2008, l'anno del computer quantistico

D-Wave Systems annuncia che il suo primo elaboratore quantistico sarà immesso sul mercato nel corso di quell'anno. Un enorme passo avanti? Tutti i particolari

Roma - La start-up canadese D-Wave Systems, che ha ricevuto cospicui finanziamenti per lo sviluppo di un elaboratore quantistico, ha annunciato che il primo modello commerciale sarà pronto per il 2008.

Un elaboratore quantistico è un elaboratore in cui il valore 0 o 1 di un bit è codificato in una proprietà di una particella elementare detta in questo caso qubit. Effettuando delle trasformazioni sulle particelle elementari, ad esempio sottoponendole ad opportuni campi elettro-magnetici, se ne modificano le proprietà e quindi il valore del qubit, realizzando così delle operazioni di calcolo.

Il punto principale è che le particelle elementari non soddisfano le leggi della fisica macroscopica a cui siamo abituati nella vita di tutti i giorni, ma soddisfano le leggi della Meccanica Quantistica, teoria sviluppata dai fisici a partire dagli anni '30 per descrivere il mondo sub-atomico. Le leggi della Meccanica Quantistica sono notevolmente diverse da quelle delle fisica macroscopica, e spesso contro-intuitive.

Ad esempio non è possibile fare una copia esatta di una particella sconosciuta, ovvero le fotocopiatrici quantistiche non esistono; ed anche non è possibile misurare una proprietà di una particella senza perturbarla.

Se da un lato le particelle elementari sono molto difficili da maneggiare, sia per le loro dimensioni che per le leggi della Meccanica Quantistica, dall'altro grazie proprio alla Meccanica Quantistica è possibile utilizzarle per fare delle cose altrimenti impossibili.

Ad esempio, per gli elaboratori quantistici esiste l'algoritmo di Shor per fattorizzare velocemente il prodotto di due numeri primi grandi. Questo problema matematico è alla base della sicurezza dell'algoritmo RSA e di altri algoritmi crittografici Asimmetrici, ed è quindi fondamentale per la sicurezza dei certificati digitali e della maggior parte dei protocolli di sicurezza informatica odierni. L'avvento di un elaboratore quantistico in grado di implementare l'algoritmo di Shor comporterebbe la fine della sicurezza garantita oggi da questi algoritmi. L'altro principale algoritmo quantistico è l'algoritmo di Grover, che permette di effettuare velocemente ricerche in spazi non strutturati.

Ad oggi il più grande prototipo di elaboratore quantistico è stato costruito nei laboratori Almaden Research Center di IBM nel 2001. Era un elaboratore quantistico a 7 qubit ed è stato in grado di fattorizzare il numero 15 in 3 per 5. Questo elaboratore quantistico era formato da una molecola con 7 spin nucleari che rappresentavano i 7 qubit. Le operazioni venivano effettuate utilizzando impulsi in radio frequenza, mentre i risultati sui 7 spin nucleari venivano letti con tecniche di risonanza magnetica nucleare (NMR) simili a quelle adottate negli ospedali e laboratori chimici.

Uno dei principali problemi degli elaboratori quantistici è quello della "de-coerenza". Ovvero le particelle elementari utilizzate come qubit possono interagire con le particelle del mondo circostante e trasformarsi in modo praticamente casuale. Questo ovviamente porterebbe a risultati praticamente casuali per i calcoli.

Per superare questo problema è stato proposto di utilizzare dei sistemi a superconduttori, in pratica speciali circuiti a temperature vicine allo zero assoluto. Usando in maniera particolare delle "giunzioni Josephson", è possibile creare degli stati quantistici che possono essere usati come qubit. Applicando dei micro-voltaggi si possono effettuare delle operazioni i cui risultati si possono leggere nelle modifiche dei campi magnetici generati dalle giunzioni.

D-Wave Systems sta costruendo un prototipo di elaboratore quantistico a superconduttori, alla temperatura di -269 gradi, che dovrebbe essere pronto per la fine del 2006. La versione commerciale dovrebbe invece essere pronta entro il 2008. Secondo D-Wave Systems questo elaboratore quantistico non sarà in grado di implementare l'algoritmo di Shor per fattorizzare il prodotto di numeri primi, ma sarà in grado di risolvere problemi solubili con l'algoritmo di Grover, quali alcune equazioni particolarmente complesse nella fisica delle particelle elementari o delle interazioni molecolari, ed il famoso problema del "Commesso Viaggiatore" che ha moltissime applicazioni pratiche, dalla organizzazione di merci e magazzini ai portafogli finanziari.

D-Wave Systems dichiara sin d'ora che il loro elaboratore quantistico sarà uno strumento "delicato" e che non pensano di venderlo ma di vendere solo il tempo macchina sullo stesso. I clienti effettueranno la maggior parte dell'elaborazione sulle proprie macchine, e richiederanno all'elaboratore quantistico solo di elaborare la parte più complessa del calcolo.

Sino ad oggi si riteneva che fossero necessari almeno una decina di anni prima di poter costruire il primo elaboratore quantistico commerciale. L'annuncio di D-Wave Systems sembrerebbe quindi essere in contraddizione con quanto sostenuto dalla maggior parte degli scienziati e ricercatori.

In realtà, è stato dimostrato nel 1999 che è possibile implementare l'algoritmo di Grover su delle versioni semplificate di elaboratori quantistici. D-Wave Systems vuole appunto sviluppare un elaboratore quantistico di questo tipo che richiede componenti molto più semplici rispetto a quelli utilizzati sinora. Per questo D-Wave Systems ritiene di poter riuscire a commercializzare il primo elaboratore quantistico nel 2008, il che comunque rimane una scommessa da verificare.

Andrea Pasquinucci