



5 miti da sfatare sul quantum computing

Scritto da [Stefano Patelli](#) il 29/07/2026

Indice dei contenuti

- [Quali sono i miti più diffusi sul quantum computing?](#)
- [Mito 1. Il computer quantistico sostituirà il computer classico?](#)
- [Mito 2. Un computer quantistico è semplicemente più veloce?](#)
- [Mito 3. La crittografia sarà rotta domani mattina?](#)
- [Mito 4. Serve hardware quantistico per iniziare?](#)
- [Mito 5. È troppo presto perché un'azienda se ne occupi?](#)
- [Perché nascono i miti sul quantum computing e chi li alimenta?](#)
- [Come si riconosce una promessa quantistica poco credibile?](#)
- [Che cosa può fare oggi un'azienda senza comprare hardware?](#)
- [Quali domande porsi prima di avviare un progetto quantistico?](#)

Nelle riunioni con imprenditori e direzioni tecniche capita spesso la stessa scena. Qualcuno cita un titolo di giornale, qualcun altro alza gli occhi al cielo, e in pochi minuti la discussione si sposta su un piano che con il calcolo quantistico ha poco a che vedere, i miti sul quantum computing nascono proprio lì, nello spazio fra un annuncio industriale scritto per gli investitori e una lettura frettolosa fatta da chi deve decidere un budget.

Abbiamo voluto allora mettere assieme i cinque miti che abbiamo sentito più spesso, convinzioni ragionevoli che però in certi contesti potrebbero portare a decisioni sbagliate, in un verso o nell'altro. C'è chi si convince di dover comprare una macchina (che non gli servirà), e c'è chi archivia il tema per altri dieci anni proprio mentre i suoi dati cifrati vengono copiati da qualche parte... ecco, entrambi gli errori possono costare parecchio.

Quali sono i miti più diffusi sul quantum computing?

I cinque miti sul quantum computing che si incontrano con maggiore regolarità riguardano la sostituzione delle macchine classiche, la natura del vantaggio, i tempi della crittografia, la necessità di hardware dedicato e il momento giusto per muoversi. Sono ricorrenti perché ognuno contiene un pezzo di verità, ed è quel pezzo a renderli resistenti; smontarli non significa ridimensionare la tecnologia, visto che il calcolo quantistico resta una delle poche direzioni credibili per problemi che oggi restano fuori portata,

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

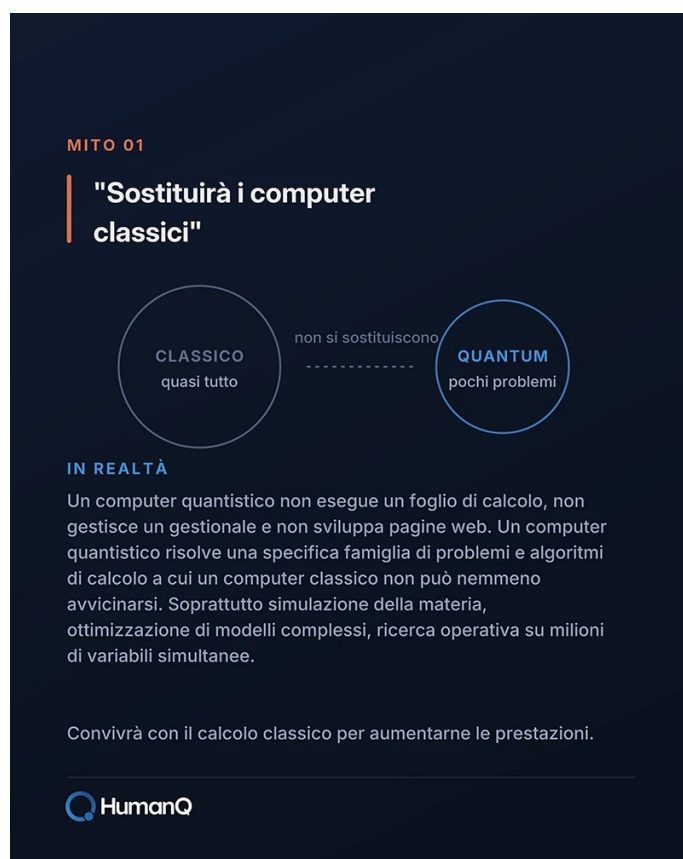
Ente accreditato
ID n. 1458 del 17/10/24



ma significa capire dove si colloca davvero il confine fra ciò che funziona in laboratorio e ciò che entrerà a breve in un reale processo aziendale.

Mito 1. Il computer quantistico sostituirà il computer classico?

Questa è la convinzione più diffusa e anche la più facile da sfatare. Un [computer quantistico](#) non manda in pensione gli attuali server aziendali, per il semplice motivo che non sa fare quasi nulla di ciò che quei server fanno oggi tutto il giorno. Il quantum non è in grado di erogare un gestionale, non sviluppa fogli di calcolo o contratti e offerte, non archivia fatture, non serve per l'archiviazione di banche dati. Al contrario invece lavora su una classe di problemi matematici totalmente diversa, e di conseguenza va pilotato da una macchina classica che prepari questi dati, li invii al circuito, valuti le risposte, raccolga i risultati e li integri nel processo aziendale o nel sistema di ricerca.



Mito 1. Il computer quantistico sostituirà il computer classico?

Il modello mentale corretto è quello dell'acceleratore. Nessuno ha smesso di usare la CPU quando sono arrivate le GPU, perché hanno semplicemente preso in carico la parte di calcolo per cui erano più adatte.

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

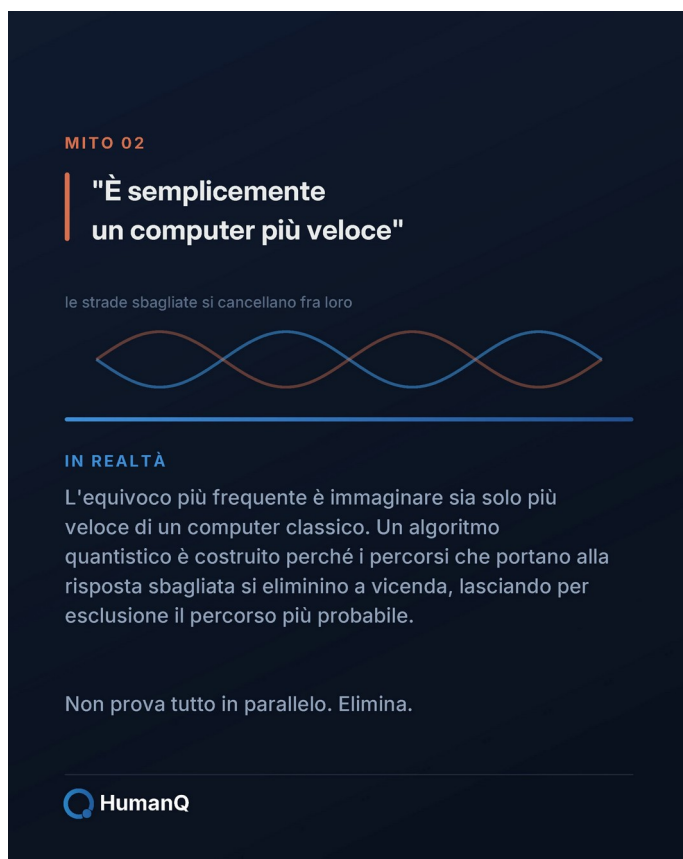
Ente accreditato
ID n. 1458 del 17/10/24



Se vuoi vedere il confronto voce per voce, è sviluppato nella pagina su [computer quantistico e computer classico](#). Il punto pratico è che nessuna architettura aziendale andrà riscritta da capo, l'integrazione somiglierà molto più all'aggiunta di un servizio specializzato per migliorare il risultato complessivo, due strumenti uno complementare all'altro.

Mito 2. Un computer quantistico è semplicemente più veloce?

Il secondo dei miti sul quantum computing è quello che genera più delusioni, perché porta le persone ad aspettarsi un miglioramento generalizzato che non arriverà mai. Un processore quantistico gioca su tutt'altre misure, infatti ha frequenze di lavoro modeste e tempi di lettura lunghi, quindi su un compito ordinario come la gestione di un sistema operativo perde il confronto con un hardware di fascia medio-bassa senza nemmeno lottare.



MITO 02

"È semplicemente un computer più veloce"

le strade sbagliate si cancellano fra loro

IN REALTÀ

L'equivoco più frequente è immaginare sia solo più veloce di un computer classico. Un algoritmo quantistico è costruito perché i percorsi che portano alla risposta sbagliata si eliminino a vicenda, lasciando per esclusione il percorso più probabile.

Non prova tutto in parallelo. Elimina.

 **HumanQ**

Mito 2. Un computer quantistico è semplicemente più veloce?

Il guadagno non viene dalla velocità del singolo passo, viene dal numero di passi necessari. Quando esiste un [algoritmo quantistico](#) capace di sfruttare [sovrapposizione](#) e [entanglement](#) per far interferire fra

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



loro le strade di calcolo sbagliate, il conto delle operazioni crolla di ordini di grandezza. Fuori da quei casi il conto resta identico, o peggiora, è una distinzione che sembra sottile in una slide ma che diventa decisiva quando si sceglie il caso d'uso di un progetto pilota.

Approfondimento. Perché non tutti i problemi accelerano

La misura su un registro quantistico restituisce un solo esito, con probabilità pari al modulo quadro dell'ampiezza associata. Avere 2^n ampiezze in gioco su n [qubit](#) non equivale quindi ad avere 2^n risultati leggibili. Un algoritmo utile deve costruire un'interferenza che concentri l'ampiezza sulle soluzioni corrette prima della misura, cosa che riesce solo se il problema possiede una struttura sfruttabile, come la periodicità nel caso dell'[algoritmo di Shor](#). Per la ricerca non strutturata l'algoritmo di Grover si ferma a un guadagno quadratico, da N a circa $\sqrt{N}$ valutazioni, che su hardware reale viene in buona parte eroso dal costo della [correzione degli errori](#). Da qui la formulazione reale del vantaggio, discussa nella pagina su [supremazia e vantaggio quantistico](#).

Mito 3. La crittografia sarà rotta domani mattina?

Qui il mito viaggia in due direzioni opposte e sbagliate entrambe. Purtroppo infatti da un lato c'è l'allarme che immagina il collasso dei sistemi bancari, bitcoin, blockchain entro pochi mesi, dall'altro la scrollata di spalle di chi considera la faccenda un problema per il 2050. La realtà è meno spettacolare della prima versione e più urgente della seconda.

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018

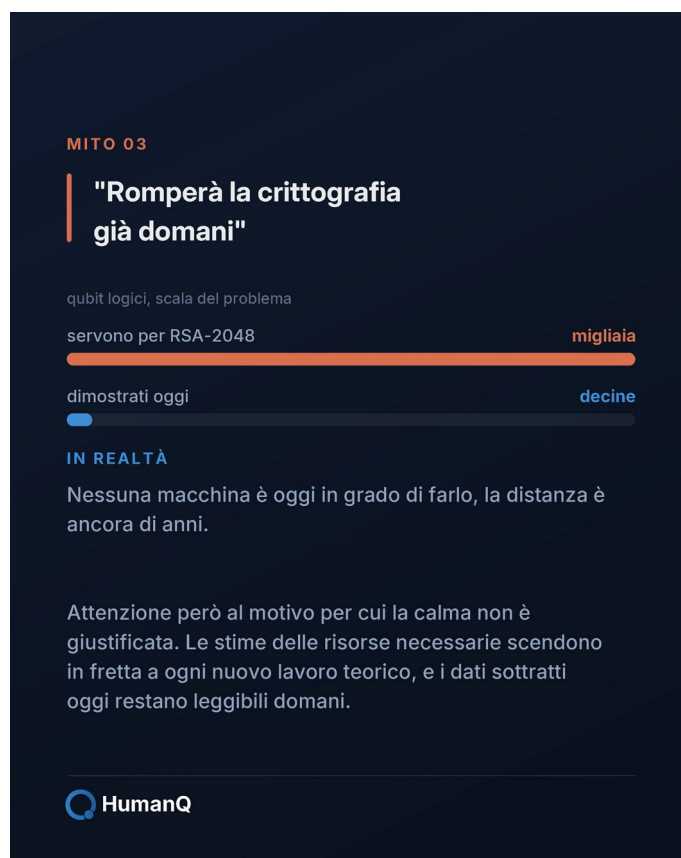


Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione
Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



Mito 3. La crittografia sarà rotta domani mattina?

Nessuna macchina esistente si avvicina alle risorse necessarie per fattorizzare una chiave RSA da 2048 bit, perché servirebbero milioni di [qubit](#) fisici per sostenere qualche migliaio di qubit logici stabili. Il problema quindi è un altro, e non dipende dalla data in cui quella macchina arriverà. Il vero pericolo è che il traffico cifrato intercettato oggi può essere conservato per parecchi anni e decifrato quando la capacità di calcolo per la rottura della cifratura sarà disponibile, una pratica nota come raccolta anticipata. Chi tratta cartelle cliniche, contratti pluriennali o segreti industriali ha quindi un'esposizione che decorre già da adesso e non fra vent'anni.

Il NIST ha pubblicato nel 2024 i primi standard di [crittografia post-quantistica](#), fra cui ML-KEM per lo scambio di chiavi e ML-DSA per le firme, e le indicazioni sono consultabili sul [progetto post-quantum del NIST](#). Sostituire gli algoritmi in un parco applicativo stratificato, dove convivono sistemi che nessuno tocca da dieci anni, richiede molti anni di lavoro organizzato. Ecco perché la domanda utile non è quando arriverà il calcolo o la fantomatica macchina, ma quanto tempo serve alle organizzazioni per cambiare cifratura senza fermare tutto.

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



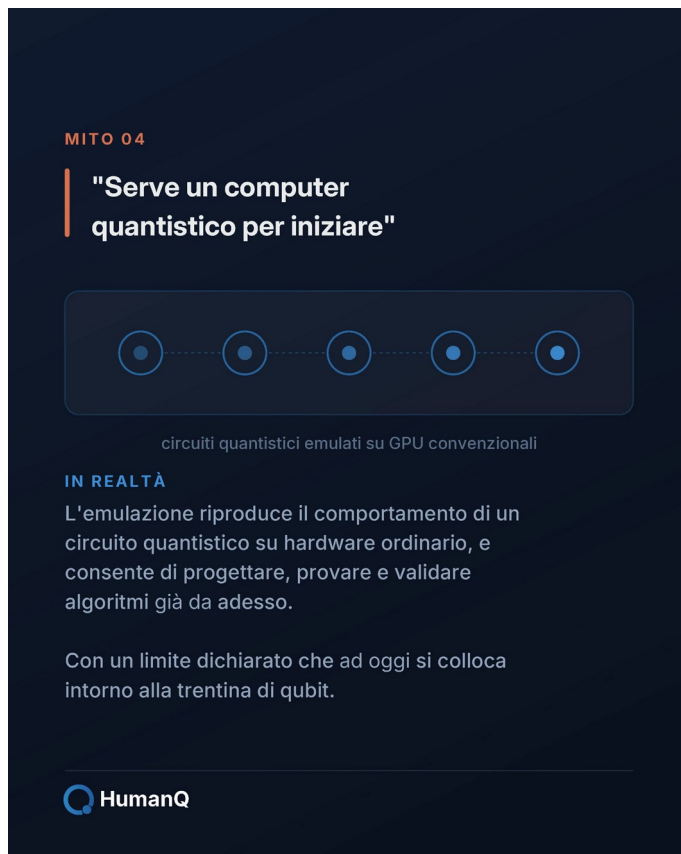
Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



Mito 4. Serve hardware quantistico per iniziare?

Questo è il mito che blocca più progetti, e anche quello che si smonta più volentieri. L'idea che per fare **quantum computing** occorra un criostato in azienda o un contratto cloud costoso con un fornitore extraeuropeo non regge, perché la parte difficile di un progetto non è l'esecuzione sul processore fisico, bensì quello di saper formulare il problema in termini quantistici, preparare i dati e capire se il vantaggio esista veramente.



MITO 04

"Serve un computer quantistico per iniziare"

circuiti quantistici emulati su GPU convenzionali

IN REALTÀ

L'emulazione riproduce il comportamento di un circuito quantistico su hardware ordinario, e consente di progettare, provare e validare algoritmi già da adesso.

Con un limite dichiarato che ad oggi si colloca intorno alla trentina di qubit.

 **HumanQ**

Mito 4. Serve hardware quantistico per iniziare?

Tutto questo si fa su hardware classico. La [simulazione](#) e soprattutto l'[emulazione quantistica](#) riproducono il comportamento di un registro di qubit con precisione controllata, permettendo di scrivere circuiti, eseguirli, misurarne i risultati e confrontarli con l'approccio classico già in uso. **HumanQ** sviluppa progetti di emulazione quantistica proprio per questo motivo, perché consente di lavorare oggi sulla parte che produce valore senza aspettare la maturità dell'hardware di un domani ancora incerto e utilizza in questo ambito l'emulazione quantistica.

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



C'è un vantaggio ulteriore che spesso sorprende i tecnici. Nelle macchine fisiche il disturbo, cioè la decoerenza e il rumore che degradano lo stato dei qubit, è un fenomeno spontaneo e difficile da isolare. In emulazione non c'è hardware fisico, quindi il rumore non compare da solo e viene ricreato deliberatamente, con i parametri che decidi tu. In tal modo puoi così misurare quanta tolleranza al disturbo serve al tuo algoritmo per restare efficace, questa è un'informazione impossibile da ottenere su una macchina fisica.

Mito 5. È troppo presto perché un'azienda se ne occupi?

La risposta dipende da cosa si intende per occuparsene. Se significa comprare hardware, allora sì, per quasi tutte le imprese è presto e probabilmente lo sarà ancora per parecchi anni, se invece significa costruire le condizioni per usare il calcolo quantistico quando servirà, allora i tempi sono già stretti, perché le attività di formazione e ingegnerizzazione allo sviluppo di un linguaggio quantistico hanno cicli di impiego molto lunghi e non si comprano a comando.



Mito 5. È troppo presto perché un'azienda se ne occupi?

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



Mettere ordine nei dati di processo, formare qualcuno in azienda che sappia leggere un circuito, censire dove si trovano le chiavi crittografiche nei sistemi in produzione, individuare i due o tre problemi di ottimizzazione che oggi risolvi in modo approssimato sono tutte cose che richiedono mesi e che rimarranno utilissime anche se il calcolo quantistico dovesse slittare di anni, perché migliorano comunque il modo in cui lavorare oggi per il futuro. Il percorso completo con le sue tappe è descritto nella pagina sulla [quantum readiness per le aziende](#).

Perché nascono i miti sul quantum computing e chi li alimenta?

Una parte della responsabilità è della comunicazione scientifica divulgativa, che per rendere accessibile la sovrapposizione ricorre a immagini come il gatto o il calcolo parallelo infinito, metafore che funzionano finché restano metafore e diventano fuorvianti quando qualcuno le prende alla lettera per stimare un ritorno sull'investimento.

Un'altra parte arriva dal mercato. Le aziende che sviluppano hardware competono per capitali e attenzione, quindi presentano oggi, anche se molto in anticipo, i risultati nella luce migliore possibile, e i numeri sui qubit vengono comunicati senza il contesto che li renderebbe leggibili. Un annuncio da qualche centinaio di qubit fisici dice poco se non si comprende quale sia la fedeltà delle porte logiche e quanti qubit logici ne derivino dopo la correzione degli errori. Programmi pubblici come il [Quantum Flagship europeo](#) pubblicano roadmap più sobrie, e sono una lettura più affidabile dei comunicati commerciali. Per il quadro generale della tecnologia resta valida anche la voce di [Wikipedia sul computer quantistico](#).

C'è poi una terza componente, quella normativa, che alimenta il rumore in modo indiretto; da quando le tecnologie quantistiche sono entrate nel perimetro delle tecnologie critiche, con le implicazioni di controllo statale che abbiamo raccolto nella pagina su [tecnologie quantistiche critiche e Golden Power](#), il tema ha assunto un peso geopolitico che tende a gonfiare le aspettative sul breve periodo.

Come si riconosce una promessa quantistica poco credibile?

Nel valutare una proposta serve guardare prima di tutto se il confronto con il metodo classico esista. Se un fornitore mostra il risultato di un algoritmo quantistico senza dati tangibili su quanto tempo impiegherebbe un buon solver classico sullo stesso problema, manca il termine di paragone che rende il numero interpretabile. Molti presunti vantaggi si sono dissolti proprio così, quando qualcuno ha riscritto la versione classica con maggior cura e rigore scientifico nella raccolta di dati e tempi.

Il secondo segnale riguarda la dimensione dell'istanza. Un caso d'uso raccontato su venti variabili non dice quasi nulla sul comportamento invece di mille variabili, e il salto in mezzo è esattamente la parte non risolta. Il terzo segnale è l'assenza di condizioni. Un algoritmo quantistico ha ipotesi di applicabilità precise, che riguardano la struttura del problema e il modo in cui i dati entrano nel circuito, e chi le omette

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



sta vendendo una promessa generica. Vale anche per il [quantum machine learning](#), dove il collo di bottiglia della codifica dei dati è spesso più costoso del calcolo stesso.

Che cosa può fare oggi un'azienda senza comprare hardware?

Le attività che consigliamo sono quattro e nessuna richiede una macchina quantistica. La prima è l'inventario crittografico, cioè sapere quali algoritmi proteggono quali dati e per quanti anni quei dati devono restare riservati, perché senza questa mappatura la migrazione post-quantistica non si riuscirà certamente a pianificare.

La seconda è la formazione mirata di un piccolo team interno, tre o quattro persone che sappiano leggere un circuito e discutere alla pari con un fornitore. La terza è la selezione dei candidati applicativi, che nella nostra esperienza escono quasi sempre dalle stesse famiglie di problemi, ottimizzazione con molti vincoli, simulazione di materiali e chimica, modelli di rischio. Ne abbiamo raccolto una rassegna nella pagina sulle [applicazioni del quantum computing](#), con gli approfondimenti verticali su [finanza](#) e [sanità](#).

La quarta è il progetto pilota (POC) in emulazione, dove si prende un problema reale e piccolo, lo si formula in modo quantistico e lo si esegue confrontandolo in modo scientifico con il metodo tradizionale. Il risultato potrà dire se vi sia o meno vantaggio oggi o se vi sarà un vantaggio futuro, sarà comunque un risultato che vale la pena conoscere, perché arrivarci con qualche settimana di lavoro è sicuramente meglio che scoprirlo dopo un monumentale investimento in hardware. Se vuoi capire come funziona la macchina che stai emulando, il funzionamento passo per passo è descritto nella pagina su [come funziona un computer quantistico](#).

Quali domande porsi prima di avviare un progetto quantistico?

Le domande che servono nella prima riunione sono poche e volutamente scomode. Quale problema state resolvendo oggi in modo approssimato perché la soluzione esatta costerebbe troppo tempo di calcolo. Quanto vale, in denaro o in ore, una risposta migliore del dieci per cento su quel problema. Per quanti anni i vostri dati devono restare riservati. Chi in azienda avrebbe il tempo di seguire un progetto pilota per tre mesi.

Chi risponde a queste quattro domande ha già fatto la parte più faticosa, perché ha trasformato un tema tecnologico in un problema aziendale con evidenze numeriche a corollario. Da lì in poi si tratta di lavoro ordinario di progettazione, con obiettivi misurabili e una scadenza. I miti sul quantum computing si dissolvono da soli quando si smette di chiedersi cosa sarà possibile un giorno e si comincia a chiedersi cosa è misurabile entro il prossimo trimestre.

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione
Lombardia

Ente accreditato
ID n. 1458 del 17/10/24



Vuoi verificare quali di questi miti pesano sulle tue decisioni?

HumanQ accompagna imprese e istituzioni nel passaggio dalla curiosità al progetto verificabile. I servizi su cui lavoriamo sono questi.

- Emulazione quantistica di algoritmi su casi d'uso aziendali reali
- Assessment di quantum readiness e costruzione della roadmap
- Formazione e divulgazione per team tecnici e direzioni
- Progetti pilota industriali con confronto misurato rispetto al metodo classico
- Sviluppo di algoritmi quantistici su problemi specifici

[Richiedi una prima valutazione](#) • [Parti dalla quantum readiness](#)

Approfondimenti correlati

[qubit](#) • [sovrapposizione quantistica](#) • [entanglement quantistico](#) • [computer quantistico](#) • [quantistico vs classico](#) • [come funziona un computer quantistico](#) • [algoritmi quantistici](#) • [algoritmo di Shor](#) • [simulazione quantistica](#) • [emulazione quantistica](#) • [correzione degli errori](#) • [supremazia e vantaggio quantistico](#) • [quantum machine learning](#) • [applicazioni quantistiche](#) • [crittografia post-quantistica](#) • [quantum computing in sanità](#) • [quantum computing in finanza](#) • [Golden Power](#) • [quantum readiness](#).

Stefano Patelli

Direttore tecnico di Polo Innovativo, incubatore e acceleratore di tecnologie certificato MIMIT. Polo Innovativo è uno degli investitori di HumanQ. [Altri articoli di Stefano Patelli](#)

Articolo pubblicato su humanq.it

HumanQ s.r.l.

P.IVA e C.F.: 04790260980
Via delle Scuole 1/G, 25128 Brescia (BS)
030 64 90 099 – info@humanq.it
humanq@pec.it

5-miti-da-sfatare-sul-quantum-computing.docx

Incubatore Certificato

Polo Innovativo s.r.l.
P.IVA e C.F.: 04389320989



Certificazioni:
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018



Polo Innovativo
ESPERTI DI ACCELERAZIONE, PARTNER PER IL CAMBIAMENTO



Regione Lombardia

Ente accreditato
ID n. 1458 del 17/10/24