

## CRONOLOGIA DEI COMPUTER QUANTISTICI

**Primi anni del 1900:** Albert Einstein, Max Plank, Enrico Fermi, Werner Heisenberg, Wolfgang Pauli, Louis de Broglie ed altri diedero vita alla teoria che prende il nome di "fisica quantistica".

**1936:** Birkhoff e Von Neumann pubblicano l'articolo "The Logic of Quantum Mechanics". L'idea di fondo fu quella di far vedere come il formalismo matematico della meccanica quantistica potesse ispirare un nuovo tipo di logica.

**1940:** Shannon e Warren Weaver presentano un primo tentativo di definire la Teoria dell'Informazione (classica) nel loro articolo "The Mathematical Theory of Communications".

**1948:** Shannon pubblica il suo lavoro che segna ufficialmente la nascita della Teoria dell'Informazione (classica).

**1973:** Alexander Holevo pubblica un articolo che pone le prime basi della Quantum Information Theory.

**1976:** Un matematico polacco, Roman Ingarden, in uno dei primi tentativi di creare una teoria quantistica dell'informazione, mostra che la teoria dell'informazione classica di Shannon non può essere generalizzata al caso quantistico, ma viceversa, è possibile costruire una teoria quantistica dell'informazione che può essere una generalizzazione della teoria classica di Shannon.

**1981:** Richard Feynman nel suo discorso alla "First Conference on the Physics of Computation" tenutosi al MIT, osservò che sembrava impossibile in generale simulare l'evoluzione di un sistema quantistico su un computer tradizionale. Ma in questa occasione Feynman uscì con un suo classico colpo di genio. Al posto di vedere questa come una limitazione o un problema, egli ribaltò la situazione, vedendola come una opportunità. Egli fece notare che se è necessaria una enorme quantità di computazione per simulare quello che accade in un esperimento di interferenza fra particelle, allora il fatto stesso di preparare l'esperimento e misurare il risultato è **computazione**.

**1985:** David Deutsch, all'Università di Oxford, descrive il primo computer quantistico. Come una qualsiasi macchina di Turing (un modello astratto di computer) può simulare un qualsiasi computer tradizionale, così il computer quantistico di Deutsch può simulare una qualsiasi computazione quantistica. Questa affermazione sollevò la speranza che con un semplice meccanismo (quantistico) si potesse eseguire molti differenti algoritmi quantistici.

**1993:** Dan Simon, alla "Universite de Montreal", inventò un problema teorico per il quale un computer quantistico sarebbe stato esponenzialmente più veloce di un computer tradizionale. Questo algoritmo introdusse le idee principali che furono poi alla base dell'algoritmo di fattorizzazione di Shor.

**1994:** Peter Shor, presso gli AT&T's Bell Labs nel New Jersey, scoprì un algoritmo sorprendente. L'algoritmo di Shor consente ad un computer quantistico di scomporre facilmente nei suoi fattori primi numeri interi, anche enormi. Si capì subito che questo algoritmo avrebbe potuto essere utilizzato per violare la stragrande maggioranza delle attuali chiavi di sicurezza. Questa scoperta innescò un fortissimo interesse verso il calcolo quantistico che prima era quasi solo ambito di fisici e ricercatori informatici.

**1995:** Shor propone il primo schema per la correzione degli errori in un computer quantistico. La correzione degli errori è indispensabile per poter creare un computer che lavori con un numero elevato di qbit. Purtroppo non è ancora disponibile un sistema che corregga gli errori generati dal processo di correzione. Un'alternativa potrebbe essere l'utilizzo di speciali stati che sono immuni dall'errore, ovviamente molto più complessi da gestire.

**1996:** Lov Grover, dei Bell Labs, inventa l'algoritmo di ricerca quantistico per i database.

**1997:** David Cory, A.F. Fahmy e Timothy Havel, contemporaneamente a Neil Gershenfeld e Isaac Chuang del MIT pubblicano un articolo nel quale per la prima volta viene proposto un computer fatto da una singola molecola che memorizza i suoi qbit nello spin dei suoi protoni e neutroni.

In un bicchiere d'acqua ci possono essere miliardi e miliardi di molecole d'acqua. Questo bicchiere, posizionato in una macchina per la risonanza magnetica, simile a quelle utilizzate negli ospedali, avrebbe un enorme quantità di ridondanza, che consentirebbe al sistema di mantenere coerenza quantistica per migliaia di secondi, risultato estremamente migliore di molti altri modelli proposti.

**1998:** viene realizzato il primo computer quantistico a 2-qubit, dimostrato presso l'University of California a Berkeley.

**1999:** viene realizzato il primo computer quantistico a 3-qubit, dimostrato presso l'IBM Almaden Research Center.

**2000:** viene realizzato il primo computer quantistico a 5-qubit, dimostrato presso l'IBM Almaden Research Center. Viene effettuato per la prima volta il calcolo di una parte importante dell'algoritmo di Shor.

**2001:** viene realizzato il primo computer quantistico a 7-qubit, dimostrato sempre presso l'IBM. Prima esecuzione integrale dell'algoritmo di Shor. Viene fattorializzato il numero 15 utilizzando 1018 molecole identiche ognuna contenente 7 atomi.

**2001-oggi:** in molte università di tutto il mondo e in molti centri di ricerca privati sono allo studio le applicazioni reali di quanto è stato già dimostrato su carta essere fattibile tramite un computer quantistico. Dovranno comunque passare ancora almeno 10 anni prima di vedere una applicazione reale raggiungere qualche oggetto della nostra vita di tutti i giorni e prima di vedere i computer quantistici entrare nelle nostra quotidianità come hanno fatto ormai i computer tradizionali. Per approfondire: <http://www.qubit.org>