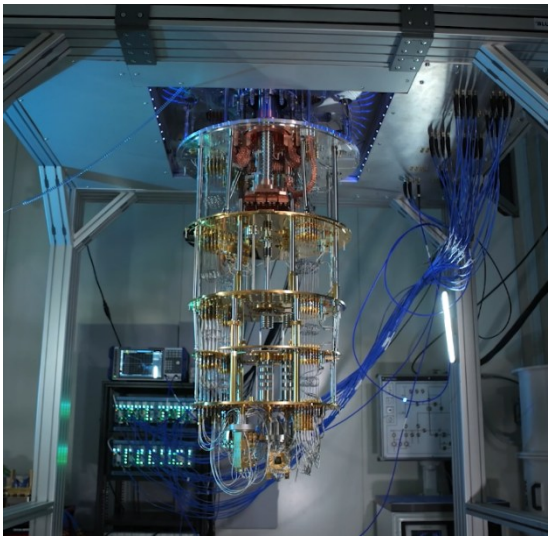
I Computer Quantistici



Computer quantistico in funzione presso il Dipartimento di Fisica dell'Università degli Studi di Napoli Federico II

La scienza offre la metafisica più audace della nostra epoca. È una costruzione profondamente umana, animata dalla fede che se sogniamo, ci sforziamo di scoprire, di spiegare e sognare di nuovo, immergendoci ripetutamente in territori inesplorati, il mondo in qualche modo diventerà più chiaro e coglieremo la vera stranezza dell'universo. E quella stranezza si rivelerà tutta collegata, e avrà un senso.

– Edward O. Wilson

Introduzione

Il presente articolo è rivolto a chi, pur non possedendo conoscenze tecniche specifiche, desidera capire in modo semplice e intuitivo il funzionamento dei computer quantistici e le innovazioni che questi potranno apportare nel futuro.

Negli ultimi decenni, i computer hanno trasformato il nostro modo di vivere, lavorare e comunicare. Oggi sta emergendo una tecnologia rivoluzionaria destinata a ridefinire il concetto stesso di calcolo: il **computer quantistico**.

Anche i supercomputer più potenti incontrano dei limiti, ad esempio nelle simulazioni molecolari, nei modelli climatici o nell'ottimizzazione di reti complesse, che possono richiedere giorni – o persino mesi – di calcolo.

Già negli anni '80, il fisico Richard Feynman e il matematico Yuri Manin intuirono che simulare la natura con computer tradizionali avrebbe richiesto risorse enormi. Fu allora che Feynman lanciò la sua celebre sfida[1]: «*Se vogliamo simulare la natura, costruiamo un computer che obbedisca alle leggi della meccanica quantistica*.»

Da questa intuizione nacque l'idea dei computer quantistici: macchine che sfruttano i principi della fisica subatomica per affrontare problemi oggi fuori portata dei computer tradizionali.

I computer quantistici si basano su un paradigma radicalmente nuovo, con regole proprie e scenari ancora del tutto inediti.

Sebbene ancora in fase sperimentale, il loro potenziale stimola già la ricerca scientifica e l'innovazione tecnologica. Dalla progettazione di nuovi farmaci alla scoperta di materiali avanzati, dalla sicurezza informatica al potenziamento dell'Intelligenza Artificiale, i computer quantistici promettono di cambiare il modo in cui si affrontano le sfide più complesse del nostro tempo.

[1] Richard Feynman, "*Simulating Physics with Computers*", discorso tenuto al MIT nel 1981 alla First Conference on Physics of Computation.

Limiti fisici dei computer classici

Per decenni, l'informatica ha seguito la Legge di Moore, secondo la quale il numero di transistor su un chip raddoppia circa ogni due anni.

Oggi, però, si è arrivati a un punto critico: i transistor, ormai su scala nanometrica, sono talmente piccoli da manifestare effetti quantistici rilevanti. Uno di questi è il cosiddetto **effetto tunnel**, che può compromettere l'affidabilità dei circuiti elettronici.

In pratica, gli elettroni possono attraversare barriere che, secondo la fisica classica, sarebbero invalicabili: come una pallina che, invece di rimbalzare, passa attraverso un muro grazie a un tunnel invisibile.

È proprio questo limite che segna il confine oltre cui la tecnologia al silicio non può più spingersi, aprendo la strada a soluzioni del tutto nuove, come i computer quantistici.

La base del funzionamento di un computer classico

Prima di capire cos'è un computer quantistico, è utile capire come funziona un computer classico.

Un computer classico (CC) si basa su una memoria costituita da elementi chiamati **bit** (abbreviazione di *binary digit*). Un bit è l'unità elementare di informazione e può assumere solo due valori: **0** oppure **1**, corrispondenti a due diversi stati fisici, come livelli differenti di tensione, corrente o carica elettrica.

Otto bit formano un **byte**, l'unità base per misurare la memoria digitale.

Combinando più bit, si possono rappresentare lettere, numeri, istruzioni, immagini e suoni.

Ad esempio, nella codifica ASCII, la lettera "A" maiuscola è rappresentata da 01000001, mentre la lettera "a" minuscola da 01100001.

Nei CC, i calcoli avvengono sui bit. Si prenda, ad esempio, la somma di due numeri, 7 + 2. In binario, 7 si scrive 00000111 e 2 come 00000010. Il calcolo segue le regole dell'aritmetica binaria, producendo 00001001, che è la rappresentazione di 9.

Convertendolo in decimale, si ottiene il numero 9: $00001001 = 1\times2^3+0\times2^2+0\times2^1+1\times2^0 = 8+0+0+1 = 9$

Concetti base del Computer Quantistico

La fisica quantistica studia il comportamento delle particelle piccolissime, come elettroni, fotoni e atomi.

A queste scale, la natura non obbedisce più alle regole della fisica classica che si usano per descrivere oggetti grandi – come corpi terrestri o pianeti – ma segue leggi particolari e spesso sorprendenti.

Per esempio, in fisica quantistica:
- una particella può comportarsi sia come onda sia come oggetto materiale;
- può trovarsi in più stati contemporaneamente, finché non viene osservata;
- due particelle possono restare collegate a distanza, influenzandosi istantaneamente.

In poche parole, la fisica quantistica permette di comprendere il mondo invisibile dell'infinitamente piccolo, da cui derivano molte tecnologie moderne: dai laser ai computer, fino ai pannelli solari. E oggi, proprio grazie a questi principi, si apre la strada a una nuova rivoluzione: il computer quantistico.

Il computer quantistico (CQ) sfrutta queste leggi per elaborare i dati in modo radicalmente diverso dal CC.

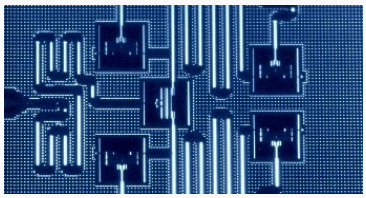
La sua unità fondamentale non è il bit, ma il **qubit** (*quantum bit*), l'equivalente quantistico del bit classico.

Un qubit può essere realizzato in diversi modi; in termini semplici, si può immaginare come una particella che può trovarsi in due stati distinti. Ad esempio, un **elettrone con spin "su" o "giù"**, associati agli stati 0 e 1, oppure un **fotone con polarizzazione verticale o orizzontale.**

Lo **spin è una proprietà degli elettroni** che li fa comportare come minuscoli magneti con due orientamenti possibili: 'su' o 'giù'. Non è una vera rotazione come quella di una trottola, ma un modo per descrivere come interagiscono con i campi magnetici.

Lo spin è fondamentale per fenomeni come il magnetismo, ed è alla base di numerose tecnologie, dalle **risonanze magnetiche** in medicina ai **sensori magnetici** utilizzati nell'industria e nella ricerca.

Manipolare una singola particella è però estremamente difficile: il sistema è instabile e può essere alterato da qualsiasi interazione esterna, anche minima, come l'assorbimento di un fotone.



Per creare sistemi più stabili e controllabili, aziende come IBM e Google realizzano qubit usando "*atomi artificiali*": sistemi quantistici abbastanza grandi da poter essere controllati con precisione, ma ancora sufficientemente piccoli da conservare le proprietà quantistiche della materia.

Un esempio di un processore Yorktown di IBM, contenente 5 qubit. Ogni qubit misura circa 100 micron (0,1 mm).

1. Sovrapposizione

Un bit, come viene definito, può trovarsi soltanto in uno dei due stati possibili: 0 oppure 1.

Un qubit, invece, può trovarsi **in una combinazione sovrapposta** degli stati 0 e 1: questo fenomeno è detto **sovrapposizione** *(superposition)*.

Una metafora intuitiva è quella della moneta lanciata in aria: finché è in volo, non è semplicemente testa o croce, ma si trova in una sovrapposizione dei due stati. Allo stesso modo, un qubit può essere sia 0 sia 1 contemporaneamente. **Solo al momento della "caduta"** – cioè quando si misura il qubit – **il sistema si stabilizza in uno stato definito**: 0 o 1, secondo le probabilità associate alla sovrapposizione. Questo comportamento riflette l'interpretazione di Copenhagen, secondo cui lo stato di un sistema quantistico si definisce solo al momento dell'osservazione.

I fisici descrivono questo comportamento con una formula chiamata *funzione d'onda*[2], che **assegna a ogni risultato una certa probabilità** (ad esempio 70% testa e 30% croce), e in cui la somma di tutte le probabilità è sempre pari a 1. In pratica è uno strumento matematico che serve a tenere traccia delle possibilità finché non si effettua una misura, proprio come accade con una moneta in aria prima di cadere.

Grazie a questa proprietà, un CQ può elaborare un numero di combinazioni esponenzialmente più alto rispetto a un CC.

Con ***n* qubit** è possibile rappresentare **in sovrapposizione** – cioè simultaneamente – tutte le $\mathbf{2^n}$ **combinazioni** binarie. Ad esempio, con 2 bit classici si può rappresentare solo uno stato alla volta tra i quattro possibili: 00, 01, 10 e 11. Con 2 qubit, invece, il sistema può mantenere aperti contemporaneamente tutti e quattro questi stati.

Aggiungendo qubit, le possibilità raddoppiano ogni volta: con 3 qubit diventano 8 stati, con 4 qubit 16, e così via.

[2] La funzione d'onda, descritta dall'equazione di Schrödinger, rappresenta lo stato quantistico di una particella o di un sistema e consente di calcolare la probabilità di trovarlo in una certa posizione in un determinato momento.

Solo nel momento in cui il qubit viene misurato emerge uno solo degli stati possibili, selezionato in base alla loro probabilità. Se le probabilità sono identiche per tutti gli stati, ciascuno ha la stessa possibilità di essere scelto.

2. Entanglement

Un'altra proprietà straordinaria dei qubit è l'**entanglement quantistico**, un legame profondo (letteralmente "*intreccio*") che si crea tra particelle quando interagiscono, anche solo per un istante. Da quel momento non possono più essere descritte separatamente: **formano un unico sistema, anche se rimangono fisicamente distanti**.

È un po' come una scatola che contiene due guanti, uno destro e uno sinistro. Se la scatola viene divisa e spedita in due luoghi diversi, nel momento in cui si apre una metà e si trova, ad esempio, il guanto destro, si sa subito che l'altro è quello sinistro, anche senza osservarlo.

Nel mondo quantistico, però, la situazione è ancora più sorprendente. Se le due particelle sono entangled, prima della misura non è stabilito quale "guanto" sia destro e quale sia sinistro: è come se fossero entrambe sospese in una condizione di possibilità condivisa. Solo nel momento della misurazione si definisce lo stato, e immediatamente anche l'altra particella assume quello coerente con il sistema condiviso.

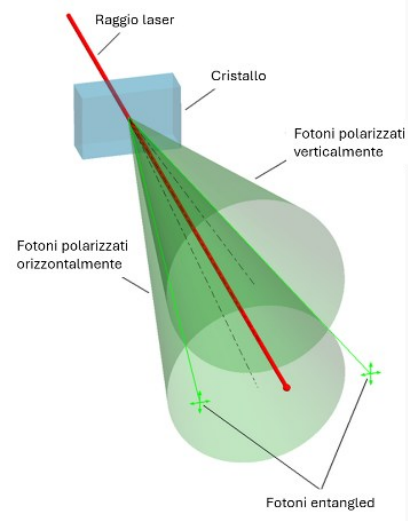
Il punto chiave è che **questa correlazione non nasce da uno scambio di informazioni**, ma dal fatto che le particelle fanno parte di **un unico sistema quantistico**. È una connessione profonda, ma non causale: non c'è un'azione dell'una sull'altra, semplicemente si comportano come un tutt'uno, anche a distanza.

Quando n qubit sono entangled, non si hanno semplicemente 2^n stati in parallelo, ma un unico stato quantistico globale che li unisce in un sistema coerente. L'informazione viene distribuita sull'insieme dei qubit e non è più contenuta in ciascuno separatamente. Questo consente di manipolarli collettivamente, trasformando la sovrapposizione in una forma di **parallelismo "intelligente"**.

Grazie a questa proprietà diventano possibili algoritmi che sfruttano le correlazioni e le interferenze quantistiche per raggiungere prestazioni esponenzialmente superiori rispetto ai metodi classici.

È un po' come un'orchestra: ogni qubit è uno strumento, e solo se tutti suonano in perfetta sintonia si ottiene la melodia desiderata.

Per generare fisicamente coppie di particelle entangled, si usano tecniche ottiche avanzate. In pratica, un fotone può essere diviso in due "fotoni gemelli" che restano collegati tra loro, anche a grande distanza.



In questo processo, un singolo fotone ad alta energia – ad esempio, proveniente da un raggio UV – viene fatto passare attraverso un cristallo non lineare, cioè un materiale con particolari proprietà ottiche. Il cristallo può "scindere" quel fotone in due fotoni di energia inferiore (e quindi con lunghezza d'onda maggiore), che risultano entangled tra loro.

Questi fotoni "gemelli" condividono proprietà correlate, come la **polarizzazione**, in modo tale che la misura su uno influenzi istantaneamente il risultato della misura sull'altro, indipendentemente dalla distanza che li separa. Variando i parametri del processo, i ricercatori possono **controllare le caratteristiche dell'entanglement**, adattandolo agli esperimenti desiderati.

Dopo aver visto come i qubit possano essere strettamente legati tra loro tramite l'entanglement, si può ora passare all'interferenza, che permette di guidare il sistema quantistico verso le soluzioni corrette.

3. Interferenza

L'interferenza è uno dei principi fondamentali del calcolo quantistico. Attraverso operazioni accuratamente progettate, è possibile **rafforzare le soluzioni corrette e attenuare quelle sbagliate**. Questo meccanismo è alla base di molti algoritmi quantistici.

Si immagini di cercare un nome in una rubrica telefonica con 1.000 contatti, senza sapere dove si trovi. Un CC deve sfogliare una voce alla volta: in media serviranno circa $N/2$ tentativi (500). Un CQ, invece, grazie alla sovrapposizione, può esplorare tutte le voci contemporaneamente e usare l'interferenza per aumentare la probabilità di trovare molto più rapidamente quella giusta. Con l'algoritmo di Grover, un CQ può riuscirci in circa $\sqrt{N}$ passi (cioè circa 30).

Non è fantascienza, ma fisica quantistica: è come avere molte persone che cercano insieme e convergono sulla soluzione più probabile.

Più qubit entangled ci sono, più "persone" partecipano alla ricerca simultanea: con 3 qubit si hanno $2^3 = 8$ possibilità attive; con 10 qubit, oltre 1.000; con 20, più di un milione.

Finché il sistema resta in sovrapposizione, tutte queste alternative continuano a "coesistere". Le operazioni quantistiche sono progettate affinché le soluzioni sbagliate si cancellino tra loro (interferenza distruttiva), mentre quelle coerenti con il risultato atteso si rafforzino (interferenza costruttiva).

Alla fine del calcolo, lo stato quantistico si stabilizza (in termini tecnici, "*collassa*") in uno degli stati possibili. Questo avviene nel momento della misura, che costringe il sistema a sceglierne uno, eliminando tutte le altre possibilità.

Non c'è la certezza di ottenere il risultato corretto al primo tentativo, ma l'interferenza quantistica – se opportunamente sfruttata dagli algoritmi – può aumentare in modo significativo la probabilità di ottenerlo. Per questo motivo, i calcoli vengono spesso ripetuti più volte, così da fornire una risposta statisticamente affidabile.

Il calcolo quantistico si basa sull'elaborazione di stringhe di qubit in sovrapposizione, ottenendo un **parallelismo intrinseco** che può accelerare in modo significativo molte elaborazioni complesse.

Anche i CC possono eseguire più operazioni in parallelo (*parallel computing*), utilizzando più processori fisici. I CQ, invece, non moltiplicano le macchine: sfruttano le leggi della fisica per far coesistere molte possibilità nello stesso momento e analizzarle tutte insieme.

Il computer quantistico non è una semplice evoluzione del computer classico

I CQ non sono semplicemente "versioni più veloci" dei CC: si basano su principi diversi e affrontano classi di problemi differenti.

Il CC è efficiente nelle **operazioni deterministiche e sequenziali**, come l'aritmetica di base: basti pensare all'esempio precedente della somma binaria di due numeri, che restituisce sempre lo stesso risultato.

Il CQ, come già accennato, si basa invece su un modello probabilistico, sfruttando sovrapposizione e interferenza per elaborare molte possibilità contemporaneamente. In questo caso, il **risultato non è un valore deterministico, ma un esito statistico**, che emerge solo al momento della misurazione.

Attualmente, i CC resteranno indispensabili per l'uso quotidiano, mentre i CQ saranno preziosi per esplorare spazi di possibilità altrimenti inaccessibili ai CC.

Limiti dei computer quantistici

Il principale ostacolo allo sviluppo dei CQ è la **decoerenza**. I qubit sono molto sensibili all'ambiente circostante: anche un disturbo minimo – come una vibrazione, una variazione di temperatura, un campo elettromagnetico o persino una radiazione cosmica – può far **perdere il loro stato** quantistico e con esso le informazioni.

Proseguendo con la metafora dell'orchestra: dirigere un CQ significa mantenere ogni strumento perfettamente accordato. Basta che uno sia fuori tono perché l'intera sinfonia venga compromessa.

Per evitarlo, i qubit devono essere isolati in condizioni estreme, spesso prossime allo zero assoluto (-273,15 °C), e protetti con schermature sofisticate.

Un altro limite dei CQ attuali è il numero ancora troppo esiguo di qubit disponibili. Per affrontare problemi oggi irrisolvibili persino per i supercomputer, sarà necessario disporre di centinaia di migliaia di qubit **stabili, interconnessi e corretti dagli errori**. Aumentare il numero di qubit rende il sistema più complesso: servono più cablaggi, più controllo, più energia da dissipare. E cresce anche il rischio di interferenze, che peggiora il problema della decoerenza.

I CQ attuali sono ancora dispositivi sperimentali fragili e soggetti a un'alta probabilità di errore. Hanno un numero limitato di qubit e richiedono condizioni operative estremamente delicate.

La ricerca si concentra proprio sul superamento di questi limiti, con l'obiettivo di rendere il calcolo quantistico stabile, affidabile e pronto per applicazioni pratiche.

Ambiti applicativi

Quando i CQ disporranno di qubit stabili, corretti dagli errori e programmabili in modo affidabile, potranno affrontare problemi che oggi risultano proibitivi per i CC, sia per limiti di velocità sia per limiti strutturali.

Di seguito, alcuni ambiti in cui il calcolo quantistico potrà avere un impatto significativo.

1. Simulazioni e ottimizzazione

I CQ sono particolarmente efficaci nel simulare sistemi complessi, grazie alla loro capacità di rappresentare più stati contemporaneamente.

Questa caratteristica li rende particolarmente adatti a campi come la **medicina e la farmacologia**, dove potranno modellare il comportamento molecolare e le interazioni chimiche, accelerando la scoperta di **nuovi farmaci** e lo sviluppo di **terapie personalizzate**.

In **chimica computazionale**, potranno aiutare a comprendere meglio le reazioni chimiche e le proprietà della materia. Nella **scienza dei materiali**, potranno essere impiegati per progettare sostanze con caratteristiche specifiche, come i **superconduttori**, con applicazioni nell'**energia** e nella **mobilità elettrica**.

Anche nella **climatologia**, i CQ potranno contribuire a costruire **modelli atmosferici e oceanici** più accurati, fondamentali per comprendere e affrontare i **cambiamenti climatici**.

Nel campo dell'**ottimizzazione**, i CQ potranno essere usati in settori come logistica, pianificazione urbana, gestione delle risorse energetiche e mobilità intelligente.

Si potranno ottimizzare **reti logistiche**, catene di approvvigionamento e processi industriali complessi.

In **ambito finanziario**, potranno essere impiegati per l'ottimizzazione di portafogli, l'analisi del rischio e il rilevamento delle frodi.

2. Crittografia

I CQ promettono grandi vantaggi, ma pongono anche una sfida: potrebbero mettere in difficoltà alcuni dei sistemi che oggi proteggono le informazioni riservate.

Gli algoritmi di crittografia più diffusi, come RSA[3], si basano su problemi matematici che per i CC richiedono tempi impraticabili, mentre un CQ maturo potrebbe risolverli molto più rapidamente.

Questo è rilevante per dati **sensibili e strategici** (bancari, governativi, sanitari, militari), soprattutto se devono restare segreti per anni. Esiste poi il rischio "*rubare ora, decifrare dopo*": dati cifrati oggi potrebbero essere intercettati e conservati per essere decifrati in futuro, quando i CQ saranno più maturi.

D'altra parte, si stanno sviluppando nuovi metodi di cifratura progettati per resistere anche a questo tipo di attacchi (*post-quantum cryptography*), e si sperimentano tecniche di comunicazione quantistica in grado di segnalare eventuali tentativi di intercettazione, almeno in scenari controllati. Queste tecnologie sono importanti per proteggere i dati di lunga durata.

La transizione sarà graduale, con la coesistenza di sistemi tradizionali e quantistici. Gli utenti comuni potranno limitarsi ad aggiornare i dispositivi, mentre le organizzazioni con esigenze di riservatezza a lungo termine dovranno avviare per tempo il passaggio a metodi più sicuri.

3. Intelligenza Artificiale e Machine Learning

Il calcolo quantistico potrà rafforzare sia il *Machine Learning (ML)*, che analizza grandi quantità di dati per individuare relazioni e formulare previsioni, sia l'*Intelligenza Artificiale Generativa (GenAI)*, come i modelli ChatGPT di OpenAI, capaci di generare nuovi contenuti: testi, immagini, ambienti virtuali o molecole[4]. In alcuni settori specialistici questa integrazione è già in atto. In futuro, si prevede che potrà estendersi anche ad ambiti più generali, accelerando l'addestramento e migliorando l'efficienza dei modelli

Un esempio concreto è lo sviluppo di farmaci: il ML può individuare le caratteristiche delle molecole efficaci, la GenAI può progettare nuove combinazioni, e il calcolo quantistico può simulare il comportamento di vasti spazi molecolari in parallelo.

Questo approccio potrebbe ridurre drasticamente tempi e costi di sviluppo, come evidenziato anche dal **World Economic Forum 2025**[5].

Alcune aziende sono già attive in questo settore. **XtalPi** utilizza algoritmi quantistici per calcolare strutture molecolari e addestrare Intelligenze Artificiali in grado di proporre nuovi composti. **Quantinuum** ha sviluppato un framework di Generative Quantum AI con applicazioni in chimica, finanza e logistica. **Microsoft**, con Azure Quantum Elements, integra Intelligenza Artificiale, calcolo ad alte prestazioni e strumenti quantistici per accelerare la ricerca chimica e la progettazione di nuove molecole.

[3] https://it.wikipedia.org/wiki/RSA_(crittografia)
[4] In ambito **drug discovery** e **material design**, esistono modelli di IA generativa addestrati per generare strutture molecolari chimicamente valide, basati su rappresentazioni standard, grafi molecolari o modelli tridimensionali.
[5] https://www.weforum.org/stories/2025/01/quantum-computing-drug-development/?utm_source=chatgpt.com

Il futuro del calcolo quantistico

Ci vorranno ancora diversi anni prima che il calcolo quantistico trovi applicazioni su larga scala in ambito commerciale.

Nel frattempo, lo sviluppo di nuovi hardware, algoritmi e strategie di correzione degli errori renderà possibile il salto qualitativo e quantitativo atteso. Secondo alcune stime, il cosiddetto "vantaggio quantistico" – ovvero la capacità di superare concretamente i CC nella risoluzione di problemi reali – potrebbe essere raggiunto tra il 2030 e il 2040.

Oggi i CQ sono ancora prototipi fragili, ma in futuro potrebbero diventare strumenti fondamentali per superare barriere che oggi appaiono invalicabili. Non risolveranno ogni problema, ma apriranno nuove strade per affrontare quelli che oggi sembrano insormontabili.

È plausibile che il calcolo quantistico segua un'evoluzione simile a quella della GenAI: una tecnologia concettualmente matura da anni, ma esplosa a livello commerciale e mediatico solo quando l'hardware è divenuto sufficientemente potente, come nel caso di ChatGPT. A tale proposito, si veda il rapporto di McKinsey & Company riportato nei riferimenti.

Quando la tecnologia quantistica riuscirà a superare gli attuali limiti, il suo impatto potrebbe persino superare quello dell'Intelligenza Artificiale.

Per affrontare questa trasformazione servirà un impegno congiunto: nella **formazione**, per preparare nuove competenze; nella **ricerca**, per ampliare i progressi scientifici; e nelle **imprese**, per trasformare queste scoperte in innovazione concreta.

Riferimenti

Questo rapporto di McKinsey & Company offre un'ottima panoramica su come i CQ stiano passando da semplice curiosità scientifica a risorsa aziendale concreta.

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

Per un'introduzione ai concetti basilari della meccanica quantistica dal punto di vista della fisica, della storia e della filosofia, nel contesto in cui si è sviluppata:

Baroni, S. (2024), *La meccanica quantistica. Volume I. La prima rivoluzione quantistica*, Amazon, ISBN 979-8334053281

Un'opera autorevole nel campo: introduce in modo accessibile i principi della meccanica quantistica e dell'informatica, per poi descrivere in dettaglio i CQ e le loro applicazioni. È un ottimo punto di partenza per chi possiede una conoscenza di base di fisica quantistica e informatica:

Nielsen, M.A. e Chuang, I.L. (2010), *Quantum Computation and Quantum Information. 10th Edition*, Cambridge University Press, New York.

Contatti

studio roccato
Data Science Training & Consulting

e-mail: alfredo.roccato[at]fastwebnet.it

www.alfredoroccato.it