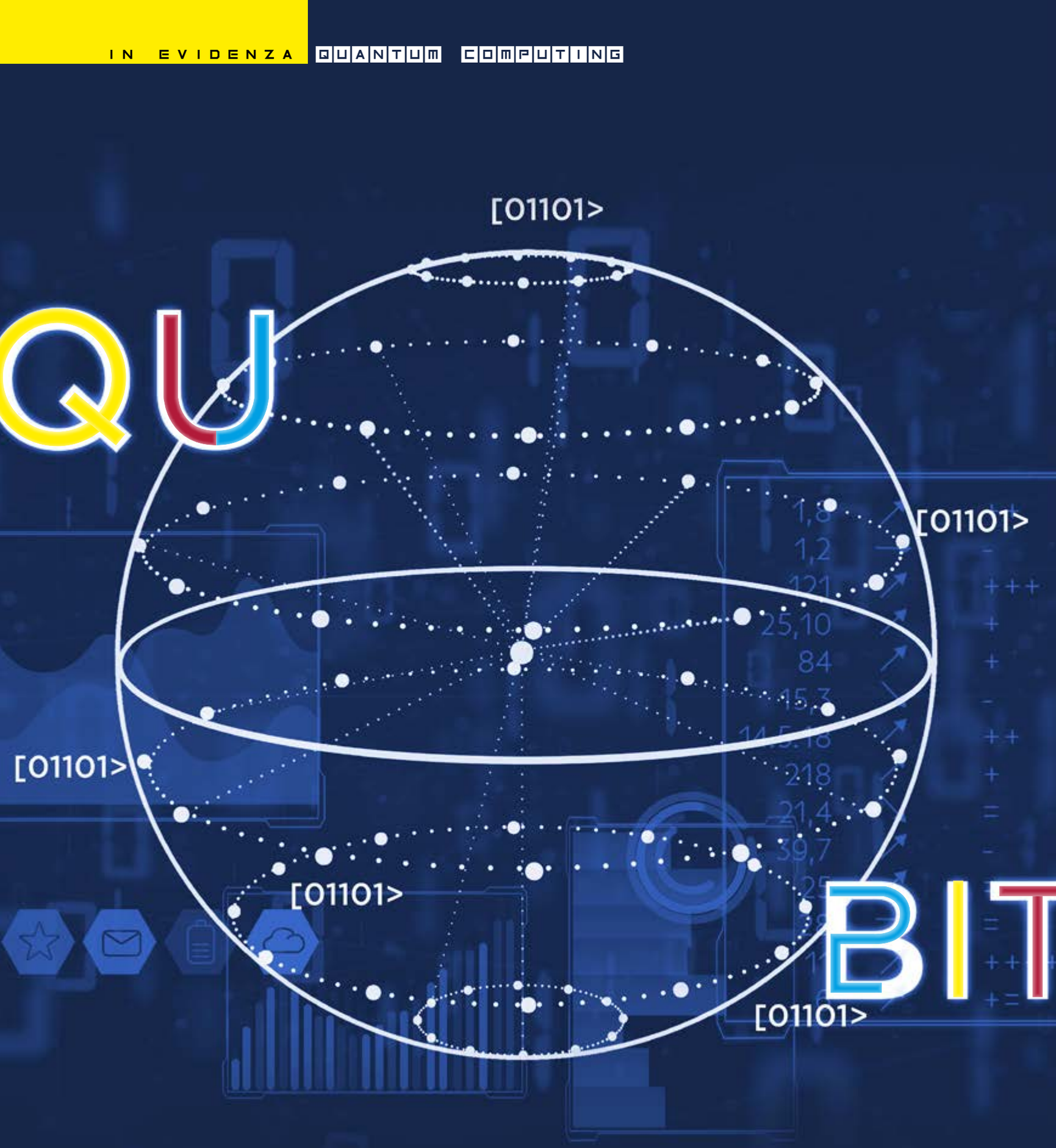

[01101>
QU
[01101>
[01101>
[01101>
[01101>
BIT

QUELLO QUANTISTICO È UN VIAGGIO TRA PROMETTENTI SPERIMENTAZIONI DEL PRESENTE E NOTEVOLI PROMESSE PER IL FUTURO, CHE INTERESSANO TUTTI I SETTORI. L'OBIETTIVO, ADESSO, È CERCARE DI AVERE UNA PANORAMICA DELLE POSSIBILI IMPLICAZIONI, PER TROVARSI PRONTI QUANDO ARRIVERÀ LA VERA RIVOLUZIONE QUANTISTICA

SILVIA MARIGONDA

TECNOLOGIE QUANTISTICHE DAI LABORATORI ALL'INDUSTRIA

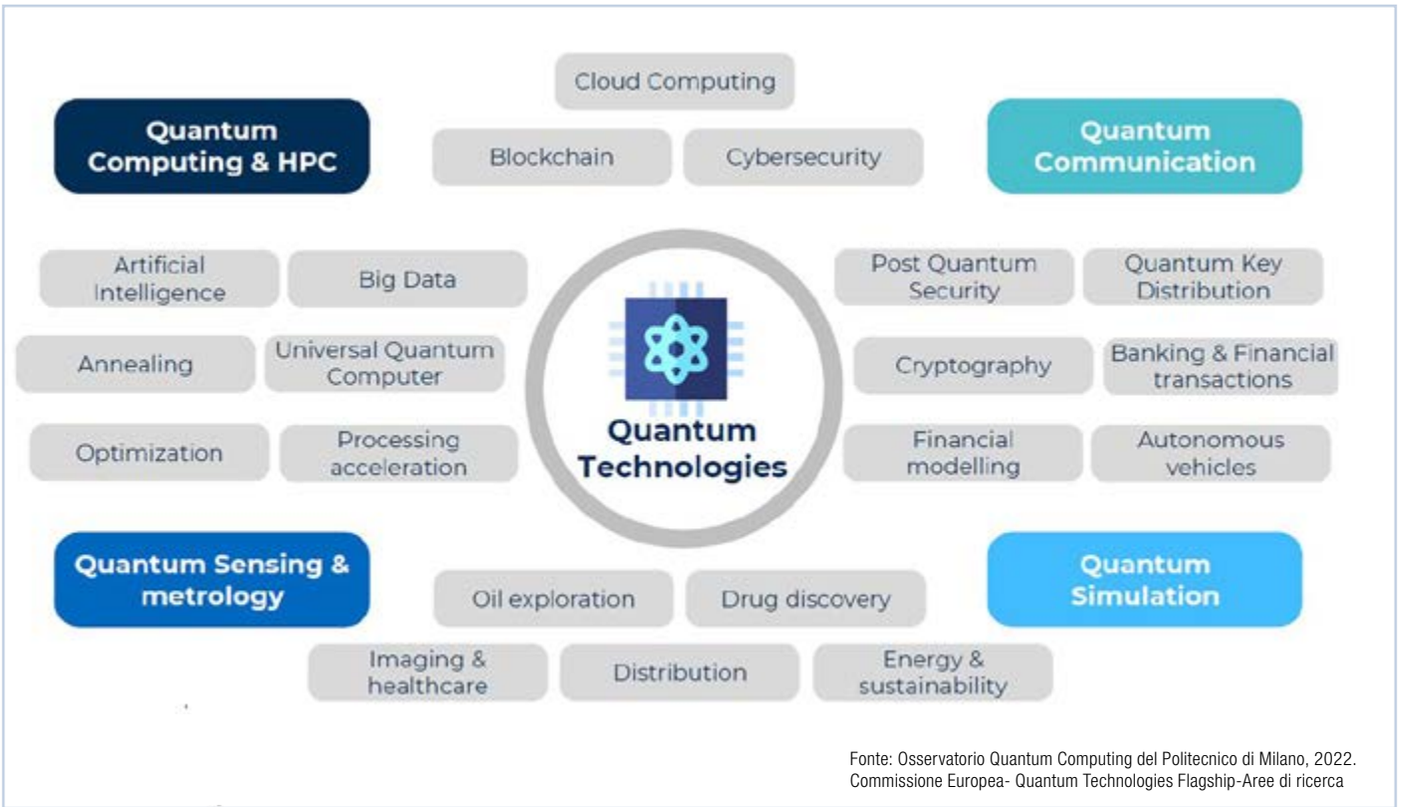
Le attuali previsioni collocano l'impiego diffuso di tecnologie quantistiche fra cinque-dieci anni, in base al campo applicativo considerato, ma l'adozione potrebbe avvenire in tempi anche più brevi. L'interesse oggi è volto soprattutto ai rischi per la cybersecurity che queste tecnologie comportano e, nello stesso tempo, alle soluzioni che esse rendono disponibili sempre in questo ambito.

Nella vita quotidiana, fra qualche anno, ad esempio, gli algoritmi di individuazione del percorso migliore di Google saranno tutti quantistici. Pensiamo a un calcolatore degli anni Cinquanta del secolo scorso: quanto a complessità, difficoltà di gestione e dimensioni, esso è molto simile agli attuali computer quantistici. Questo per dire che il futuro forse ci porterà a usare calcolatori quantistici nella vita di tutti i giorni.

Ma non è tutto, perché la meccanica quantistica ha permesso di comprendere anche alcuni fenomeni naturali: la fotosintesi è stata ad esempio spiegata attraverso il principio quantistico di sovrapposizione, aprendo la strada a importanti ricerche sul risparmio energetico, e lo stesso è accaduto per comportamenti molto particolari, come il meccanismo di orientamento del pettirosso. Non solo, dunque, la meccanica quantistica ci permette di sfruttare nuove tecnologie, ma anche allarga il nostro modo di ragionare intorno alla scienza in generale.

Per tecnologie quantistiche intendiamo una classe di tecnologie il cui funzionamento è basato sulla manipolazione attiva degli stati quantistici della materia, sfruttando i principi della meccanica quantistica.

Figura 1. L'ampio campo applicativo delle tecnologie quantistiche



Fonte: Osservatorio Quantum Computing del Politecnico di Milano, 2022.
Commissione Europea- Quantum Technologies Flagship-Aree di ricerca

Parliamo dunque di quattro grandi filoni.

- **Quantum communication**: processing e storage di informazioni; è questo l'ambito più avanzato e area di pertinenza della cosiddetta Quantum Internet, che garantirà connessioni quantistiche.
- **Quantum computing & Hpc**: accelerazione della capacità di calcolo; si pensi ad esempio alla possibilità di effettuare complesse analisi meteorologiche su aree molto più estese di oggi e nell'ordine di minuti.
- **Quantum sensing & metrology**: sensoristica e sistemi di misurazione più precisi degli attuali.
- **Quantum technology**: protocolli di comunicazione più sicuri, implementazione di sistemi resistenti agli attacchi di potenziali computer quantistici.
- **Quantum simulation**: si utilizza la computazione quantistica per risolvere problemi quantistici complessi.

La Quantum 2.0 ha un grosso vantaggio, rispetto alla prima formulazione della meccanica quantistica avvenuta all'inizio del XX secolo, quello di poter disporre di tecnologie avanzate per la manipolazione di particelle subatomiche. Tutto ciò apre la strada a un gran numero di potenziali applicazioni.

VERSO L'INFORMATICA QUANTISTICA

La meccanica quantistica è, allo stato attuale, il modello matematico più accurato che disponiamo dell'Universo e permette di prevedere con precisione assoluta il comportamento di ogni sistema fisico. Ciò che però lascia stupefatti è che, nonostante le continue conferme sperimentali della completa correttezza teorica, molte delle regole alla base della meccanica quantistica sono radicalmente controintuitive e numerosi fenomeni quantistici non hanno analogie con fenomeni del mondo della fisica classica a cui siamo abituati. La difficoltà che la nostra mente incontra nel comprendere la reale natura dei fenomeni quantistici deriva dal fatto che non abbiamo esperienza diretta di tali fenomeni, poiché negli oggetti macroscopici dei quali abbiamo esperienza la natura quantistica è di fatto non percepibile. Questa situazione è destinata a cambiare nel prossimo futuro grazie all'avvento dei primi computer quantistici perché essi sono il primo esempio di oggetti macroscopici che mostrano un comportamento decisamente quantistico. La stessa difficoltà tecnologica nel realizzare i computer quantistici risiede proprio nella difficoltà di generare nel mondo macroscopico i comportamenti che invece sono tipici delle particelle subatomiche e descrivibili con precisione solo utilizzando la meccanica quantistica. Ma la realizzazione di sistemi macroscopici e controllabili, dal comportamento quantistico, è

essenziale per trarre vantaggio dall'informatica quantistica.

I COMPUTER QUANTISTICI

Se il calcolatore tradizionale si basa sul fatto di racchiudere l'informazione nel cosiddetto bit, oggetto che può assumere valore 0 oppure 1 (nella rappresentazione della sfera di Bloch può dunque trovarsi solo ai poli di essa), il calcolatore quantistico si basa invece sul qubit, struttura quantistica con due stati ma che, in base al principio di indeterminazione di Heisenmberg, può trovarsi in qualunque sovrapposizione sia dello stato 0 che dello stato 1 (può dunque trovarsi in qualunque punto della sfera di Bloch). Consideriamo, ad esempio, una moneta posta su un tavolo: essa può segnare testa oppure croce. Ma quando la lanciamo in aria, mentre è sospesa, in qualche modo si comporta come un oggetto quantistico, prima che la misura la costringa a rivelarsi (come testa o come croce), perché ha in sé entrambe le potenzialità di essere testa e di essere croce.

Grazie a questa proprietà, un certo numero di qubit può dunque rappresentare tanti dati diversi, superando così la logica binaria della computazione tradizionale e passando da una misura deterministica a una probabilistica. Con pochi qubit, si può allora rappresentare una quantità enorme di informazioni ed eseguire operazioni contemporaneamente con un singolo dispositivo: se con n bit si possono realizzare n operazioni di calcolo, con n qubit ne sono realizzabili 2 alla n (2^n).

L'idea del computer quantistico venne proposta già da Richard Feynman all'inizio degli anni Ottanta del secolo scorso, ma sono state necessarie le tecnologie maturate negli ultimi vent'anni, come il vuoto e la criogenica, perché diventasse realtà. Gli oggetti quantistici sono infatti strutture molto delicate, il cui stato può essere alterato in modo incontrollato e ignoto, perdendo il contenuto informativo, a causa dell'interazione con altri oggetti ed elementi ambientali. Per evitare che questo accada, occorre limitare il più possibile lo scambio di energia fra ambiente e sistema quantistico e per questo è necessario operare a centesimi di grado sopra lo zero assoluto, grazie per esempio a refrigeratori ad induzione.

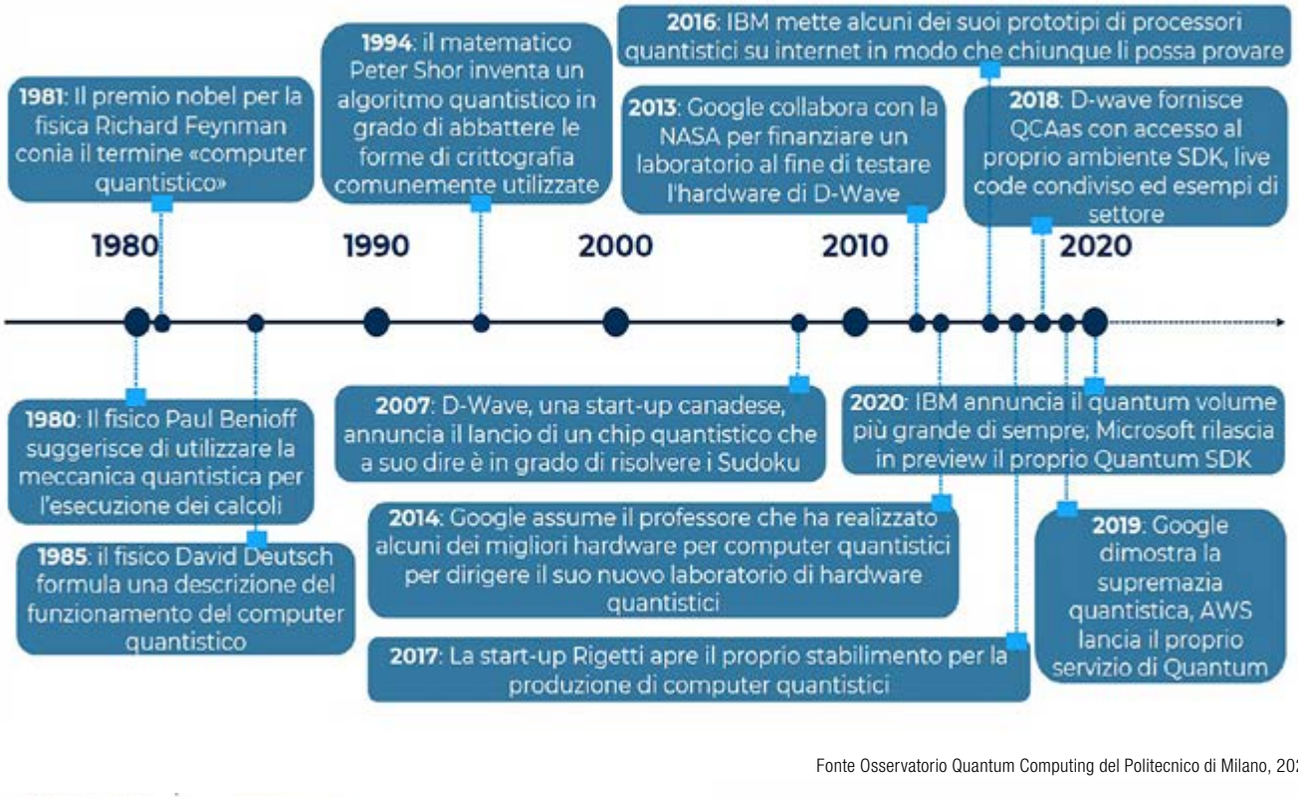
Con il termine Quantum Supremacy, ci si riferisce all'abilità umana di costruire un computer quantistico capace di risolvere un problema irrisolvibile per i computer classici. La prima volta, questa supremacy è stata ottenuta nel 2019 da un gruppo di lavoro di Google usando qubit superconduttivi. Sycamore, il computer a 54 qubit di Google, richiedeva 200 secondi per calcoli che a un supercomputer attuale richiederebbero circa diecimila anni. Nel 2021 anche un gruppo di lavoro cinese ha raggiunto la Quantum Supremacy, ma con una tecnologia del tutto diversa, basata su fotoni, utilizzando un computer prima a 60 e poi 64 qubit.

IL COMPUTER A 54 QUBIT DI GOOGLE RICHIEDEVA, NEL 2019, 200 SECONDI PER CALCOLI DI 10.000 ANNI CON ALTRI PC

Nel novembre 2021, Ibm ha annunciato la nascita di Eagle, processore quantistico a 127 qubit, del quale non ha però reso note le prestazioni, pur affermando che Eagle è il primo processore che non può essere simulato su un supercomputer tradizionale. Eagle è stato realizzato utilizzando una nuova tecnica che prevede componenti di controllo dei qubit collocati in un'architettura a più livelli fisici, con i qubit mantenuti in un livello separato. Questo processore è l'ultimo passo lungo il percorso di scalabilità dell'informatica quantistica tracciato da Ibm per consentire ai circuiti quantistici di raggiungere il Quantum Advantage, cioè il punto in cui i sistemi quantistici superano significativamente quelli classici. Non parliamo dunque di qualcosa di futuribile, ma di una realtà, anche se questi esperimenti implicano ancora problemi accademici complessi: il prossimo passo sarà risolvere problemi applicativi, ad esempio nell'ambito della chimica o della scienza dei materiali. Un altro campo importante di ricerca è quello dei nuovi farmaci e di tutte le applicazioni che sfruttano il machine learning. Non solo. Lo scrivere algoritmi quantistici, che sono completamente ripensati, in modo tale da sfruttare al massimo la possibilità di più operazioni contemporanee, ha avuto anche delle ricadute sugli algoritmi classici, che si è potuto ottimizzare grazie alle conoscenze acquisite.

Dal punto di vista tecnologico, la storia della realizzazione del computer quantistico inizia già con la tecnologia silicon gate, introdotta da Federico Faggin nel 1968, con la quale diventava possibile racchiudere milioni di transistor in un unico chip di silicio. In tal modo, alla metà degli anni Settanta, sempre maggiore potenza di elaborazione poté essere contenuta in piccole dimensioni e venne definita la Legge di Moore, secondo la quale ogni 18 mesi sarebbe raddoppiata la potenza, perché sarebbe raddoppiato il numero di transistor integrabili in un microprocessore. Negli anni più recenti questa Legge, prima rigorosamente seguita, appare essere meno rispettata, perché ormai i transistor sono di soli pochi atomi e occorre dunque realizzarli ancora più piccoli. Il computer quantistico, però, non si chiama tale perché i microprocessori sono dell'ordine di dimensione subatomica, dei quanti, ma

Figura 2. Qualche cenno storico sul Quantum Computing



Fonte Osservatorio Quantum Computing del Politecnico di Milano, 2022

perché si fonda su una branca dell'informatica totalmente diversa da quella classica: l'informatica quantistica.

A tal proposito, Chris Bernhardt, autore del libro "Quantum Computing for Everyone" (2019), scrive: "L'informatica quantistica è una splendida fusione di meccanica quantistica e informatica, che incorpora alcune delle idee più sbalorditive della fisica del ventesimo secolo in un modo completamente nuovo di pensare al calcolo".

Se nell'informatica classica, ad esempio, si utilizzano operazioni aritmetiche, e viene adottata la logica dei diagrammi di flusso per descrivere i passi elementari degli algoritmi, nell'informatica quantistica si adotta invece l'algebra lineare e al posto dei diagrammi di flusso ci sono quelli ad hoc per rappresentare i circuiti quantistici. Ad esempio, pensiamo alla scomposizione di un intero in numeri primi. Il metodo classico funziona bene se le cifre sono poche, poi la sua complessità cresce in misura esponenziale, e con essa il tempo computazione. Come cambia la fattorizzazione di un numero intero con l'informatica quantistica? Nel 1994, Peter Schor ha proposto l'algoritmo che da lui prende il nome e che utilizza, per la fattorizzazione, al proprio interno, anche la serie (trasformata) quantistica di Furier, operazione per la quale un computer classico impiegherebbe miliardi di anni. Ma se invece si avesse a disposizione un dispositivo che si comporta in modo quantistico, su cui far girare questo algoritmo? Allora la trasformata si risolverebbe in pochi passi e la stessa complessità della fattorizzazione scenderebbe da "qualcosa alla n" ad "n al cubo", richiedendo tempistiche di risoluzioni al massimo mesi: si passa dunque da un tempo esponenziale ad uno polinomiale di computazione. Gli strumenti usati dall'informatica quantistica sono totalmente nuovi. Ad esempio, laddove i computer classici vengono programmati principalmente attraverso linguaggi come l'oggi celebre Python, per i computer quantistici al contrario si usano le operazioni logiche, anche se sono in corso di sviluppo linguaggi più vicini a quello naturale.

Infine, esistono sono due classi principali di algoritmi quantistici, che derivano fondamentalmente dal già citato algoritmo di Schor per la fattorizzazione (capace di decriptare la maggior parte dell'attuale crittografia a chiave pubblica) e dall'algoritmo di Grover, per il searching.

LE PROPRIETÀ DEL QUBIT

Il qubit ha tre proprietà principali: superposition (sovrapposizione di stati), entanglement (correlazione) e interferen-

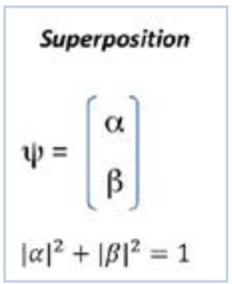


Figura 3. Principio di sovrapposizione del qubit

za. Se il bit è rappresentato dalla cifra, il qubit è rappresentato invece dal vettore (il cosiddetto array della programmazione), in particolare ci si riferisce al più semplice dei vettori, a due valori. Per convenzione, α è la quantità di zero e ß è la quantità di uno presente nel qubit. α e ß devono essere scelti in modo da rispettare il comportamento quantistico e dunque, dal punto di vista matematico, la somma dei loro quadrati deve valere uno. Ma α e ß in realtà non sono neppure numeri reali, bensì sono complessi (cioè con una parte reale ed una immaginaria) e per questo motivo nella formula sono presenti le norme. ψ è detto vettore di stato (rappresentazione matematica dello stato del qubit), mentre α e ß sono chiamate ampiezze. Lo stato diverso da 0 e 1 si chiama stato di superposition.

Il primo comportamento bizzarro che si rileva è che, nonostante il qubit possa essere in superposition, quando lo si misura, si può misurare solo 0 oppure 1. Finché non lo si misura, il qubit è effettivamente nei due stati combinati, abbiamo tantissime evidenze sperimentali di questo, ma se lo si misura, si trova 0 oppure 1. E, se lo si misura molte volte, a volte lo si trova a 0 e a volte ad 1, tanto che si può calcolare la probabilità p che assuma stato 1 oppure 0. p(0), ad esempio, è la probabilità che il qubit si trovi nello stato 0.

Nello stato di superposition, di fatto il qubit non è misurabile e si può solo calcolare le probabilità di cui sopra. Questo comportamento non deterministico ma probabilistico degli oggetti di tipo quantistico è qualcosa che ha sconcertato numerosi scienziati: il solo fatto di andare a guardare l'oggetto quantistico fa collassare lo stato di superposition in uno dei due stati fondamentali (principio di no-cloning: l'informazione non può essere né copiata né letta con assoluta precisione) e questo non dipende dal metodo utilizzato per misurare o osservare lo stato, ma è un preciso e ineluttabile postulato della meccanica quantistica.

Sui qubit si possono poi fare delle operazioni attraverso delle porte cosiddette quantistiche, in analogia con quelle dell'informatica classica. Ad esempio, la porta di Hadamard restituisce sempre un qubit in uno stato di superposition nel quale i due stati base sono equiprobabili al 50% ciascuno. L'interferenza è la seconda proprietà fondamentale del qubit. In base ad essa, lo stato iniziale che precede la sequenza delle operazioni logiche, influenza lo stato finale. Negli algoritmi quantistici complessi, l'interferenza è molto utile perché cancella i risultati non validi, lasciando solo quelli validi. La terza proprietà, l'entanglement, non riguarda il singolo qubit, ma un insieme costituito da più qubit, almeno due, ed è una delle proprietà più difficili da comprendere, perché non trova analogie nel mondo della fisica classica. Dati due qubit, se lo stato misurato del primo è zero (oppure è uno), anche quello del secondo, persino se molto distante, presenta la medesima misura. I valori dei due qubit sono allora strettamente collegati (entangled). Individualmente, essi sono nello stato di superposition ma osservare il primo, automaticamente vincola l'osservazione del secondo, cioè ne determina la misura. Einstein la definì una "spaventosa azione a distanza" e negò sempre che dietro l'entanglement ci fosse un reale fenomeno fisico.

IL COMPORTAMENTO NON DETERMINISTICO MA PROBABILISTICO DEGLI OGGETTI QUANTISTICI ANCORA SCONCERTA

Per dare un'idea delle implicazioni connesse all'entanglement, basta pensare che su questa proprietà è basato un algoritmo chiamato Quantum Teleportation, cioè teletrasporto quantistico: volendo semplificare al massimo, la meccanica quantistica ci dice che la smaterializzazione dell'astronave di Star Trek e la sua ri-materializzazione su un altro pianeta, è fisicamente possibile. Il trasporto di fotoni fra Tenerife-La Palma 143 km è in realtà stato realizzato già nel 2012, mentre ad oggi solo il fatto di non avere ancora la disponibilità tecnologica ci impedisce già di teletrasportare oggetti, anche se in linea di principio sapremmo come farlo. La Quantum Teleportation è la soluzione che permetterà di superare i limiti della distanza trasmissiva, rendendo nello stesso tempo le reti effettivamente quantistiche: l'informazione non sarà infatti più trasmessa fisicamente sui mezzi trasmissivi, ma veicolata attraverso l'entanglement.

Al momento attuale, invece, le distanze tra cui può avvenire efficacemente la trasmissione dell'informazione quantistica tramite fotoni sono ancora limitate: alcune decine di chilometri per trasmissione su fibra e poche migliaia di chilometri in free space, cioè via satellite. Questo perché il "quantum" di informazione trasportato da un flying photon non può essere amplificato o rigenerato e, al crescere della distanza percorsa, si accumulano gli effetti di attenuazione e rumore.

La soluzione alla quale si ricorre attualmente, per ovviare al problema, consiste nel suddividere le distanze lunghe in tratte più brevi, sulle quali i fotoni possono essere trasmessi e ricevuti in maniera sufficien-

IL QUANTUM COMPUTING: STATO DELL'ARTE, TENDENZE E APPLICAZIONI

	Funzionamento	Ambito	Dimensioni HW (2021)	Prestazioni (2021)	Orizzonte temporale	Limiti
Universal Quantum Computer	All'interno di un circuito, porte quantistiche eseguono un'operazione di calcolo alla volta, in modo simile a un computer classico	General-purpose	Centinaia di qubit	È già dimostrata la supremazia quantistica	Lungo (5-10 anni)	• Dimensioni e prestazioni dell'hardware sono limitate, perché il computer quantistico è difficile da controllare ed è sensibile all'ambiente esterno. Tanto da risultare soggetto a perdita di coerenza (decoherence), cioè a perdita della capacità di mantenere la sovrapposizione degli stati e dunque l'informazione quantistica • In attesa dell'hardware, è già possibile lavorare sul software per ottenere benefici nel breve termine e velocizzare l'industrializzazione delle soluzioni (identificazione dei casi d'uso e riprogettazione di algoritmi)
Quantum Annealer	Riproduce il fenomeno fisico che porta un sistema a raggiungere la condizione di equilibrio a minima energia	Special-purpose: è adatto alla risoluzione di problemi di ottimizzazione combinatoria	Migliaia di qubit	Non è ancora dimostrata la supremazia quantistica	Breve e medio (1-3 anni)	

Fonte: rielaborazione dati dell'Osservatorio Quantum Computing del Politecnico di Milano, 2021- 2022

temente affidabile. Questi vari segmenti componenti sono attestati ai cosiddetti trusted node, nodi nei quali l'informazione da trasmettere viene estratta dai fotoni ricevuti e ricodificata nei fotoni che verranno inviati al nodo successivo lungo il cammino che collega i due end-node.
Una rete costituita da trusted node non può però definirsi propriamente quantistica, perché l'informazione trasmessa è classica e viene protetta a livello quantistico solo sui link trasmissivi, mentre nei trusted node questi dati sono decodificati e disponibili "in chiaro".

LA QUANTUM INTERNET

La Quantum Internet costituirà l'infrastruttura per trasmettere i qubit e condividere il loro stato tra gli end-node quantistici. L'architettura delle reti quantistiche rifletterà quella delle reti classiche, in quanto sarà costituita da elementi che avranno ruoli analoghi ai loro corrispondenti classici, anche se funzioneranno basandosi sui principi della meccanica quantistica. Ci saranno dunque nodi sede di processori quantistici, switch e router quantistici, oltre ai mezzi trasmissivi.
È bene sottolineare come alla base dello sviluppo della Quantum Internet non ci sia l'obiettivo di sostituire, migliorare o surclassare l'Internet classica. Al contrario, la Quantum Internet opererà in sinergia con la rete esistente, andando a costituire una rete Internet ibrida, "classica" e "quantistica" insieme. In questa nuova rete ibrida, la Quantum Internet interverrà per supportare nuove funzionalità che consentiranno di migliorare e arricchire le comunicazioni, ma anche applicazioni "classiche". Le nuove applicazioni "quantistiche" a loro volta, per poter funzionare, si appoggeranno alle comunicazioni classiche della rete Internet. La soluzione al momento più realistica per la trasmissione dei qubit (i cosiddetti "flying" qubit, per distinguerli dai matter qubit residenti negli end-node quantum e utilizzati per processare o memorizzare informazioni), consiste nell'utilizzo dei fotoni, grazie al fatto che questi hanno proprietà i cui stati possono essere utilizzati per codificare facilmente i qubit, interagiscono debolmente con l'ambiente, hanno velocità di trasmissione elevata e permettono il riutilizzo dell'infrastruttura in fibra ottica, salvaguardando così gli investimenti. Oltre ad abilitare comunicazioni sicure, le funzionalità della Quantum Internet possono essere utili nei problemi che richiedono il coordinamento dell'azione di una flotta di entità (come un insieme di computer o di robot industriali), oppure per aumentare l'accuratezza delle applica-

Approcci nel breve termine	Tendenze in atto	Tipologie di progetti
Approccio Quantum-inspired: eseguire gli algoritmi quantistici su computer tradizionali ***Approccio Ibrido:*** il quantum computing viene utilizzato per risolvere solo una parte di un problema più ampio *Dopo il 2025: lancio della fase commerciale* **Sfide aperte** • Come valutare un computer quantistico? E quali benchmark adottare? • Come valutare la superiorità quantistica? • Quali competenze occorrono?	• La ricerca in ambito industriale sta crescendo: +1.942 domande di brevetto sul Quantum Computing negli ultimi 7 anni • L'ambito del Quantum Computing è ancora piccolo ed emergente, ma fondamentale per accelerare l'industrializzazione delle tecnologie • 80 progetti mappati a livello internazionale: 49% in Europa, 29% in Usa e Canada, 19% in Asia, 3% in Australia (dati luglio 2021) • I progetti sono ancora esplorativi e realizzati in un ambito di ricerca e sviluppo • Le sperimentazioni sono spesso un investimento congiunto, anche attraverso accordi pluriennali. Fondamentale la creazione di ecosistemi di imprese e centri di ricerca • Il Quantum Computing si legherà soprattutto, almeno in questo decennio, all'accesso as-a-service abilitato dal Cloud	• ***Optimization*** (trovare la soluzione ottimale all'interno di una serie di soluzioni applicabili. Esempi: routing problem, resource allocation problem) -42% (su base 80 progetti) • ***Simulation*** (rappresentare e simulare il comportamento di sistemi complessi. Esempi: molecular dynamic simulation, multiscale simulation, Monte Carlo simulation) -39% • ***Pattern Recognition*** (identificazione di pattern all'interno di grandi dataset e sviluppo di modelli predittivi basati su dati) -19% • ***Classification/Clustering*** (classificazione di dati all'interno di grandi dataset, clusterizzazione e valutazione di affinità tra i cluster) **I progetti riguardano principalmente:** • ***Chemistry/Pharma*** (24%, prevale simulation) - Esempio: ricerca di trattamenti contro l'Alzheimer • ***Finance*** (19%, prevalgono optimization e simulation) - Esempio: ottimizzazione portafoglio finanziario • ***Aerospazio e difesa*** (15%, prevale optimization) - Esempio: simulazione della fluidodinamica nella progettazione di velivoli • ***Energy/Utility/Telco*** (12%, prevale optimization) - Esempio: studio di materiali che catturino CO_2 per poterla riutilizzare all'interno di impianti • ***Manufacturing*** (11%, prevale simulation) - Esempio: creazione di batterie più performanti, durevoli ed ecologicamente sostenibili per dispositivi consumer • ***Automotive*** (9%, prevale optimization) - Esempio: ottimizzazione della rete distributiva di componenti per automobili • ***Logistics/Retail*** (6%, solo progetti di optimization) - Esempio: ottimizzazione della logistica in-store nei supermercati per ridurre gli sprechi

zioni che si basano sulla sincronizzazione del timing su oggetti distribuiti (un esempio è il Gps). Va anche rilevato che, allo stato attuale della tecnologia, mantenere i qubit in un ambiente protetto (isolati e ad una temperatura prossima allo zero assoluto) risulta sempre più difficile all'aumentare del numero di qubit e questo limita l'espansione della potenza di calcolo dei computer quantistici. Se questa difficoltà dovesse persistere, una delle prime applicazioni della Quantum Internet potrebbe essere il Distributed Quantum Computing cioè la costituzione di cluster di computer quantistici con una potenza di calcolo complessiva superiore a quella delle singole macchine. Un altro campo applicativo per la Quantum Internet è quello dei servizi di quantum computing in Cloud in cui si mantiene la riservatezza dei dati sorgenti, per preservare la privacy delle informazioni. Tutte le funzionalità della Quantum Internet saranno totalmente sfruttabili quando l'entanglement verrà reso disponibile a livello commerciale: nel frattempo, le prime applicazioni già in produzione sono la Qkd e il Qrng.

LA QUANTUM KEY DISTRIBUTION (QKD)

A livello generale, la crittografia può essere considerata un sistema matematico di trasformazione dell'informazione. Essa consente di trasmettere messaggi mantenendoli segreti a tutti tranne a chi possiede la chiave per decriptare i dati. Gli obiettivi della crittografia sono essenzialmente: confidenzialità (cioè riservatezza dell'informazione, che non deve essere accessibile

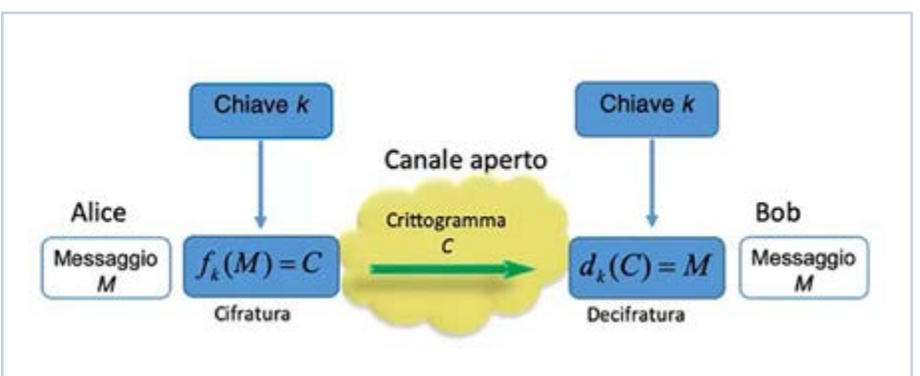


Figura 4. Schema classico cifratura-decifratura

COME PREPARARSI ALLE TECNOLOGIE QUANTISTICHE IN CINQUE MOSSE

Sono stati individuati cinque passi concreti che le aziende possono compiere per prepararsi nel modo migliore all'avvento delle tecnologie quantistiche

a terze parti), autenticazione (il destinatario deve essere sicuro del mittente) e integrità del messaggio che viene ricevuto. Lo schema standard prevede che il mittente (Alice) prenda un messaggio M, gli applichi una funzione di cifratura f(k), dove k, un sistema random di bit, è la chiave, ottenendo il crittogramma C che viene mandato, su canale aperto, al destinatario (Bob). Bob, che possiede la chiave k, applica ad M l'algoritmo di decifratura, anch'esso dipendente da k, e ottiene il messaggio M.

A livello più astratto, Shannon, nel 1946, ha dimostrato che un sistema di crittografia è totalmente sicuro se la chiave k è composta da numeri casuali, è usata una sola volta (Otp, One Time Pad) ed è lunga quanto il messaggio. Questo sistema crittografico è detto anche cifrario di Vernam, o cifrario perfetto. Il problema cruciale è costituito dal momento dello scambio delle chiavi fra Alice e Bob: il metodo di Shannon, cioè lo schema di crittografia basato su chiavi segrete, è sì totalmente sicuro, ma di fatto complicato da implementare nella realtà (si usa tuttavia, ad esempio, fra governo ed ambasciate: corrieri fisici portano le chiavi). Comunemente, si utilizza allora uno schema cosiddetto a chiave pubblica, detto Rsa (dalle iniziali dei nomi degli inventori). Esso prevede una distribuzione di chiavi cosiddetta asimmetrica. In un esempio tratto dalla vita quotidiana, è questo il caso dei pagamenti nell'e-commerce: Amazon distribuisce a tutti una chiave pubblica per consentire agli acquirenti di trasmettere i dati della propria carta di credito, l'utente cripta i propri dati con essa e successivamente Amazon li decripta usando la propria chiave privata. Il metodo è semplice, non vi è necessità che gli interlocutori si accordino su una determinata chiave, ma la sicurezza non è completa: teoricamente, chiunque potrebbe decriptare il messaggio, avendo un computer sufficientemente potente, oppure abbastanza tempo per attendere che avvenga la decriptazione. Questo tempo dipende, in misura esponenziale, dal numero di cifre impiegato nella chiave pubblica.

Negli anni, di conseguenza, per aumentare la sicurezza si è aumentato il numero di cifre, ma i computer quantistici oggi sanno fare bene poche cose e una di queste è proprio decriptare codici Rsa in pochi secondi. Inoltre, numerosi hacker attualmente salvano i dati Rsa (ad esempio sanitari o bancari) in attesa che la tecnologia sia pronta per decriptarli (si tratta di attacchi Harvest Now - Decrypt Later). Se da un lato la tecnologia quantistica pone dunque problemi di sicurezza, dall'altro, permette però anche di realizzare una tecnologia in grado di garantire che la sicurezza delle comunicazioni sia intrinseca, cioè inviolabile. Di fatto, questo avviene agendo sul sistema di distribuzione delle chiavi: è la cosiddetta Qkd. La Quantum Key

Distribution si realizza con un trasmettitore e un ricevitore (più propriamente due stazioni), collegati in fibra ottica, che permettono ad Alice e Bob di condividere la stessa chiave crittografica.

Il protocollo più usato per la Qkd è il BB84, introdotto nel 1984: la chiave è codificata sfruttando la polarizzazione di un singolo fotone (gli stati di polarizzazione sono usati per codificare 0 e 1). Il vantaggio è che, se qualcuno (in gergo Eva) tenta di misurare il singolo fotone per capirne la polarizzazione, automaticamente il sistema rivela un certo grado di rumore e di conseguenza Alice e Bob si ritrovano con chiavi diverse che di fatto impediscono la loro comunicazione reciproca. Nessun sistema di comunicazione classico è in grado di garantire che nessuna Eva sia "in ascolto" della comunicazione, tanto quanto la Qkd. Questo anche se, a livello pratico, le cose sono un po' più complicate, perché abbiamo tutta una serie di errori e di interferenze. Diventa necessario allora introdurre codici di correzione degli errori e di verifica delle chiavi. Ad esempio, si fa in modo che Alice e Bob confrontino una parte delle rispettive sequenze di 0 e 1: se le sequenze sono uguali, cioè se Qber non supera ad esempio il valore soglia del 12%, dove Qber è il Quantum Bit Error Rate, siamo certi che non ci sia stato alcun attacco.

La Qkd è già una tecnologia matura: abbiamo da tempo sperimentazioni in aree metropolitane, e anche un satellite cinese in grado di distribuire le chiavi in maniera quantistica (fra Pechino e Vienna). Esistono anche già aziende commerciali che vendono Qkd, come la Svizzera ID Quantique, di recente acquisita dall'azienda di telecomunicazioni della Corea del Sud. Sempre la Cina ha realizzato un backbone in fibra ottica da Pechino a Shangai: circa 2.000 km con 32 trusted node (uno ogni meno di 100 km): non si tratta di amplificatori ottici, perché gli amplificatori distruggerebbero il segnale quantistico, ma di punti di rigenerazione del segnale quantistico. Nello spazio libero, cioè utilizzando il satellite, non abbiamo necessità di introdurre trusted node: con i satelliti si raggiungono quindi grandissime distanze. Un backbone quantistico simile a quello cinese è presente anche in Italia, tra il Frejus e Matera, coordinato dall'Istituto Nazionale di Ricerca Metrologica (Inrim). Mentre il backbone cinese è però in produzione e vengono scambiate chiavi per impieghi reali (ad esempio esse sono utilizzate da banche), quello italiano è usato solo per la ricerca.

A Firenze un tratto metropolitano dell'Italian Quantum Backbone è stato usato per lo scambio di chiavi in modo quantistico (su una distanza inferiore ai 40 km). A Trieste, nel settembre 2020, è stata sperimentata una videochiamata criptata fra il Porto Vecchio e l'Università

IN BREVE...

- Il quantum computing si presenta come veramente disruptive, soprattutto nel medio e lungo periodo;
  - Serviranno 5-10 anni per le installazioni sperimentali,
  - Serviranno 10-20 anni per avere un vero e proprio mercato del computer quantistico.
- L'architettura di un computer quantistico è totalmente differente da quella del computer classico.
- La logica quantistica è del tutto nuova rispetto a quella classica.
- Anche gli algoritmi sono nuovi: un programma scritto in logica booleana non eseguirà più velocemente per il semplice fatto di essere eseguito su un computer quantistico ma un programma per un computer quantistico deve essere scritto in logica quantistica per essere superiore all'equivalente classico.
- Il computer quantistico non sostituirà i computer digitali (Qpu come Gpu o coprocessore), ci sarà invece collaborazione fra computer quantistici e supercomputer. Inoltre, non tutti gli algoritmi booleani hanno un equivalente quantistico più veloce. Il mercato per i computer digitali non diminuirà, anzi, servono tanti computer tradizionali per far funzionare un computer quantistico.
- Parliamo di Quantum Computing ma anche Quantum Competence: Computer Science + Hpc + Quantum Theory.
- Il rischio R, nell'adozione di tecnologie quantistiche, è ancora in molti casi alto (non è detto, ad esempio, che l'utilizzo di un computer quantistico sia più efficace per un certo problema), l'impatto I è però altrettanto alto (rendere un problema intrattabile solvibile). In molti casi, si è valutato, R*I è sufficiente a giustificare l'investimento.

(circa 10 km). Nell'occasione, è stato anche rilevato che un attacco hacker è stato in grado di mettere immediatamente in allarme il sistema, dimostrandone così la sicurezza. Qti è un'azienda, spin-off del Cnr, appositamente costituita un paio di anni fa per avviare l'industrializzazione di sistemi Qkd. Un altro esperimento di rilievo, finanziato dalla Nato, è stato effettuato su 96 km di cavo in fibra sottomarino fra Malta e la Sicilia. La rilevanza di questo esperimento è stata data dal fatto che si è dimostrato l'entanglement quantistico in uno scenario in campo e non solo in laboratorio.

La tecnologia Qkd interessa in primo luogo governi e pubbliche amministrazioni, ad esempio per comunicazioni fra ministeri, ambasciate, trasmissione di risultati elettorali o di dati personali, ma anche banche (per comunicazioni tra filiali), servizi digitali, aeroporti, industrie ad alto contenuto tecnologico che necessitano di proteggere brevetti. Un altro campo di utilizzo è quello della trasmissione di dati sanitari e assicurativi, mentre allo studio vi sono anche tutta una serie di progetti per rendere sicure le blockchain attraverso la Qkd. Le blockchain si basano infatti, per generare la firma digitale, sulla crittografia a chiave pubblica o sulla fattorizzazione di numeri primi: la sicurezza di questi algoritmi è attualmente fondata essenzialmente sulla complessità computazionale dei problemi matematici sottesi, che tuttavia potrebbero essere teoricamente risolti da computer quantistici.

Va sottolineato che l'uso della Qkd non risolve il problema della sicurezza intrinseca delle chiavi, cioè non garantisce che le chiavi scambiate con la Qkd siano robuste ai tentativi di decifratura: la Qkd garantisce unicamente la sicurezza delle chiavi durante lo scambio delle medesime. Le chiavi, eventualmente intercettate successivamente alla procedura di scambio, sono soggette agli stessi rischi di sicurezza delle chiavi scambiate in modalità classica.

IL 5G POTREBBE ABILITARE UNA COMUNICAZIONE QUANTISTICA SICURA "AS-A-SERVICE"

Un'altra grande sfida è l'utilizzo massiccio della Qkd in applicazioni quali IoT, Big Data, Cloud e così via. Per un utilizzo massivi è però necessario che il mercato della Qkd si attesti su costi inferiori rispetto a quelli attuali. Altro aspetto importante è che i protocolli BB84 e simili sono concepiti per lo scambio di chiavi point-to-point e le architetture tipo point-to-multipoint devono ancora essere esplorate. La spinta maggiore a un utilizzo diffusivo della Qkd verrà poi sicuramente dall'integrazione di tutti i componenti costituenti un trasmettitore o un ricevitore in un unico modulo integrato, il gateway Qkd leggeri, compatti ed economici.

Infine, le prestazioni della Qkd sono piuttosto limitate in bit-rate e distanza: i dispositivi oggi utilizzati negli esperimenti in campo consentono di coprire distanze di un centinaio di chilometri circa e bit-rate fra le decine e le centinaia di Mbit/s, con un trade-off fra bit-rate e distanza (con un record di 250 km, ma limitato a 16 bit/s), ma, come detto, ci si aspetta che gli attuali limiti di distanza potranno essere superati in futuro con l'uso dell'entanglement.

In Italia, un'azienda di telecomunicazioni come Tim, ad esempio, sta valutando il probabile impatto della Qkd nel proprio settore, identificando alcuni casi d'uso, sia interni sia rivolti alla clientela:

- Lato utente finale: utilizzo per la crittografia quantistica di dati critici e la distribuzione quantica di segnali di sincronizzazione temporale (via entanglement) tra applicazioni dislocate in siti remoti;
- Lato operatore: possibilità di rendere quantum-safe le parti critiche della rete e

delle infrastrutture dei datacenter, anche sfruttando le nuove potenzialità del 5G, di offrire alla clientela una comunicazione quantistica sicura as-a-service, di abilitare servizi che potrebbero avere una ricaduta nel breve e medio termine anche nel settore Industria 4.0, soprattutto per quanto riguarda soluzioni di IoT.

IL QUANTUM RANDOM NUMBER GENERATOR (QRNG)

In diversi campi della scienza, della tecnica, e anche della vita quotidiana, è richiesta la generazione di numeri casuali, il cui requisito fondamentale, la non predicibilità, in realtà non può essere garantito con assoluta certezza utilizzando metodi classici, basati per esempio su algoritmi di calcolo deterministici. La parvenza di casualità di questi metodi è infatti fondata su una elevata complessità che rende difficile, sebbene non impossibile, una predizione. Anche nel caso dei generatori fisici di numeri casuali, basati su fenomeni fisici caotici, come la corrente di rumore di un resistore o di un diodo, non è possibile garantire l'assenza di interazioni con l'ambiente, che potrebbero compromettere la qualità del risultato.

Tra i pochi fenomeni fisici in cui è garantita l'assoluta casualità ci sono invece quelli descritti dalla fisica quantistica e proprio su questi fenomeni si basa lo sviluppo degli Qrng, costituiti da una sorgente casuale e da un rivelatore e le cui tipologie dipendono dal fenomeno fisico quantistico che si intende sfruttare. Molti generatori odierni si basano per esempio su sistemi fotonici, realizzabili con relativa semplicità, a basso costo e con dimensioni che ne permettono l'inserimento in dispositivi pratici. Nella pratica, tuttavia, i dispositivi sorgente e rivelatore si discostano dal modello teorico e introducono un rumore dipendente da variabili classiche: ciò può inficiare, o essere utilizzato malevolmente per inficiare la perfetta casualità del risultato, introducendo una polarizzazione, effetto che può essere rimosso, tramite metodi di randomness extraction, se è noto un modello teorico sufficientemente accurato dei dispositivi.

Esiste per esempio una soluzione, detta semi self-testing, in cui è noto con sufficiente accuratezza il modello di uno solo dei due dispositivi (sorgente o rivelatore). Questa soluzione permette di raggiungere frequenze di generazione sufficienti per molte applicazioni pratiche.

IL MERCATO DELLE TECNOLOGIE QUANTISTICHE: L'ANALISI DI MCKINSEY (2022)

Gran parte dei finanziamenti per la ricerca di base nell'informatica quantistica proviene ancora da fonti pubbliche ma stanno aumentando rapidamente i finanziamenti privati: solo nel 2021, gli investimenti annunciati nelle start-up di informatica quantistica hanno superato a livello globale gli 1,7 miliardi di dollari, più del doppio dell'importo raccolto nel 2020.

La vera svolta nella diffusione dell'impiego dell'informatica quantistica sarà il raggiungimento di un calcolo quantistico fault tolerant, dunque in grado di fornire risultati esatti e matematicamente accurati (il rumore tecnico nell'elettronica, nei laser e in altri componenti dei computer quantistici porta a piccole imperfezioni in ogni singola operazione di calcolo. Questi piccoli errori alla fine portano a risultati di calcolo errati. Tali errori possono essere contrastati codificando un qubit logico in modo ridondante in più qubit fisici. Si parla di decoherence quando un sistema quantistico perde la sua proprietà di superposition: questa è una delle principali fonti di errori quando si lavora con i computer quantistici).

Gli esperti, infatti, non sono d'accordo sul fatto che i computer quantistici possano creare valore di business prima di diventare fault tolerant e i maggiori produttori di hardware hanno annunciato il raggiungimento di questo traguardo entro il 2030.

La maggior parte delle startup operanti nel campo dell'informatica quantistica si occupano di sviluppano software e i principali attori, per creare comunità di sviluppatori attorno alle loro offerte, spesso forniscono gratuitamente servizi di quantum computing basati su Cloud (è ad esempio possibile attivare un account gratuito sul sistema Quantum Experience di Ibm - https://quantum-computing.ibm.com - per creare e mandare in esecuzione un proprio "circuito quantistico").

I casi d'uso più noti delle tecnologie quantistiche rientrano in quattro tipologie: simulazione quantistica, algebra lineare quantistica per intelligenza artificiale e apprendimento automatico (machine learning migliorato grazie ad una struttura previsionale più rapida, dovuta al calcolo parallelo), ottimizzazione e ricerca quantistica e fattorizzazione quantistica.

Secondo McKinsey ("Quantum Compu-

L'IMPATTO DELL'INFORMATICA QUANTISTICA SUI SETTORI INDIVIDUATI DA MCKINSEY

Tipologia di industria	Risultato applicativo
Farmaceutica	• Ricerca più veloce, mirata ed economica di nuovi farmaci. Il possibile impatto in termini economici, stimando un range di incidenza da 1 a 5% sull'incremento di fatturato annuo, sarebbe inquadrabile tra i 15 e i 75 miliardi di dollari, con un'incidenza fiscale variabile tra i 2 e i 12 miliardi (Ebit). • Migliore valutazione dell'assorbimento di un farmaco e della sua eliminazione da parte dell'organismo (esempio: stima della solvibilità dei farmaci candidati attraverso la barriera ematoencefalica, che attualmente impedisce alla maggior parte degli agenti terapeutici di entrare nel cervello; ottimizzazione dei dosaggi). • Selezione ottimizzata dei gruppi umani per i test farmacologici. • Generazione di algoritmi di apprendimento automatico per colmare i dati di sperimentazione mancanti, soprattutto nel caso di malattie rare. • Personalizzazione dei trattamenti. • Migliore comprensione del ruolo di un gene o una proteina in una malattia. • Migliore previsione della struttura proteica (ripiegamento proteico). • Miglioramento di produzione e logistica. (Ulteriori miglioramenti in campo medico, ad esempio disponendo di immagini ancora più dettagliate (Advanced Imaging), oppure ottimizzando trattamenti di radioterapia in tempi molto più brevi di oggi).
Chimica	• Miglioramento in ambito ricerca, sviluppo, produzione e approvvigionamento (un notevole impatto è ad esempio atteso nella progettazione dei catalizzatori, che da soli incidono per 800 miliardi di dollari all'anno. I vantaggi stimati da McKinsey variano, in questo caso, da 20 a 40 miliardi di dollari all'anno). • Previsione delle strutture molecolari e della tossicità già nelle prime fasi di sviluppo, ad esempio, di prodotti chimici più sicuri per l'ambiente. • Ricerca e messa a punto di nuovi materiali/vernici anticorrosive/lubrificanti/semiconduttori e simili. • Ricerca e messa a punto di nuovi fertilizzanti.
Automobilistica	• Miglioramento in ricerca e sviluppo, progettazione, approvvigionamento, mobilità, gestione del traffico (ad esempio, pianificazione del percorso in complessi processi multirobot). • Risparmi in prototipazione e test. • Guida autonoma. • Sviluppo di carburanti avanzati. • Sviluppo di materiali migliori per lo stoccaggio dell'idrogeno e le batterie. • Ottimizzazione nelle prestazioni dello scambiatore di calore. • Ispezione ottica automatica e manutenzione predittiva. • Gestione delle flotte e del traffico. (McKinsey stima che un aumento della produttività pari al 2%, per un'industria che, solo in costi di produzione, impegna 500 miliardi all'anno, potrebbe generare un valore utile variabile da 10 a 25 miliardi di dollari).
Finanziaria	• Gestione del portafoglio e del rischio (ad esempio, prestiti ottimizzati). • Sicurezza finanziaria (alternative agli algoritmi Rsa). • Modellazione della previsione delle frodi. • Ottimizzazione delle strategie di trading. • Simulazioni di mercato. • Previsioni finanziarie.

ting: an emerging ecosystem and industry use cases", 2022), in particolare alcuni settori potrebbero trarre i maggiori benefici a breve termine dalla tecnologia: farmaceutico, chimico, automobilistico e finanziario. Complessivamente (e prudentemente), il valore in gioco per questi settori potrebbe essere compreso fra circa 300-700 miliardi di dollari.

A medio termine, fino al 2030 circa, i casi d'uso del calcolo quantistico avranno un modello operativo ibrido quantistico-Hpc (High Performance Computer). A lungo termine, sei fattori chiave (finanziamenti, accesso all'hardware, standardizzazione, consorzi di settore, talento e infrastruttura digitale) determineranno il percorso dell'informatica quantistica verso la commercializzazione.

LE TECNOLOGIE QUANTISTICHE NELL'INDUSTRIA 4.0

Nell'Industria 4.0, le tecnologie quantistiche possono trovare applicazione attraverso:

• maggiore sicurezza infrastrutturale;

• gateway Qkd in alcuni punti del processo di produzione ("isole" lungo la catena di montaggio, supply chain con i fornitori)

• chiavi quantistiche per proteggere il data plane di sistemi cyberfisici (ad esempio, robot, droni) a breve termine;

• sviluppo di una stazione Qkd mobile (modulo Qkd montato su robot), nel medio termine;

• robot come mobile trusted repeater per reti Qkd, a lungo termine;

• sviluppo di reti Qkd con nodi cyberfisici e stazionari - a lungo termine.

Le supply chain si stanno spostando da un modello lineare, con processi discreti, sequenziali e basati su eventi, a un modello più reattivo, basato sull'evoluzione delle richieste del mercato in tempo reale. Aggiungendosi alle tecnologie chiave di Industria 4.0, il calcolo quantistico potrebbe potenzialmente accelerare il processo

I SEI FATTORI CHIAVE CHE INFLUENZANO I PROGRESSI NELL'INFORMATICA QUANTISTICA SECONDO MCKINSEY: SITUAZIONE ODIERNA E PROSPETTIVE

FINANZIAMENTI

Sono cresciuti in modo significativo gli investimenti privati al punto che scarseggiano le startup in grado di assorbirli. Si rende necessaria una distribuzione dei finanziamenti su un'ampia fascia di imprese di calcolo quantistico.

ACCESSIBILITÀ

Rendere l'hardware quantistico accessibile come servizio Cloud, a prezzi accessibili, sarà fondamentale. Sebbene esistano già servizi Cloud di calcolo quantistico, i provider dovranno aumentare la capacità hardware per soddisfare la crescente domanda.
I principali fornitori di Cloud e Hpc integreranno anche il miglior hardware quantistico disponibile nei loro servizi e faciliteranno l'esecuzione di flussi di lavoro ibridi quantistici-convenzionali: la tecnologia quantistica costituirà effettivamente una sorta di "coprocessore" per l'infrastruttura informatica convenzionale.
Inoltre, i fornitori di hardware e software dovrebbero sviluppare e promuovere un linguaggio di programmazione standardizzato, open source e indipendente dall'hardware per abbassare la barriera di accesso per gli sviluppatori di software che vogliano impegnarsi nella programmazione quantistica.

STANDARDIZZAZIONE

Gli standard del settore, per elementi come interfacce e linguaggi di programmazione, saranno importanti per semplificare la collaborazione all'interno dell'ecosistema del calcolo quantistico. Allo stesso modo, le metriche delle prestazioni per l'hardware quantistico sono necessarie per creare trasparenza e sicurezza per gli utenti finali.
Il benchmarking è oggetto di un intenso dibattito all'interno del settore, soprattutto perché le prestazioni di ciascuna piattaforma hardware quantistica dipendono ancora fortemente dalle metriche specifiche.

CONSORZI DI SETTORE

I consorzi di partecipanti provenienti da tutto l'ecosistema quantistico, compreso il mondo accademico, possono guidare la standardizzazione, identificare casi d'uso praticabili e sfruttare l'informatica quantistica per affrontare le sfide globali, come il cambiamento climatico. In Europa e negli Stati Uniti si sono già formati consorzi industriali e accademici.

TALENTI

La scarsità di talenti è una delle principali preoccupazioni dell'informatica quantistica. Si prevede che, senza misure di mitigazione attive (ad esempio collaborazioni con le università), la carenza di talenti sarà risolta solo dopo il 2030.

INFRASTRUTTURE DIGITALI

Molti campi che potrebbero trarre vantaggio dall'informatica quantistica mancano ancora dell'infrastruttura digitale di base: le aziende dovranno evolvere fin d'ora le proprie piattaforme di dati e i processi di governance degli stessi.

decisionale e migliorare la gestione del rischio per ridurre i costi operativi, nonché perdite a causa di prodotti esauriti o fuori produzione.

Migliorando l'agilità competitiva, l'informatica quantistica potrebbe infatti trasformare completamente la catena di approvvigionamento, riprogettandola in modo adattivo per ottimizzare gli ordini dei fornitori e accompagnare la logistica utilizzando un processo decisionale dinamico quasi in tempo reale, basato sulle mutevoli richieste del mercato.

Nel campo della sensoristica, le tecnologie quantistiche sono ritenute promettenti per la ricerca di giacimenti di petrolio e di gas e per la geodesia di precisione. Per quanto riguarda la possibilità di avere una scansione del tempo di elevatissima precisione, le tecnologie quantistiche si rileveranno utili, ad esempio nelle smart energy grid, nei sistemi di navigazione. I moderni processi di controllo nella produzione hanno un pesante impatto computazionale, soprattutto nei casi in cui si utilizzi l'apprendimento automatico. L'informatica quantistica potrebbe aiutare a trovare nuove correlazioni nei dati e migliorare la classificazione, rispetto all'informatica classica. Si prevede che la combinazione di calcolo quantistico e apprendimento automatico, soprattutto nella sua applicazione all'ottimizzazione, avrà un impatto significativo nella produzione in aree come:

- fabbricazione di chip a semiconduttore: qui si utilizzano già l'apprendimento automatico e una semplice analisi multivariabile, ma il quantum computing potrebbe aumentare in modo significativo la resa della produzione;
- flussi di produzione e pianificazione della robotica per prodotti complessi, come le automobili: il calcolo quantistico potrebbe consentire ottimizzazione più rapide e dinamiche;
- controllo di qualità nello sviluppo del software (poiché le funzionalità di prodotto sono sempre più definite dal software): i futuri computer quantistici dovrebbero avere la capacità di analizzare software sostanzialmente più complessi di quanto i computer classici riescono a valutare oggi, rilevando ad esempio anomalie statistiche, e classificando dati non strutturati.

Ma come capire, nel concreto, quando è opportuno usare un computer quantistico? L'unità di analisi è sempre lo specifico caso

CONVIENE DAVVERO IMPEGNARSI NELL'INFORMATICA QUANTISTICA?

Ecco una breve check list di domande da porsi:

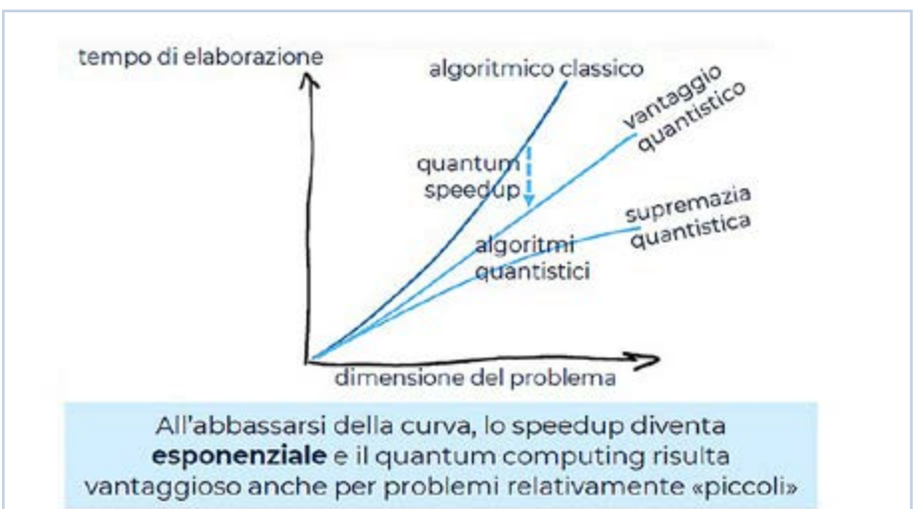
- Ho veramente bisogno di una applicazione quantistica?
- Il valore economico raggiunto dall'accelerazione quantistica, o la risoluzione di un problema precedentemente irrisolvibile, giustifica l'investimento?
- Quanto è necessaria una velocità quantistica per creare un vantaggio pratico rispetto agli Hpc convenzionali?
- Come posso avere accesso a un vero computer quantistico?
- Di quale quantum computing hardware/modello ho bisogno (Universal QC/Quantum Simulator/ Quantum Annealer...)?
- Conosco l'equivalente quantistico del miglior algoritmo digitale?
- Devo sviluppare un nuovo algoritmo per quantum computing? Esiste già in letteratura o non esiste?
- Di quali competenze ho bisogno (informatici/fisici/ingegneri...)?
- Come posso collaudare/validare l'algoritmo quantistico?
- Ho davvero bisogno di un quantum computing o posso usare un emulatore?
- Come posso calcolare la quantità di risorse umane necessarie?
- Quali esperimenti su piccola scala (basso budget) posso pianificare ed effettuare?
- Quali sono le competenze necessarie per l'utilizzo?
- Essere un early mover in questo ambito garantirà un vantaggio strategico a lungo termine?

d'uso e per esso, possiamo distinguere fra:
- quantum speedup, che si ha quando, per uno specifico problema, un algoritmo quantistico supera un algoritmo classico in termini di scalabilità rispetto alla crescita del problema;
- vantaggio quantistico: quando un computer quantistico può eseguire un particolare calcolo in modo significativamente più veloce del miglior computer classico. Il vantaggio quantistico può essere considerato la dimostrazione pratica del quantum speedup,
- supremazia quantistica, che si manifesta quando il computer quantistico riesce a risolvere un problema che non sarebbe risolvibile da un computer classico, almeno in un tempo ragionevole.

GLI SVILUPPI IN EUROPA, IN ITALIA E NEL RESTO DEL MONDO

Lo sviluppo di un'infrastruttura quantistica di comunicazione si ritiene costituisca un prerequisito fondamentale affinché l'Europa possa competere sul piano internazionale. Nelle linee guida politiche, presentate per la Commissione Europea 2019-2024, le tecnologie quantistiche ricoprono infatti una posizione di primo piano, insieme a 5G, intelligenza artificiale e blockchain. Per affrontare questa sfida, nel 2018 è stata lanciata la Quantum Technologies Flagship, un'iniziativa di ricerca a lungo termine che riunisce istituti di ricerca, industrie e finanziatori pubblici e prevede investimenti di 1 miliardo di euro per dieci anni.
Obiettivi della Quantum Flagship sono: consolidare ed espandere la leadership scientifica europea nella ricerca quantistica; dare avvio a un'industria europea competitiva nell'ambito delle tecnologie quantistiche con la prospettiva di rendere l'Europa leader nel futuro panorama industriale globale; attrarre in Europa ricerca, business ed investimenti in tecnologie quantistiche. Nello specifico della Quantum Communication, gli obiettivi sono: integrare la crittografia quantistica nei sistemi di comunicazione critici; combinare componenti terrestri e satellitari per ampliare la copertura; proteggere le reti dati (ad esempio, per clock synchronization ed e-voting); realizzare un'infrastruttura di backbone per la Quantum Internet. All'interno della Flagship, è stata firmata nel giugno 2019, da 26 Stati membri dell'UE, la dichiarazione EuroQci

Figura 5. Speedup e supremazia quantistica



Fonte: rielaborazione Osservatorio Quantum Computing del Politecnico di Milano, 2022

INVESTIMENTI PUBBLICI NELLA RICERCA SULLE TECNOLOGIE QUANTISTICHE

Area geografica	Orizzonte temporale	Investimenti (miliardi dollari/anno)
Asia (principalmente Cina)	2014/2030	613
Europa	2014-2029	517
Stati Uniti	2018-2022	250
Russia	2020-2024	165
Canada	2010-2019	74

Fonte: osservatorio Quantum Computing del Politecnico di Milano, dati luglio 2021

(European Quantum Communication Infrastructure), per sviluppare un'infrastruttura di comunicazione quantistica sicura che copra l'intera Unione, integrando infrastrutture convenzionali in fibra ottica e un segmento spaziale. Nello specifico, uno degli obiettivi dichiarati di EuroQci è rendere disponibili servizi di Qkd. L'obiettivo a lungo termine è che la rete Qci diventi la spina dorsale dell'Internet quantistico europeo, il quale, collegando computer quantistici, permetterà analisi e previsioni con un'accuratezza senza precedenti su scala globale e in totale sicurezza. Nel 2021, la Commissione Europea ha individuato un consorzio di aziende e istituti di ricerca per studiare la progettazione della futura rete europea di comunicazione quantistica. Il consorzio europeo, guidato da Airbus, è composto da Leonardo, Orange, PwC France e Maghreb, Telespazio, il Consiglio Nazionale delle Ricerche (Cnr) e l'Istituto Nazionale di Ricerca Metrologica (INRiM). Lo studio, della durata di 15 mesi, intende progettare il segmento terrestre a supporto servizio Qkd. L'obiettivo è quello di far funzionare un dimostratore EuroQci entro il 2024 e un servizio operativo iniziale entro il 2027. In Italia, il Pnrr ha stanziato 1,6 miliardi di euro nella creazione di Campioni Nazionali di R&S nelle Key Enabling Technology, tra cui le tecnologie quantistiche. Già nel gennaio 2021 il Programma Nazionale per la Ricerca 2021-2027 del Ministero dell'Università e della Ricerca specificava che "per la loro natura abilitante, le Quantum Technology (QT) richiedono una priorità di investimento molto elevato, giustificata dalle proiezioni macroscopiche che prevedono (...) un impatto significativo sia sul PIL sia sui livelli occupazionali (...) i Paesi avanzati si divideranno che avranno accesso diretto alle QT e quelli che non lo avranno. I primi potranno ambire ad acquisire una leadership tecnologica, mentre gli altri potrebbero sperimentare gravi problemi di dipendenza per le infrastrutture strategiche e la propria sicurezza nazionale".