28 dicembre 2021 12:36

Computer quantistici, finanza e coscienza

di Alessandro Pedone

Più volte abbiamo scritto da queste colonne che il decennio che stiamo vivendo sarà caratterizzato dalla convergenza di una serie di innovazioni tecnologiche che cambieranno drasticamente il nostro modo di vivere. I principali settori che saranno coinvolti sono: l'energia (batterie e solare/rinnovabili), il trasporto (veicoli elettrici e guida autonoma), la produzione di merci (stampa 3d), le telecomunicazioni (la rete satellitare che porterà internet in ogni luogo del mondo), la medicina (genomica) ed infine l'alimentazione (con la fermentazione di precisione).
Una tecnologia trasversale che porterà contributi in tutti i settori è l'intelligenza artificiale ed in particolare le reti neurali ed il machine learning che saranno sempre più in grado di fare cose che in precedenza richiedevano intelligenza (intesa in senso umano).
In questo articolo parliamo di una tecnologia emergente che - come l'intelligenza artificiale, ed anzi in congiunzione con essa - darà un contributo enorme a rivoluzionare praticamente tutti i settori dell'attività umana, ma farà ancora di più: darà una spinta decisiva nel cambiamento di paradigma scientifico, nella Weltanschauung, che è già in corso, ma solo agli inizi. Da poco tempo è possibile iniziare ad investire specificatamente in questa tecnologia, che cambierà drasticamente anche la finanza stessa come praticamente ogni cosa, e per questo vogliamo iniziare ad affrontarla con un articolo introduttivo. Come si sarà compreso dal titolo, mi riferisco ai computer quantistici e più in generale alla scienza dell'informazione quantistica di cui i computer rappresentano il supporto materiale, ma - come vedremo - la parte immateriale sarà ancora più rilevante nel cambio di paradigma in corso.

L'informatica: il motore di tutte le innovazioni

Praticamente tutte le innovazioni tecnologiche e di processo più rilevanti degli ultimi 50 anni sono state rese possibili grazie al contributo fondamentale del costante incremento della potenza computazionale.
Il primo microprocessore costruito dall'italiano Federico Faggin (1) agli inizi degli anni '70 conteneva circa 2300 transistor. Oggi, a 50 anni di distanza, i microprocessori sono più potenti di oltre **un milione di volte!** I microprocessori sono praticamente dappertutto, perfino in qualche spazzolino da denti! Se non ci si sofferma un poco a pensarci, non ci si rende facilmente conto di cosa significhi incrementare di un milione di volte qualcosa. Hegel ci ha insegnato che un aumento quantitativo implica anche una variazione qualitativa. Ancora meno si riesce a comprendere cosa significhi incrementare la **potenza computazionale**. La capacità di fare calcolo è qualcosa di parzialmente astratto che facciamo fatica a comprendere, in particolare nei suoi aspetti di calcolo logico (algebra booleana).
Così come l'invenzione del motore a vapore aprì la strada a tutta una serie di cambiamenti (prima tecnologici e poi sociali) e la stessa cosa accadde con l'elettrificazione nei primi del '900, negli ultimi 50 anni abbiamo assistito alla diffusione pervasiva di strumenti elettronici in grado di processare informazioni dai quali praticamente dipendiamo.

Lo stesso denaro e tutto il sistema finanziario dipende da questi strumenti. Si pensi ad un qualsiasi servizio o strumento un minimo complesso di utilizzo comune e ci si rende conto che oggi non sarebbe fattibile se da qualche parte non ci fosse stato un microprocessore che ha realizzato qualche tipo di calcolo booleano indispensabile affinché quel servizio o prodotto fosse realizzato.
Il settore che forse è stato (e sarà ancora di più in futuro) maggiormente influenzato dall'informatica è proprio la scienza in generale.
L'informatica sta impattando la scienza in modo determinante sia in un senso superficiale, cioè fornendo degli strumenti che potenziano le sue capacità, sia in un senso più profondo, ovvero modificando il suo paradigma di base cioè la sua **visione del mondo**.
La scienza per eccellenza è la fisica, dalla quale quasi tutto deriva.
La fisica vede(va?) il mondo come composto essenzialmente di materia ed energia. Questo modo di vedere il mondo è coerente con la fisica cosiddetta "classica", cioè quella newtoniana fatta di corpi che vengono spostati da forze.
Questa fisica è stata messa in discussione dalla meccanica quantistica che vede la fisica newtoniana come un'approssimazione valida se parliamo di corpi composti da miliardi di particelle, ma quando affrontiamo l'infinitamente piccolo, come nel caso delle particelle elementari, valgono leggi completamente diverse ed apparentemente assurde di cui accenneremo qualcosa in seguito.
La validità scientifica della meccanica quantistica non è assolutamente in discussione anche perché è posta a fondamento di una serie di avanzamenti tecnologici che dimostrano senza ombra di dubbio la sua consistenza (per la costruzione degli gli stessi transistor che compongono i microprocessori, date le dimensioni così piccole che hanno raggiunto, oggi ci avvaliamo della meccanica quantistica). Vi è però un problema importante che sta occupando, da svariati decenni, le migliori menti del pianeta: non si riesce ad unificare la teoria quantistica con la relatività generale ed in particolare con la forza di gravità. Entrambe le teorie sono indubbiamente valide, ma non sono conciliabili e quindi deve esserci qualcosa di ancora più fondamentale che non abbiamo compreso.
Ed è qui che entra in gioco l'informatica in un senso più profondo.
Qualche mente particolarmente illuminata, come John Archibald Wheeler (forse fra i 10 fisici moderni più importanti insieme a Einstein, Fermi, Bohr, Feynman, Planck, Marie Curie, Tesla e pochi altri), iniziò a vedere la teoria dell'informazione non più come un insieme di strumenti atti a fare computer, ma come qualcosa di più fondamentale, ontologico. In un suo celebre scritto del 1989 riassunse la sua teoria con la celeberrima espressione "*it from bit*". Con questa espressione Wheeler voleva affermare che ciò che esiste materialmente (*it*) deriva da qualcosa di immateriale (*bit*), cioè l'informazione.
Dalla "provocazione" di Wheeler è nata una nuova teoria dell'informazione che va anche oltre l'informazione di Shannon, quel tipo di informazione alla base dell'informatica tradizionale. Una serie di fisici inizia a descrivere il mondo non tanto in termini di materia o energia, quanto di informazione (le tre cose sono aspetti inscindibili di una stessa cosa). Come vedremo in seguito, con l'avvento dei computer quantistici, è ragionevole pensare che questo cambio di paradigma subirà un'enorme accelerazione e porterà ad innovazioni assolutamente impensabili ed impensate.

Cosa differenzia un computer quantistico?

I computer tradizionali si basano sulla fisica classica e fondamentalmente manipolano "bit" di informazioni.
Nell'informatica tradizionale, un bit è l'unità minima di informazione ed è binaria, ovvero può assumere solo uno stato o il suo opposto: acceso/spento, pieno/vuoto, zero/uno, ecc.
Per conservare questi bit, i computer tradizionali utilizzano pezzi di materia sempre più piccoli, ma ancora sufficientemente grandi da essere ricondotti alle leggi della fisica classica (ultimamente le dimensioni sono così piccole che nei processi produttivi devono essere utilizzati i principi della meccanica quantistica, ma poi il funzionamento è riconducibile alla fisica classica).
I computer quantistici si basano sulla meccanica quantistica e fondamentalmente manipolano "qubit" i quali hanno caratteristiche assolutamente particolari, direi strabilianti. Per conservare questi qubit i computer quantistici utilizzano "oggetti" appartenenti al mondo dell'infinitamente piccolo, spesso proprio fotoni oppure atomi raffreddati a temperature prossime allo zero assoluto.
Quali sono queste caratteristiche strabilianti dei qubit? Per comprenderlo dobbiamo accennare, anche se molto, molto superficialmente, a due concetti della meccanica quantistica: la *sovrapposizione* e l'*entanglement.*

Dal momento che sono due concetti che appaiono fantascientifici è bene prima precisare che non si tratta di teorie filosofiche o ipotesi, ma di qualcosa di reale ormai sperimentato oltre ogni ragionevole dubbio. Indubbiamente, se applichiamo a questi fenomeni il contesto interpretativo dello spazio/tempo tradizionale, che si accorda con i nostri sensi percettivi, facciamo fatica ad accettare che questi fenomeni siano reali. Se proviamo ad ipotizzare una realtà nella quale lo spazio/tempo che noi conosciamo è solo un caso particolare di una realtà più vasta, allora riusciamo ad accettare anche il bizzarro comportamento della “materia” (più precisamente di ciò che ci appare come materia) ai livelli dell’infinitamente piccolo.
Tornando al concetto di sovrapposizione, una particella può avere delle proprietà che possono essere osservate con degli appositi rilevatori. La più citata proprietà è lo *spin*. Per semplicità, possiamo immaginare lo spin come una freccia che può puntare in una certa direzione. Immaginiamo adesso che quella particella sia il nostro qubit. Quando “interroghiamo” il qubit (cioè rileviamo lo spin) lo stato della “freccia” può essere in alto, in basso oppure in una infinità di stati tra le due possibilità.
Fin qui non ci sarebbe niente di particolarmente strabiliante, il principio di sovrapposizione però ci dice che fino a quando il qubit non viene effettivamente osservato si trova in una sovrapposizione di tutti gli stati possibili. Si potrebbe pensare che semplicemente noi non sappiamo in che stato si trovi e quindi possiamo *ipotizzare* che si trovi in uno qualsiasi degli stati possibili, ma non è questo che la meccanica quantistica ci dice. Il fatto è che quel qubit è proprio contemporaneamente (per quanto questo termine implichi il tempo, e qui stiamo parlando di realtà che vanno oltre il concetto stesso di tempo) in una sovrapposizione di tutti gli stati possibili. Questo cambia assolutamente tutto. In modo improprio, ma cercando di far capire il concetto, si potrebbe dire che da un certo punto di vista, è come se “dentro” un qubit vi fossero infiniti bit.
Il secondo principio utilizzato dai computer quantistici, forse ancor più stupefacente, è quello dell’entanglement. Il termine è difficilmente traducibile in italiano e tutti utilizzano la parola inglese. Si potrebbe tradurre come “intreccio” o “aggrovigliamento”, ma non renderebbe l’idea. Si tratta del collegamento fra due particelle che sono state in relazione in qualche processo fisico. Questo collegamento fa sì che *indipendentemente* dalla distanza alla quale queste due particelle si trovano, se una particella cambia una sua proprietà (ad esempio lo spin), istantaneamente anche l’altra particella cambia in maniera speculare.
Se non c’hai capito niente non ti preoccupare, è normale. Il grandissimo fisico Feynman (sembra che la frase sia anche di Bohr) diceva che nessuno capisce veramente la meccanica quantistica.
Se invece la cosa ti lascia incredibilmente stupito ed anche incredulo, questo è un ottimo segno perché significa che forse hai iniziato a comprendere l’enorme grandezza delle implicazioni di tutto questo.

Cosa si può fare con un computer quantistico?

Avere come base i qubit invece dei bit consente di realizzare algoritmi completamente diversi perché i qubit permettono di costruire porte logiche totalmente diverse ed inconcepibili in assenza delle due proprietà quantistiche accennate nel paragrafo precedente.
Senza entrare nel tecnico, si può dire che un certo tipo di calcoli che con i computer tradizionali richiederebbero un tempo enorme, nell’ordine di decine o centinaia di anni, con i computer quantistici si possono realizzare nello spazio di secondi o minuti.
Questo è particolarmente rilevante nel settore della crittografia e della sicurezza dei dati in generale. Ad oggi, la sicurezza dei dati è strettamente connessa all’incapacità dei computer tradizionali di fare dei calcoli estremamente complessi in tempi ragionevoli.
Quando i computer quantistici saranno diffusi, questo genere di applicazioni di sicurezza non avranno più senso e si aprirà la via ad una nuova categoria di sistemi di sicurezza basati sul cosiddetto “teletrasporto quantistico” (2) che non ha niente a che vedere con Star Trek, ma molto a che vedere con l’entanglement.
Questa cosa rende i computer quantistici un tema strettamente legato alla sicurezza nazionale e per questo tutte le grandi nazioni stanno facendo la corsa alla realizzazione dei migliori computer quantistici.
Gli USA, ad esempio, hanno avviato il “NATIONAL QUANTUM INITIATIVE” che finanzia con centinaia di milioni di dollari progetti di ricerca nel campo dei computer quantici.
Uno dei cinque centri che fanno parte del progetto, probabilmente il più prestigioso, è guidato da una ricercatrice italiana che ha studiato all'università di Pisa, Anna Grassellino, che lavora presso il FermiLab (il corrispondente USA del CERN). Il progetto diretto da Anna Grassellino ha l’obiettivo di realizzare entro 5 anni il più potente computer quantistico al mondo.

Per avere un'idea della potenza di calcolo che potrebbero avere questi computer, per certi tipi specifici di calcolo, un unico computer quantistico con 256 qubit (effettivamente realizzato presso l'Harvard-MIT Center for Ultracold Atoms??) può calcolare un numero di stati quantistici superiori al numero di atomi presenti nell'universo! Una volta affinata questa tecnologia relativamente a tutti gli altri componenti del computer quantistico, la potenza di calcolo di uno solo di questo genere di computer sarà superiore alla potenza combinata di tutti i computer connessi attualmente funzionanti, compresi i supercomputer!
Tutta una serie di problemi, in particolare quelli troppo complessi legati alla realizzazione di nuovi materiali o ancora di più alla biologia, che oggi non sono affrontabili con gli algoritmi tradizionali potrebbero essere affrontati e risolti da questi nuovi computer.
Non bisogna commettere l'errore di pensare ai computer quantistici come ai sostituti dei computer tradizionali, sicuramente non nel futuro ipotizzabile (magari fra 50 o 100 anni).
Al momento, il rapporto che c'è fra un computer tradizionale ed uno quantistico è lo stesso che potremmo immaginare tra un'automobile ed una navicella spaziale.
Non useremo i computer quantistici per fare fogli di calcolo, navigare sul web o scrivere articoli come sto facendo in questo momento.
Nei prossimi 10 o 20 anni avremo qualche migliaia, forse qualche decina di migliaia di computer quantistici collegati alla rete ed accessibili attraverso computer tradizionali che faranno girare particolari tipologie di algoritmi.
A meno di innovazioni tecnologiche strabilianti (magari realizzate proprio grazie ai primi computer quantistici) difficilmente potremo vedere un computer quantistico miniaturizzato per un limite fisico di cui parleremo nel prossimo paragrafo nel quale entriamo nell'aspetto finanziario del tema.

Finanza e quantum computing

Fra le grandi aziende quotate che maggiormente si stanno occupando di computer quantistici troviamo Google, Microsoft, IBM, Intel ed Honeywell.
Come spesso accade quando ci troviamo in presenza di cambiamenti tecnologici dirompenti è probabile che i leader delle vecchie tecnologie non sia in grado di diventare anche i leader nella nuova. Tra le nuove aziende quotate troviamo due realtà interessanti: una è IonQ e l'altra è Rigetti Computing (quotata da poche settimane).
Ci sono diverse aziende non ancora quotate che lavorano nel campo, una delle più famose è probabilmente D-Wave che ha un approccio ai computer quantici piuttosto originale e difficile da valutare (computer quantistici adiabatici). Ma vi sono anche la canadese Xanadu, QC Ware che opera prevalentemente nel software, ColdQuanta che sviluppa materiali per computer quantistici e diverse altre aziende.
Dal punto di vista degli investimenti finanziari, il settore dei computer quantistici è decisamente ancora troppo agli albori.
Il problema fondamentale è che non abbiamo ancora trovato una tecnologia sufficientemente affidabile, stabile e scalabile per costruirli.
Al momento, affinché non si perdano le proprietà quantistiche delle particelle che vengono utilizzate per realizzare i qubit dobbiamo tenerle a temperature prossime allo zero assoluto (oltre -273 gradi celsius).
Alcuni ricercatori hanno perfino paragonato i computer quantistici alla fusione nucleare. Volendo dire, con questo paragone, che si tratta di una tecnologia che in teoria risolve tutti i problemi, ma in pratica non riusciamo a trovare il modo per realizzarla profittevolmente (3).
Personalmente ritengo che il paragone sia del tutto improprio e che lo sviluppo dei computer quantistici sarà molto, ma molto più rapido rispetto a quello dei reattori a fusione nucleare.
Ad oggi esistono diversi computer quantistici nel mondo ed hanno dimostrato che la teoria sviluppata nell'ambito dell'informatica quantistica, prima che questo tipo di computer fossero fisicamente realizzati, è assolutamente valida.

I finanziamenti pubblici in questo settore sono abbondanti proprio perché il possesso di questa tecnologia è una questione di sicurezza nazionale e non c'è nessuna grande nazione che possa permettersi di esserne fuori.
Ad oggi, quindi, non mi sentirei di consigliare a nessuno di investire direttamente in questo settore cifre non dico importanti, ma anche solo significative.
Gli appassionati di tecnologia potrebbero investire delle cifre trascurabili più per avere una buona scusa per restare informati sul tema ed investire più pesantemente mano a mano che questa tecnologia evolverà.

E' di fondamentale importanza, per chi intenda investire anche piccolissime cifre in questo settore, comprendere che siamo ancora lontani dall'avere un "prodotto" stabile e che le aziende che si occupano esclusivamente di questo settore non possono che perdere soldi e necessiteranno in futuro di molto capitale. Si tratta di un investimento i cui frutti apprezzabili si potranno vedere non prima di 5/10 anni.
Tra i settori che saranno completamente trasformati dai computer quantistici ci sarà sicuramente anche il settore finanziario che è già stato radicalmente trasformato dall'avvento dell'informatica e che si appresta a subire una nuova trasformazione legata sia alla blockchain che all'intelligenza artificiale.

Il problema "difficile" della coscienza e la teoria dell'informazione

Ritengo che il problema più importante che la scienza affronterà nei prossimi decenni non sarà l'unificazione della meccanica quantistica con la relatività generale (chiamata anche "teoria del tutto") bensì quello che il filosofo David Chalmers ha chiamato, con un'espressione che ha riscosso un enorme successo nel mondo accademico, "*the hard problem of consciousness*". (4) Per capire il "problema difficile della coscienza" è necessario in primo luogo comprendere il concetto filosofico di qualia. Un qualia rappresenta l'aspetto qualitativo di una esperienza che si distingue dall'aspetto fisico al quale essa si associa. Tipicamente si fa l'esempio del profumo di una rosa. L'esperienza del profumo di una rosa non è costituito da tutte le percezioni bioelettriche del nostro corpo che si associano con quell'esperienza. Il nostro apparato fisico percepisce una serie di sostanze che poi tramuta in impulsi elettrici i quali viaggiano nei nostri nervi fino al cervello e qui subiscono una serie molto complessa di trasformazioni chimiche ed elettriche. Secondo l'interpretazione filosofica proposta da David Chalmers (e molti altri insieme e prima di lui) in nessun modo l'esperienza del profumo della rosa può essere ridotta a questi aspetti fisici.
Se anche un giorno fossimo in grado di descrivere nei minimi dettagli, perfino a livello atomico, il funzionamento del cervello, non potremo comunque spiegare l'esistenza dei qualia.
Ad oggi, la maggioranza degli scienziati continua a ritenere che la coscienza sia un epifenomeno, o fenomeno emergente, dalla materia. In sostanza ritiene che il cervello "produca" la coscienza più o meno come il fegato produce la bile.
La maggior parte degli scienziati tende ancora a vedere il mondo in termini di materia ed energia e non può che ritenere che tutto ciò che non è né materia né energia debba necessariamente essere un prodotto di questi ultimi che considera i costituenti basilari di ogni cosa esistente.
Negli ultimi decenni, però, ha iniziato a farsi spazio una disciplina, figlia dell'informatica, che prende il nome di teoria dell'informazione e che tende a vedere il mondo in termini di informazioni che prescindono dal supporto materiale attraverso il quale tale informazione viene veicolata. Come già scritto, il primo esponente di questa scuola è il fisico Wheeler, ma in questo ultimo paragrafo ci tengo a citare la più recente (e credo promettente) teoria che è stata sviluppata dal fisico teorico dell'università di Pavia, Giacomo Mauro D'Ariano con il contributo di Federico Faggin (sì, lo stesso che ha inventato il microprocessore ed il touchscreen). Per la prima volta nella storia abbiamo una teoria scientifica, matematicamente modellizzata e falsificabile (5), che risolve il problema difficile della coscienza!
E' in pubblicazione su una rivista scientifica l'articolo "Hard Problem and Free Will: an information-theoretical approach" che descrive questo nuovo approccio al problema della coscienza.
Naturalmente, descrivere questa teoria va ben oltre gli scopi di questo articolo (e le possibilità del suo autore) ma ci tengo a sottolineare come l'informatica quantistica abbia giocato un ruolo chiave nello sviluppo di questa teoria e come sia la prima che consente di affrontare su un piano scientifico una questione che la quasi totalità degli scienziati, fino ad oggi, riteneva che non fosse neppure di sua competenza poiché non c'è niente di più "soggettivo" che il problema della coscienza. Cambiando il paradigma scientifico, spostando l'accento dalla materia/energia all'informazione è possibile affrontare (ed un giorno forse anche risolvere) questo problema insieme a molti altri.
Questo è l'esempio più rilevante di come i computer quantistici stiano aprendo la strada ad una serie di possibilità inimmaginabili perché non sono semplicemente un avanzamento tecnologico, sono il mezzo attraverso il quale l'umanità cambierà il modo di concepire il mondo stesso.

Note

1. Considero Federico Faggin l'italiano vivente che ha maggiormente contribuito allo sviluppo dell'umanità e che sta maggiormente contribuendo al suo sviluppo futuro. Inventore, imprenditore, scienziato, filosofo e ricercatore spirituale ha dato un contributo fondamentale allo sviluppo della tecnologia necessaria per sviluppare i microprocessori - che poi ha effettivamente realizzato - ed ha inoltre capeggiato il team di ingegneri che hanno inventato i sistemi di puntamento sensibili al tocco che tutti utilizziamo nei nostri telefonini, nei touchpad ed in tutti gli schermi touch che si stanno diffondendo ovunque, automobili comprese. Sebbene il contributo che ha dato nell'evoluzione tecnologica degli ultimi 50 anni sia enorme, questa è poca cosa rispetto al contributo che sta dando alla scienza con la sua fondazione che si occupa di finanziare un settore della ricerca teorica di base che molto difficilmente sarebbe sviluppata senza il suo contributo determinate: la coscienza non intesa come epifenomeno, ma intesa come costituente base della realtà.
2. Il termine teletrasporto è ampiamente fuorviante spesso abusato dai media. In sostanza è una tecnica di informatica quantistica la quale, sfruttando l'entanglement, permette di trasferire uno stato quantico da un punto all'altro istantaneamente. Ad oggi, sono stati realizzati diversi esperimenti di questo tipo con distanze di alcune decine di chilometri.
3. In realtà anche nel campo della fusione nucleare qualcosa sta cambiando e si stanno realizzando i primi reattori a fusione nucleare che producono più energia di quanto ne consumano.
4. Non tutti gli studiosi che si occupano del problema mente/cervello accettano l'esistenza del "problema difficile della coscienza". Fra gli studiosi di una certa rilevanza a livello internazionale che contestano il problema vi sono Daniel Dennett e Antonio Damasio. Fra gli studiosi che accolgono la posizione di David Chalmers autorevolissimi neuroscienziati cognitivisti come Francisco Varela, Giulio Tononi, e Christof Koch.
5. La concezione moderna della scienza, molto influenzata dal pensiero del grande filosofo Karl Popper, ritiene che una teoria sia scientifica solo se consente, almeno in ipotesi, di essere smentita, cioè se è possibile in teoria, realizzare degli esperimenti che possano dimostrare che è sbagliata.

CHI PAGA ADUC
l'associazione non **percepisce ed è contraria ai finanziamenti pubblici** (anche il 5 per mille)
La sua forza sono iscrizioni e contributi donati da chi la ritiene utile
DONA ORA (http://www.aduc.it/info/sostienici.php**)**