LA STAMPA

diffusione:91637
tiratura:147112

Simone Montangero

"La nuova rivoluzione dei computer quantistici trasformerà il futuro"

Quali sono le invenzioni che stanno per cambiare la nostra vita? Calcolatori avveniristici e IA ci porteranno a progressi inimmaginabili

L'invenzione che ci manca

LE IDEE

GABRIELE BECCARIA

L'invenzione che ci manca sta prendendo forma. Primo salto nel futuro: il computer quantistico. Secondo salto: un'Intelligenza Artificiale addestrata a funzionare con un computer quantistico. Terzo salto: l'IA quantistica che dà vita a un robot androide o ginoide. Le conseguenze di questi tre salti (quantistici, naturalmente)? «Ancora inimmaginabili», riflette Simone Montangero, professore di fisica teorica, responsabile del Centro di Calcolo e Simulazioni Quantistiche all'Università di Padova e autore, con Giuliano Benenti e Giulio Casati, di un saggio dal titolo volutamente provocatorio: *Il computer impossibile*, edito da Raffaello Cortina.

«Ciò che sembra impossibile diventa possibile grazie al metodo scientifico: scopriremo nuovi materiali e nuovi farmaci e, chissà, potremmo disporre di un cervello positronico, come quello immaginato da Isaac Asimov. Di sicuro, l'IA non consumerà più tutta l'energia che consuma adesso, ma dovremo imparare a gestire i super-robot quantistici, anche ricorrendo a discipline vecchie solo in apparenza: l'etica, la filosofia, la giurisprudenza…»

Professore, perché il computer quantistico è stato così a lungo considerato impossibile e solo ora prende forma?

«È una macchina costruita per calcolare, manipolando bit di informazione come un computer classico, ma i bit sono quantistici, i qubit. Potrebbero sembrare innocui, eppure cambiano tutto: seguono leggi diverse da quelle degli oggetti classici».

Di quali leggi si tratta?

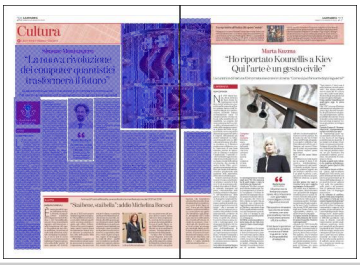
«"Nessuno capisce la meccanica quantistica", diceva il Nobel Richard Feynman, perché le cose che vi accadono sono controintuitive rispetto alla logica naturale. Due sono le proprietà fondamentali. La prima si chiama sovrapposizione quantistica: un bit classico può trovarsi solo nello stato 0 o nello stato 1, mentre un oggetto quantistico può stare in un'infinità di stati intermedi. La seconda, ancora più sorprendente, è l'entanglement, l'intreccio quantistico. Manipolando un qubit, determino istantaneamente lo stato dell'altro, indipendentemente dalla distanza: è come se fossero gemelli».

Quali saranno gli effetti, quando riusciremo a fare quei calcoli "impossibili"?

«Con queste proprietà eseguiremo calcoli in modo molto più efficiente. Efficiente non vuol dire solo più veloce. Mi spiego con un esempio: trovare l'ago nel pagliaio. Se ho 10 pagliuzze e un ago, troverò l'ago dopo aver fatto, in media, cinque tentativi. Il numero di tentativi scala linearmente con la taglia del pagliaio: pensiamo al caso in cui il pagliaio sia il database di Google e, quindi, Internet. Con un computer quantistico si risolve un problema tanto complesso grazie a specifici algoritmi, come quello di Grover, con una velocità impressionante: il tempo di ricerca non è più proporzionale al numero di elementi nel database, ma alla sua radice quadrata. E più grande è il database e più grande è il guadagno».

Sta parlando di una rivoluzione in arrivo…

«L'aveva spiegato Peter Shor negli Anni 90: con un computer quantistico, sfruttando gli


Cultura

"La nuova rivoluzione dei computer quantistici trasformerà il futuro"

"Ho riportato Kounellis a Kiev Qui l'arte è un gesto civile"

LA STAMPA

diffusione:91637
tiratura:147112

stati di cui parlavo prima e, quindi, eseguendo operazioni che non sono possibili per un computer classico, si risolveranno problemi in tempi polinomiali, anziché esponenziali, e per esempio diventerebbe possibile craccare la sicurezza mondiale. Così il mondo come lo conosciamo collasserebbe».

Come si affronterà questo caos globale?

«Un trentennio fa si trattava di una mera possibilità teorica, mentre oggi, con i prototipi dei computer quantistici, si fanno previsioni realistiche: se ci si pone nella fascia degli ottimisti, c'è una possibilità che tra 5-10-20 anni la crittografia attuale possa essere violata. Dobbiamo, quindi, fare qualcosa: fortunatamente quel qualcosa esiste e sono specifiche contromisure».

Quali contromisure?

«È la famiglia degli algoritmi noti come post-quantum cryptography o, direttamente, si ricorre alla crittografia quantistica, entrambi disegnati per resistere agli attacchi dei computer quantistici».

A che punto sono questi super-computer?

«Si trovano nella fase dei prototipi. Quelli classici sono costruiti con la tecnologia del silicio, quelli quantistici si basano su altre tecnologie: a superconduttori (studiati da Google), ad atomi e a ioni. Hanno potenze che vanno dalle decine a qualche centinaio di qubit e raggiungono una taglia con cui si iniziano a fare cose interessanti, in grado di sfidare i computer classici».

Su che modelli sta lavorando?

«Coordino il progetto europeo PASQuans2 che, per il 2030, punta a realizzare simulatori quantistici con 10 mila qubit. Sarà un boost per la ricerca, dalle scienze dei materiali alla biomedicina e a cascata per la ricerca in generale».

Nella gara per la supremazia quantistica come si colloca l'Europa rispetto a Usa e Cina?

«L'Europa è stata pioniera delle tecnologie quantistiche e la gara è aperta. Intanto le Big Tech americane hanno scommesso sui computer quantistici e quindi Ibm, Google, Amazon, Nvidia e altri hanno investito in programmi decennali, con finanziamenti equiparabili, per singola azienda, a quelli stanziati dall'intera Europa».

L'Ue, allora, rischia di perdere la sfida?

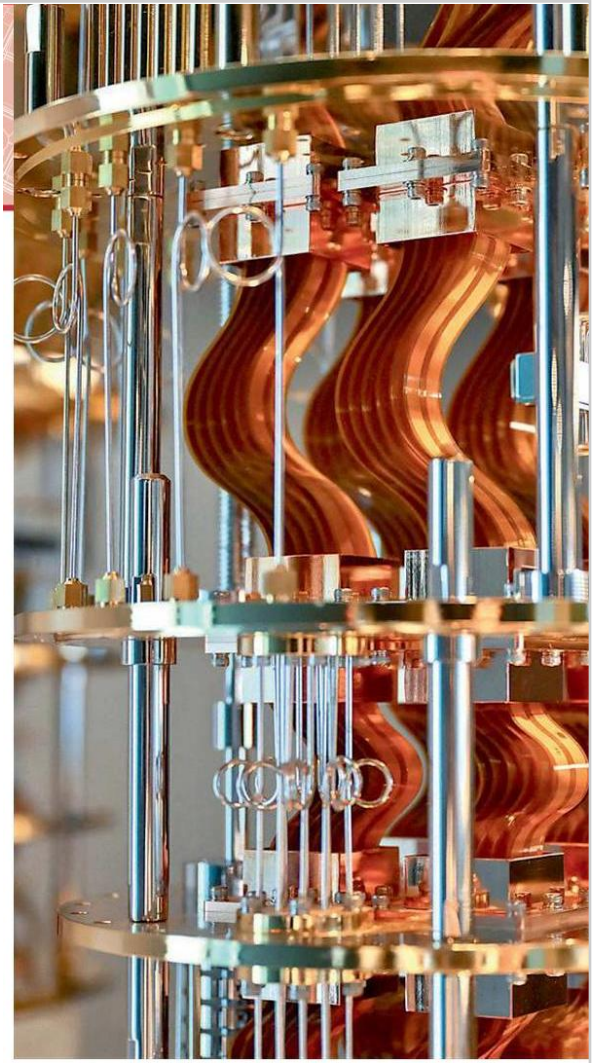
«Sta rispondendo con centri di ricerca e start-up: l'Ue con la Quantum Flagship del 2018 è stata la prima istituzione a ideare un programma continentale per finanziare le tecnologie quantistiche. E ci si aspetta che venga lanciato un nuovo programma decennale».

E l'Italia che ruolo ha?

«Fa parte di diversi consorzi europei e ha realtà finanziate dal Pnrr che stimolano la ricerca, come la Fondazione Icsc e il Partenariato Nqsti. Intanto, otto atenei e centri di ricerca hanno fondato l'Aqi, l'Allenza Quantistica Italiana: è una rete che punta a costruire un ecosistema competitivo, in grado di dialogare con gli attori del settore, nazionali e internazionali».

Saltiamo nel 2030: come avranno trasformato il mondo i computer quantistici?

«Credo che il mondo della persona comune non cambierà molto, nel senso che il grande pubblico non saprà quando si connetterà con un computer quantistico, proprio come succede ora quando si usa ChatGPT e non ci interessa conoscere il supercalcolatore che lo fa girare. Ma per gli scienziati la scala dei problemi che si potranno risolvere verrà ulteriormente aumentata: dai nuovi materiali ai nuovi farmaci e alle ottimizzazioni industriali, come quelle per la logistica e i trasporti. E ogni aspetto della ricerca sarà trasformato: come fisico, penso che potremo studiare le interazioni tra le particelle elementari a un livello senza precedenti e capire questioni tuttora aperte nella comprensione dell'Universo». —

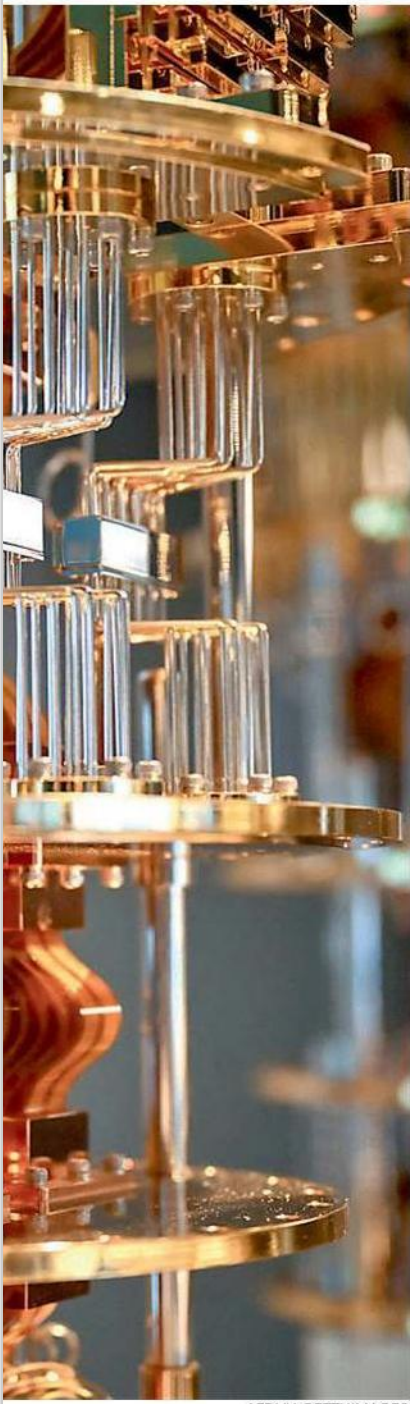


Simone Montangero
Professore di fisica teorica

Diventerà possibile craccare la sicurezza mondiale. Così il mondo come lo conosciamo collasserebbe

LA STAMPA

diffusione:91637
tiratura:147112



AFP VIA GETTY IMAGES