CEFRIEL.COM – 23 SETTEMBRE 2025

Quantum Computing: prospettive e sfide tecnologiche per le imprese

di Francesco Villa e Gianluca Ripa

Dalla ricerca alla business innovation: come la computazione quantistica apre scenari inediti per lo sviluppo dell'Intelligenza Artificiale e per le imprese

Negli ultimi anni il termine Quantum Computing è uscito dai laboratori di ricerca ed è entrato nel lessico di aziende e media, attirando l'attenzione non solo dei fisici, ma anche di informatici, ingegneri ed esperti di business. La promessa è chiara: affrontare con nuovi strumenti problemi che i computer tradizionali, anche i supercomputer più potenti, non riescono a gestire in tempi utili.

Gli esempi sono molteplici: una casa automobilistica può simulare nuove leghe leggere per ridurre i consumi senza perdere performance, una banca d'investimento può ottimizzare in tempo reale un portafoglio di migliaia di asset, un'azienda di logistica come quelle della filiera agroalimentare può ridurre i tempi e i costi di distribuzione calcolando rotte ottimali su scala europea, una compagnia farmaceutica può accelerare la scoperta di nuove molecole simulando interazioni chimiche a livello quantistico. In tutti questi casi il limite consiste nella capacità dei computer classici di gestire lo spazio esponenziale di combinazioni richiesto dai calcoli. È qui che il Quantum Computing entra in gioco: sfruttando fenomeni come la sovrapposizione e l'entanglement, apre la possibilità di esplorare simultaneamente scenari che un computer classico deve analizzare uno per uno.

Nel 2019 Google ha dichiarato la cosiddetta "supremazia quantistica", comunicando di essere riuscita a svolgere in pochi minuti col proprio computer quantistico un calcolo che avrebbe richiesto migliaia di anni con il supercomputer più potente di allora. Anche se questa affermazione è stata considerata da alcuni eccessivamente trionfalistica, da quel momento le big tech americane (IBM, Google, Microsoft ecc.) hanno cominciato

a darsi battaglia in ambito mediatico e di ricerca per chi riuscisse a ottenere i migliori risultati in tempi sempre più brevi.

I vantaggi competitivi del Quantum Computing per le aziende

Il vantaggio nell'adozione di questa tecnologia si traduce, per la risoluzione di specifiche classi di problemi, in una potenziale accelerazione esponenziale, aprendo scenari applicativi del tutto nuovi. Infatti, il quantum computing non rende semplicemente più veloci i calcoli attuali; esso apre l'accesso a un modello computazionale completamente nuovo. Non si tratta di accelerare una query su un database, ma di risolvere classi di problemi la cui complessità cresce in modo esponenziale, rendendoli intrattabili per qualsiasi supercomputer classico, presente o futuro.

Per quanto riguarda le aziende, esse ne trarrebbero enormi benefici in diversi ambiti, come ad esempio:

- **Ottimizzazione**: dalla logistica alla finanza, i problemi complessi di ottimizzazione (routing, planning, allocazione risorse, gestione portafoglio) possono trovare soluzioni più veloci ed efficaci.
- **Machine Learning e AI**: gli algoritmi quantistici per il machine learning promettono di elaborare dati in spazi ad alta dimensionalità con efficienza superiore.
- **Chimica e materiali**: la simulazione quantistica permette di modellare reazioni chimiche e proprietà dei materiali in modo molto più preciso, con impatti su farmaceutica, energia e manifattura avanzata.
- **Cybersecurity**: mette in crisi le attuali basi della crittografia classica, ma allo stesso tempo abilita nuovi protocolli intrinsecamente più sicuri.

Di fronte a queste prospettive, il Quantum Computing potrebbe sembrare la soluzione universale a ogni problema computazionale. Tuttavia, per comprenderne le reali potenzialità e limitazioni, è necessario esplorare prima i suoi fondamenti passando dall'informatica tradizionale.

Da bit a qubit: l'evoluzione dei paradigmi computazionali

L’informatica tradizionale si basa sul concetto di bit (binary digit), l’unità fondamentale dell’informazione digitale. Un bit può assumere esclusivamente due valori: 0 o 1, che corrispondono fisicamente a due stati elettrici distinti in un circuito. Nel caso più semplice, possiamo pensare al bit come a un interruttore: quando è “aperto” (nessuna corrente passa) rappresenta lo 0, quando è “chiuso” (la corrente passa) rappresenta l’1.

Nei circuiti integrati moderni, questi stati sono rappresentati da diversi livelli di tensione e i transistor, che fungono da interruttori controllati elettronicamente, permettono di manipolare questi stati in modo estremamente rapido e preciso. Sopra questo concetto fondamentale è stato possibile costruire delle porte logiche, circuiti elettronici in grado di effettuare operazioni logiche sui bit (NOT, AND, OR, XOR ecc.). Combinando queste porte logiche si creano circuiti più complessi fino alla realizzazione dei computer che conosciamo oggi.

Il Quantum Computing si discosta in modo radicale da questa concezione di “stato binario” dell’informazione, introducendo il concetto di qubit (quantum bit). A differenza del bit classico, un qubit non si trova necessariamente in una condizione definita (0 o 1), ma può esistere in una sovrapposizione di entrambi gli stati simultaneamente. Questa sovrapposizione significa che, finché non viene effettuata una misura, il qubit contiene potenzialmente tutte le informazioni relative ad entrambi gli stati. È importante sottolineare che non si tratta semplicemente di un valore intermedio tra 0 e 1, ma di una condizione diversa in cui il sistema esiste letteralmente in entrambi gli stati contemporaneamente. Quando si effettua una misura, si dice che lo stato “collassa”, passando dalla sovrapposizione a un valore determinato (0 o 1 per i qbit).

L’ultimo concetto fondamentale per comprendere il potere del Quantum Computing è l’entanglement, un fenomeno che esiste solamente nella meccanica quantistica e che non trova una traduzione esatta in italiano. Questo fenomeno si verifica quando due o più stati quantistici interagiscono in modo da formare un sistema correlato, diventando indissolubilmente legati. La caratteristica sorprendente dell’entanglement è che, una volta che due particelle (o qubit) sono entangled, la misura effettuata su una di esse

influenza istantaneamente lo stato dell'altra, indipendentemente dalla distanza che le separa. Se misuriamo il primo qubit e otteniamo il valore 0, l'altro qubit collegato rivelerà immediatamente un valore correlato, "rompendo" l'entanglement e manifestando la propria informazione binaria.

Questi appena introdotti possono sembrare dei concetti complicati e ci si può chiedere cosa c'entrino sovrapposizione ed entanglement con l'informatica. Il motivo in realtà è semplice, perché questo nuovo modo di concepire l'informazione ha reso possibile la realizzazione di nuove porte logiche quantistiche (come la porta CNOT, Hadamard, Pauli-X ecc.) che stanno alla base dei processori quantistici. Queste porte manipolano i qubit sfruttando le proprietà quantistiche della materia, implementate attraverso diverse tecnologie: circuiti superconduttori, ioni intrappolati, fotoni, o atomi ultra-freddi.

Grazie all'intrinseca capacità dei qubit di esistere in sovrapposizione e all'entanglement che permette di correlare multiple informazioni simultaneamente, un processore quantistico può processare enormi quantità di dati in parallelo. Mentre un computer classico con n bit può rappresentare uno solo dei 2^n possibili stati alla volta, un computer quantistico con n qubit può rappresentare tutti i 2^n stati contemporaneamente durante il calcolo. Tuttavia, è importante sottolineare che non tutti i problemi computazionali beneficiano di questo approccio: il quantum computing eccelle in specifiche categorie di calcoli, mentre per molte applicazioni quotidiane i computer classici rimangono più efficienti ed economici.

Stato attuale e prospettive strategiche per le aziende

Ad oggi non abbiamo ancora raggiunto una piena maturità relativamente a questa tecnologia. I quantum computer disponibili operano con poche centinaia di qubit fisici e sono ancora soggetti a limiti rilevanti, dovuti alla fragilità degli stati quantistici (de-coerenza). Inoltre, molti algoritmi devono ancora essere ripensati per adattarsi a questo nuovo paradigma. Nonostante ciò, big tech e start-up specializzate stanno già offrendo accesso cloud a hardware quantistico reale, aprendo le porte alla sperimentazione sia accademica che privata.

In conclusione, per un CxO oggi il Quantum Computing non è ancora un tema tecnologico, ma di visione. Può essere lungimirante dedicare qualche attenzione adesso

al tema per comprendere quali problemi rilevanti potranno essere risolti tra alcuni anni e per essere attenti a cogliere per tempo le opportunità che si prospetteranno, considerando anche che il talento in questo campo è ancora estremamente scarso. Avviare ora iniziative anche molto piccole, permette di iniziare ad attrarre e formare le competenze necessarie, creare partnership con l'ecosistema italiano ed europeo e posizionare l'azienda come un innovatore, con benefici anche in altri ambiti tecnologici di impatto più immediato.