IL FATTO

Siamo entrati nell'era quantistica, lo ha detto Google

TECNOLOGIA / Alla scoperta della nuova generazione di computer: la corsa è lanciata
Il colosso americano ha annunciato il proprio vantaggio sulla ricca e variegata concorrenza

Il gigante americano sta dettando i tempi della corsa alla supremazia quantistica. © SHUTTERSTOCK

Giona Carcano

Paolo Galli

La scienza è come lo sport. Per vincere, o meglio, per arrivare primi - ma anche per vincere, suvvia -, bisogna correre, correre più veloci degli altri. Oltre il traguardo, oltre la gloria, è anche una questione economica. E politica. In questo senso, mandare un razzo su Marte o sfondare un varco verso una nuova tecnologia dipendono dallo stesso paradigma. E da esso allora dipende anche la corsa dell'informatica quantistica, giunta finalmente a una possibile svolta. Google ha infatti annunciato un mese fa di aver raggiunto la supremazia quantistica. Cosa significa? Lo abbiamo chiesto al professore dell'USI Stefan Wolf e ai suoi collaboratori Arne Hansen e Xavier Coiteux-Roy. Hansen spiega: «I risultati teorici mostrano che computer che sfruttano principi della fisica quantistica possono risolvere problemi specifici molto più velocemente dei computer classici. Questo sulla carta: nessun computer è stato completato. Google ora reclama di averlo fatto». Wolf aggiunge: «La superiorità di un computer quantistico non ha comunque ancora controprove: per la maggior parte dei problemi i computer classici hanno infatti margini di miglioramento. Quanto a Google, il calcolo che affermano di aver eseguito non è un calcolo "utile". Dire che un computer quantistico può fare cose molto complicate per uno classico non è di per sé significativo: processi difficili da replicare sui computer classici avvengono in ogni bicchiere d'acqua. Un computer quantistico che faccia solo una cosa non vale il più economico degli smartphone, dunque parlare di "supremazia" – espressione particolarmente brutta – è eccessivo». «Insomma non siamo davanti né alla "supremazia" di un particolare computer quantistico capace di svolgere compiti generali né alla "supremazia" generale dei computer quantistici sui classici», chiosa Hansen.

Utilità nella crittografia

Parlando di utilità, viene da chiedersi, relativamente all'informatica quantistica, quali saranno le sue applicazioni e quale sarà il ramo economico/scientifico con il maggiore potenziale di sviluppo. Wolf: «Probabilmente la crittografia. Ironia della sorte: la fisica quantistica non si limita a rompere i tradizionali sistemi crittografici, li rende anche disponibili a nuovi livelli. Una scoperta di Gilles Brassard, dottore honoris causa dell'USI». Coiteux-Roy conferma: «L'unica applicazione abbastanza matura è la crittografia quantistica: oggi può essere usata per rendere comunicazioni o transazioni più private e sicure». Wolf conclude con una postilla centrale: « Proprio perché come ricercatori ci occupiamo di informatica quantistica, siamo i primi a interrogarci su quali tecnologie e applicazioni vogliamo davvero come società, oggi e in futuro». Impossibile per ora pensare a una diffusione del computer quantistico su larga scala, che possa raggiungere tutti noi, le nostre case. Wolf: «Il Governo cinese sta investendo ingenti somme di denaro per una dorsale di rete di telecomunicazione a tecnologia quantistica, la cui sicurezza è tuttavia da testare. È in gioco soprattutto una lotta simbolica per la leadership tecnologica. Ma i benefici concreti per l'individuo e la sua libertà?».

Una lotta poco rassicurante

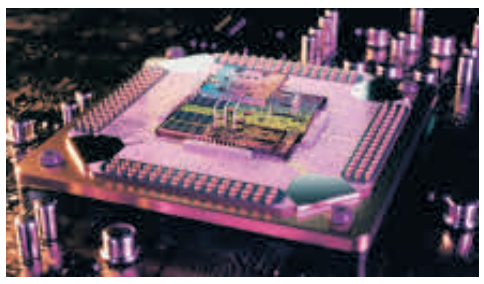
La Cina c'è. Ma non è sola. Chiamatela per l'appunto corsa, o lotta. Wolf: «È possibile che in futuro il calcolo quantistico contribuisca a ridefinire la "geopolitica tecnologica", ma non siamo ancora giunti ad applicazioni pratiche a largo raggio. In tutte le epoche abbiamo assistito a vere e proprie battaglie tecnologiche. La crittografia, ad esempio, è stata per anni "matematica di battaglia". Pensiamo ad Alan Turing e alla decrittazione della macchina di cifratura tedesca Enigma durante la Seconda guerra mondiale. Oggi, comunque, l'Europa è a un ottimo livello nella ricerca in campo tecnologico. Tuttavia diversi ricercatori stanno osservando che, con le grosse società private che giocano un ruolo sempre maggiore, molte cose sono sfuggite di mano. La situazione è un po' "unheimlich", poco rassicurante, come ha sintetizzato un professore che abbiamo incontrato di recente». Dunque no, il Vecchio Continente non è in ritardo, o lo è con consapevolezza. «Alcune società decidono di non percorrere alcune strade», commenta Wolf. «Prendiamo ad esempio l'atomica: certi Paesi hanno scelto di non averla. La Cina è più avanti di noi rispetto all'intelligenza artificiale o alla crittografia quantistica. Sì, è vero. Ma queste tecnologie vengono usate da Pechino per creare uno stato di sorveglianza. L'Europa, invece, ha sorprendentemente creato leggi per la protezione dei dati dei cittadini. Sono due differenti modi di interpretare e sfruttare la tecnologia».

Da sapere

Ecco di cosa si sta parlando

La supremazia

Ma cosa sono i computer quantistici? Citiamo una spiegazione pubblicata dal magazine *Wired*: «Un computer quantistico sfrutta alcune tra le proprietà più bizzarre e controintuitive della meccanica quantistica per ottenere una potenza di calcolo di gran lunga superiore rispetto a quella di un computer classico». L'unità minima di informazione di un processore convenzionale è il bit, ovvero un'entità binaria che può assumere i valori zero e uno a seconda del passaggio o meno di corrente. I processori quantistici invece usano i qubit, in genere particelle subatomiche come fotoni o elettroni, che invece possono immagazzinare molte più informazioni, permettendo di parallelizzare i calcoli e di svolgere molte operazioni contemporaneamente. E la supremazia quantistica? Semplicemente: riuscire a risolvere con un computer quantistico un calcolo che un computer tradizionale non sarebbe in grado di risolvere. Va ricordato come il quanto sia la quantità elementare indivisibile di una certa grandezza, una particella elementare insomma.



Un processore quantico. © SHUTTERSTOCK

I dubbi di IBM

Immediatamente dopo l'annuncio di Google, IBM – altro colosso informatico – si è affrettato a mettere in dubbio la supremazia quantistica della «Grande G». «Stiamo parlando di due aziende direttamente concorrenti», spiega Stefan Wolf. «In campo tecnologico, riuscire a conquistare la leadership è fondamentale: chi è in una posizione di superiorità ottiene più attenzione, finanziamenti e talenti. E le differenze crescono. I ricchi diventano più ricchi e i poveri diventano più poveri: ciò che è vero per gli individui vale anche per le aziende». Xavier Coiteux-Roy aggiunge: « Il piccolo prototipo di computer quantistico di Google ha completato in 200 secondi un compito computazionale che sarebbe stato impossibile simulare in così poco tempo utilizzando le attuali tecnologie non quantistiche. Una prova confortante e condivisa da IBM». Confortante, sì, ma non definitiva. Google ha risolto un calcolo: per l'effettiva supremazia bisognerebbe traslare questo risultato a tutte le operazioni.

Chi lavora a queste tecnologie

Per sviluppare questi processori di ultimissima generazione occorrono capitali importanti. Chi si può permettere di lavorarci? Stefan Wolf spiega: «Direi una dozzina di aziende. E vanno considerati anche i servizi segreti, come l'NSA, in merito alla crittografia e ai protocolli di sicurezza. Gli investimenti necessari sono ingenti, è vero. Ma comunque è in corso, tra questi attori, una lotta, simbolica, a chi fa per primo il prossimo passo nell'era digitale. Una lotta che potrebbe riguardare più l'immagine che non reali applicazioni volte a migliorare la vita delle persone».

Che tipo di formazione viene richiesta

Il campo dei computer quantistici è uno dei rami dell'informatica del futuro. Già oggi sempre più scuole offrono la possibilità di seguire questa via specialistica. «All'USI facciamo ricerche nel campo dell'informatica quantistica e della crittografia quantistica, concentrandoci in una prospettiva di matematica e filosofia piuttosto che sulle applicazioni vere e proprie», spiegano Arne Hansen e Stefan Wolf. «Presentiamo questi argomenti nei nostri Master in informatica e offriamo studi di dottorato specializzati. Anche in altre università svizzere ed europee si può fare un percorso simile». I due studiosi affrontano poi una questione etica: «Un dibattito sulle tecnologie – quantistiche o meno – è troppo pressante per lasciarlo a una piccola cerchia di ricercatori. Una democrazia non può permettersi spazi lasciati interamente agli esperti. Una società libera e aperta deve decidere consapevolmente e pubblicamente su tecnologie che incidono sulla vita di tutti, senza lasciare la scelta solo a esperti e grandi aziende».

La «Grande G»

Non è più solo un motore di ricerca «Un rischio»

Il dominio

Google è un colosso impegnato ormai in vari campi. Non è più soltanto un motore di ricerca. Un pericolo per l'indipendenza della ricerca? Stefan Wolf: «Sì, un rischio per la nostra società. È davvero spaventoso». Arne Hansen aggiunge: «Non è un fenomeno nuovo, se si pensa a Xerox, IBM, AT&T...». Wolf ribatte: «Vero, ma oggi può essere ancora più totalitario».

L'immagine

La sensazione è che con il suo annuncio, Google abbia messo a segno un punto importante in termini di immagine. «Una teoria coerente con gli ulteriori tentativi di Google di essere in pole position per "l'era dell'informazione"», spiega Wolf. E Hansen specifica: «Ciò mostra che la ricerca aziendale precedentemente svolta da IBM o Xerox si sta ora spostando verso i nuovi monopoli tecnologici. Una tendenza che abbiamo visto con le tecnologie spaziali diventa evidente oggi in altri campi. Il campo delle tecnologie quantistiche è particolarmente interessante, poiché i progressi sarebbero immediatamente vantaggiosi per aziende come Google o Amazon».

Responsabile di redazione
Paolo Galli

E-mail
ilfatto@cdt.ch

Telefono
091 9603131