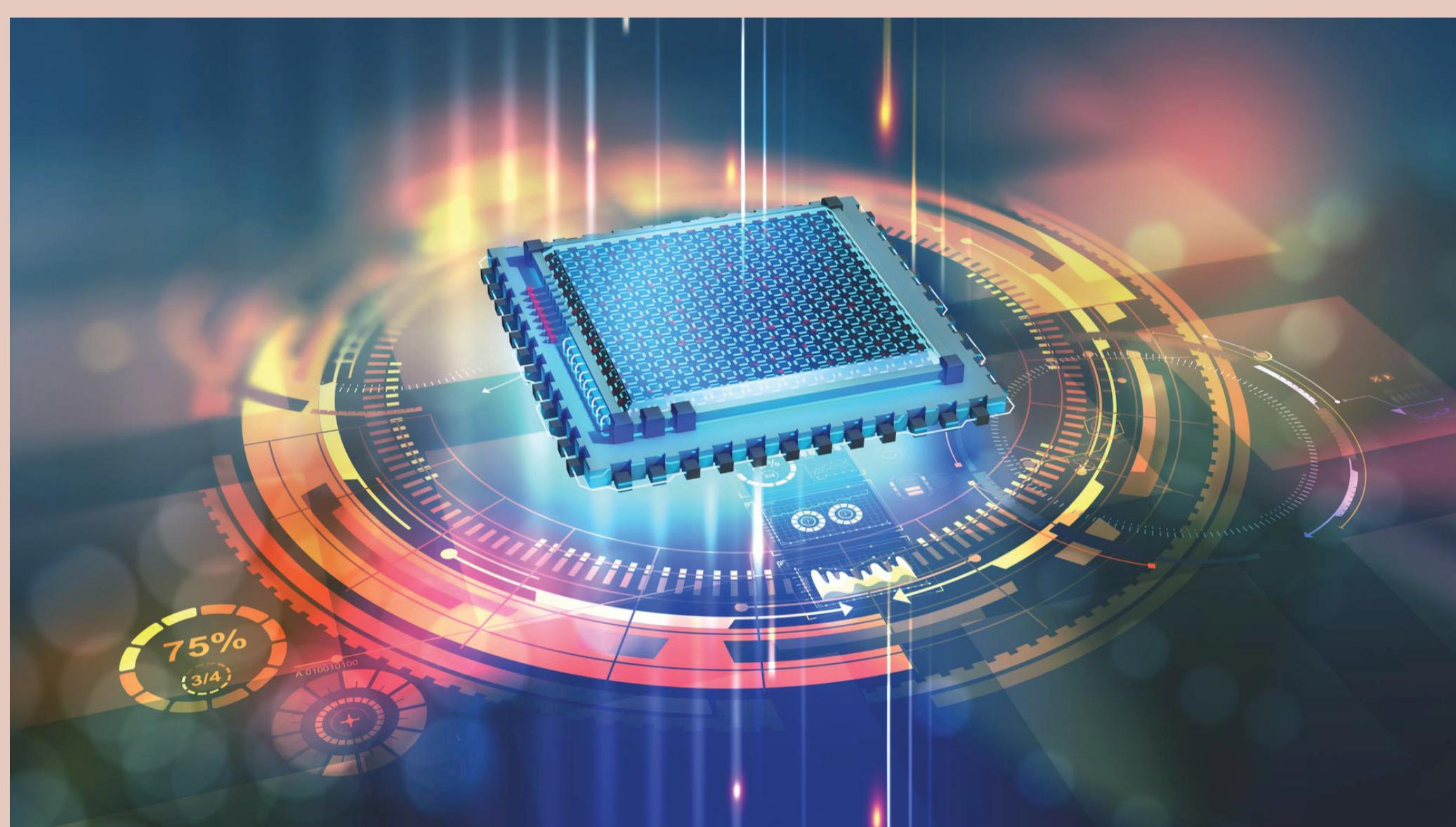


Quantum Computing



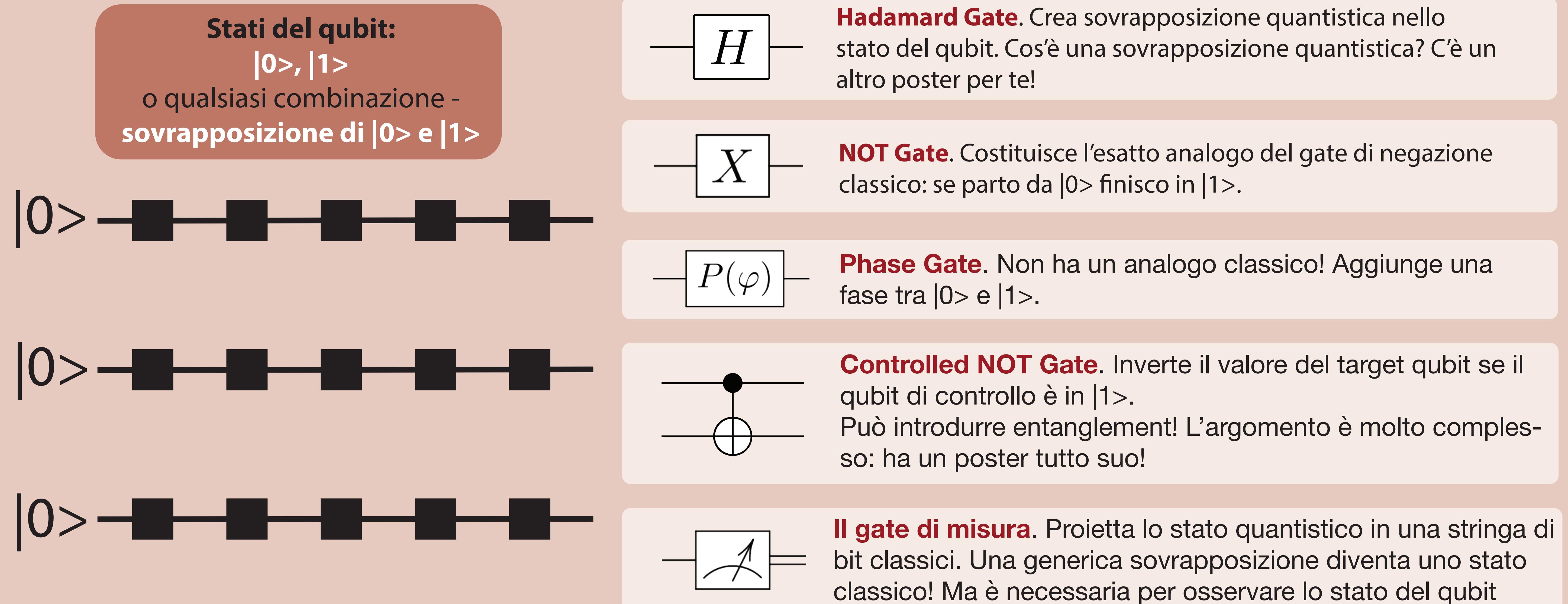
I computer quantistici saranno potenti strumenti che utilizzano le regole della meccanica quantistica per velocizzare i processi computazionali. L'unità fondamentale dei computer quantistici è il **qubit**, e sovrapposizione quantistica e entanglement vengono sfruttati per ottenere un vantaggio rispetto ai computer classici.

Le vere potenzialità dei computer quantistici nascono quando utilizziamo più di un singolo qubit. Per descrivere classicamente lo stato di un computer quantistico di **300 qubits** avremmo bisogno di più di **10⁹⁰** bits classici: più degli atomi nell'universo che sono stimati essere **10⁸²!**

Parlare con i QC

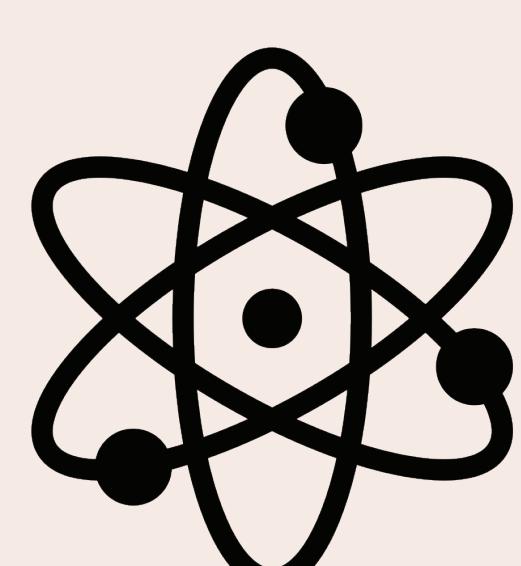
Il linguaggio che parliamo con i QC è quello dei circuiti quantistici. L'approccio è lo stesso delle porte logiche utilizzate nei circuiti classici. Le linee rappresentano i qubit, con il tempo che scorre da sinistra verso destra. Per evolvere lo stato dei qubits e quindi processare l'informazione quantistica, applichiamo le porte logiche quantistiche (quantum gates).

Usando una combinazione di queste porte logiche è possibile calcolare una **qualsiasi quantità**:



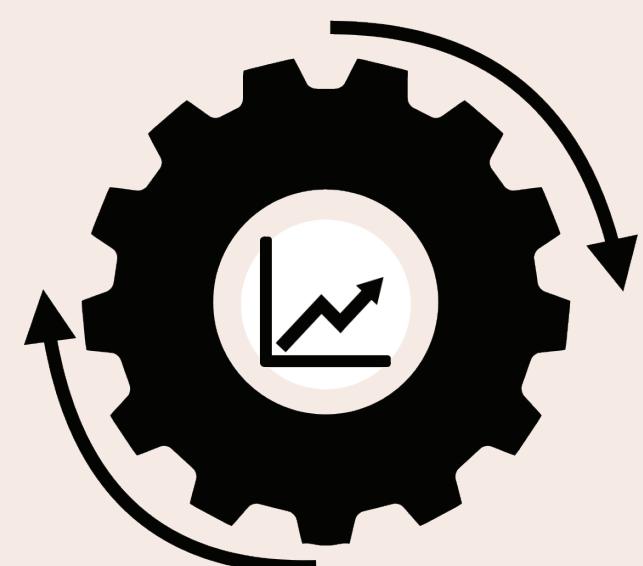
Applicazioni

Fisica quantistica



Lo studio dei sistemi a molti corpi quantistici è esattamente quello che ha ispirato Feynman nel teorizzare un computer quantistico. Studiare come differenti materiali interagiscono a livello atomico è molto complicato classicamente!

Ottimizzazione



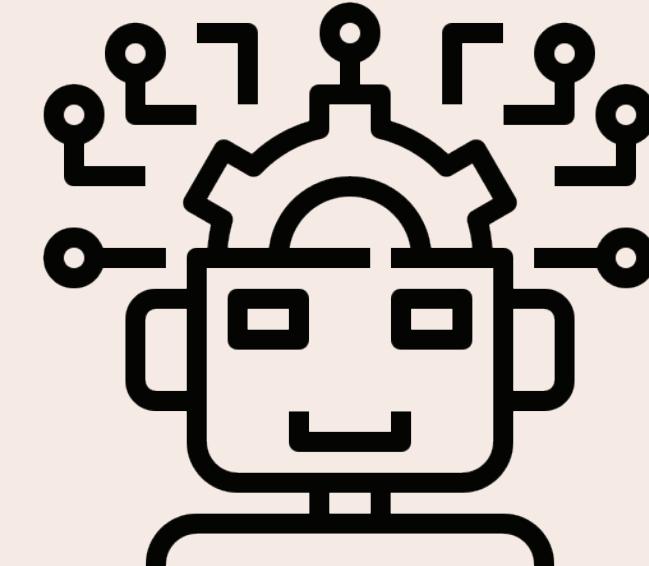
Il numero di possibilità in uno stato quantistico è esponenziale, e può quindi dare un gran vantaggio per ottimizzare un problema. Esempi di utilizzo sono: ottimizzazione del traffico, pianificazione di missioni spaziali...

Crittografia



L'algoritmo di Shor permette di rendere obsoleto l'attuale metodo crittografico RSA. Ma niente paura: ci sono molti algoritmi crittografici quantistici pronti a proteggerci da Shor! Un esempio è il BB84.

Intelligenza artificiale



L'intelligenza artificiale sta facendo passi da gigante. Una domanda aperta è: sarà possibile migliorare le prestazioni dell'intelligenza artificiale con un computer quantistico, nonostante le difficoltà che al momento presentano?