UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA
DIPARTIMENTO DI INGEGNERIA «ENZO FERRARI»
Corso di Laurea in Ingegneria Informatica

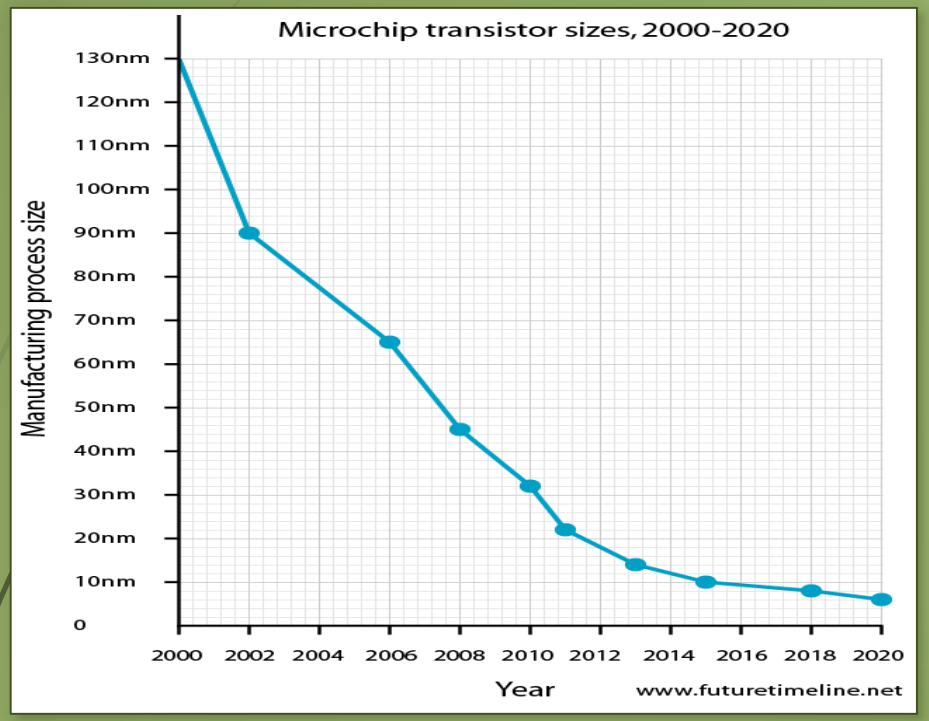
QUANTUM COMPUTER: THE FUTURE OF ENGINEERING

Relatore: Prof.ssa Sonia Bergamaschi

Laureando: Alex Gugliotta

ANNO ACCADEMICO 2015/2016

L'informatica quantistica: ai confini della legge di Moore



Nel 2020 la legge di Moore smetterà di essere valida: Il limite dei transistor sarà di 7 nm

Un po' di storia

- 1965 legge di Moore
- 1980 viene coniato il termine «computazione quantistica»
- 1982 Feynman dimostra che una macchina di Touring non può simularne una quantistica
- Anni '80-'90 studi di Deutsch Jozsa, algoritmi di Shor e Grover
- Inizio secolo: primi *qubit*
- 2007 D-Wave System presenta il «primo» computer quantistico adiabatico

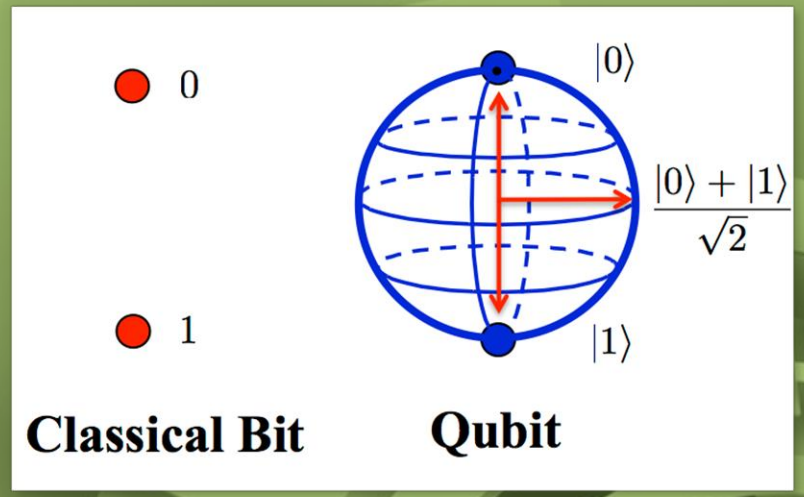
Il *qubit* e la sovrapposizione quantistica

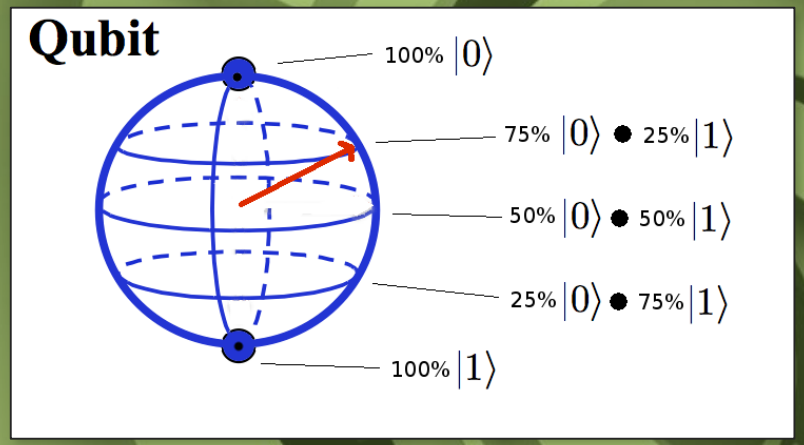
Il *qubit* è l'astrazione di un sistema quantistico che può assumere infiniti valori dati da una sovrapposizione dei due stati logici 1 e 0.

Quando viene osservato la sua funzione d'onda decade in uno dei due stati logici possibili

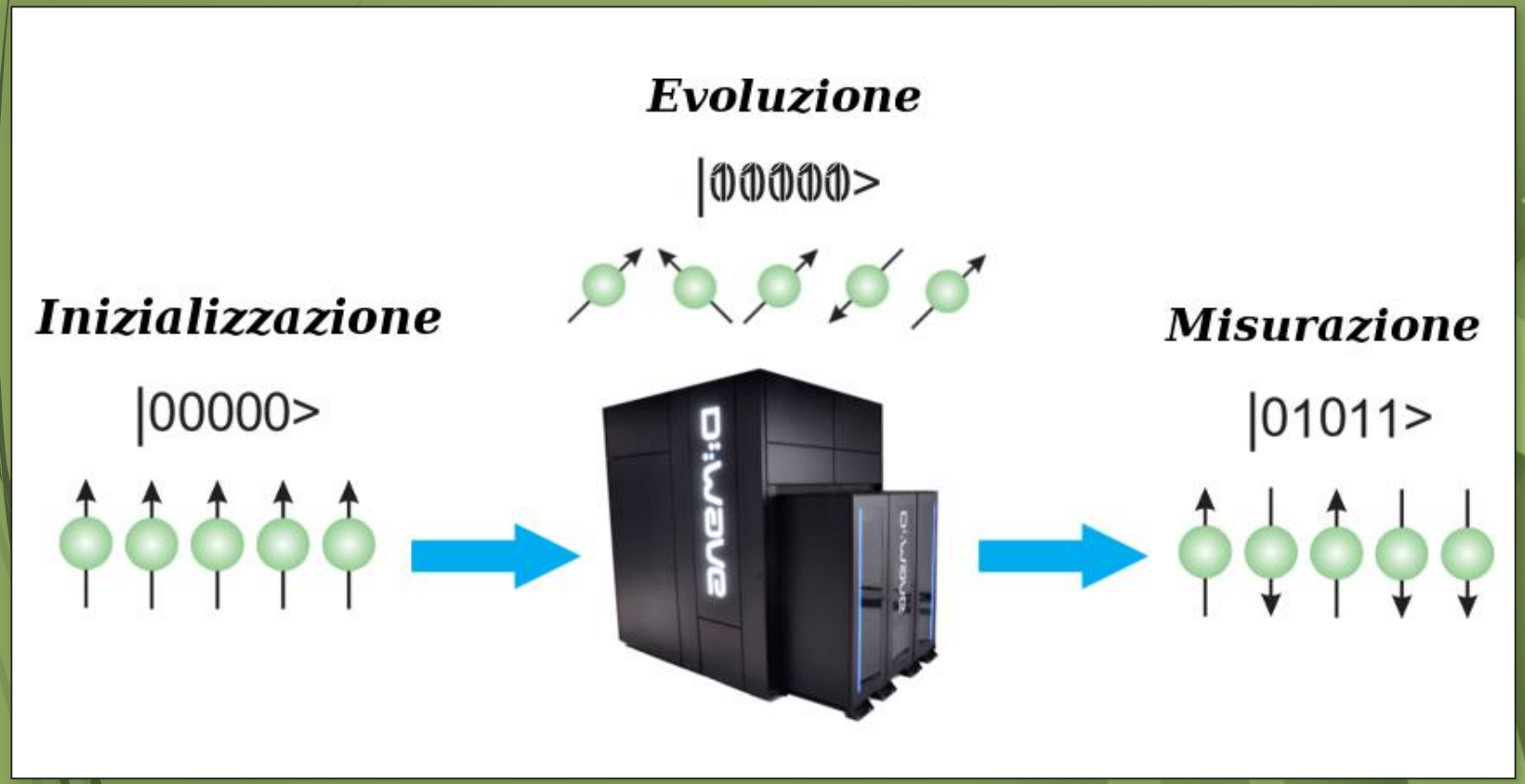
Lo stato ottenuto dipende dalla posizione del vettore probabilistico

L'informazione trasportata dal *qubit* è appunto la probabilità di decadere in uno dei due stati





Parallelismo quantistico



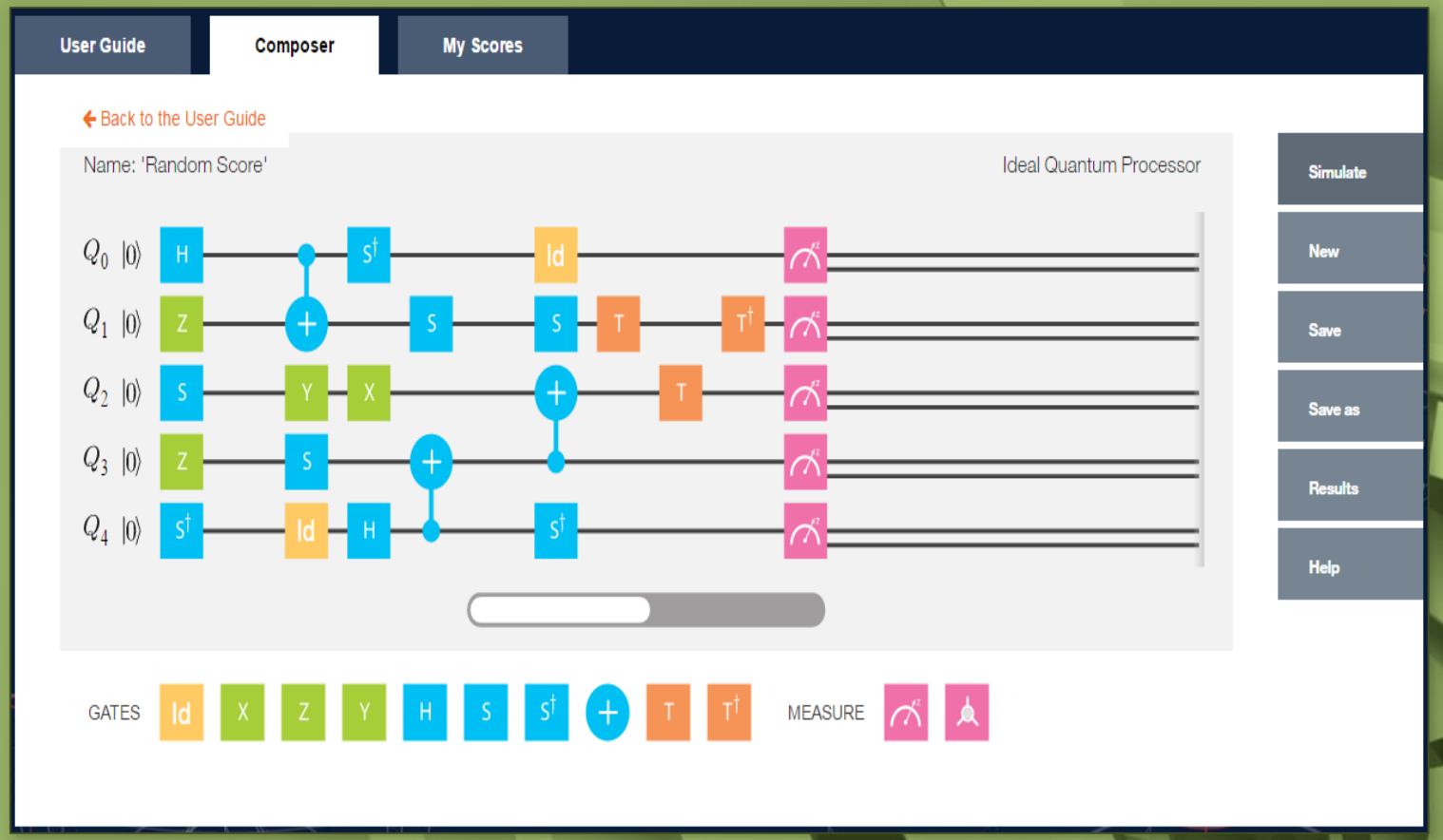
Tutti i possibili calcoli vengono effettuati in parallelo ma alla fine otteniamo un solo risultato

In base all'accuratezza dell'algoritmo il risultato ha una certa probabilità di essere quello desiderato

I gate quantistici

Modificano l'andamento delle equazioni di Schrödinger:

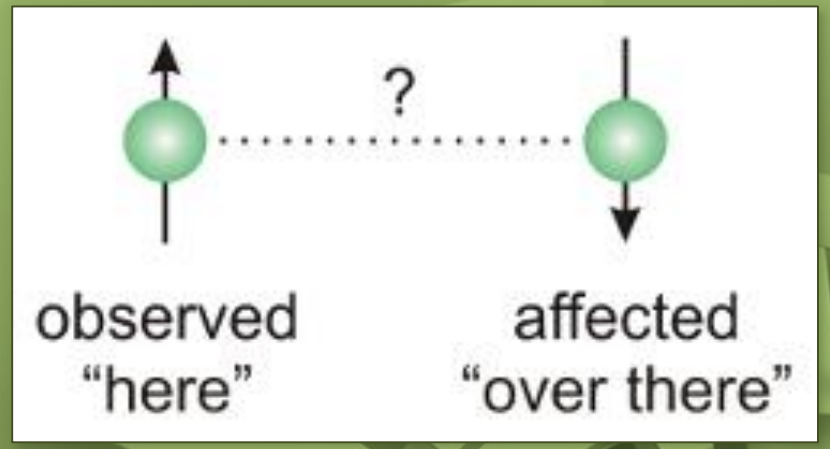
- Gate di Pauli
- Gate identità
- Gate di Hadamard
- Gate C-not
- Gate non «cliffordiani»
- Gate di Toffoli



L'entanglement

L'entanglement è un legame tra le particelle che trascende il tempo e lo spazio.

Ci permette di conoscere lo stato di uno dei *qubit* conoscendo quello dell'altro



Perché sia possibile il calcolo quantistico occorre che i qubit del sistema siano in «entanglement» tra loro e isolati dall'esterno

La decoerenza

Il più grande problema del calcolo quantistico è la decoerenza, ovvero la perdita di entanglement. È costituita da:

- *energy relaxation*
- *dephasing*

Quando il legame tra i *qubit* viene a mancare il calcolo perde valore

Rilevamento e correzione di errore

La decoerenza non costringe soltanto a ridurre i tempi di calcolo ma introduce un errore. Il problema può essere affrontato in diversi modi:

- *Laissez-faire*
- Correzione di errore: simmetrizzazione, sfruttamento di *codeword,* codici concatenati
- Computer a tolleranza di errore
- *Topological quantum computer*

C'è stato un forte miglioramento dei tempi di coerenza nel corso degli anni

I linguaggi di programmazione quantistici

Linguaggi imperativi: basati su C e C++, alcuni permettono di simulare i *qubit* anche in ambienti rumorosi grazie a specifiche librerie. Il primo è stato lo «pseudocodice di Knill»

- QCL, Q Language, qGCL, Lan Q

Linguaggi funzionali: attualmente i più studiati, alcuni prevedono semplicemente un controllo classico su dati quantistici

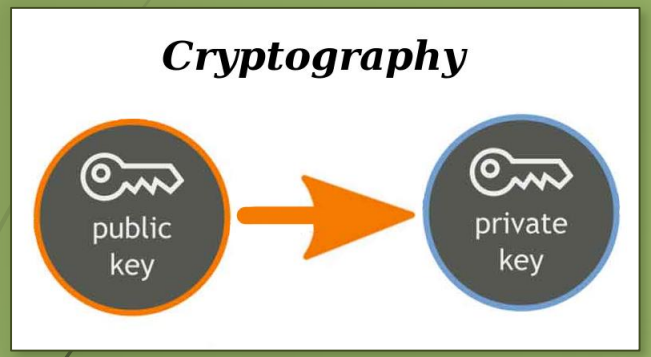
- QFC e QPL, QML, Quipper, Q Lambda Calculus

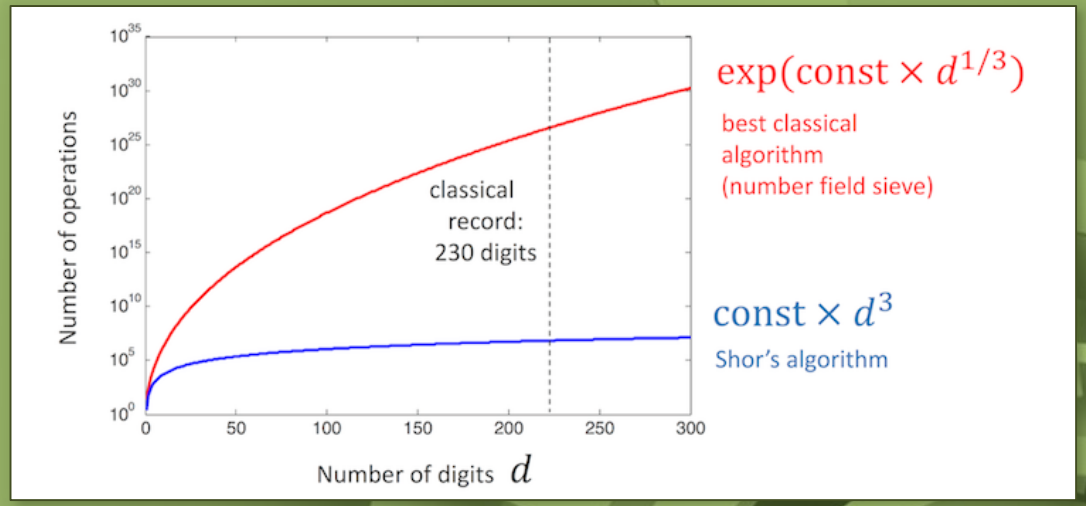
Algoritmo di Shor - Pseudocodice di Knill

FACTORIZE(N)

1 **if** N is even
2 **then return** $(2, N/2)$
3 **if** $N = q^b$ for prime $q \geq 3$ and $b \geq 2$
4 **then return** $(q, N/q)$
5 **repeat**
6 **repeat** choose $a \in \mathbb{Z}_N$, $a \geq 2$
7 $d \leftarrow \gcd(a, N)$
8 **if** $d > 1$
9 **then return** $(d, N/d)$
10 $r \leftarrow$ FIND-ORDER$_N(a)$
11 **until** no failure indicated and r is even
12 $d_+ \leftarrow \gcd(N, a^{r/2} + 1)$
13 **until** $d_+ < N$
14 $d_- \leftarrow \gcd(N, a^{r/2} - 1)$
15 **return** (d_+, d_-)
16 ▷ the algorithm guarantees $1 < d_+, d_- < N$

Perché usare il computer quantistico ?

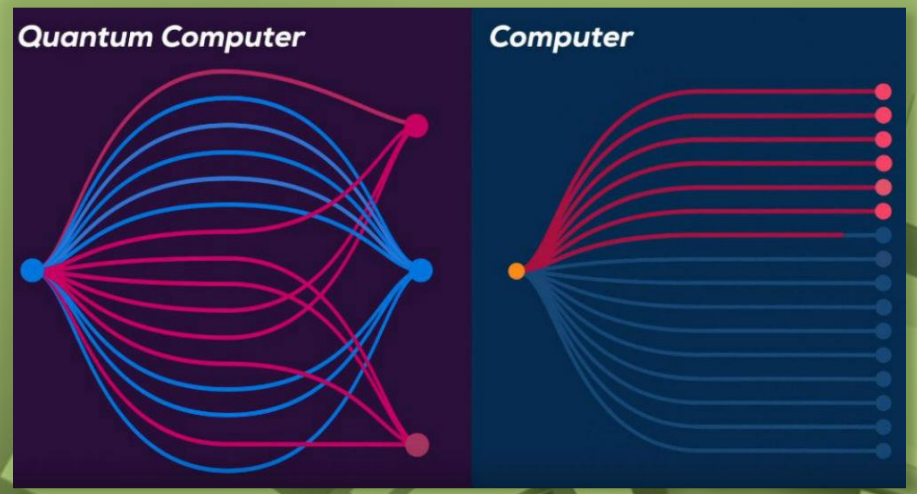




L'algoritmo quantistico di Shor permette di fattorizzare grandi numeri in tempi polinomiali

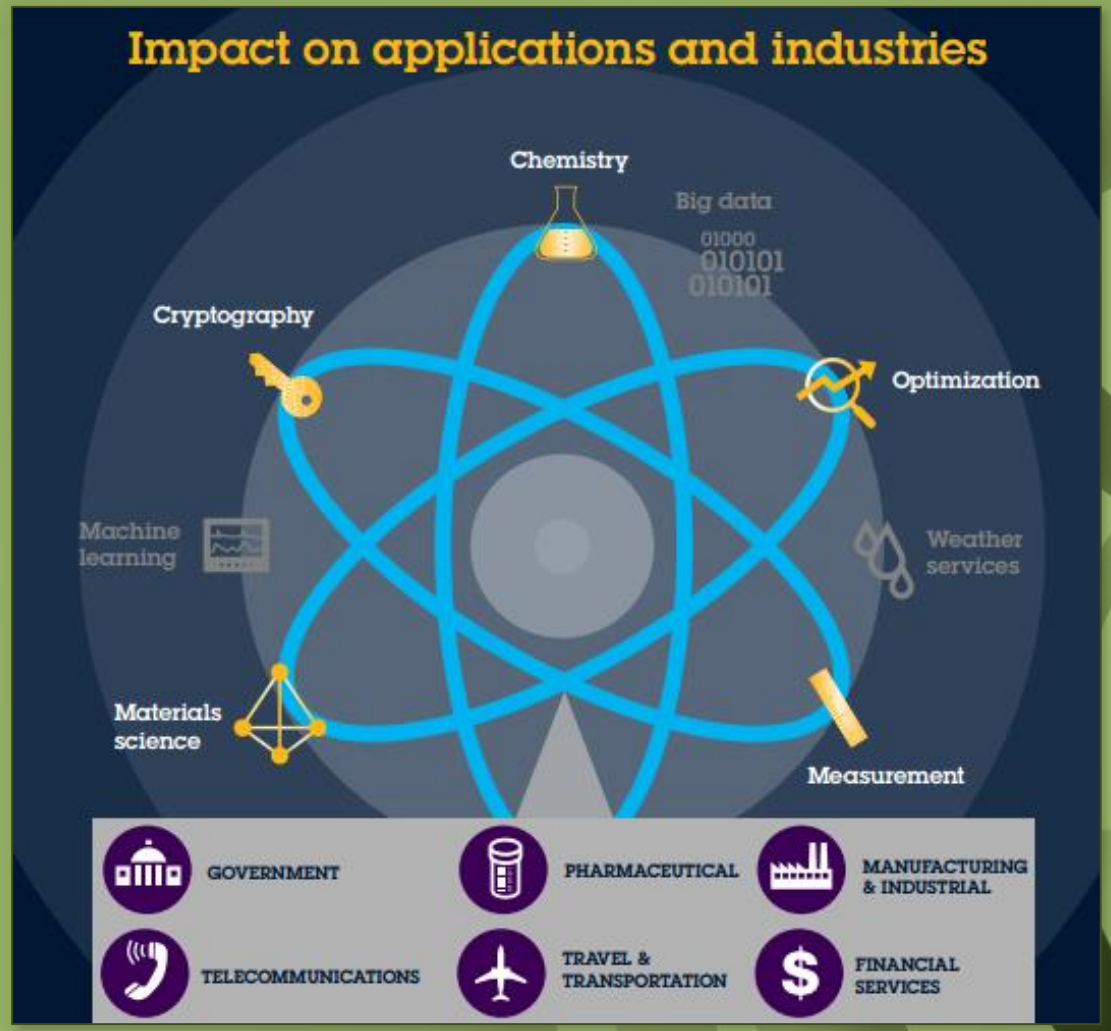
Perché usare il computer quantistico ?

Grazie all'algortimo di Grover i tempi di ricerca in un database sono ridotti da un tempo *O(n)* a uno dell'ordine $O(\sqrt{n})$



Una rete di dati che richiederebbe 2^{300} unità di calcolo può essere studiata con «solo» 300 *qubit* con la tecnica della topologia

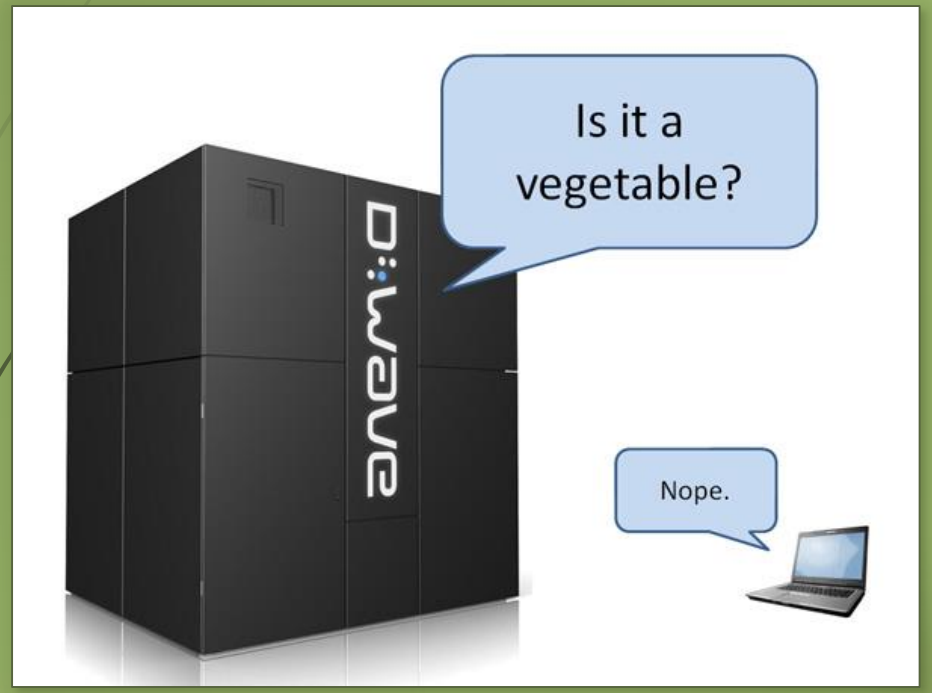
Perché usare il computer quantistico ?



I 3 tipi di computer quantistici

- Quantum Annealer
- Analog Quantum
- Universal Quantum

Quanto è quantistico un computer quantistico?



Non è ancora possibile sfruttare tutte le proprietà quantistiche in un calcolatore: è necessario l'appoggio a macchine classiche:

Computer quantistici come centri di calcolo

Ibridazioni a livello di processore

Grazie per l'attenzione!