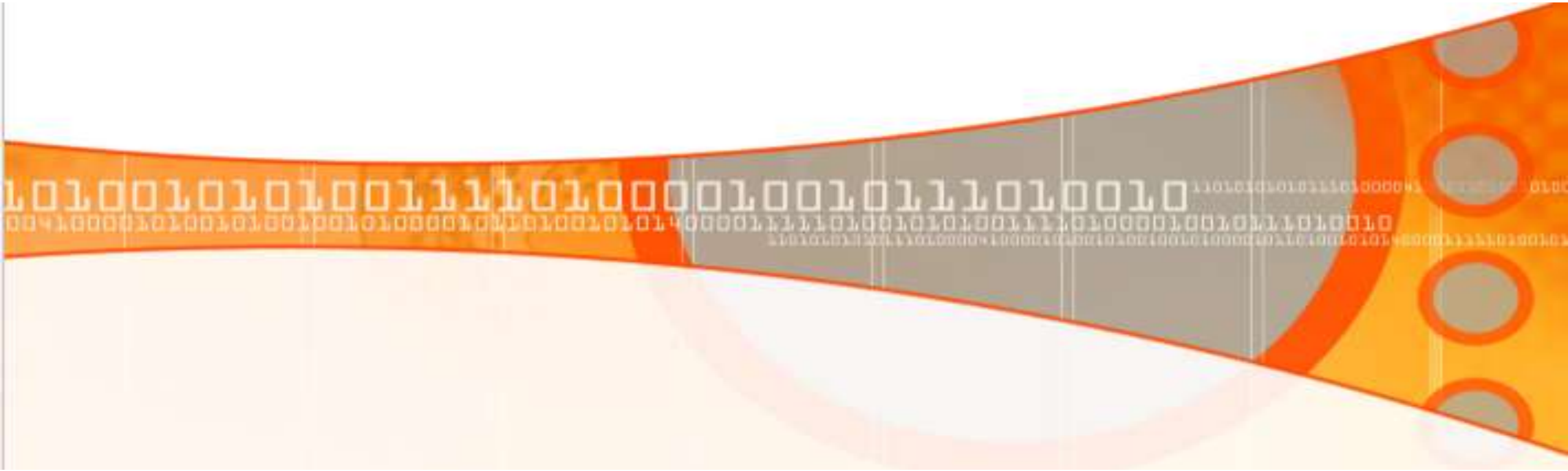
Seminar Topic

Quantum Computing

The Next Generation of Computing Devices?



Outline :

- History of Computer .
- What is Quantum Computer ?
- Why Quantum Computer ?
- How Quantum Computer works ?
- What can Quantum Computer do?
- Summary.

History of Computer :

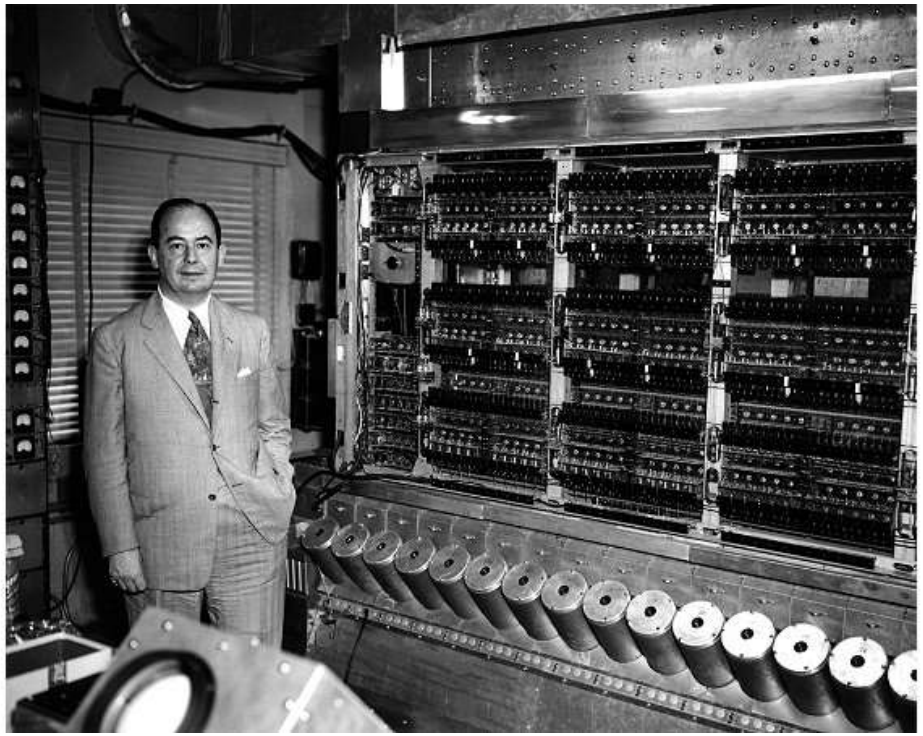
There are totally five Generations of Computer till now. Initially Generation term is used to distinguish between varying hardware technology. But nowadays include Hardware and Software.

Following are five main generation of computers :

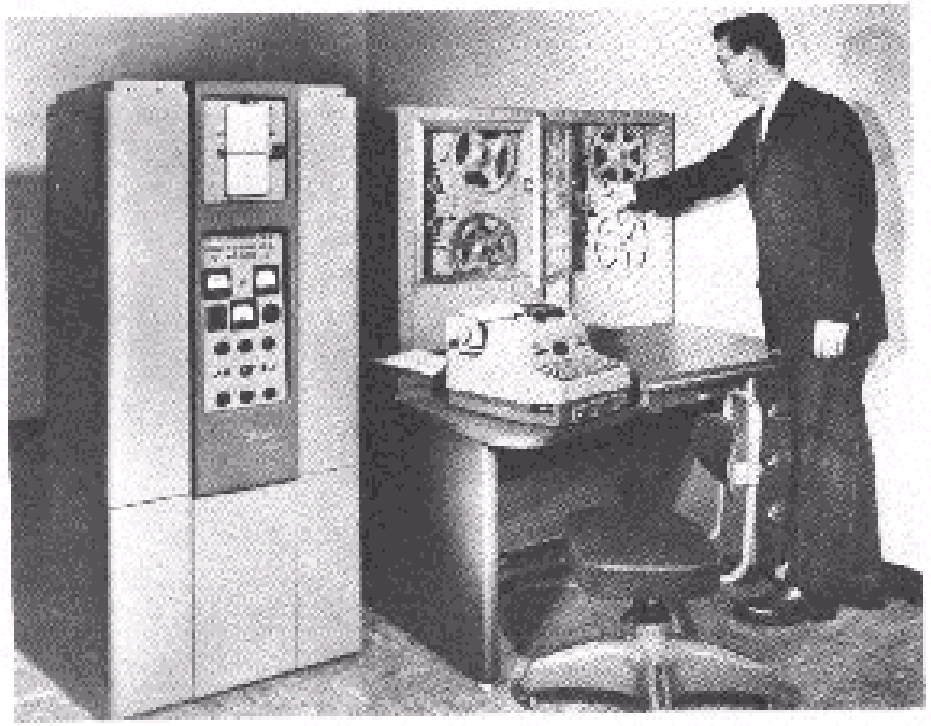
S.N	Generation	Generation-period	Description
1.	First	1946-1959	Vacuum tube based
2.	Second	1959-1965	Transistor based
3.	Third	1965-1971	Integrated Circuit based
4.	Fourth	1971-1980	VLSI microprocessor based
5.	Fifth	1980-present	ULSI microprocessor based

Computers Generation :

First Generation



Second Generation

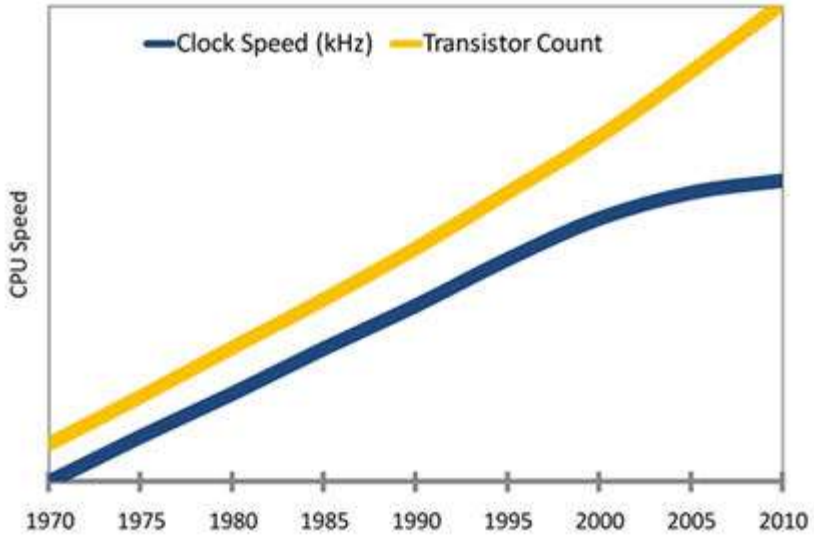


Computer Generation :

Third Generation

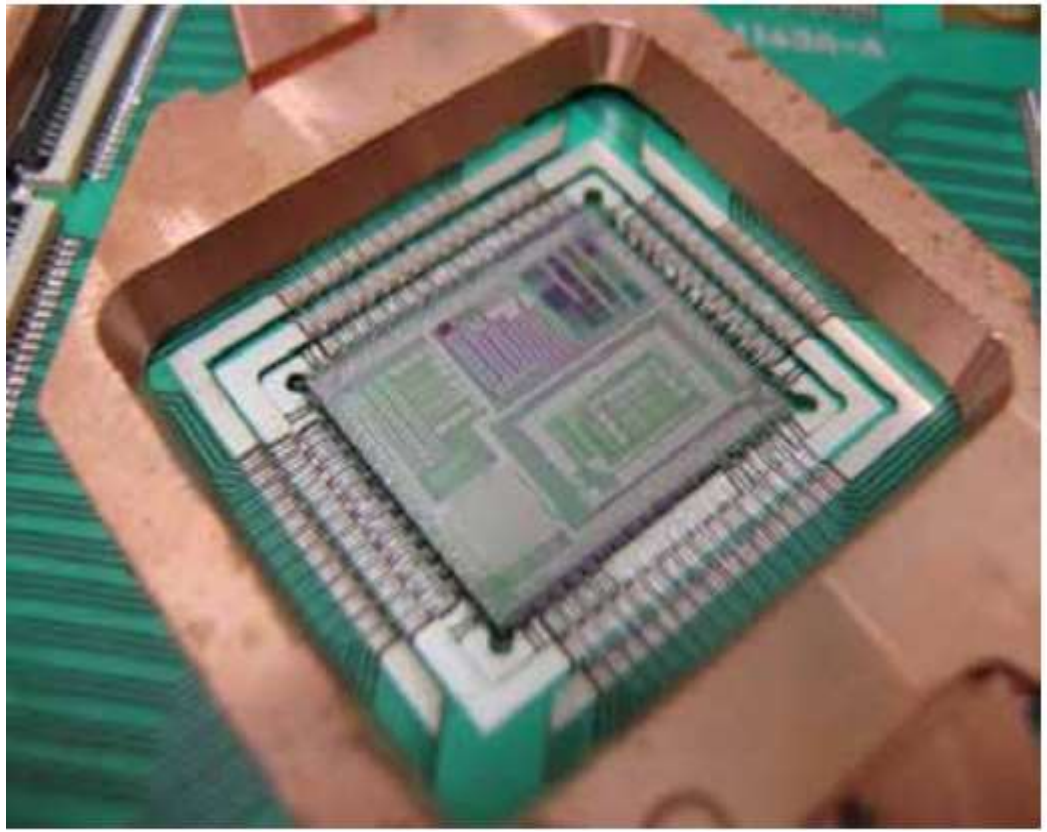
Fifth Generation

Fourth Generation



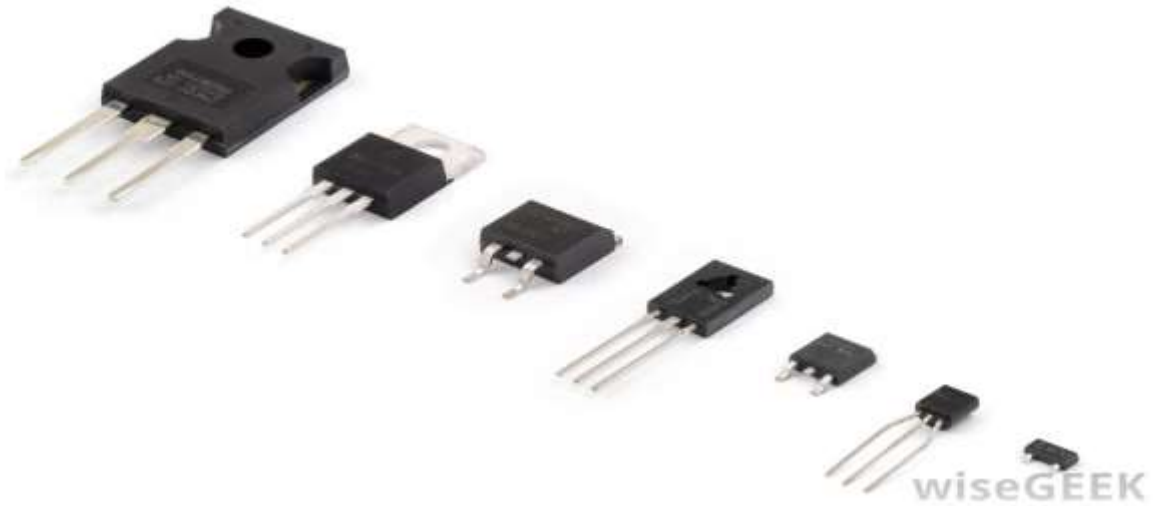
Quantum Computer :

A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.



Classical Computer :

A computer that uses voltages flowing through circuits and gates, which use principle of Digital electronics to perform operation .



Nobel Prize in Quantum Computing

David Jeffrey Wineland

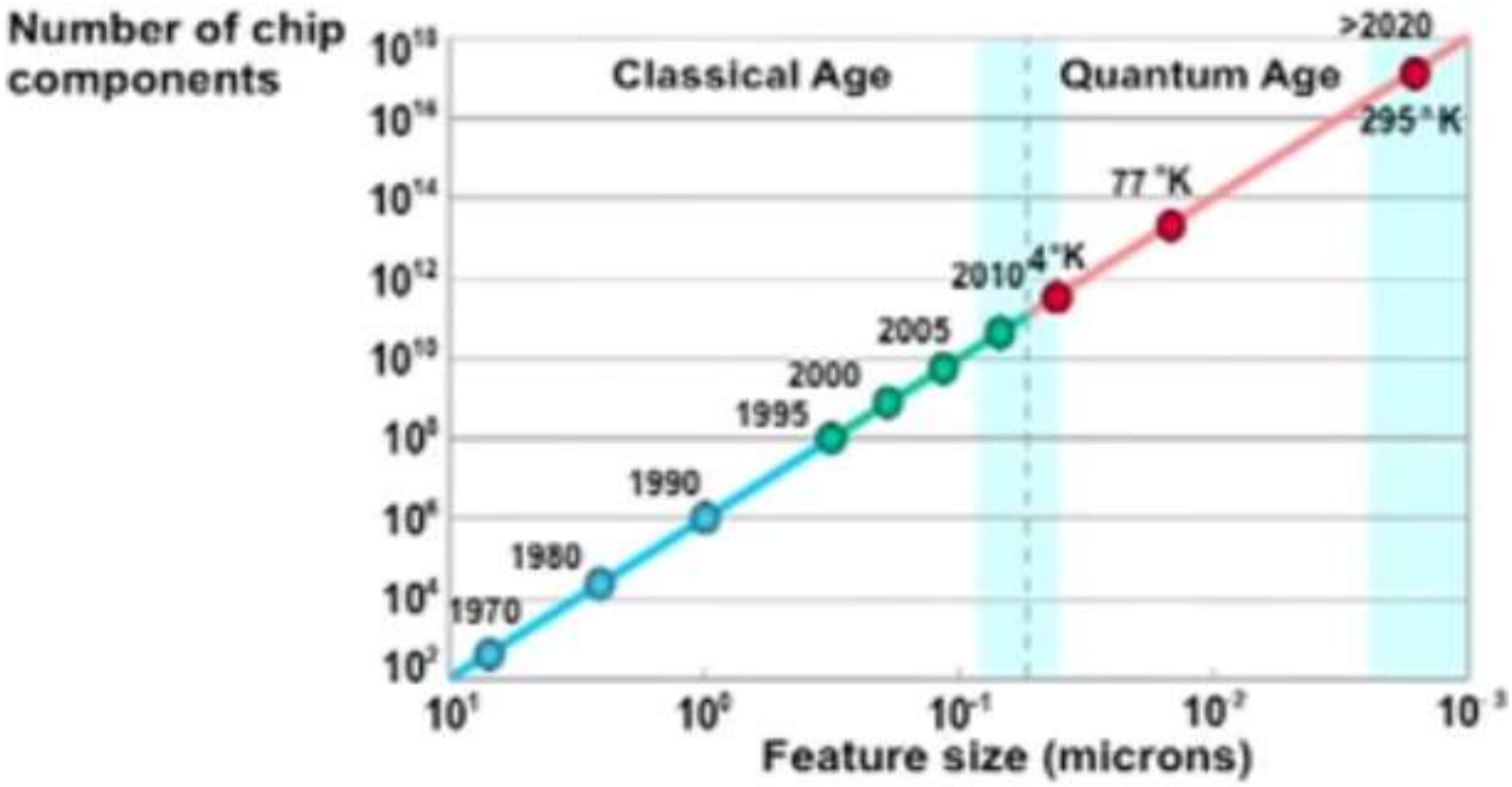
Serge Haroche

David J Wineland And Serge Haroche were Awarded with the Nobel Prize for their work regarding measurement and manipulation of individual Quantum Systems in 2012 .

The author

Dr. Gordon E. Moore is one of the new breed of electronic engineers, schooled in the physical sciences rather than in electronics. He earned a B.S. degree in chemistry from the University of California and a Ph.D degree in physical chemistry from the California Institute of Technology. He was one of the founders of Fairchild Semiconductor and has been director of the research and development laboratories since 1959.

Moore's Law to the Atomic-scale



Gordon Moore :
Co-founder of Intel

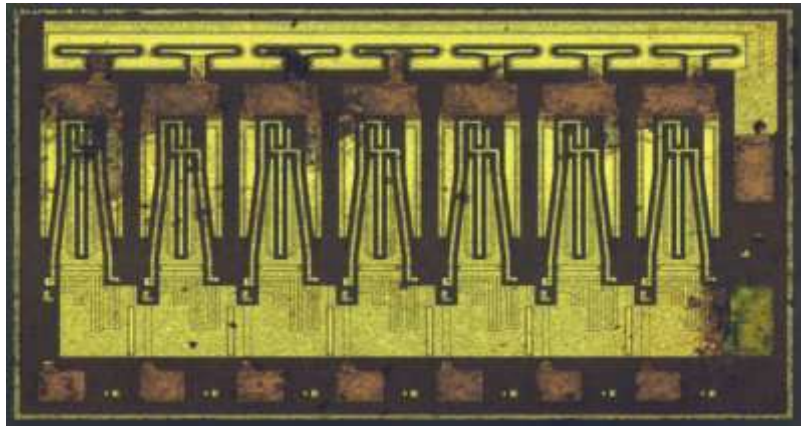
No of transistor double after 18 month or 2 year.

Classical bits :

In the classical computer every thing is decoded in binary number and these two binary bits are called Classical bits. Classical computer use these bits as combination and perform the desired result.

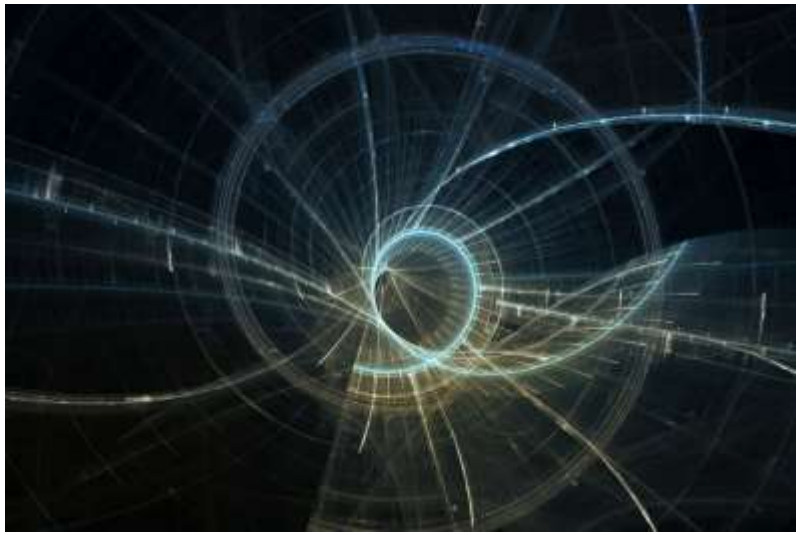
We know that a single chip made of large no of transistor and all this transistor must work reliably so that our computer/mobile/machine(based on binary bit) can work properly.

Transistor



Quantum bits :

Quantum Physics (Quantum theory) is fundamental branch of Physics which describe physical phenomena at atomic or sub-atomic scale. Quantum mechanics provides an extremely accurate description of the behaviour of photons , electrons and other atomic and molecular-scale objects or sometime it is called ***reality***.



Quantum Physics

Schrodinger Cat Experiment

Essential Elements of Quantum Physics

- **Particles are waves, and vice versa**

  Quantum physics tells us that every object in the universe has both particle like and wave-like properties.

- **Quantum states are discrete**

  The “quantum” in quantum physics refers to the fact that everything in quantum physics comes in discrete amounts.

- **Well defined Spin**

  All the Quantum Element (electron, proton, neutron)have a well defined spin .Actually they have momentum and Orientation in space.

- **Measurement determines reality**

  After a measurement is made, the state of the particle is absolutely determined.

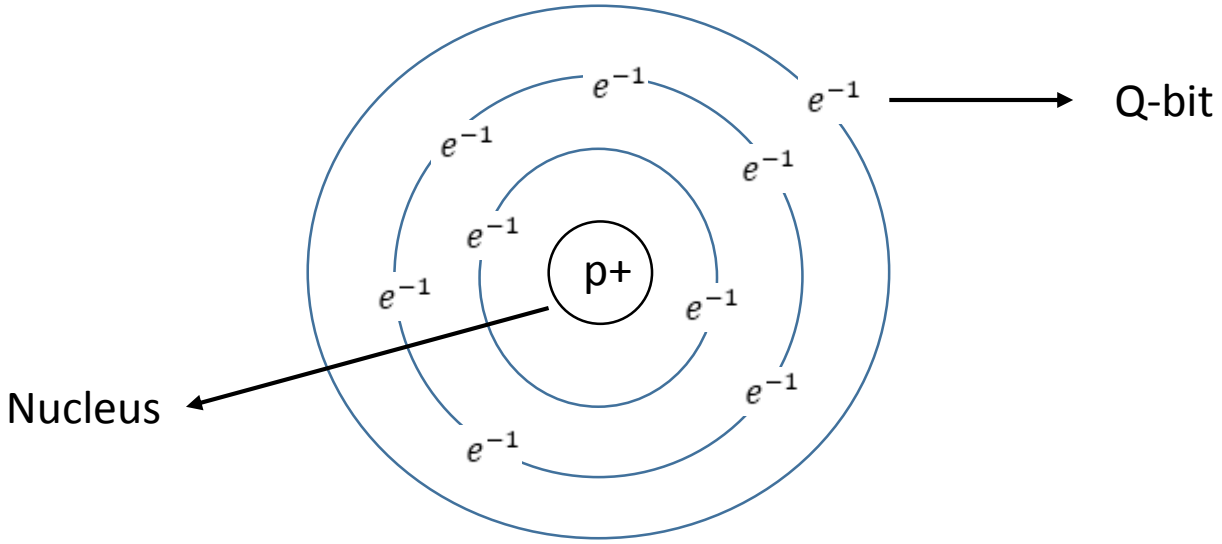
- **Quantum physics is not magic**

  The bedrock principles of physics are still intact: energy is still conserved, entropy still increases, nothing can move faster than the speed of light.

Quantum bits :

As we know that to perform operation we must need binary bits or something equivalent to binary bits.

By using Q-bits we can do similar operation as classical computer. Quantum computer use Quantum object to perform operation. We can either can use a electron/proton as Q-bit. But it is very difficult to do operation with proton because proton reside in nucleus. Electron of any material can be use as Q-bit .



Quantum bits :

=

1

Digital information : 1

Quantum bits :

=

0

Digital information : 0

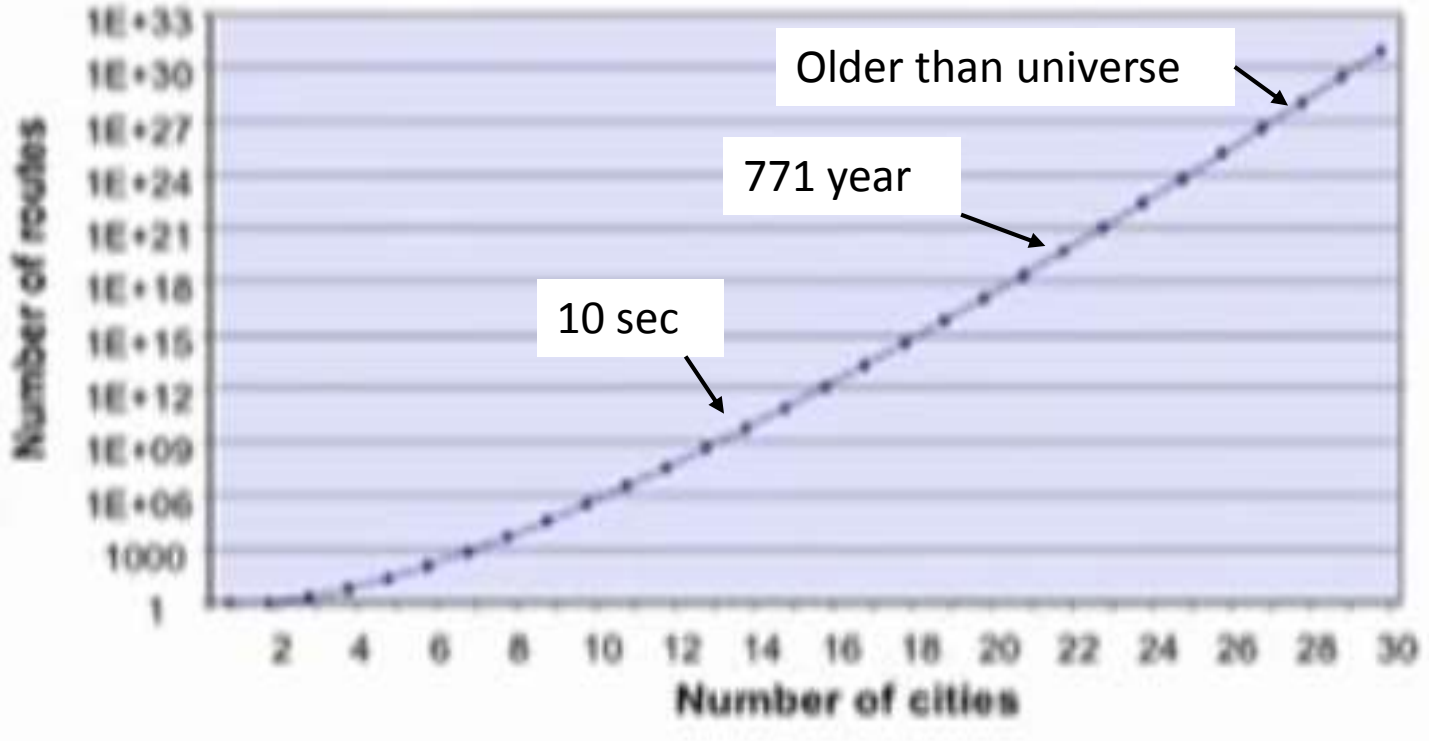
In this situation it can be either “0” or “1 ”. To predicate this information we use Quantum formula that is :

$$P(\uparrow)=\cos^2(\theta/2)$$

Why Quantum Computer

Problem: A salesman has to travel to many cities and want to work out the shortest possible route.

Difficult problem : travelling salesman



Cities	routes	time taken
14	10^{11}	10 sec
22	10^{19}	771 year
28	10^{30}	----------

Lets assume our classical computer speed is 4.4 GHz (intel i-7) (10^{10}operation/sec)

How Quantum Computer works

A Quantum computer use the principle of Quantum physics. Like as classical computer's binary bits, in quantum Computer we use Q-bits. So now to understand that how Quantum computer works we need to manipulate these Q-bits.

Quantum computers promise to do computation more powerfully than classical computers due to the ability of a quantum computer to be in some states that have no equivalence in a classical computer such as a superposition of values and/or an entanglement between some particles of a quantum system.

Main building blocks of Quantum computer is :

- Q-bits
- Superposition
- Entanglement

Superposition

Superposition is a principle of Quantum physics that describe a challenging concept about the nature and behaviour of matter at atomic level. Principle of super-position states that while we don't know what is the state of any Q-bit, actually it is all the possible state simultaneously, as long as we don't measure it.

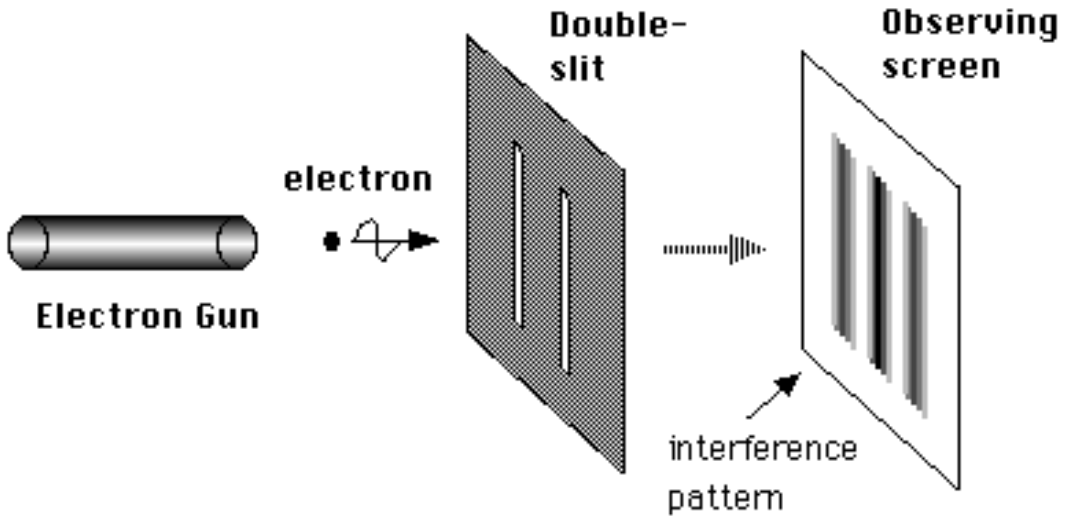
Think of a qubit as an electron in a magnetic field. The electron's spin may be either in alignment with the field, which is known as a *spin-up* state, or opposite to the field, which is known as a *spin-down* state. Changing the electron's spin from one state to another is achieved by using a pulse of energy, such as from a laser.

But what if give half of the energy to total energy to change the spin of electron ?

Superposition

By using this property we can do parallel processing , Classical computers today, even so called parallel processors, truly they still do one task at a time. But their time to do one task is so small that we can't feel it and its seems as parallel processing.

We can proof Superposition theorem with Double slit Experiment / Schrodinger's cat Experiment

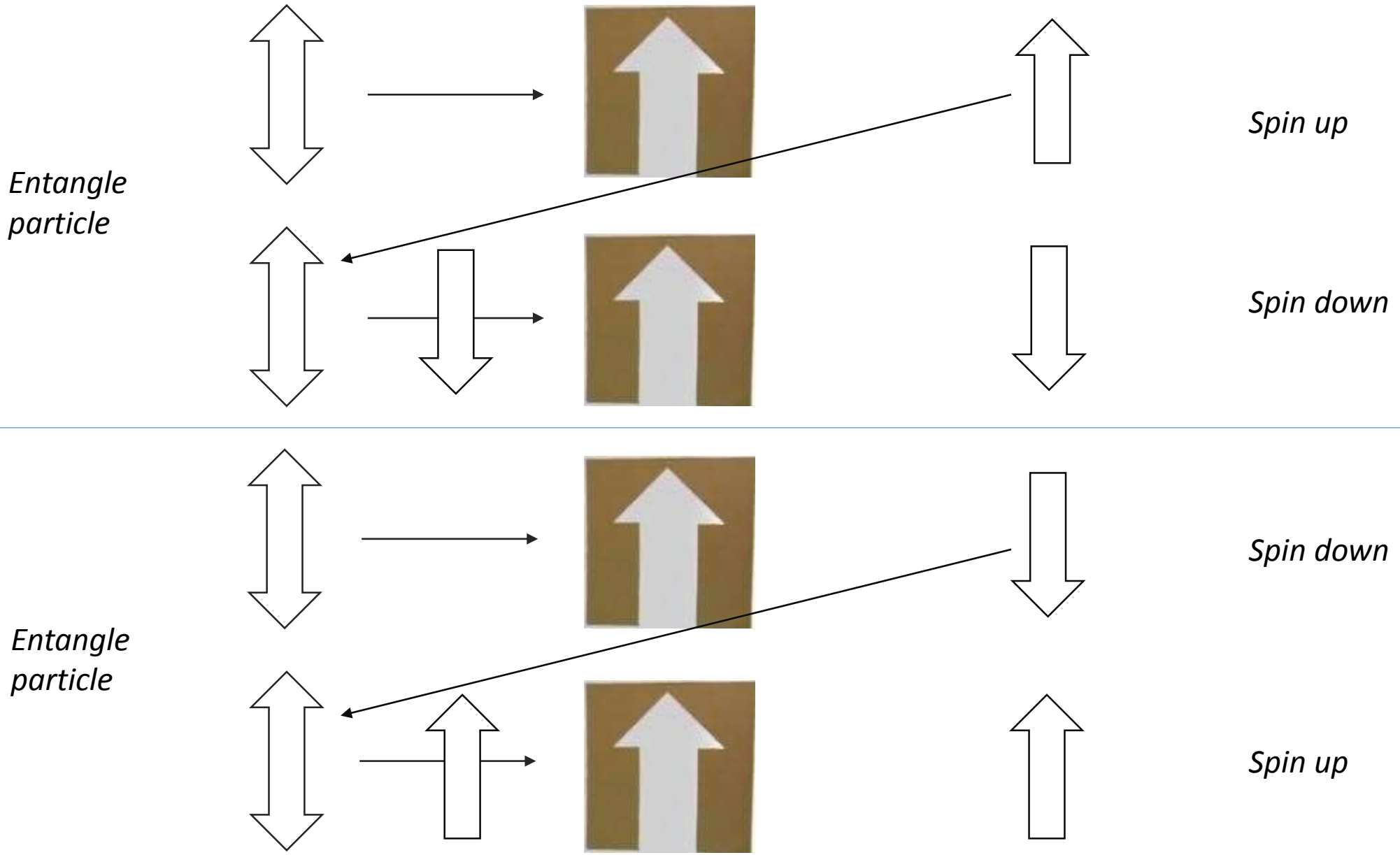


Entanglement

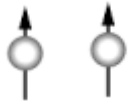
Particles (such as photons, electrons, or q-bits) that have interacted at some point retain a type of connection and can be entangled with each other in pairs, in process known as *correlation*. Knowing the spin state of one entangled particle up or down allows one to know that the spin of its mate is in the opposite direction and this is known as Entanglement.

Quantum entanglement allows qubits that are separated by incredible distances to interact with each other instantaneously (not limited to the speed of light). Taken together, quantum superposition and entanglement create an enormously enhanced computing power.

Entanglement – spooky reaction



Power of Q-bits

No of Q-bits	Classical possibilities	power
	0 or 1	2
	00,01,10,11	4
	000,001,010,011 100,101,110,111	8
N	----------	2^n

A 100 Q-bit quantum computer is more power full than a super computer….

A Quantum computer with 500 Q-bits is more power full than all the computer of world connect together.

Representation of Q-bits/states

States can be represented via either the vector/matrix notation, or Dirac Notation. Dirac Notation is more useful for describing the quantum states and the evolution of the state of the system

Dirac notation :

1. |ψ> : denotes a column vector that represents a quantum state.

2. <ψ| : denotes a row vector that represents the dual of 1 , i.e. the complex conjugate transpose

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

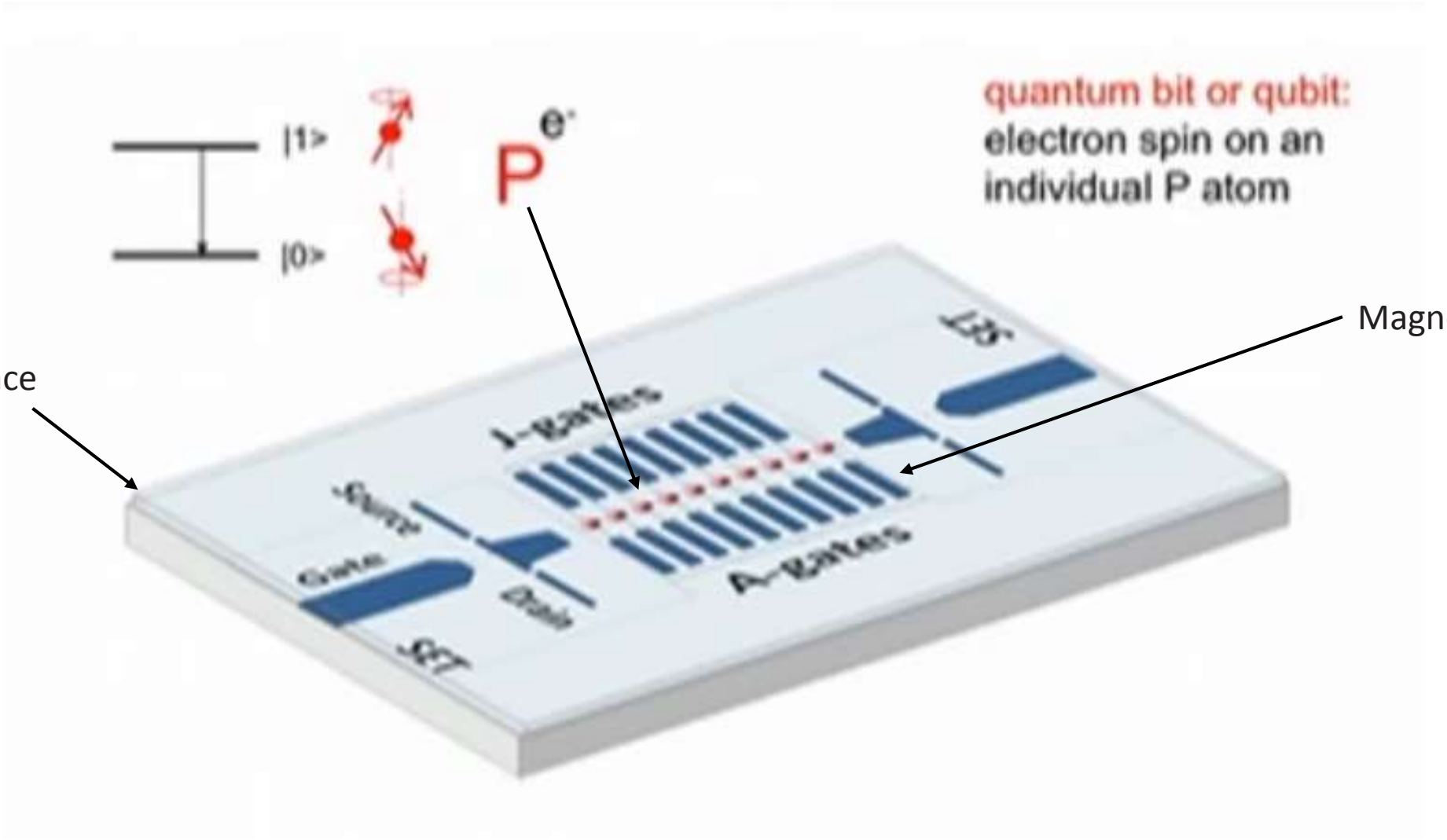
Quantum Gates

Quantum Gates are same as classical Gates (AND,OR,NOT,XOR. etc.) but with a little change that is we use Quantum vector/matrix instead of classical transistor. although Quantum gates do the same functional operation.

Quantum gates used during the computation must follow the fundamental laws of quantum physics. To satisfy this condition , using any matrix U as a quantum gate, it must be unitary.

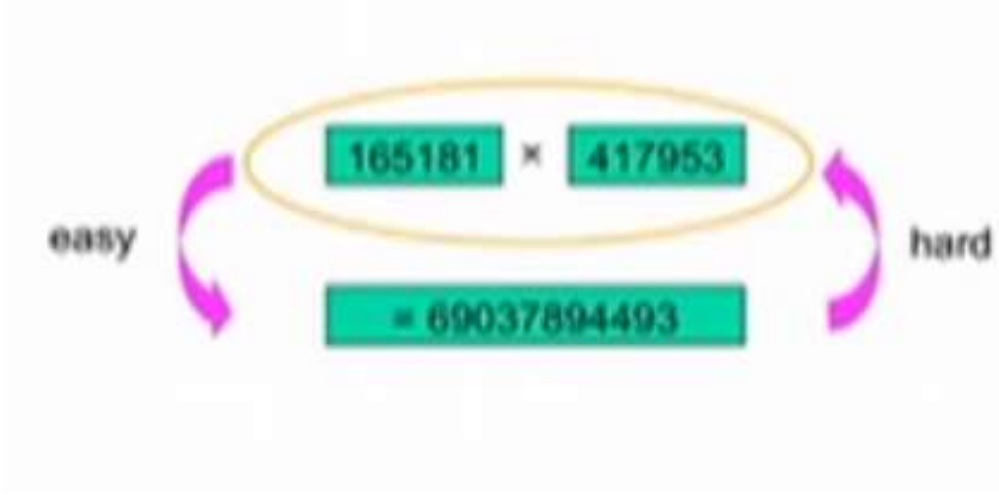
2 × 2 unitary matrix for $NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. : $U^{-1} = U^{\dagger}$ and $UU^{\dagger} = I$,

Quantum Architecture



What can Quantum Computer do ?

Data Encryption



RSA= Public-key encryption protocol

Current RSA-768 take 3 year

Ron Rivest , Adi Shamir , Leonard Adleman

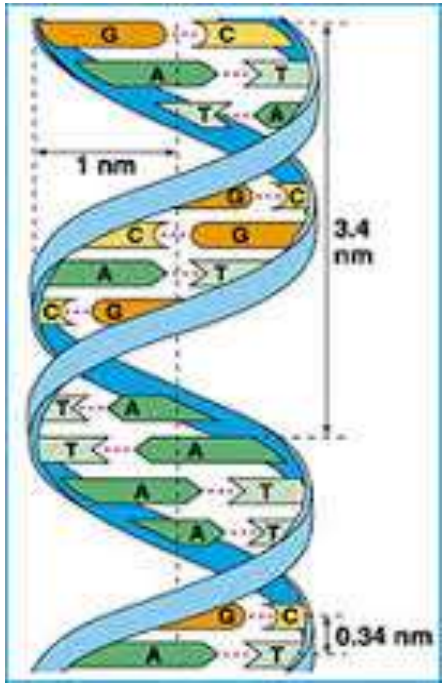
But Quantum computer can solve in minutes

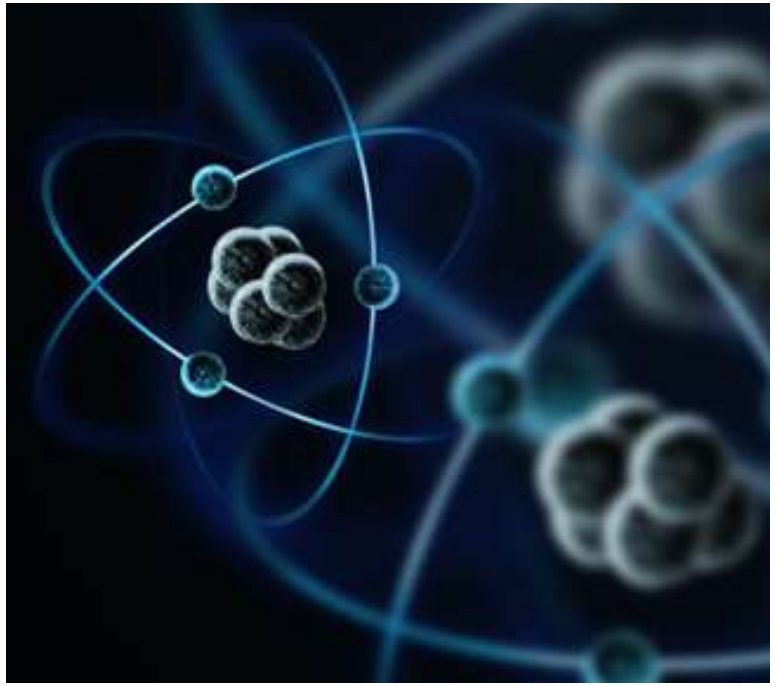
1024 bit number will take 3000 year

What can Quantum Computer do?

Application :

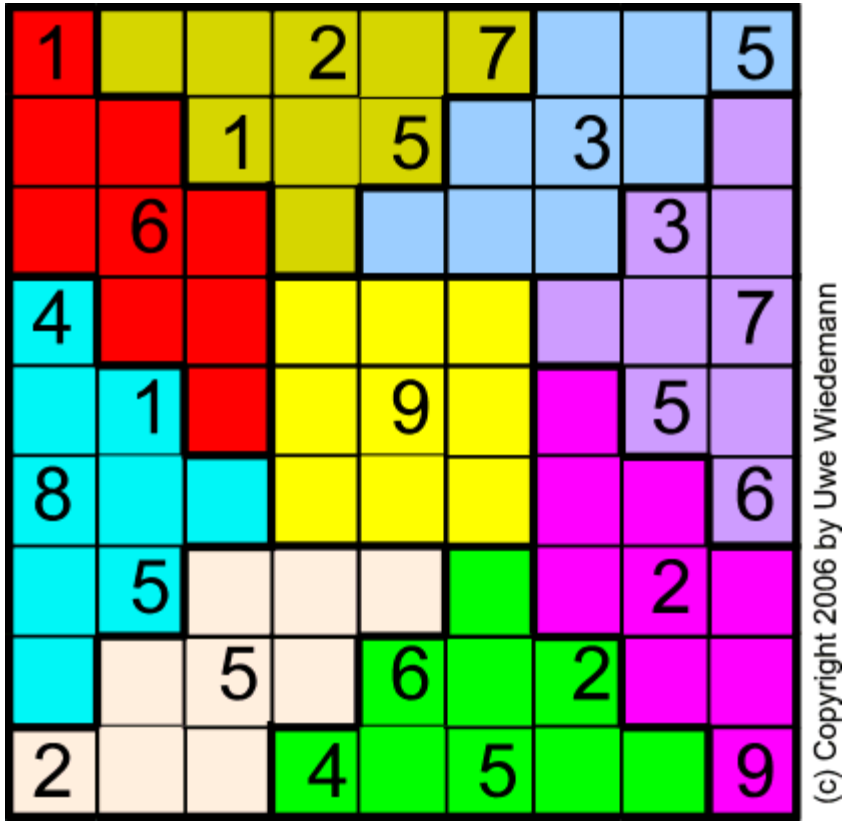
- ✓ Factorisation (data security)
- ✓ Physical modelling (climate , economic , engineering)
- ✓ Simulation (chemistry ,material)
- ✓ Data bases searching (bioinformatics)





Abacus of Quantum computer

Canadian start up company D-wave demonstrate a 30 Q-bit Quantum computer . The Computer solve the Sudoku puzzle and other pattern matching problems.

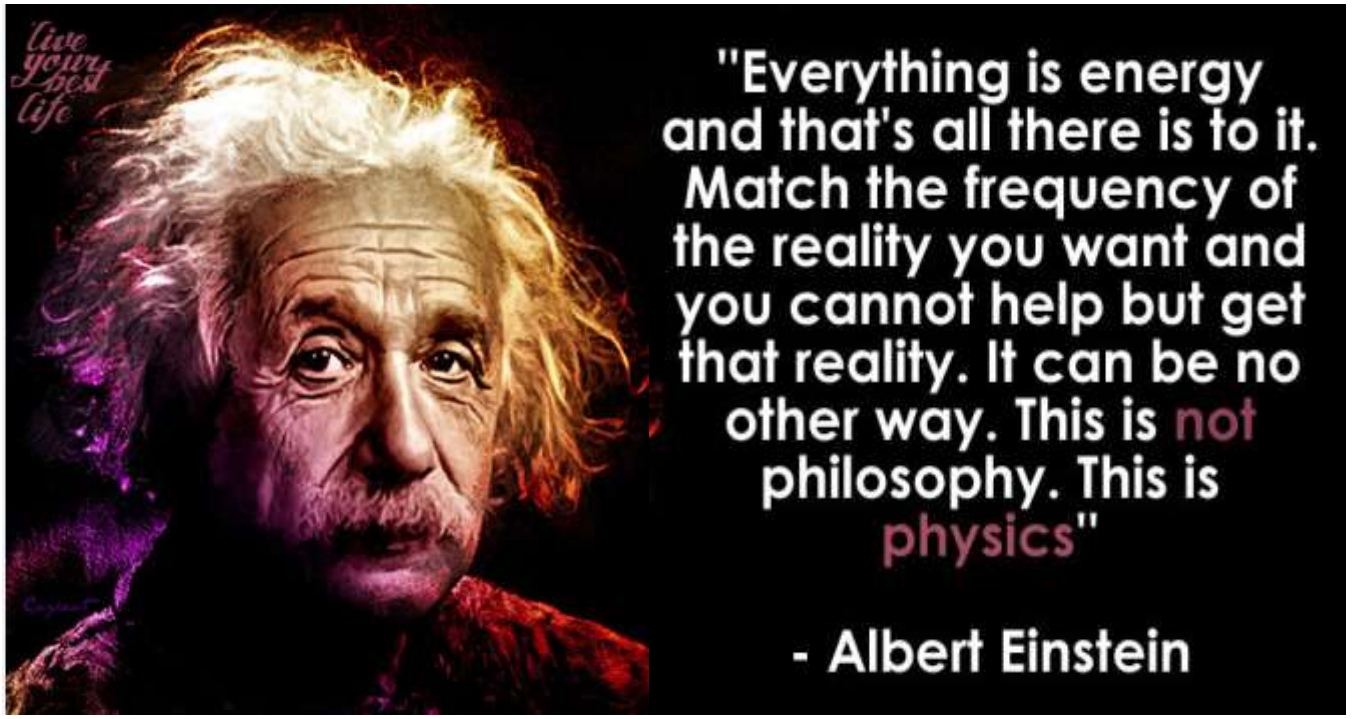


D-wave

Summary :

- A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.
- David J Wineland And Serge Haroche were Awarded with the Nobel Prize for their work regarding measurement and manipulation of individual Quantum Systems in 2012.
- Quantum computer use Q-bits to do operation. Electron, proton can be use as Q-bits.
- Superposition and Entanglement are main building block of Quantum computing and these property speed up Quantum computer exponentially.
- Every time we add a Q-bit we double the computation power of Quantum computer .

Quantum Physics



If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet.

(Niels Bohr)