REPORT TECNOLOGICO

Perché il futuro dell'informatica è ibrido

Classico e quantistico insieme: calcolo, reti e crittografia nell'era della convergenza

Analisi su hybrid computing, algoritmi quantistici, error correction, quantum networking e post-quantum cryptography

Agosto 2026

Indice

Perché il futuro dell'informatica è ibrido: classico e quantistico insieme

Per decenni l'informatica quantistica è stata raccontata come una tecnologia destinata a *sostituire* quella classica: computer capaci di risolvere in pochi secondi problemi che oggi richiederebbero secoli ai supercomputer più potenti. La realtà che sta emergendo nei laboratori e nei data center di tutto il mondo è molto diversa e, per certi versi, più interessante: il futuro non sarà "quantistico al posto di classico", ma **quantistico insieme a classico**, in architetture sempre più intrecciate tra loro.

I processori quantistici (QPU) eccellono in un insieme ristretto ma prezioso di problemi — ottimizzazione combinatoria, simulazione molecolare, alcuni compiti di crittografia e di machine learning — grazie a fenomeni come la sovrapposizione e l'entanglement. Ma restano del tutto inadatti a compiti come l'inserimento dati, la gestione della memoria, il rendering grafico o l'addestramento di modelli linguistici di grandi dimensioni, dove le CPU e le GPU classiche continuano a essere insostituibili. Da questa complementarità nasce l'esigenza di un'infrastruttura ibrida.

> *Il futuro non sarà quantistico al posto di classico, ma quantistico insieme a classico: non sostituzione di un paradigma, ma integrazione sempre più stretta tra i due mondi.*

Il punto centrale, però, non è *se* classico e quantistico debbano collaborare, ma *come*. Ed è qui che emerge una distinzione cruciale tra due modelli di cooperazione molto diversi: l'architettura **sequenziale** (o "a isole separate") e l'architettura **ibrida stretta** (tightly-coupled), in cui i due tipi di computazione si intrecciano in tempo reale.

Il modello sequenziale: due computer che si passano la palla

Nel modello più semplice — e storicamente il primo a essere implementato nei servizi cloud di calcolo quantistico — un computer classico prepara i parametri di un problema, li invia a un computer quantistico attraverso una rete o un servizio cloud, attende che il QPU esegua il calcolo e riceve indietro un risultato. È un flusso lineare, quasi "a richiesta-risposta", che viene attivato solo per quella classe ristretta di problemi in cui il vantaggio quantistico è netto e dimostrabile.

Vantaggi di questo approccio

- **Semplicità architetturale.** Non serve un'infrastruttura di interconnessione dedicata e a bassissima latenza tra CPU e QPU: bastano un'API e una connessione di rete, esattamente come avviene oggi con i servizi di quantum computing su cloud pubblico (IBM Quantum, Azure Quantum, Amazon Braket).
- **Isolamento e affidabilità.** Se il computer quantistico non è disponibile o restituisce un errore, il sistema classico continua a funzionare autonomamente; i due domini sono disaccoppiati e più facili da testare, aggiornare e mettere in sicurezza separatamente.
- **Accessibilità.** Le aziende possono sperimentare il quantum computing senza possedere hardware quantistico proprio, affittando tempo di calcolo su QPU remoti e integrandolo in applicazioni classiche già esistenti.

- **Adatto a problemi "chiusi".** Per compiti ben definiti, con un input e un output netti (es. un problema di ottimizzazione che si risolve una tantum), il modello sequenziale è più che sufficiente e non introduce complessità inutile.

Svantaggi e limiti

- **Latenza e overhead di comunicazione.** Ogni chiamata al QPU comporta tempi di coda, trasferimento dati e sincronizzazione che possono superare di gran lunga il tempo di calcolo effettivo, specialmente su servizi cloud condivisi.
- **Inadeguatezza per gli algoritmi variazionali.** Molti degli algoritmi quantistici più promettenti nel breve-medio termine — come VQE (*Variational Quantum Eigensolver*) o QAOA (*Quantum Approximate Optimization Algorithm*) — richiedono **migliaia di iterazioni rapide** tra classico e quantistico per ottimizzare parametri, non un singolo scambio di dati. Il modello sequenziale, con la sua latenza intrinseca, rende questi cicli enormemente più lenti e costosi.
- **Nessuna mitigazione degli errori in tempo reale.** L'hardware quantistico attuale (l'era cosiddetta NISQ, *Noisy Intermediate-Scale Quantum*) è rumoroso e soggetto a decoerenza. Senza un dialogo stretto e veloce con il classico, diventa difficile correggere gli errori mentre il calcolo è in corso.
- **Sottoutilizzo del QPU.** Le risorse quantistiche, ancora scarse e costose, rischiano di restare inattive durante le fasi di preparazione e trasferimento dati, riducendo il ritorno sull'investimento.

Il modello ibrido stretto: quantistico e classico che "respirano insieme"

Nell'architettura ibrida stretta, QPU, CPU e GPU non si limitano a scambiarsi un risultato finale: **collaborano in cicli continui e ravvicinati**, spesso nello stesso data center o addirittura sullo stesso rack, con interconnessioni ad altissima velocità (come NVQLink di NVIDIA o le architetture di quantum-centric supercomputing di IBM). Un esempio concreto: nella tecnica SQD (Sample-based Quantum Diagonalization) sviluppata da IBM insieme ad AMD e NVIDIA, il QPU esegue i circuiti quantistici mentre le GPU elaborano in parallelo le operazioni tensoriali più pesanti, in un processo che ha permesso di ottenere un miglioramento di velocità di circa 100 volte rispetto ai soli metodi classici, con ulteriori guadagni prestazionali tra 1,8 e 3 volte grazie all'aggiunta di GPU AMD e NVIDIA di ultima generazione.

Vantaggi di questo approccio

- **Sfrutta al meglio l'hardware NISQ.** Il ciclo iterativo continuo tra QPU e classico consente tecniche di mitigazione e correzione degli errori in tempo reale, cruciali finché non esisteranno QPU pienamente fault-tolerant.
- **Abilita nuove classi di algoritmi.** Gli algoritmi ibridi variazionali diventano realmente praticabili quando la latenza tra le migliaia di iterazioni classico-quantistico è ridotta al minimo, aprendo la strada ad applicazioni in chimica computazionale, scoperta di farmaci, scienza dei materiali e ottimizzazione logistica su larga scala.
- **Massimizza l'utilizzo delle risorse quantistiche.** Integrando il QPU come acceleratore specializzato all'interno di un cluster HPC (esattamente come oggi avviene con le GPU), si riduce il tempo morto e si aumenta il throughput complessivo del sistema.
- **Prepara il terreno per il fault-tolerant computing.** Anche quando i computer quantistici diventeranno più affidabili, la correzione d'errore in tempo reale continuerà a richiedere una potenza di calcolo classica enorme: l'infrastruttura ibrida stretta costruita oggi sarà la base di quella di domani.

Svantaggi e sfide

- **Complessità ingegneristica.** Sincronizzare hardware con caratteristiche fisiche radicalmente diverse (temperature criogeniche per i QPU superconduttori, condizioni operative standard per CPU/GPU) richiede soluzioni di interconnessione, orchestrazione e software estremamente sofisticate.
- **Costi infrastrutturali elevati.** Servono reti a bassissima latenza, hardware dedicato e, spesso, la co-locazione fisica di QPU e sistemi classici: un investimento significativamente più alto rispetto al semplice accesso cloud sequenziale.
- **Scarsità di competenze.** Progettare software per questi sistemi richiede professionisti che padroneggino sia l'informatica quantistica sia l'HPC classico, un profilo professionale ancora raro sul mercato.
- **Ecosistema e standard immaturi.** Framework come CUDA-Q di NVIDIA o le architetture quantum-centric di IBM stanno ancora convergendo verso standard comuni; il rischio di lock-in verso un singolo fornitore hardware o software è concreto.
- **Banchi di prova limitati.** La ricerca stessa segnala che, nonostante le solide basi teoriche, mancano ancora infrastrutture sperimentali su larga scala e dataset empirici che dimostrino i benefici in produzione, non solo in laboratorio.

Caratteristica	Modello sequenziale	Modello ibrido stretto
Latenza tra classico e QPU	Alta (coda cloud, trasferimento dati)	Minima (co-locazione, interconnessioni dedicate)
Adatto a	Problemi isolati, un solo scambio di dati	Algoritmi iterativi (VQE, QAOA), QEC in tempo reale
Costo infrastrutturale	Basso, accesso via cloud pubblico	Elevato, hardware dedicato e co-locato
Complessità ingegneristica	Bassa	Alta (sincronizzazione, orchestrazione)
Maturità dell'ecosistema	Consolidata (IBM Quantum, Azure, Braket)	In rapida evoluzione (CUDA-Q, NVQLink)

Tabella 1. Confronto sintetico tra architettura sequenziale e architettura ibrida stretta.

Gli algoritmi ibridi in azione: VQE e QAOA

Se c'è una prova concreta del perché l'architettura ibrida stretta non sia un capriccio ingegneristico ma una necessità, è negli algoritmi che oggi rappresentano il cuore pulsante del quantum computing nell'era NISQ: il **VQE** (Variational Quantum Eigensolver) e il **QAOA** (Quantum Approximate Optimization Algorithm).

Entrambi condividono la stessa architettura di fondo, chiamata "loop variazionale": un circuito quantistico parametrico viene eseguito sul QPU, il risultato della misura viene inviato a un ottimizzatore classico (algoritmi come COBYLA, SPSA o metodi basati sul gradiente), quest'ultimo aggiorna i parametri del circuito per avvicinarsi a un obiettivo — minimizzare un'energia, massimizzare una funzione di costo — e il ciclo si ripete. Non una volta, ma **centinaia o migliaia di volte**, fino a convergenza.

- **VQE** è pensato principalmente per la chimica computazionale: stima l'energia dello stato fondamentale di una molecola, un calcolo cruciale per la scoperta di farmaci, la progettazione di catalizzatori e lo sviluppo di nuovi materiali (ad esempio per batterie o celle solari più efficienti).
- **QAOA** è invece rivolto a problemi di ottimizzazione combinatoria — instradamento logistico, pianificazione, allocazione di portafogli finanziari, problemi di tipo max-cut — alternando strati di operatori quantistici la cui intensità è governata da parametri ottimizzati classicamente.

Il motivo per cui questi algoritmi *richiedono* un'architettura ibrida stretta è evidente: i QPU attuali sono rumorosi e possono eseguire solo circuiti relativamente brevi prima che la decoerenza distrugga l'informazione quantistica. VQE e QAOA sono stati progettati proprio per convivere con questo limite, usando circuiti poco profondi e delegando la parte "pesante" dell'ottimizzazione al calcolo classico. Ma questo scambio continuo funziona solo se la latenza tra un'iterazione e l'altra è minima: con un modello sequenziale basato su cloud, ogni singola iterazione sconterebbe tempi di coda e trasferimento dati, moltiplicando per migliaia di volte un ritardo che diventerebbe rapidamente insostenibile.

Restano, tuttavia, limiti aperti: il fenomeno dei "*barren plateaus*" (gradienti che si annullano al crescere del numero di qubit, rendendo l'ottimizzazione sempre più difficile), la sensibilità al rumore hardware e l'assenza, a oggi, di una dimostrazione univoca di vantaggio quantistico netto rispetto alle migliori euristiche classiche per la maggior parte dei casi d'uso reali. VQE e QAOA restano quindi banchi di prova fondamentali, più che soluzioni già mature su scala industriale.

Il ruolo cruciale della correzione d'errore quantistica

Se gli algoritmi variazionali mostrano perché il classico e il quantistico devono dialogare *durante* il calcolo, la correzione d'errore quantistica (QEC, Quantum Error Correction) mostra perché devono farlo a una velocità quasi impensabile. Abbiamo già trattato l'argomento nel nostro Approfondimento del 29 maggio 2026; lo riprendiamo in questa sede in quanto esempio pratico di integrazione ibrida.

I qubit fisici sono estremamente fragili: basta un'interazione con l'ambiente circostante, una vibrazione, un fotone indesiderato, per introdurre un errore che si propaga rapidamente nel calcolo (decoerenza). La soluzione concettuale, nota fin dagli anni '90, è codificare un singolo **qubit logico** — stabile e affidabile — distribuendo l'informazione su molti **qubit fisici** ridondanti, secondo schemi come il *surface code* o i più recenti codici *qLDPC* (quantum Low-Density Parity-Check). Il sistema misura continuamente delle "sindromi di errore" senza toccare direttamente lo stato quantistico codificato (per non distruggerlo), e queste sindromi devono essere interpretate e corrette.

Ed è qui che il classico diventa indispensabile: il **decoding**, cioè la traduzione delle sindromi misurate in istruzioni di correzione concrete, è un calcolo che deve avvenire in tempo reale, entro il tempo di coerenza dei qubit — nell'ordine dei **microsecondi**. Un decoder troppo lento significa che gli errori si accumulano più velocemente di quanto vengano corretti, vanificando l'intero impianto della QEC. Per questo motivo sono nati decoder hardware dedicati (spesso basati su FPGA o chip specializzati), fisicamente vicini al criostato che ospita i qubit superconduttori, capaci di decodificare in meno di un microsecondo.

Il paradosso interessante è questo: più i computer quantistici diventeranno grandi e affidabili, **più — non meno — cresceranno le esigenze di calcolo classico**. Con l'aumentare del numero di qubit fisici necessari per ogni qubit logico e con la scalata verso sistemi fault-tolerant, il volume di dati di sindrome da decodificare in tempo reale cresce enormemente. Non a caso, le roadmap di IBM verso sistemi fault-tolerant entro la fine del decennio prevedono di incorporare direttamente GPU e calcolo classico all'interno dell'infrastruttura criogenica dei sistemi quantistici, proprio per gestire la correzione d'errore in tempo reale su larga scala. La

QEC, in altre parole, è forse l'esempio più estremo — e più necessario — di cooperazione ibrida stretta tra i due mondi.

Sequenziale o ibrido stretto? Una questione di problema, non di dogma

Nessuno dei due modelli è "superiore" in assoluto: la scelta dipende dal tipo di problema da risolvere. Per compiti isolati, con un vantaggio quantistico dimostrato e un solo scambio di dati (ad esempio la fattorizzazione di un numero o un singolo problema di ottimizzazione ben definito), il modello sequenziale resta efficiente, economico e più che adeguato. Per contro, ogni volta che il problema richiede iterazione, apprendimento progressivo o correzione d'errore continua — cioè per la stragrande maggioranza degli usi pratici del quantum computing nell'era NISQ — l'architettura ibrida stretta è destinata a diventare lo standard. Non a caso, gli osservatori del settore prevedono che nel 2026 il calcolo ibrido quantistico-classico, supportato da piattaforme middleware come CUDA-Q, possa diventare la modalità di implementazione standard nei data center, con i QPU sempre più integrati come acceleratori nei cluster di calcolo ad alte prestazioni.

Chi sta costruendo questo futuro

La transizione verso l'informatica ibrida stretta non è più solo teoria accademica: è già una priorità strategica per i principali attori del settore tecnologico.

- **IBM** punta su un'architettura di *quantum-centric supercomputing*, dimostrando insieme ai suoi partner risultati concreti come il già citato speedup di 100 volte ottenuto integrando QPU e GPU presso il supercomputer Frontier dell'Oak Ridge National Laboratory e il supercluster Miyabi del RIKEN in Giappone.
- **AMD** ha stretto una partnership con IBM incentrata su architetture di supercalcolo quantum-centriche che uniscono processori quantistici, HPC e risorse di intelligenza artificiale, mettendo a disposizione CPU EPYC, GPU Instinct e SoC adattivi Versal come infrastruttura classica per i sistemi quantistici. AMD collabora inoltre con organizzazioni come JPMorganChase e l'Oak Ridge National Laboratory per esplorare l'integrazione tra sistemi quantistici, intelligenza artificiale e calcolo ad alte prestazioni.
- **NVIDIA** sta emergendo come uno snodo centrale di questa convergenza grazie alla piattaforma software CUDA-Q e all'interconnessione NVQLink, pensata per collegare in tempo reale QPU e GPU. La stessa **Google Quantum AI** utilizza l'infrastruttura NVIDIA per simulare sistemi quantistici a 40 qubit impiegando oltre 1.000 GPU H100, mentre la startup **Infleqtion** ha annunciato l'integrazione dei propri computer quantistici Sqale con i sistemi GPU NVIDIA tramite NVQLink presso l'Illinois Quantum & Microelectronics Park, per abilitare un'architettura unificata di calcolo ibrido in tempo reale.
- **Microsoft**, con la piattaforma Azure Quantum, continua a proporsi come livello di integrazione tra hardware quantistico eterogeneo e flussi di lavoro classici già esistenti nel cloud, puntando nel lungo periodo su architetture fault-tolerant di tipo topologico.
- Sul fronte specifico della correzione d'errore in tempo reale, la britannica **Riverlane** è oggi uno degli specialisti più citati del settore: con il suo stack Deltaflow e decoder hardware capaci di decodificare errori in meno di un microsecondo, l'azienda collabora con diversi produttori di hardware quantistico per raggiungere la scala del "MegaQuOp" (un milione di operazioni quantistiche prive di errore). Accanto a lei operano **Quantum Machines** (piattaforma di controllo OPX1000) e **Q-CTRL** (software di mitigazione Fire Opal), mentre Google e IBM continuano a pubblicare i propri progressi su surface code e codici qLDPC.

E l'internet quantistico? Ibrido, separato-ma-cooperativo, o destinato a prevalere?

Lo stesso interrogativo che riguarda il calcolo — sostituzione, integrazione stretta o coesistenza a isole separate — si pone in modo speculare per le reti: l'**internet quantistico** rimpiazzerà quello classico, resterà un'infrastruttura parallela che collabora solo a distanza, o i due finiranno per fondersi in un'unica rete ibrida?

Prima di rispondere, vale la pena chiarire cosa si intende con "internet quantistico": non un sostituto della rete che trasporta video, email e pagine web, ma un'infrastruttura pensata per compiti che il quantistico sa fare meglio di chiunque altro — distribuire **entanglement** tra nodi distanti, trasmettere chiavi crittografiche intrinsecamente sicure (QKD, Quantum Key Distribution) e, in prospettiva, collegare tra loro più computer quantistici per formare cluster distribuiti più potenti di un singolo QPU. Non è pensato per sostituire il traffico dati di tutti i giorni, che classico rimarrà.

Lo scenario della sostituzione totale è il meno probabile. Le reti quantistiche non trasportano dati "in chiaro" nel senso classico: trasmettono stati quantistici fragilissimi, soggetti a decoerenza, che non possono essere amplificati con i normali ripetitori ottici (il teorema del "*no-cloning*" impedisce di copiare uno stato quantistico sconosciuto). Costruire una rete quantistica globale che rimpiazzi la fibra ottica esistente richiederebbe *repeater* quantistici, memorie quantistiche e infrastrutture ancora immature; nessun osservatore serio del settore prevede che l'internet classico venga soppiantato.

Lo scenario più concreto, oggi, è quello ibrido/cooperativo su un'unica infrastruttura fisica condivisa. La ricerca più recente mostra che segnali quantistici e classici possono coesistere sulla stessa fibra ottica già esistente, sfruttando bande di lunghezza d'onda diverse (tecniche di multiplexing WDM): un esperimento ha dimostrato che canali quantistici a più di 40 nanometri di distanza nella banda O possono co-propagarsi insieme a segnali classici ad alta potenza nella banda C mantenendo la fedeltà del segnale quantistico. Un approccio ancora più stretto è quello "classical-decisive": un segnale classico guida in tempo reale l'instradamento dell'entanglement quantistico lungo la rete, preservandone l'integrità — un protocollo ibrido che consente l'instradamento dinamico di entanglement ad alta fedeltà sulle reti in fibra già esistenti, aprendo una strada concreta verso un internet quantistico scalabile costruito sopra l'infrastruttura di oggi, non accanto ad essa.

Nel medio termine, tuttavia, prevale ancora un modello "separato ma cooperativo". Le reti quantistiche metropolitane realmente operative — a Chattanooga, a New York, a Pechino-Shanghai — funzionano oggi come infrastrutture dedicate e distinte, pensate per servire inizialmente casi d'uso specifici (sicurezza governativa, settore finanziario, ricerca) più che il traffico internet di massa. La cooperazione con la rete classica avviene a livello di orchestrazione — instradamento, gestione, interfacce software — più che di condivisione fisica del mezzo trasmissivo. È lo stesso schema già visto nel calcolo: prima isole separate che collaborano su richiesta, poi, con la maturazione tecnologica, un'integrazione via via più stretta.

> *L'internet quantistico non sostituirà quello classico, ma vi si sovrapporrà in modo sempre più stretto: prima come rete separata che dialoga solo per orchestrazione e sicurezza, poi come infrastruttura realmente ibrida sulla stessa fibra.*

Chi lavora sull'internet quantistico

- **Aliro Quantum** è oggi il principale specialista software per l'orchestrazione delle reti quantistiche: la sua piattaforma *Entanglement-as-a-Service* e il router Aliro QN permettono ai reparti IT aziendali di gestire una rete quantistica come una rete definita da software (SDN) classica. Una partnership annunciata con

Cisco nel febbraio 2026 segnala che anche gli incumbent del networking classico stanno prendendo sul serio questo strato di orchestrazione.

- **Photonic Inc.**, dopo una dimostrazione di teletrasporto quantistico su fibra metropolitana di 30 km realizzata con TELUS, sta virando verso un'esecuzione più commerciale, in stretta collaborazione con Microsoft per l'integrazione con Azure Quantum.
- **Xanadu**, produttore canadese di processori quantistici fotonici, ha firmato un accordo con **TELUS** per costruire la prima infrastruttura sovrana ibrida quantistico-classica del Canada, integrando i propri processori direttamente nella rete in fibra nazionale PureFibre.
- **China Telecom**, in collaborazione con l'Università della Scienza e Tecnologia della Cina, gestisce il dorsale di comunicazione quantistica Pechino-Shanghai, una rete di circa 2.000 km, e ha lanciato il satellite Micius per la distribuzione di chiavi quantistiche (QKD) su scala intercontinentale.
- **EPB** (l'utility elettrica di Chattanooga, Tennessee) gestisce la prima rete quantistica commerciale statunitense e sta costruendo, in collaborazione con **IonQ**, un polo che unirà calcolo e networking quantistico nella stessa struttura.
- **Qunnect** (rete GothamQ a New York), **ID Quantique** e **Qubitekk** (oggi parte di IonQ, quotata al NYSE) e **Arqit** (quotata al Nasdaq) completano il quadro dei principali attori commerciali, mentre iniziative governative come EuroQCI in Europa, AUKUS Pillar 2 e la National Quantum Initiative statunitense continuano a rappresentare la quota più consistente della domanda attuale.

La crittografia post-quantistica: la difesa classica contro la minaccia quantistica

C'è un ultimo tassello, forse il più urgente sul piano pratico, che completa il quadro della cooperazione tra i due mondi: la **crittografia post-quantistica** (PQC, Post-Quantum Cryptography). A differenza della QKD e dell'internet quantistico, che usano fenomeni fisici quantistici per proteggere le comunicazioni, la PQC è un approccio interamente **classico**: nuovi algoritmi matematici, eseguibili sui normali computer e microchip di oggi, ma progettati per resistere agli attacchi di un futuro computer quantistico.

La minaccia è concreta e ha un nome: **algoritmo di Shor** (1994). Un computer quantistico sufficientemente grande e fault-tolerant potrebbe fattorizzare numeri primi enormi ed estrarre logaritmi discreti in un tempo praticabile, demolendo di fatto le basi matematiche di RSA, Diffie-Hellman e della crittografia a curve ellittiche (ECC) — gli stessi schemi che oggi proteggono la stragrande maggioranza delle comunicazioni internet, delle transazioni bancarie, delle blockchain e dei dati governativi. Il momento in cui questo diventerà possibile viene chiamato informalmente "Q-Day", e nessuno sa con certezza quando arriverà — ma il rischio non è solo futuro: nel modello di minaccia noto come "*harvest now, decrypt later*", un avversario può intercettare e conservare oggi il traffico cifrato, in attesa di poterlo decifrare retroattivamente non appena l'hardware quantistico sarà abbastanza potente. Per dati che devono restare riservati per decenni — segreti di stato, cartelle cliniche, proprietà intellettuale — o per alcune le transazioni su cripto-valute, la minaccia è quindi già attiva, anche se il computer capace di sfruttarla non esiste ancora.

La risposta della comunità crittografica non ha aspettato l'arrivo dell'hardware quantistico. Dopo un processo di selezione durato quasi un decennio, il NIST statunitense ha pubblicato i primi standard ufficiali di crittografia resistente al quantistico, basati principalmente su problemi matematici legati ai **reticoli** (lattice-based cryptography), ritenuti sicuri anche contro un attaccante dotato di computer quantistico:

- **FIPS 203 (ML-KEM)** — per lo scambio di chiavi crittografiche;
- **FIPS 204 (ML-DSA)** — per le firme digitali;

- **FIPS 205 (SLH-DSA)** — uno schema di firma alternativo basato su funzioni hash, pensato come rete di sicurezza in caso emergessero debolezze negli schemi a reticolo;
- a questi si aggiunge l'algoritmo **HQC**, selezionato dal NIST come quinto standard per la cifratura a chiave pubblica, e un futuro **FIPS 206**, pensato per offrire firme più compatte e ottimizzate in termini di banda.

Ciò che rende questo tema perfettamente coerente con il filo conduttore ibrido dell'intero articolo è il modo in cui la migrazione sta effettivamente avvenendo: quasi nessuno sta sostituendo di colpo la crittografia classica con quella post-quantistica. La strada scelta da giganti come Google, Cloudflare e Apple (con il protocollo PQ3 di iMessage) è la **crittografia ibrida**: nella stessa connessione sicura vengono combinati un algoritmo classico consolidato (ad esempio una curva ellittica) e un algoritmo post-quantistico di nuova generazione, così che la comunicazione resti protetta anche se uno dei due schemi dovesse rivelarsi, in futuro, più debole del previsto. È lo stesso principio di prudenza ingegneristica visto nel calcolo ibrido: non si abbandona lo strumento maturo finché il nuovo non ha dimostrato piena affidabilità sul campo.

Sul piano regolatorio, la pressione sta aumentando rapidamente. Negli Stati Uniti, la Suite di Algoritmi Commerciali per la Sicurezza Nazionale 2.0 (CNSA 2.0) della NSA fissa scadenze precise per i sistemi di sicurezza nazionale, con piena adozione della crittografia quantum-resistant attesa entro il 2035, mentre un ordine esecutivo del giugno 2026 (EO-14412) impone un'accelerazione della migrazione a livello dell'intera amministrazione federale statunitense, con scadenze vincolanti per gli asset più critici. Diversi settori — difesa, banche con segreti a lunga scadenza, archivi governativi — sono attesi migrare ben prima di queste soglie generali.

Chi lavora sulla crittografia post-quantistica

- Tra gli specialisti "puri" spiccano **PQShield**, **SandboxAQ** (spin-off di Google), **ISARA** (nata come spin-out del laboratorio di ricerca di BlackBerry, oggi focalizzata su strumenti di "crypto-agilità" e inventario crittografico più che sui soli algoritmi), **Crypto4A**, **evolutionQ**, **Post-Quantum**, **QuintessenceLabs** e **Quantum Xchange**.
- Tra i grandi integratori che stanno già distribuendo la PQC su scala globale figurano **Cloudflare**, **AWS**, **Microsoft** e **Google**, che nel corso del 2026 hanno rivisto al rialzo i propri obiettivi e tempistiche per rendere le connessioni TLS "quantum-safe" per impostazione predefinita.
- Sul fronte pubblico, il NIST guida il processo di standardizzazione insieme a CISA e NSA, mentre iniziative come il *Quantum Computing Cybersecurity Preparedness Act* impongono alle agenzie federali statunitensi di censire i propri sistemi crittografici e pianificarne la migrazione — un obbligo che si riversa inevitabilmente anche sui fornitori e appaltatori privati.

In un certo senso, la crittografia post-quantistica è la prova più chiara che la convivenza tra classico e quantistico non riguarda solo l'hardware dei data center, ma l'intera infrastruttura digitale che diamo per scontata ogni giorno: non aspettiamo che il quantistico sostituisca il classico per proteggerci da esso — usiamo il classico, reso più intelligente, per blindarci in anticipo contro una minaccia che verrà dal quantistico stesso.

Conclusione

Il quadro che emerge è chiaro, tanto per il calcolo quanto per le reti e per la sicurezza che le attraversa: la corsa non è più (solo) a chi costruisce il QPU con più qubit o il collegamento quantistico più lungo, ma a chi riesce a integrare meglio, più velocemente e in modo più efficiente il quantistico con l'infrastruttura classica che già oggi sostiene gran parte del mondo digitale.

È in questa integrazione — non nella sostituzione di un paradigma con l'altro — che si gioca il futuro dell'informatica, delle reti che la collegano e della sicurezza che la protegge.