RAIFFEISEN

Raiffeisen Svizzera
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Il parere dell'economista capo di Raiffeisen

Un quantum di consolazione

"Un quantum di consolazione" è un'espressione che ho tratto dal film intitolato in italiano "Quantum of Solace – Solo per i tuoi occhi", che in lingua inglese originale era "Quantum of Solace" tout court, ossia tradotto "un quantum di consolazione" oppure "un minimo di sollievo", della serie di James Bond del registra Marc Forster, uscito nelle sale cinematografiche a fine 2008 e che vedeva l'attore inglese Daniel Craig impersonare per la seconda volta il ruolo dell'agente segreto 007. Anche in tedesco il film avrebbe dovuto intitolarsi "Ein Minimum an Trost", per l'appunto "una minima consolazione", per evidenziare il legame con l'organizzazione segreta che Bond combatte nel film, ma fu poi cambiato per motivi promozionali in "Ein Quantum Trost", ossia "un quantum di consolazione". Un po' di sollievo lo possiamo trovare anche quando ci avventuriamo nel mondo del "quantum computing", che possiamo definire come computazione quantistica o anche informatica quantistica. Al momento tutto ruota ancora attorno alla grande novità dell'intelligenza artificiale, ma il quantum computing potrebbe presto essere "la prossima grande scoperta". Si tratta di una tecnologia emergente molto promettente, che si sta sviluppando a ritmo sostenuto, ma che sta già gettando un'ombra sul presente. Qui e ora.

Come funzionano questi computer quantistici?

I computer quantistici o quantum computer si basano sui cosiddetti bit quantistici, noti anche come qubit, i quali possono assumere non solo valore zero e uno contemporaneamente, ma anche qualsiasi stato intermedio. Questa capacità, denominata "superposizione", consente ai quantum computer di eseguire un gran numero di calcoli in contemporanea. Inoltre, grazie al principio della correlazione quantistica, o "entanglement quantistico", i qubit possono rimanere in contatto tra loro anche a grandi distanze, poiché connessi. Queste due proprietà conferiscono al computer quantistico il potenziale per risolvere problemi che altrimenti sarebbero irrisolvibili per i computer classici o che potrebbero essere risolti soltanto con un onere gigantesco e sproporzionato.

Le comuni procedure di crittografia verso l'inutilità

Questa evoluzione comporta, tuttavia, una delle maggiori preoccupazioni: la sicurezza dei dati. Considerato che i computer quantistici sono molto più potenti e performanti dei supercomputer convenzionali, tutti i metodi di crittografia dei dati attualmente in uso non saranno più sufficienti a soddisfare i requisiti di sicurezza. L'algoritmo per decifrare gli odierni processi di crittografia esiste già. Manca solo un computer che disponga della potenza sufficiente per eseguire questo algoritmo. Per ora il giorno "Q" in cui i computer quantistici raggiungeranno questa soglia è ancora lontano diversi anni. Ciononostante, già oggi sussiste una necessità di intervento ragguardevole.

Urgente necessità d'intervento

Ovviamente, la sicurezza dei dati è un pilastro centrale del nostro mondo e, di conseguenza, la crittografia è onnipresente. L'accesso a un sito web sicuro o il trasferimento di denaro avvengono in maniera criptata. Se le informazioni sensibili non fossero protette, la fiducia nel sistema finanziario globale crollerebbe all'istante. E senza la protezione garantita dalla crittografia la gestione delle infrastrutture nazionali critiche sarebbe esposta all'accesso da parte di forze oscure. Un'eventualità che è un vero e proprio incubo. Lo stesso dicasi altresì per la proprietà intellettuale e i segreti aziendali di molte imprese. Va detto che già oggi i criminali e gli Stati canaglia rubano e conservano i dati codificati allo scopo di poterli decifrare con un computer quantistico tra qualche anno quando disporremo di questa tecnologia. Tale strategia è nota anche come "harvest now, decrypt later", che tradotto in italiano significa "raccogli ora (i dati), decripta dopo". È quindi giunto il momento di passare piuttosto urgentemente a un processo di codifica migliore. I ricercatori di tutto il mondo stanno già lavorando a metodi di codifica "post quantum" o "quantum resistant", ossia per l'era post quantum o resistenti alla potenza di calcolo dei computer quantistici.

RAIFFEISEN

Raiffeisen Svizzera
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Il parere dell'economista capo di Raiffeisen

Un quantum di consolazione

Piccola consolazione

Una piccola consolazione risiede nel fatto che, quantomeno secondo gli esperti, siamo ancora a circa dieci anni di distanza dalla rivoluzione quantistica e pertanto disponiamo ancora di un po' di tempo. Per arrivare a calcoli utili da parte dei computer quantistici occorre un numero gigantesco di qubit. Il più grande computer quantistico attualmente esistente è quello di Atom Computing, che dispone di 1180 qubit. Secondo le stime calcolate da Craig Gidney, scienziato in forza presso Google, per decifrare una crittografia effettuata secondo gli standard più moderni e all'avanguardia sarebbero necessari 20 milioni di qubit. A ciò si aggiunge anche il problema che i bit quantistici sono soggetti a errori. Vibrazioni termiche, raggi cosmici, interferenze elettromagnetiche o disturbi di altro genere possono causare un errore ogni intervallo composto da cento fino a diecimila operazioni. Con un tale tasso di errore non è possibile risolvere compiti complessi che richiedono milioni di fasi di calcolo. Ciononostante, lo sviluppo compie passi avanti progredendo rapidamente anche in questo campo. Di recente, infatti, i ricercatori di Google sono riusciti a ridurre in misura considerevole il tasso di errore raggruppando diversi bit quantistici in un bit quantistico logico simile a una scacchiera, che consente nello specifico di riconoscere e correggere gli errori.

È affascinante seguire lo sviluppo del quantum computing, la tecnologia informatica quantistica, in quanto racchiude in sé un enorme potenziale economico. Allo stato attuale sono ipotizzabili applicazioni, ad esempio, nel campo della gestione dei rischi, dell'ottimizzazione dei processi logistici, ma anche della scoperta di nuovi materiali e dei processi chimici, i quali in futuro potrebbero anche portare a nuovi farmaci rivoluzionari e pertanto magari altresì all'eliminazione di determinate malattie. Ma i computer quantistici ci ricordano anche ed evidenziano chiaramente quanto il nostro mondo sia diventato fragile. Tanto per citare un esempio, a luglio si è verificato il più grande guasto informatico di tutti i tempi. Guasto di cui era responsabile la società di software di sicurezza Crowdstrike. Un bug, ossia un difetto, nell'aggiornamento ha paralizzato aeroporti, ospedali e società operanti nel settore dei media a livello globale. Nel mondo reale le serrature meccaniche proteggono gli oggetti di valore. Certo, un lucchetto può essere forzato e rotto con uno sforzo corrispettivo, ma non tutti i lucchetti del mondo possono essere aperti in contemporanea. Tuttavia, con l'avvento dei computer quantistici, le serrature digitali in uso da decenni a livello mondiale potrebbero essere aperte in un colpo solo, se non le sostituiamo al più presto. E forse questo è uno dei motivi che contribuisce a far registrare al prezzo dell'oro sempre nuovi record.

Fredy Hasenmaile,
economista capo di Raiffeisen

RAIFFEISEN

Raiffeisen Svizzera
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Il parere dell'economista capo di Raiffeisen

Un quantum di consolazione