



UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

TESI DI LAUREA

Le blockchain ed il loro impatto sugli algoritmi di intelligenza artificiale

RELATORE

Prof. Fabio Palomba

Università degli Studi di Salerno

CANDIDATO

Francesco Paciello

Matricola: 0512109085

Anno Accademico 2021-2022

A mia mamma e alla mia famiglia

Sommario

Blockchain è una tecnologia che sta diventando sempre più diffusa, dati i suoi innumerevoli vantaggi. Tra questi, il più rilevante è sicuramente l'elemento di decentralizzazione, che ha portato Blockchain ad essere una delle tecnologie più in voga degli ultimi anni, soprattutto in ambito finanziario.

Anche l'Intelligenza Artificiale sta facendo passi da gigante negli ultimi anni, andando a ricoprire quasi tutti i campi della nostra vita.

Tuttavia ci sono molti vantaggi che riguardano l'impiego dell'Intelligenza Artificiale a favore della Blockchain e viceversa. Vari studi dimostrano come l'Intelligenza artificiale possa portare dei vantaggi se applicata alla Blockchain, e la stessa cosa si può dire per l'applicazione della Blockchain all'Intelligenza Artificiale.

In questa tesi viene quindi formalizzato il concetto di Blockchain, andando a studiare come funziona e come è strutturata. Inoltre vengono riportati vari studi che mostrano i vantaggi che Blockchain e AI si trasmettono, e i campi di applicazione attuali.

Dall'analisi condotta, si è potuto osservare che i vantaggi principali che l'Intelligenza artificiale può offrire alla Blockchain sono: l'applicazione dell' "intelligenza" agli smart contracts, le transazioni più rapide ed una maggiore efficienza della rete.

D'altra parte, i vantaggi che sono risultati dall'applicazione di Blockchain sull'Intelligenza Artificiale sono: maggiore sicurezza sui dati, la presenza di community ed una maggiore scalabilità'.

Inoltre, si è visto che i campi di applicazione principali che vedono coinvolti Blockchain e AI insieme, sono: Deep Learning, Internet of Things ed e-Health.

Indice	ii
Elenco delle figure	iv
Elenco delle tabelle	v
1 Introduzione	1
1.1 Contesto applicativo	1
1.2 Motivazioni e Obiettivi	2
1.3 Risultati	2
1.4 Struttura della tesi	3
2 Background	4
2.1 Blockchain	4
2.1.1 Perché nasce Blockchain	4
2.1.2 Definizione	5
2.2 Smart contracts	5
2.3 Transazioni e consenso	6
2.4 Proof of Work e Proof of Stake	7
2.5 Decentralized Applications	8
2.6 Machine Learning	9
3 Metodologia utilizzata	11
3.1 Obiettivi dell'analisi	11

3.2	Formulazione search query	12
3.3	Raccolta e selezione degli articoli	12
3.4	Definizione dei criteri di esclusione/inclusione	13
4	Risultati	14
4.1	Stato dell'arte	14
4.1.1	Integrazione di Blockchain e AI e futuri casi d'uso	14
4.1.2	Blockchain e AI nell'IoT	17
4.1.3	Blockchain e AI nell'e-Health	18
4.1.4	Vantaggi dell'applicazione di AI su Blockchain	18
4.1.5	Vantaggi dell'applicazione di Blockchain su AI	19
4.1.6	Campi applicativi per AI e Blockchain	19
5	Conclusioni	21
5.1	Lavoro svolto	21
5.2	Sviluppi futuri	21
	Ringraziamenti	23

Elenco delle figure

2.1	Rappresentazione grafica di una Blockchain. Fonte: https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036?gi=9af01879e494	5
-----	--	---

Elenco delle tabelle

1.1 Contesto applicativo

Oggigiorno produciamo quantità di dati enormi, che partono dai nostri smartphones, computer e altri dispositivi, e che arrivano in dei server dislocati nel mondo.

La centralizzazione è sempre stata la soluzione più utilizzata per conservare e gestire i dati che viaggiano sulle reti.

Con la nascita di Bitcoin, ha preso piede il concetto di Blockchain, ovvero un libro mastro decentralizzato, autogestito, e distribuito, capace di risolvere tutti i problemi di un sistema centralizzato, garantendo sicurezza, affidabilità, e tanti altri vantaggi. [1].

Attualmente Blockchain sta prendendo piede in molti ambiti, nonostante fino a qualche anno fa, veniva considerata ancora una tecnologia "acerba", difatti è esplosa soltanto nel 2008 con il paper pubblicato da Satoshi Nakamoto [1].

L'ambito finanziario è sicuramente quello dove Blockchain sta dando il suo maggior contributo, grazie alla nascita di varie criptovalute. Tra le più famose troviamo Bitcoin ed Ether.

Recentemente si sta sperimentando come l'intelligenza artificiale possa dare una mano alla Blockchain, andando a colmare vari punti deboli che essa espone, e dando vita a nuove tecnologie che sfruttino entrambe.

I principali vantaggi che l'intelligenza artificiale può andare ad offrire alla Blockchain sono i seguenti:

- **Intelligenza agli smart contracts**
- **Maggiore efficienza**
- **Transazioni più rapide**

Ma non solo, anche la Blockchain può andare ad offrire vari vantaggi ad un'intelligenza artificiale, tra i quali:

- **Sicurezza dei dati**
- **Scalabilità**
- **Presenza di community**

1.2 Motivazioni e Obiettivi

Questo lavoro di ricerca si prefigge 3 scopi principali:

- analizzare la tecnologia Blockchain e le sue attuali implementazioni;
- analizzare le attuali implementazioni che vedono coinvolte Blockchain e AI
- scoprire in che modo la Blockchain e l'intelligenza artificiale possono convergere, al fine di creare nuove tecnologie future

1.3 Risultati

I risultati di questa ricerca hanno dimostrato che le tecnologie di Intelligenza Artificiale e Blockchain possono convergere in vari modi, andando a migliorare molti campi esistenti già da anni.

In particolare si è visto come Blockchain e AI, combinate insieme, stiano riscontrando maggior successo nei seguenti campi:

- **Deep learning**, si può dare vita ad agenti di IA in grado di decodificare gli schemi delle onde cerebrali umane, un'entità di questo tipo potrebbe interagire direttamente con il cervello umano, utilizzarlo come serie di dati per acquisire informazioni sul suo funzionamento e, inoltre, fornire una conoscenza approfondita in molti campi della scienza, che prima era impossibile acquisire,

- **Internet of Things**, in questo ambito si è visto come Blockchain e AI possono convergere per dare vita alle cosiddette "smart cities", sfruttando la sicurezza di Blockchain per salvaguardare i vari sensori che compongono queste "città intelligenti", e utilizzando l'AI per fornire intelligenza,
- **e-Health**, si è visto come l'IA può migliorare la sicurezza delle attuali applicazioni sanitarie basate su Blockchain, andando ad utilizzare algoritmi di machine learning per rilevare la presenza di exploit sconosciuti.

1.4 Struttura della tesi

Le tematiche sopra menzionate sono state ampiamente discusse successivi capitoli. Di preciso, la tesi si compone di:

- **Capitolo 1: Introduzione**, tratta le motivazioni che hanno portato allo sviluppo di questa ricerca ed i vari obiettivi che si prefigge,
- **Capitolo 2: Background e Stato dell'arte**, spiega tutte le nozioni che sono alla base della ricerca, e illustra l'attuale stato dell'arte,
- **Capitolo 3: Approccio alla Ricerca**, illustra le varie metodologie utilizzate per effettuare la ricerca,
- **Capitolo 4: Risultati**, descrive quali risultati sono stati ottenuti dalla ricerca effettuata,
- **Capitolo 5: Conclusioni**, spiega in che modo la ricerca possa essere utilizzata ed i suoi possibili sviluppi futuri.

2.1 Blockchain

La tecnologia **Blockchain** ha espanso i suoi confini con la nascita di **Bitcoin**, in particolare, nel 2008, venne pubblicato un paper dal titolo "Bitcoin: A Peer-to-Peer Electronic Cash System" da un autore dall'identità ancora oggi misteriosa, quale Satoshi Nakamoto. In realtà, non solo non si conosce ancora l'identità di quest'ultimo, si immagina per di più che si possa addirittura trattare di un collettivo di persone. [1]

2.1.1 Perché nasce Blockchain

Come descritto da Chiap et al. [2] nel libro "Blockchain. Tecnologia e applicazioni per il business", l'**intermediazione** è oggi la soluzione più utilizzata negli attuali sistemi finanziari, come anche per la verifica della proprietà dei beni e l'elaborazione delle transazioni.

Questo però comporta vari **problemi**, in quanto sono proprio gli intermediari a dover effettuare le varie verifiche, ad esempio, quelle per risalire ad una lunga catena di transazioni. Questa soluzione pertanto è costosa, poco efficiente, e soprattutto **non sicura**, in quanto nel caso in cui un intermediario fallisca, c'è il rischio di **perdere il proprio capitale**.

Nofer et al. [3] fanno notare come la tecnologia Blockchain promette di superare questi aspetti critici, rappresentando *"un passaggio dalla fiducia nelle persone alla fiducia nella matematica"* (Antonopoulos 2014), poiché gli **interventi umani non sono più necessari**

2.1.2 Definizione

Chiap et al. [2], definiscono Blockchain come:

un libro mastro digitale, decentralizzato e distribuito su un network, strutturato come una catena di blocchi responsabili dell'archiviazione dei dati.

È possibile aggiungere nuovi blocchi di informazioni, ma non è invece possibile la modifica o la rimozione di blocchi precedentemente aggiunti alla catena.

È fornita una rappresentazione grafica nella Figura 2.1

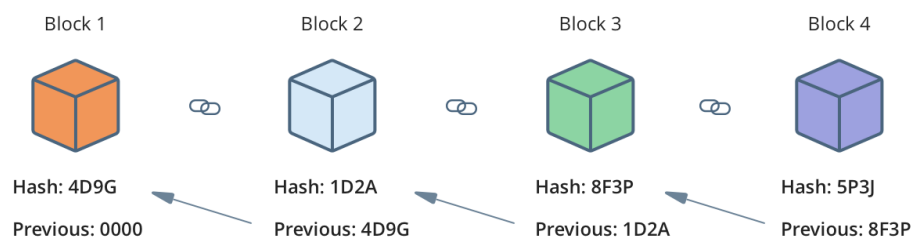


Figura 2.1: Rappresentazione grafica di una Blockchain. Fonte: <https://blog.goodaudience.com/blockchain-explained-in-1000-words-6bb83020b036?gi=9af01879e494>

Come riportato nella Figura 2.1, ogni blocco ha un collegamento col blocco precedente, ed inoltre, utilizza la funzione crittografica di hash, infatti, secondo Chiap et al. [2], in questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza e immutabilità.

Il risultato è un sistema aperto, neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di avere fiducia nel sistema non dipendono dalle intenzioni di nessun individuo o istituzione.

Blockchain non deve essere associata soltanto a Bitcoin, in quanto essa è molto più di un'infrastruttura di pagamento: è un sistema con le potenzialità per portare un nuovo livello di fiducia nelle applicazioni, introducendo un cambio di paradigma nelle modalità con cui esse vengono realizzate, dandoci l'opportunità di innovare liberamente.

2.2 Smart contracts

Come descritto da Chiap et al. [2], il termine smart contract è stato proposto per la prima volta da Nick Szabo e definito come **"un protocollo di transazione digitale che esegue i termini di un contratto"**

Uno smart contract ha l'obiettivo di **soddisfare** le condizioni del contratto in maniera **automatica**, minimizzando la possibilità di azioni malevole e il bisogno di fiducia negli

intermediari. Questi ultimi, infatti, nella forma di autorità centralizzate, tendono ad essere inefficienti, lenti e costosi.

Un contratto è un accordo tra due o più parti applicabile come vincolo legale. I contratti sono essenziali per creare fiducia tra le parti coinvolte in una transazione e possono essere considerati gli elementi costitutivi di ogni business. Un contratto può essere semplice, come un biglietto dell'autobus, o più complesso, come un contratto di lavoro. [2]

Nel caso di Blockchain, si può dire che uno Smart Contract è essenzialmente un programma, che a tutti gli effetti ha le sembianze di un vero contratto, ma con la differenza che esso viene salvato sulla Blockchain. Quindi non c'è più una legge a vincolare i termini del contratto, bensì si fa uso del **consenso del network**

Gli smart contract sono scritti utilizzando un linguaggio di programmazione, il che li rende privi di ambiguità.

Come descritto da Chiap et al. [2] essi **definiscono delle regole e automaticamente impongono alle parti coinvolte di rispettarle**, in modo decentralizzato, senza avere la necessità di affidarsi ad un ente centrale.

Quando le condizioni del contratto vengono soddisfatte esso, in modo automatico, esegue delle azioni specifiche, come ad esempio il trasferimento di denaro o di un bene.

2.3 Transazioni e consenso

Come descritto da lavori precedenti [2; 3], l'unità elementare di informazione che viene scritta su una Blockchain è chiamata **transazione**.

L'aggiunta di una nuova transazione implica un cambio di stato in una blockchain la quale, essendo logicamente centralizzata, è necessario trovare un modo per raggiungere un accordo sullo stato corretto della medesima.

Le transazioni sono operazioni **atomiche** in quanto non posso generare nessuno stato intermedio, difatti esse possono essere:

- **valide**, le quali vanno a modificare lo stato della blockchain;
- **invalidi**, le quali lasciano la blockchain nel suo stato attuale.

Inoltre le transazioni sono immutabili, infatti, non appena ne viene aggiunta una, il blocco ad essa collegato non può più essere modificato, né cancellato.

Per creare una transazione c'è bisogno di possedere l'oggetto ad essa associato, nel caso di una transazione di Bitcoin, c'è bisogno di un modo per dimostrare il possesso della relativa

quantità, bisogno che viene soddisfatto dalla presenza delle **firme digitali**. Il mittente, infatti, firma digitalmente una transazione prima di inviarla.

I vantaggi dell'utilizzo di firme digitali sono i seguenti:

- **autenticazione**, conferma il fatto che l'indirizzo che ha creato la transazione appartiene effettivamente all'utente;
- **integrità**, la transazione non ha subito alcuna modifica dopo la firma;
- **non ripudio**, l'utente che ha creato ed inviato la transazione non può negare di averlo fatto

Le transazioni vengono raggruppate in blocchi, i quali vengono poi aggiunti alla blockchain in modo sequenziale. Prima di essere aggiunta in un blocco, una transazione è senza conferme, con l'aggiungere di altri blocchi in modo sequenziale, la transazione avrà sempre più conferme.

E' da notare che una transazione con una sola conferma **non** è ancora considerata immutabile. Nel caso di Bitcoin, una transazione diventa immutabile dopo circa 6 conferme, in Ethereum invece 12.

Come detto in precedenza, i nodi di una blockchain si devono sempre trovare d'accordo su un unico stato.

Il consenso è l'unico modo per ottenere questo "stato unico" su tutta la blockchain, poichè permette di validare una transazione se e solo se si è ottenuto il consenso da parte del network.

In una blockchain il consenso è un accordo su ciò che è accaduto, e detiene l'unica possibile verità sullo stato attuale della blockchain.

Esistono principalmente due algoritmi di consenso più utilizzati nell'ambito delle blockchain, essi sono il **Proof of Work** (PoW) e il **Proof of Stake** (PoS).

2.4 Proof of Work e Proof of Stake

Chiap definisce Proof of Work e Proof of Stake nel seguente modo[2]:

Il Proof of Work è un protocollo utilizzato per raggiungere il consenso distribuito. Il PoW si basa sulla ricerca di un numero computazionalmente difficile da trovare, ma una volta trovato diventa facile per gli altri verificarne la correttezza. In un sistema che utilizza il PoW, un blocco è valido solo se contiene una soluzione valida al PoW. Coloro che si occupano della ricerca del numero, vengono definiti **miners**.

Il mining è il processo attraverso il quale le transazioni vengono validate, aggregate in blocchi e aggiunte alla blockchain.

Più in generale, il mining può essere visto come il meccanismo decentralizzato tramite il quale viene raggiunto il consenso distribuito e garantita la sicurezza del network.

Il Proof of Work viene visto come una competizione, infatti, i miners competono tra di loro, sfruttando la loro potenza di calcolo, e alla fine, colui che sarà riuscito a calcolare il numero, verrà ricompensato con un bene, nel caso di Bitcoin, egli riceverà una piccola quantità di Bitcoin, che equivalgono alle commissioni delle transazioni che sono state inserite nel blocco "*minato*".

Lo svantaggio principale del Proof of Work è lo spreco di energia prodotto dal mining, infatti, tutta l'energia utilizzata dai miners per competere tra di loro, sarà sprecata inutilmente.

Questo però, non risulta un problema nel caso del Proof of Stake.

Il Proof of Stake è un altro protocollo per raggiungere il consenso distribuito. Il suo scopo è lo stesso del Proof of Work, ma a differenza di quest'ultimo, i validatori vengono alternati scelti in anticipo in base alla quantità di criptovalute in loro possesso per la relativa blockchain, definita come **stake**.

2.5 Decentralized Applications

In un recente studio condotto nel 2020 da Metcalfe et al.[4] intitolato "*Ethereum, smart contracts, DApps*", gli autori descrivono le Decentralized Applications nel modo seguente:

Le applicazioni decentralizzate (o DApps) sono spesso descritte come "trustless" (senza fiducia) o "peer-to-peer" con la caratteristica distintiva: non c'è un singolo server o un'entità che le controlla, come in un modello client-server.

Utilizzando le DApps, possiamo ora disaccoppiare l'applicazione da una singola azienda o proprietario e creare una "applicazione decentralizzata".

Per capire cosa rende davvero differente una DApp rispetto a un'applicazione centralizzata, bisogna considerare come funzionano le attuali applicazioni.

Un'applicazione software moderna comprende almeno un'interfaccia utente (UI).

Può trattarsi di un'applicazione mobile scaricata da un'app store, di un sito web, o un'applicazione desktop installata su un computer. Le applicazioni moderne coinvolgono molti dati che possono essere forniti da un singolo gruppo o da una singola azienda, come nel caso di un'applicazione meteo che utilizza un'organizzazione meteorologica nazionale,

oppure, come nel caso di un'applicazione di social network, possono essere forniti dall'utente finale.

Una DApp utilizza la blockchain come base per l'archiviazione e l'elaborazione dei dati.

Essa viene implementata utilizzando uno smart contract. Attualmente l'interfaccia utente di una DApp è solitamente creata utilizzando un modello di sito web tradizionale. Si può quindi pensare a una DApp come a un sito web collegato ad uno o più smart contracts.

Una DApp ha le stesse proprietà generali di un'applicazione tradizionale.

La differenza principale, quindi, è che i dati e la computazione sono forniti dalla blockchain.

2.6 Machine Learning

Burkov e Andriy [5] definiscono il Machine Learning (Apprendimento Automatico) come un sottocampo dell'informatica che si occupa della creazione di algoritmi che, per migliorare, si basano sulla raccolta di dati di esempio che possono provenire dalla natura, dall'uomo o generati da un altro algoritmo.

L'apprendimento automatico può anche essere definito come il processo di risoluzione di un problema pratico attraverso:

1. la raccolta di un insieme di dati;
2. la costruzione algoritmica di un modello statistico basato su tale insieme di dati.

Ci sono vari tipi di apprendimento. Esso può essere supervisionato, semi-supervisionato, non supervisionato, con rinforzo:

- **Apprendimento supervisionato.** Gli elementi del dataset sono etichettati. L'obiettivo è quello di utilizzare il dataset per produrre un modello che prenda in input un vettore di features e fornisca informazioni che permettano di dedurre l'etichetta per questo vettore di features.
- **Apprendimento non supervisionato.** Gli elementi del dataset non sono etichettati. L'obiettivo è quello di creare un modello che prenda in input un vettore di features e lo trasformi in un altro vettore, o in un valore che possa essere utilizzato per risolvere un problema pratico.
- **Apprendimento semi-supervisionato.** Il dataset contiene sia elementi etichettati che non. Di solito gli elementi non etichettati sono in quantità maggiore rispetto a quelli

etichettati. L'obiettivo è lo stesso dell'apprendimento supervisionato, con la speranza che, utilizzando molti dati non etichettati, si possa produrre un modello migliore.

- **Apprendimento con rinforzo.** E' un sottocampo del Machine Learning nel quale la macchina "vive" in un ambiente ed è capace di percepire lo stato dello stesso come un vettore di features.

Azioni differenti portano a ricompense differenti. L'obiettivo è quello di imparare una policy. Una policy è una funzione che prende in input il vettore di features di uno stato e produce un'azione ottimale da eseguire in quello stesso stato. Questa funzione misura il grado di successo di un'azione o decisione, rispetto a un obiettivo predeterminato, fornendo un feed-back:

- Se il feed-back è positivo, la macchina si è avvicinata all'obiettivo e le viene assegnato un premio.
- Se il feed-back è negativo, la macchina si è allontanata dall'obiettivo dopo l'azione e le viene assegnata una penalità.

Metodologia utilizzata

Al fine di mettere luce sulla questione, si è deciso di utilizzare una metodologia di ricerca che si compone in diverse fasi: a partire dalla formulazione della domanda da cui avviare la scansione dei documenti, passando per la selezione di materiale inerente agli obiettivi preposti, fino all'analisi dei risultati ottenuti. La fonte da cui si sono attinti i materiali è **Google Scholar**: un database contenente un vasto numero di articoli scientifici accreditati.

3.1 Obiettivi dell'analisi

L'obiettivo di questa ricerca è quello, innanzitutto, di capire cos'è la tecnologia Blockchain, come funziona, e quali sono i suoi campi applicativi.

In secondo luogo, si vuole identificare i vantaggi che si ottengono combinandola all'intelligenza artificiale, oltre ad identificare i campi nei quali esse possono dare i maggiori risultati.

Si è quindi cominciata l'analisi con l'identificazione di quattro domande, che guideranno tutta la ricerca:

- **Cos'è la tecnologia Blockchain?**
- **Quali sono i vantaggi dell'applicare l'AI alla Blockchain?**
- **Quali sono i vantaggi dell'applicare la Blockchain all'AI?**
- **In che ambito Blockchain e AI possono convergere?**

Per poter rispondere a queste domande, è stata utilizzata la metodologia della Systematic Literature Review (SLR), ovvero una tecnica che, dato un soggetto d'interesse, consiste nell'esaminare articoli inerenti già esistenti e, sintetizzandoli, riuscire a pervenire ad una visione complessiva dell'argomento.[6]

3.2 Formulazione search query

Uno dei punti più importanti per riuscire ad identificare dei buoni articoli, è quello di trovare delle parole chiave che identifichino al meglio il fulcro della ricerca. Per formulare quindi la "frase" da cui far partire la ricerca, sono state inizialmente identificate come parole chiave "Blockchain" , "Artificial Intelligence" ed "applications".

Per massimizzare il numero degli articoli ottenuti, sono stati identificati anche sinonimi delle parole chiavi sovrastanti, ad esempio il termine "machine learning", nonostante indichi un sottoinsieme dell'Intelligenza Artificiale, sarebbe potuto essere stato utilizzato come termine ad esclusione del primo, quindi è stato successivamente aggiunto alla search query, data la sua correlazione al termine "artificial intelligence".

Ciò è stato fatto perchè ci sono articoli che potrebbero passare in secondo piano, soltanto perchè invece di utilizzare la parola chiave che noi cerchiamo, usano proprio dei sinonimi, riducendo così la visibilità dell'articolo

La query è stata composta nel modo seguente:

- tutte le parole che identificavano uno stesso risultato, sono state accorpate all'interno di una parentesi, e congiunte tramite l'operatore logico "OR";
- il resto delle parole, sono state unite sia tra di loro, che con quelle tra parentesi, attraverso l'operatore "AND".

La query, al termine di questa fase, è stata quindi costruita in questo modo:

```
"blockchain" AND ( "machine learning" OR  
"artificial intelligence") AND "applications"
```

3.3 Raccolta e selezione degli articoli

Una volta definita la search query, essa è stata utilizzata per ottenere tutti gli articoli.

Nella fase iniziale, si è deciso di effettuare una scrematura degli articoli, in modo da selezionare tutti quelli che effettivamente erano correlati all'obiettivo della tesi, ovvero sono

stati selezionati tutti gli articoli che riguardano la convergenza tra Blockchain ed Intelligenza Artificiale.

In una seconda fase, gli articoli più rilevanti, dopo essere stati selezionati, sono stati raggruppati in cluster, in particolare ne sono stati individuati 3:

- **integrazione di Blockchain e AI e futuri casi d'uso**, dove sono stati raccolti tutti gli articoli che parlano in generale dell'integrazione di Blockchain e Intelligenza Artificiale, ed i loro possibili futuri sviluppi;
- **Blockchain e AI nell'IoT**, dove sono stati raccolti tutti gli articoli che parlano delle attuali integrazioni di Blockchain e AI nel campo dell'IoT e delle smart cities;
- **Blockchain e AI nell'e-Health**, dove sono stati raccolti tutti gli articoli che parlano delle attuali integrazioni di Blockchain e AI nel campo dell'e-health.

3.4 Definizione dei criteri di esclusione/inclusione

La formulazione delle query richiede la definizione di alcuni criteri di esclusione e di inclusione al fine di evitare risultati incoerenti o non in linea con i nostri obiettivi.

Per la ricerca, in particolare sono stati esclusi dallo studio:

- articoli non in inglese,
- articoli non completamente accessibili,
- articoli il cui principale soggetto non appartenesse al campo blockchain o intelligenza artificiale.

Sono invece stati inclusi nella ricerca:

- articoli che trattavano applicazioni attuali della blockchain,
- articoli che trattavano dell'utilizzo di blockchain applicata all'intelligenza artificiale, e viceversa.

4.1 Stato dell'arte

Questo capitolo illustra lo stato dell'arte e i lavori presenti in letteratura relativi all'impatto della blockchain sugli algoritmi di intelligenza artificiale, alle applicazioni attuali e a quelle possibili.

4.1.1 Integrazione di Blockchain e AI e futuri casi d'uso

Gli scienziati hanno lottato a lungo per mantenere la qualità di un dataset, per l'apprendimento automatico, da parte di un'entità AI.

Infatti, come descritto da Ekramifard et al. [7], i dataset sono molto costosi, come pure la costruzione e il mantenimento dell'integrità dei loro dati sono molto difficili.

La Blockchain, come spiegato pocansi, rappresenta un mezzo di archiviazione altamente sicuro e anche un sistema efficiente per mantenere l'integrità dei dati.

Inoltre, essendo essa anche immutabile, permette di creare dataset di alta qualità, permanenti e in continua crescita.

Blockchain quindi potrebbe andare a sopperire molti dei problemi relativi ad un'intelligenza artificiale. Un esempio di come un'intelligenza artificiale possa migliorare, se combinata con la tecnologia Blockchain, deriva dal Deep Learning.

In base ad uno studio pubblicato sul Journal *Future Internet*[8], è emerso proprio come l'utilizzo di Blockchain insieme all'IA possa dare vita ad un nuovo mondo di applicazioni

per un'umanità migliore, dalla governance assistita da computer, alla previsione di eventi di livello estintivo; si può dare vita anche alla creazione di IA in grado di decodificare gli schemi delle onde cerebrali umane.

Un'entità di questo tipo potrebbe interagire direttamente con il cervello umano, utilizzarlo come serie di dati per acquisire informazioni sul suo funzionamento e, in ultima analisi, fornire una conoscenza approfondita in molti campi della scienza, che prima era impossibile acquisire.

Utilizzando tecniche di deep learning, il livello evolutivo dell'IA potrebbe raggiungere livelli esponenziali senza precedenti, utilizzando i big data acquisiti da Smart Contracts, transazioni quotidiane, condizioni meteorologiche, IoT o letteratura archiviata su una Blockchain.

Ma il deep learning non è l'unico campo nel quale l'AI può utilizzare le capacità della blockchain per scopi importanti, ce ne sono altri tra cui, l'Internet of Things (IoT) e l'analisi Monte Carlo.

Inoltre ci potrebbe essere anche la possibilità di memorizzare su una blockchain agenti di AI già addestrati, permettendone poi la fruizione da parte degli utenti attraverso un sistema di pagamento pay per use, come vedremo in seguito, anche in un Ted Talk di Ben Goertzel [9] si è fatto riferimento ad un sistema del genere.

Come già detto, una blockchain costituisce un metodo innovativo per archiviare informazioni su uno spazio pubblico, attraverso una procedura di pagamento. Oltre alle informazioni statiche, potremmo anche memorizzare il codice dei programmi in modo simile a Github, e in effetti il sistema git sottostante è molto simile a una blockchain sotto molti aspetti. Questi programmi possono essere letti liberamente perché fanno parte dei blocchi immutabili della catena.

Il problema principale però è che ogni transazione che inserisce i dati nella blockchain ha un costo e quindi l'utente non è incentivato a inserire programmi a meno che non ci sia almeno una possibilità minima di guadagno.

Una raccolta di applicazioni basata su Blockchain può essere resa navigabile tramite un portale come Agora, formando un nuovo canale di distribuzione del software. In questo modo si gettano le basi per un ideale a lungo coltivato dai programmatori: un mercato indipendente in cui gli sviluppatori possano guadagnare tramite il loro lavoro senza la necessità di intermediari.

Anche nel settore medico ci saranno nuove possibilità di sviluppo dovute all'integrazione di Blockchain e IA, ad esempio, per aumentare la sicurezza delle applicazioni sanitarie basate

su Blockchain, possono essere utilizzate tecniche di apprendimento automatico per rilevare gli exploit sconosciuti.

Inoltre, l'IA, può anche essere utilizzata per rilevare e bloccare l'attacco di maggioranza o i comportamenti anomali nella rete Blockchain.

Ricordiamo anche importanti Ted Talk che hanno parlato dell'efficacia della convergenza tra Blockchain e AI.

L'autore Steve Lund, in un Ted Talk del 2018 intitolato "*The Convergence of Blockchain, Machine Learning and the Cloud*"[10], afferma che la tecnologia Blockchain è pronta per la produzione, in quanto essa è stata dimostrata, validata, certificata ed è anche già utilizzata in 16 delle più grandi banche.

Inoltre dichiara che le tecnologie Machine Learning ed Artificial Intelligence sono maturate ancora di più rispetto agli scorsi anni, e che l'utilizzo di queste, insieme alla Blockchain, dia la possibilità di risolvere problemi, sia vecchi che nuovi, implementando nuove soluzioni che facciano convergere queste tecnologie nel migliore dei modi.

In un altro Ted Talk del 2019 intitolato "*Decentralized AI*"[9], l'autore Ben Goertzel fa riferimento ad un progetto chiamato SingularityNET, esso tratta una piattaforma decentralizzata basata sulle tecnologie Blockchain ed Artificial Intelligence, in particolare è un DApp Store, ovvero un marketplace che offre applicazioni decentralizzate (DApps).

SingularityNET in particolare offre un insieme di intelligenze artificiali, che operano su una rete decentralizzata.

Il funzionamento è il seguente: se un'azienda ha bisogno di un AI, può fare richiesta all'interno della rete, dopodiché, l'AI che sarà più conforme alla richiesta dell'azienda farà un'offerta.

Anche l'autore Giuseppe Bertone nel suo Ted Talk intitolato "*AI e Blockchain, una collaborazione virtuosa*"[11], afferma che si potrebbe creare un'intelligenza artificiale che utilizzi degli smart contract che vincolino ciò che essa stessa può fare, facendola evolvere, rimanendo comunque sotto il nostro controllo.

Per fare ciò è necessario l'intervento di strumenti che forniscano la capacità di esprimere la volontà in maniera democratica.

Il corretto funzionamento dell'AI viene garantito proprio dalla capacità di azione dell'uomo, il quale è il responsabile dell'immissione dei dati all'interno dell'AI.

Ciò comporta necessariamente la responsabilità e consapevolezza per l'uomo del proprio ruolo.

Inoltre, come descritto dall'azienda IBM[12], l'IA è in grado di leggere, comprendere e correlare i dati in modo rapido e completo ad una velocità incredibile, portando un nuovo livello di intelligenza alle reti aziendali basate su blockchain. Questo potrebbe far aumentare la velocità delle transazioni, rendendo più efficiente la Blockchain.

4.1.2 Blockchain e AI nell'IoT

Uno dei campi nei quali Blockchain e AI, combinati insieme, stanno avendo il maggior successo, è quello dell'**Internet Of Things**. Esso sta stravolgendo giorno dopo giorno le nostre vite, comportando la nascita di nuove applicazioni destinate alla creazione delle smart cities e degli smart transports, rendendo la vita umana più affidabile.

Alla base di tutto ciò c'è sicuramente l'Intelligenza Artificiale la quale riesce a dare vita a creazioni incredibili, che migliorano continuamente grazie anche all'utilizzo del Machine Learning, sfruttando una grandissima quantità di dati.

Dati che però sono centralizzati, e quindi si portano dietro tutti gli svantaggi di un'architettura centralizzata, quali la sicurezza e la privacy, i vincoli di risorse e la mancanza di dati di addestramento sufficienti.

Ed è qui che entra in gioco la Blockchain: infatti, come riportato nei recenti studi di Singh [13], quest'ultima può dare una grande mano al campo dell'intelligenza artificiale, fornendo un'architettura decentralizzata che va a risolvere tutti i problemi descritti pocansi.

Infatti essi riportano come la Blockchain unita all'AI stia dando un grande contributo nell'ambito delle smart cities, le cosiddette "città intelligenti", e che nonostante ciò è bene ricordare che, come sempre, l'arrivo di una nuova tecnologia porta con sé sia tanti benefici che altrettante sfide.

Come riportato pocansi, i dati sono essenziali quando si parla di intelligenza artificiale, soprattutto se combinata all'IoT, che porta con sé la peculiarità di salvare immense quantità di dati relative ai vari sensori.

In un recente studio del medesimo Singh [14], l'obiettivo principale è stato quello di progettare e sviluppare un'architettura IoT con blockchain e AI per supportare un'efficace analisi dei big data. Egli propone un'architettura IoT intelligente, abilitata da blockchain e intelligenza artificiale, che fornisce un modo efficiente per far convergere blockchain e AI per l'IoT con le tecniche e le applicazioni più avanzate.

La valutazione dell'architettura proposta è suddivisa in due parti: **analisi qualitativa** e **analisi quantitativa**:

- Nell'analisi qualitativa, si descrive come utilizzare l'IA e la blockchain nelle applicazioni IoT con "**AI-driven Blockchain**" e "**Blockchain-driven AI**".
- Nell'analisi quantitativa si presentano una valutazione delle prestazioni dell'architettura *BlockIoTIntelligence* per confrontare le ricerche esistenti sull'intelligenza dei dispositivi, della nebbia, dei bordi e del cloud in base ad alcuni parametri quali precisione, latenza, sicurezza e privacy, complessità computazionale e costo energetico nelle applicazioni IoT.

Singh, con i risultati di queste applicazioni, mostra che l'architettura proposta, basata sulla tecnologia Blockchain, ha prestazioni superiori alle architetture IoT esistenti e mitiga le sfide attuali.

4.1.3 Blockchain e AI nell'e-Health

Un altro campo nel quale Blockchain e AI hanno avuto una grande convergenza è sicuramente quello dell'e-Health, ovvero la pratica della salute attraverso il supporto di strumenti informatici.

Difatti con l'avvento e lo sviluppo del machine learning negli ultimi anni, questo campo è cresciuto a dismisura.

In un recente articolo pubblicato sull'IEEE Internet of Things Magazine[15], emerge come esista un'elevata possibilità di manomettere i dataset di addestramento e di produrre risultati distorti. Per questo motivo, viene proposta una soluzione basata su Blockchain per proteggere i dataset generati dai dispositivi IoT per le applicazioni di e-Health.

Nel paper "*A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence*" [7], gli autori fanno anche loro riferimento al campo dell'e-health, dimostrando come l'IA può migliorare la sicurezza delle attuali applicazioni sanitarie basate su Blockchain, andando ad utilizzare algoritmi di machine learning per rilevare la presenza di exploit sconosciuti.

Dopo aver terminato la fase di analisi del materiale raccolto, è possibile adesso tirare delle somme e rispondere alle domande che ci eravamo posti come obiettivo.

4.1.4 Vantaggi dell'applicazione di AI su Blockchain

Dopo aver letto e analizzato tutti gli articoli, di seguito si riportano i vari vantaggi che l'Intelligenza Artificiale offre se applicata alla Blockchain:

- **Intelligenza agli smart contracts.** Attualmente, gli smart contracts si basano sulle decisioni prese in base agli input e alle regole. L'intelligenza artificiale può migliorare l'efficacia dei contratti intelligenti rendendoli più adattivi, ovvero andando ad includere logica, grafi neurali e reti neurali. Inoltre l'intelligenza artificiale potrà anche fare previsioni sul fatto che un contratto debba essere eseguito o meno.
- **Transazioni più rapide.** L'intelligenza artificiale è in grado di leggere, comprendere e correlare i dati in modo rapido e completo ad una velocità incredibile, ciò permetterebbe di effettuare le transazioni, ovvero creazioni di nuovi blocchi, in un modo più veloce.
- **Maggiore efficienza.** Questo è un effetto collaterale dato dal punto precedente, ovvero, dall'accelerazione delle transazioni. Difatti, transazioni più veloci, portano alla creazione di più transazioni in meno tempo, e quindi ad un'efficienza della rete blockchain maggiore.

4.1.5 Vantaggi dell'applicazione di Blockchain su AI

Dopo aver letto e analizzato tutti gli articoli, di seguito si riportano i vari vantaggi che la Blockchain offre se applicata all'Intelligenza artificiale:

- **Sicurezza dei dati.** La sicurezza è il vantaggio principale che blockchain offre agli algoritmi di intelligenza artificiale, in quanto, i dati utilizzati per addestrare gli agenti, sono sempre stati centralizzati, e ciò conseguiva in un *single point of failure*. La decentralizzazione di blockchain va a risolvere questo problema.
- **Presenza di community.** Come nell'esempio di *SingularityNet*, ci sarà la possibilità di permettere a più utenti di contribuire alla crescita di una piattaforma. In *SingularityNet*, ogni utente, può creare e modificare degli agenti di AI sulla rete blockchain, in modo da contribuire a renderla sempre migliore.
- **Scalabilità.** Essa è un effetto collaterale della presenza di community, in quanto, permettere a più persone di proporre le proprie soluzioni attraverso un sistema decentralizzato, permetterebbe agli agenti di AI di evolvere in modo più veloce, creando agenti sempre più intelligenti.

4.1.6 Campi applicativi per AI e Blockchain

Durante la ricerca, i principali campi che hanno visto Blockchain ed Intelligenza Artificiale convergere tra loro sono stati:

- **Deep Learning.** In questo campo si è visto come è possibile applicare entrambe le tecnologie per dare vita ad agenti in grado di interagire direttamente con il cervello umano e, inoltre, è anche possibile fornire una conoscenza approfondita in molti campi della scienza, che prima era impossibile acquisire .
- **Internet of Things.** In questo campo si è visto come blockchain e intelligenza artificiale stanno collaborando, al fine di creare le cosiddette "smart cities", sfruttando e manipolando i dati dei sensori.
- **E-Health.** In questo campo, in particolare, si è visto come l'intelligenza artificiale stia dando una mano in ambito medico sulle attuali implementazioni sanitarie basate su blockchain, andando a migliorare la sicurezza, utilizzando il machine learning per la rilevazione di exploit sconosciuti.

Inoltre è anche emerso un progetto chiamato *SingularityNet*, il quale si basa su un insieme di intelligenze artificiali che operano su una rete decentralizzata.

Esso funziona come un marketplace, ovvero, offre un insieme di applicazioni, ma, essendo basato su blockchain, esso viene definito DApp Store.

5.1 Lavoro svolto

Il lavoro svolto in questa tesi di ricerca si è incentrato sullo studio della tecnologia Blockchain, delle sue attuali implementazioni, e delle possibili implementazioni correlate all'utilizzo dell'Intelligenza Artificiale.

La ricerca è stata condotta attraverso la metodologia della "Systematic Literature Review", che consiste nel:

1. Scegliere delle parole chiavi da cui partire;
2. Utilizzare dei criteri di inclusione ed esclusione, al fine di ottenere una visione globale dell'argomento d'interesse;
3. Raccogliere articoli già esistenti, correlati all'argomento di interesse;
4. Analizzarli e riassumerli.

5.2 Sviluppi futuri

Dati i risultati ottenuti dalla ricerca, si potrebbe ambire a:

- promuovere l'utilizzo dell'intelligenza artificiale all'interno degli Smart Contracts al fine di migliorare l'efficienza della Blockchain andando a ridurre i tempi di creazione di una transazione;

- creare un'intelligenza artificiale che utilizzi degli smart contract che vincolino ciò che essa stessa può fare, facendola evolvere, rimanendo comunque sotto il nostro controllo.
- continuare a sfruttare queste due tecnologie all'interno dei campi dove esse sono già presenti, quali Internet of Things, E-Health e Deep Learning, andando a migliorare la loro collaborazione, e allo stesso tempo, iniziare ad applicarle in altri campi dove ancora non sono presenti.

Dal punto di vista delle tecnologie utilizzate per eseguire la Systematic Literature Review, invece, possibili sviluppi potrebbero riguardare:

Lo sviluppo di una Intelligenza Artificiale capace di identificare le keywords necessarie al fine di massimizzare i risultati utili di una ricerca.

Ringraziamenti

I miei ringraziamenti vanno al professor Fabio Palomba, che mi ha spronato durante il corso di Fondamenti di Intelligenza artificiale, allo studio e alla passione per i suoi argomenti. Grazie per la sua professionalità.

Bibliografia

- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008. (Citato alle pagine 1 e 4)
- [2] G. Chiap, J. Ranalli, and R. Bianchi, *Blockchain. Tecnologia e applicazioni per il business: Tutto ciò che serve per entrare nella nuova rivoluzione digitale*. HOEPLI EDITORE, 2019. (Citato alle pagine 4, 5, 6 e 7)
- [3] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017. (Citato alle pagine 4 e 6)
- [4] W. Metcalfe *et al.*, "Ethereum, smart contracts, dapps," *Blockchain and Crypt Currency*, p. 77, 2020. (Citato a pagina 8)
- [5] A. Burkov, *The hundred-page machine learning book*, vol. 1. Andriy Burkov Quebec City, QC, Canada, 2019. (Citato a pagina 9)
- [6] G. Giordano, F. Palomba, and F. Ferrucci, "On the use of artificial intelligence to deal with privacy in iot systems: A systematic literature review," *Journal of Systems and Software*, p. 111475, 2022. (Citato a pagina 12)
- [7] A. Ekramifard, H. Amintoosi, A. H. Seno, A. Dehghantanha, and R. M. Parizi, *A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence*, pp. 147–160. Cham: Springer International Publishing, 2020. (Citato alle pagine 14 e 18)
- [8] K. Sgantzios and I. Grigg, "Artificial intelligence implementations on the blockchain. use cases and future applications," *Future Internet*, vol. 11, no. 8, 2019. (Citato a pagina 14)

- [9] B. Goertzel, "Decentralized ai," 2019. (Citato alle pagine 15 e 16)
- [10] S. Lund, "The convergence of blockchain, machine learning and the cloud," 2018. (Citato a pagina 16)
- [11] G. Bertone, "Ai e blockchain, una collaborazione virtuosa," 2017. (Citato a pagina 16)
- [12] (Citato a pagina 17)
- [13] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, p. 102364, 2020. (Citato a pagina 17)
- [14] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2020. (Citato a pagina 17)
- [15] T. R. Gadekallu, M. Manoj, N. Kumar, S. Hakak, S. Bhattacharya, *et al.*, "Blockchain-based attack detection on machine learning algorithms for iot-based e-health applications," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 30–33, 2021. (Citato a pagina 18)