Quantum Internet: la rivoluzione quantistica; conoscerla per non subirla…

Data 08 agosto 2026
Categoria Medicinadigitale

Le tecnologie quantistiche, rimaste per molti decenni soprattutto oggetto di ricerca teorica, stanno i diventando strumenti concreti capaci di modificare profondamente il calcolo, la crittografia e le telecomunicazioni. Da qualche tempo la stampa pubblica articoli più o meno approfonditi ed affidabili su "Quantum Internet", spesso presentato come un'Internet più rapido o più potente, mentre costituisce un nuovo paradigma di comunicazione, fondato su princìpi fisici profondamente differenti da quelli che governano le reti tradizionali.

In questa pillola riassumiamo articoli di alcuni esperti che ci possono aiutare a capire, almeno in parte, cosa sta avvenendo, valorizzandone gli aspetti positivi e, se possibile, difendendoci da quelli negativi …

Dalla fisica classica alla meccanica quantistica
Nel mondo quotidiano, descritto dalla fisica classica, gli oggetti possiedono caratteristiche relativamente definite e intuitive: un interruttore è acceso oppure spento, una palla si trova in un luogo oppure in un altro. Nel mondo atomico e subatomico, invece, queste categorie non sono più sufficienti. *La meccanica quantistica descrive una realtà nella quale una particella può trovarsi contemporaneamente in più stati, sistemi separati possono conservare correlazioni profonde e la semplice osservazione modifica inevitabilmente ciò che viene osservato…*

Per comprendere meglio il mondo quantistico è utile richiamare quattro princìpi fondamentali.
Il primo è la sovrapposizione, secondo cui una particella quantistica può trovarsi in una combinazione di più stati contemporaneamente. **Il secondo è l'entanglement,** ossia una correlazione tra particelle differenti e talora molto distanti che non possiede un equivalente nel mondo classico. Due particelle "entanglate" si comportano come parti di un unico sistema, anche quando sono separate da grandi distanze. **Il terzo principio è il teorema del no-cloning,** che impedisce di copiare perfettamente uno stato quantistico sconosciuto. **Il quarto è il postulato della misura,** secondo cui misurare uno stato quantistico non è un'osservazione passiva, ma un'interazione che modifica irreversibilmente il sistema.
Queste caratteristiche rappresentano contemporaneamente la forza e la fragilità dell'informazione quantistica. Consentono di immaginare nuove forme di calcolo e di comunicazione, ma rendono impossibile applicare alle reti quantistiche le stesse tecniche utilizzate nell'Internet attuale.

Dal bit al qubit
L'Internet classica rappresenta e trasmette l'informazione attraverso sequenze di bit. Ogni bit può assumere uno di due valori: 0 oppure 1. Questi valori possono essere letti, copiati, conservati, amplificati e ritrasmessi senza che l'informazione originaria venga necessariamente distrutta.
La Quantum Internet utilizza invece i qubit, o bit quantistici. Un qubit non è limitato ai due valori nettamente separati 0 e 1, ma può trovarsi in una sovrapposizione dei due stati. Quando diversi qubit sono entanglati, le loro proprietà non possono più essere descritte separatamente: essi formano un unico sistema quantistico.
Questa differenza non significa soltanto che i qubit contengano una quantità maggiore di informazione. Significa soprattutto che l'informazione quantistica possiede una natura completamente diversa. Non può essere letta liberamente, perché la misura ne modifica lo stato; non può essere duplicata, perché il teorema del no-cloning ne impedisce la copia perfetta; non può essere amplificata con i normali ripetitori usati nelle telecomunicazioni classiche.
La Quantum Internet richiede quindi un ripensamento della intera architettura delle comunicazioni. Non è sufficiente sostituire i bit con i qubit all'interno delle reti esistenti. Occorre progettare nuovi dispositivi, nuovi protocolli e nuovi sistemi di gestione dell'informazione.
Le potenzialità sono comunque enormi. L'entanglement potrebbe permettere comunicazioni con livelli di sicurezza non raggiungibili mediante le sole tecniche classiche. Inoltre, una rete quantistica potrebbe collegare diversi computer quantistici, consentendo loro di collaborare come parti di un grande sistema di calcolo distribuito.

Il teletrasporto quantistico
Uno dei protocolli centrali del futuro Quantum Internet è il teletrasporto quantistico. Il termine può suscitare immagini fantascientifiche, ma non indica il trasferimento istantaneo di persone od oggetti. Il teletrasporto quantistico riguarda esclusivamente il trasferimento dello stato quantistico di un qubit da un punto della rete a un altro.
Gli autori descrivono il protocollo attraverso il consueto esempio di due utenti, Alice e Bob(2). I due condividono inizialmente una coppia di qubit entanglati. Alice possiede inoltre un terzo qubit, contenente lo stato quantistico che desidera trasferire a Bob. Alice effettua un'operazione quantistica sui propri qubit e successivamente li misura. Il risultato della misura viene trasformato in due bit classici, che vengono comunicati a Bob mediante una rete tradizionale. Utilizzando questi due bit, Bob applica al proprio qubit una determinata trasformazione. Alla fine del procedimento, il qubit di Bob assume lo stesso stato posseduto inizialmente dal qubit di Alice.
Lo stato originario non viene copiato. Nel corso della procedura, esso viene distrutto nel punto di partenza e ricostruito

nel punto di arrivo. In questo modo viene rispettato il teorema del no-cloning.
Il teletrasporto quantistico mostra bene la differenza tra comunicazione classica e quantistica. Nelle telecomunicazioni tradizionali, un messaggio viene codificato in un segnale che attraversa fisicamente il canale. Nel teletrasporto quantistico, invece, lo stato viene trasferito grazie alla combinazione di entanglement, misura quantistica e comunicazione classica. Secondo gli autori, l'informazione quantistica da trasferire non transita direttamente lungo la rete e non può quindi essere intercettata attraverso un semplice ascolto passivo del canale.
Ciò non significa che il protocollo permetta comunicazioni istantanee o superiori alla velocità della luce. La componente classica del processo rimane indispensabile: Bob non può completare la ricostruzione dello stato finché non riceve da Alice i risultati della misura.

Complementarità con l'Internet classica
Un punto fondamentale è che la Quantum Internet non sostituirà l'Internet attuale. Le due reti saranno destinate a coesistere ed a collaborare. La rete quantistica permetterà di svolgere funzioni impossibili per l'Internet classica, mentre quest'ultima continuerà a garantire la trasmissione dei dati ordinari e le comunicazioni di controllo necessarie al funzionamento dei protocolli quantistici.
Si formerà pertanto un'architettura ibrida. La componente classica gestirà il traffico tradizionale, il coordinamento tra i nodi e il cosiddetto signaling. La componente quantistica sarà utilizzata per operazioni specifiche, come la distribuzione sicura delle chiavi crittografiche, il teletrasporto degli stati quantistici e il collegamento tra computer quantistici.
Nel breve periodo, una delle applicazioni più concrete sarà la Quantum Key Distribution, o QKD. Questi protocolli utilizzano i princìpi della meccanica quantistica per generare e distribuire chiavi segrete, successivamente impiegate per cifrare messaggi trasmessi attraverso l'Internet classica.
La sicurezza della crittografia tradizionale dipende generalmente dalla difficoltà di risolvere determinati problemi matematici. Un aggressore dotato di capacità di calcolo sufficienti potrebbe, almeno in linea di principio, superare alcune di queste protezioni. La QKD si fonda invece sulle leggi fisiche: poiché la misura modifica lo stato quantistico, un tentativo di intercettazione lascia inevitabilmente una traccia rilevabile.
Nel lungo periodo, per informazioni particolarmente sensibili, potrebbe essere utilizzato il teletrasporto quantistico. Anche in questo caso, tuttavia, la rete classica resterebbe necessaria per trasmettere le informazioni di controllo richieste dal protocollo.

Le principali difficoltà tecnologiche
La realizzazione di una Quantum Internet su larga scala incontra numerosi ostacoli. Il primo riguarda la fragilità dei qubit. Gli stati quantistici sono estremamente sensibili alle interazioni con l'ambiente, che possono provocare perdita di informazione e decoerenza.
Nelle reti classiche, un segnale indebolito può essere letto, copiato, amplificato e nuovamente trasmesso. Questo procedimento non è possibile per i qubit, perché la misura altererebbe lo stato e la copia perfetta è impossibile in base al teorema del no-cloning. Per estendere le comunicazioni quantistiche su grandi distanze sono quindi necessari dispositivi specifici, come i ripetitori quantistici e le memorie quantistiche.
I ripetitori quantistici dovrebbero permettere di distribuire l'entanglement lungo una successione di nodi, senza copiare direttamente gli stati. Le memorie quantistiche dovrebbero invece conservare temporaneamente i qubit, mantenendone le proprietà fino al completamento delle operazioni di rete. Entrambe le tecnologie sono ancora oggetto di intensa ricerca.
Un secondo problema è la trasduzione quantistica, cioè la capacità di convertire l'informazione tra differenti piattaforme fisiche. I computer quantistici, le memorie e i sistemi di trasmissione possono infatti utilizzare tecnologie diverse. Alcuni funzionano con fotoni, altri con atomi, ioni intrappolati, circuiti superconduttori o difetti nei cristalli. Una rete realmente interoperabile dovrà permettere a questi sistemi di comunicare senza distruggere l'informazione quantistica.
Occorre inoltre sviluppare protocolli completamente nuovi. I protocolli dell'Internet classica presuppongono che i dati possano essere copiati, memorizzati e ritrasmessi. Le reti quantistiche devono invece tenere conto della fragilità degli stati, dell'impossibilità di copiarli e della necessità di distribuire e gestire l'entanglement.
Alla ricerca teorica dovrà seguire la definizione di standard comuni, indispensabili per creare un mercato industriale interoperabile. Prima della costruzione di grandi infrastrutture sarà inoltre necessario sviluppare simulatori di rete aperti e scalabili, capaci di verificare protocolli e architetture in condizioni realistiche.

Le sperimentazioni e il ruolo dell'Europa
La Quantum Internet non è ancora una rete globale, ma esistono già importanti sperimentazioni. Sono stati realizzati prototipi di reti quantistiche metropolitane in Italia e in città come Shanghai, Vienna e Tokyo. Il satellite cinese Micius ha inoltre dimostrato la possibilità di distribuire collegamenti quantistici su distanze molto elevate.
Gli autori paragonano l'attuale fase di sviluppo della Quantum Internet agli inizi di Arpanet, la rete sperimentale statunitense dalla quale si sarebbe progressivamente sviluppata Internet. Siamo quindi in una fase pionieristica: le potenzialità sono già visibili, ma le tecnologie, gli standard e le applicazioni definitive devono ancora essere costruiti.
L'Unione europea occupa una posizione rilevante grazie agli investimenti nella ricerca fondamentale e applicata. Programmi finanziati anche dall'European Research Council stanno contribuendo allo sviluppo di nuove architetture e alla definizione dei fondamenti teorici delle reti quantistiche.
Secondo gli autori, l'Europa si distingue da altre aree del mondo per l'attenzione alla ricerca di base. Questa impostazione può produrre progressi concettuali profondi, ma deve essere accompagnata da una maggiore capacità di trasformare le scoperte scientifiche in tecnologie scalabili e applicazioni industriali. Sono quindi necessari investimenti nel trasferimento tecnologico, nella formazione di esperti, nel coordinamento tra infrastrutture nazionali e nella costruzione di una strategia continentale. La competizione non è soltanto scientifica, ma anche economica e geopolitica: i paesi che controlleranno le tecnologie quantistiche potranno influenzare gli standard, la sicurezza e le regole delle comunicazionifuture.

Una trasformazione epistemologica

Gli autori ampliano la riflessione oltre gli aspetti tecnologici (1,2). La Quantum Internet non modifica soltanto il modo di trasmettere dati, ma mette in discussione la nozione stessa di informazione.

L'informazione classica è generalmente considerata oggettiva, copiabile, conservabile e riproducibile. Può essere trasferita senza che l'originale venga necessariamente distrutto. L'informazione quantistica è invece fragile e contestuale: non può essere osservata senza essere modificata, non può essere duplicata perfettamente e può essere consumata dall'atto stesso della misura.

La rete quantistica introduce pertanto una comunicazione fondata sull'anti-replicazione. In un sistema digitale dominato dalla copia, dall'archiviazione permanente e dalla sorveglianza, la Quantum Internet potrebbe rendere possibili scambi che non possono essere registrati o intercettati con i metodi tradizionali.

Questa caratteristica impone anche limiti alla conoscenza dell'osservatore. Non è sempre possibile conoscere completamente uno stato quantistico e, nello stesso tempo, conservarlo intatto per una successiva utilizzazione. *La conoscenza dell'informazione e la sua disponibilità futura non sono più aspetti indipendenti.*

Conclusione

La Quantum Internet rappresenta dunque un ponte tra due mondi. Da una parte vi è il mondo classico, fondato sulla stabilità, sulla ripetibilità e sulla possibilità di copiare l'informazione. Dall'altra vi è il mondo quantistico, caratterizzato dalla sovrapposizione, dall'entanglement, dalla non-località e dall'impossibilità di duplicare perfettamente uno stato sconosciuto.

La costruzione di questo ponte è già iniziata, ma richiederà progressi considerevoli nelle memorie quantistiche, nei ripetitori, nei sistemi di trasduzione, nei protocolli e negli standard. Richiederà inoltre la collaborazione tra università, centri di ricerca, governi e industria.

La Quantum Internet non sarà semplicemente un aggiornamento dell'Internet esistente e non la sostituirà. Le due infrastrutture formeranno probabilmente un sistema integrato, nel quale le reti classiche continueranno a gestire gran parte delle comunicazioni, mentre le tecnologie quantistiche forniranno nuovi servizi di sicurezza, calcolo distribuito e trasferimento degli stati.

La portata della trasformazione non sarà soltanto tecnica. Le reti quantistiche potranno cambiare il significato della sicurezza, della riservatezza e della conoscenza dell'informazione. Per questo motivo gli autori considerano decisivo il ruolo dell'Europa: chi riuscirà a sviluppare e controllare queste tecnologie non disporrà soltanto di strumenti più avanzati, ma potrà contribuire a stabilire le regole delle comunicazioni del futuro.

Riccardo De Gobbi e Giampaolo Collecchia

Bibliografia

1) Cacciapuoti A.,Illiano J, Caleffi M.: Quantum Internet Addressing IEEE Network vol 34 2020 e vol 38 2024
2) Cacciapuoti A., Caleffi M: Quantum Internet Un ponte tra due mondi Micromega n. 6 2025