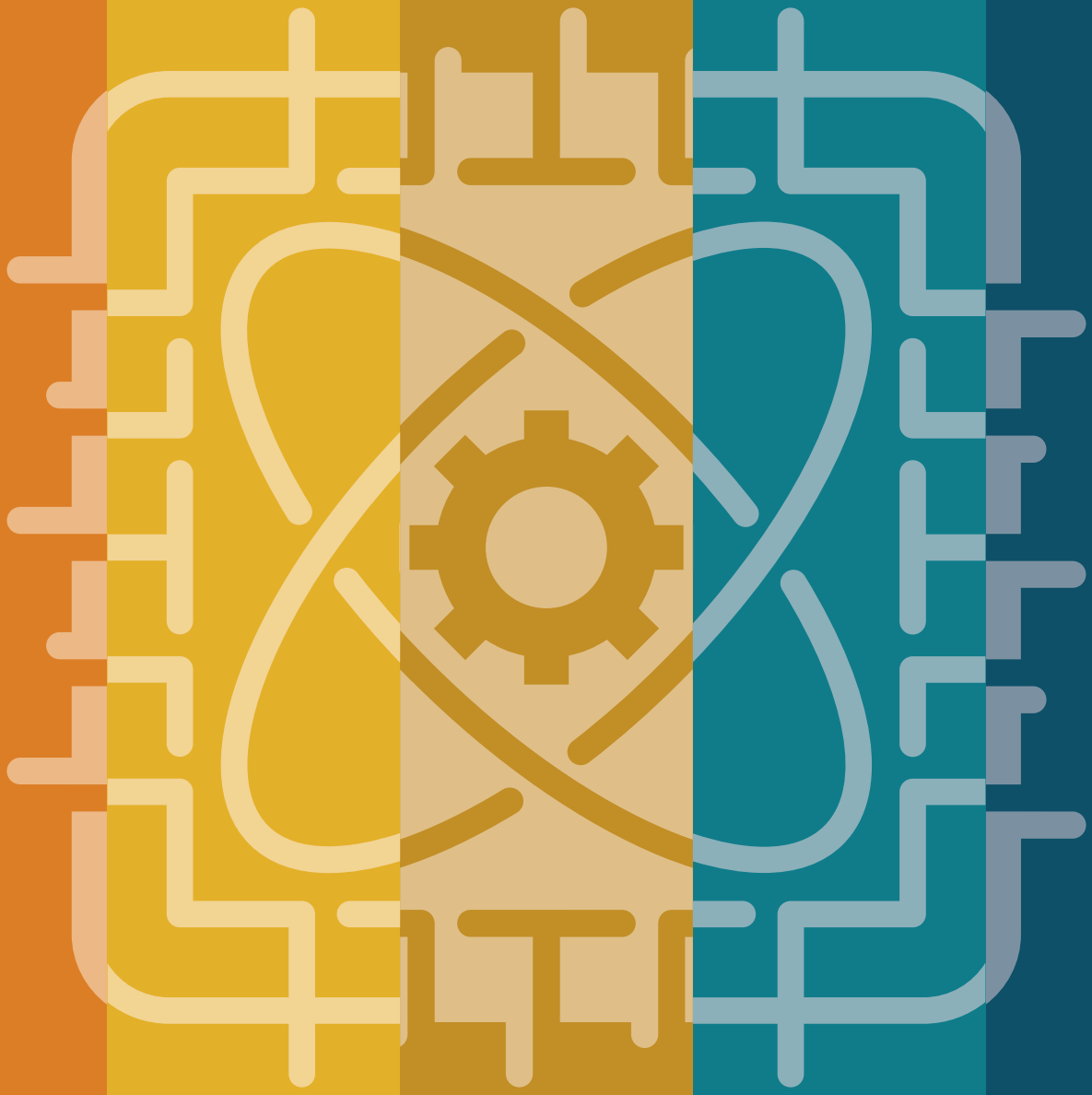
REGIONE PUGLIA

·a·r·t·i·
Agenzia regionale
per la tecnologia
e l'innovazione

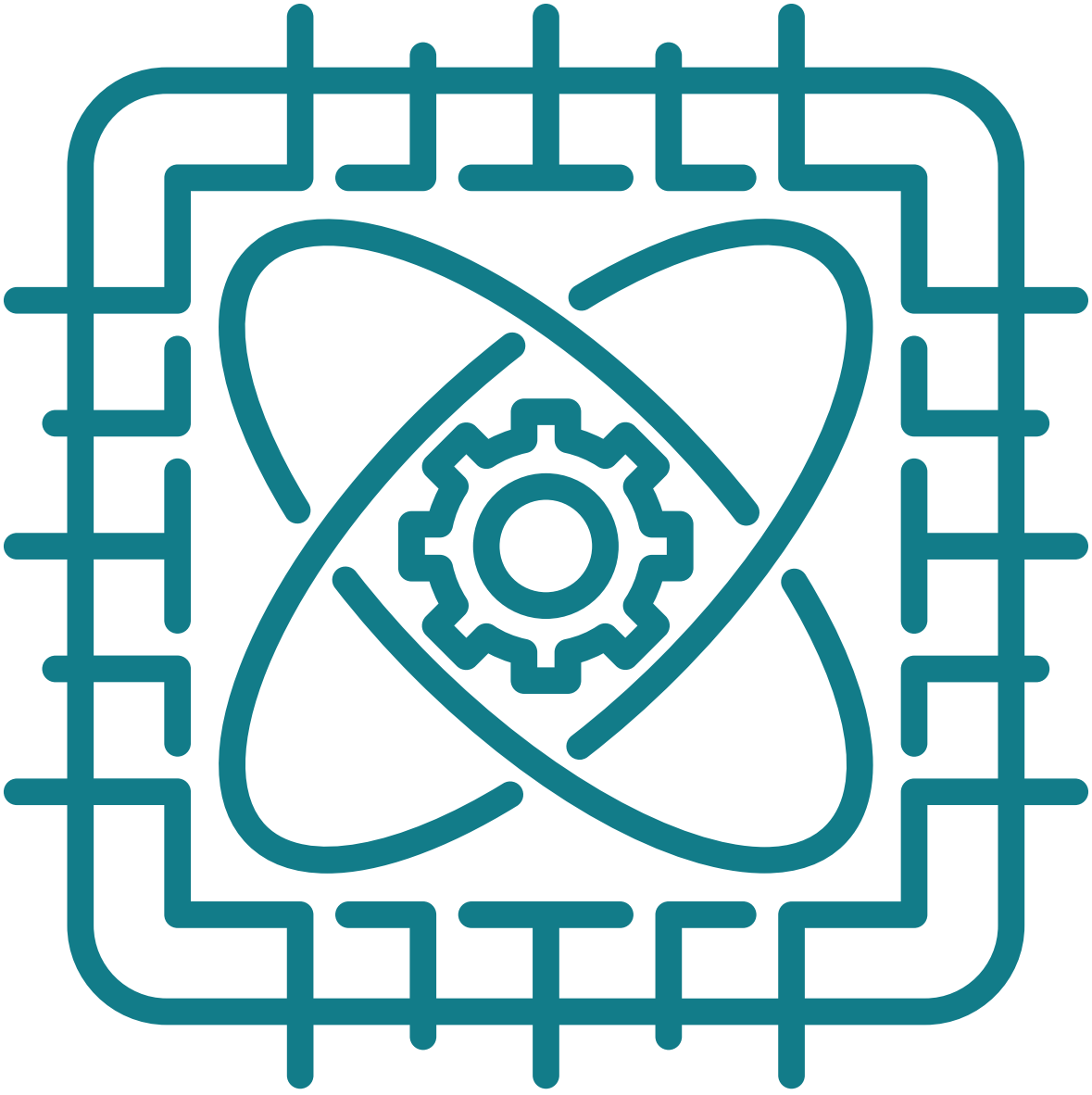


Technology Focus Report

TECNOLOGIE QUANTISTICHE

REGIONE PUGLIA

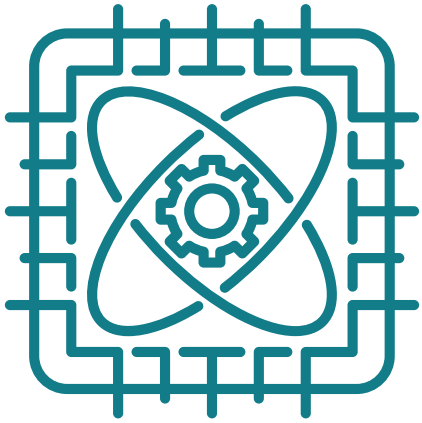
·a·r·t·i·
Agenzia regionale
per la tecnologia
e l'innovazione



Technology Focus Report

TECNOLOGIE QUANTISTICHE

SOMMARIO



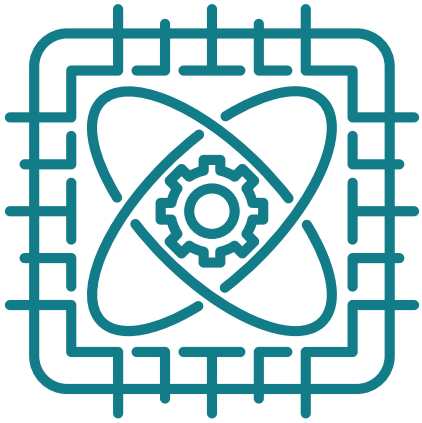
1. INTRODUZIONE

ARTI, l'Agenzia Regionale per la Tecnologia e l'Innovazione della Puglia, opera da tempo come osservatorio delle dinamiche innovative regionali, proponendo analisi, studi e raccolte di dati statistici che, oltre a fotografare lo stato di salute delle filiere regionali dell'innovazione, ne individuano le problematiche e ne delineano i possibili sviluppi futuri. Con questo primo "Technology Focus Report", l'Agenzia intende affiancare alle sue tradizionali indagini sul fronte della domanda di innovazione una serie di snelli rapporti tecnici che raccontino lo stato dell'arte e le opportunità generate dall'offerta di nuove tecnologie, con una particolare attenzione a quelle posizionate sulla frontiera dello sviluppo tecnologico.

Il tema scelto per questo rapporto è quello della nuova generazione di tecnologie per il calcolo, la sensoristica e la comunicazione che fondano i propri principi di funzionamento sulle proprietà quantistiche della materia. Si tratta di un tema piuttosto "caldo", che sempre più spesso cattura l'interesse dei media di larga diffusione, soprattutto a riguardo del *quantum computing*, registrando e suscitando reazioni che oscillano dal grande entusiasmo per le potenzialità di una tecnologia percepita come assolutamente *"disruptive"* allo scetticismo per l'attuale carenza di esempi di applicazioni industriali concrete.

Come spesso accade, la verità sta un po' nel mezzo: se infatti è vero che alcune tecnologie di base per il calcolo quantistico hanno bisogno ancora di almeno un decennio per poter passare dalla fase di sperimentazione a quella di applicazione su larga scala, è anche vero che il raggiungimento di quel traguardo rappresenterà una vera e propria rivoluzione in molti ambiti vitali della nostra economia e società, in primis nella sanità, nella finanza e nella sicurezza dei dati. Le tecnologie quantistiche non si limitano in ogni caso al solo calcolo quantistico e nell'ambito della sensoristica e della comunicazione quantistiche sono attesi impatti altrettanto rilevanti e in un orizzonte temporale molto più breve.

In questo breve rapporto, pensato per offrire a un lettore non specialista un quadro il più possibile completo ma al contempo accessibile al mondo delle tecnologie quantistiche, ci proponiamo di rispondere, in maniera sperabilmente chiara, a tre domande di fondo: Cosa sono le tecnologie quantistiche? Quali sono i loro ambiti di applicazione? Perché sono importanti anche per le imprese della nostra regione? Il rapporto si apre con un breve sommario dei contenuti chiave del report e si chiude con un glossario e una serie di suggerimenti di lettura per chi volesse ulteriormente documentarsi e approfondire i temi trattati, una bibliografia assolutamente incompleta e parziale vista la vastità dell'argomento e l'enorme quantità di materiali disponibili in rete.



2. EXECUTIVE SUMMARY

Quando la materia è osservata a scala molto piccola, ad esempio quella degli atomi o delle particelle elementari, manifesta proprietà che alla scala macroscopica della nostra vita quotidiana non sono percepibili e che spesso risultano spiazzanti e controintuitive. Siamo ad esempio abituati all'idea che le quantità fisiche varino con continuità, mentre a scala microscopica succede che quantità come l'energia o il campo elettromagnetico variano in maniera discreta, per multipli di un'unità di base: nel gergo della fisica si dice che esse sono quantizzate.

Anche il concetto ordinario di conoscibilità viene messo in discussione: se nel mondo fisico classico la limitata esattezza con cui possiamo osservare e misurare un certo fenomeno è solo legata all'imprecisione dei nostri strumenti di misura, nel mondo quantistico questa ignoranza ha uno statuto più fondamentale. Non è ad esempio possibile conoscere con esattezza entrambe le quantità di una coppia di grandezze associate, ad esempio la posizione e la velocità di una particella: se ne determiniamo con esattezza una, dobbiamo accettare un certo grado di indeterminazione per l'altra. Di più, non è proprio possibile "osservare" un sistema quantistico senza disturbarlo e dunque modificarne al tempo stesso lo stato. È come se, prima della misura, un sistema quantistico fosse in uno stato indeterminato, di cui possiamo solo dare una descrizione probabilistica, in termini di sovrapposizione, con una certa distribuzione di probabilità, di tutti i possibili stati che esso può assumere.

Queste proprietà, insieme alla possibilità di "gemellare" due sistemi quantistici, ad esempio una coppia di elettroni o di fotoni, in modo che lo stato di un membro della coppia determini automaticamente lo stato dell'altro membro (un fenomeno detto entanglement), sono alla base delle tecnologie quantistiche, siano esse quelle del calcolo, della sensoristica o della comunicazione. Si tratta di tecnologie che condividono in larga parte principi operativi e problematiche realizzative e che promettono un grande salto in avanti in termini di velocità, precisione e sicurezza delle applicazioni e la possibilità di implementare applicazioni che sono semplicemente irrealizzabili con i sistemi classici.

Il settore probabilmente più noto è quello dell'**informatica quantistica** che è stata testimone di significativi progressi negli ultimi anni, pur restando ancora in piedi importanti sfide tecnologiche per la sua penetrazione di mercato, tra cui la riduzione di peso, ingombro e costi, il miglioramento dell'affidabilità dei componenti hardware, lo sviluppo di architetture di calcolo scalabili e tolleranti ai guasti e la creazione di tecniche pratiche di correzione degli errori. I ricercatori continuano per questo a esplorare nuovi materiali, tecniche e algoritmi e giganti tecnologici come IBM, Microsoft e Google, oltre a numerose startup, continuano a investire molto nella ricerca, alimentando un rapido progresso nel campo.

Sono oggi operativi diversi computer quantistici, spesso allocati presso centri di calcolo ad alte prestazioni e funzionanti in modalità ibrida, accoppiati a supercalcolatori tradizionali, in grado di risolvere problemi specifici molto complessi, grazie ad architetture ad hoc specializzate nell'esecuzione di particolari algoritmi. I progressi sono in ogni caso costanti e già nei prossimi 4 o 5 anni si stima sarà possibile impiegare questi sistemi per risolvere problemi anche di natura commerciale, inattaccabili dai computer classici, sia per ragioni di velocità che di più fondamentale impossibilità.

Gli ambiti in cui si sta concentrando lo sforzo di messa a punto di casi d'uso e che con maggiore probabilità saranno impattati dal computing quantistico sono la salute, la sicurezza informatica e la finanza, con sviluppi interessanti anche in ambito manifatturiero (aerospazio e automotive in particolare), energetico e logistico. Nel mondo privato, le prime industrie a puntare e investire sul calcolo quantistico saranno quelle che necessitano di immense potenze di calcolo come quelle chimiche o farmaceutiche, che potranno accorciare sensibilmente i tempi necessari per individuare nuovi farmaci e sostanze chimiche. La disponibilità di sistemi quantistici di calcolo più versatili permetterà di risolvere problemi di più vasto interesse commerciale, per esempio legati a problemi di ottimizzazione, allargando il loro impiego all'aerospazio, all'automotive e alla finanza.

Ci vorranno comunque ancora molti anni prima che queste applicazioni si possano affermare a livello commerciale, anni in cui lo sviluppo di hardware sempre più efficiente e affidabile e di nuove tecniche algoritmiche permetteranno l'atteso salto qualitativo e quantitativo: alcune stime danno il raggiungimento del cosiddetto "vantaggio quantistico", per cui i computer quantistici diverrebbero più veloci dei computer classici nella risoluzione di una vasta gamma di problemi reali di grande rilevanza, tra il 2030 e il 2040, l'incertezza essendo dovuta alla molteplicità di approcci e tecnologie che centri di ricerca e grandi aziende stanno perseguendo.

Si prospetta dunque un percorso molto graduale di adozione di questa tecnologia, che certamente presenterà i suoi alti e bassi e sarà presumibilmente ricco di sorprese e, possibilmente, di brusche accelerazioni legate alla messa a punto di piattaforme hardware più economiche ed efficienti e di nuovi algoritmi.

Se dunque la diffusione commerciale del *quantum computing* propriamente detto (computer quantistico di uso generale, programmabile e scalabile) si proietta su un orizzonte temporale almeno decennale, le tecnologie quantistiche per la sensoristica e la comunicazione sono invece molto più prossime al mercato, in particolare alcune tipologie di sensori, quali quelli magnetici, i sistemi di crittografia post-quantistica e le reti di comunicazione quantistica.

Quello che nel calcolo quantistico rappresenta infatti un problema e una sfida tecnologica, la grande sensibilità dei componenti hardware quantistici ai disturbi esterni, è proprio ciò che viene sfruttato per costruire **sensori quantistici** estremamente sensibili a stimoli esterni quali il movimento, il campo magnetico e la gravità. Oltre a un'estrema sensibilità e precisione, i sensori quantistici permettono misure non invasive senza contatto con tempi di risposta molto rapidi e consentono di rilevare e misurare le più piccole variazioni di tempo, gravità, temperatura, pressione, rotazione, accelerazione, frequenza e campi magnetici ed elettrici. A questi si aggiungono i sensori per il *quantum imaging*, che sfruttano le proprietà quantistiche della luce per realizzare sistemi di acquisizione di immagini caratterizzati da elevatissima sensibilità e risoluzione spaziale e spettrale.

Allo stato attuale dello sviluppo, caratterizzato da sistemi di grande peso, ingombro e soprattutto costo, la parte preponderante dei casi d'uso dei sensori quantistici è stata sviluppata per il settore della difesa/aerospazio e per industrie e applicazioni caratterizzati da produzioni massive, come l'elettronica, o da alte priorità in termini di prestazioni e bassa sensibilità ai costi unitari dei sistemi sensore, come l'industria

della salute e farmaceutica e il settore delle prospezioni geologiche ed energetiche.

Tra le tipologie di sensori quantistici maggiormente adatte ad applicazioni di larga diffusione troviamo i sensori di campo magnetico, applicabili nell'industria automotive e nei dispositivi indossabili, e gli orologi atomici, che permettono un livello di accuratezza dell'ordine dei nanosecondi, 3 ordini di grandezza superiore a quello possibile con gli oscillatori a cristalli di quarzo utilizzati nei nostri dispositivi digitali. La combinazione di orologi atomici e giroscopi o accelerometri quantistici può infatti fornire capacità di navigazione di precisione, anche in ambienti privi di copertura GPS, con importanti applicazioni nel campo dei veicoli a guida autonoma, nello spazio, nell'industria e nella difesa, oltre che in ambito scientifico.

La progressiva riduzione di dimensioni e costo dei sensori permetterà l'allargamento delle applicazioni sopra elencate ad altri ambiti, quali il monitoraggio di infrastrutture quali strade, dighe o impianti industriali e la navigazione autonoma nell'industria automotive. Da sottolineare anche che i sensori quantistici avranno un ruolo fondamentale anche per le applicazioni trasversali del computing quantistico e della **comunicazione quantistica**.

Quest'ultimo ambito vede la concentrazione di notevoli investimenti in ricerca anche da parte di operatori privati e raggruppa un insieme di tecniche e applicazioni finalizzate ad aumentare la sicurezza dello scambio dei dati, vero tallone d'Achille delle moderne comunicazioni informatiche. Un pilastro fondamentale della comunicazione quantistica è infatti rappresentato dalle tecniche di crittografia quantistica, a cui si accompagnano quelle di generazione di numeri "realmente" casuali e tutte quelle altre tecnologie in fase di sviluppo, come i ripetitori quantistici, finalizzate alla realizzazione di un vero e proprio Internet Quantistico, una rete di reti quantistiche che si affiancherebbe al classico Internet per fornire servizi di comunicazione quantistiche a organizzazioni particolarmente sensibili alla sicurezza dei dati, oltre che per connettere tra loro i computer quantistici presenti su cloud.

Se la sfida tecnologica sul *quantum computing* si gioca principalmente tra i colossi dell'informatica e poche aziende high-tech, ben più ampio è lo spazio di opportunità negli ambiti del *quantum sensing e communication*, che peraltro offrono allo stato attuale le maggiori opportunità di mercato. Questo dato è tanto più significativo per un Paese come l'Italia che, se non dispone degli asset necessari per giocare un ruolo significativo nello sviluppo dell'hardware di calcolo quantistico, è invece ben posizionata, per competenze scientifiche e tecnologiche e capacità industriali, per giocarlo sulla sensoristica e la comunicazione quantistiche, oltre che nello sviluppo di software quantistico.

Sono questi ultimi ambiti che presentano interessanti opportunità di investimento anche per **imprese di piccola e media dimensione**, ad esempio nell'integrazione di sensoristica quantistica in sistemi per applicazioni biomedicali, aerospaziali o di altra natura, nello sviluppo dell'elettronica di controllo e processamento del segnale, nello sviluppo del software di elaborazione dei dati, eccetera. Tenendo anche conto del fatto che per una decina d'anni i sistemi più diffusi saranno di natura ibrida classico-quantistica, è infatti evidente come ci sia ampio spazio per attività di innovazione tecnologica che si svolgano a ridosso della quantistica, senza per questo necessariamente coinvolgere sviluppi nelle tecnologie quantistiche propriamente dette. Per collocarsi con successo in questa filiera è comunque fondamentale che le imprese imparino a parlare il linguaggio delle tecnologie quantistiche, a comprenderne il funzionamento e le problematiche.

Considerando un orizzonte un po' più lungo, è molto probabile che per il calcolo quantistico succederà quello che è successo per l'intelligenza artificiale di tipo generativo, una tecnologia le cui basi scientifiche e concettuali erano mature già da molti anni ma che ha avuto una vera e propria esplosione di mercato e di attenzione pubblica con l'avvento di ChatGPT e di piattaforme analoghe, rese possibili dagli avanzamenti tecnologici dell'hardware di calcolo. Quando l'hardware quantistico raggiungerà un sufficiente livello di

maturità assisteremo infatti a un cambio radicale di paradigma, paragonabile per molti versi a quello dell'IA ma ancora più dirompente, rispetto al quale è bene che il sistema della formazione, il mondo della ricerca e quello delle imprese si facciano trovare preparati.

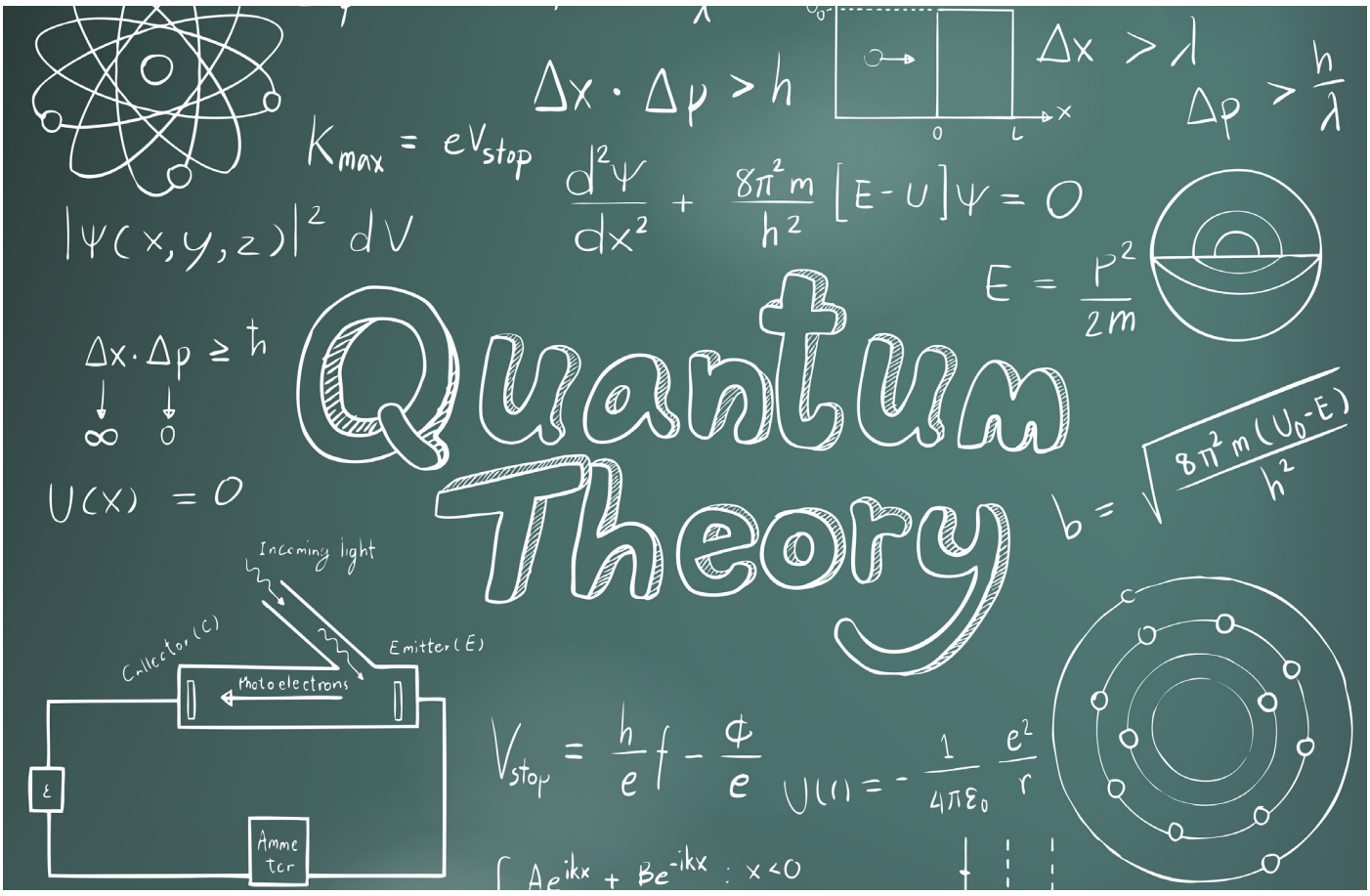
Si tratta di una sfida rilevante anche per la nostra **Puglia**: vi sono infatti ambiti applicativi delle tecnologie quantistiche o ibride classico-quantistiche che possono impattare in maniera rilevante gran parte delle filiere regionali a più alta intensità tecnologica, a cominciare da aerospazio, automotive, meccatronica, servizi avanzati, industria della salute, dell'energia e dell'ambiente. Pensiamo ad esempio alla simulazione di sistemi complessi, all'apprendimento automatico, alla guida autonoma, al monitoraggio ambientale, alla diagnostica per immagini, alla sicurezza informatica e a molte altre applicazioni che possono trarre vantaggio dalle più elevate performance offerte dalle nuove tecnologie quantistiche.

Per poter sfruttare appieno le opportunità offerte dalle tecnologie quantistiche è certamente necessaria la creazione di un **"ecosistema quantistico"**, in cui sapere scientifico, ricerca industriale, formazione delle competenze e politiche pubbliche di sostegno collaborino in maniera strategica. In Puglia esistono le condizioni di base perché questo possa avvenire, a partire dalle competenze del sistema universitario regionale e dalle progettualità di grande respiro in cui esso è correntemente impegnato e dall'articolato sistema di incentivi alla ricerca e all'innovazione messo a disposizione dalla Regione Puglia: occorre partire di qui per costruire una prospettiva credibile di sviluppo che collochi la regione in una posizione ottimale per intercettare le opportunità che si andranno a delineare in un futuro ormai prossimo.

3. COSA SONO LE TECNOLOGIE QUANTISTICHE?

3.1 LA MECCANICA QUANTISTICA APPLICATA

Per tecnologie quantistiche si intendono tutte quelle tecnologie che si fondano sullo sfruttamento delle proprietà quantistiche della materia. Per certi versi non si tratta di nulla di completamente nuovo: molti dei dispositivi oggi di uso corrente, dai semiconduttori con cui sono realizzati i chip dei nostri computer e cellulari, ai laser, alle lampadine LED, ai sistemi medicali di risonanza magnetica, sono stati sviluppati grazie a una profonda conoscenza della meccanica quantistica, una teoria che ha preso corpo nei primi anni del secolo passato e che ha visto tra i suoi pionieri fisici come Plank, Einstein, Bohr, Heisenberg e Schrödinger.



In tutti i casi citati, la meccanica quantistica ha fornito una chiara interpretazione delle "strane" proprietà che esibiscono i sistemi fisici quando sono indagati a scala atomica e subatomica. Siamo ad esempio abituati a pensare che le grandezze fisiche varino in maniera continua, cosa che invece non succede a scala microscopica, dove quantità come l'energia o il campo elettromagnetico variano invece in maniera discreta, "per salti". Lo stesso termine **"quanto"** si riferisce a una quantità che non è ulteriormente divisibile: ad esempio all'elettrone è associato il quanto di elettricità, ovvero la più piccola quantità possibile di carica elettrica, che non è possibile dividere ulteriormente.

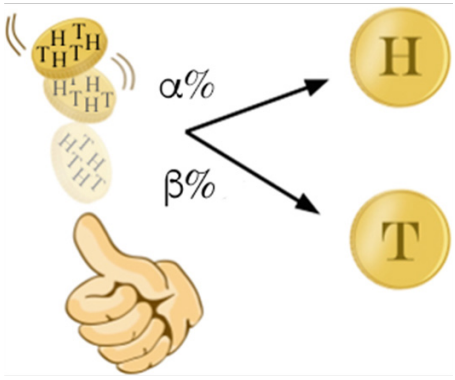
Allo stesso modo il fotone è il quanto del campo elettromagnetico e dunque della luce, che per inciso la fisica classica considera come un fenomeno di tipo puramente ondulatorio mentre è intrinsecamente caratterizzata dal **dualismo onda-particella**. Lo stesso termine di particella "elementare" con cui designiamo ad esempio sia l'elettrone che il fotone (ma anche altre particelle come i neutrini e i quark di cui sono fatti i protoni e i neutroni del nucleo atomico) si riferisce alla loro indivisibilità.

BOX 1: Il fenomeno della sovrapposizione

Supponiamo di lanciare una monetina in aria, per poi farla ricadere sul palmo della mano. Una volta caduta in mano, il suo valore o "stato" sarà testa o croce, ma mentre volteggia in aria il suo stato è per noi non definito, possiamo dire che è in una sovrapposizione degli stati testa e croce. L'atterrare della monetina sulla mano rappresenta la "misura" del suo stato, un processo che distrugge la sovrapposizione (in meccanica quantistica si direbbe che dopo la misura lo stato della monetina "collassa" in uno dei due valori possibili, testa o croce).

La monetina è un oggetto classico e volendo noi potremmo filmare le sue evoluzioni nell'aria e in ogni momento sapere quale delle due facce (stati) mostra da un certo angolo visuale: con questo artificio potremmo ovviare alla nostra ignoranza sul suo stato di sovrapposizione mentre è in aria.

Una monetina quantistica (ad esempio un elettrone) permarrebbe invece in uno stato di sovrapposizione tra i due stati testa e croce di cui per definizione non possiamo sapere nulla: qualsiasi tentativo di "spiare" in esso porterebbe al suo collasso in uno dei due esiti possibili: testa o croce. Il massimo che possiamo arrivare a conoscere è la probabilità dei due esiti, la nostra ignoranza sullo stato di sovrapposizione è in questo caso di tipo fondamentale, legata alla natura stessa della realtà fisica: in esso la monetina è contemporaneamente sia testa che croce.



Una Q-monetina è in uno stato di sovrapposizione fino a che il suo lancio non si conclude con la lettura del valore testa oppure croce, ciascuno possibile con una certa probabilità

Fonte: Adattato da *Quantum Computing for the Quantum Curious*, Springer.com

La fisica quantistica mette in discussione molte nostre assunzioni sulla natura della realtà, che ci derivano dalla nostra concreta esperienza di vita in un mondo "classico", costituito da oggetti di dimensioni incomparabilmente maggiori di quelle degli atomi e delle particelle. Tra queste l'idea stessa della conoscibilità di un sistema fisico: se infatti nella fisica classica la limitata esattezza con cui possiamo osservare e misurare un certo fenomeno è solo legata all'imprecisione dei nostri strumenti di misura, nel mondo quantistico questa ignoranza ha uno statuto di tipo fondamentale. Non è ad esempio possibile conoscere con esattezza entrambe le quantità di una coppia di grandezze associate, ad esempio la posizione e la velocità di una particella: se ne determiniamo con esattezza una, dobbiamo accettare un certo grado di indeterminazione per l'altra, come postula il **principio di indeterminazione** di Heisenberg.

Di più, non è proprio possibile "osservare" un sistema quantistico senza disturbarlo e dunque modificarne al tempo stesso lo stato. Per misurare ad esempio la velocità o la posizione di un elettrone lo dobbiamo in qualche modo "illuminare", cioè colpirlo con un fotone, che inevitabilmente gli trasmetterà parte della sua energia, modificandone lo stato. Quello che andiamo dunque a rilevare è lo stato dell'elettrone dopo la misura. Cosa possiamo allora dire dello stato di un sistema quantistico prima della misura? La nostra intuizione ci porterebbe a ritenere che esso sia definito ma che noi lo ignoriamo, il fatto è che questa ignoranza è, ancora una volta, di tipo fondamentale. È come se, prima della misura, un sistema quantistico fosse in uno stato indeterminato, di cui possiamo solo dare una descrizione probabilistica, in termini di **sovrapposizione**, con una certa distribuzione di probabilità, di tutti i possibili stati che esso può assumere dopo la misura.

Un altro fenomeno estraneo al mondo classico è quello dell'**entanglement**, una forma molto peculiare di correlazione in cui due particelle si legano in modo che lo stato di una di esse sia sempre "intrecciato" a quello dell'altra, una condizione che permane anche laddove le due particelle dovessero essere separate da grandi distanze. L'aspetto più singolare è quello per cui, date due particelle *entangled* separate nello spazio di cui non conosciamo lo stato, se andiamo ad effettuare una misura su una di esse, distruggendo lo stato di sovrapposizione in cui si trova e portandola nello stato misurato, allora anche l'altra particella ad essa entangled "collasserà" nello stato correlato, automaticamente e nello stesso istante: è come se due oggetti distanti e non interagenti potessero influenzarsi a distanza.

Queste proprietà sono alla base delle nuove tecnologie quantistiche, siano esse quelle del calcolo, della sensoristica o della comunicazione, caratterizzate dal fatto che, a differenza di quella di prima generazione, sono in grado di controllare in maniera molto fine gli stati quantistici di singoli atomi, molecole o particelle. Si tratta di tecnologie che condividono in larga parte principi operativi e problematiche realizzative e che promettono un grande salto in avanti in termini di velocità, precisione e sicurezza delle applicazioni e la possibilità di implementare applicazioni che sono semplicemente irrealizzabili con i sistemi classici.

BOX 2: Il fenomeno dell'entanglement

Supponiamo adesso di lanciare contemporaneamente in aria due monetine A e B, gli esiti possibili saranno quattro: testaA-testaB, testaA-croceB, croceA-testaB e croceA-croceB.

Questo significa che le evoluzioni nell'aria delle due monetine sono completamente indipendenti l'una dall'altra. Dopo un numero molto elevato di lanci avremmo la stessa distribuzione di probabilità tra i quattro possibili esiti (25% ciascuna se le monetine non sono truccate), sia lanciando le due monetine

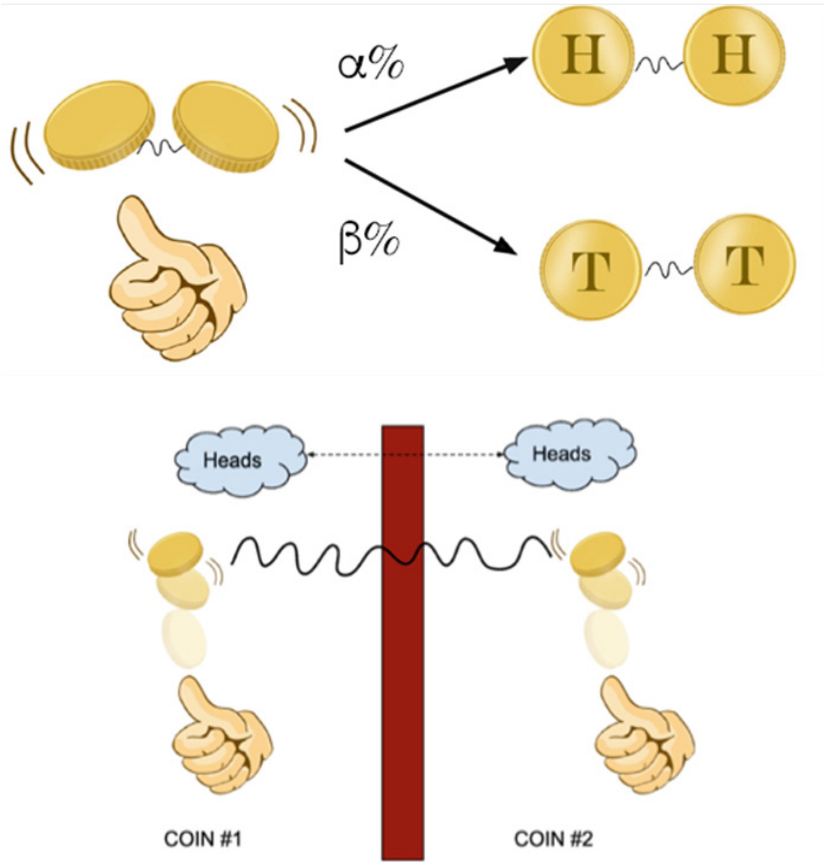
contemporaneamente che separatamente una dopo l'altra.

A una coppia di monetine quantistiche (chiamiamole Q-monetine) potrebbe invece succedere di "intrecciare" (*to entangle*) i propri destini, in modo tale che il comportamento di una delle due Q-monetine sia sempre correlato a quello dell'altra. In questo caso, l'esito del lancio non è più indipendente per le due Q-monetine: se ottengo "testa" per la Q-monetina A potrei per esempio sapere con certezza che lo stesso esito è valido per la Q-monetina B, idem per "croce": le due Q-monetine sono "entangled".

Per quanto possa cozzare contro il nostro senso comune (costruito sulla base della nostra esperienza in un mondo classico, in cui gli effetti quantistici non sono direttamente osservabili), l'entanglement è una forma di correlazione tra sistemi quantistici (ad esempio elettroni o fotoni) che permane anche quando questi sono separati da migliaia di chilometri. Se ad esempio le due Q-monetine fossero lanciate contemporaneamente in due luoghi diversi, i due esiti sarebbero sempre e comunque correlati: il lanciatore della prima monetina saprebbe automaticamente cosa è successo all'altra monetina.

Il "lancio" della monetina del nostro esempio corrisponde alla lettura dello stato del sistema quantistico in questione.

L'esito del lancio di due Q-monetine entangled è sempre correlato, anche se effettuato a distanza



Fonte: Adattato da *Quantum Computing for the Quantum Curious,* Springer.com

3.2 IL CALCOLO QUANTISTICO

Bit classici e bit quantistici

Sappiamo tutti che nei computer classici le informazioni sono rappresentate in forma binaria, come sequenze di cifre che possono assumere solo due valori, 1 o 0. Ciascuna di queste cifre è un "bit" di informazione e se vogliamo rappresentare quantità che possono assumere più di due valori dobbiamo usare sequenze di più bit. Ad esempio, per rappresentare 256 valori abbiamo bisogno di 8 bit (28=256).

Una stringa di bit può essere usata per codificare sia valori strettamente numerici che informazioni di altro tipo, ad esempio lettere dell'alfabeto in un programma di scrittura. In un computer classico le informazioni binarie vengono memorizzate in appositi dispositivi elettronici in grado di assumere due diversi valori di tensione o corrente in corrispondenza dei valori 1 e 0, sia in forma temporanea nei passaggi intermedi (le memorie RAM e i registri interni del computer) che in maniera più o meno permanente per i dati in uscita (ad esempio il disco rigido).

Queste stringhe di bit vengono elaborate attraverso operazioni logiche che combinano in maniera opportuna due o più valori in ingresso per generare un valore di uscita. Queste operazioni si basano su un insieme di operatori logici elementari, anche detti "porte logiche" (AND, OR, NOT e loro combinazioni), implementati da circuiti elettronici digitali e organizzati in reti complesse. La potenza dei moderni elaboratori digitali sta tutta nella velocità con cui vengono eseguite queste operazioni logiche e nella grande dimensione delle loro memorie, frutto della miniaturizzazione e velocizzazione dei circuiti microelettronici che ne sono i costituenti di base.

Torniamo al nostro esempio della monetina. Una monetina classica può assumere due valori digitali, possiamo ad esempio associare 1 a "testa" e 0 a "croce". Così, per rappresentare ad esempio 8 diversi valori abbiamo bisogno di tre monetine, come illustrato nella seguente tabella.

Monetina A	Monetina B	Monetina C	**Valore**
0	0	0	**0**
0	0	1	**1**
0	1	0	**2**
0	1	1	**3**
1	0	0	**4**
1	0	1	**5**
1	1	0	**6**
1	1	1	**7**

Ma se usassimo delle monetine quantistiche? Una volta effettuata la misura anche esse potranno solo dare come esito 1 oppure 0 e dunque con tre Q-monetine l'esito della misura sarebbe sempre e solo uno dei possibili 8 valori. La differenza, fondamentale, sta nel fatto che prima della "lettura" le Q-monetine sono in uno stato di sovrapposizione tra 0 e 1 (o in altri termini ogni Q-monetina è contemporaneamente sia 0 che 1), per cui in realtà in ciascun instante possono rappresentare tutti gli 8 valori contemporaneamente!

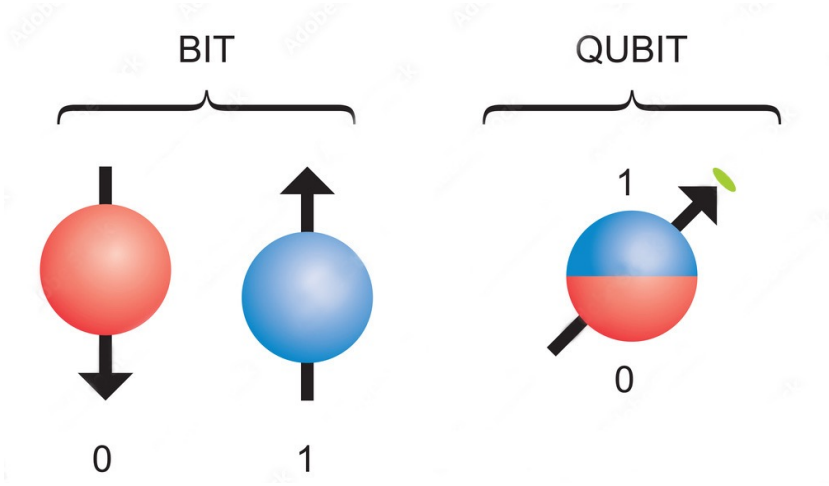
Q-monetina A	Q-monetina B	Q-monetina C	**Valore**
0/1	0/1	0/1	**0,1,2,3,4,5,6,7**

L'idea di base del calcolo quantistico è quella di eseguire delle elaborazioni su stringhe di bit quantistici (i Qubit), mantenendo questi ultimi in uno stato di sovrapposizione, conseguendo così una forma molto particolare di parallelismo che può accelerare di molto alcune elaborazioni.

BOX 3: I Qubit e i loro stati

Essendo i Qubit oggetti quantistici, i valori che possono assumere non sono associati a numeri interi reali, gli 1 e 0 dei bit classici, ma piuttosto a vettori di numeri complessi (gli stati del Qubit), che sono usualmente rappresentati nel formalismo di Dirac, come |1> e |0>. Va anche sottolineato che l'operazione di misura comporta l'interazione del sistema quantistico - il nostro Qubit - con un sistema classico, un processo a cui è sempre associata un'impredicibilità di tipo fondamentale: il massimo che possiamo arrivare a conoscere è la *probabilità* con cui il nostro Qubit "collassa" negli stati |1> oppure |0>. Per comodità, in seguito ci riferiremo agli stati |1> e |0> di un Qubit come ai "valori" 1 e 0 che esso assume.

Mentre un bit classico può solo assumere i due valori 1 e 0, un Qubit può essere in uno stato che è la sovrapposizione, con una certa distribuzione di probabilità, dei due "autostati" I1> e I0>



Fonte: Adobe Stock

Porte, circuiti e algoritmi quantistici

Analogamente ai bit classici, anche i Qubit possono essere processati attraverso specifici operatori, detti "porte quantistiche" (*quantum gates*), con cui possiamo manipolare le probabilità con cui la loro misura fornisca |1> o |0>. Ad esempio è possibile definire una porta che pone in uno stato di sovrapposizione un Qubit precedentemente inizializzato in uno stato noto (|1> o |0>), oppure possiamo invertire lo stato di un Qubit, ad esempio da I1> a |0>. Un tipo speciale di operazioni sono quelle consentite dalle cosiddette porte di misura dei Qubit, dopo le quali essi cessano di essere in uno stato di sovrapposizione e assumono gli stati |1> o |0>.

L'insieme dei Qubit e delle porte quantistiche può essere organizzato in circuiti quantistici che permettono l'esecuzione di algoritmi appositamente disegnati per sfruttare le proprietà di sovrapposizione ed entanglement proprie dei Qubit e conseguire vantaggi di velocità di tipo esponenziale rispetto agli algoritmi che possono essere eseguiti su un computer classico o risolvere problemi che non sono in linea di principio risolvibili classicamente.

Un algoritmo quantistico è dunque implementato come un circuito quantistico costituito da Qubit di ingresso e di uscita e da porte che alterano lo stato quantistico dei Qubit, cioè la distribuzione di probabilità dei loro valori. Il fatto che un Qubit possa esistere in uno stato di sovrapposizione, in cui assume contemporaneamente i valori |1> e |0> con una certa distribuzione di probabilità, permette di operare contemporaneamente, attraverso le porte quantistiche, su tutti i valori possibili del Qubit, fintanto che esso rimane nello stato di sovrapposizione. L'entanglement di più Qubit permette inoltre di manipolarli contemporaneamente, conseguendo un altro livello di parallelismo. Alla fine della catena di elaborazione, le porte di lettura consentono di misurare l'esito del calcolo, distruggendo lo stato di sovrapposizione in cui il sistema si trovava in precedenza.

Un grande sforzo di ricerca è rivolto alla ricerca di algoritmi che possano sfruttare al meglio il parallelismo quantistico e l'entanglement e ad oggi è stato scoperto solo un piccolo insieme di algoritmi autenticamente quantistici.

Qubit logici e Qubit fisici

Finora ci siamo riferiti a Qubit, porte e circuiti in quanto entità astratte, puramente logiche, ma, come per i computer classici, tutto questo ha ovviamente bisogno di essere implementato in un hardware di qualche tipo. I prototipi di computer quantistici oggi disponibili sono basati su una gamma piuttosto ampia di tecnologie, ognuna delle quali sfrutta le proprietà quantistiche di un determinato tipo di sistema, tipicamente alla scala atomica o subatomica, per realizzare i Qubit fisici. Esempi ne sono i sistemi a superconduttore refrigerati a temperature prossime allo zero assoluto, gli ioni intrappolati in un campo elettromagnetico, i sistemi fotonici ed altri sistemi atomici ed elettronici.

Le più diffuse tecnologie per la realizzazione di Qubit fisici

TECNOLOGIA	SUPPORTO AZIENDALE	VANTAGGI	SVANTAGGI
Loop a superconduttore	Google, IBM, Rigetti, QCI	Velocità, basato sull'esistente industria dei semiconduttori	I Qubit collassano facilmente e devono essere refrigerati
Ioni intrappolati	IonQ, Honeywell	Velocità, basato sull'esistente industria dei semiconduttori	I Qubit collassano facilmente e devono essere refrigerati
Punti quantici su silicio	Intel, HRL, SQC	Stabilità, basato sull'esistente industria dei semiconduttori	Limitata possibilità di entanglement, necessita refrigerazione
Qubit topologici	Microsoft	Riduce grandemente gli errori	La loro esistenza non è ancora confermata
Vacanze nel diamante	Quantum Diamond Technologies	Può operare a temperatura ambiente	Difficoltà a creare entanglement
Atomi neutri	Atom Consulting, QuEra	Molti Qubit, reticoli 2D e potenzialmente 3D	Necessita di laser, gli atomi tendono a sfuggire
Fotonica	PsiQuantum, Xanadu	Porte ottiche lineari integrate su chip	Nessuna memoria, non è chiara la scalabilità

Fonte: Adobe Stock

Abbiamo visto in precedenza che il calcolo quantistico sfrutta il particolare parallelismo che offrono i Qubit quando sono nello stato di sovrapposizione. Nella realtà fisica non è però semplice far sì che un Qubit fisico rimanga a lungo in questo stato: si tratta infatti di una condizione molto delicata e sensibile ai disturbi esterni, che può essere facilmente distrutta dalle interazioni del sistema quantistico con l'ambiente circostante, un fenomeno chiamato **decoerenza**.

BOX 4: Qubit fisici e decoerenza

Caratteristica essenziale che un sistema fisico deve possedere per poter implementare un Qubit fisico è quella di poter esistere in due stati discreti distinti e "osservabili" da un osservatore esterno, cioè misurabili, che rappresentiamo come |0> e |1>.

Esso deve inoltre essere in grado di esibire i tipici comportamenti quantistici della sovrapposizione e dell'entanglement, mantenendoli per un tempo sufficientemente lungo, in modo da consentire lo

svolgimento delle elaborazioni. Ne consegue che deve trattarsi di un oggetto *molto piccolo e debitamente isolato dal suo ambiente*, con buona pace dell'improbabile gatto di Schrödinger, che un'infelice esposizione della meccanica quantistica vorrebbe contemporaneamente vivo e morto fintanto che rimane chiuso nella sua scatola.

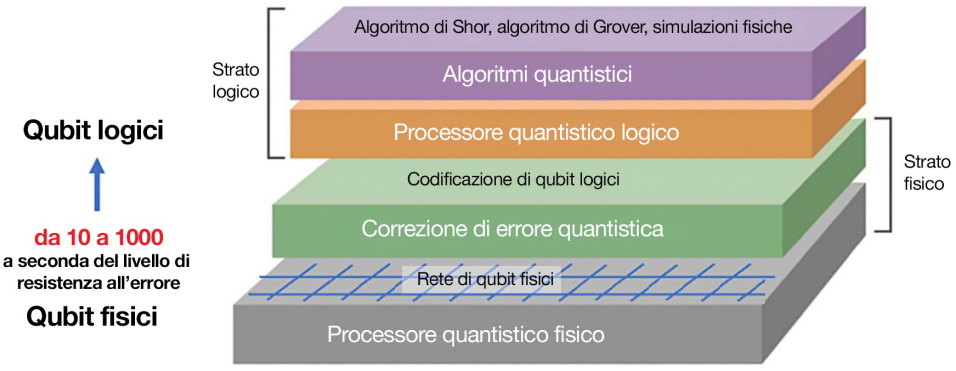
Molto piccolo perché nei sistemi di massa sufficientemente grande gli effetti quantistici vengono in qualche modo mediati e cancellati attraverso le interazioni tra i loro componenti e con l'ambiente. Isolato dall'ambiente circostante perché le interazioni con esso producono lo stesso effetto di perdita della coerenza interna dello stato di sovrapposizione quantistica (decoerenza) rendendo il sistema non utilizzabile per la computazione quantistica.

Il fatto è che le manipolazioni stesse dei Qubit attraverso le porte quantistiche comportano interazioni che, se non sufficientemente "gentili", rischiano di farli collassare. Lo stesso dicasi per la misura finale dello stato dei Qubit di uscita, che non deve distruggere l'informazione che si vuole recuperare. A parte questo, è virtualmente impossibile isolare completamente un sistema quantistico dal suo ambiente e, prima o poi, subentrano effetti di decoerenza e il Qubit in questione diventa portatore di errori che possono inficiare il calcolo.

Si tratta di un problema che pone importanti sfide ingegneristiche per la costruzione dell'hardware che implementa i Qubit, le porte quantistiche e l'elettronica/fotonica di inizializzazione, lettura e controllo, e gli approcci che seguono le diverse aziende impegnate in questa sfida variano a seconda della tecnologia di base utilizzata. A parte costruire Qubit e porte meno "rumorosi" e portatori di errori, una possibilità è quella di realizzare le funzioni di un Qubit logico usando un gran numero di Qubit fisici, sfruttando così la ridondanza con cui è implementata la funzione.

Se un pilastro della ricerca nel *quantum computing* riguarda lo sviluppo di tecnologie hardware per la realizzazione di Qubit fisici affidabili, l'altro, altrettanto importante pilastro, è quello dello sviluppo di algoritmi quantistici in grado di risolvere problemi reali, che i computer classici non possono risolvere o che risolvono in tempi troppo lunghi, sfruttando al meglio gli inediti vincoli e possibilità dettati dalla natura quantistica del sistema di calcolo.

I diversi livelli di un computer quantistico: dai Qubit fisici agli algoritmi

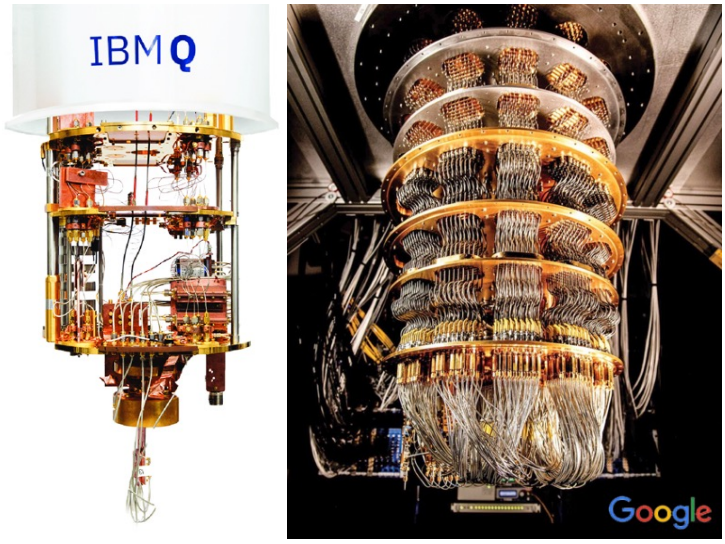


Fonte: Adattato da Mattsson e altri, *Quantum-Resistant Criptografy*, Ericsson Security Research

L'era quantistica rumorosa a scala intermedia

Come abbiamo visto, la principale difficoltà nella realizzazione di un computer quantistico sta nella caratteristica fondamentale del mondo quantistico, per cui non possiamo osservare un sistema quantistico senza produrre disturbi non controllabili nel sistema stesso. Una possibile soluzione a questo problema può essere trovata nel mondo quantistico stesso: se invece di codificare l'informazione in singoli Qubit la codifichiamo in gruppi di Qubit fortemente entangled tra loro conseguiamo infatti una maggiore robustezza, in quanto un eventuale disturbo su uno o più Qubit della collezione di Qubit entangled non è in grado di distruggere completamente l'informazione, che è in qualche modo distribuita sull'intera collezione.

È questo il principio della correzione di errore quantistica (*quantum error correction*) e la sua applicazione potrebbe consentire di costruire computer quantistici tolleranti all'errore, ma il costo in termini di Qubit e porte addizionali rende al momento questo traguardo ancora al di là della portata delle tecnologie attualmente disponibili: per eseguire algoritmi che coinvolgono migliaia di Qubit non rumorosi avremmo infatti bisogno di un numero di Qubit fisici dell'ordine di milioni o più, laddove oggi ci posizioniamo nell'ordine delle centinaia.



I principali player dell'ICT stanno investendo nel quantum computing

L'approccio pragmatico al *quantum computing* in questa fase intermedia (battezzata come era NISQ, un acronimo che sta per *noisy intermediate-scale quantum*) è quello di convivere con Qubit fisici rumorosi, cercando di migliorare sempre più la loro qualità, ottenere tassi di errore di gate più bassi e ridurre al minimo i tempi di elaborazione, in modo da rendere il sistema complessivamente più resiliente rispetto ai fenomeni di decoerenza.

Un traguardo considerato significativo è quello di poter costruire computer quantistici "general purpose" con 70-75 Qubit logici, che sarebbero in grado di conseguire il cosiddetto "vantaggio quantistico", per cui i computer quantistici diverrebbero più veloci dei computer classici nella risoluzione di una vasta gamma di problemi reali di grande rilevanza. Alcune stime danno il raggiungimento di questo traguardo tra il 2030 e il 2040, l'incertezza essendo dovuta alla molteplicità di approcci e tecnologie che centri di ricerca e grandi aziende stanno perseguendo.

Quello che i computer quantistici possono già fare oggi è risolvere problemi specifici molto complessi, grazie ad architetture ad hoc specializzate nell'esecuzione di particolari algoritmi.

Per le applicazioni pratiche, i computer NISQ sono utilizzati come acceleratori in combinazione con sistemi di calcolo tradizionali ad alte prestazioni, i cui servizi di calcolo sono accessibili tramite cloud. È proprio questa l'area in cui si concentra oggi lo sforzo degli sviluppatori di algoritmi quantistici, che necessitano di essere disegnati per sfruttare al meglio le potenzialità di questi sistemi ibridi quantistici/classici.

Computer quantistici analogici

L'architettura che abbiamo descritto precedentemente, sia che si tratti di un futuro computer quantistico universale e tollerante ai guasti con migliaia di Qubit logici che un più modesto sistema di calcolo quantistico NISQ su piccola scala per applicazioni specifiche, è costituita da Qubit di ingresso, circuiti di porte quantistiche che consentono di effettuare manipolazioni sui Qubit e Qubit di uscita e ricorda, almeno da un punto di vista concettuale, quella di un computer digitale.

La computazione algoritmica non è però l'unica strada possibile per risolvere problemi complessi utilizzando un dispositivo quantistico: è infatti possibile, e in alcuni casi più conveniente, ricorrere ad un approccio di tipo analogico, in cui per studiare un sistema complesso si costruisce un sistema fisico più semplice da controllare e osservare che ne approssima, entro certi limiti, il comportamento.

Un ambito applicativo molto rilevante è quello della simulazione di sistemi quantistici complessi, come quelli che si incontrano nella fisica delle alte energie e degli stati condensati e nella chimica quantistica. Si tratta di problemi la cui complessità computazionale cresce in maniera esponenziale con la dimensione del sistema quantistico considerato e che si prestano dunque molto bene ad un approccio analogico.

Il principale vantaggio dei dispositivi quantistici analogici rispetto ai computer quantistici "digitali" è che le loro condizioni operative sono più facili da realizzare e controllare, poiché non utilizzano porte quantistiche per manipolare i Qubit e non richiedono la correzione degli errori.

Un altro ambito in cui dispositivi quantistici analogici relativamente piccoli e rumorosi potranno essere utilmente impiegati è quello dell'ottimizzazione combinatoria, ad esempio nella pianificazione dei percorsi e nell'ottimizzazione dei costi, una classe di problemi comune a quasi tutti i campi, dall'industria alla finanza alle scienze sociali.

3.3 LA SENSORISTICA QUANTISTICA

Quello che nel calcolo quantistico rappresenta un problema e una sfida tecnologica, la grande sensibilità degli stati quantistici alle interazioni con fattori esterni che possono provocare la loro decoerenza, è proprio ciò che viene sfruttato per costruire sensori quantistici estremamente sensibili a stimoli esterni quali il movimento, il campo magnetico e la gravità.

L'idea di sfruttare effetti quantistici per realizzare sistemi diagnostici e di misura non è nuova: la risonanza magnetica nucleare (RMN), una tecnica di indagine sulla materia basata sulla misura della precessione dello spin di protoni o di altri nuclei dotati di momento magnetico, con vaste applicazioni in medicina, chimica, petrografia e geofisica, è ad esempio stata messa a punto negli anni '40 del secolo scorso. Altri esempi sono gli orologi atomici a microonde, un elemento fondamentale dei nostri sistemi GPS, e i magnetometri SQUID (*superconducting quantum interference device*), anch'essi noti da tempo.

La novità sta nella mole di attività di ricerca e sviluppo tecnologico dedicate alla messa a punto di sensori quantistici di livello atomico, che sfruttano l'entanglement per aumentare la sensibilità e la robustezza delle misure, condividendo spesso le stesse tecnologie dei sistemi di calcolo quantistico, ad esempio sistemi a superconduttore, sistemi fotonici, ioni intrappolati, qubit di spin e atomi freddi.

Qubit sensibili

Come per il *quantum computing*, il mattone fondamentale del *quantum sensing* è un Qubit, i cui due possibili stati |1> e |0> sono in questo caso associati a due livelli energetici distinti, tra cui il Qubit può transitare in seguito all'interazione con una qualche forma di energia esterna. Come per i Qubit computazionali, anche in questo caso deve essere possibile inizializzare il Qubit del sensore a uno stato noto, deve essere possibile eseguire delle manipolazioni mantenendo il Qubit in uno stato di sovrapposizione e deve essere possibile mettere in entanglement più Qubit, sia per migliorare la resilienza del sensore al rumore che per conseguire maggiore sensibilità e precisione della misura.

L'estrema sensibilità dei sensori quantistici ai disturbi esterni, se ne è la prerogativa realizzativa, rappresenta anche una delle principali sfide tecnologiche, in quanto essi devono sì potersi accoppiare con il fenomeno che si intende misurare ma al tempo stesso rimanere isolati da qualsiasi altra fonte di disturbo esterno. Come nel caso dei Qubit rumorosi nell'informatica quantistica, questo problema può essere mitigato in vari modi, come la realizzazione di hardware ad-hoc per l'applicazione specifica, il calcolo della media delle misure e l'uso di sensori entangled.

Una famiglia molto ampia

Oltre a un'estrema sensibilità e precisione, i sensori quantistici permettono misure non invasive senza contatto con tempi di risposta molto rapidi e consentono di rilevare e misurare le più piccole variazioni di tempo, gravità, temperatura, pressione, rotazione, accelerazione, frequenza e campi magnetici ed elettrici. A questi si aggiungono i sensori per il *quantum imaging*, che sfruttano le correlazioni quantistiche della luce per realizzare sistemi di acquisizione di immagini caratterizzati da elevatissima sensibilità e risoluzione spaziale e spettrale, una categoria che spesso viene tenuta distinta dal *quantum sensing* ma che in questo rapporto includiamo nella categoria più generale di sensoristica quantistica.

Le tipologie di sensori ad oggi sviluppati sono molto varie, rendendo difficile una loro elencazione esaustiva. La tabella seguente ne riporta le principali tipologie: la prima colonna descrive il tipo di sistema quantistico utilizzato, la seconda la grandezza quantistica associata al Qubit e la terza le grandezze misurate.

Esempi di sensori quantistici

IMPLEMENTAZIONE	QUBIT	QUANTITÀ MISURATA
Atomi neutri		
Vapori atomici	Spin atomico	Campo magnetico, rotazione, tempo/frequenza
Nubi atomiche fredde	Spin atomico	Campo magnetico, accelerazione, tempo/frequenza
Ioni intrappolati		
	Stati elettronici longevi	Tempo/frequenza, rotazione
	Modi vibrazionali	Campo elettrico, forza
Atomi di Rydberg		
	Stati di Rydberg	Campo elettrico
Spins allo stato solido (ensemble)		
Sensori d'insieme NMR	Spin nucleare	Campo magnetico
Ensemble di centri NV*	Spin elettronico	Campo elettrico, campo magnetico, temperatura, pressione, rotazione
Spin allo stato solido (spin singolo)		
Donatori di lacune P nel silicio	Spin elettronico	Campo magnetico
Punti quantici a semiconduttore	Spin elettronico	Campo elettrico, campo magnetico
Centri singoli NV*	Spin elettronico	Campo elettrico, campo magnetico, temperatura, pressione, rotazione
Circuiti superconduttori		
SQUID	Supercorrente	Campo magnetico
Qubit di flusso	Correnti circolanti	Campo magnetico
Qubit di carica	Autostati di carica	Campo elettrico
Particelle elementari		
Muoni	Spin muonico	Campo magnetico
Neutroni	Spin nucleare	Campo magnetico, densità di fononi, gravità
Altri sensori		
Transistor a singolo elettrone SET	Autostati di carica	Campo elettrico
Optomeccanica	Fononi	Forza, accelerazione, massa, campo magnetico, voltaggio
Fotoni	Fotoni	Spostamento, indice di rifrazione

* centri NV: centri di azoto vacanti

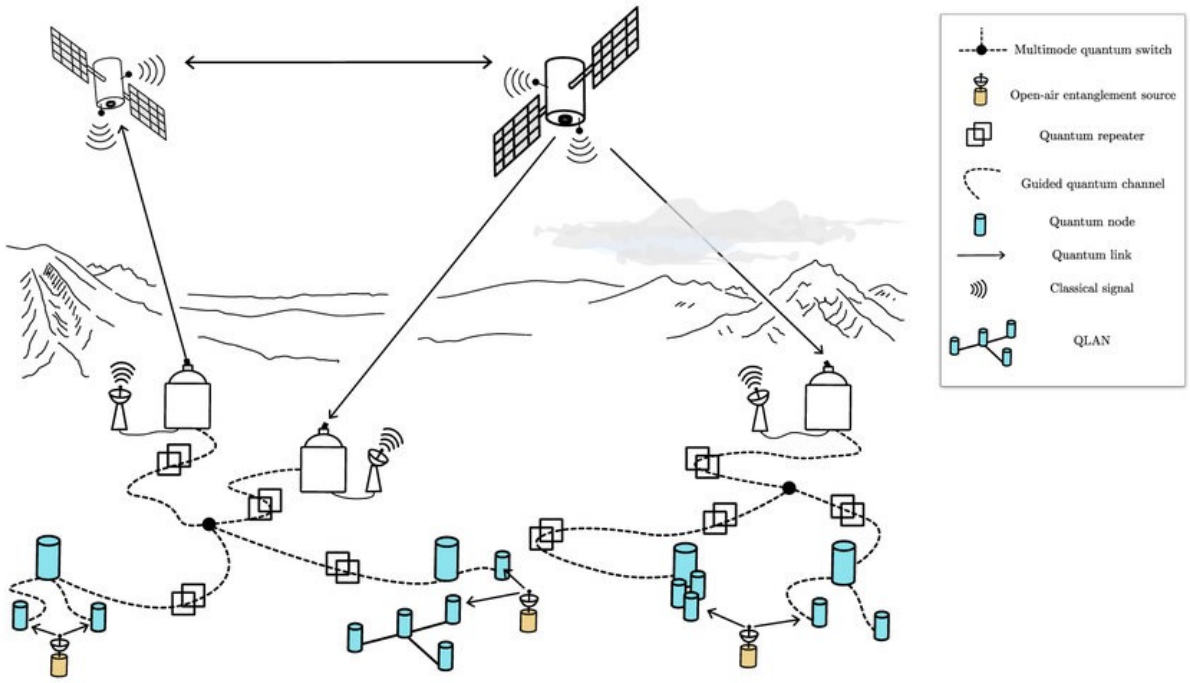
Fonte: Adattato da Degen, Reinhard, Cappellaro, *Quantum Sensing*, Rev. Mod. Phys. 89, 2017

3.4 LA COMUNICAZIONE QUANTISTICA

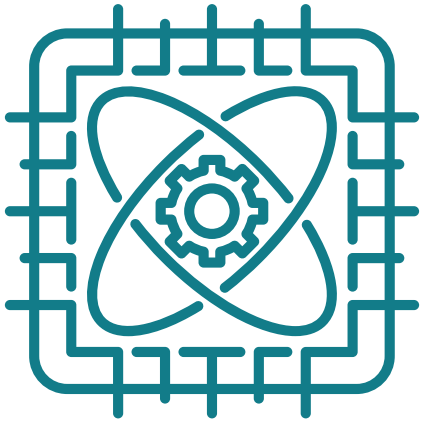
La comunicazione quantistica, su cui si concentrano notevoli investimenti in ricerca anche da parte di operatori privati, raggruppa un insieme di tecniche e applicazioni, di cui diciamo più in dettaglio nel prossimo capitolo, finalizzate ad aumentare la sicurezza dello scambio dei dati, vero tallone d'Achille delle moderne comunicazioni informatiche.

Un pilastro fondamentale della comunicazione quantistica è rappresentato dalle tecniche di crittografia quantistica, a cui si accompagnano quelle di generazione di numeri "realmente" casuali e tutte quelle altre tecnologie in fase di sviluppo, come i ripetitori quantistici, finalizzate alla realizzazione di un vero e proprio Internet Quantistico, una rete di reti quantistiche che si affiancherebbe al classico Internet per fornire servizi di comunicazione quantistiche a organizzazioni particolarmente sensibili alla sicurezza dei dati, oltre che per connettere tra loro i computer quantistici presenti su cloud.

Vista idealizzata di una sezione di una rete di comunicazione quantistica interconnessa e su larga scala che combina collegamenti ottici e a microonde



Fonte: Casariego e altri, *Propagating quantum microwaves: towards applications in communication and sensing*, Quantum Sci. Technol. 8 (2023) 023001



4. QUALI SONO I LORO AMBITI DI APPLICAZIONE?

4.1 I COMPUTER QUANTISTICI NELL'ERA NISQ E OLTRE

Abbiamo visto che, grazie al fenomeno della sovrapposizione, con N Qubit possiamo rappresentare l'informazione codificata in 2^N bit classici. Con 10 Qubit possiamo dunque rappresentare contemporaneamente $2^{10} = 1024$ diversi valori, che un computer classico processa in un tempo dell'ordine dei microsecondi. Già con 50 Qubit arriviamo a valori di bit classici dell'ordine del migliaio di Terabyte, per tempi di calcolo che superano la settimana. Con 100 Qubit arriviamo a valori astronomici dei tempi di calcolo classici, dell'ordine dei trilioni (miliardi di miliardi) di anni!

Stiamo ovviamente parlando di Qubit logici tolleranti ai guasti e di un computer quantistico di uso generale (scalabile), programmabile alla stregua di un computer classico e dunque in grado di eseguire in modo affidabile algoritmi quantistici arbitrari sotto forma di una sequenza di porte logiche quantistiche elementari.

Siamo ancora molto lontani dalla possibilità di costruire un computer del genere, essendo lo stato attuale dello sviluppo tecnologico caratterizzato da computer quantistici NISQ "rumorosi", con un numero limitato di Qubit e di porte quantistiche (nell'ordine delle poche decine), che possono ottenere risultati affidabili solo per specifici problemi e quindi non possono essere scalati per eseguire calcoli arbitrari. Il loro uso resta in ogni caso oggi confinato nell'ambito della ricerca accademica e dello sviluppo di nuovi algoritmi e casi d'uso e non è stata ancora realizzata alcuna applicazione di reale utilità che non possa essere implementata con i computer classici.

Anche i computer quantistici analogici, che non operano sulla base di porte quantistiche ma modellano in maniera analogica i sistemi che si vogliono simulare, sono in grado di risolvere problemi specifici potenzialmente di grande interesse.

I progressi sono in ogni caso costanti e già nei prossimi 4 o 5 anni si stima[1] sarà possibile impiegare questi sistemi per risolvere problemi specifici anche di natura commerciale, inattaccabili dai computer classici, sia per ragioni di velocità che di più fondamentale impossibilità. Vediamo di seguito brevemente le principali classi di problemi che meglio si prestano ad essere affrontati con il calcolo quantistico.

1 *The Next Five Years of Quantum Technology: Hype vs. Reality*, www.IDTechEx.com

Simulazione

L'intuizione del grande fisico Richard Feynman, soventemente citata come l'idea che ha dato il via alla ricerca sulla computazione quantistica, esprimeva la convinzione che solo un sistema di calcolo inerentemente quantistico avrebbe potuto simulare un sistema quantistico minimamente complesso.

Di fatto, la simulazione quantistica rappresenta oggi uno degli ambiti applicativi più promettenti del quantum computing, che potrebbe permettere di comprendere meglio la struttura, la dinamica e le proprietà di sistemi quantistici a livello molecolare e sub-molecolare, spesso difficili o impossibili da studiare con i metodi classici, con ricadute nei campi della chimica, della scienza dei materiali, della biologia, delle nanotecnologie e della farmaceutica.

In quest'ultimo ambito, l'informatica quantistica, combinata con l'apprendimento automatico, potrebbe ad esempio ridurre significativamente i tempi e i costi di sviluppo di nuovi farmaci, aumentandone al contempo il tasso di successo; lo stesso approccio potrebbe essere utilizzato per simulare la biologia umana in modo da testare virtualmente i nuovi farmaci prima di ricorrere ai trial clinici.

Crittografia quantistica

Un'altra operazione che i computer quantistici possono eseguire in modo esponenzialmente più veloce degli omologhi classici, è la **fattorizzazione**, che consiste nello scomporre un numero intero nei suoi "fattori" primi, cioè nel trovare i numeri primi che moltiplicati tra loro creano quel numero. Ad esempio, il numero 315 può essere fattorizzato nei tre numeri primi 3, 5 e 7, in quanto 3x5x7= 315. Può sembrare un compito semplice ma la sua difficoltà cresce esponenzialmente con l'aumento della grandezza del numero che si vuole fattorizzare.

L'algoritmo messo a punto nel 1994 dal matematico americano Peter Shor sfrutta le proprietà uniche dei sistemi quantistici, come la sovrapposizione e l'entanglement, per ridurre la complessità della fattorizzazione da esponenziale a polinomiale, rendendola molto più veloce dei metodi classici.

La fattorizzazione svolge un ruolo cruciale in vari campi, come la crittografia e la teoria dei numeri, ed è alla base di molti algoritmi di crittografia, dove la difficoltà di fattorizzare grandi numeri garantisce la sicurezza delle informazioni sensibili. Di fatto, è stato dimostrato che i computer quantistici sono in grado in linea di principio di violare gli algoritmi di crittografia più comuni, come il sistema crittografico a chiave pubblica RSA, anche se ad oggi non esiste alcun computer con numero sufficiente di Qubit logici per violare una chiave RSA-2048.

Se dunque in prospettiva i computer quantistici potrebbero mettere in crisi i sistemi consolidati di crittografia, lo sviluppo di nuovi algoritmi di crittografia quantistica potrà permettere di conseguire livelli ancora superiori di sicurezza. Grazie alla *Quantum Key Distribution* (QKD), di cui parliamo estesamente più avanti, le parti possono infatti criptare le comunicazioni condividendo in modo sicuro le chiavi segrete ad alta velocità e su lunghe distanze.

Ottimizzazione

Quella dell'ottimizzazione è una classe di problemi molto ampia, in cui risulta necessario trovare i valori che rendono minima o massima una certa funzione. Un esempio è il problema del commesso viaggiatore, che deve minimizzare la distanza percorsa nel visitare un dato numero di città, ma problemi di questo tipo si trovano praticamente in tutti gli ambiti di attività, dalla logistica alla finanza, alla produzione industriale, all'energia.

Anche in questo caso i computer quantistici possono offrire dei vantaggi in termini di velocità, tramite algoritmi quantistici variazionali (VQA) che minimizzano una funzione di costo (nel nostro esempio la distanza percorsa dal commesso viaggiatore) codificando i parametri di variazione (i diversi ordini in cui vengono visitate le città) nello stato di uno o più Qubit.

Esempi di possibili applicazioni li troviamo nella logistica (ottimizzazione di flotte, rotte, traffico, catene di fornitura e inventari), nell'energia (ottimizzazione della produzione energetica e della rete di distribuzione elettrica) e nella finanza (ottimizzazione del portafoglio finanziario, analisi di rischio finanziario, valutazione di strumenti e premi assicurativi, rilevamento di frodi finanziarie ecc.).

Intelligenza artificiale

Il grande successo di applicazioni di intelligenza artificiale generativa come ChatGPT, basate su architetture di reti neurali dotate di meccanismi di auto-attenzione, in grado di processare in parallelo i propri input e dunque sfruttare appieno la potenza di calcolo delle moderne GPU, ha recentemente e rapidamente polarizzato l'attenzione del pubblico e dei governi e mobilitato gli investimenti privati. Questa vera e propria "febbre dell'IA" sembra avere in qualche modo ridotto l'attenzione mediatica e l'interesse degli investitori verso le tecnologie quantistiche, percepite come più di frontiera e i cui potenziali benefici sembrano proiettarsi in un futuro ancora non ben definito.

Questa apparente concorrenza tra le due tecnologie può però in prospettiva trasformarsi in una potente sinergia: da un lato infatti il quantum computing potrebbe offrire versioni quantistiche degli algoritmi di apprendimento automatico, caratterizzati dal richiedere molti meno parametri e dati di addestramento, e dall'altra l'intelligenza artificiale potrebbe contribuire alla messa a punto di schemi efficaci di correzione degli errori e di gestione dei Qubit nei computer quantistici. Si tratta certamente di una prospettiva di medio-lungo periodo, ma il suo impatto potrebbe essere dirompente.

I settori industriali di interesse

Gli ambiti in cui si sta concentrando lo sforzo di messa a punto di casi d'uso e che con maggiore probabilità saranno impattati dal computing quantistico sono la salute, la sicurezza informatica e la finanza, con sviluppi interessanti anche in ambito manifatturiero (aerospazio e automotive in particolare), energetico e logistico. Ci vorranno comunque ancora molti anni prima che queste applicazioni si affermino a livello commerciale, anni in cui lo sviluppo di hardware sempre più efficiente e affidabile e di nuove tecniche algoritmiche permetteranno l'atteso salto qualitativo e quantitativo.

La figura seguente elenca i problemi di interesse industriale su cui alcuni grandi player stanno lavorando, investendo nello sviluppo di casi d'uso e algoritmi quantistici, spesso con il supporto di o in partnership con i fornitori di hardware quantistico. Si tratta di ambiti applicativi molto sfidanti, in cui un salto in avanti in termini di prestazioni (riduzione dei tempi di calcolo, precisione, ecc.) e fattibilità può determinare vantaggi competitivi di grande portata.

I problemi che il calcolo quantistico potrebbe risolvere nelle principali industrie

Fonte: Adattato da *The Next Five Years of Quantum Technology: Hype vs. Reality*, www.IDTechEx.com

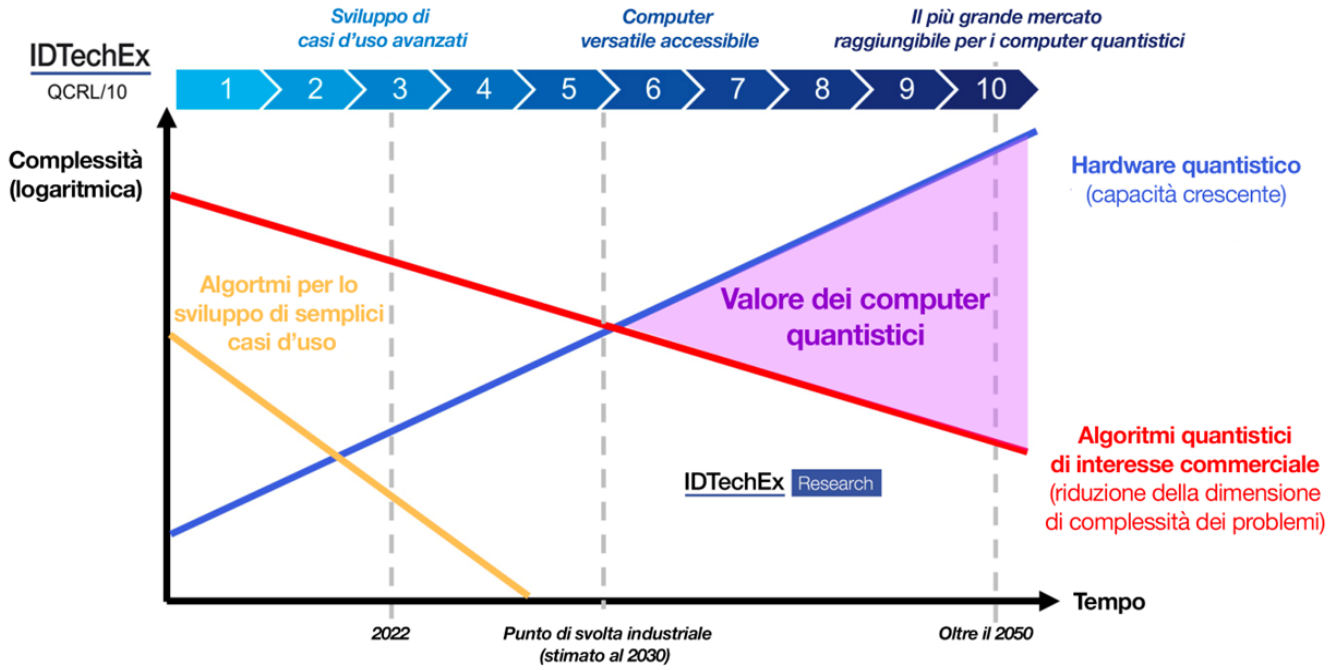
Una traiettoria graduale di adozione

Abbiamo visto che, da un punto di vista tecnologico, il quantum computing sarà caratterizzato a breve termine (4-5 anni) da sistemi NISQ per applicazioni specifiche, con complessità ridotta e prestazioni ottimizzate. Superato il giro di boa del 2030, potremo verosimilmente assistere alla messa a punto di computer quantistici più versatili, dall'elevato costo unitario, le cui prestazioni di calcolo saranno accessibili via cloud.

Il diagramma in figura illustra qualitativamente questa prospettiva. La linea rossa rappresenta la riduzione nel tempo della complessità dei problemi consentita dall'uso di algoritmi quantistici: si prevede che nel tempo questi diventino sempre più potenti e che dunque siano sempre più in grado di ridurre la complessità dei problemi affrontati (maggiore capacità di risolvere problemi di interesse commerciale, minori tempi di calcolo ecc.). La linea blu mostra invece la crescente capacità di calcolo offerta dai calcolatori quantistici, legata al numero dei Qubit e delle porte quantistiche, oltre che all'architettura interna dei calcolatori.

Perché il quantum computing possa divenire una tecnologia di interesse commerciale e iniziare la sua penetrazione di mercato occorrono un hardware quantistico sufficientemente versatile e potente e algoritmi quantistici sufficientemente sofisticati, cosa che nella figura è rappresentata dal punto di

Previsione sullo sviluppo del Quantum Computing



Fonte: Adattato da *Quantum Computers: What Are They and When Will They Create Commercial Value?*, www.IDTechEx.com

intersezione delle due linee, stimato nel 2030. A partire da questo punto di svolta, il mercato dei computer quantistici diventa sempre più ampio (area viola tra le due linee rossa e blu). La linea gialla sulla sinistra del grafico mostra la crescente capacità degli algoritmi quantistici di ridurre la complessità di casi d'uso semplici, legati a problemi moto specifici, che possono essere affrontati anche con computer quantistici di ridotta potenza e versatilità: si tratta in sostanza della fase in cui siamo adesso.

Sicuramente l'interesse preponderante per l'informatica quantistica continuerà ancora per un po' di tempo ad essere espresso dalle università e dalle altre istituzioni scientifiche, con applicazioni prevalenti nel campo della ricerca scientifica. I forti investimenti pubblici porteranno inoltre a una sempre maggiore diffusione di computer quantistici presso centri di calcolo ad alte prestazioni (HPC), che potranno così offrire servizi di calcolo ibrido classico-quantistico (presso l'Università Federico II di Napoli è operativo uno di questi sistemi e presto lo sarà un altro presso il CINECA di Bologna). Nell'attuale era NISQ, i sistemi HPC saranno infatti essenziali per effettuare la correzione degli errori e l'elaborazione dei dati, permettendo di sfruttare al meglio le ancora limitate capacità del computer quantistico.

Nel mondo privato, le prime industrie a puntare e investire sul calcolo quantistico saranno quelle che necessitano di immense potenze di calcolo come quelle chimiche o farmaceutiche, che potranno accorciare sensibilmente i tempi necessari per individuare nuovi farmaci e sostanze chimiche. La disponibilità nel prossimo decennio di sistemi quantistici di calcolo più versatili permetterà di risolvere problemi di più vasto interesse commerciale, per esempio legati a problemi di ottimizzazione, allargando il loro impiego all'aerospazio, all'automotive e alla finanza.

Si prospetta dunque un percorso molto graduale di adozione di questa tecnologia, che certamente presenterà i suoi alti e bassi e sarà presumibilmente ricco di sorprese e, possibilmente, di brusche accelerazioni legate alla messa a punto di piattaforme hardware più economiche ed efficienti e di nuovi algoritmi.

Se è vero che si tende a sopravvalutare ogni nuova tecnologia emergente nel breve periodo e a sottovalutarla nel lungo periodo, è molto probabile che agli entusiasmi iniziali per il quantum computing possano seguire fasi di flessione dell'interesse pubblico, per ritrovarsi improvvisamente proiettati in una rivoluzione tecnologica che si prospetta ancora più dirompente di quella prodotta dall'intelligenza artificiale.

4.2 LA VASTA GAMMA DI APPLICAZIONE DEI SENSORI QUANTISTICI

Sensori diversi per applicazioni specifiche

A differenza dei computer quantistici, potenzialmente dispositivi "general-purpose" applicabili in un'infinità di ambiti diversi, i sensori quantistici sono molto più specifici rispetto alle applicazioni. Questa specificità tecnologica e applicativa porta a un ecosistema più frammentato rispetto al calcolo quantistico, diluendo sia il clamore mediatico di cui sono oggetto che la concorrenza tra i player.

Allo stato attuale dello sviluppo, caratterizzato da sistemi di grande peso, ingombro e soprattutto costo, la parte preponderante dei casi d'uso dei sensori quantistici è stata sviluppata per il settore della difesa/aerospazio e per industrie e applicazioni caratterizzati da produzioni massive, come l'elettronica, o da alte priorità in termini di prestazioni e bassa sensibilità ai costi unitari dei sistemi sensore, come l'industria della salute e farmaceutica e il settore delle prospezioni geologiche ed energetiche.

In ambito biomedicale, a sensibilità e risoluzione spaziale senza precedenti dei sensori quantistici, alcuni dei quali della dimensione di un singolo atomo, li rende particolarmente interessanti per quelle applicazioni che richiedono di indagare processi e sistemi a micro e nano scala, quali possono essere singoli neuroni, cellule o molecole, come anche di rilevare biosegnali molto deboli, come quelli rilevati nella risonanza magnetica nucleare (NMR), nella magnetoencefalografia (MEG), nella magnetocardiografia (MCG) e nella tomografia a induzione magnetica.

Rilevanti sono anche le applicazioni della sensoristica quantistica in ambito aerospaziale, divisibili in tre grandi categorie: quelle geospaziali legate all'osservazione della terra, quelle concernenti il posizionamento, la navigazione e la temporizzazione e quelle dedicate alla rilevazione ottica di oggetti spaziali. Il Box 5 ne offre una breve descrizione.

La tabella seguente fornisce un elenco parziale delle applicazioni possibili delle diverse tipologie di sensori negli ambiti sopra indicati.

Principali ambiti applicativi dei sensori quantistici

TECNOLOGIA	DIFESA / AEROSPAZIO	SALUTE	ELETTRONICA	GEOLOGIA / ENERGIA
Sensori elettromagnetici quantistici	• Rilevazione anomalie magnetiche; • Analisi dei segnali; • Cartografia magnetica; • Rilevazione sottomarini e mine	• Imaging attività cerebrale; • Spettroscopia su scala nanometrica; • Sistemi per risonanza magnetica portabili	• Controllo qualità in produzione di chip; • Controllo qualità prestazioni batterie e celle fotovoltaiche	Rilevazione anomalie magnetiche (attività sismiche e vulcaniche)
Imaging quantistico	• Lidar e radar quantistici; • Imaging ad alta risoluzione spaziale e spettrale	Imaging medicale (microscopia 3D ad alta risoluzione, imaging a raggi X)	Ispezione industriale	Monitoraggio fughe di gas ed emissioni CO_2
Gravimetri e gradiometri* quantistici	Navigazione inerziale			Prospezione sottosuolo
Termometri e barometri	Sonar	Monitoraggio pazienti	Gestione temperatura dei semiconduttori	• Gestione infrastrutture e impianti; • Monitoraggio metereologico

* Gradiometri: misurano le variazioni di un campo gravitazionale

Fonte: Adattato da BCG, *Making Sense of Quantum Sensing*, www.bcg.com

La progressiva riduzione di dimensioni e costo dei sensori permetterà l'allargamento delle applicazioni sopra elencate ad altri ambiti, quali il monitoraggio di infrastrutture quali strade, dighe o impianti industriali e la navigazione autonoma nell'industria automotive. Da sottolineare anche che i sensori quantistici avranno un ruolo fondamentale anche per le applicazioni trasversali del computing quantistico e della comunicazione quantistica.

BOX 6: Sensori quantistici per l'aerospazio

I sensori quantistici di **gravità e campo magnetico** permettono di realizzare una serie di applicazioni diverse, fungendo da carico utile sia per osservazioni da satellite che per rilevamenti operati da aereo; essi permettono infatti di misurare piccoli cambiamenti attualmente invisibili, di mappare le deviazioni nei livelli delle falde acquifere sotterranee, di monitorare i cambiamenti nelle calotte glaciali e di rilevare gli impatti del sottosuolo derivanti da attività minerarie o di altro genere. Applicazioni importanti le troviamo nell'indagine dei processi e delle cause sottostanti al cambiamento climatico, attraverso l'osservazione satellitare dei cambiamenti nella distribuzione della massa terrestre, ad esempio a causa dello scioglimento dei ghiacciai o della perdita di acqua sotterranea.

L'**interferometria atomica** è un potente strumento per applicazioni di questo tipo, in quanto consente misurazioni di alta precisione del campo gravitazionale terrestre, sfruttando le proprietà quantistiche degli atomi che fungono da massa di prova. In orbita, questi dispositivi possono essere utilizzati per osservare processi globali come l'innalzamento del livello del mare con una sensibilità senza pari. Il progetto Horizon Europe CARIOQA-PMP (Cold Atom Rubidium Interferometer in Orbit for Quantum Accelerometry - Pathfinder Mission Preparation) della Commissione Europea, lanciato nel dicembre 2022, farà maturare questi sensori quantistici e preparerà quindi il terreno per future missioni di gravimetria di alta precisione nello spazio.

Le accurate misure di **accelerazione** fornite dai sensori quantistici hanno il potenziale per rivoluzionare i sistemi di navigazione, consentendo di soppiantare i correnti sistemi GPS, di limitata precisione e affidabilità negli ambienti urbani, alle alte latitudini, nel sottosuolo e nei campi di battaglia, permettendo un calcolo molto più preciso della posizione senza il supporto di sistemi satellitari. Anche i sensori di campo magnetico, ad esempio quelli basati sulle lacune di azoto in reticoli cristallini di diamante, hanno un rilevante potenziale applicativo in ambito aerospaziale (e difesa), soprattutto nel posizionamento, tramite un giroscopio che rileva il **campo magnetico** terrestre per la navigazione, e nella rilevazione di anomalie magnetiche (vedi altri velivoli o mezzi sottomarini).

Applicazioni in ambito aerospaziale sono possibili anche con i sensori di **imaging quantistico**, che sfruttano le correlazioni insite nella luce per acquisire immagini, cosiddette *quantum-enhanced*, con qualità più elevata rispetto a quanto imposto dai limiti tipici dell'ottica classica, sia in termini di rumore che di risoluzione. La disponibilità di fasci di luce correlati ha dato altresì il via allo sviluppo di nuove modalità di acquisizione di immagine, quali il cosiddetto ghost imaging, in cui l'immagine dell'oggetto di interesse si ottiene puntando la camera non all'oggetto, ma alla sorgente luminosa, consentendo di sopprimere il rumore di fondo e di ottenere immagini ad alta risoluzione di oggetti difficili da rilevare, come oggetti distanti di interesse astronomico. Questa tecnica si presta per l'imaging spaziale e l'osservazione della terra.

L'entaglement di fasci di luce coerente può essere impiegato anche per altre applicazioni, come l'illuminazione di oggetti opachi circondati da uno sfondo termico luminoso (*Quantum Illumination*), utilizzabile nel dominio delle microonde per realizzare i cosiddetti **radar quantistici**. In questi contesti trova naturale applicazione anche l'emergente tecnologia dell'imaging iperspettrale in correlazione, che risolve il tipico trade-off tra risoluzione e velocità, garantendo la combinazione di elevate risoluzioni spaziali e spettrali e velocità di acquisizione delle immagini. Come nel caso dell'immagine plenottica in correlazione, anche questa tecnologia porta con sé i vantaggi connessi all'indipendenza dalle delicate risorse quantistiche, quale l'entanglement.

Le sfide per l'adozione

Per molte delle grandezze di interesse esistono già soluzioni basate su sensori tradizionali: affinché un settore industriale decida di optare per i più sensibili e precisi sensori quantistici sarà necessario superare alcune barriere legate all'attuale alto costo di impianto ed esercizio dei sensori quantistici e alle problematiche legate all'estrema sensibilità di questi dispositivi, che li espone al rischio di disturbi quando utilizzati al di fuori dell'ambiente protetto del laboratorio, un elemento quest'ultimo cruciale anche dal punto di vista delle norme di accuratezza e sicurezza vigenti in molti ambiti, come quello sanitario e militare.

Altre barriere a un'ampia diffusione della sensoristica quantistica sono legate alle necessarie attività di customizzazione necessarie per la loro integrazione nei sistemi e processi in cui essi devono essere impiegati e alla necessaria miniaturizzazione che possa consentirne la produzione su larga scala, una sfida tecnologica importante, vista la loro complessità realizzativa e la necessità di attingere a un vasto spettro di expertise.

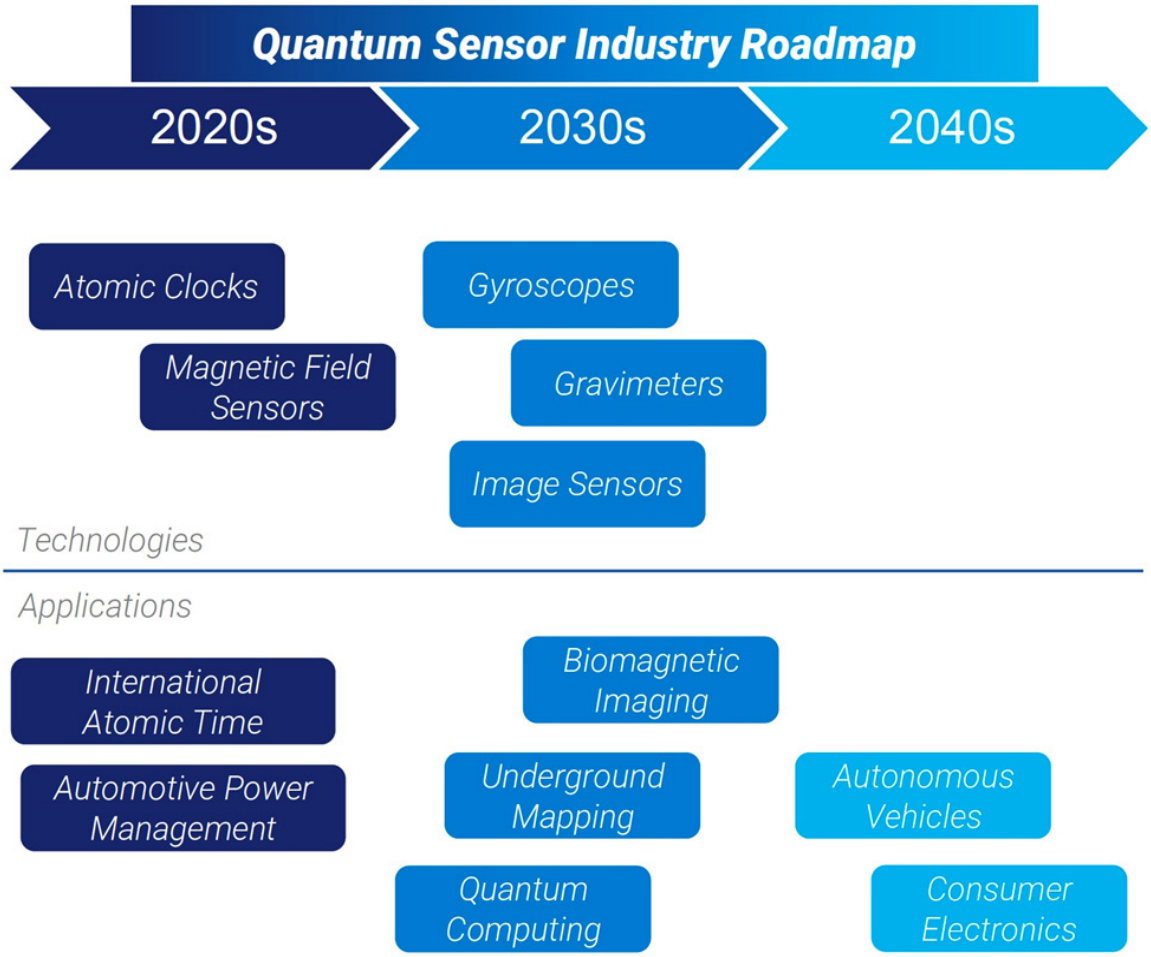
Se l'estrema sensibilità, le difficoltà di integrazione e la limitata scalabilità sono dunque ostacoli alla standardizzazione dei sensori quantistici, prerequisito fondamentale per la penetrazione e la crescita del mercato, gli esperti concordano sul fatto che il quantum sensing avrà un impatto rilevante su molte delle nostre industrie nei prossimi anni.

Alcune tipologie di sensori quantistici sembrano in particolare "appetibili" per applicazioni con un potenziale di mercato molto alto, tra queste i sensori di campo magnetico, applicabili nell'industria automotive e nei dispositivi indossabili, e gli orologi atomici, che permettono un livello di accuratezza dell'ordine dei nanosecondi, tre ordini di grandezza superiore a quello possibile con gli oscillatori a cristalli di quarzo utilizzati nei nostri dispositivi digitali. La combinazione di orologi atomici e giroscopi o accelerometri quantistici può infatti fornire capacità di navigazione di precisione, anche in ambienti privi di copertura GPS, con importanti applicazioni nel campo dei veicoli a guida autonoma, nello spazio, nell'industria e nella difesa, oltre che in ambito scientifico.

Per quanto riguarda i dispositivi di imaging quantistico, quali le camere plenottiche e le camere iperspettrali a correlazione, la loro industrializzazione e commercializzazione sono attese nel breve termine anche grazie al mancato condizionamento dallo sviluppo di sorgenti efficienti di fotoni entangled e di array di sensori ad un singolo fotone.

IDTechEx prevede che il mercato dei sensori quantistici raggiunga il valore di 7,1 miliardi di dollari nel 2044, con un tasso di crescita percentuale medio del 18% e propone uno sviluppo temporale come quello illustrato nella figura seguente.

Possibile roadmap dell'industria dei sensori quantistici



Fonte: *Quantum Sensors: A Bigger Opportunity Than Quantum Computers?*, www.IDTechEx.com

4.3 VERSO UN INTERNET QUANTISTICO

Come abbiamo accennato nel precedente capitolo, per Quantum Internet si intende una rete di computer quantistici che funziona in sinergia con Internet, offrendo nuove funzionalità e servizi per la sicurezza delle telecomunicazioni e l'elaborazione dei dati in cloud. Dobbiamo pensare al Quantum Internet come a un ecosistema di tecnologie e applicazioni che concorrono a rendere possibile lo scambio e l'elaborazione dei dati in modalità sicura, appoggiandosi sulle peculiari proprietà dei sistemi quantistici, quali la sovrapposizione, l'entanglement e l'impossibilità di clonare un sistema quantistico.

Si tratta di un'area di sviluppo strategica, che anche la Commissione Europea ha selezionato come area privilegiata di investimento, lanciando la Quantum Internet Alliance (QIA), guidata da QuTech (una collaborazione tra le olandesi Technische Universiteit Delft e TNO), che implementerà un programma della durata di sette anni con lo scopo di sviluppare un prototipo di rete *full-stack* che connetta città distanti tra loro.

Dal suo canto, la Cina si dimostra uno degli attori più attivi in questo campo, con il lancio qualche anno fa di un satellite dedicato alle comunicazioni quantistiche, chiamato Micius, che nel 2017 ha contribuito a

organizzare la prima videoconferenza intercontinentale protetta da crittografia quantistica tra Pechino e Vienna e che è collegato alla rete terrestre Pechino-Shanghai, lunga duemila chilometri. Progetti analoghi di cablaggio di reti quantistiche a fibra ottica sono anche in corso negli Stati Uniti.

BOX 7: La crittografia quantistica

Per comprendere quali sono i vantaggi della crittografia quantistica è utile riassumere brevemente come funzionano gli attuali sistemi di crittografia. Abbiamo essenzialmente due diversi metodi, il primo dei quali è noto come **crittografia simmetrica** e consiste nello scambio di messaggi cifrati tra due soggetti che sono entrambi in possesso della stessa "chiave" di cifratura. È un sistema molto semplice e veloce, ma ha il problema che la chiave segreta deve essere prima o poi condivisa tra i due soggetti ed esiste dunque un momento in cui un terzo soggetto può intercettare la comunicazione della chiave e impossessarsene.

Il secondo metodo è quello della **crittografia asimmetrica**, in cui il messaggio scambiato tra i due soggetti viene criptato attraverso una chiave pubblica che viene condivisa tra loro (e che dunque può essere intercettata da un terzo) ma viene poi decriptato attraverso un'altra chiave privata di proprietà del solo ricevente, che non ha dunque bisogno di essere scambiata. Essendo un sistema più lento, viene di solito impiegato nella fase iniziale di una comunicazione in crittografia simmetrica, per lo scambio della chiave di cifratura.

La sicurezza della crittografia asimmetrica non è comunque assoluta e si basa sull'elevata complessità computazionale della fattorizzazione in numeri primi, sfruttata dall'algoritmo RSA utilizzato per creare le chiavi pubblica e privata: i sistemi di calcolo attuali impiegherebbero troppo tempo per rompere una chiave RSA-2048 ma questa difficoltà potrebbe in futuro essere superata con l'utilizzo di computer quantistici e un rischio concreto è quello che un attore malintenzionato possa impossessarsi oggi di informazioni sensibili per poterle decriptare nel prossimo futuro.

La **distribuzione quantistica delle chiavi** (*Quantum Key Distribution*, QKD) promette di risolvere questo problema sfruttando l'estrema sensibilità dei sistemi quantistici (i nostri Qubit) alle perturbazioni esterne. L'idea di base è quella di scambiare le chiavi attraverso un flusso di Qubit (tipicamente fotoni su una fibra ottica) in stato di sovrapposizione: qualsiasi tentativo di lettura da parte di un terzo distruggerà lo stato di sovrapposizione dei Qubit e questo evento potrà essere riconosciuto attraverso un controllo incrociato tra i due soggetti coinvolti nella comunicazione della chiave quantistica, effettuato su una frazione dei Qubit (setacciatura della chiave).

Il processo è in realtà un po' più complesso, perché anche le interazioni tra i fotoni e la fibra ottica possono dare origine a fenomeni di decoerenza che corrompono la chiave, cosa di cui si tiene conto attraverso un processo noto come "distillazione della chiave" che consiste nel calcolare se il tasso di errore è sufficientemente alto da far pensare che un hacker abbia cercato di intercettare la chiave, nel qual caso si butta via la chiave e se ne trasmette un'altra, fino ad ottenere una chiave "pulita".

Alla base dell'Internet Quantistico vi sono diverse tecnologie che sfruttano le peculiari proprietà dei sistemi quantistici per realizzare protocolli più affidabili di comunicazione, a cominciare dalla generazione e trasmissione delle chiavi di crittografia fino al "teletrasporto" dei dati.

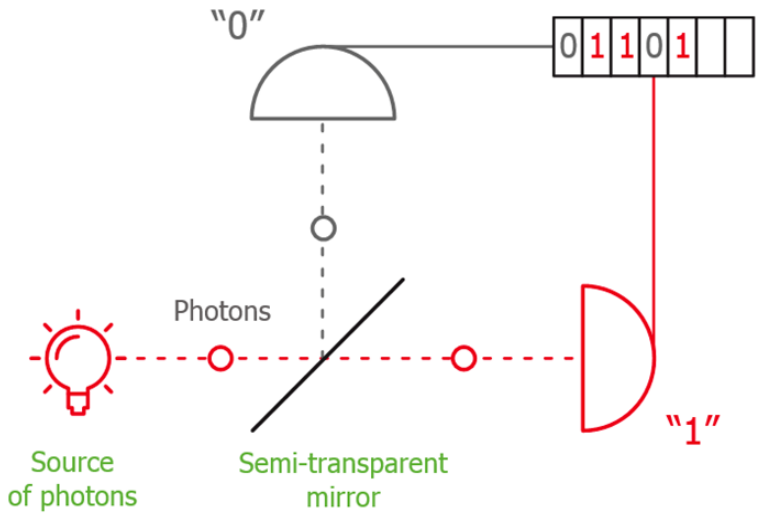
Un mattone fondamentale per queste tecniche è la generazione di **numeri casuali**, utilizzati dai principali algoritmi di crittografia per generare le loro chiavi: l'approccio corrente utilizza metodi matematici che approssimano soltanto un'effettiva causalità dei numeri generati, mentre la struttura fondamentalmente probabilistica dei fenomeni che seguono le leggi della meccanica quantistica offre la possibilità di creare sistemi molto più robusti, come descritto nel Box 7.

BOX 8: Numeri realmente causali

Gli approcci correntemente utilizzati in crittografia non producono numeri veramente casuali (si parla infatti di numeri pseudocasuali): il metodo algoritmico, basato su complesse procedure matematiche, è infatti chiaramente deterministico (conoscendo l'algoritmo e i dati di partenza si potrebbe generare la stessa sequenza di numeri in uscita) e anche molti fenomeni naturali apparentemente causali, come l'andamento del mercato azionario o il rumore della radiazione cosmica, non sono in realtà intrinsecamente tali, si tratta piuttosto di fenomeni complessi, spesso di natura caotica, ma comunque deterministici: chi possedesse una conoscenza molto dettagliata delle condizioni iniziali e dell'ambiente potrebbe infatti prevederne in linea di principio l'andamento, anche se questo può nella realtà risultare praticamente impossibile.

Questo significa che la sequenza dei valori generati dai metodi citati possiede una certa struttura interna, seppure difficilmente individuabile o, detta in altri termini, presenta delle correlazioni che ne fanno abbassare l'**entropia informativa**, intesa come misura della casualità con cui si presentano i diversi valori. Più è basso il valore di entropia di una chiave crittografica, maggiori sono le chance che essa possa essere decriptata, di qui la necessità di mettere a punto metodi di generazione di numeri casuali realmente efficaci.

A differenza dei fenomeni classici, quelli quantistici sono casuali in senso fondamentale, un esempio sono i processi di decadimento radioattivo, come il decadimento beta, in cui il neutrone del nucleo di un elemento chimico si trasforma in protone emettendo un elettrone veloce: Il momento esatto in cui avviene il decadimento non può essere previsto da nessuna legge fisica, è un fenomeno del tutto casuale.



Sistema ottico per la generazione di numeri casuali

Fonte: Adattato da *Quantum Computing for the Quantum Curious*, Springer.com

Un altro fenomeno intrinsecamente casuale è la direzione che prende un fotone quando colpisce uno specchio semiriflettente: il suo essere riflesso o trasmesso è completamente casuale e non può essere influenzato da alcun parametro esterno. Attribuendo ad esempio il valore 1 all'evento "fotone trasmesso" e 0 a quello "fotone riflesso" è possibile generare una stringa di bit casuali.

Vi sono anche altri approcci possibili al *Quantum Random Number Generation* (QRNG), come il già citato decadimento beta, l'effetto tunnel e la computazione quantistica, ma le tecniche di tipo ottico come quella sopra descritta sono al momento le più diffuse e sono alla base delle soluzioni commerciali di aziende come IDQ, Toshiba e Quantum CTek.

I sistemi di generazione di numeri casuali quantistici ad alta entropia sono un componente essenziale per la creazione di algoritmi crittografici in grado di resistere agli attacchi perpetuabili con un computer quantistico. Questi algoritmi sono spesso definiti come **crittografia post-quantistica** (*post-quantum cryptography*, PQC) e si basano su svariati approcci matematici e sono oggetto di una intensa attività di sviluppo e implementazione da parte di molti player dell'informatica, da Google a Microsoft e Apple.

Come abbiamo visto, nella distribuzione quantistica delle chiavi (QKD, vedi Box 6) le chiavi vengono scambiate con metodologie quantistiche ma i dati sottostanti vengono comunque trasmessi sotto forma di bit crittografati attraverso le reti convenzionali. Ciò significa che un hacker che violasse le difese di una rete potrebbe comunque copiare i bit di dati senza essere individuato e poi usare potenti computer per cercare di decifrare la chiave quantistica usata per crittografarli.

Il **teletrasporto quantistico** offre la possibilità di trasferire i dati in modo intrinsecamente sicuro, sfruttando il fenomeno dell'entanglement per trasmettere anche il contenuto informativo del messaggio in modalità quantistica. Anche in questo caso c'è un'informazione ausiliaria di tipo classico che deve essere scambiata tra mittente e destinatario, ma questa, pur essendo indispensabile per decodificare il messaggio inviato, non è di alcuna utilità ad un eventuale hacker. L'informazione quantistica viene infatti resa disponibile, in forma di fotoni entangled con quelli del mittente, solo e soltanto al destinatario e, anche se l'informazione classica che serve al destinatario per leggere questa informazione fosse intercettata, da essa non sarebbe in nessun modo possibile recuperare l'informazione quantistica oggetto della comunicazione tra mittente e destinatario.

Il blocco o l'alterazione dell'informazione classica possono comunque impedire di fatto al destinatario di accedere all'informazione quantistica presente nel suo fotone entangled e in questo sta il principale limite del teletrasporto quantistico, che si accompagna all'attuale limitazione della distanza a cui fotoni entangled possono essere trasmessi su fibra ottica. Ciononostante, si tratta di una tecnica molto promettente e ampiamente sperimentata sia su canali in fibra ottica che in collegamenti da satellite a terra.

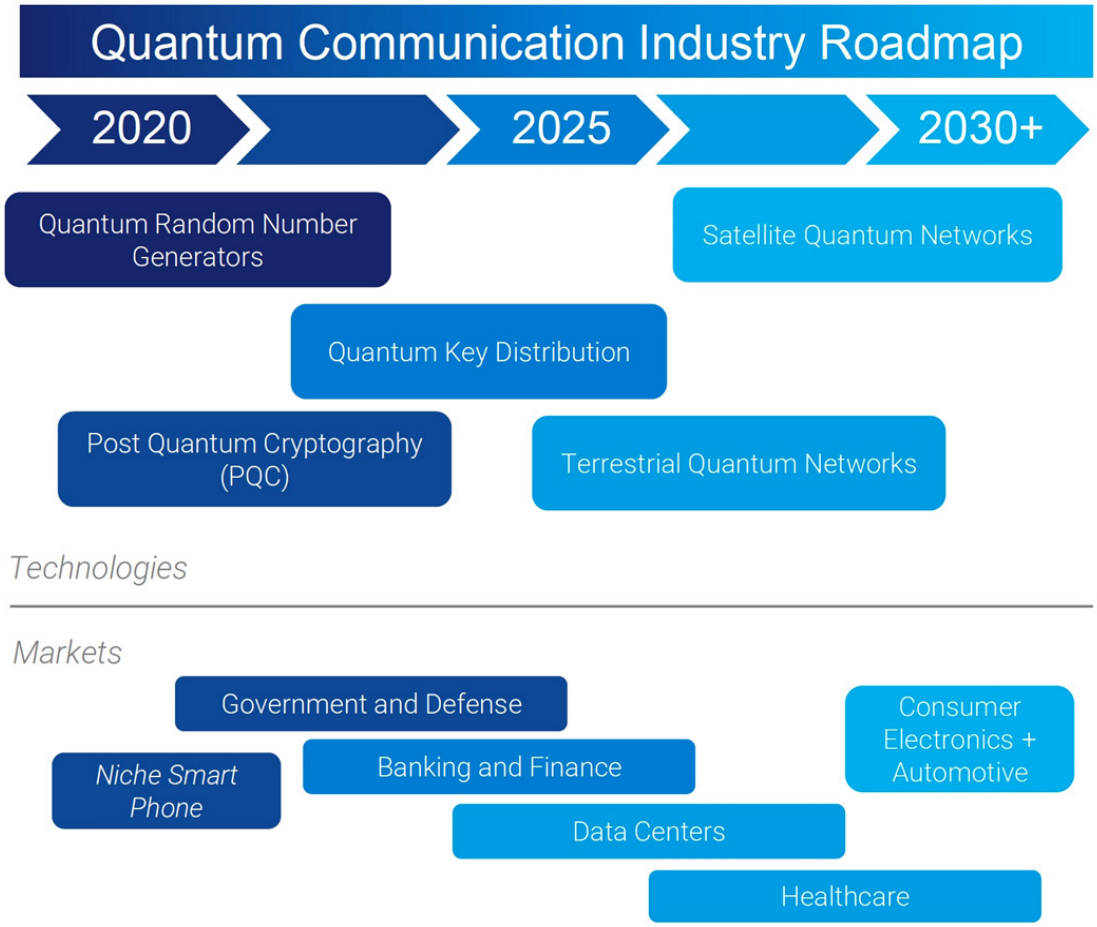
BOX 9: Il meccanismo del teletrasporto quantistico

Il teletrasporto quantistico funziona creando coppie di fotoni entangled e poi inviando uno di questi fotoni (chiamiamolo fotone A) al mittente dei dati e l'altro (fotone B) al destinatario.

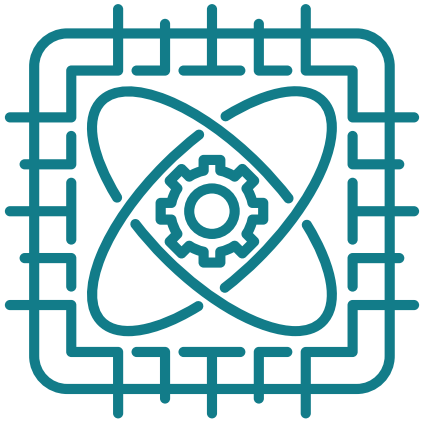
Quando il mittente riceve il suo fotone entangled, lo fa interagire con il Qubit il cui stato codifica l'informazione che vuole trasmettere al destinatario; questa interazione cambia lo stato del suo fotone A e di conseguenza anche lo stato del fotone B del destinatario cambia in maniera analoga, anche se localizzato a migliaia di chilometri.

Dopo questa operazione, l'informazione quantistica risulta dunque virtualmente immediatamente disponibile al destinatario nel fotone B, ed in questo sta il teletrasporto. Tuttavia, affinché il destinatario possa effettivamente recuperare l'informazione dal suo fotone B, ha bisogno che il mittente gli invii i dati delle letture da esso effettuata sul fotone A e sul Qubit, un'informazione di tipo classico che deve comunque essere trasmessa su un canale fisico, salvaguardando così l'impossibilità di inviare segnali a velocità superiori a quella della luce.

Possibile roadmap dell'industria della comunicazione quantistica



Fonte: *Quantum Communication Technology: How Can Physics Protect Our Data Security?*, www.IDTechEx.com



5. TECNOLOGIE QUANTISTICHE, RICERCA E IMPRESA

5.1 NON FARSI COGLIERE IMPREPARATI

Cosa ci insegna il caso dell'Intelligenza Artificiale

Le tecnologie quantistiche, seppure in misura diversa tra loro, sono oggi appannaggio pressoché esclusivo dei laboratori di ricerca delle università, di quelli dei più grandi player del mondo dell'informatica e delle telecomunicazioni e di uno sparuto gruppo di start up.

È abbastanza chiaro che siamo ancora piuttosto lontani, soprattutto per quello che riguarda il *quantum computing*, da uno scenario di diffusione di massa di applicazioni industriali e commerciali *quantum-based* paragonabile a quello a cui assistiamo oggi per l'intelligenza artificiale.

BOX 10: La lunga storia delle reti neurali

Fino a pochissimi anni fa, l'IA era percepita come una tecnologia un po' futuristica, con applicazioni di nicchia nei campi della robotica e del software. Poi nel 2023 è arrivato ChatGPT e l'IA generativa, in grado cioè di generare contenuti di qualsiasi natura - testi, immagini, video, musica o altro - in base a semplici istruzioni discorsive, ha polarizzato l'attenzione del grande pubblico, invadendo le pagine dei giornali e le chat dei social.

Ci siamo improvvisamente resi conto che queste tecnologie possono cambiare - stanno già cambiando - in modo inedito le nostre vite, sia in meglio che in peggio, creando e distruggendo posti di lavoro e facilitando compiti e attività sia lecite che illecite. Grazie al suo impatto immediato, l'IA generativa ha mobilitato l'interesse aziendale e gli investimenti privati, come pure l'attività legislativa degli stati, che si sono ritrovati a dover velocemente riempire un vuoto normativo su aspetti delicati come la privacy e l'uso discriminatorio di queste tecnologie.

È successo tutto molto in fretta, eppure le teorie e gli algoritmi di IA che sono alla base di applicazioni come ChatGPT sono noti da molti anni e hanno una storia piuttosto lunga, iniziata negli anni '40 del secolo scorso con i lavori di McCulloch e Pitts sui modelli computazionali delle reti neurali e di Hebb sull'apprendimento non supervisionato e proseguito poi negli anni '50 da Rosenblatt e altri.

All'entusiasmo iniziale per le reti neurali e l'approccio connessionistico all'intelligenza artificiale subentrò però negli anni '70 una fase di declino, dovuta per un verso alle limitate capacità di calcolo dei computer dell'epoca, non sufficientemente potenti per addestrare le reti neurali, e per l'altro all'emergenza degli approcci cognitivisti all'IA, basati sull'elaborazione simbolica e le regole formali.

Ciò che ha permesso alle reti neurali di ritornare in auge, prima lentamente negli anni '80 e '90 e poi in maniera decisamente esplosiva negli ultimi anni, sono stati i progressi delle tecnologie microelettroniche e dunque dell'hardware di calcolo. Lo sviluppo delle tecnologie dei chip CMOS a larghissima scala di integrazione (VLSI) hanno infatti consentito di realizzare processori sempre più veloci e memorie sempre più capienti, con cui poter simulare reti neurali di complessità crescente.

L'accelerazione registrata nel ventunesimo secolo è anch'essa in gran parte attribuibile ai progressi dell'hardware e soprattutto all'utilizzo di processori ad architettura parallela come le GPU (*Graphical Processing Unit*), originariamente sviluppati per accelerare l'elaborazione delle immagini e utilizzati nei computer, nei cellulari e nelle console per videogiochi. Si tratta di un'evoluzione tuttora in corso, che vede lo sviluppo di processori con architetture non standard, ottimizzati per l'elaborazione di reti neurali, come i processori tensoriali TPU (*Tensor Processing Unit*).

Perché dunque un'impresa di medie o piccole dimensioni di una regione periferica come la Puglia dovrebbe interessarsi a tecnologie così avanzate, la cui diffusione commerciale è proiettata in avanti di almeno una decina di anni? Proprio l'intelligenza artificiale (IA), con la sua storia, può insegnarci qualcosa a questo proposito: l'impennata di interesse e l'esplosione di applicazioni a cui assistiamo in questi anni non è infatti principalmente dovuta a recenti sviluppi teorici ma alla disponibilità di hardware di calcolo sufficientemente potente ed economico, in grado di eseguire in maniera efficiente gli algoritmi di IA, le cosiddette GPU (*Graphical Processing Unit*).

BOX 11: L'altrettanto lunga storia della meccanica quantistica

Anche le tecnologie quantistiche hanno una storia piuttosto lunga, che origina con i lavori pionieristici di scienziati chiave come Max Planck, Albert Einstein, Niels Bohr, Werner Heisenberg ed Erwin Schrödinger, che contribuirono attivamente agli inizi del secolo scorso alla nascita della meccanica quantistica, il framework teorico su cui si fondano l'informatica quantistica e le altre tecnologie quantistiche descritte nei capitoli precedenti.

Se consideriamo che il concetto di livelli di energia quantizzati è stato introdotto da Max Plank nel 1900, l'idea che fosse possibile sviluppare un sistema di calcolo quantistico è emersa piuttosto tardi, all'inizio degli anni '80, grazie a figure chiave come Richard Feynman, Paul Benioff e David Deutsch. La conferenza PhysComp del 1980 ha segnato una tappa significativa in questo percorso, riunendo fisici, informatici e matematici per discutere le potenziali applicazioni della meccanica quantistica al calcolo. Questo incontro interdisciplinare ha facilitato lo scambio di idee e l'esplorazione di nuovi approcci all'informatica quantistica, portando infine alla nascita del campo come lo conosciamo oggi.

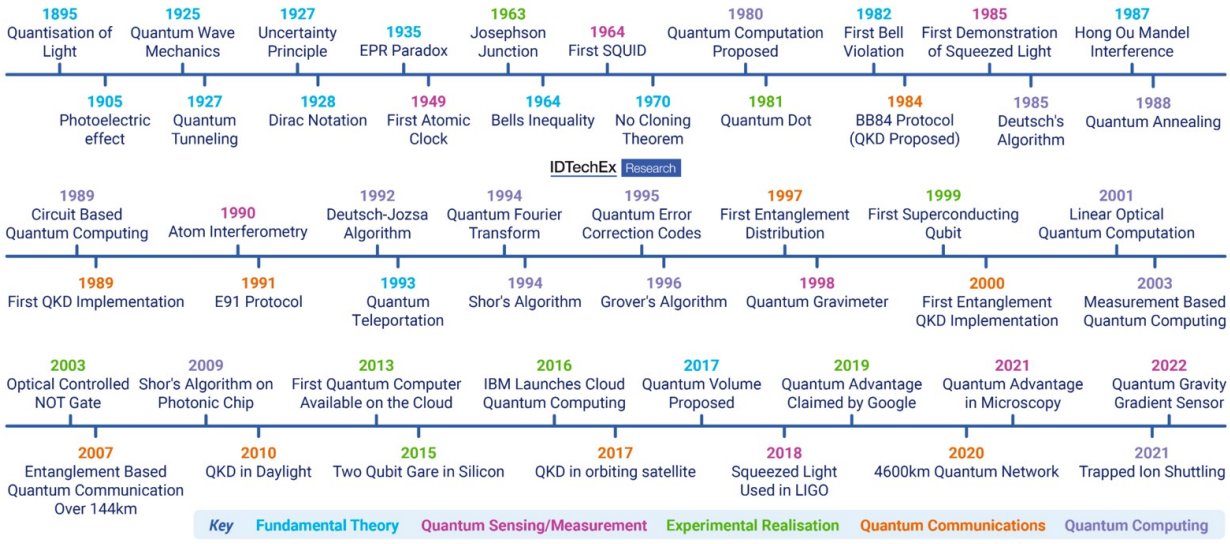
Nel 1982, Paul Benioff, un fisico teorico, pubblicò un articolo che descriveva un modello meccanico quantistico di una macchina di Turing. Questo modello, oggi noto come Macchina di Turing Quantistica (QTM), gettò le basi per i modelli di calcolo quantistico, dimostrando che i principi della meccanica quantistica potevano essere applicati alle basi teoriche del calcolo.

Nel 1985, David Deutsch, un fisico britannico, pubblicò un articolo innovativo che introduceva il concetto di "computer quantistico universale", dimostrando che un tale dispositivo era in linea di principio in grado di eseguire qualsiasi calcolo eseguibile da un computer classico, con i vantaggi aggiunti della meccanica quantistica.

Tra la fine degli anni '80 e l'inizio degli anni '90, i ricercatori hanno proposto diverse porte logiche quantistiche, come la porta CNOT e la porta Toffoli, che sarebbero poi diventate componenti essenziali di algoritmi e circuiti quantistici. La metà degli anni Novanta ha visto progressi significativi nello sviluppo di algoritmi quantistici, che sono metodi di calcolo specializzati progettati per sfruttare le proprietà uniche dei computer quantistici. Il lavoro pionieristico di Peter Shor e Lov Grover in questo periodo ha mostrato le potenzialità dell'informatica quantistica, stimolando l'interesse e gli investimenti nel settore.

Arriviamo così all'oggi, in cui assistiamo a un'intensa gara tra ricercatori, giganti della tecnologia e startup per costruire computer quantistici di uso pratico, utilizzando piattaforme hardware spesso analoghe a quelle impiegate per realizzare sensori quantistici e sistemi per la comunicazione quantistica. Delle numerose sfide tecnologiche ancora aperte abbiamo già detto nelle pagine precedenti: quando, come e in quale misura essere verranno risolte non è facile da prevedere con precisione e di qui nasce la prudenza con cui gli investitori si approcciano al mondo delle tecnologie quantistiche.

Breve storia della quantistica



Fonte: *The Next Five Years of Quantum Technology: Hype vs. Reality*, www.IDTechEx.com

Anche se oggi non sappiamo quando sarà trovato il Sacro Graal del *quantum computing* – l'analogo delle GPU che hanno reso possibile ChatGPT –, il parallelo con la storia dell'IA ci suggerisce però che prima o poi esso salterà fuori e allora l'impatto sarà veramente dirompente, molto più di quello dell'IA generativa, basti pensare alla trasversalità degli ambiti toccati oggi dalle tecnologie ICT e alla loro pervasività e di come queste ultime saranno trasformate dalla rivoluzione quantistica.

Come sta succedendo oggi per l'IA generativa, le imprese che si faranno cogliere impreparate da questo nuovo paradigma tecnologico non saranno in grado di sfruttarne i potenziali benefici e rischieranno di soccombere ai leader di mercato, meglio preparati e attrezzati. Quando questo salto tecnologico avverrà, verosimilmente verso la fine del prossimo decennio o poco più in là, il divario tra chi sarà in grado di padroneggiare e sfruttare appieno le tecnologie quantistiche e chi non lo sarà si tradurrà infatti automaticamente in un divario di ricchezza e potere, sia economico che politico, e questo varrà per le singole imprese come per i territori e gli stati.

La rivoluzione quantistica è insomma una rivoluzione da cui è bene non farsi cogliere impreparati, investendo oggi in infrastrutture di ricerca, tecnologie e, soprattutto, competenze. Come nel caso di altre tecnologie avanzate, chi si muove per tempo può assicurarsi talenti e alleanze che gli consentiranno di avere un grande vantaggio quando le tecnologie quantistiche diventeranno di uso corrente.

Riportiamo a questo proposito una riflessione tratta dalla prefazione di OpenOcean al report "State of Quantum 2024", riferita al quantum computing ma valida per tutti gli ambiti delle tecnologie quantistiche:

> *"[...] c'è un altro livello che richiede attenzione per realizzare pienamente il potenziale dell'informatica quantistica: il livello umano. Abbiamo l'opportunità di rivedere i nostri sistemi educativi: per prepararsi all'era quantistica è necessario che la prossima generazione inizi a pensare in termini quantistici. Una generazione cresciuta nell'era dell'informatica classica dovrà adattarsi e imparare a far funzionare e codificare le macchine quantistiche. [...] Immaginate un mondo in cui gli scolari imparano i principi della sovrapposizione accanto alle teorie della gravità o della luce. Acquisiranno una comprensione dei principi fisici destinati a plasmare le loro vite per i decenni a venire."*

Nel considerare le strategie di preparazione e adattamento a questo scenario di transizione tecnologica va tenuto conto, soprattutto da parte delle imprese di piccole e medie dimensioni, che i sistemi quantistici hanno sempre e comunque bisogno di interfacciarsi con sistemi tradizionali per poter funzionare: un sensore quantistico ha bisogno della sua elettronica di lettura ed elaborazione del segnale, un computer quantistico idem ma anche di un sistema di calcolo classico per la programmazione e post-elaborazione dei dati, e così via.

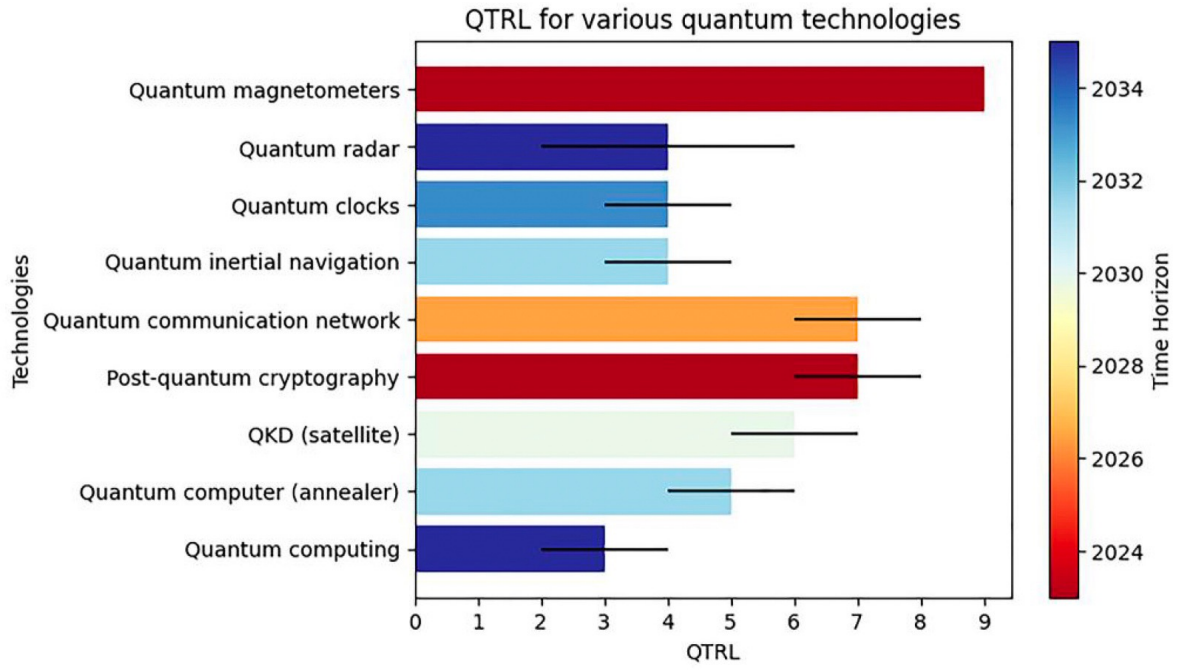
Tenendo anche conto del fatto che per una decina d'anni i sistemi più diffusi saranno di natura ibrida classico-quantistica, è evidente come ci sia ampio spazio per attività di innovazione tecnologica che si svolgano a ridosso della quantistica, senza per questo necessariamente coinvolgere sviluppi nelle tecnologie quantistiche propriamente dette. Per collocarsi con successo in questa filiera è comunque fondamentale che le imprese imparino a parlare il linguaggio delle tecnologie quantistiche, a comprenderne il funzionamento e le problematiche, e dunque ancora una volta torniamo sul tema del capitale umano e delle competenze.

Un'opportunità anche per le PMI

Nonostante i significativi progressi compiuti negli ultimi tempi nel campo dell'informatica quantistica e delle tecnologie quantistiche in generale, rimangono ancora diverse sfide da affrontare, soprattutto sul fronte computing, tra cui la riduzione di peso, ingombro e costi, il miglioramento dei tempi di coerenza dei Qubit, lo sviluppo di architetture di calcolo scalabili e tolleranti ai guasti e la creazione di tecniche pratiche di correzione degli errori. I ricercatori continuano per questo a esplorare nuovi materiali, tecniche e algoritmi e giganti tecnologici come IBM, Microsoft e Google, oltre a numerose startup, continuano a investire pesantemente nella ricerca, alimentando un rapido progresso nel campo.

D'altra parte, lo stato di maturità tecnologica delle diverse tecnologie quantistiche, e dunque il loro livello di vicinanza al mercato, è notevolmente differenziato e vede alcune tipologie di sensori, quali quelli magnetici e di imaging, i sistemi di crittografia post-quantistica e le reti di comunicazione quantistica vicinissime a un'ampia diffusione commerciale, mentre proietta su un orizzonte almeno decennale il *quantum computing* propriamente detto (computer quantistico di uso generale, programmabile e scalabile), con le altre tecnologie in posizioni intermedie, come illustrato nella seguente figura, che fornisce una valutazione degli attuali livelli di maturità tecnologica quantistica (QTRL) per varie tecnologie quantistiche e un orizzonte temporale che indica il tempo previsto per raggiungere un QTRL pari a 9 (con le relative barre di errore), corrispondente a soluzioni messe in opera e utilizzate in applicazioni reali.

QTRL e aspettative di orizzonte temporale (con barre di errore) per diverse tecnologie quantistiche



Fonte: Purohit e altri, *Building a quantum-ready ecosystem*, IET Quantum Communication, DOI: 10.1049/qtc2.12072

La forbice tra *quantum computing* da un lato e *quantum sensing* e *communication* dall'altro è tanto più significativa, in termini di opportunità di mercato, per un Paese come l'Italia che, se non dispone degli *asset* necessari per giocare un ruolo significativo nello sviluppo dell'hardware di calcolo quantistico, è invece ben posizionata, per competenze scientifiche e tecnologiche e capacità industriali, per giocarlo sulla sensoristica e la comunicazione quantistiche, oltre che nello sviluppo di software quantistico.

Sono questi ultimi ambiti che presentano interessanti opportunità di investimento anche per imprese di piccola e media dimensione, ad esempio nell'integrazione di sensoristica quantistica in sistemi per applicazioni biomedicali, aerospaziali o di altra natura, nello sviluppo dell'elettronica di controllo e processamento del segnale, nello sviluppo del software di elaborazione dei dati, eccetera. Perché questo sia possibile è però necessaria la creazione di un "ecosistema quantistico", in cui sapere scientifico, ricerca industriale, formazione delle competenze e politiche pubbliche di sostegno collaborino in maniera strategica.

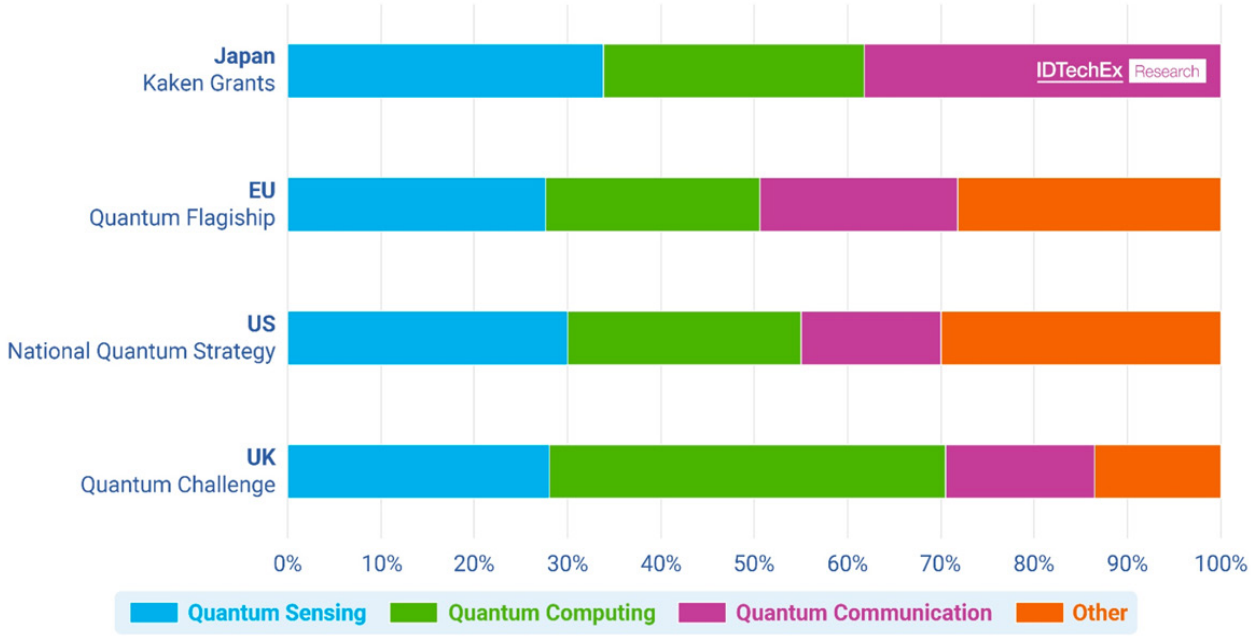
In Puglia esistono le condizioni di base perché questo possa avvenire, a partire dalle competenze del sistema universitario regionale e dalle progettualità di grande respiro in cui esso è correntemente impegnato, di cui diciamo più avanti, e dall'articolato sistema di incentivi alla ricerca e all'innovazione messo a disposizione dalla Regione Puglia: occorre partire di qui per costruire una prospettiva credibile di sviluppo che collochi la regione in una posizione ottimale per intercettare le opportunità che si andranno a delineare in un futuro ormai prossimo, come ad esempio il collegamento all'infrastruttura a fibra ottica Italian Quantum Backbone (IQB) gestita dall'Istituto Nazionale di Ricerca in Metrologia (INRiM), che è previsto arriverà a Matera ma non in Puglia.

5.2 INVESTIMENTI E PROGRAMMI

Gli investimenti privati in tecnologia quantistica hanno raggiunto un massimo di circa 2,5 miliardi di dollari nel 2022, indicando una forte fiducia degli investitori in questo mercato emergente. Tuttavia, nel 2023 gli investimenti sono diminuiti di circa il 50%, facendo parlare di "inverno quantistico", un'idea peraltro confutata da quanti sostengono che il calo sia in linea con le tendenze generali del *venture capital* e non riflette una diminuzione della fiducia nel potenziale della quantistica.

D'altra parte, in forte crescita risultano gli investimenti pubblici dei governi dei principali paesi, per un impegno di spesa stimato di 4-5 miliardi di dollari all'anno per 10 anni, nella forma di ambiziosi programmi nazionali e transnazionali che toccano i diversi ambiti delle tecnologie quantistiche (si veda la figura seguente).

Ripartizione dei finanziamenti governativi nelle diverse tecnologie quantistiche



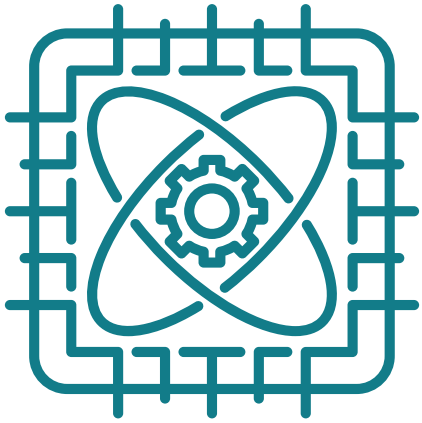
Fonte: *The Next Five Years of Quantum Technology: Hype vs. Reality*, www.IDTechEx.com

L'iniziativa faro europea **Quantum Flagship** è stata lanciata nel 2018 come uno dei più grandi e ambiziosi programmi di ricerca dell'UE, che con un budget di almeno 1 miliardo di euro e una durata di 10 anni, riunisce istituti di ricerca, università, industrie, imprese e responsabili politici, in un'iniziativa congiunta e collaborativa di portata senza precedenti.

L'obiettivo è consolidare ed espandere la leadership scientifica e l'eccellenza europea in quest'area di ricerca, dare il via a un'industria europea competitiva nelle tecnologie quantistiche e rendere l'Europa una regione dinamica e attraente per la ricerca innovativa, le imprese e gli investimenti in questo campo. Gli inviti a presentare progetti si basano sull'agenda strategica di ricerca dell'iniziativa, garantendo così che tutti gli attori siano allineati nel perseguire gli obiettivi dell'iniziativa. Sono attualmente attivi più di 40 diversi progetti, nelle diverse aree coperte dall'iniziativa.

Sul fronte nazionale, il **National Quantum Science and Technology Institute** (NQSTI) è un Partenariato Esteso finanziato dal Piano Nazionale di Ripresa e Resilienza (PNRR) nell'ambito dell'Unione Europea – NextGenerationEU, con l'obiettivo di aggregare le realtà italiane che svolgono una ricerca competitiva e innovativa nel campo della scienza e della tecnologia quantistica (QST) e stimolare l'innovazione industriale in questo campo, fornendo un forum in cui le nuove idee e opportunità vengano trasferite alle aziende.

Una parte significativa delle risorse del progetto, che vede tra i suoi 20 partner l'Università di Bari, diversi enti di ricerca e università e imprese come Leonardo SpA e Thales Alenia Space, è dedicata inoltre a sostenere un programma educativo completo, a favorire il trasferimento tecnologico alle aziende e a implementare un robusto programma di sensibilizzazione per rendere la QST pervasiva nella società.



6. LA PUGLIA PER LE TECNOLOGIE QUANTISTICHE

6.1 L'OFFERTA DI COMPETENZE

Le attività di ricerca sulle tecnologie quantistiche propriamente dette si concentrano in Puglia prevalentemente nell'**Università di Bari** coinvolgendo, attraverso il Dipartimento Interateneo di Fisica, anche docenti e ricercatori del Politecnico di Bari. Considerando invece il più ampio ecosistema di tecnologie di calcolo, sensoristica e processamento del segnale occorre includere anche l'Università del Salento e diversi istituti del CNR, tra cui l'Istituto di Nanotecnologie NANOTEC e quello di Microelettronica e Microsistemi IMM, entrambi localizzati nel campus Ecotekne a Lecce.

La lunga tradizione di ricerca dell'ateneo barese nel campo della fisica quantistica si traduce in un suo notevole protagonismo in diverse iniziative nazionali e internazionali. Nell'ambito del citato Partenariato Esteso NQSTI, l'Università di Bari partecipa in qualità di soggetto affiliato degli *spoke* di seguito riportati:

- Spoke 1 – Elaborazione dell'informazione e Comunicazione, coordinato dall'Università degli studi di Pavia, nel quale UniBa coordina le attività di: 1. Interfacce fra sistemi quantistici; 2. Sistemi quantistici complessi; 3. Risorse quantistiche;
- Spoke 2 – Simulazione, sensoristica e metrologia, coordinato dall'Università degli studi di Camerino, nel quale UniBa coordina le attività di Network quantistici complessi per il trasposto dell'informazione e la sensoristica;
- Spoke 7 – Sistemi completi, coordinato dalla Fondazione Bruno Kessler, nel quale UniBA ha il coordinamento nazionale delle attività sull'*imaging quantistico*;
- Spoke 8 – Trasferimento Tecnologico, coordinato dal CNR;
- Spoke 9 – Educazione e sensibilizzazione, coordinato dall'Università degli studi di Catania.

Università di Bari e **Politecnico di Bari** hanno anche attivo un gruppo di ricerca comune, il Bari Quantum Theory Group, le cui attività coprono un ampio spettro di argomenti nei campi della computazione e della simulazione quantistiche, delle dinamiche quantistiche dell'entanglement e della comunicazione e crittografia quantistiche. Gli stessi atenei partecipano alla Fondazione ICSC, il Centro Nazionale di Ricerca in High-Performance Computing, Big Data and Quantum Computing che svolge attività di ricerca e sviluppo per l'innovazione nel campo delle simulazioni, del calcolo e dell'analisi dei dati ad alte prestazioni.

L'Università di Bari e l'**INFN** hanno altresì un gruppo di ricerca dedicato allo sviluppo delle tecnologie ottiche quantistiche di seconda generazione, caratterizzato da un forte vantaggio competitivo a livello internazionale nel settore del *quantum imaging*, grazie ad un pacchetto di 8 brevetti internazionali incentrati su tecnologie di imaging plenottico ed imaging iperspettrale in correlazione, imaging 3D basato sulla coerenza e dispositivi e procedimenti per il filtraggio spaziale in post-processing. Il gruppo è coinvolto in diversi progetti nazionali (PNRR PE NQSTI, in cui coordina l'attività sul *quantum imaging* a livello nazionale, Passion-PoC-SIMP3D, INFN CSN5 QUISS) ed europei (QuantERA Qu3D, QuantHEP e PACE-IN; EDF Adequade) e sta avviando l'iter per la creazione di una startup nella forma di spinoff universitario congiunto UniBA-INFN, la QPI Systems, volta alla valorizzazione dei brevetti e alla diffusione e commercializzazione dei dispositivi di imaging quantistico.

Una spin-off del Dipartimento Interateneo di Fisica (DIF) di Bari è QSENSATO srl, che mira allo sviluppo, produzione e commercializzazione di chip atomico-fotonici e di sensori atomici quantistici integrati.

Sempre in ambito europeo, il Politecnico di Bari è coinvolto nel progetto Quantum Flagship Quantum Secure Networks Partnership.

L'Università di Bari ha inoltre competenze su applicazioni di calcolo quantistico a problemi di ottimizzazione e simulazione e all'addestramento di reti neurali.

L'Università di Bari sta inoltre organizzando, attraverso il Dipartimento di Fisica:

- La prima edizione del Master di II livello in Quantum Science and Technology[2], ideato in compartecipazione con esperti internazionali e a numerosi partner aziendali e di ricerca[3], con l'obiettivo di creare un ponte tra l'Università e le imprese e favorire l'attrazione e la formazione di giovani talenti che possano contribuire alla creazione di un ecosistema quantum in Puglia e in Italia. Il Master copre tutti i pilatri del progetto Flagship sulle Quantum Technologies dell'Unione Europea, è aperto a laureati in discipline STEM ed è altamente specializzante, con corsi incentrati su casi d'uso di interesse industriale, una predominanza di attività pratiche e laboratoriali, uno stage di 4 mesi basato su progetti ad alto impatto tecnologico, interventi e supporto da parte di aziende specializzate nel quantum (Xanadu, Qureca, e molte altre), borse di studio finanziate da partner aziendali nonché un forte interesse all'assunzione dei giovani tirocinanti da parte delle aziende partner.
- La seconda edizione della Summer School Quantum, dedicata alle scienze e tecnologie quantistiche, che si terrà a Bari dal 16 al 20 settembre 2024[4]; la prima edizione, tenutasi a Trani nel 2022, finanziata dalla Regione Puglia, ha visto la partecipazione di oltre 140 laureandi, dottorandi e giovani ricercatori da tutto il mondo, attratti dal nostro territorio e dal programma di eccellenza reso possibile dalla partecipazione di docenti di alto calibro e di fama internazionale[5]. La Summer School è ispirata all'omonimo workshop (From Foundations of Quantum Mechanics to Quantum Information and Quantum Metrology & Sensing) organizzato con cadenza biennale dall'Università di Torino in collaborazione con l'Università di Bari, ormai alla 10ª edizione, capace di attrarre oltre 300 scienziati.

2 www.masterquantum.it

3 Lutech, Leonardo, Planetek Italia, GAP, Quantum Telecommunications Italia, Exprivia, OptoprimQreca, Quside technologies, Quandela, LuxQuanta Technologies, Xanadu, GEM elettronica, CNR-INO

4 https://agenda.infn.it/event/39737/

5 https://agenda.infn.it/event/21449/

Ci si aspetta che entrambe queste iniziative di eccellenza rendano l'Università di Bari e il territorio un punto di riferimento nel quadro internazionale e ne favoriscano l'attrattività e quindi la crescita.

Il **CNR NANOTEC**, che ha a Lecce la sua sede principale, sviluppa attività di ricerca fondamentale e applicata in nanoscienze e nanotecnologie, tra cui quelle legate alla fotonica avanzata, nel cui ambito sono studiati e sviluppati sistemi quantistici integrati in dispositivi a semiconduttore, sia di tipo classico che ibridi organici-inorganici, con possibili ricadute nella realizzazione di porte quantistiche, di transistor ottici e di reti neurali. L'istituto è parte del partenariato esteso NQSTI e della rete di infrastrutture di ricerca PNRR I-PHOQS[6] (Integrated Infrastructure Initiative in Photonic and Quantum Science), che mette in connessione strutture di eccellenza nei settori strategici della Fotonica, delle Nanotecnologie e delle Tecnologie Quantistiche. L'istituto dispone di importanti facility di ricerca e laboratori, tra cui una camera pulita per la realizzazione di dispositivi a semiconduttore e sensori, ed è molto attivo nei programmi europei.

A livello privato, particolarmente attive sono la Planetek Italia Srl e l'azienda del gruppo Planetek Hellas EPE, che hanno sviluppato attività e collaborazioni con l'Università di Bari su acquisizione ed elaborazione dati per quantum imaging.

Considerato che anche in altri atenei e centri di ricerca pugliesi si svolgono attività di ricerca con potenziali ricadute in ambito quantistico (ad esempio su sensoristica e calcolo), risulta evidente come la Puglia abbia tutte le carte in regola per partecipare a questa importante sfida tecnologica, sia sul fronte della ricerca che su quello industriale.

6.2 TECNOLOGIE QUANTISTICHE E FILIERE REGIONALI

La Strategia di Specializzazione Intelligente (S3) della Regione Puglia SmartPuglia2030 individua, in un quadro generale caratterizzato da sfide sociali prioritarie e macro-driver dell'innovazione, dieci filiere regionali dell'innovazione, per ciascuna delle quali sono definiti le principali aree di innovazione e le relative priorità tecnologiche.

Considerando le tecnologie quantistiche come un elemento di un'ecologia più ampia di tecnologie con cui esse si andranno ad integrare, sia da un punto di vista strettamente sistemistico che da quello delle applicazioni finali, è possibile tracciare una mappa dei possibili impatti sulle filiere regionali, come delineato nella tabella seguente.

Delle dieci filiere individuate nella S3 restano fuori dalla tabella quella relative ai settori più tradizionali del Made in Italy, quali l'agroalimentare, il sistema casa (mobilio e costruzioni), il sistema moda (tessile, abbigliamento e calzature), l'industria culturale del turismo, non direttamente impattate dalle tecnologie quantistiche.

Per le altre filiere - meccatronica, automotive, aerospazio, salute, energia e ambiente e servizi avanzati - la tabella individua, per ciascuna sottoclasse tecnologico/applicativa del calcolo, della sensoristica e della comunicazione quantistiche, i possibili ambiti di applicazione.

Una lettura orizzontale della tabella, per aree di applicazione, evidenzia come la disponibilità di sistemi di calcolo ibridi classico-quantistici in grado di velocizzare gli algoritmi di simulazione di sistemi complessi e

6 https://www.i-phoqs.eu

quelli di intelligenza artificiale (legati ad esempio a compiti di apprendimento automatico, manutenzione predittiva o guida autonoma) possa impattare la quasi totalità delle filiere citate. Similmente, i sistemi di analisi di immagine basati su imaging quantistico possono trovare larga applicazione nell'ispezione industriale e nella diagnostica, un ambito quest'ultimo in cui possono giocare un ruolo di rilievo anche i sensori magnetici quantistici, utili anche in applicazioni di monitoraggio ambientale ed osservazione della terra.

Data la pervasività del tema della sicurezza delle comunicazioni, i sistemi di crittografia quantistica e, più in generale, la disponibilità di un Internet quantistico potranno impattare trasversalmente i più diversi settori industriali regionali.

Si tratta di una mappatura provvisoria e sicuramente incompleta, utile a stimolare il confronto tra i player industriali regionali e il sistema della ricerca, che verosimilmente aiuterà a meglio delineare i possibili scenari di sviluppo della rivoluzione quantistica in Puglia.

Aree di impatto delle tecnologie quantistiche sulle filiere regionali

	MECCANICA AVANZATA, ELETTRONICA E AUTOMAZIONE	AUTOMOTIVE	AEROSPAZIO	INDUSTRIA DELLA SALUTE	SISTEMI ENERGETICI E AMBIENTALI	SERVIZI AVANZATI
QUANTUM COMPUTING						
CALCOLO AD ALTE PRESTAZIONI			fluidodinamica, analisi materiali			cloud computing, big data, quantum algorithms
OTTIMIZZAZIONE PROBLEMI COMPLESSI						pianificazione logistica
SIMULAZIONE	simulazione industriale, digital twin				simulazione industriale, digital twin	
APPLICAZIONI AVANZATE DI IA	apprendimento automatico, manutenzione predittiva	apprendimento automatico, manutenzione predittiva, guida autonoma		sistemi di supporto alle decisioni	manutenzione predittiva	logistica intelligente, data mining, data analytics, apprendimento automatico, sistemi di supporto alle decisioni

Aree di impatto delle tecnologie quantistiche sulle filiere regionali

	MECCANICA AVANZATA, ELETTRONICA E AUTOMAZIONE	AUTOMOTIVE	AEROSPAZIO	INDUSTRIA DELLA SALUTE	SISTEMI ENERGETICI E AMBIENTALI	SERVIZI AVANZATI
QUANTUM SENSING						
RILEVAZIONE ANOMALIE MAGNETICHE	sistemi diagnostici		osservazione della Terra	imaging medicale, diagnostica medica	monitoraggio ambientale	
IMAGING QUANTISTICO AD ALTA RISOLUZIONE	ispezione industriale			imaging medicale, microscopia 3D		
APPLICAZIONI LIDAR/RADAR			navigazione, osservazione della Terra			
SPETTROSCOPIA						
RILEVAZIONE CAMPI GRAVITAZIONALI			navigazione, osservazione della Terra		monitoraggio ambientale	
QUANTUM COMMUNICATION						
CRITTOGRAFIA QUANTISTICA		sicurezza informatica				
QUANTUM INTERNET	connettività avanzata				connettività avanzata	

GLOSSARIO

Algoritmo
Lo possiamo definire come un insieme di istruzioni precise per eseguire, in un numero finito di passi e seguendo un insieme finito di regole, un determinato compito. In campo informatico questo si traduce come un insieme di istruzioni eseguite da un computer.

Caso d'uso
Si tratta di una espressione usata nell'ingegneria del software per rappresentare le funzionalità complessive di un sistema, specificando le modalità con cui degli attori esterni (esseri umani o altri sistemi) interagiscono con esso. Per estensione, la descrizione funzionale di una applicazione.

Cifratura
È un procedimento che consente di trasformare un messaggio espresso "in chiaro" e dunque leggibile da chiunque, in un messaggio espresso in un formato non immediatamente leggibile da chi non conosce la procedura di cifratura. Un esempio è quello della trasformazione di ogni lettera dell'alfabeto in una cifra numerica, utilizzando un algoritmo di cifratura.

CMOS
Una tecnologia di fabbricazione di circuiti integrati a larghissima scala di integrazione (VLSI), basata sull'impiego di transistor MOS (Semiconduttore a Ossido Metallico) di tipo complementare, che a partire dagli anni '80 ha consentito di realizzare microprocessori, memorie e sensori ottici.

Connessionismo
Un approccio alla progettazione di sistemi intelligenti basato sull'emulazione delle reti neurali umane, costituite da numerosi componenti di base (i neuroni) collegati tra loro da un grande numero di connessioni (le sinapsi) e organizzati in una gerarchia di sottosistemi. Secondo questo approccio, il comportamento intelligente non è frutto di un'elaborazione di tipo simbolica (come vuole il cognitivismo), ma emerge spontaneamente dall'interazione dei componenti elementari nei sottosistemi e dei sottosistemi tra loro.

Correlazione
È una relazione tra due grandezze (o variabili), per cui il comportamento di una di esse presenta una corrispondenza di qualche tipo con il comportamento dell'altra. In statistica, il coefficiente di correlazione misura il grado con cui una variabile tende a variare in funzione di un'altra.

Criogenia
Tecnologia per generare e utilizzare temperature molto basse, tipiche della liquefazione di gas come l'azoto (-196 C° = 77 K). Ha una vasta gamma di applicazioni in fisica, chimica, medicina, ingegneria.

Discreto (stato)
Si dice di uno degli stati appartenenti a una collezione finita di stati possibili tra cui un sistema può transitare. Un sistema del genere si dice appunto discreto, per distinguerlo da un sistema continuo o analogico, che può assumere stati che variano con continuità. Molti sistemi quantistici sono discreti, ad esempio un elettrone in un atomo può assumere un numero finito di valori discreti di energia.

Distribuzione di probabilità
La funzione matematica che esprime la probabilità con cui si manifestano i diversi possibili risultati di un esperimento. A seconda del tipo di esperimento, la distribuzione di probabilità può essere continua oppure

discreta. Nel caso del lancio di una monetina, ad esempio, i risultati possibili dell'esperimento sono solo due, testa o croce, e avremo dunque una distribuzione di probabilità discreta.

Elettromagnetico (campo)

I campi elettrici e magnetici sono intimamente connessi. Sappiamo tutti che facendo fluire una corrente elettrica in una bobina di filo conduttore possiamo generare un campo magnetico: è questo il principio alla base dell'elettrocalamita, che troviamo nel meccanismo dell'apriporta e del relais. Se d'altra parte facciamo ruotare una bobina di filo conduttore in un campo magnetico generato da calamite fisse possiamo generare un flusso di corrente nella bobina, e questo è il principio con cui funzionano la dinamo della bicicletta e l'alternatore dell'automobile. Più in generale, la continua generazione reciproca tra un campo magnetico e un campo elettrico, dovuta all'accelerazione di cariche elettriche in una data regione di spazio, genera un campo elettromagnetico, che può propagarsi nello spazio in forma di onde elettromagnetiche, che viaggiano nel vuoto alla velocità della luce. La frequenza di oscillazione di queste onde determina come questa radiazione interagisce con la materia e come noi la percepiamo, passando dalle onde radio alle microonde, alla luce infrarossa (che percepiamo come calore), alla luce visibile, alla luce ultravioletta ai raggi X e ai raggi gamma. La meccanica quantistica associa al campo elettromagnetica una particella indivisibile, di massa zero, che è il fotone, la cui energia è tanto più alta quanto più alta è la frequenza del campo.

Elettrone

È il quanto elementare di carica elettrica negativa, una particella leggera che può essere legata ad un atomo, trattenuto dall'attrazione esercitata dai protoni carichi positivamente del nucleo, o essere libero, generando ad esempio una corrente elettrica in un conduttore. Di massa molto piccola se confrontata con quella dei neutroni e dei protoni che costituiscono il nucleo atomico, gioca un ruolo fondamentale nel determinare le proprietà chimiche degli atomi. L'elettrone si comporta come una piccola trottola, avendo associato a sé un "momento" magnetico intrinseco (detto spin) e quando è in movimento genera un campo magnetico, mentre la sua accelerazione o variazioni della sua energia provocano l'emissione di fotoni.

Fonone

In un solido cristallino gli atomi sono disposti regolarmente, ai vertici di un reticolo tridimensionale. Queste posizioni non sono però fisse, in quanto l'interazione del cristallo con una forma di energia esterna, nella forma di una radiazione, può causare lo spostamento di uno o più atomi dalla loro posizione di equilibrio, generando oscillazioni che si propagano all'interno del cristallo. È stato osservato che queste oscillazioni potevano essere descritte come sovrapposizioni di quanti fondamentali di vibrazione meccanica, chiamati fononi, in analogia con i fotoni della radiazione luminosa, con cui condividono il dualismo onda-particella. I fononi giocano un ruolo importante in molti fenomeni della fisica dei solidi, come la conduzione termica ed elettrica e la superconduttività.

Fotone

La scoperta che l'energia trasportata da un'onda elettromagnetica è proporzionale alla sua frequenza, fatto alla base dell'effetto fotoelettrico, per cui la separazione di un elettrone dal proprio atomo dipende esclusivamente dalla frequenza della radiazione che lo colpisce e non dalla sua intensità, ha portato a formulare l'ipotesi che l'energia del campo elettromagnetico fosse "quantizzata", cioè composta da quantità discrete (quanti) di energia, denominati fotoni. Un fotone esibisce sia una natura corpuscolare (i fotoni possono essere rivelati uno alla volta e contati) che ondulatoria (essi hanno associata una lunghezza d'onda e possono dar luogo a fenomeni di interferenza tra loro), possiede massa nulla e si muove sempre alla velocita della luce (la massima velocità possibile in natura) nel vuoto.

Giroscopio

Una semplice trottola che ruota velocemente intorno al proprio asse tende a mantenere stabile la posizione

dell'asse nello spazio, nel senso che se proviamo con un colpetto a inclinarlo esso ritorna nella posizione iniziale. Questo avviene per una legge fisica detta "di conservazione del momento angolare" ed è sfruttata per costruire dispositivi in cui la parte rotante è sospesa in una struttura fissa e lasciata dunque libera di orientarsi nello spazio. I giroscopi trovano molte applicazioni, ad esempio come bussole che indicano il nord geografico piuttosto che quello magnetico e nei sistemi di navigazione inerziale dei satelliti e delle sonde spaziali.

Interferenza

Se gettiamo un sasso in uno specchio di acqua tranquillo possiamo osservare le onde che si propagano in forma di anelli circolari a partire dal punto di impatto del sasso con l'acqua. Se adesso lanciamo un secondo sasso potremo vedere come le onde generate dall'impatto dei due sassi creano delle figure complesse nei punti in cui si incontrano, sommandosi tra loro se sono in fase, sottraendo le loro ampiezze se non lo sono. Questo fenomeno interessa tutte le grandezze di tipo ondulatorio, come ad esempio la luce, ed è chiamato in fisica interferenza. Data la natura duale onda-corpuscolo di tutte le particelle elementari, il fenomeno di interferenza interessa anche particelle come gli elettroni.

Ione

Un atomo è un sistema composto da un ugual numero di protoni (carichi positivamente) ed elettroni (carichi negativamente), più un certo numero di neutroni, elettricamente neutri. Il bilanciamento delle cariche fa sì che l'atomo sia elettricamente neutro. La sottrazione o l'aggiunta di uno o più elettroni all'atomo altera questo equilibrio elettrico e l'atomo elettricamente carico viene definito ione. Gli ioni negativi vengono detti anioni e quelli positivi cationi.

Laser

Il termine laser è un acronimo inglese che sta per "amplificazione della luce tramite emissione stimolata di radiazione". Si tratta di un dispositivo che produce un fascio di luce monocromatico e ben collimato, in grado di concentrare un'elevatissima potenza in un'area molto piccola, rendendolo così utile a moltissime applicazioni, da quelle chirurgiche al taglio dei metalli, all'interferometria, allo studio dell'interazione della radiazione con la materia. La monocromicità della luce laser e la sua capacità di viaggiare lungo fibre ottiche senza subire forti attenuazioni la rende inoltre idonea per trasportare grandi quantità di informazioni.

Lidar

Il lidar è un radar ottico, che invece di utilizzare microonde impiega luce laser. Poiché la luce laser ha una lunghezza d'onda molto più piccola di quella delle microonde ed è emessa in fasci molto più stretti e collimati, i lidar consentono misure più precise e con una maggiore risoluzione spaziale dei radar.

Navigazione inerziale

Utilizzata sia nella navigazione marittima che in quella aerea, è una tecnica che consente di ricavare informazioni su posizione, velocità e accelerazione del veicolo, senza utilizzare riferimenti esterni o collegamenti radio. Un sistema di questo tipo utilizza giroscopi e accelerometri per calcolare la posizione e la velocità aggiornate del veicolo, a partire da una condizione nota di partenza, senza bisogno di ulteriori informazioni esterne. Essendo basati sulle informazioni fornite dai loro sensori e sui calcoli eseguiti su di esse, questi sistemi tendono nel tempo ad accumulare errori e necessitano di periodici riallineamenti, operati ad esempio con un sistema GPS.

Ottimizzazione

Nei problemi matematici di ottimizzazione, si ricerca il valore massimo o minimo di una funzione che rappresenta il problema che si vuole risolvere. A seconda del problema di ottimizzazione affrontato, la funzione di cui si vogliono trovare i valori migliori possibili (detta funzione obiettivo) può dipendere da molte variabili e la ricerca dei suoi massimi e minimi divenire difficile o impossibile in maniera esatta: in

questi casi si usano tecniche di calcolo numerico per risolvere il problema in maniera approssimata, con l'utilizzo del computer.

Parallelo (calcolo)

Si parla di calcolo parallelo quando un algoritmo, debitamente diviso e adattato, viene eseguito da più processori che lavorano contemporaneamente, una tecnica utilizzata per velocizzare i tempi di calcolo e che si presta particolarmente bene all'accelerazione di diverse classi di processi computazionali, come il rendering grafico, l'editing video, il machine learning e la simulazione di sistemi complessi. Un esempio di processori con architettura interna parallela sono le GPU (Graphical Processing Unit) utilizzate nelle schede grafiche dei PC, oggi largamente impiegate nell'implementazione delle reti neurali. Anche i supercalcolatori utilizzano architetture parallele per conseguire le loro prestazioni di supercalcolo.

Quanto

In fisica il termine quanto è usato sia per riferirsi al valore più piccolo possibile, dunque indivisibile, di una grandezza che può assumere solo valori discreti, che per designare la particella elementare (dunque indivisibile) associata ad un certo campo di forze; ad esempio il quanto del campo elettromagnetico è il fotone.

Radar

Il radar è un dispositivo di rivelazione e localizzazione di oggetti basato sull'emissione di radioonde e sull'analisi della loro riflessione da parte dell'oggetto stesso. Con esso è possibile misurare distanza, posizione angolare e velocità degli oggetti inquadrati dal fascio di microonde.

Rete neurale

Nella sua accezione biologica, una rete neurale è una rete in cui un certo numero di neuroni sono tra loro fittamente interconnessi al fine di svolgere una determinata funzione. Caratteristica peculiare delle reti neurali biologiche è la capacità di apprendere, basata sul rinforzo delle connessioni tra neuroni (sinapsi). Una rete neurale artificiale è un modello computazionale in cui i singoli neuroni sono unità di calcolo che eseguono specifiche elaborazioni sui dati in ingresso, inviando il proprio output ad altri neuroni o all'uscita della rete. I neuroni possono essere organizzati in strati, ad esempio uno strato di ingresso, uno nascosto e uno di uscita, e la modulazione delle connessioni è realizzata cambiando i pesi delle connessioni secondo determinati algoritmi, in relazione alle informazioni in ingresso o agli output dei neuroni, realizzando così un sistema adattivo in grado di apprendere.

Scalabile (computer)

La scalabilità è un concetto ampiamente utilizzato in informatica per designare la capacità di un sistema (sia hardware che software) di gestire quantità crescenti di lavoro attraverso un aumento delle sue risorse hardware o software. Un esempio banale è la possibilità di aggiungere altra memoria RAM e un disco rigido esterno a un personal computer, in questo caso una scalabilità limitata alle risorse di memoria. Per un computer quantistico, la sua scalabilità consiste nella capacità di espanderne le risorse interne (Qubit, porte ecc.) al livello necessario a risolvere problemi sempre più grandi e complessi.

Semiconduttori

I semiconduttori sono materiali con proprietà intermedie tra quelle degli isolanti e quelle dei conduttori, che rendono possibile la creazione di strutture composte da semiconduttori di diversa natura e dotate di particolari caratteristiche elettriche. Un esempio è il diodo, un dispositivo che, in un certo intervallo di valori di tensione applicata, si comporta come un conduttore per la corrente che lo percorre in un verso e come un isolante per la corrente che vorrebbe percorrerlo nel verso opposto. Un altro dispositivo, fondamentale per la realizzazione dei circuiti integrati con cui sono ad esempio realizzati i nostri computer, è il transistor, una sorta di valvola elettronica che permette di modulare l'intensità del flusso di corrente tra due terminali

in base alla tensione applicata su un terzo terminale di controllo. Esempi di materiali semiconduttori sono il germanio, il silicio, l'arseniuro di gallio.

Sonar
Il sonar è sostanzialmente un radar acustico, usato in ambito marittimo per localizzare oggetti sommersi tramite l'emissione di ultrasuoni e l'analisi delle loro riflessioni.

Spettro (di frequenze)
Data una grandezza di tipo oscillatorio, ad esempio il suono o la luce, con spettro di frequenze ci si riferisce all'insieme di tutte le frequenze comprese tra un limite inferiore e uno superiore. Ad esempio lo spettro delle frequenze sonore udibili dall'uomo è all'incirca compreso tra 20 Hz (cicli al secondo) e 20 KHz, quello delle radiazioni elettromagnetiche visibili va invece da 428 THz (migliaia di miliardi di Hz) a 749 THz. A volte per qualificare uno spettro invece dei valori di frequenza f espressi in Hertz si usano le corrispondenti lunghezze d'onda λ espresse in unità di misura lineari, laddove $\lambda=v/f$, con v pari alla velocità di propagazione dell'onda.

Spin
"To spin" significa ruotare in inglese e lo spin è una grandezza che la meccanica quantistica associa alle particelle elementari e che richiama in qualche modo la rotazione di queste intorno al proprio asse. Si tratta tuttavia di una grandezza squisitamente quantistica, che per l'elettrone può valere solo ± 1/2 e per un fotone ± 1.

Superconduttività
La superconduttività è un fenomeno fisico che si manifesta in alcuni materiali, come metalli e leghe, quando questo sono portati a temperature inferiori a un certo valore di soglia, detto temperatura critica, spesso estremamente basso, consistendo nell'azzeramento della resistenza elettrica. Una corrente iniettata in un superconduttore può così circolare teoricamente all'infinito, anche se la tensione che l'ha generata viene rimossa, senza peraltro i fenomeni dii dissipazione di calore che si generano a causa della resistenza elettrica. Questo permette ad esempio di realizzare i grandi e potenti elettromagneti impiegati negli acceleratori di particelle, come pure di realizzare i magnetometri SQUID usati nella diagnostica medica. Il limite principale di questa tecnologia è il costo, l'ingombro e il consumo dei sistemi di raffreddamento necessari a mantenere il materiale superconduttore a temperature criogeniche, ad esempio con elio liquido a -170C°.

Turing (macchina di)
La macchina di Turing è un modello di calcolo proposto dall'omonimo scienziato nel 1936, che riduce qualsiasi algoritmo all'esecuzione di operazioni elementari di lettura e scrittura operati da una testina che scorre su un nastro di lunghezza infinita diviso in caselle. La congettura di Church-Turing postula che per ogni funzione calcolabile esista un'equivalente macchina di Turing, la cui esistenza può dunque essere utilizzata come criterio per stabilire la calcolabilità di un problema matematico.

Zero assoluto (temperatura)
La temperatura minima possibile a cui può trovarsi un sistema fisico, pari a -273,15 C°. Nella scala Kelvin la temperatura di -273,15 C° corrisponde al valore 0 K.

PER APPROFONDIRE

MECCANICA QUANTISTICA

Chi volesse cimentarsi in uno studio sistematico degli elementi di base della meccanica quantistica, non meramente qualitativo ma pur sempre di livello intermedio, può fare riferimento all'ottimo:

- Leornard Susskind, Art Friedman, Meccanica quantistica, Raffaello Cortina Editore

QUANTUM COMPUTING

Per un'introduzione elementare al quantum computing, pensata per studenti liceali:

- Quantum Computing as a High School Module, https://arxiv.org/pdf/1905.00282.pdf

Un testo di livello intermedio, adatto a studenti e professionisti nel campo delle discipline STEM (scaricabile gratuitamente, ma con alcuni refusi):

- David McMahon, Quantum Computing Explained, John Wiley & Sons, 2008, https://www.academia.edu/31537353/_David_McMahon_Quantum_Computing_Explained_BookFi_1_

Un'utile rassegna sullo stato dell'arte del quantum computing:

- State of Quantum 2024 Report, https://meetiqm.com/technology/state-of-quantum-report-2024/

Articoli e risorse su vari aspetti e problematiche del quantum computing:

- A Brief History of Quantum Computing, https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0
- John Preskill, Quantum Computing in the NISQ era and beyond, https://quantum-journal.org/papers/q-2018-08-06-79/
- Fabio Sanches, Application-Specific Quantum Hardware is the Most Promising Approach for Early Practical Applications, https://medium.com/bleximo/application-specific-quantum-hardware-is-the-most-promising-approach-for-early-practical-a1fd7604699a
- Roads to Quantum Advantage, https://ianhellstrom.org/roads-to-quantum-advantage/
- Wei Wu e altri, Quantum computing and simulation with trapped ions: On the path to the future, https://www.sciencedirect.com/science/article/pii/S2667325820300121

Sulle applicazioni del quantum computing:

- Top 20 Quantum Computing Use Cases & Applications in 2024, https://research.aimultiple.com/quantum-computing-applications/
- Ignacio Cirac, Quantum computing and simulation, https://www.degruyter.com/document/doi/10.1515/nanoph-2020-0351/html

QUANTUM SENSING

Sulle diverse tipologie di sensori quantistici e le loro applicazioni:

- Degen, Reinhard, Cappellaro, Quantum Sensing, Rev. Mod. Phys. 89, 2017, https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.89.035002

- Quantum Sensors in '24: Best 8 Use Cases & Case Studies, https://research.aimultiple.com/quantum-sensors/
- Aslam e altri, Quantum sensors for biomedical applications, https://www.nature.com/articles/s42254-023-00558-3
- Advancements in Types of Quantum Imaging, https://andor.oxinst.com/learning/view/article/advancements-in-types-of-quantum-imaging

Per una analisi delle potenzialità di mercato del quantum sensing vedi:

- Making Sense of Quantum Sensing, https://www.bcg.com/publications/2023/making-sense-of-quantum-sensing
- Quantum Sensing and its Value: A Brief Overview, https://thequantuminsider.com/2023/05/03/quantum-sensing-and-its-value-a-brief-overview/
- Quantum Sensors vs. Quantum Computers: IDTechEx Takes a Look at the Next 10 Years, https://www.microwavejournal.com/articles/print/41137-quantum-sensors-vs-quantum-computers-idtechex-takes-a-look-at-the-next-10-years?gad_source=1&gclid=CjwKCAiA0PuuBhBsEiwAS7fsNV-YkNApevtcE1BiH7UsAGBwseYDWiPH-WML1GYpIv7GiFxuDpNVmhoC7ngQAvD_BwE

QUANTUM COMMUNICATION

- Martin Giles, MIT Technology Review, Explainer: What is quantum communication?, https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/
- Guerra, Valvo, Quantum Commmunication in pratica: tecnologie e applicazioni, TIM, https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/2020/2020-2/cap05_Quantum-Communication-pratica-%20tecnologie-applicazioni.pdf
- Boella, Rossotto, Quantum Commmunication: i primi passi verso la Quantum Internet, TIM; https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/2020/2020-2/cap04_quantum-communication-primi-passi.pdf

PROGRAMMI E INIZIATIVE

- UE Quantum Flagship, https://qt.eu/about-quantum-flagship/
- QuantERA, https://quantera.eu
- National Quantum Science and Technology Institute, https://nqsti.it/
- ICSC, Centro Nazionale di Ricerca in High Performance Computing, Big Data e Quantum Computing, https://www.supercomputing-icsc.it/
- Bari Quantum Theory Group, https://www.quantumbari.com
- Bari Quantum Optical Technologies Lab, https://www.quotlab.uniba.it

ARTI Technology Focus Report è la collana editoriale che l'Agenzia dedica agli approfondimenti sulle tecnologie emergenti, sui loro ambiti di applicazione e sul potenziale innovativo per il territorio regionale.

Data di rilascio: agosto 2024

ISBN: 979-12-985238-0-7

Il presente rapporto è stato redatto da:
Giuseppe Creanza (ARTI)

Editing: Francesca Tondi (ARTI)
Grafica e impaginazione: Gianfranco D'Onghia (ARTI)

In copertina: Quantum engineering by KUSNIYAH from Noun Project (CC BY 3.0)