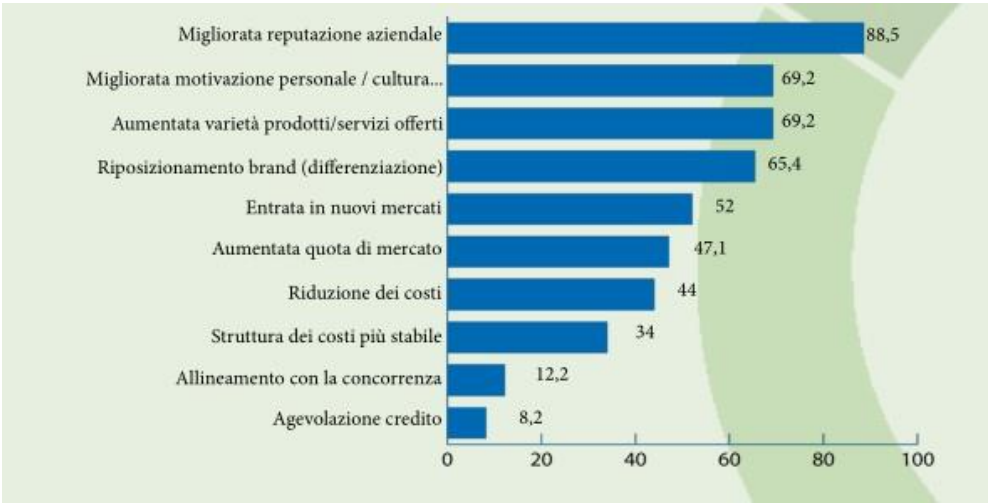


Figura 2: Principali difficoltà per l'adozione del modello di business circolare (%)

Le organizzazioni che sono state in grado di superare queste difficoltà saranno in grado di migliorare sensibilmente la loro reputazione e la motivazione del personale oltre che garantirsi ritorni economici maggiori sia dai business precedenti che da quelli che hanno creato ex-novo, come sottolineato in Figura 3.

Figura 3: Benefici riscontrati



1.1.1 Modelli di business per l'Economia Circolare

Il raggiungimento dei benefici sopra citati dipende fortemente dalla capacità di implementare correttamente nuovi modelli di business circolari. Tuttavia, scegliere o progettare questi modelli può essere decisamente complicato in quanto ogni realtà possiede bisogni specifici che molto spesso richiedono soluzioni ad hoc.

Molti modelli sono stati creati nel tempo, tra i più noti ci sono:

- ecologia industriale, è un campo di studio focalizzato sulle fasi dei processi di produzione di beni e servizi dal punto di vista della natura, cercando di imitare un sistema naturale conservando e riutilizzando le risorse.

- efficienza ecologica,

- emissioni zero,

- *from creadle to cradle* (C2C), Cradle to Cradle è un concetto di design ispirato alla natura, in cui i prodotti vengono creati secondo i principi di un'economia circolare ideale.

- progettazione rigenerativa, una progettazione che tende ad una fusione armoniosa tra spazio antropizzato e contesto naturale, applicabile specialmente nel settore delle costruzioni.

- Biomimicry, Biomimicry o Biomimesi è una disciplina che studia e imita i processi biologici e biomeccanici della natura e degli esseri viventi come fonte di ispirazione per il miglioramento delle attività e tecnologie umane. La natura viene vista come Modello, Misura, e come Guida della progettazione degli oggetti e dei manufatti tecnici.

- Blue Economy, La blue economy si occupa di salvaguardare la "purezza del mare" e di attuare un tipo di pesca sostenibile tramite un modello di economia a livello globale dedicato alla creazione di un ecosistema sostenibile grazie alla trasformazione di sostanze precedentemente sprecate in merce redditizia.

- LCA Il Life Cycle Assessment (LCA) è una metodologia analitica e sistematica che valuta l'impronta ambientale di un prodotto o di un servizio, lungo il suo intero ciclo di vita.

- simbiosi industriale. La simbiosi industriale è una forma di intermediazione per facilitare una collaborazione innovativa tra le aziende, in modo tale che i rifiuti prodotti da una di esse vengano valorizzati come materie prime per un'altra

Tutte queste sono sfaccettature dell'Economia Circolare che si possono applicare in casi specifici.

Quello che in generale si può affermare su un modello di business circolare è che deve essere conforme ai principi 3R: ridurre, riutilizzare e riciclare. Ove possibile, il riutilizzo e la rigenerazione sono preferibili al riciclaggio per motivi economici, in quanto una parte significativa del valore aggiunto nel processo di produzione originale rimane intatto. Si immagini a titolo di esempio il riciclaggio di una bottiglia di vetro per ricreare la medesima bottiglia, sarebbe meglio cercare un processo alternativo per riutilizzare la bottiglia.

I modelli di business circolari (CBM) sono modelli di business che devono mettere in pratica i principi circolari a tutte le dimensioni dell'attività commerciale: business-to-business (B2B), business-to-consumer (B2C) e consumer-to-consumer (C2C). Le CBM offrono nuove opportunità commerciali e provocano un cambiamento nei rapporti tra produttori e consumatori.

Perché un business si possa definire Circolare è inoltre necessario che rispetti quattro requisiti:

- La prima è una proposta di valore che riflette l'equilibrio dei bisogni economici, ecologici e sociali;
- La seconda è una supply chain che coinvolge i fornitori in una gestione sostenibile della stessa;
- Il terzo è un'interfaccia cliente che li motivi ad assumersi la responsabilità per il loro consumo rendendoli parte integrante del processo;
- Il quarto è un modello finanziario, che riflette principalmente un'adeguata distribuzione dei costi e dei benefici economici tra gli attori coinvolti nel modello aziendale.

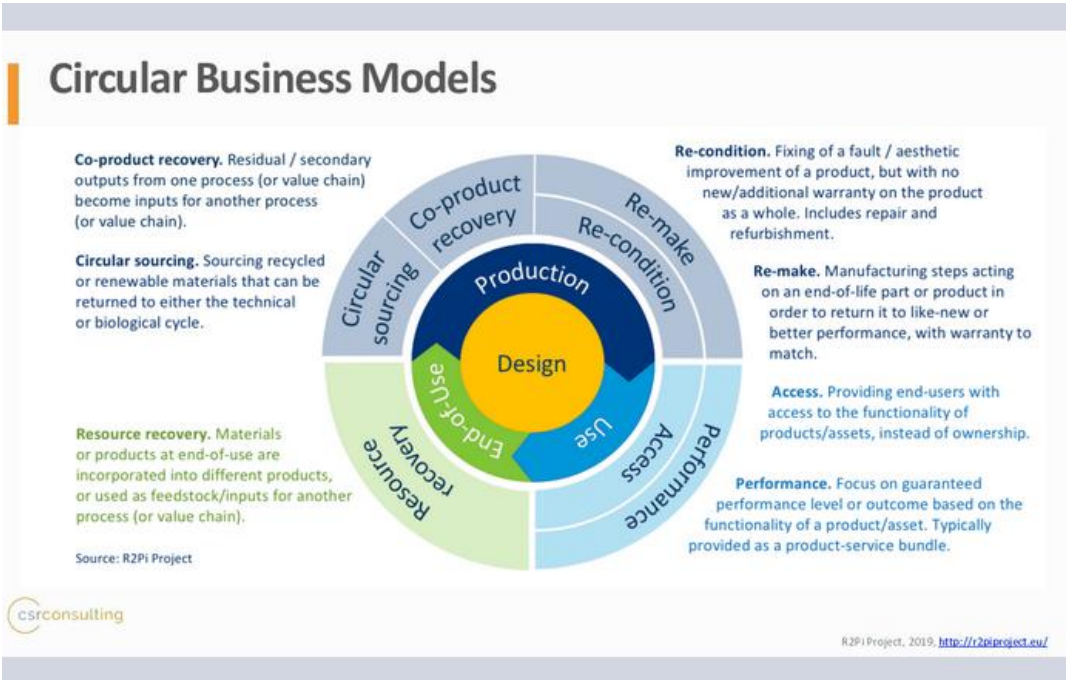


Figura 4 modelli di Economia Circolare

1.1.2 Classificazione dei modelli di business circolari

Al fine di fare chiarezza sull'argomento in modo da supportare le organizzazioni nella transizione dall'Economia Lineare a quella Circolare sono stati condotti svariati studi che hanno come scopo la definizione di modelli di business largamente applicabili e scalabili. Di seguito vengono proposti i modelli più conosciuti e diffusi.

La Business and Sustainable Development Commission (BSDC) ha elencato quattro modelli di business innovativi del futuro che consentiranno alle imprese di rispondere alle sfide dell'Economia Circolare. Essi comprendono:

- Il modello sociale, che crea anche valore diverso da quello economico avendo un impatto sociale positivo;

- Il modello lean, che comporta l'ottimizzazione dell'uso di tutte le forme di capitale;

- Il modello integrato, che significa gestire l'impatto economico e non economico del processo di creazione di valore nella società;

- Il quarto modello è il modello a circuito chiuso, caratterizzato dall'impatto meno negativo rispetto agli altri in tema di risorse, ecosistemi e benessere. Come parte di questo modello, BSDC indica attività quali: simbiosi industriale (condivisione di risorse e servizi tra industrie correlate e geograficamente vicine), fornitura a circuito chiuso (utilizzo di materie prime rinnovabili o completamente riciclabili), servizi di raccolta dei rifiuti per recuperare i prodotti alla fine della loro vita, virtualizzazione (la sostituzione di un prodotto o servizio reale con uno virtuale, disponibile online), rimaterializzazione (acquisizione di materiali da materie prime recuperate per creare prodotti completamente nuovi), trash to cash (i prodotti usati sono raccolti e venduti o trasformati in nuovi prodotti) o piattaforme peer-to-peer (che consentono agli utenti di comunicare e condividere informazioni o servizi).

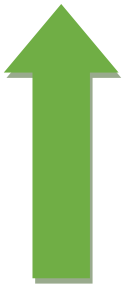
Un altro studio prodotto dalla Ellen MacArthur Foundation sottolinea come l'Economia Circolare si basi sulla creazione di circuiti chiusi. Lo studio elenca sei pratiche che le aziende dovrebbero attuare per migliorare la circolarità, vale a dire: rigenerare, condividere ottimizzare, circuiti chiusi, virtualizzare e scambiare (Tabella 1).

Tabella 1: Modelli di business circolari secondo ReSOLVE.

Rigenerare	Attività volte a ripristinare, preservare e riparare la qualità degli ecosistemi, nonché restituendo alla biosfera le risorse biologiche recuperate.
Condividere	Condivisione di risorse tra diversi utenti, ad esempio attraverso la condivisione di prodotti privati con più comproprietari o utilizzando pubblicamente un determinato gruppo di prodotti, riutilizzandoli durante l'intera vita; estendendo la loro durata attraverso la manutenzione, la riparazione e la progettazione che estenda la vita utile dei prodotti.
Ottimizzare	Aumentare l'efficienza di un dato prodotto, eliminando gli sprechi nella catena di produzione e di approvvigionamento a tutte le fasi del ciclo di vita.
Circuiti chiusi	Mantenere i componenti e i materiali in circuiti chiusi il che significa riutilizzare prodotti o componenti nella produzione.
Virtualizzare	Digitalizzazione di prodotti e processi.
Scambio	Scambio di materiali non rinnovabili vecchi con materiali avanzati, utilizzando nuove tecnologie o nuove forme di servizi

Il modello ReSOLVE non è l'unico che si è occupato di definire le caratteristiche di un modello di business circolare. Il PBL Netherland Enviromental Assesment Agency pone una maggiore enfasi sulla gerarchia della gestione dei rifiuti, come evidenziato nella Tabella 2.

Tabella 2: Classificazione delle attività utilizzate nei modelli di business circolari

Economia Circolare	Migliori processi di produzione e uso dei prodotti	Creare prodotti ridondanti[7] (Refuse)
		Aumentare l'intensità di utilizzo dei prodotti (Rethink)
		Incrementare l'efficienza del prodotto (Reduce)
	Estensione vita utile del prodotto e delle sue parti	Riuso
		Riparazione
		Modifiche e aggiornamenti del prodotto (Refurbish)
		Riutilizzo delle parti del prodotto (Remanufactoring)
		Riutilizzo delle parti del prodotto per uno scopo differente da quello di progetto
Economia Lineare	Metodi di recupero dei materiali	Processare i materiali per ottenere materiale grezzo (Recycle)
		Risparmio energetico (Recover)

Un'altra classificazione viene proposta dal Forum for the Future[8], il quale sostiene che i modelli di business circolari sono innovativi modelli di business volti ad aumentare il livello di sostenibilità del

[7] La ridondanza, nell'ingegneria, è definita come l'esistenza di più mezzi per svolgere una determinata funzione, disposti in modo tale che un guasto di un sistema possa verificarsi solo in conseguenza del guasto contemporaneo di tutti questi mezzi. In pratica la ridondanza in ingegneria consiste nella duplicazione dei componenti critici di un sistema con l'intenzione di aumentarne l'affidabilità e la disponibilità, in particolare per le funzioni di vitale importanza per garantire la sicurezza delle persone e degli impianti o la continuità della produzione.

[8] Forum for the Future è un'organizzazione senza scopo di lucro che opera in collaborazione con le imprese, il governo e la società civile per accelerare il passaggio verso un futuro sostenibile. Funziona catalizzando il cambiamento nei sistemi globali chiave (energia, cibo, abbigliamento, spedizione).

sistema economico attraverso concetti circolari. La classificazione proposta consiste in cinque modelli di base supportati da altri due non direttamente correlati all'Economia Circolare (Tabella 3).

Tabella 3: Classificazione dei modelli di business circolari secondo il Forum per il Futuro

<table>
<tr><td rowspan="5">Modelli circolari di base</td><td>Riciclaggio a ciclo chiuso: utilizzo di materiali riciclati come materia prima per la produzione.</td><td rowspan="5">Concetti che supportano i modelli di base</td><td rowspan="3">Product as a service: vendere una soluzione, non un prodotto tramite contratti a lungo termine.</td></tr>
<tr><td>Downcycling: trasformare le materie prime da uno o più prodotti usati in un nuovo prodotto di qualità inferiore.</td></tr>
<tr><td>Upcycling: trasformare i materiali provenienti da uno o più prodotti in un nuovo prodotto che abbia un valore maggiore per il consumatore</td></tr>
<tr><td>Simbiosi Industriale: condivisione di servizi, strumenti e sottoptodotti tra industrie per aumentare l'efficienza.</td><td rowspan="2">Modularità del prodotto: la creazione di un prodotto con parti indipendenti permette il loro rimpiazzo e riutilizzo con maggiore facilità.</td></tr>
<tr><td>Servizi di raccolte: instaurare un servizio di raccolta per i prodotti vecchi che hanno raggiunto il loro fine vita.</td></tr>
</table>

Nonostante lo studio e la ricerca di modelli di business che possano essere largamente utilizzati non si è ancora arrivati a questo risultato. In moti casi si sono tracciate delle linee guida ricavate da casi studio, la cui applicabilità e limitata al settore (molto spesso questo non è neanche sempre vero) nel quale sono stati definiti.

A causa di ciò si richiede alle organizzazioni di compiere uno sforzo rilevante, in termini economici e tecnici, per adattare i modelli esistenti alla loro realtà o, molto spesso, di creare modelli completamente nuovi.

In questo senso le tecnologie basate sull'Intelligenza Artificiale possono dare una spinta decisa all'implementazione dell'Economia Circolare supportando le organizzazioni in questo cambiamento.

2. Intelligenza artificiale

L'intelligenza artificiale è un ramo del campo dell'ingegneria del software in cui gli esperti matematici stanno tentando di stabilire un'intelligenza avanzata all'interno dei sistemi informatici. Le definizioni per questa tecnologia sono svariate, per citarne alcune: "*The art of creating machines that perform functions that require intelligence when performed by people*." (Kurzweil, 1990); "*The study of how to make computers do things at which, at the moment, people are better*." (Rich and Knight, 1991). Da queste definizioni si capisce che l'intelligenza artificiale vuole ricreare il modo di pensare umano all'interno dei calcolatori, rendendoli capaci di comprendere e apprendere acquisendo capacità cognitiva, rappresentazione della conoscenza, logica, risoluzione dei problemi e la pianificazione, consentendo loro di gestire problemi complessi e scarsamente definiti in una soluzione deliberata, perspicace e adattiva.

Dati gli ineguagliabili vantaggi enfatizzati anche dall'interconnessione tra uomo e macchina, si è registrata negli ultimi anni una notevole percentuale di investimenti nella ricerca e sviluppo in questo campo.
Il Machine Learning, nello specifico, rappresenta una parte sostanziale dei finanziamenti sull'IA, poiché permette di apprende correttamente dati forti[9] da fonti diverse e trarne informazioni per ottenere decisioni intelligenti in modo dinamico. Queta caratteristica permette all'AI di poter essere utilizzato in diversi settori e per diversi scopi, per citarne alcuni si può fare riferimento agli assistenti personali intelligenti o ai sistemi che consentono il riconoscimento facciale.

Dal punto di vista etico invece esiste una certa discrepanza che divide gli scettici, coloro che temono che questa tecnologia sostituisca le persone nei vari settori, dai fervidi sostenitori, i quali credono che l'AI sia il modo migliore per permettere all'umanità di progredire.

Secondo uno studio della società Accenture, l'intelligenza artificiale sta ora cambiando ogni area della vita, con il potenziale di aumentare la produttività del lavoro del 40% e di raddoppiare i tassi di crescita economica annuale nel 2035. Per garantire che l'IA soddisfi queste aspettative, un numero crescente di aziende e organizzazioni, tra cui la Commissione Europea, si stanno impegnando attivamente in diverse tecnologie di IA per ampliarne il contesto applicativo e permetterne una maggiore diffusione.

[9] Generalmente, un linguaggio forte ha regole di digitazione più severe al momento della compilazione. La maggior parte di queste regole influisce sull'assegnazione delle variabili, sui valori di ritorno delle funzioni, sugli argomenti di procedure e sulle chiamate alle funzioni.

2.1. Artificial Narrow Intelligence (ANI)

L'intelligenza artificiale viene classificata in termini di apprendimento, ragionamento e autocorrezione, e viene suddivisa in tre categorie:

- Artificial Narrow Intelligence (ANI);
- Artificial General Intelligence (AGI);
- Artificial Super Intelligence (ASI);

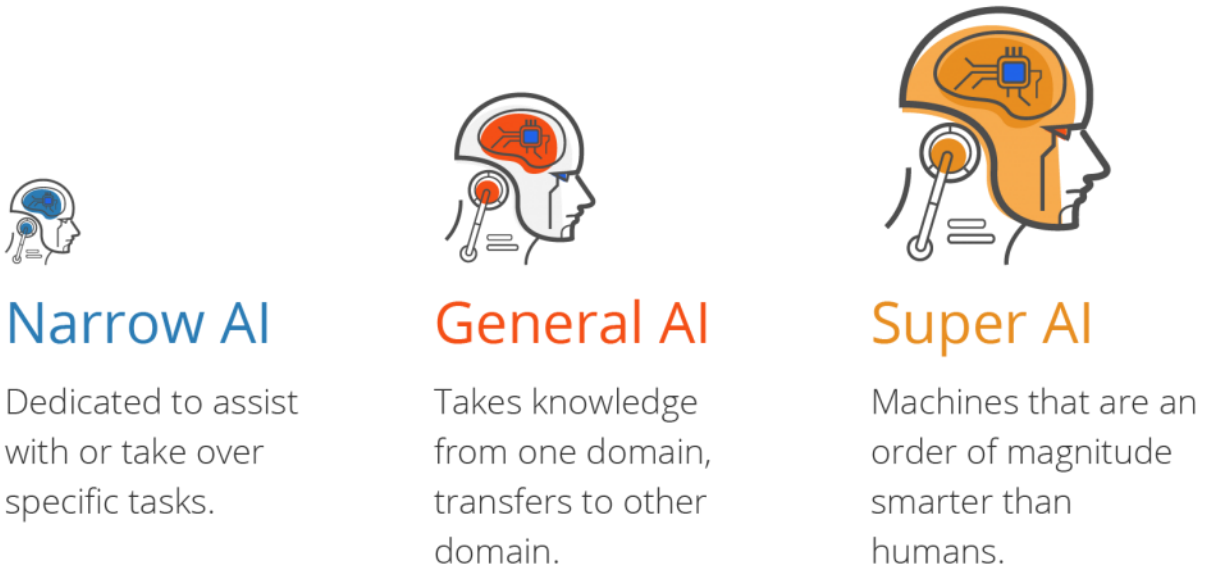


Figura 5 rappresentazione tipologie di AI

Artificial General Intelligence (AGI) detta anche Intelligenza Artificiale di Livello Umano, che si riferisce ai sistemi che possono imitare gli esseri umani e può eseguire tutti i tipi di compiti che una persona sarebbe in grado di assolvere. Questa tecnologia non verrà sviluppata prima di almeno una decina di anni ma il suo studio sta permettendo di raffinare i sistemi basati sull'ANI.

Artificial Super Intelligence (ASI): i sistemi ASI dovrebbero essere il tipo di sistemi AGI che progredirebbero rapidamente fino al punto in cui saranno in grado di sostituire gli esseri umani in quasi tutti i campi, tra cui il ragionamento cognitivo e le abilità sociali.

Artificial Narrow Intelligence (ANI) I sistemi ANI, anche conosciuti come AI debole, sono in grado di eseguire una singola attività o una gamma limitata di attività superando in molti casi persino gli esseri umani nei loro campi d'applicazione. Il limite di questa tecnologia è che al di fuori di questi campi specifici falliscono e non hanno la capacità di trasferire la conoscenze da un campo ad un altro. Nonostante questi limiti l'ANI è largamente utilizzata ad esempio nelle query dei motori di ricerca, nella proposta di elementi suggeriti (Netflix, YouTube), creazione di playlist in Spotify oppure in tutti gli assistenti vocali come Alexa e Siri.

Questa tecnologia può essere ulteriormente divisa in due sottocategorie: intelligenza artificiale simbolica e Machine Learning.

L'Intelligenza Artificiale Simbolica: L'intelligenza artificiale simbolica utilizza un set di regole definite in precedenza dai programmatori in modo molto preciso, ovvero senza alcun tipo di adattamento. Pertanto, l'Intelligenza Artificiale Simbolica è adatta per applicazioni in cui l'ambiente è prevedibile e le regole sono chiare. Sebbene l'IA simbolica sia in qualche modo caduta in disuso negli ultimi anni, la maggior parte delle applicazioni che usiamo oggi sono sistemi basati su regole.

Machine Learning (ML): è un ramo dell'IA ristretta che supporta la progettazione e lo sviluppo di algoritmi che principalmente possono imparare a completare le attività senza essere specificamente programmati dallo sviluppatore. Il grande vantaggio di questa tecnologia è che può processare una grande quantità di dati, provenienti anche da fonti differenti, e usarli per produrre previsioni basate su attività future.

Ad esempio, un algoritmo di Machine Learning formato su migliaia di transazioni bancarie con il loro esito (legittimo o fraudolento) sarà in grado di prevedere se una nuova transazione bancaria è fraudolenta o meno.

Questo approccio presenta molte declinazioni come il Deep Learning (che verrà approfondito in seguito) che è diventato particolarmente popolare negli ultimi anni. Il Deep Learning è particolarmente efficace a svolgere attività in cui i dati sono disordinati, come il Computer Vision[10] e l'elaborazione del linguaggio naturale, ovvero il linguaggio usato comunemente dalle persone.

Il Machine Learning viene diviso in tre sottocategorie principali (Il Supervised Learning, il Unsupervised Learning e il Reinforcement Learning) che si differenzia per il tipo di approccio con cui si "istruisce" l'algoritmo. Ne esiste un quarto tipi, il Semi-Supervisioned Learning, che si colloca nel mezzo dei primi due.

[10] La Computer Vision è il campo dell'informatica che si concentra sulla replica di parti basandosi sul sistema di visione umano per consentire ai computer di identificare ed elaborare oggetti in immagini e video nello stesso modo in cui fanno gli esseri umani.

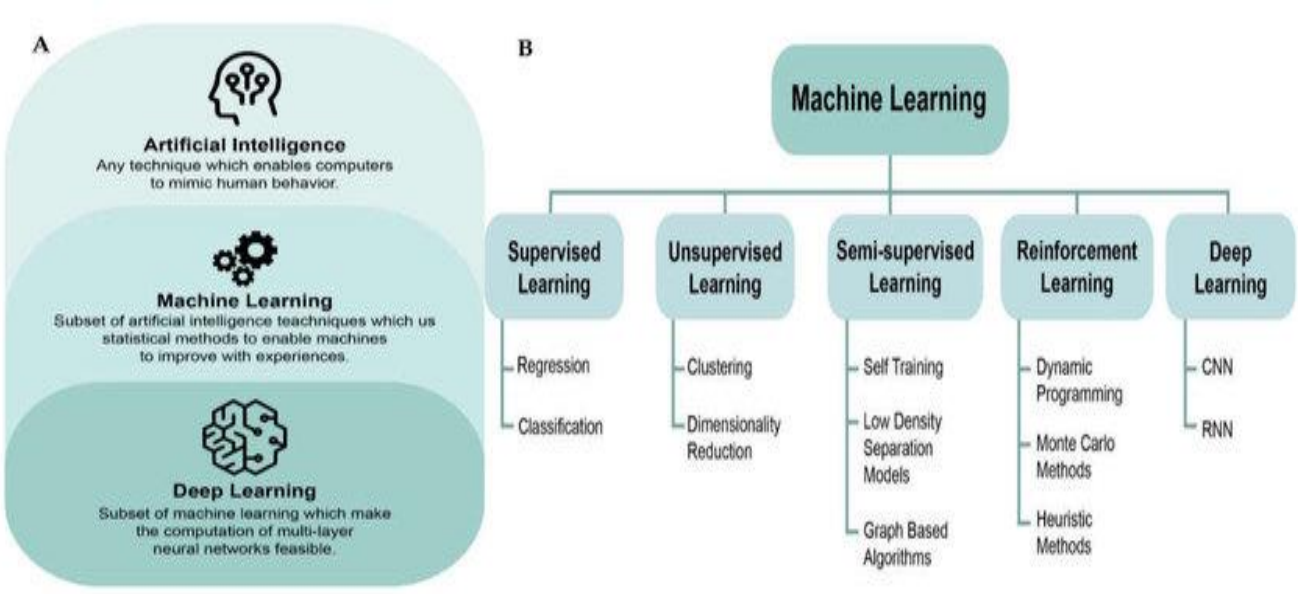


Figura 6 rappresentazione Intelligenza Artificiale, Machine Learning e Deep Learning

In conclusione, possiamo dire che l'Intelligenza Artificiale Simbolica e il Machine Learning catturano parti dell'intelligenza umana ma non riescono a essere un'intelligenza artificiale a livello umano onnicomprensivo che permetta di superare l'Intelligenza Artificiale Ristretta.

Tuttavia, gli studi in questo campo stanno permettendo sviluppi notevoli di soluzioni che vadano a supporto delle attività umane, come quella trattata nel sotto-capitolo <<Intelligenza Artificiale per Piccole e Medie Imprese>>. Nei sotto-capitoli precedenti a questo si trova una descrizione dei concetti che sono stati appena introdotti, riassunti in figura 6.

2.1.1 Machine Learning

Il Machine Learning è la scienza che ha stravolto il modello di programmazione tradizionale aiutando a creare software in grado di modificarsi e migliorarsi in termini di prestazioni senza la necessità per i programmatori d'intervenire. Questa è la tecnologia che sta dietro molte delle innovazioni che si stanno creando oggi come i suggerimenti intelligenti presenti nei siti web, assistenti digitali, auto senza conducente, software di analisi e altro ancora.

Quello che rende questa tecnologia così versatile ed innovativa è che il software impara da esempi, attraverso un "addestramento" basato su grandi insiemi di dati. Per esempio, invece di cercare di "spiegare" come è fatto un gatto ad un algoritmo (quindi creando un sistema di regole rigide) lo si "istruisce" utilizzando milioni di foto di gatti. In questo modo l'algoritmo capirà da solo come è fatto un gatto e sarà in grado di riconoscerlo anche in una foto che non ha mai "visto". Questo approccio viene anche sfruttato nell'ambito dei ANN (Artificiale Neural Networks) e nel DL (Deep Learning) come mostrato in figura 7.

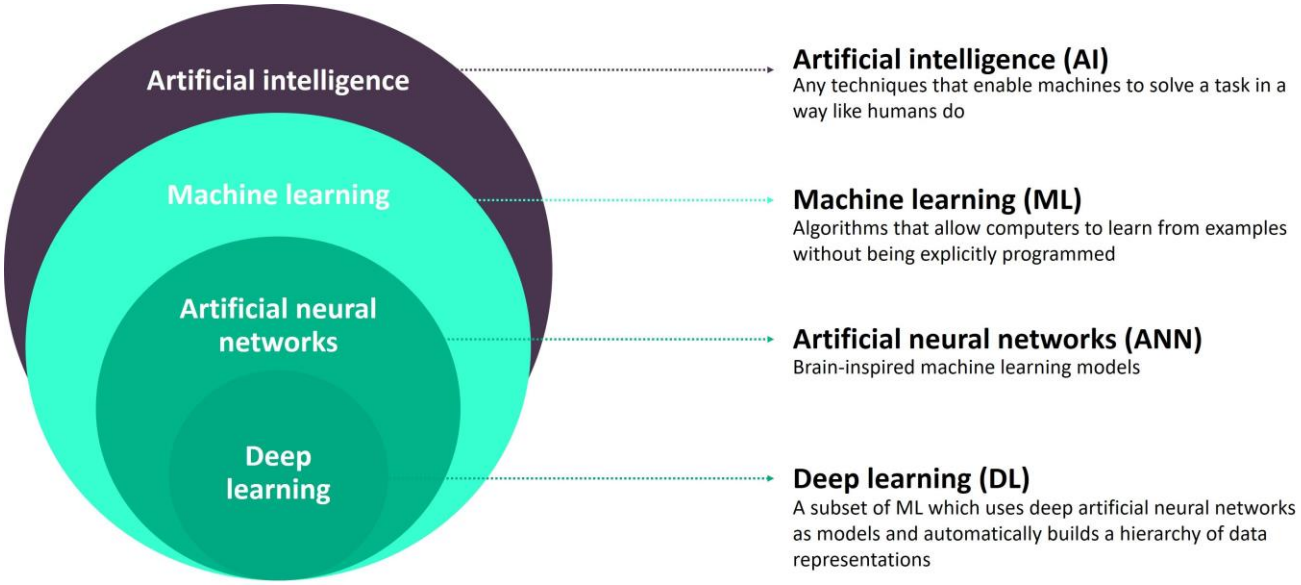


Figura 7 rappresentazione AI, ML, ANN, DL

Il processo di apprendimento inizia con osservazioni o dati, quali esempi, esperienze dirette o istruzioni, al fine di cercare modelli su cui prendere decisioni sulla base degli esempi forniti. La premessa di base del machine learning è quella di costruire algoritmi in grado di ricevere dati di input e utilizzare l'analisi statistica per prevedere un output, aggiornando i risultati man mano che nuovi dati diventano disponibili, con l'obiettivo di consentire ai calcolatori di apprendere automaticamente senza l'intervento o l'assistenza umana e regolare le azioni di conseguenza.

L'obiettivo principale di un algoritmo di Machine Learning è quello di generalizzare dalla sua esperienza. La generalizzazione in questo contesto è la capacità di un calcolatore di eseguire con

precisione nuovi compiti sfruttando l'esperienza che ha maturato in precedenza. Gli esempi di formazione provengono da una distribuzione di probabilità generalmente sconosciuta (considerata rappresentativa dello spazio delle occorrenze) e il calcolatore deve costruire un modello generale su questo spazio che gli consenta di produrre previsioni sufficientemente accurate in nuove situazioni. Per ottenere le migliori prestazioni nel contesto della generalizzazione, la complessità dell'ipotesi dovrebbe corrispondere alla complessità della funzione alla base dei dati, se l'ipotesi fosse meno complessa della funzione il modello ha sottostimato il problema. Se invece, la complessità dell'ipotesi fosse maggiore della funzione l'errore di stima si riduce, ma nel caso fosse troppo complessa il modello sarebbe soggetto a sovradimensionamento e la generalizzazione sarà più povera.

Il ML è impiegato in una serie di attività di elaborazione in cui la progettazione e la programmazione di algoritmi espliciti con buone prestazioni è difficile o impossibile. I casi includono marketing personalizzato, rilevamento delle frodi, filtraggio dello spam, rilevamento delle minacce di sicurezza di rete, la manutenzione predittiva e i notiziari sulla costruzione.

Ci sono diversi tipi di algoritmi di Machine Learning e sono tipicamente classificati in tre gruppi principali in base al tipo di dati con cui si istruiscono gli algoritmi, e sono: Supervised Learning, Unsupervised Learning e Reinforcement Learning. In figura 8 vengono rappresentati i tre tipi con le finalità d'uso relative.

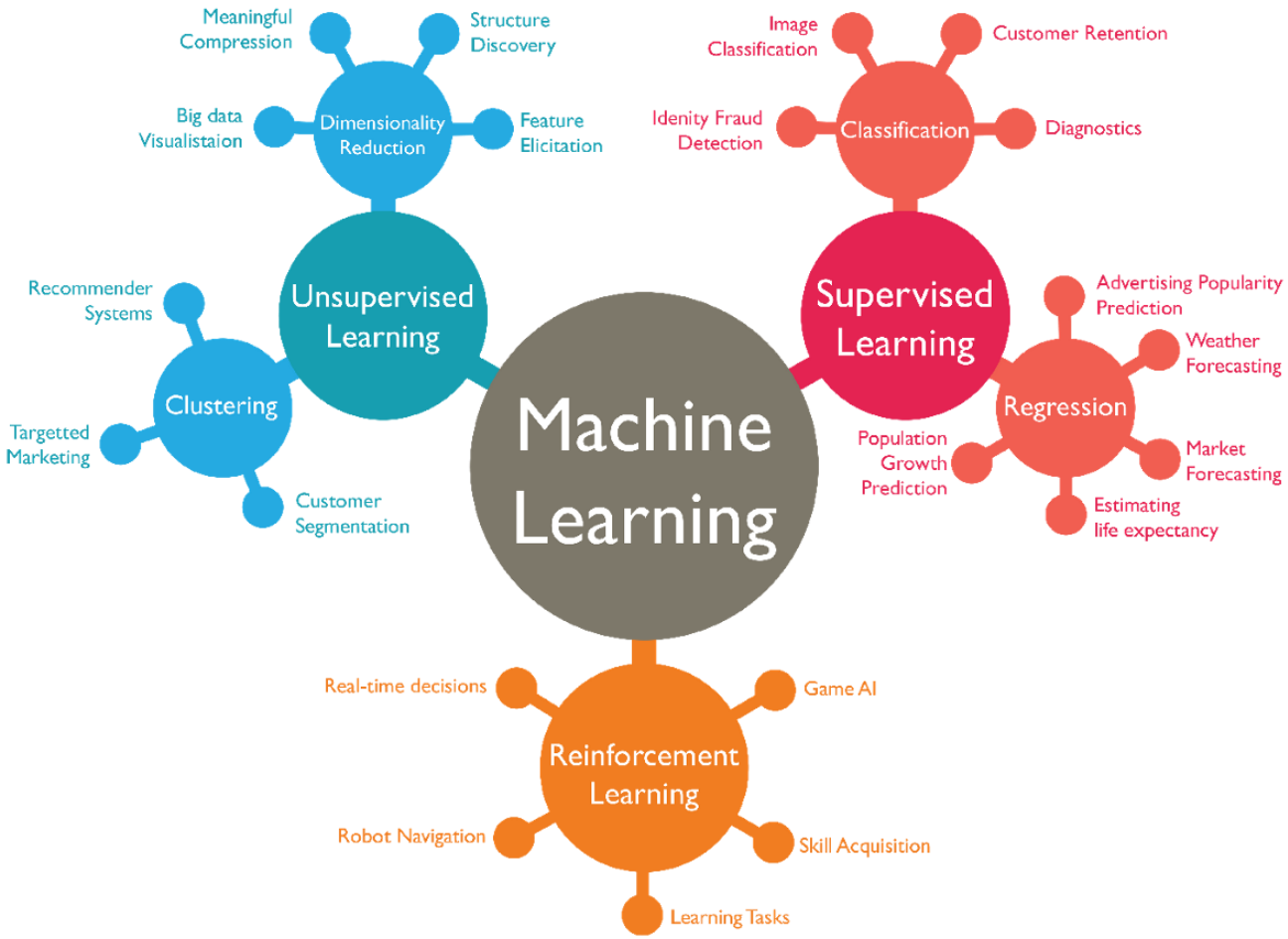


Figura 8 Machine Learning e metodi d'apprendimento

2.1.1.1 Supervised learning

Nel Supervised Learning, il computer viene "istruito" con dei dati di training in input di cui si conoscono già le soluzioni, fornite da un "insegnante", con l'obiettivo di imparare una regola generale che mappa gli input alle uscite (come rappresentato in figura 9).

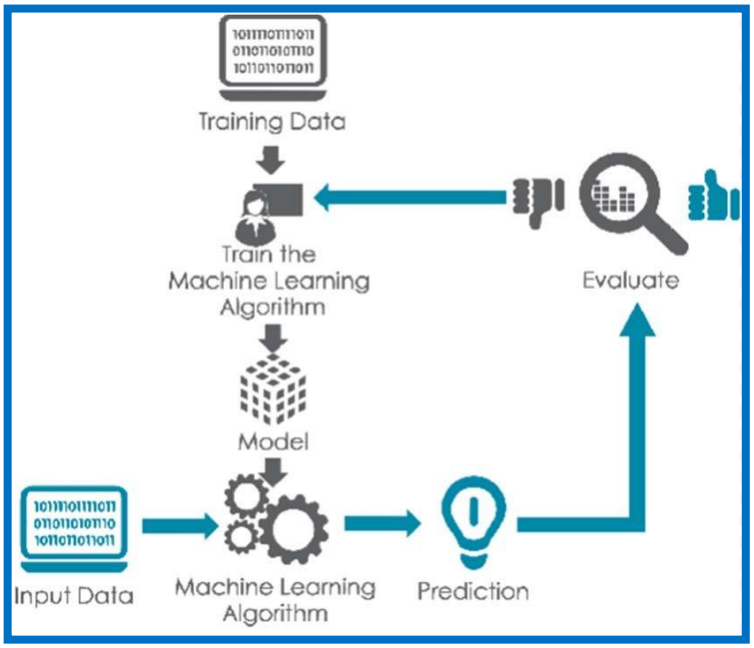


Figura 9 schema Supervised Learning

Questi algoritmi possono applicare ciò che è stato appreso in passato a nuovi dati utilizzando esempi etichettati, cioè corredati dalla loro soluzione, per prevedere eventi futuri. Partendo dall'analisi di un set di dati di allenamento noto, l'algoritmo di apprendimento produce una funzione per fare previsioni sui valori di output. Il sistema è in grado di fornire obiettivi per ogni nuovo input dopo un addestramento sufficiente.

L'algoritmo di apprendimento può anche confrontare i risultati ottenuti con i risultati corretti previsti e trovare errori per modificare di conseguenza il modello.

L'apprendimento supervisionato richiede che i possibili output dell'algoritmo siano già noti e che i dati utilizzati per addestrare l'algoritmo siano già etichettati con risposte corrette. Questo accade quando si hanno variabili di input (x) e una variabile di output (Y) e si usa un algoritmo per imparare la funzione di mapping dall'input all'output [Y = f(X)]. L'obiettivo è quello di approssimare la funzione di mappatura così bene che quando si dispone di nuovi dati di input (x) è possibile prevedere l'output variabili (Y) per tali dati.

L'apprendimento supervisionato è così chiamato perché chi crea l'algoritmo agisce come una guida per insegnargli quali conclusioni dovrebbe trarre. I programmatori determinano quali variabili, o caratteristiche, il modello dovrebbe analizzare e utilizzare per sviluppare previsioni. La risposta corretta è nota e il l'algoritmo produce iterativamente predizioni sui dati di allenamento e viene corretto dall'insegnante.

L'apprendimento si ferma quando l'algoritmo raggiunge un livello accettabile di prestazioni. Una volta completato l'addestramento, l'algoritmo applicherà ciò che è stato appreso ai nuovi dati.

L'utilizzo di questo approccio impone all'utilizzatore di seguire degli step ben precisi, che sono:

1. Determinare il tipo di esempi di formazione. Prima di fare qualsiasi altra cosa, l'utente dovrebbe decidere quale tipo di dati deve essere utilizzato come set di formazione. Nel caso dell'analisi

della scrittura a mano, ad esempio, questo potrebbe essere un singolo carattere scritto a mano, un'intera parola scritta a mano, e così via.

2. Raccogliere un set di formazione. Il set di formazione deve essere rappresentativo dell'uso reale della funzione.
   seguendo sempre l'esempio della scrittura a mano si potrebbe prendere un intero testo scritto a mano corredandolo dalle etichette, ovvero dando già in input la soluzione corretta.

3. Determinare la rappresentazione caratteristica di input della funzione appresa. L'accuratezza della funzione appresa dipende fortemente da come viene rappresentato l'oggetto di input. Tipicamente, l'oggetto di input viene trasformato in un vettore di funzionalità, che contiene una serie di caratteristiche che sono descrittive dell'oggetto. Il numero di caratteristiche non dovrebbe essere troppo grande, ma dovrebbe contenere abbastanza informazioni per prevedere con precisione l'output.

4. Determinare la struttura della funzione appresa e il corrispondente algoritmo di apprendimento. Ad esempio, l'ingegnere può scegliere di utilizzare macchine vettoriali di supporto o alberi di decisione.

5. Eseguire l'algoritmo di apprendimento sul set di formazione raccolti. Alcuni algoritmi di apprendimento supervisionato richiedono all'utente di determinare alcuni parametri di controllo. Questi parametri possono essere regolati ottimizzando le prestazioni su un sottoinsieme (chiamato set di convalida) del set di allenamento, o tramite validazione incrociata.

6. Valutare l'accuratezza della funzione appresa. Dopo la regolazione dei parametri e l'apprendimento, le prestazioni della funzione risultante devono essere misurate su un set di test diverso dal set di allenamento.

I tipi di algoritmi di apprendimento supervisionato includono l'apprendimento attivo[11], la classificazione e la regressione. Gli algoritmi di classificazione sono utilizzati quando gli output sono limitati a un insieme limitato di valori e gli algoritmi di regressione sono utilizzati quando gli output possono avere un valore numerico entro un intervallo. Ad esempio, per un algoritmo di classificazione che filtra le e-mail, l'input sarebbe un'e-mail in arrivo e l'output sarebbe il nome della cartella in cui archiviare l'e-mail.

L'apprendimento per somiglianza è un'area di apprendimento automatico supervisionato strettamente correlato alla regressione e alla classificazione, ma l'obiettivo è quello di imparare dagli esempi utilizzando una funzione di somiglianza che misura quanto simili o correlati due oggetti sono. Ha applicazioni nella produzione dei ranking, sistemi di raccomandazione, tracciamento dell'identità visiva, verifica facciale e verifica degli altoparlanti.

---

[11] L'apprendimento attivo è un caso speciale di apprendimento automatico in cui un algoritmo di apprendimento può interrogare interattivamente un utente (o qualche altra fonte di informazioni) per etichettare nuovi punti di dati con gli output desiderati. Nella letteratura statistica, è talvolta chiamato anche disegno sperimentale ottimale. La fonte di informazioni è chiamata anche insegnante o oracolo.

2.1.1.2 Unsupervised learning

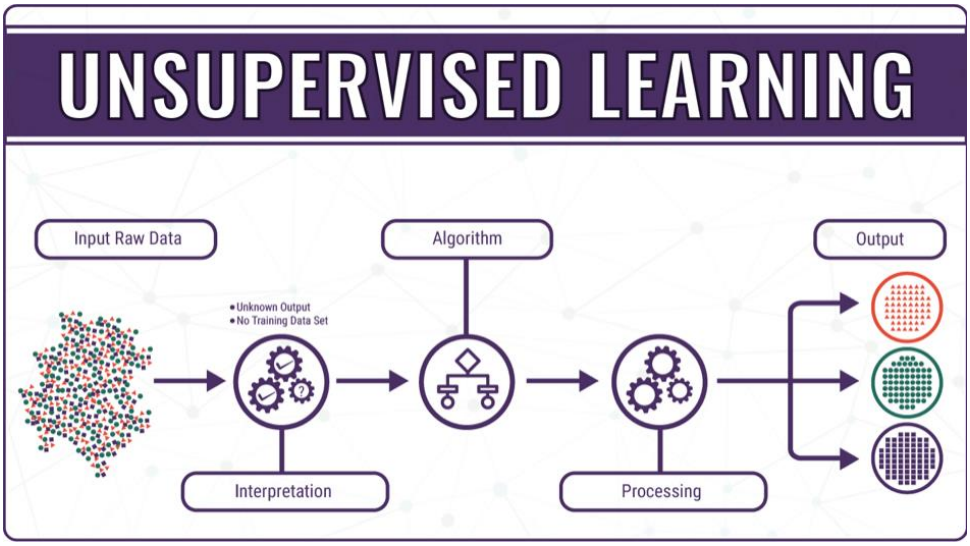


Figura 10 schema funzionamento Unsupervised Learning

A differenza dell'apprendimento supervisionato, non ci sono risposte corrette e non c'è nessun insegnante. Gli algoritmi sono "lasciati a loro stessi" per scoprire la struttura dei dati arrivando alla soluzione del problema tramite un approccio iterativo. Questo approccio è più strettamente allineato con quella che alcuni chiamano "vera intelligenza artificiale", ovvero l'idea che un computer possa imparare a identificare processi e modelli complessi senza un essere umano che fornisca una guida lungo il percorso.

Questa caratteristica permette a questi sistemi di essere più efficaci; infatti, vengono utilizzati per attività di elaborazione più complesse manipolando milioni dati identificando automaticamente correlazioni spesso sottili. Questa caratteristica ha anche reso questa tecnologia irrealizzabile fino all'inizio dell'era dei Big Data[12].

Generalmente questa tecnologia viene impiegata per risolvere problemi di raggruppamento e associazione:

- Clustering: il compito di raggruppare un insieme di oggetti in modo tale che gli oggetti nello stesso gruppo (chiamato cluster) siano più simili tra loro rispetto a quelli di altri gruppi;

- Associazione: scoprire frequenti modelli, correlazioni, associazioni o strutture causali tra le variabili in un set di dati.

[12] Il termine è utilizzato in riferimento alla capacità di analizzare ovvero estrapolare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati (grazie a sofisticati metodi statistici e informatici di elaborazione), al fine di scoprire i legami tra fenomeni diversi (ad esempio correlazioni) e prevedere quelli futuri.

2.1.1.3 Semi-Supervised Learning

Il Semi-Supervised Learning è un approccio che combina una piccola quantità di dati etichettati (ovvero che sono accoppiati ad informazioni rilevanti, es. nella foto è presente un cane) con una grande quantità di dati non etichettati (ovvero un gruppo di foto nelle quali non si sa cosa viene raffigurato) durante l'allenamento. Il Semi-Supervised Learning rientra tra l'apprendimento non supervisionato (senza dati di formazione etichettati) e l'apprendimento supervisionato (con solo dati di formazione etichettati).

I dati non etichettati, se utilizzati in combinazione con una piccola quantità di dati etichettati, possono produrre un notevole miglioramento nella precisione dell'apprendimento. L'acquisizione di dati etichettati richiede spesso personale esperto (ad es. per trascrivere un segmento audio) o un esperimento fisico (ad es. determinare la struttura 3D di una proteina o determinare se c'è olio in una particolare posizione).
Il costo di etichettature di grossi set di dati risulterebbe troppo oneroso, mentre l'acquisizione di dati non etichettati è relativamente economica. In tali situazioni, si procede producendo un piccolo insieme di dati etichettati da personale esperto, che può essere ottenuto ad un costo più basso, da utilizzare in combinazione con un sistema semi-supervisionato e dati non etichettati.

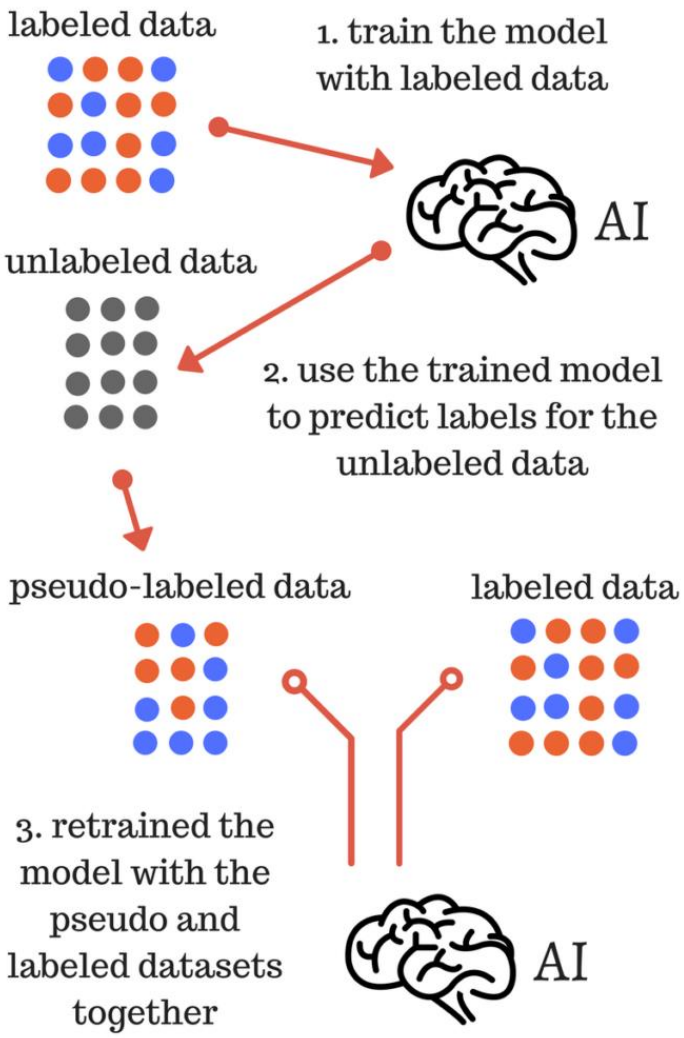


Figura 11 schema semi-supervisioned learnig

L'apprendimento semi-supervisionato può utilizzare due impostazioni: trasduttivo o induttivo. La trasduzione o l'inferenza trasduttiva è il ragionamento da casi osservati, specifici (di formazione) a casi specifici (test). Al contrario, l'induzione è il ragionamento da casi di formazione osservati a regole generali, che vengono poi applicate ai casi di prova.
L'obiettivo del primo è quello di dedurre le etichette corrette solo per i dati non etichettati forniti mentre l'obiettivo del secondo è quello di definire le etichette corrette per i dati.

2.1.1.4 Reinforcement Learning

L'apprendimento con rinforzo differisce dall'apprendimento supervisionato nel non aver bisogno di coppie di input/output etichettate da presentare e nel non aver bisogno di azioni non ottimali da correggere esplicitamente. L'obiettivo è invece quello di trovare un equilibrio tra esplorazione di nuovi dati, per apprendere di più, e sfruttamento di quelli attualmente a disposizione, per arrivare alla soluzione del problema.

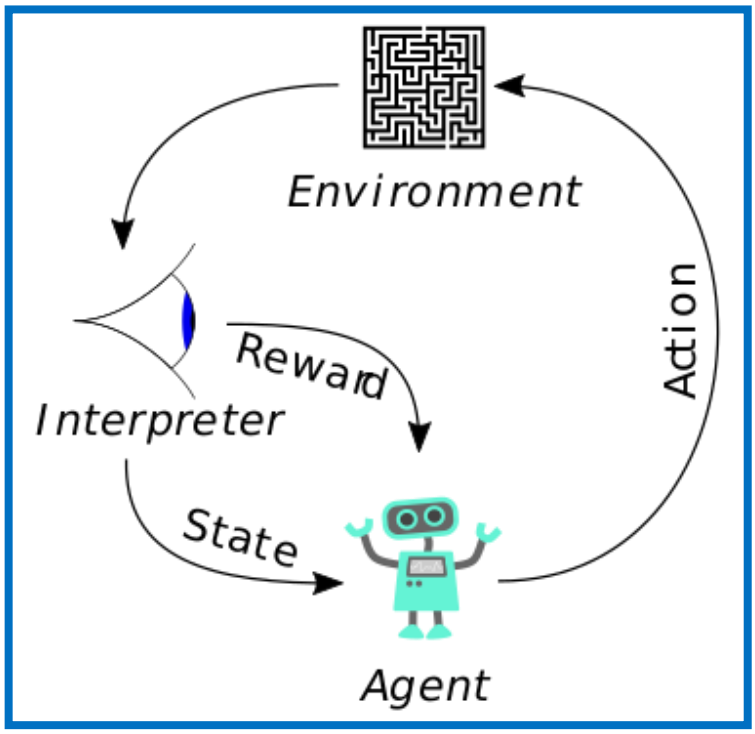


Figura 12 schema tipico di un apprendimento di rinforzo

L'ambiente è tipicamente indicato sotto forma di un processo decisionale Markov (MDP)[13], perché molti algoritmi di apprendimento con rinforzo utilizzano tecniche di programmazione dinamica[14].

I problemi di interesse nell'apprendimento con rinforzo sono stati studiati anche nella teoria del controllo ottimale, che si occupa principalmente dell'esistenza e della caratterizzazione di soluzioni ottimali e algoritmi per il loro calcolo esatto, e meno con l'apprendimento o l'approssimazione, in particolare in assenza di un modello matematico dell'ambiente.

Il rinforzo di base è modellato come un processo decisionale Markov (MDP) utilizzando:

- un insieme di stati ambientali e agenti, S;
- una serie di azioni, A, dell'agente;
- la probabilità di transizione al momento t dallo stato s allo stato s'in azione a.

---

[13] In matematica, un processo decisionale di Markov (MDP) è un processo di controllo stocastico a tempo discreto. Fornisce un quadro matematico per modellare il processo decisionale in situazioni in cui i risultati sono in parte casuali e in parte sotto il controllo di un decisore. Gli MDP sono utili per studiare i problemi di ottimizzazione risolti tramite la programmazione dinamica.

[14] La programmazione dinamica è sia un metodo di ottimizzazione matematica che un metodo di programmazione informatica. In entrambi i contesti si riferisce alla semplificazione di un problema complicato scomponendolo in sotto-problemi più semplici in modo ricorsivo.

- la ricompensa immediata dopo il passaggio da s a s'con l'azione a.

Lo scopo dell'apprendimento con rinforzo è che l'agente impari una politica ottimale, o quasi ottimale, che massimizzi la "funzione di ricompensa" o altro segnale di rinforzo fornito dall'utente che viene accumulato. Questo sistema è molto simile a quello che si verifica nel regno animale, ad esempio nell'addestramento di un cane, nel quale una punizione rappresenta un rafforzo negativo (e quindi un'azione da non ripetere in futuro) mentre un premio è un rafforzamento positivo (ovvero un'azione che devi ripetere in futuro).

Per agire in modo ottimale, l'agente deve ragionare sulle conseguenze a lungo termine delle sue azioni (cioè, massimizzare il reddito futuro), anche se la ricompensa immediata associata a questo potrebbe essere negativa. Pertanto, l'apprendimento con rinforzo è particolarmente adatto a problemi che includono un compromesso tra ricompensa a lungo termine rispetto a breve termine.

In conclusione, si può affermare che siano due le caratteristiche che rendono il Reinforcement Learning prestazionale e versatile: l'uso di campioni per ottimizzare le prestazioni e l'uso dell'approssimazione delle funzioni per affrontare ambienti di grandi dimensioni. Grazie a questi due componenti chiave può essere utilizzato nelle seguenti situazioni:

- Esiste un modello dell'ambiente, ma non è disponibile una soluzione analitica;
- Ottimizzazione di un modello che simula l'ambiente già esistente;
- L'interazione con l'ambiente è necessaria per raccogliere informazioni su di esso.

I primi due di questi problemi potrebbero essere considerati problemi di pianificazione (dal momento che è disponibile una qualche forma di modello), mentre l'ultimo potrebbe essere considerato un vero e proprio problema di apprendimento.

2.1.1.5 Artificial Neural Networks

Le Artificial Neural Networks (ANNs) sono sistemi di calcolo ispirati alle reti neurali biologiche che costituiscono i cervelli animali. Tali sistemi imparano (progressivamente migliorano la loro capacità) a svolgere compiti prendendo in considerazione esempi, generalmente senza una programmazione specifica del compito. Ad esempio, nel riconoscimento delle immagini, potrebbero imparare a identificare le immagini che contengono gatti analizzando immagini di esempio che sono state etichettate manualmente come "gatto" o "no gatto" e utilizzando i risultati analitici per identificare i gatti in altre immagini. Hanno trovato la maggior parte dell'uso nelle applicazioni difficili da esprimere con un algoritmo tradizionale che utilizza la programmazione basata su regole.

Un ANN si basa su una collezione di unità collegate chiamate neuroni artificiali (analoghi ai neuroni biologici in un cervello). Ogni connessione (sinapsi) tra neuroni può trasmettere un segnale ad un altro neurone. Il neurone ricevente (postsinaptico) può elaborare il segnale (o i segnali) e quindi inviarlo ai neuroni a valle ad esso collegati. I neuroni possono avere uno stato, generalmente rappresentato da numeri reali, tipicamente tra 0 e 1.

I neuroni sono divisi in strati, detti layer, e devono essercene almeno tre: input layer (nel quale i dati vengono immessi, hiden layer (nei quali è contenuto il modello matematico) e output layer (che emette il risultato).

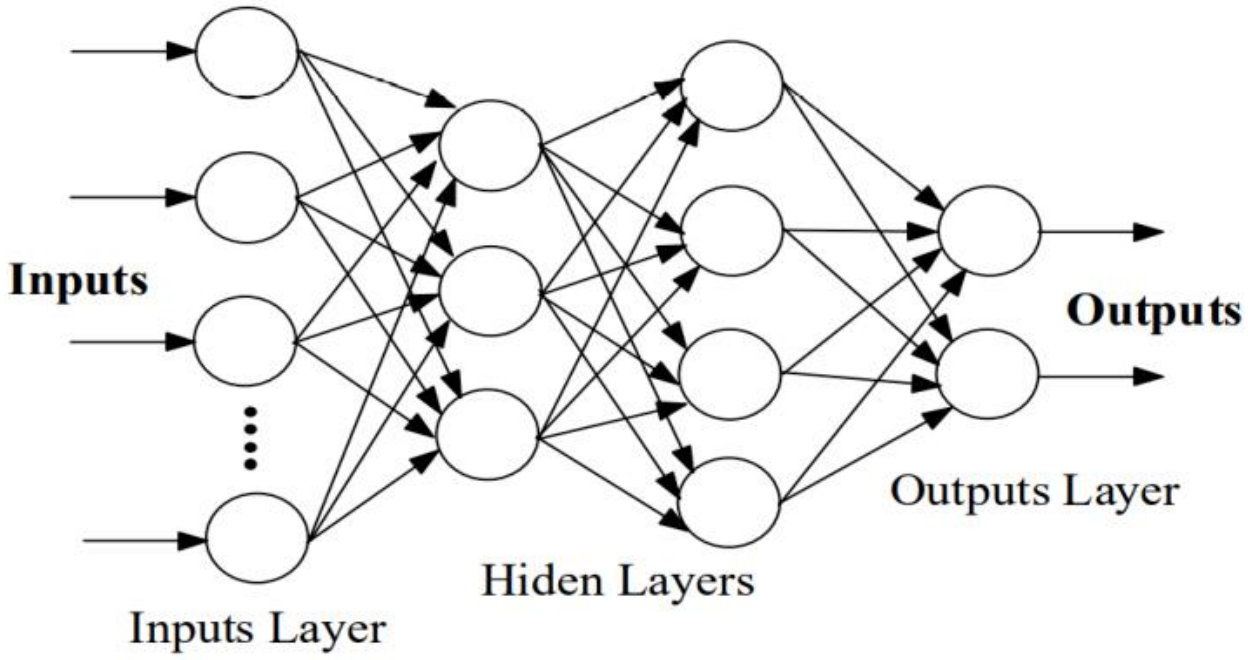


Figura 13 struttura dei layer nei ANN

Neuroni e sinapsi possono anche avere un peso che varia con il processo di apprendimento, che può aumentare o diminuire l'intensità del segnale che invia a valle, la variazione dei pesi permette al programma di apprendere.
In un primo momento, l'ANN crea una mappa dei neuroni virtuali e assegna valori numerici casuali, o "pesi", alle connessioni tra di essi. I pesi e gli input sono moltiplicati e restituiscono un output tra 0 e 1. Se la rete non riconoscesse accuratamente un particolare pattern, un algoritmo regolerebbe i pesi. In questo modo l'algoritmo può rendere alcuni parametri più influenti, fino a determinare la corretta manipolazione matematica per elaborare completamente i dati.

In particolare, il programma ottimizza la funzione di loss (ovvero la differenza tra l'output predetto dal programma con il risultato corretto) correggendo iterativamente i pesi di tutte le connessioni partendo dall'ultimo arrivando al primo. Questo procedimento prende il nome di Backpropagation.

Queste caratteristiche permettono all'ANN di modellare relazioni complesse non lineari generando modelli composti in cui l'oggetto è espresso come una composizione stratificata di primitive. Gli strati aggiuntivi consentono la composizione di caratteristiche provenienti da strati inferiori, potenzialmente modellando dati complessi con un numero inferiore di unità rispetto a una rete superficiale (ovvero con meno di 2 layer) con prestazioni simili.

Gli ANN sono tipicamente reti feedforward, ovvero i dati fluiscono dal livello di input al livello di output senza looping back (quindi senza riattivare i neuroni nei layer precedenti).

2.1.1.5.1 Deep Learning

Il Deep Learning è un sottoinsieme specializzato del Machine Learning, che utilizza le reti neurali, ovvero una replica artificiale della struttura e della funzionalità del cervello.

Il Deep Learning risolve uno dei principali problemi presenti nelle vecchie generazioni di algoritmi di apprendimento: con la crescita dei set di dati, l'efficienza e le prestazioni degli algoritmi di Machine Learning crollano, mentre gli algoritmi di Deep Learning continuano a migliorare man mano che vengono alimentati con più dati.

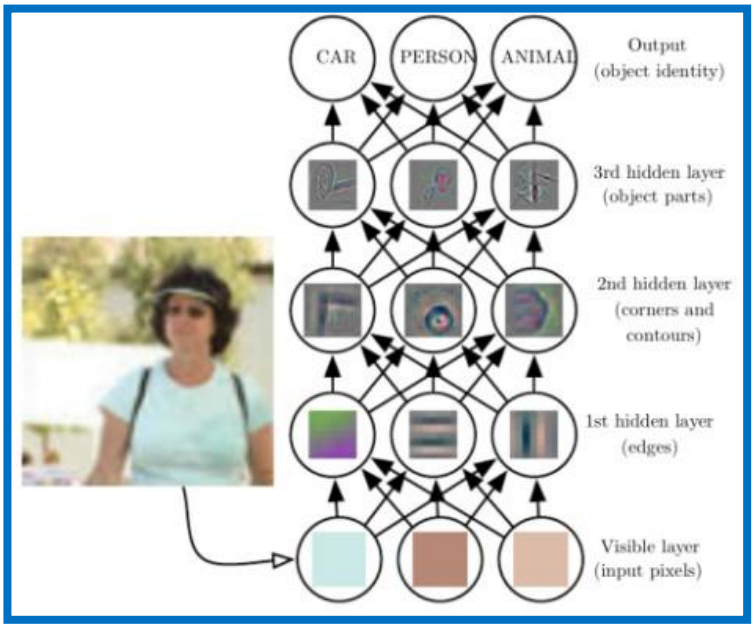


Figura 14 Rappresentazione di immagini su più livelli di astrazione in deep learning

La maggior parte dei modelli di deep learning sono basati su reti neurali artificiali, in particolare Convolutional Neural Networks CNN, sfruttando una struttura multy-layer. Le CNN sono un caso particolare delle ANN in cui gli hiden layer hanno hanno all'interno dei filtri con cui manipolano i dati.

Nel Deep Learning ogni livello impara a trasformare i propri dati di input in una rappresentazione leggermente più astratta. In un'applicazione di riconoscimento di immagini, l'input grezzo può essere una matrice di pixel; il primo livello rappresentativo può astrarre i pixel e codificare i bordi; il secondo livello può comporre e codificare le disposizioni dei bordi; il terzo livello può codificare un naso e gli occhi; e il quarto strato può riconoscere che l'immagine contiene un volto. In figura 14 è si può vedere una rappresentazione grafica di come funziona questa struttura multy-layer.

È importante sottolineare che un processo di Deep Learning può imparare quali caratteristiche posizionare per ogni livello, in assoluta autonomia. Tuttavia, una taratura manuale del sistema può essere necessaria in determinate condizioni.

La parola "deep" in "deep learning" si riferisce al numero di livelli attraverso i quali i dati vengono trasformati. Un algoritmo per essere definito di Deep Learning deve possedere almeno 2 strati tra l'Input e L'output layer.

In particolare, i primi due layer permettono al sistema di elaborare il modello matematico che approssima la rete mentre quelli successivi aiutano ad apprendere le funzionalità in modo efficace.

2.2. Intelligenza Artificiale per Piccole e Medie Imprese

Come discusso nel primo capitolo di questa tesi è chiaro come le aziende, specialmente quelle medio-piccole, necessitino di questa transizione green anche se, a livello pratico, non è sempre chiaro quali siano gli obbiettivi da raggiungere e come raggiungerli.

La mancanza di un contesto normativo chiaro e di una cultura adeguata in materia rendono questi cambiamenti ancora più difficili da applicare.
Per colmare questa lacuna è stato progettato, in sede di tirocinio, un modulo di Intelligenza Artificiale che ha l'obbiettivo di supportare e guidare le PMI attraverso l'implementazione di processi circolari sostituendo o migliorando i processi aziendali che sono già in atto.

È importante sottolineare che questo strumento è stato concepito come un "mentore" che aiuta e supporta gli ingegneri, senza mai cercare di sostituirli. Questa condizione, fondamentale per la buona riuscita del progetto, è necessaria per due motivazioni:

- La prima è quella di "utilizzare" l'esperienza degli Ingegneri per migliorare i processi delle aziende in cui lavorano, avendone visione più ampia di quello che può avere questo modulo di intelligenza artificiale, in modo da rendere lo strumento più efficace.

- La seconda è di carattere etico in quanto l'obbiettivo del progetto è quello di insegnare e far risaltare le criticità dando spunti per risolverle, esattamente come farebbe un buon mentore.

Queste richieste sono state concretizzate in un modulo di Intelligenza Artificiale strutturato come in figura 15.

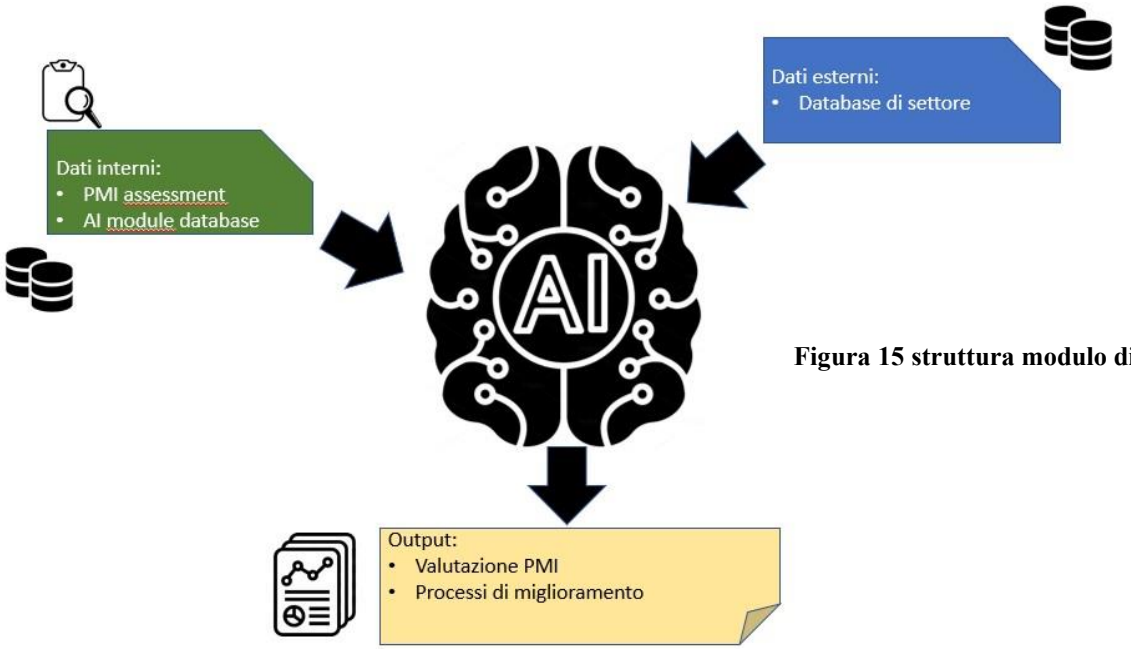


Figura 15 struttura modulo di AI

2.2.1 Funzionamento

Per l'utilizzo di questo modulo di AI è stato predisposto un processo a 5 step:

1. PMI assessment[15]: in questa fase le imprese devono compilare un assessment creato con l'obbiettivo di valutare il loro grado di circolarità. L'assessment è diviso in categorie che comprendono le risorse (es. materiche e non materiche) e i processi aziendali (come la logistica) alle quali verrà assegnato un punteggio nello step 3.

2. Analisi dei dati: il modulo di AI confronta i dati ottenuti dall'assessment con i dati esterni e i dati presenti nel AI Module Database, nel quale sono raccolti tutti gli assessment precedentemente compilati.
   I dati esterni vengono raccolti dalle banche dati settoriali di ogni nazione aderente al progetto e normalizzati in modo da essere il più affini possibili alla struttura del PMI assesment.
   L'utilità di questo database è quello di permettere al modulo di AI di effettuare analisi efficaci anche quando i dati interni non sono disponibili o sono scarsi.

3. Valutazione PMI: Conclusa l'analisi il modulo di intelligenza artificiale conferisce una valutazione della circolarità dell'organizzazione, divisa sia per categoria sia come dato aggregato. Questo dato risulta di fondamentale importanza in quanto identifica il punto di partenza per l'organizzazione, mostrando quali sono le aree o processi su cui intervenire.
   questa valutazione può essere usata dall'azienda anche per altri scopi, ad esempio come leva per richiedere finanziamenti.

4. Report di circolarità: Con la conclusione dello step 3 il modulo di AI emette un report che contiene sia la valutazione di circolarità sia le azioni da intraprendere per migliorarla. Alla fine di questo passaggio tutti i report vengono immagazzinati nel AI Module Database.

5. PMI assessment: il processo riparte dallo step 1, con cadenza periodica di almeno sei mesi o un anno a seconda delle attività che si sono intraprese, compilando il PMI assesment per valutare se c'è stato un miglioramento e misurarne l'entità.
   Nello stesso assesment viene anche richiesto all'utente di valutare le azioni di miglioramento suggerite allo step 4 indicando anche le attività che hanno realmente svolto. Questo feedback è estremamente importante per il modulo di AI in quanto lo utilizzerà per migliorarsi e diventare sempre più preciso nel proporre azioni di miglioramento.

Come risultato di questo processo si otterranno un miglioramento della circolarità dell'organizzazione che lo utilizza e un affinamento dello strumento. Perché questi due risultati vengano raggiunti è stato necessario scegliere attentamente la struttura di questo modulo di AI.

[15] I contenuti e le specifiche di questo assessment sono proprietà intellettuale del progetto, pertanto non condivisibile all'interno di questo documento. La struttura dello stesso è basata sulla ISO/TS 11820 che al momento di scrittura di questo documento è in inchiesta pubblica ufficiale che si concluderà il 20 Aprile 2022.

2.2.2 Sviluppo modulo di Intelligenza Artificiale

Lo sviluppo di questo modulo di intelligenza artificiale parte dalla creazione di una Artificial Neuronal Network nella quale l'input layer è composto dagli indicatori presenti nell'assesment, gli hidden layer processano queste informazioni e restituiranno in output le informazioni che saranno contenute nel report.

Il metodo scelto per l'apprendimento è il Semi-Supervisioned Learning in quanto:

1. non è possibile avere dati totalmente etichettati (quindi corredati già con una soluzione), rendendo inutilizzabile il Supervisioned Learning.

2. utilizzare dati totalmente non etichettati, quindi per il Unsupervisioned Learning, renderebbe il processo di apprendimento molto lungo visto che le iterazioni sono lente. In questo caso per iterazioni si intende il miglioramento di almeno un processo aziendale con la misurazione dell'entità di quest'ultimo.

Per superare questi ostacoli si procederà nel seguente modo:

1. Verranno inviati degli esperti di Economia Circolare in quattro aziende differenti con l'obbiettivo di:

    a. Migliorare i loro processi, partendo dall'assessment, senza utilizzare il modulo di intelligenza artificiale

    b. Raccoglierne i dati relativi a queste attività. Queste informazioni diventeranno il data labeled set;

2. In contemporanea si diffonderà l'assesment anche ad altre organizzazioni senza una supervisione diretta, quindi senza inviare esperti. Con questi dati si otterrà il data unlabeled set. Da notare che questo secondo set sarà molto più grande del primo;

3. Addestramento dell'ANN usando il primo set di dati etichettati, come nel caso di un Supeervised Learning, suddividendolo in tre sottogruppi:

    a. Training set: questi dati vengono consegnati al programma con le loro etichette, quindi la soluzione trovata dagli esperti, in modo che possa capirne la logica. L'algoritmo di ottimizzazione modificherà le funzioni contenute negli hidden layer per ottimizzare quella che viene chiamata la funzione di loss, ovvero la differenza tra l'output del programma e quello ottenuto dagli esperti.

    b. Validation test: questi dati vengono anch'essi consegnai con l'etichetta ma hanno la funzione di misurare l'overfitting del sistema, che verrà discusso in seguito;

c. Test set: questi dati vengono consegnati senza l'etichetta in modo da verificare se il sistema arriva alla soluzione corretta;

4. In questo passaggio si conferiscono al sistema solo i dati unlabeled in modo da attuare un sistema noto come lo Pseudo-Labeling, ovvero il sistema conferisce le etichette ai dati in autonomia.

5. Addestramento del sistema tramite l'uso congiunto sia dei dati labeled che quelli unlabeled. L'utilizzo di questi dati in modo congiunto aumenta sensibilmente l'accuratezza del sistema e la sua capacità di generalizzazione.

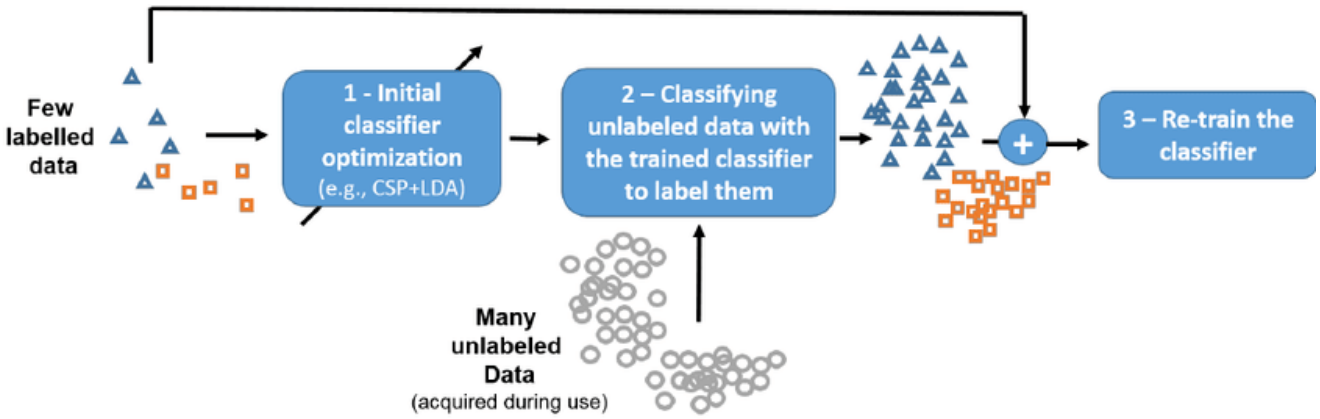


Figura 16 schema dell'addestramento del modulo di AI

2.2.3 Ottimizzazione

L'implementazione di processi circolari all'interno delle aziende richiede attività molto diverse che però dipendono anche dal settore a cui appartengono. Pertanto, per rendere efficace il modulo di AI e ridurne i tempi di apprendimento, si è deciso di focalizzarsi sul settore del Manufacturing che è anche quello che più necessita di velocizzare la Twin Transition.

Come anticipato nel capitolo precedente, sono state selezionate 4 aziende per la raccolta dei dati con i quali si addestreranno il modulo di AI. La selezione ha preso in considerazione:

- Dimensione dell'azienda: si è preferito scegliere aziende più grandi e strutturate in modo da semplificare la raccolta dei dati e l'utilizzo stesso del modulo di AI;
- Precedenti esperienze nella Economia Circolare: questo è un fattore determinante in quanto permette di semplificare notevolmente i lavori;
- Settore di appartenenza: si sono scelte quattro organizzazioni operanti in ambiti differenti (Automotive, produzione e riciclaggio delle batterie, Metallurgia, Tessile) in modo da ottenere un sistema versatile che non fosse affetto da overfitting.

L'overfitting si verifica quando un modello di machine learning diventa troppo specifico sui dati su cui è stato addestrato e quindi perde la sua applicabilità per qualsiasi altro set di dati. Un modello è overfitted quando è così specifico per i dati originali che cercare di applicarlo ad altri dati porterebbe ad ottenere risultati errati e quindi a decisioni non ottimali. L'overfitting viene anche evitato grazie all'utilizzo dei dati Unlabeled provenienti da altre aziende.
Al contrario l'underfitting del sistema è l'incapacità di interpretare correttamente il training data set, come rappresentato in figura 17.

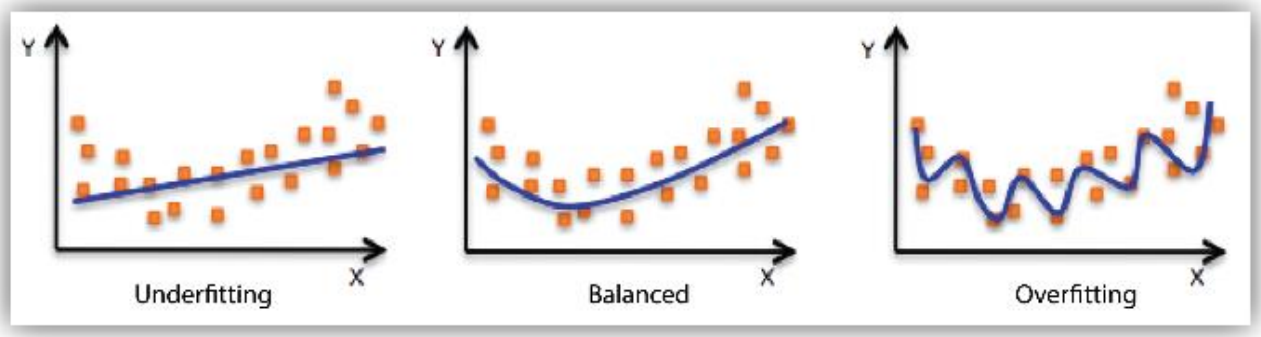


Figura 17 rappresentazione fitting del sistema

Il secondo problema da risolvere è la normalizzazione dei dati ovvero la congruenza tra loro dei dati, ovvero bisogna fare in modo che le valutazioni non siano dipendenti dalla dimensione dell'azienda. Questo problema viene raggiunto tramite l'assesment che converte tutti i risultati in percentuali o in sì/no a seconda del tipo di domanda, garantendo una perfetta confrontabilità tra i dati.

3. Blockchain

La parola Blockchain era inizialmente solo un termine in informatica che rappresentava un modo con cui strutturare e scambiare i dati. Oggi la Blockchain è considerata la "quinta evoluzione" nell'ambito dell'informatica che si sta integrando con i vecchi sistemi. Si può pensare alla Blockchain come database distribuiti che sono gestiti da un gruppo di persone, che sono in grado di memorizzare e scambiare dati, generando una un network.

Il termine Blockchain è un termine generico del quale fanno parte svariate architetture sia software che hardware. In generale si può vedere la Blockchain come un libro mastro che aiuta a tenere traccia di tutte le transazioni che avvengono tra utenti all'interno di un network. La peculiarità è che tutti gli utenti possiedono lo storico di tutte le transazioni avvenute, e verificate, all'interno di una stessa rete.

L'altra caratteristica che rende la Blockchain unica è l'impossibilità di cancellare o modificare i registri a posteriori. In termini pratici ogni utente possiede un registro nel quale vengono scritte in ordine temporale tutte e transazioni avvenute che nessuno, neanche il proprietario, può modificare una volta che la transazione sarà verificata. Questo concetto, che rende la Blockchain sicura e trasparente, verrà illustrato meglio nel capitolo relativo.

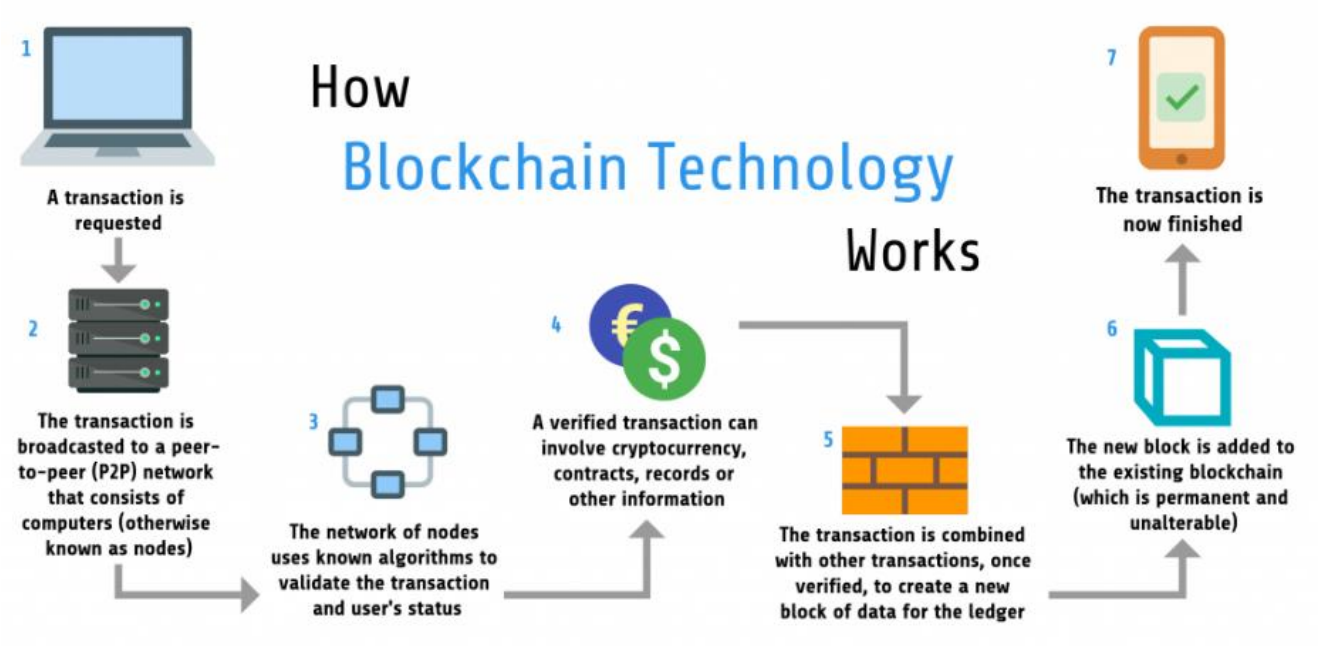


Figura 18 il processo della Blockchain

Per apprezzare meglio questa tecnologia bisogna fare un passo indietro e analizzare un sistema tradizionale, ad esempio quello del settore bancario.

Nel caso di una transazione monetaria, come un bonifico, se una persona (A) volesse fare un bonifico ad un'altra (B) necessiterebbe di passare tramite un intermediario soverchiante rispetto ad entrambi (la banca). Questultimo controlla la veridicità della transazione (correttezza delle coordinate bancarie, credito sufficiente, ecc) e poi valida la transazione inpiegandoci in media qualche giorno lavorativo.

La Blockchain invece, a meno di casi particolari, non usa un ente terzo per confermare le transazioni ma si avvale di algoritmi. Il risultato è che gli enti terzi non sono più in grado di commettere frodi e rende le trasazioni molto veloci in quanto il processo di validazione impiega mediamente 10 minuti per essere completato.

3.1 Caratteristiche

Immutability and Distributed Ledger

Non c'è un'autorità centrale o una sola persona per gestire la rete. Tutti i partecipanti hanno una copia del registro digitale e chiunque può essere un nodo e può partecipare alla registrazione. Da questo segue il fatto che se si volesse corrompere la rete, si dovrebbero modificare tutti i dati memorizzati su ogni nodo della rete. Dal momento che milioni di persone hanno una copia dei dati, sarà impossibile riuscirci. Gli utenti della rete possono convalidare o rifiutare i dati in base a regole di consenso.

Secure System

I codici hash nei blocchi sono determinati dopo sofisticate operazioni matematiche, quindi, la Blockchain ha una struttura molto complessa ed è impossibile modificarla. Poiché i record sono conservati in più posizioni, le informazioni non vengono perse se una singola rete viene danneggiata o se subisce un attacco informatico. Inoltre, la modifica dei dati effettuata da un singolo utente è considerata non valida in caso di conflitto con i record su un'altra rete.

Transparency

Ogni membro autorizzato ad accedere può seguire e visualizzare in modo trasparente il ciclo di vita dei dati, la transazione e tutte le impronte storiche. Le informazioni private delle parti sono criptate per mantenere la privacy personale.

Peer to Peer Network

Contrariamente a un semplice modello Client-Server, dove le risorse sono memorizzate nel server e possono essere accessibili solo dal client su richiesta, un sistema di elaborazione P2P è composto da una rete di peer o nodi che condividono informazioni e risorse senza la necessità di un'entità centrale.

Ogni partecipante sulla rete ha la propria copia sincronizzata. Così, i partecipanti possono visualizzare e confermare le transazioni che si svolgono sulla rete.

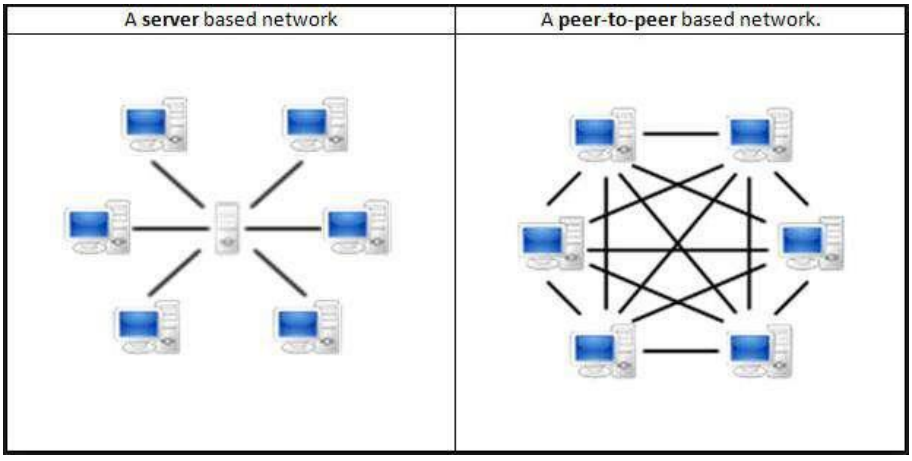


Figura 19 rappresentazione server base- peer-to-peer network

Cryptography

La Blockchain si avvale di un sistema di crittografia dei dati per anonimizzare gli utenti e rendere illeggibile il contenuto delle informazioni. Il sistema utilizzato e il cryptographic hash function (CHF)

Una funzione CHF è un algoritmo matematico che mappa i dati di una dimensione arbitraria in un vettore di dimensione fissa, che prende il nome di hash, con la caratteristica principale di essere unidirezionale, cioè una funzione per la quale è praticamente impossibile invertire il calcolo.

Oltre a questa principale ve ne sono altre, che possono anche non verificarsi sempre, che sono:

- deve essere deterministica, il che significa che lo stesso messaggio produce sempre lo stesso hash;
- veloce da calcolare;
- è impossibile generare un messaggio che produca un dato valore hash;
- è impossibile trovare due messaggi diversi con lo stesso valore di hash. Infatti, una piccola modifica del messaggio dovrebbe generare un cambiamento estremamente esteso del codice hash associato.

3.2 Tipologie di Blockchain

Esistono svariati tipi di Blockchain, le quali differiscono per tipo di architettura della rete o algoritmo di consenso. Nel primo caso si possono identificare quattro categorie:

1. Public Blockchains

Le Blockchain pubbliche sono di natura permissionless, ovvero permettono a chiunque di unirsi e sono completamente decentralizzate. Le Blockchain pubbliche consentono a tutti i nodi della Blockchain di avere uguali diritti per accedere alla Blockchain, creare nuovi blocchi di dati e convalidare i blocchi di dati.

Ad oggi, le Blockchain pubbliche sono utilizzate principalmente per lo scambio e il mining (ovvero la risoluzione di un problema matematico) di criptovalute. Gli esempi tipici di questa tipologia sono Bitcoin, Ethereum e Litecoin. Su queste Blockchain pubbliche, i nodi creano blocchi per la validazione delle transazioni richieste sulla rete risolvendo equazioni crittografiche. In cambio di questo duro lavoro, i nodi guadagnano una piccola quantità di criptovaluta.

2. Private Blockchains

Le Blockchain private, che possono anche essere indicate come Blockchain gestite, sono Blockchain autorizzate controllate da una singola organizzazione. In una Blockchain privata, l'autorità centrale determina chi può essere un nodo, quindi chi può entrare nella rete. L'autorità centrale, inoltre, non concede necessariamente a ciascun nodo uguali diritti per svolgere funzioni, ad esempio non tutti i nodi possono verificare le transazioni. Le Blockchain private sono solo parzialmente decentralizzate perché l'accesso pubblico a queste Blockchain è limitato. Alcuni esempi di Blockchain private sono la rete di cambio valuta virtuale business-to-business Ripple e Hyperledger, un progetto ombrello di applicazioni Blockchain open-source.

Sia le Blockchain private che quelle pubbliche hanno degli svantaggi - le Blockchain pubbliche tendono ad avere tempi di convalida più lunghi per i nuovi dati rispetto alle Blockchain private, e le Blockchain private sono più vulnerabili alle frodi.

3. Consortium Blockchains

Le Blockchain consortili sono Blockchain autorizzate governate da un gruppo di organizzazioni, piuttosto che da un'unica entità, come nel caso della Blockchain privata. Le Blockchain consortili, quindi, godono di una maggiore decentralizzazione rispetto alle Blockchain private, con conseguenti livelli di sicurezza più elevati. Tuttavia, la creazione di consorzi può essere un processo difficoltoso in quanto richiede la cooperazione tra un certo numero di organizzazioni, che presenta sfide logistiche e potenziali rischi antitrust.

Un popolare insieme di soluzioni Blockchain consortili per il settore dei servizi finanziari è stato sviluppato dalla società di software aziendale chiamata R3. Nel settore della supply chain, CargoSmart

ha sviluppato il Global Shipping Business Network Consortium, un consorzio Blockchain no-profit che mira a digitalizzare il settore marittimo e consentire agli operatori del settore marittimo di lavorare in modo più collaborativo.

4. Hybrid Blockchains

Le Blockchain ibride sono Blockchain che sono controllate da una singola organizzazione, ma con un livello di supervisione eseguito dalla Blockchain pubblica, che è necessario per eseguire determinate convalide di transazione. Un esempio di Blockchain ibrida è IBM Food Trust, che è stato sviluppato per migliorare l'efficienza in tutta la catena di approvvigionamento alimentare.

Sebbene il concetto di Blockchain sia stato introdotto per implementare la trasparenza totale nelle transazioni Bitcoin, a volte sorge la necessità di limitare l'accesso specialmente nel caso di scrittura per consentire agli individui e alle istituzioni di limitare le loro transazioni a sé stessi e non lasciare che gli estranei modifichino o compromettano il loro network. Per questo motivo sono state create le Blockchain permissioned.

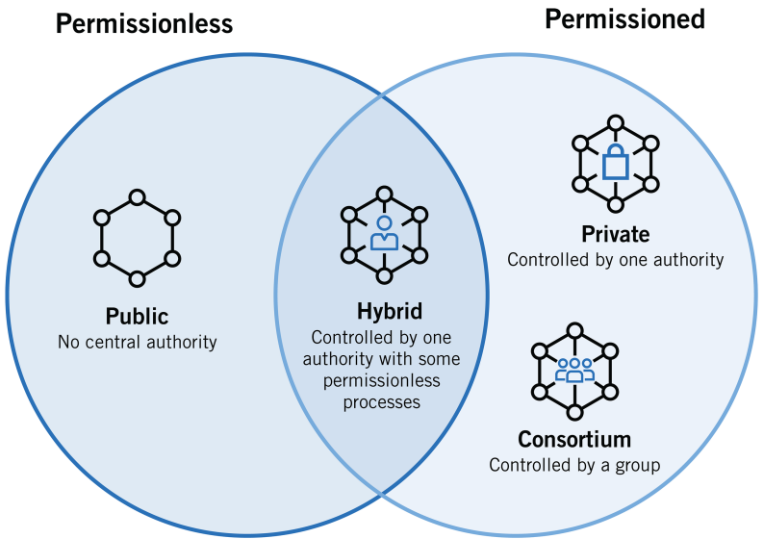


Figura 20 tipologie di Blockchain

3.3 Anatomia

Per chiarezza nella descrizione della tecnologia Blockchain in questa tesi, verranno descritti gli elementi tecnici che sono alla base di questa tecnologia. È essenziale sottolineare che questi sono elementi fondamentali che costituiscono le Blockchain in generale e non un tipo specifico. Quindi, i seguenti concetti sono elementi cruciali che possono applicarsi ad ogni singolo applicazione di questa tecnologia

Blocchi

Le strutture in cui sono memorizzati tutti i dati delle transazioni sono chiamate blocchi e sono ordinate temporalmente. Il primo blocco viene chiamato blocco di genesi. Ogni blocco contiene: l'hash univoco (ovvero il codice univoco con cui ricercare il blocco), l'hash nel blocco precedente, un timestamp (ovvero la data e e l'ora) e i dati di transazione.

I dati memorizzati in un blocco variano a seconda del tipo di Blockchain e dal tipo di utilizzo. Ad esempio, i blocchi di criptovalute memorizzano i dati delle transazioni come il mittente, il destinatario e la quantità di denaro.

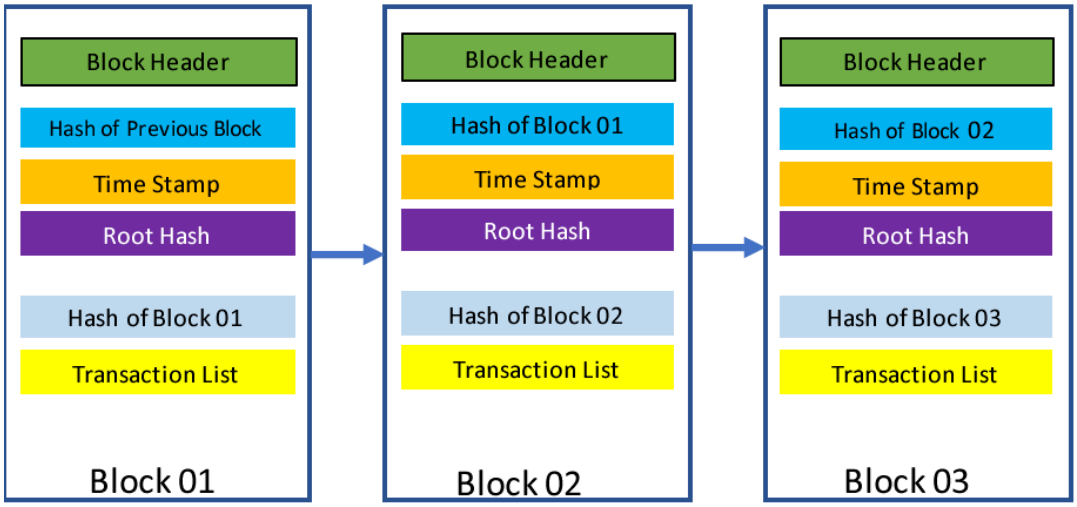


Figura 21 struttura dei blocchi

Transazioni

Una transazione è un particolare evento memorizzato in un blocco di dati. Questi eventi sono record di dati che vengono crittografati e concatenati insieme alla Blockchain. I partecipanti alla rete utilizzano delle firme digitali per autenticare la proprietà delle loro transazioni. Alcuni esempi di operazioni includono gli scambi finanziari tra utenti o il risultato dei dati immessi nella catena.

Per esempio, una transazione nel caso di Bitcoin può essere una vendita di un bene (correlata ad una certa quantità di Bitcoin) da parte di un utente ad un altro. Grazie alla natura decentralizzata della Blockchain, queste transazioni possono avvenire senza che un terzo di fiducia agisca come arbitro.

Firme digitali

In Blockchain, gli utenti possono firmare e verificare l'autenticità di una transazione. I partecipanti lungo la catena possono innescare questi eventi o dimostrare che si sono verificati in un determinato momento, recuperando le informazioni necessarie da molti nodi della rete.

Il sistema richiede che l'emittente di una transazione segni un hash contenente la transazione precedente e la chiave pubblica del destinatario, utilizzando la sua chiave privata. In questo modo, il ricevente può verificare l'autenticità di una transazione rintracciando la catena di proprietà utilizzando la chiave pubblica dell'emittente. Anche se i firmatari trasferiscono la proprietà di una transazione, la loro firma rimarrà per sempre nella catena. Il processo di firma digitale è mostrato in Figura 22.

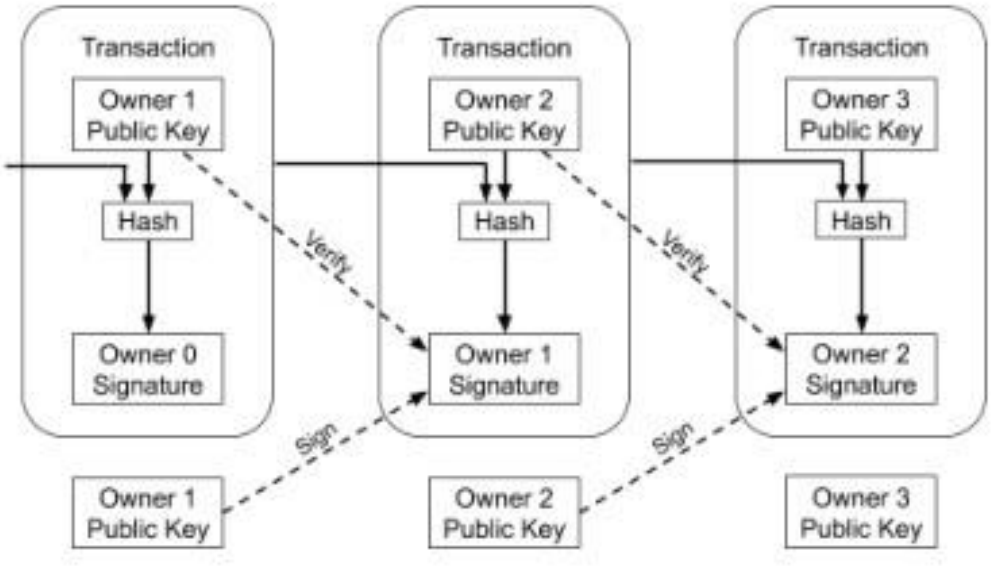


Figura 22 firma digitale

Merkle trees

Un albero di Merkle è una struttura di dati che supporta la Blockchain nel processo di autenticazione della transazione. È uno dei componenti principali di un blocco e può essere binario o MPT (Merkle-Patricia Trie).

Il Patricia Trie è una struttura di dati usa una chiave come percorso in modo che anche i nodi che condividono lo stesso prefisso possano condividere lo stesso percorso. Questa struttura è più veloce a trovare prefissi comuni, semplice da implementare, e richiede poca memoria.

Gli alberi di Merkle sono utilizzati con l'obiettivo di autenticare numerose chiavi pubbliche all'interno di un unico valore. Gli alberi di Merkle facilitano la convalida di diversi dati aggiunti in una Blockchain, consentendo così di mantenere la prova di eventi che sono accaduti in passato. La figura 23 è una rappresentazione grafica di un albero binario di Merkle.

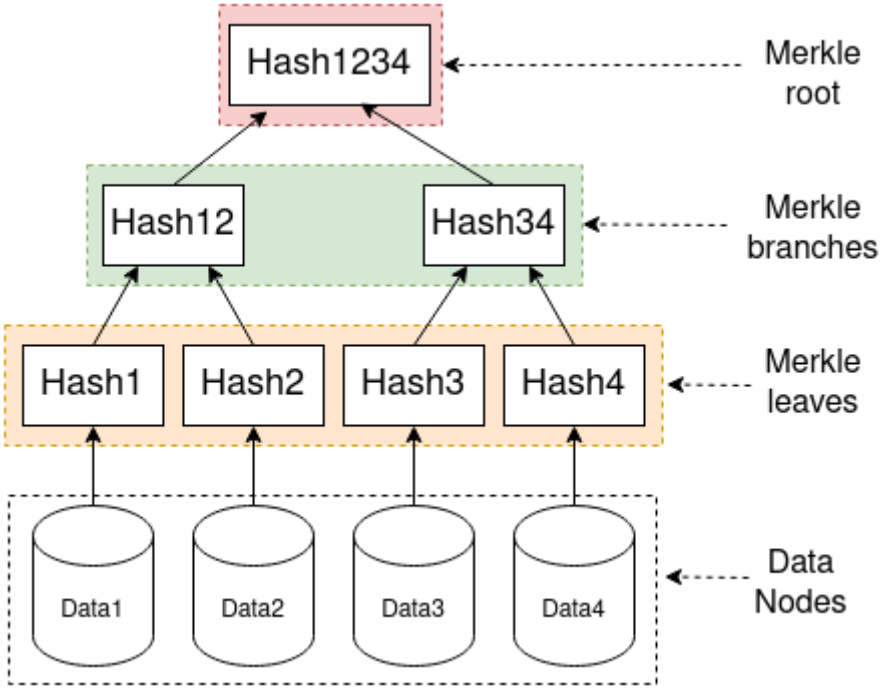


Figura 23 Merkle trees

La Merkle root è un elemento fondamentale per il processo di validazione della transazione. Si trova nella parte più alta della gerarchia in un albero di Merkle e contiene il risultato dell'hashing di tutti i dati transazionali in un blocco consecutivo. Questa particolare struttura di dati offre il vantaggio di certificare i dati attraverso l'intera catena senza dover scaricare l'intero libro mastro. I cambiamenti in una singola transazione a valle riflettono i cambiamenti nella parte più alta dell'albero di Merkle, consentendo la trasparenza dei dati, la sicurezza e la coerenza attraverso la catena.

Timestamp

Un timestamp viene utilizzato per mantenere una marca temporale sui dati. Al fine di garantire la tracciabilità, un server di timestamp fornisce la prova che i dati esistevano in un determinato momento e possono essere verificati all'interno della Blockchain, come mostrato nella figura 24. Dato che l'ultimo blocco contiene un hash di tutti i timestamp precedenti, tale blocco ha una copia esatta delle prime fasi della blockchain.

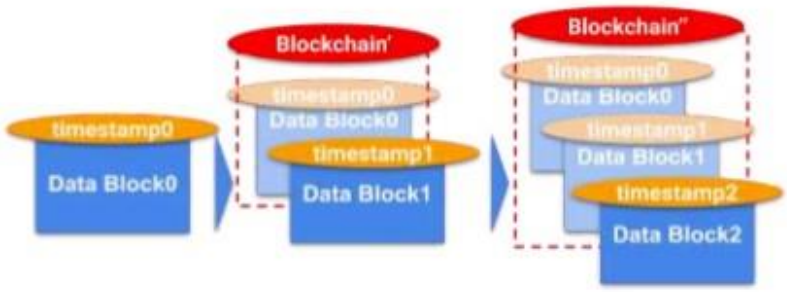


Figura 24 timestamping con la Blockchain

Hash – Hashing

È il processo di cifratura di qualsiasi testo per renderlo illeggibile. I dati inseriti vengono convertiti in un output a lunghezza fissa mediante operazioni matematiche.

L'hashing è anche un metodo per creare dati crittografici usando algoritmi. A questo proposito, gli hash crittografici sono come le firme digitali. Sia le funzioni di hash tradizionali che quelle crittografiche sono deterministiche. Finché l'input non viene modificato, l'hash associato non cambia.

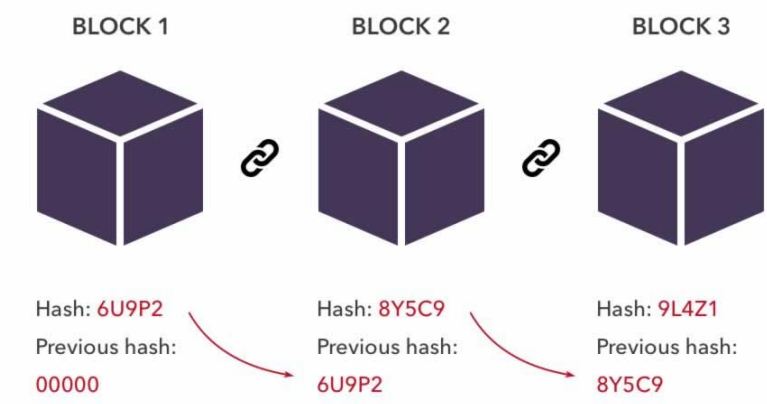


Figura 25 struttura hashing

Nodo

Un blocco trasmette a tutti i nodi della rete quando un miner cerca di aggiungere un nuovo blocco di transazioni alla blockchain. In base alla legittimità di un blocco, i nodi potrebbero accettarlo o rifiutarlo. Quando un nodo accetta un nuovo blocco di transazioni, lo salva e lo memorizza sopra i blocchi esistenti.

Qualsiasi computer o dispositivo di rete fisica collegato alla rete è considerato un nodo in quanto comunica tra loro

Smart Contracts

I contratti intelligenti sono semplicemente programmi memorizzati su una blockchain che vengono eseguiti quando sono soddisfatte alcune condizioni predeterminate. In genere vengono utilizzati per automatizzare l'esecuzione di un accordo in modo che tutti i partecipanti possano essere immediatamente certi del risultato, senza alcun coinvolgimento o perdita di tempo dell'intermediario. Possono anche automatizzare un flusso di lavoro, attivando l'azione successiva quando le condizioni sono soddisfatte.

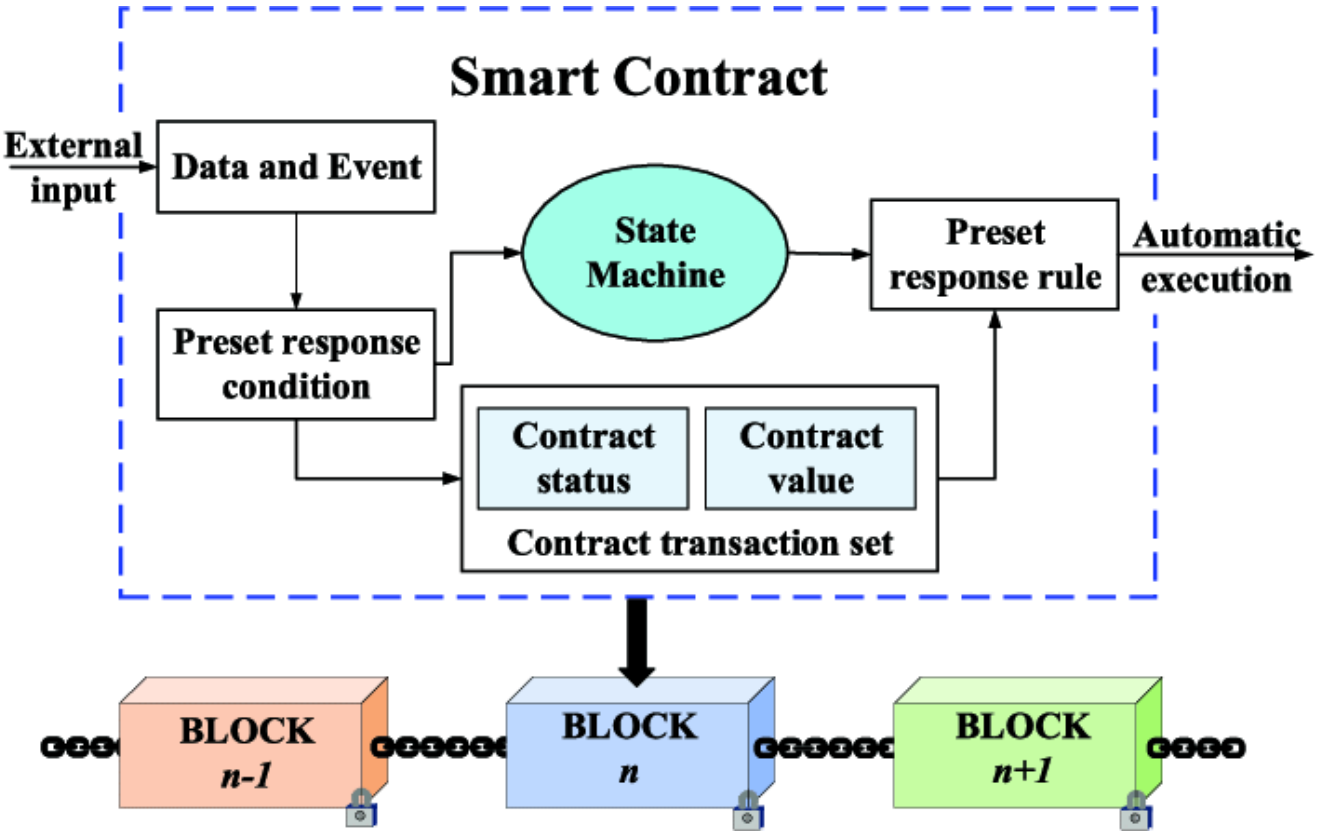


Figura 26 processo di uno smart contract

3.4 Protocollo di consenso

Il problema del raggiungimento di un consenso condiviso all'interno di una rete è un processo difficile da ottenere. Per comprendere meglio il problema bisogna utilizzare la teoria dei giochi analizzando uno dei problemi più iconici, che meglio esemplifica il raggiungimento di un consenso in una rete, chiamato il Fallimento Bitantino.

Nella sua forma più semplice, un certo numero di generali sta attaccando una fortezza e deve decidere come gruppo se attaccare o ritirarsi. Alcuni generali preferiscono attaccare, mentre altri preferiscono ritirarsi. L'importante è che tutti i generali concordino su una decisione comune, perché un attacco da parte di pochi generali diventerebbe una disfatta, e sarebbe peggio di un attacco coordinato o di una ritirata coordinata.

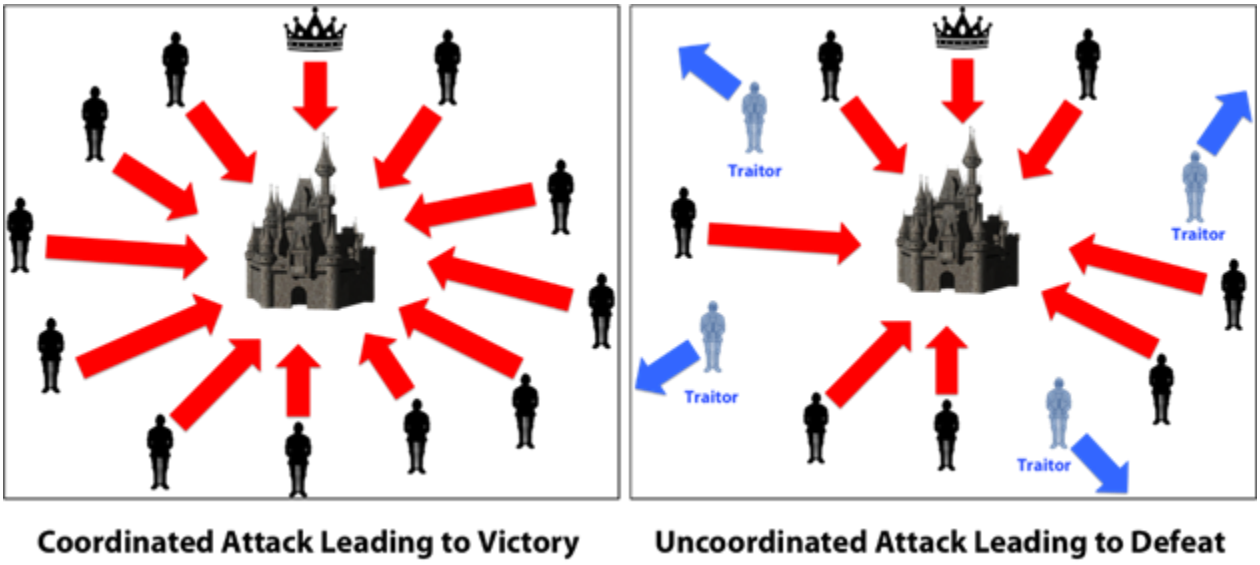


Figura 27 fallimento Bizantino

Il problema è complicato dalla presenza di generali insidiosi che non solo possono votare per una strategia non ottimale, ma possono farlo selettivamente. Ad esempio, se nove generali votano, quattro dei quali sostengono l'attacco mentre altri quattro sono a favore della ritirata, il nono generale può inviare un voto di ritirata a quei generali in favore della ritirata e un voto di attacco agli altri. Coloro che hanno ricevuto un voto di ritirata dal nono generale si ritireranno, mentre gli altri attaccheranno (il che potrebbe non andare bene per gli attaccanti). Il problema è ulteriormente complicato dal fatto che i generali sono fisicamente separati e devono inviare i loro voti tramite messaggeri che potrebbero non riuscire a dare i voti in tempo o potrebbero falsificarli.

La risoluzione può essere utilizzare la tolleranza bizantina, la quale può essere raggiunta se i generali leali hanno un accordo di maggioranza sulla loro strategia. Oppure, ci può essere un valore di voto predefinito dato ai messaggi mancanti. Per esempio, ai messaggi mancanti può essere dato un valore nullo o negativo. Inoltre, se l'accordo prevede che i voti nulli siano maggioritari, può essere utilizzata una strategia di default preassegnata (ad es. ritirata).

La mappatura tipica di questa storia sui sistemi informatici è che i computer sono i generali e i loro collegamenti al sistema di comunicazione digitale sono i messaggeri. Sebbene il problema sia formulato nell'analogia come un problema decisionale e di sicurezza, nell'elettronica, non può essere risolto semplicemente con firme digitali crittografiche, perché errori come tensioni errate possono propagarsi attraverso il processo di crittografia. Pertanto, un componente può apparire funzionante per un componente e difettoso per un altro, il che impedisce la formazione di un consenso condiviso sul fatto che il componente è difettoso o meno.

Tornando al caso specifico della Blockchain il consenso è un accordo tra nodi in una rete e viene raggiunto tramite specifici protocolli di consenso.

Un protocollo di consenso è una logica che definisce le modalità di raggiungimento di un accordo, specificando i criteri e le regole che i partecipanti alla rete devono seguire per raggiungere il consenso.

Ci sono diversi modi con i quali una rete accetta l'aggiunta di un nuovo blocco alla catena, gli esempi più utilizzati sono: Proof-of-Work e Proof-of-Stake.

Proof-of-Work (PoW)

Gli utenti devono dimostrare alla rete che è stato speso una certa potenza di calcolo per verificare la validità delle transazioni in una Blockchain in quanto si richiede di risolvere un problema matematico.

In una Blockchain che utilizza il consenso tramite POW, ci sono due tipi di utenti: Miner e Firmatari.

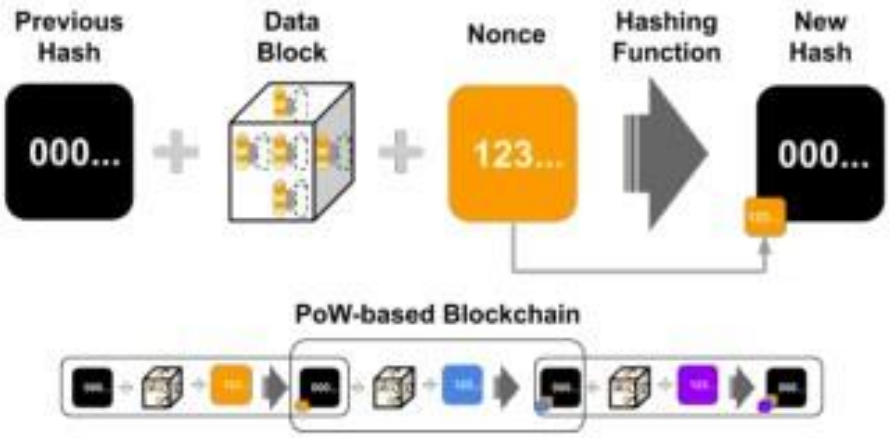


Figura 28 Proof of Work

Gli utenti di Miner verificano che le transazioni effettuate dai firmatari siano valide e, per farlo, sono tenuti a recuperare tutte le transazioni effettuate nell'intera Blockchain. Lo fanno ottenendo un hash del blocco precedente più un nonce, e tale hash deve iniziare con una certa quantità di bit al fine di essere convalidato e accettato all'interno della catena. Questo processo è mostrato nella Figura 28.

D'altra parte, i firmatari sono gli utenti che attivano le transazioni nella rete (ad esempio, effettuando un pagamento). I minatori sono incentivati a convalidare i dati perché ogni volta che risolvono il problema matematico, viene fornita una ricompensa sotto forma di token o criptovaluta. Il minatore che risolve il puzzle prima arriva ad aggiungere l'ultimo blocco alla catena. Questo minatore è chiamato leader ed è molto probabile che sia un nodo con elevata potenza di calcolo.

Questo sistema richiede una considerevole potenza di calcolo, consumando ingenti quantità di energia elettrica creando un impatto ambientale rilevante.
Oltre ciò il processo di convalidazione risulta particolarmente lungo in quanto il gioco matematico è strutturato per essere sempre più difficile ad ogni iterazione in modo da non favorire un Miner specifico.

Queste motivazioni hanno spinto i ricercatori a creare dei sistemi di consenso differenti in modo da ridurre l'impatto ambientale e il tempo di convalida.

Proof-of-Stake (PoS)

Tramite questo processo la probabilità di aggiungere un blocco alla catena dipende dal numero di attività che un partecipante possiede nella rete e dal tempo in cui lo possiede. È stato sviluppato come alternativa a basso consumo energetico al POW.

Come mostrato in figura 29, In questo processo un blocco di dati viene aggiunto alla catena tenendo conto di un hash ottenuto da un set di dati compresa l'età della moneta, che include il numero di monete che l'utente possiede al momento della transazione e da quanto tempo li possiede.

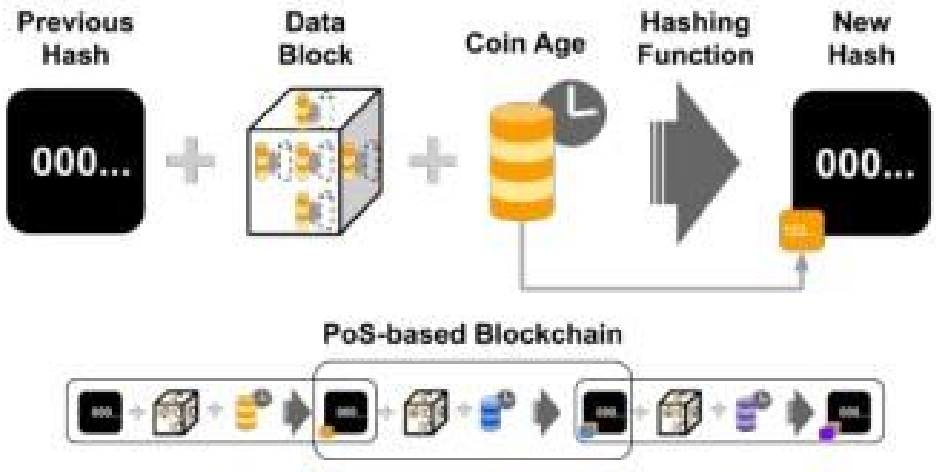


Figura 29 Proof Of Stake

Per riassumere, un protocollo POS è un'iterazione trial-and-error in cui l'utente tenta di ottenere un nuovo hash con una marca temporale diverso. Più risorse ha un utente, più è probabile che trovi un valore hash superiore al valore target della rete (ad esempio, per aggiungere un blocco alla catena) permettendogli di aggiungere il nodo. Come in POW, il leader in POS viene ricompensato con un token o criptovaluta.

3.5 vantaggi della Blockchain

La Blockchain offre il potenziale per contribuire a diversi settori della società. Finora, è stato spiegato che cos'è la Blockchain e le sue molte componenti tecniche.

Ora ci si può soffermare sul contributo al benessere sociale e sulle motivazioni che spingono le persone e le aziende ad utilizzare questa tecnologia:

- Decentralizzazione: nessuna autenticazione di terze parti viene sfruttata dalle reti P2P. in questo modo è possibile ridurre i costi di transazione e il tempo di esecuzione.

- Persistenza: gli utenti della rete convalidano ed elaborano costantemente le transazioni, rendendo difficile per utenti male intenzionati di manomettere il sistema.

- Anonimato: ogni transazione è crittografata in modo che le identità del mittente e del destinatario possano essere recuperate solo dalle parti coinvolte nello scambio.

- Verificabilità: le transazioni temporizzate consentono a ciascun partecipante di tenere traccia e avere visibilità della cronologia di tutte le transazioni che sono avvenute dalla creazione della rete.

- Abbinabilità: questa tecnologia può essere abbinata ad altre, come l'Internet of Things e l'intelligenza artificiale, permettendo di massimizzare i vantaggi di ognuna di esse.

3.6 Sfide della Blockchain

Ora, dopo aver descritto alcuni dei vantaggi apportati da blockchain, è imperativo evidenziare anche alcuni dei suoi ostacoli. Ogni tecnologia ha i suoi pro e contro, e questa non sfugge a questa realtà. È vero, però, che i suoi potenziali vantaggi superano le sfide che può porre quando la si implementa in vari scenari. In particolare, le maggiori difficoltà nell'adozione di Blockchain derivano dalle normative legali, dalla gestione del cambiamento, dalla scalabilità, dalla sicurezza e dallo spreco di risorse.

- Le iniziative di regolamentazione legale da parte del governo possono portare la tecnologia verso un quadro più conforme, ma questi richiederebbero importanti investimenti da parte delle imprese esistenti. Tali investimenti potrebbero essere indirizzati in gran parte a questioni di sicurezza e di autenticazione dell'identità. In definitiva, la blockchain ha ancora alcuni difetti di sicurezza come l'anonimato degli utenti e la difesa da attacchi informatici, il che rappresenta un problema per le reti di piccole dimensioni;

- È necessaria una gestione del cambiamento significativa per le aziende e gli utenti che alla fine si sposteranno dal tradizionale paradigma di terze parti a una struttura privata decentralizzata. Tale cambiamento comporta incorrere in costi di migrazione per trasferire i dati offline e online ai nuovi modelli di Blockchain. L'ipotesi è che i vantaggi sociali ed economici derivanti dall'adozione di questo sistema saranno superiori agli sforzi necessari per realizzarlo.

- Il ridimensionamento, d'altra parte, potrebbe rappresentare un ostacolo per l'archiviazione dei dati e la loro esecuzione. Per esempio, se i nuovi utenti volessero fare la loro prima transazione, dovrebbero prima scaricare e convalidare l'intero registro di rete per effettuare finalmente la transazione, spendendo grandi quantità di tempo e di energia.

- La sicurezza sulla blockchain è ancora una discussione in corso in quanto la regolamentazione è in una fase iniziale di sviluppo e nessun standard di settore ha ancora definito chiaramente i principali rischi posti dall'utilizzo della Blockchain.

- Il consumo di energia elettrica, specialmente nel caso di protocollo di consenso POW, è elevato e da molti considerato sprecato. Si stima che l'estrazione (ovvero l'ottenimento di una valuta digitale completando il processo di validazione di un blocco) di Bitcoin consumi circa 20 gigawatt-h di elettricità ogni anno. Ovviamente rappresenta un problema importante nel panorama odierno, nel quale l'innovazione è fortemente trainata dalla sostenibilità ambientale.

Tuttavia, gli standard per la tecnologia Blockchain sono in fase di sviluppo. Gli enti normatori stanno prendendo le disposizioni necessarie per elaborare standard di settore adeguati dal momento che le informazioni disponibili sono altamente tecniche ed eterogenee. La creazione di linee guida per l'utilizzo e l'implementazione della Blockchain faciliterà il lavoro permettendo di migliorare alcuni dei suoi difetti.

3.7 Algorand

All’interno del progetto si è deciso di utilizzare la Blockchain per garantire la sicurezza dei dati trattati nel modulo di Intelligenza Artificiale. In particolare, si vogliono proteggere i dati relativi agli assesment e ai report, che contengono considerevoli informazioni sensibili dell’organizzazione che li compila.

Tuttavia, essendo il progetto fortemente improntato sulla sostenibilità ambientale, si è reso necessario trovare una Blockchain che fosse a basso impatto. La risposta a questo problema arriva dall’azienda Algorand.

Algorand, Inc. è una società tecnologica fondata dal pioniere della crittografia, vincitore del premio Turing e professore del MIT, Silvio Micali. Ha progettato la piattaforma Algorand con un team riconosciuto a livello internazionale di ricercatori, matematici, crittografi ed economisti, dai primi principi, per garantire un vero decentramento, scalabilità e sicurezza.

Algorand ed è composta da una società e una fondazione. Algorand Foundation gestisce la crescita dell'ecosistema, il finanziamento dei premi, le ricerche in ambito di crittografia, la governance on-chain e il decentramento della rete Algorand, compresi i nodi. Lo sviluppo principale del protocollo Algorand è supervisionato da Algorand Inc., una società privata con sede a Boston.

Il protocollo di consenso utilizzato in questa applicazione mira ad essere sostenibile e scalabile. La piattaforma Algorand supporta i Smart Contract, e il suo algoritmo di consenso si basa su una Proof of Stake e un protocollo di accordo Bizantino. La criptovaluta nativa di Algorand si chiama ALGO.

Figura 30 logo Algorand

3.7.1 Struttura del sistema

L’algoritmo di consenso basato sulla Proof-Of-Stake e un accordo Bizantino decentralizzato permette di abbassare notevolmente il consumo di energia elettrica.

Ovvero, finché la maggioranza della posta in gioco è in mani non maligne, il protocollo può tollerare utenti malintenzionati, raggiungendo il consenso senza un'autorità centrale.

Prima di entrare nel dettaglio del protocollo, discutiamo i due concetti funzionali che Algorand utilizza.

3.7.2 Verifiable Random Function

Il VRF prende una chiave segreta e un valore e produce un output pseudocasuale, con una prova che chiunque può usare per verificare il risultato.

Il VRF funziona come una lotteria ed è usato per scegliere i leader per proporre un blocco e i membri del comitato per votare su un blocco. Questo output, quando eseguito da un account, viene utilizzato per campionare una distribuzione binomiale per generare una chiamata per ogni Algo in un account.

Più Algo sono posseduti da un account, maggiore è la possibilità che sia selezionato, è come se ogni Algo in un account partecipasse alla propria lotteria. Questo metodo assicura che un utente non ottiene alcun vantaggio creando più account.

3.7.3 Chiavi di partecipazione

Un account deve essere online per partecipare al protocollo di consenso. Per ridurre l'esposizione, gli utenti online non usano le loro chiavi (ad esempio, le chiavi che usano per firmare le transazioni) per il consenso.

Un utente genera e registra una chiave di partecipazione per un certo numero di round. Genera anche una raccolta di chiavi effimere (ovvero una chiave temporanea che può essere utilizzata una sola volata), una per ogni turno, firma queste chiavi con la chiave di partecipazione e quindi la cancella dopo il suo utilizzo.

Ogni chiave effimera viene utilizzata per firmare i messaggi per il round corrispondente e viene cancellata dopo la fine del round. L'utilizzo delle chiavi di partecipazione assicura che i token di un utente siano sicuri anche se il nodo partecipante è compromesso.

L'eliminazione della partecipazione e delle chiavi effimere dopo il loro utilizzo assicura che la Blockchain sia “forward-secure” (ovvero si garantisce la sicurezza delle transazioni future) e non possa essere compromessa da attacchi su vecchi blocchi utilizzando vecchie chiavi.

3.7.4 Protocollo di consenso di Algorand

Il consenso si riferisce al modo in cui i blocchi vengono selezionati e scritti nella Blockchain. Algorand usa il VRF descritto sopra per selezionare i leader per proporre i blocchi per un dato round.

Quando un blocco viene proposto alla Blockchain, un comitato di elettori viene selezionato per votare sulla proposta di blocco. Se la maggioranza di voti proviene dai partecipanti onesti, il blocco può essere certificato.

Ciò che rende questo algoritmo una Proof of Stake è che gli utenti sono scelti per i comitati in base al numero di Algo nei loro conti. I comitati sono costituiti da conti selezionati in modo pseudo-casuale con potere di voto dipendente dal numero di Algo posseduti. È come se ogni token ottenesse un'esecuzione del VRF, quindi ottenesse una chiave effimera per ogni token; pertanto, gli utenti con più token saranno probabilmente selezionati più spesso.

Per un membro del comitato questo significa che i conti più ricchi molto probabilmente avranno più voti di un account selezionato con meno token. L'utilizzo di comitati selezionati casualmente consente al protocollo di avere ancora buone prestazioni consentendo a chiunque nella rete di partecipare.

Il consenso richiede tre passaggi per proporre, confermare e scrivere il blocco alla blockchain. Questi passaggi sono:

1. Block Proposal;

2. Voto morbido;

3. Certificazione del voto;

Ognuno è descritto di seguito, assumendo il caso ideale quando non ci sono utenti malintenzionati e la rete non è partizionata (cioè, nessuno della rete è offline a causa di problemi tecnici o da attacchi). Si noti che tutti i messaggi sono firmati crittograficamente con la chiave di partecipazione dell'utente e l'appartenenza al comitato viene verificata utilizzando il VRF in questi passaggi.

3.7.5 Block Proposal

Nella fase di proposta di blocco, gli account vengono selezionati per proporre nuovi blocchi alla rete. Questa fase inizia con ogni nodo della rete che scansiona tutti gli account online e seleziona quelli con le chiavi di partecipazione valide, eseguendo il VRF di Algorand per determinare se l'account è selezionato per proporre il blocco.

Il VRF agisce come una lotteria ponderata in cui il numero di Algo che l'account possiede determinano la possibilità dell'account di essere selezionato. Una volta che un account viene selezionato dal VRF, il nodo propaga il blocco proposto insieme all'output VRF, il che dimostra che l'account è un propositore valido. Passiamo poi dalla proposta al voto morbido.

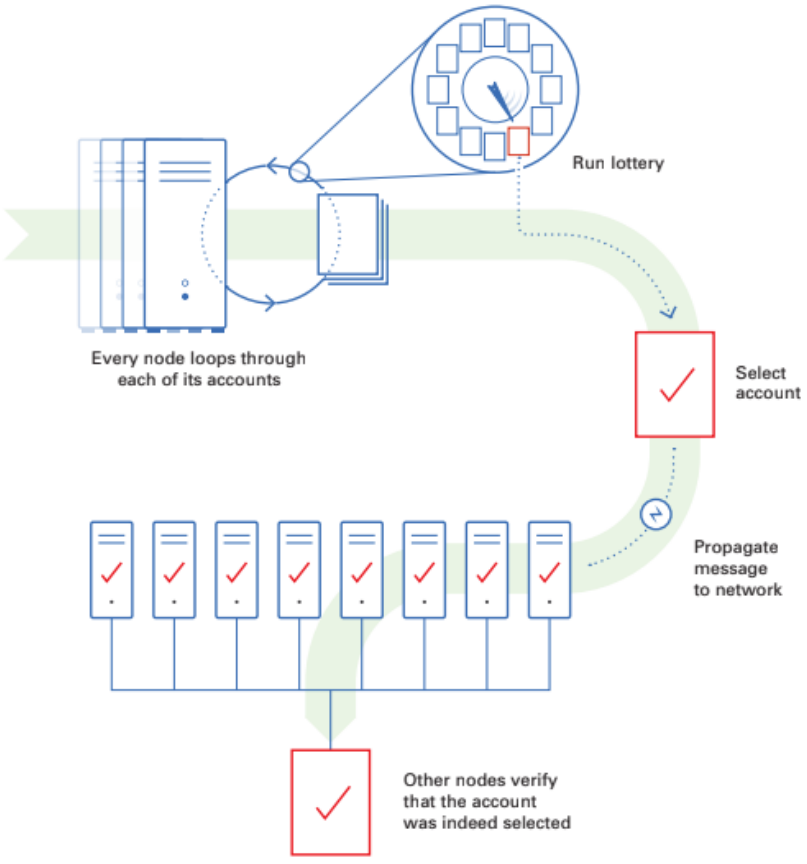


Figura 31 Block proposal

3.7.6 Voto morbido

Lo scopo di questa fase è quello di filtrare il numero di proposte fino ad una, garantendo che solo un blocco venga certificato. Ogni nodo nella rete riceverà molti messaggi di proposta da altri nodi, i quali verificheranno la firma del messaggio e quindi convalideranno la selezione utilizzando la prova VRF.

Successivamente, il nodo confronterà l'hash di ogni prova VRF del vincitore per determinare quale di questi ha il l'hash più basso in modo da poterlo propagare attraverso la rete. Questo processo continua per un determinato periodo di tempo per consentire la propagazione dei voti attraverso la rete.

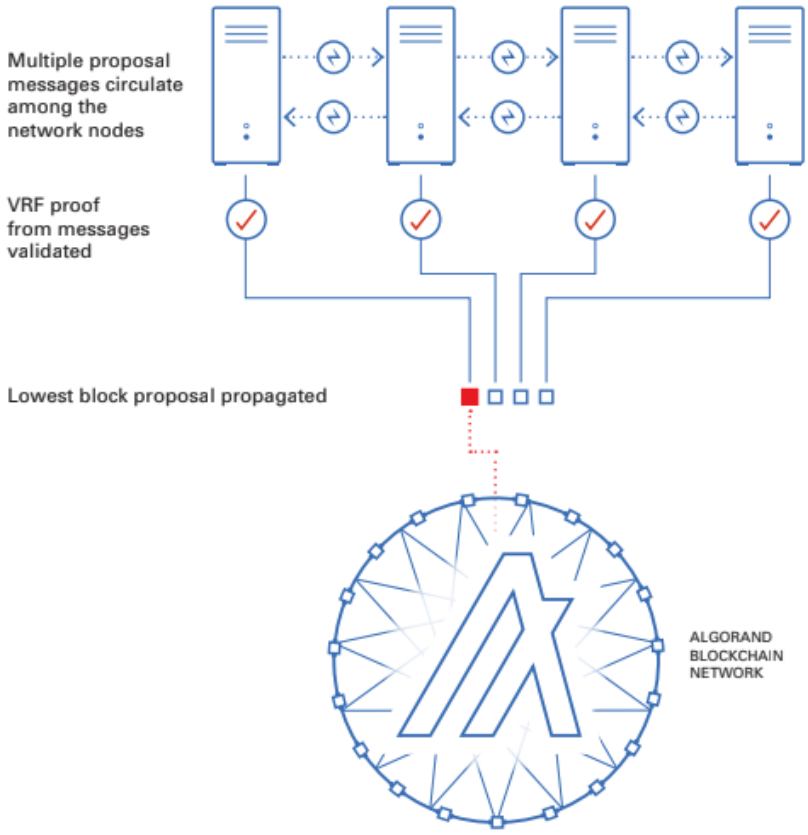


Figura 32 voto morbido parte 1

Ogni nodo, quindi, eseguirà il VRF per ogni account che riesce a vedere se sono stati scelti per partecipare al comitato di voto morbido. Se un account viene scelto avrà un voto ponderato in base al numero di Algo che l'account possiede, i quali verranno propagati attraverso la rete.

Questi voti saranno attribuiti per la proposta di blocco con un hash VRF più basso calcolata al time-out e saranno inviati agli altri nodi insieme alla prova VRF.

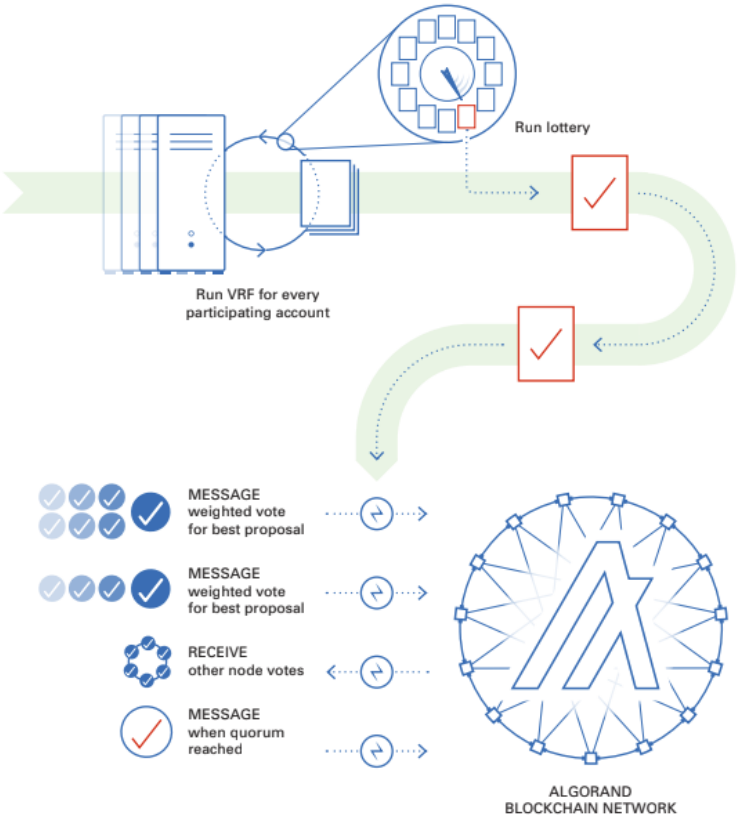


Figura 33 voto morbido parte 2

Viene selezionato un nuovo comitato per ogni fase del processo e ogni fase ha una dimensione del comitato diversa. Questa dimensione del comitato è quantificata in Algo.

Per passare alla fase successiva è necessario raggiungere un quorum che viene definito come una percentuale della dimensione del comitato. Questi voti saranno ricevuti da altri nodi della rete e ogni nodo convaliderà la prova di appartenenza al comitato tramite il VRF prima di aggiungere il proprio voto. Una volta raggiunto il quorum per il voto soft il processo si sposta alla fase di certificazione del voto.

3.7.7 Certificazione del voto

Una nuova commissione controlla la proposta di blocco che è stata votata nella fase di voto morbido per valutare overspending, double-spending[16], o altri problemi. Se valido, il nuovo comitato vota nuovamente per certificare il blocco.

Questo viene fatto in modo simile al voto morbido in cui ogni nodo itera attraverso gli account ad esso collegati per selezionare un comitato e inviare voti. Questi voti vengono raccolti e convalidati da ciascun nodo fino al raggiungimento di un quorum, terminando il round e spingendo il nodo a creare un certificato per il blocco e scriverlo sul registro. A quel punto, viene avviato un nuovo ciclo e il processo ricomincia.

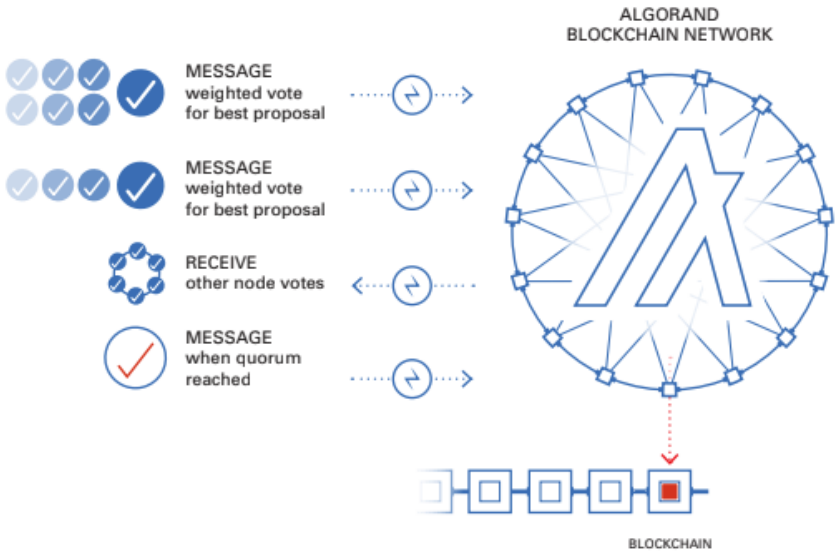


Figura 34 certificazione del voto

Se il quorum non viene raggiunto in una votazione del comitato di certificazione da un certo timeout, la rete ripartirà dal primo step.

[16] La doppia spesa è un potenziale difetto in uno schema di cassa digitale in cui lo stesso token digitale può essere speso più di una volta. A differenza dei contanti fisici, un token digitale consiste in un file digitale che può essere duplicato o falsificato. Come nel caso della moneta contraffatta, tale doppia spesa porta all'inflazione creando una nuova quantità di moneta copiata che non esisteva in precedenza. Questo svaluta la valuta rispetto ad altre unità monetarie o beni e diminuisce la fiducia degli utenti, nonché la circolazione e il mantenimento della valuta.

3.7.8 Caratteristiche dell'applicazione specifica

Fino ad ora sono state introdotte le caratteristiche principali che hanno portato alla scelta di questo specifica Blockchain. Adesso si passerà alla descrizione dello sviluppo di un sistema apposito per interfacciare i dati con la Blockchain.

Il requisito fondamentale è quello di proteggere i dati che vengono manipolati all'interno del modulo di Intelligenza artificiale. Nello specifico sono:

- I dati di input interni, ovvero gli assessment;
- I risultati output dell'analisi AI, quindi la valutazione di circolarità e il processo di miglioramento;

Al fine di ottenere un sistema efficiente si è deciso di creare un database centralizzato nel quale immagazzinare questi dati (N.B. nella figura 35 sono rappresentati 2 databese a scolpo illustrativo). Tramite la notarizzazione (che viene spiegata di seguito) è possibile consentire o vietare l'accesso alle informazioni contenute in questo database.

La notarizzazione di questi dati consiste in una transazione eseguita su Blockchain Algorand tramite la quale viene registrato l'hash dei file. Questa operazione ottiene due effetti:

- Si assegna una marca temporale al file (tramite l'hash che lo rappresenta in maniera univoca);
- Si conferisce paternità al file, ovvero se ne traccia la provenienza;

Marcando temporalmente e conoscendo la provenienza di un file è possibile:

- provare l'immutabilità dei dati di input;
- provare che i risultati in output appartengo a certi dati in input, che sono già stati notarizzati;
- provare a tutti i partecipanti che nessun dato è stato contraffatto;

3.7.8.1 Struttura e dinamica dei dati in input

Il diagramma rappresentato in figura 35 mostra le diverse parti del sistema e ne evidenzia le interazioni principali:

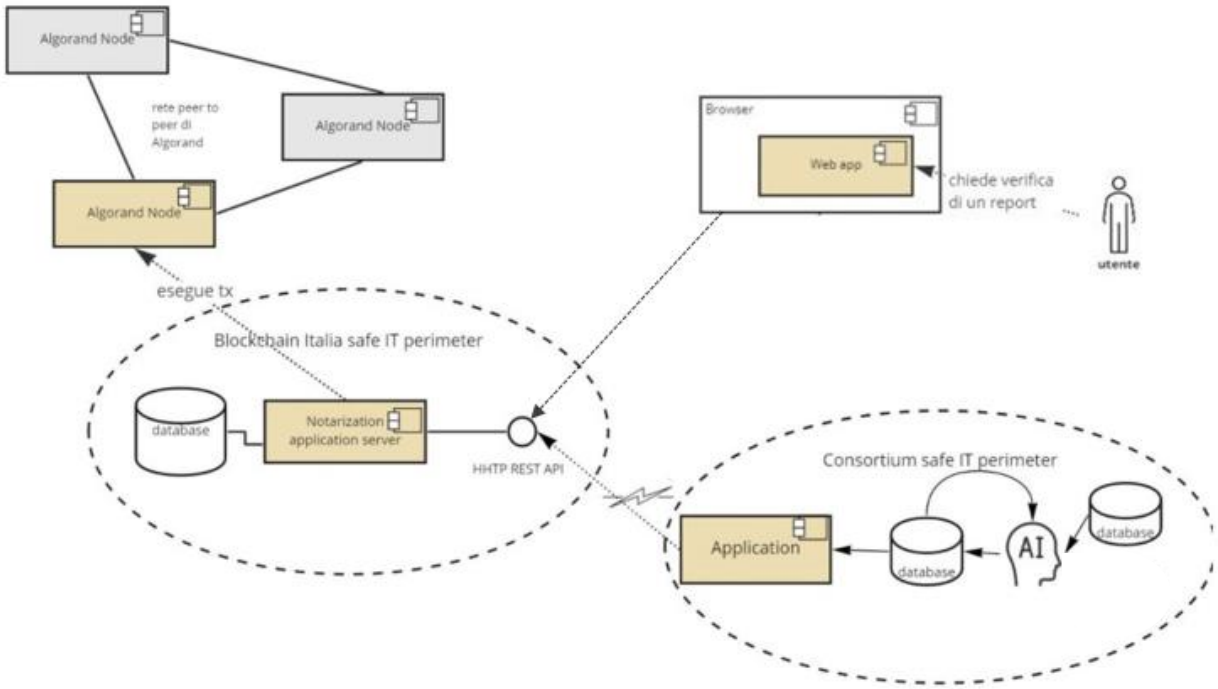


Figura 35 struttura dinamica dei dati in input

Il processo parte nel Consortium safe IT perimeter nel quale viene utilizzato il modulo di intelligenza artificiale, come spiegato nel relativo capitolo.

Alla fine di questo procedimento gli assesment e l'output del modulo di intelligenza artificiale entrano nel Blockchain Italia safe IT perimeter per essere caricati nella Blockchain di Algorand tramite il un REST[17] API con linguaggio HTTP.

[17] L'architettura REST si basa su HTTP. Il funzionamento prevede una struttura degli URL ben definita che identifica univocamente una risorsa o un insieme di risorse e l'utilizzo dei metodi HTTP specifici per il recupero di informazioni, per la modifica e per altri scopi.

L’API (Application Programming Interface) è un'interfaccia software che consente a due applicazioni di interagire tra loro senza alcun intervento da parte dell'utente e rappresenta una raccolta di funzioni e procedure del software. In termini semplici, l’API è un codice software a cui si può accedere o eseguire ed è definito come un codice che aiuta due diversi software per comunicare e scambiare dati tra loro senza dover sapere come vengono implementati.

I servizi API prevedono:

1) funzione di richiesta di notarizzazione hash e custodia

- Acquisire in ingresso contenuto da notarizzare e custodire;

- Restituire in output della richiesta usando codici di risposta http. Il buon esito indica la corretta messa in custodia dei dati;

il sistema provvede a generare un codice hash per il file che si desidera custodire in modo da poterlo recuperare in futuro.

2) funzione di recupero di una custodia

Questa funzione parte dell’acquisizione del hash del file e restituisce il contenuto originale del file.L’autenticazione avviene tramite API KEY che verrà fornita all’utente permettendogli di integrare con servizio di custodia con i suoi sistemi informativi.

Quando la transazione tra questi due perimetri viene accettata il blocco di informazioni viene caricato nella Blockchain seguendo il sistema mostrato nel capitolo Algorand.

Riassumendo, l’operazione per caricare i dati nella Blockchain si esegue in 4 step:

1. I dati vengono generati nello spazio protetto del consorzio;

2. La transazione porta la “firma” dell’account del consorzio che si è collegato e ha richiesto la notarizzazione; tale account deve possedere la password di sblocco delle chiavi crittografiche usate per la firma della transazione;

3. I dati vengono inviati al “Notarization Application Server” che la prende in carico e la esegue;

4. Caricamento dei dati nella Blockchain Algorand;

Esiste anche la possibilità per gli utenti di accedere al sistema per verificare se un loro documento è stato notarizzato e in quale momento.

L’utente si collega con un normale browser al “notarization Application Server” ad una URL precedentemente fornitogli. Il sistema si presenterà come una applicazione web (single page application). Una volta che si collega può verificare i documenti utilizzando la seguente procedura:

1. Estrae l’hash del documento;
2. Verifica nel database l’eventuale registrazione di quell’hash;
3. In caso positivo fornisce il link alla transazione su Algorand che l’ha registrata

le registrazioni su Blockchain sono indelebili ma il processo delineato, con memorizzazione e verifica delle registrazioni su database, consente di dare risposte articolate agli utenti. Ad es. si può prevedere un meccanismo per dire all’utente che sta facendo la verifica di un documento che però e stato sorpassato da nuova versione.

3.7.8.2 Sicurezza

Le chiavi crittografiche collegate all’account del consorzio che servono a firmare le transazioni sono gestite in modo da garantire che nessun altro soggetto possa usarle, neanche il Provider del servizio.

In particolare, tali chiavi:

- Sono generate al primo collegamento dell’utente sul suo dispositivo dentro il perimetro IT sicuro della piattaforma;
- Vengono cifrate tramite una password immessa dall’operatore e sono inviate al server per la loro custodia su cloud;
- Ad ogni firma l’operatore sbloccherà le chiavi tramite password ed esse verranno usate per firmare la transazione sempre dentro il perimetro IT della piattaforma;

Per semplicità la password di cifratura/decifratura delle chiavi crittografiche potrà coincidere con quella dell’account utente. Tale password non viene mandata in chiaro al server ma viene solo mandata una sua trasformazione non invertibile (hash della chiave).

Un collegamento HTTPS consente la comunicazione sicura tra gli utenti e la piattaforma di notarizzazione benché essa non sia strettamente necessaria dal momento che:

- Le chiavi viaggiano cifrate;
- La firma dei documenti è una firma crittografica non manipolabile;

Conclusioni

Questo documento nasce dall'esigenza sociale di ottenere un'economia che tenga conto delle tematiche ambientali, sostenendo e incoraggiando la creazione di business green e sostenibili. Ma questo cambiamento non può avvenire senza la giusta guida, a questo scopo ci si è posto l'obbiettivo di creare uno strumento che potesse indirizzare le PMI attraverso questo cambiamento.

I temi cardine della prima parte sono appunto legati a questo tema e si chiamano Twin Transition ed Economia Circolare, che, come si è visto, sono due concetti strettamente correlati tra loro. l'Economia Circolare è un modello nel quale si mira al riutilizzo degli scarti come materia prima creando un ciclo chiuso; la Twin Transition invece è l'applicazione del precedente concetto supportato da un uso estensivo delle tecnologie.

In seguito sono state analizzate quelle che sono le principali motivazioni che spingono gli imprenditori e le aziende ad applicare questo modello (nello studio citato si riscontra che il senso di responsabilità è in cima a tutti gli altri), i maggiori problemi riscontrati (dove troviamo la legislazione non chiara o insufficiente e la necessità di investimenti ingenti) ed in ultimo i benefici riscontrati (che sono un aumento di reputazione dell'azienda e una motivazione maggiore nelle persone che ci lavorano).

Sempre nella prima sono state mostrate le principali tecnologie utilizzate in tema di Twin Transition attraverso gli esempi di alcuni progetti già esistenti che si sono cimentati su questi temi. Questa fase all'interno del progetto si è rivelata estremamente utile per effettuare benchmarking e stringere relazioni e sinergie per svilupparlo.

Dall'attività precedente si sono scelte due tecnologie: L'Intelligenza Artificiale e la Blockchain.

La prima rappresenta la mente che guida le PMI nella decisione di quali attività intraprendere per migliorare la loro circolarità evidenziando le criticità maggiori proponendo soluzioni ad hoc. Questo strumento permetterà alle organizzazioni di prendere decisioni in modo più semplice investendo in modo mirato i loro capitali.
il raggiungimento di questo obbiettivo è permesso dall'utilizzo di un modulo di AI ristretto basato sulla Artificiale Neuronal Network istruita tramite il semi-supervisioned learning.
in questa prima fase si è deciso di specializzarsi sulle PMI in ambito Manufacturing ma si prevede che tramite sviluppi futuri ci si potrà rivolgere anche in altri settori.

La seconda invece permette di proteggere le informazioni utilizzate dal modulo di AI. Lo sviluppo predominante di questa tecnologia è stato verso la sostenibilità di questo sistema. In particolare, si è deciso di utilizzare una Blockchain pubblica sviluppata da Algorand che utilizza la Proof of Stake permettendo al sistema di avere un impatto ambientale estremamente ridotto.

Come risulta chiaro, la chiave per entrare nella transizione verso la sostenibilità è ovviamente l'implementazione di nuove tecnologie, ma ancora più importante, è rendere l'individuo il cuore dell'intero processo, insieme alla sensibilizzazione dei consumatori, applicando innovativi modelli di business. In questo modo le PMI potranno tornare competitive all'interno di un mercato che cambia e si rinnova in tempi considerevolmente ristretti, facendosi promotori della Twin Transition.

Bibliografia

https://ec.europa.eu/environment/ecoap/about-eco-innovation/policies-matters/green-and-digital-twin-transition-also-spurs-inclusive-eco_en

https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Waste_statistics

European Commission, Directorate-General for Environment, White, O., Garnett, K., Zamparutti, T. (2021). The EU Environmental Foresight System (FORENV) : final report of 2019-20 annual cycle : emerging - economic, business, technological and social - innovations in the green economy of the future, Publications Office.

https://pulse.microsoft.com/uploads/prod/2018/10/WE_AI_Report_2018.pdf

Futures, O. F. C. (2019). Blockchain Technologies as a Digital Enabler for Sustainable Infrastructure. Financing Climate Futures: Rethinking Infrastructure Initiative; OECD: Geneva, Switzerland.

Brendzel-Skowera, K. (2021). Circular Economy Business Models in the SME Sector. Sustainability, 13(13), 7059.

Di Maria, E., De Marchi, V., Blasi, S., Mancini, M., & Zampetti–Legambiente, G. (2018). L'economia circolare nelle imprese italiane e il contributo di industria 4.0. Università degli Studi di Padova, Dipartimento di Scienze Economiche e Aziendali "Marco Fanno", Laboratorio Manifattura Digitale e Legambiente.

Lewandowski, M. (2016). Designing the business models for circular economy—Towards the conceptual framework. Sustainability, 8(1), 43.

https://ellenmacarthurfoundation.org/growth-within-a-circular-economy-vision-for-a-competitive-europe

Langley, P. (2011). The changing science of machine learning. Machine learning, 82(3), 275-279.

Alpaydin, E. (2020). Introduction to machine learning. MIT press.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

Hunt, E. B. (2014). *Artificial intelligence*. Academic Press.

Boden, M. A. (Ed.). (1996). *Artificial intelligence*. Elsevier.

Indice immagini