PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5053 di Lunedì 22 novembre 2021

Facciamo il punto sui quantum computer

La rivoluzione tecnica, costituita dal passaggio dalle valvole ai semiconduttori, è comparabile alla rivoluzione tecnica, costituita dal passaggio dai computer a bit ai computer a qubit.

Sempre più spesso si parla di quantum computer, come nuova frontiera dell'informatica. Cogliamo l'occasione per offrire ai lettori una panoramica su questa nuova tecnologia, che sta compiendo solo adesso i primi passi.

Per cominciare, un recente studio ha portato ad una valutazione di un mercato per i quantum computer dell'ordine di 240 miliardi di dollari per il 2040, quando queste macchine potranno affrontare e risolvere problemi, che con i moderni computer richiedono miliardi di anni di calcoli per la risoluzione.

Vediamo quali sono i principali problemi da affrontare e risolvere.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

I quantum computer utilizzano i quantum bits, correntemente chiamati qubit.

Mentre i computer tradizionali utilizzano bit che valgono 0, oppure 1, un qubit può esistere simultaneamente sia come 0, sia come 1, conferendo ai quantum computer una potenza di calcolo terrificante. Ad esempio, se ci troviamo davanti a una stringa di 2 bit, le combinazioni possibili sono solo quattro (00,01,10, 11); se invece ci troviamo davanti ad una stringa di qubit, le combinazioni possibili sono il doppio.

Provi il lettore ad immaginare quante combinazioni possono essere sviluppate, quando ci troviamo davanti ad una stringa di 8 qubit!

Il problema da risolvere, al momento, è che questi computer commettono spesso degli errori e sono purtroppo intrinsecamente instabili, richiedendo tutta una serie di apparecchiature e sistemi di supporto, per mantenerli in efficienza. Più aumenta il numero dei qubit gestiti, maggiori sono i problemi da risolvere.

Ad oggi, i cinesi sono riusciti a mettere a punto una macchina con 76 qubit, ma tutta la potenza di calcolo di queste macchine verrà sviluppata quando il computer potrà gestire milioni di qubit.

Per costruire un quantum computer è possibile basare il progetto su circuiti, che utilizzano sistemi criogenici di alta potenza per raffreddare i circuiti elettronici a pochi decimi di grado superiori a -273° centigradi. All'aumentare del numero dei qubit trattati, aumenta in modo esponenziale anche la potenza richiesta alle macchine di refrigerazione.

Altri ricercatori stanno lavorando su quantum computer basati su una tecnica completamente diversa, che non ha bisogno di raffreddamento a temperature così basse. Degli ioni, che si comportano come qubit, vengono intrappolati in un ambiente sottovuoto utilizzando campi elettrici, in un contesto ben isolato dall'ambiente. Queste ricerche sono oltremodo promettenti, ma hanno bisogno di raggi laser per controllare ogni singolo ione o qubit e quindi il numero di raggi laser aumenta al crescere del numero di ioni o qubit trattati. Le macchine finora realizzate lavorano abbastanza bene, quando devono gestire alcune diecine di qubit, ma la gestione di milioni di qubit richiederebbe l'attivazione di milioni di raggi laser ed il problema non è certo facilmente risolvibile.

Una terza tecnica, anch'essa in corso di sviluppo negli Stati Uniti, utilizza degli ioni, ma senza utilizzare raggi laser; il controllo è invece affidato a circuiti elettronici; se quindi è possibile realizzare dei moduli standardizzati in grado di elaborare i qubit, resta ancora da superare l'ostacolo posto dalla possibilità di interazione fra numerosi circuiti standardizzati, per realizzare un vero e proprio quantum computer su larga scala.

Vi è chi usa fibre ottiche, vi è chi usa dei campi elettrici, ma queste tecniche sono ancora "rudimentali".

Al momento, certamente nessuno è in grado di affermare quale tecnica potrà affermarsi nel prossimo futuro, ma tutti gli esperti del settore concordano sul fatto che i risultati di queste ricerche sono talmente attraenti, che gli specialisti potrebbero trovare, senza eccessive difficoltà, i finanziamenti necessari per procedere.

Cybersecurity e privacy

È del tutto normale il fatto che gli esperti si preoccupino anche di problemi legati alla sicurezza informatica la protezione dei dati personali di questa particolare categoria di computer. Le tecnologie attualmente usate sono talmente avanzate che non si ha alcuna notizia del fatto che i criminali informatici stiano già lavorando per violare questi sistemi, che, d'altro canto, presentano difficoltà estremamente elevate per essere violati.

Partendo comunque dal principio che poco 0 nulla sia impossibile da realizzare, sarà bene che gli sviluppatori tengano sotto stretta vigilanza anche questi aspetti, oltre evidentemente a potenziare al massimo le capacità di elaborazione, intrinseche nei quantum computer.

Terremo aggiornati i lettori sui progressivi sviluppi.

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it