Introduction to Quantum Computing

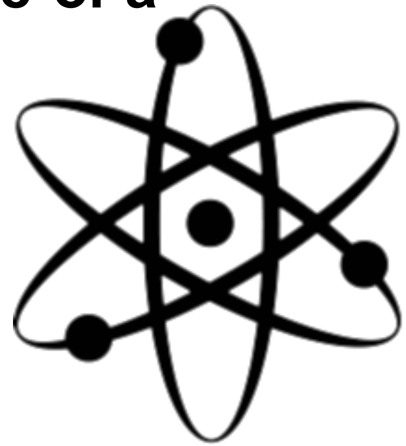
Adel SOHBI

Seoul Artificial Intelligence Meetup

25th June 2017

Quantum Information

- **Quantum Theory:** best knwon theory to describe **properties of microscopic sytems**.
- **Quantum Information:** generalization of **classical information theory** to the quantum world.
- How to use **information** stored in the **state of a quantum system**?
- Todays's aim: **Quantum Computing**.

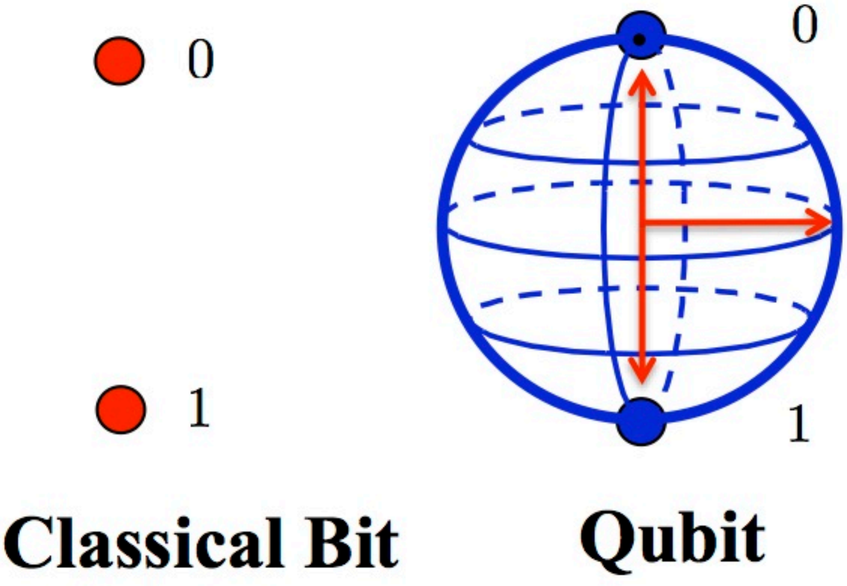


What is a bit?

- The word « bit » stands for **Binary Digit**: 0 or 1.
- Choice between **two exclusive classes** (ex: yes/no, white/black, dead/alive, star/car, head/tails, etc…).
- A bit **encodes** the **distinction** between two possibilities.

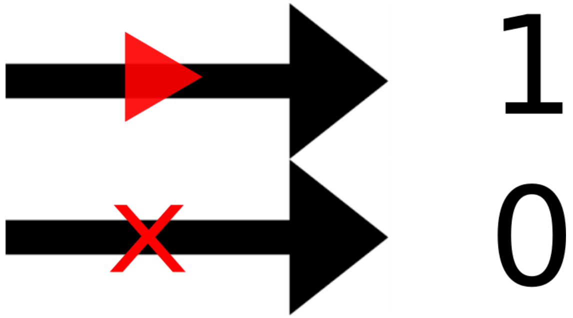
The Quantum bit: qubit

- Impossibility to have two distinct classes using a quantum ressource.
- Important quantum properties: **superposition**, **wave function collapse** (by "observation").



Classical Computer

- **Physical device** that manipulates **information** in **binary** form.

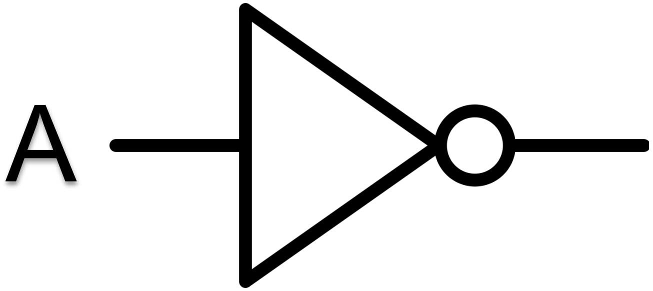


- Uses **algorithms** to treat **input** data and gives **output**.

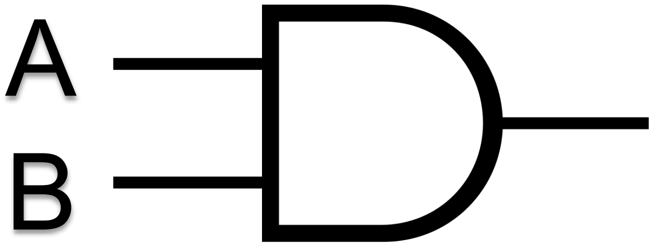
INPUT
OUTPUT

Classical Logic Gate

- Electronic device implementing a Boolean function.



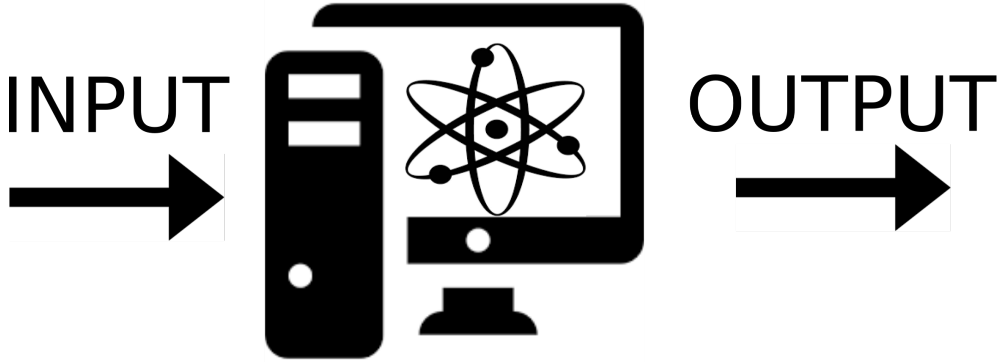
INPUT	OUTPUT
A	NOT A
0	1
1	0



INPUT		OUTPUT
A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Quantum Computer

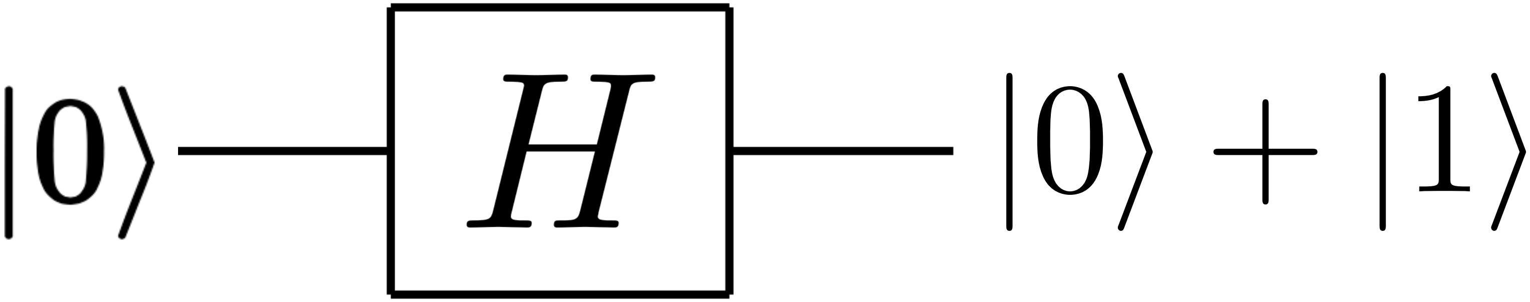
- Manipulate qubits instead of bits.
- Quantum Logic Gates.
- Physical implementation has many different candidates.



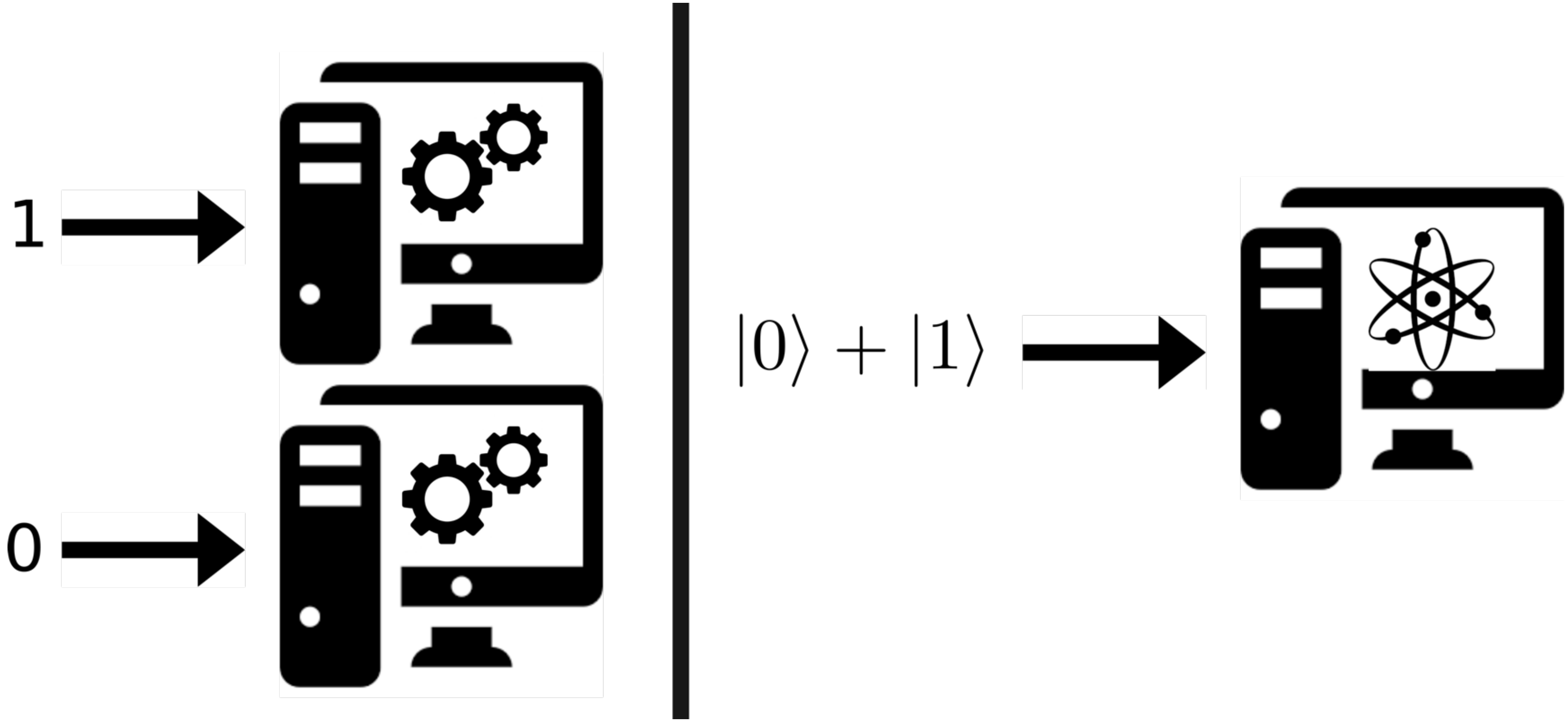
Quantum Logic Gate

- Manipulation of qubits with **Quantum Gates**.

- **Hadamard gate**:



Quantum Computer vs Classical Computers: Naive Approach



1

0

$|0\rangle + |1\rangle$

Quantum Algorithm: Searching in a Database

- Find X such that f(X) = 42:

X	f(X)
0	12
1	4
2	340
3	2
4	42
5	93
6	77

Classical Algorithm:
Exhaustive Search

$$O(N)$$

1 000 000 entries
1 000 000 steps

Quantum Algorithm:
Grover's Algorithm

$$O(\sqrt{N})$$

1 000 000 entries
1 000 steps

Quantum Algorithm: Prime factorization

- 70 = 2 × 5 × 7
  48 279 = 3 × 7 × 11^2 × 19
  56 153 = 233 × 241

- **RSA-100** = 1 522 605 027 922 533 360 535 618 378 132 637 429 718 068 114 961 380 688 657 908 494 580 122 963 258 952 897 654 000 350 692 006 139
  = 37 975 227 936 943 673 922 808 872 755 445 627 854 565 536 638 199
  × 40 094 690 950 920 881 030 683 735 292 761 468 389 214 899 724 061

- Classical Algorithm: **exponential time** (General number field sieve**).**

- Quantum Algorithm: **polynomial time** (Shor's algorithm**).**

Quick Summary

- The fundamental **difference** between:
  - A bit and a qubit.
  - A classical computer and a quantum computer.

- Two examples of **quantum algorithm**:
  - Searching in a Database.
  - Prime Factorization.

- **Quantum Information** includes also: Machine Learning, Communication, Cryptography, Random Number Generator, etc…