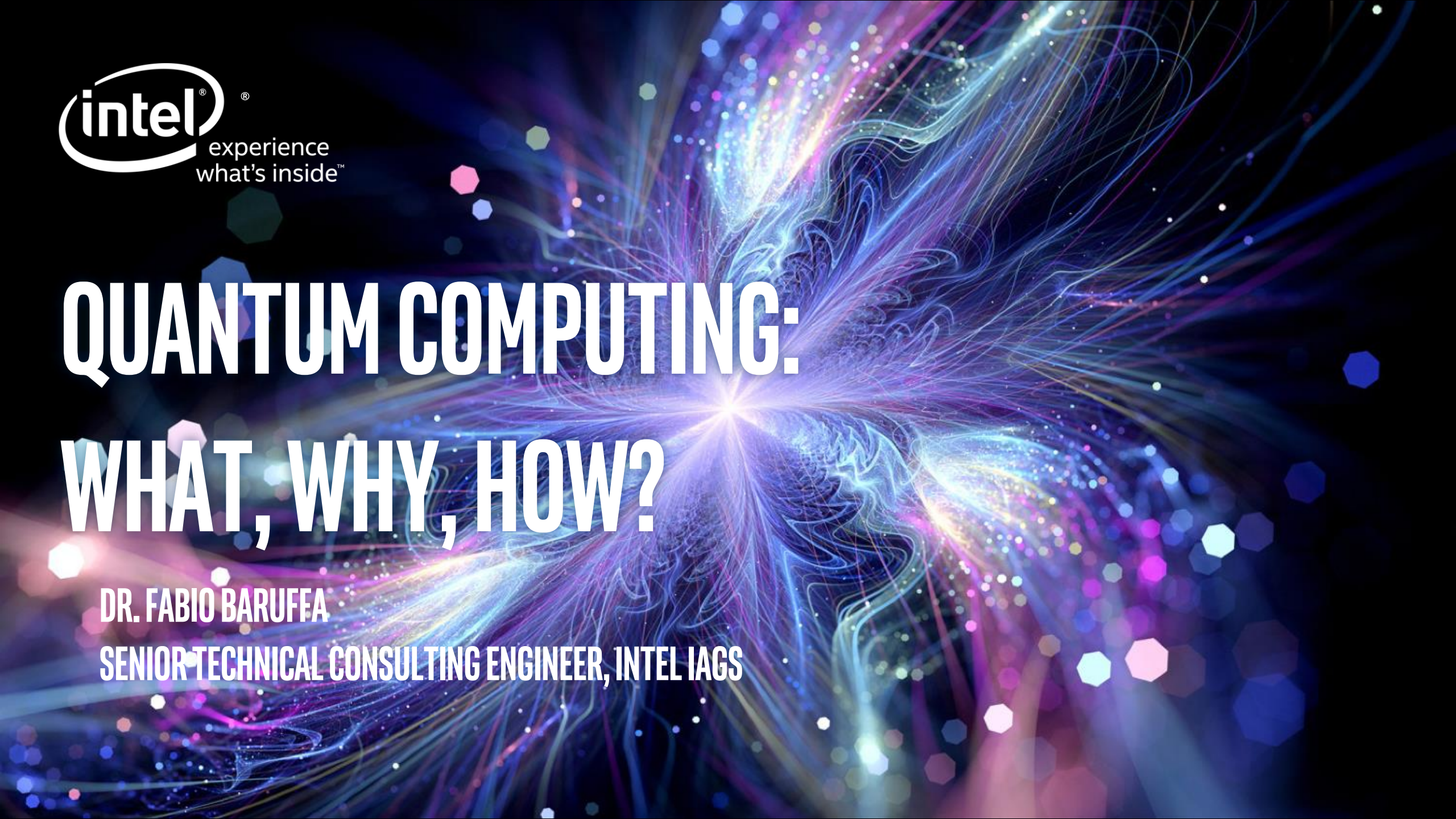


QUANTUM COMPUTING: WHAT, WHY, HOW?

DR. FABIO BARUFFA
SENIOR TECHNICAL CONSULTING ENGINEER, INTEL IAGS

AGENDA

- **What is Quantum Computing about?**
  - Quantum Mechanics key concepts
  - Basic building blocks of a quantum computer
- **Why Quantum Computation?**
  - Challenging the world on complex prolems
  - Quantum Computing system
- **How do we create and operate a Quantum Computer?**
  - DiVincenzo‘s criteria for constructing a quantum computer
  - Quantum algorithm simulations

WHAT IS QUANTUM COMPUTING?

Quantum Mechanical Computers

By Richard P. Feynman

Introduction

This work is a part of an effort to analyze the physical limitations of computers due to the laws of physics. For example, Bennett[1] has made a careful study of the free energy dissipation that must accompany computation. He found it to be virtually zero. He suggested to me the question of the limitations due to quantum mechanics and the uncertainty principle. I have found that, aside from the obvious limitation to size if the working parts are to be made of atoms, there is no fundamental limit from these sources such. We see we really have two more logical primitives, FAN OUT when two wires are connected to one, and EXCHANGE, when wires are crossed. In the usual computer the NOT and NAND primitives are implemented by transistors, possibly as in Fig. 2.

What is the minimum free energy that must be expended to operate an ideal computer made of such primitives? Since, for example, when the AND operates the output line, c' is being determined to be one of two values no matter what it was before the entropy change is $ln(2)$ units. This represents a heat generation of $kT\,ln(2)$ at temperature T. For

could be stored in an inductance, or other reactive element.

However, it is apparently very difficult to make inductive elements on silicon wafers with present techniques. Even Nature, in her DNA copying machine, dissipates about 100 kT per bit copied. Being, at present, so very far from this $kT\,ln(2)$ figure, it seems ridiculous to argue that even this is too high and the minimum is really essentially zero. But, we are going to be even more ridiculous later and consider bits written on one atom instead of the present 10^{11} atoms. Such nonsense is very entertaining to professors like me. I hope

June 1986

QUANTUM MECHANICS EFFECTS

R. Feynman, Simulating Physics with Computers, 1982

- *"...nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical..."*
- *"If you think you understand quantum mechanics, you don't understand quantum mechanics."*
- *"I think I can safely say that nobody understands quantum mechanics."*

QUANTUM SUPERPOSITION

A quantum system can exists in all the possible state, *until is measured*!

Classical Physics

Heads or Tails

Quantum Physics

Heads and Tails

Classical bit: **|0>** or **|1>**

Quantum bits: **a|0> +b|1>**,

$|a|^2$ probability to be in the state |0>

Fragility

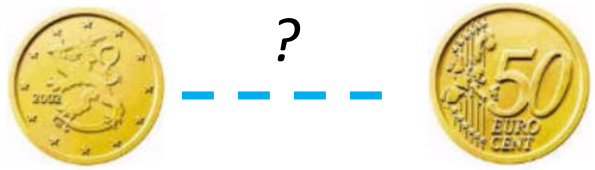
Observation or noise causes loss of information

If a **Quantum state** is measured, observed or touched, it **collapses** to a classical state.

The state does not stick around for a long time, which makes hard to build a quantum computer

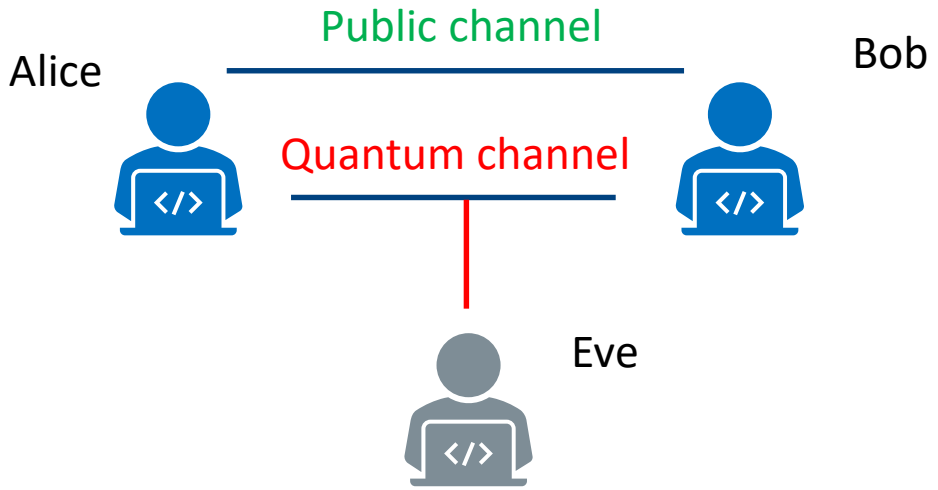
QUANTUM ENTANGLEMENT

"Spooky action at distance" – Albert Einstein



Observed here

Affected at long distance



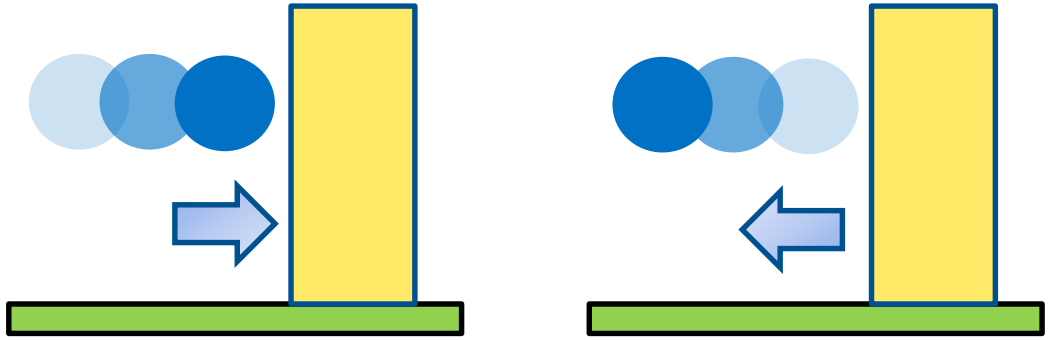
Quantum state of each particle cannot be described independently of the others

Entanglement is used for Quantum key distribution

QUANTUM TUNNELING

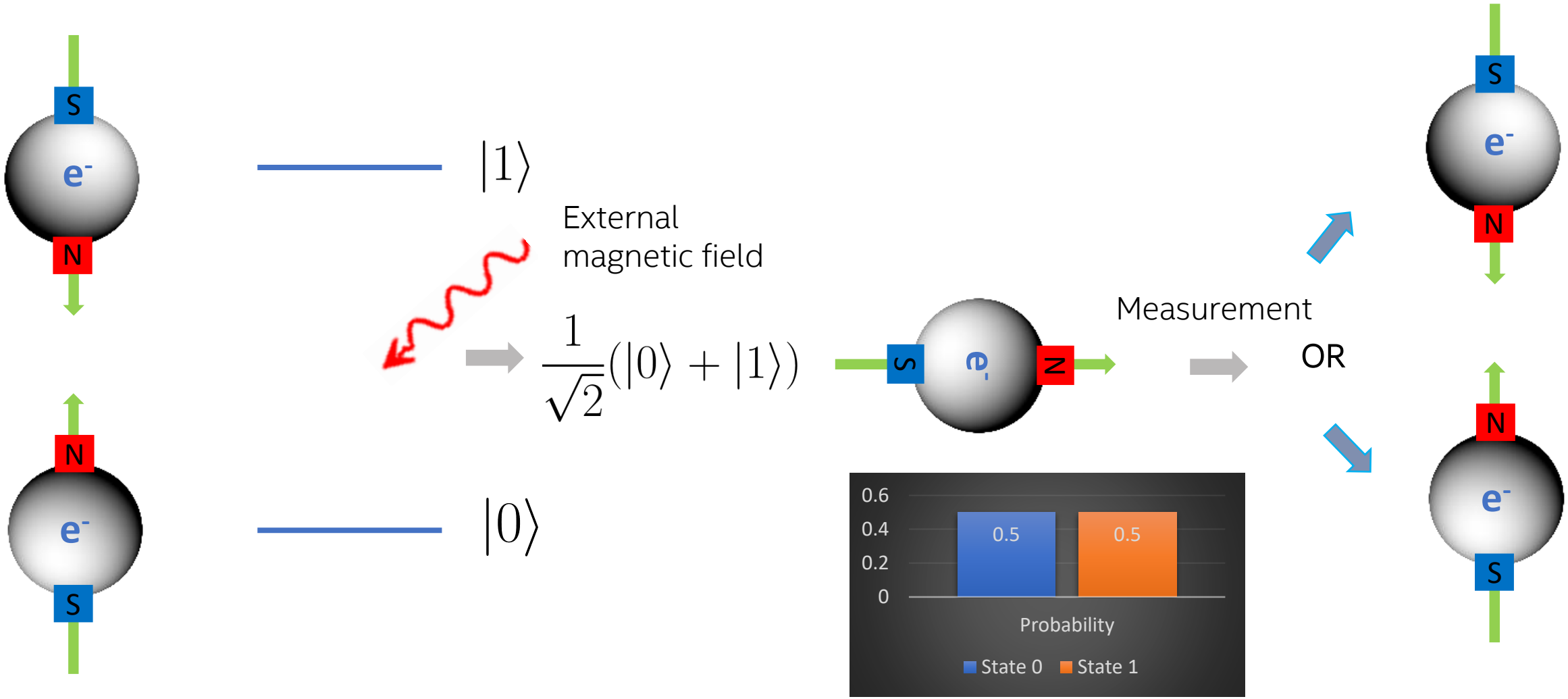
The phenomenon of quantum wave functions (and consequently quantum particles) percolating classically forbidden areas is known as Quantum Tunneling

Classical picture



Quantum picture

2-LEVEL ELECTRON SPIN AND MEASUREMENTS



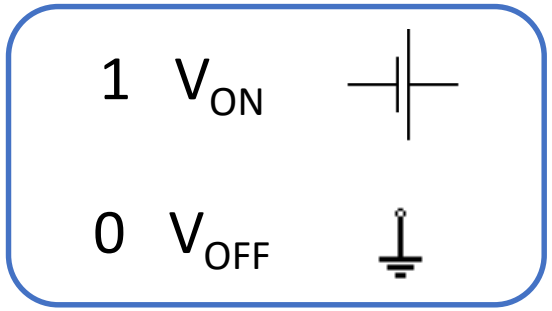
BASIC BUILDING BLOCK: QUBIT

QUBITS

Qubits are the storage element of quantum information, similar to usual bits but with all the weirdness of the previous section added on top!

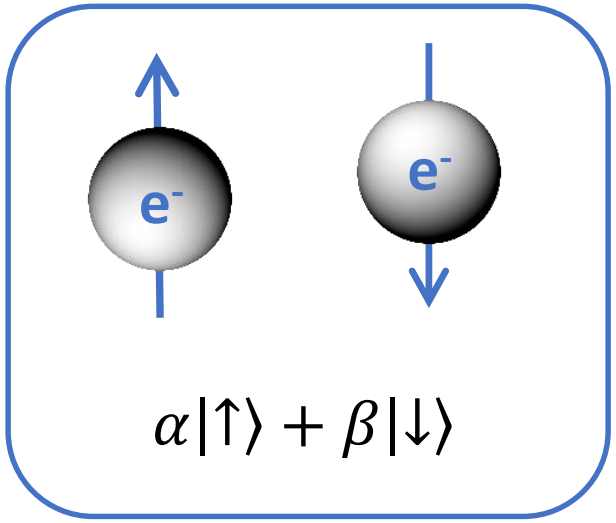
Classical

0 or 1



Quantum

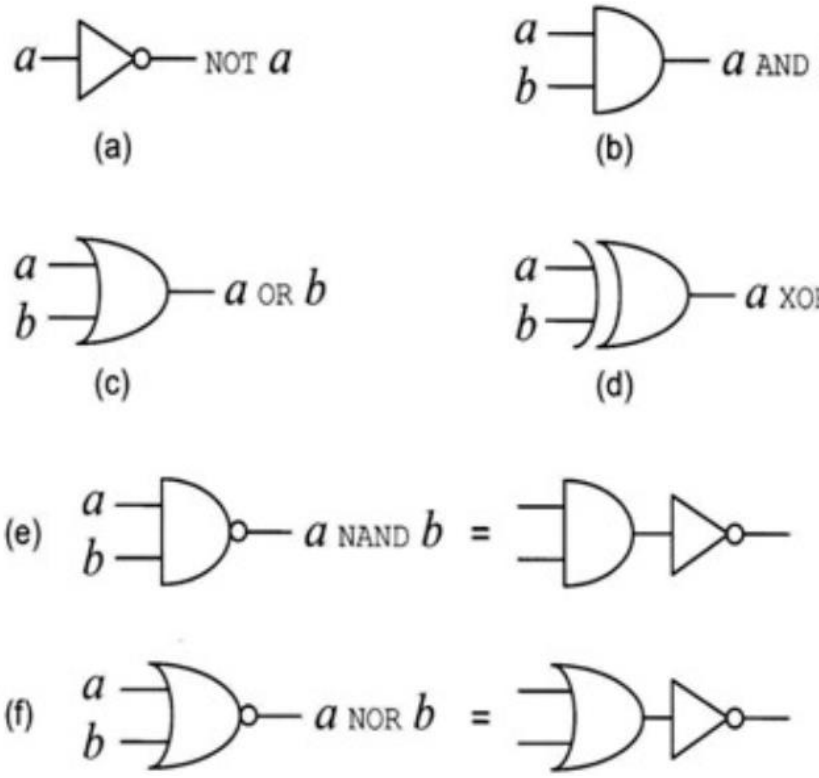
$\alpha|0\rangle + \beta|1\rangle$



QUANTUM GATES

Basic circuit operating on a single bit/qubit

Classical

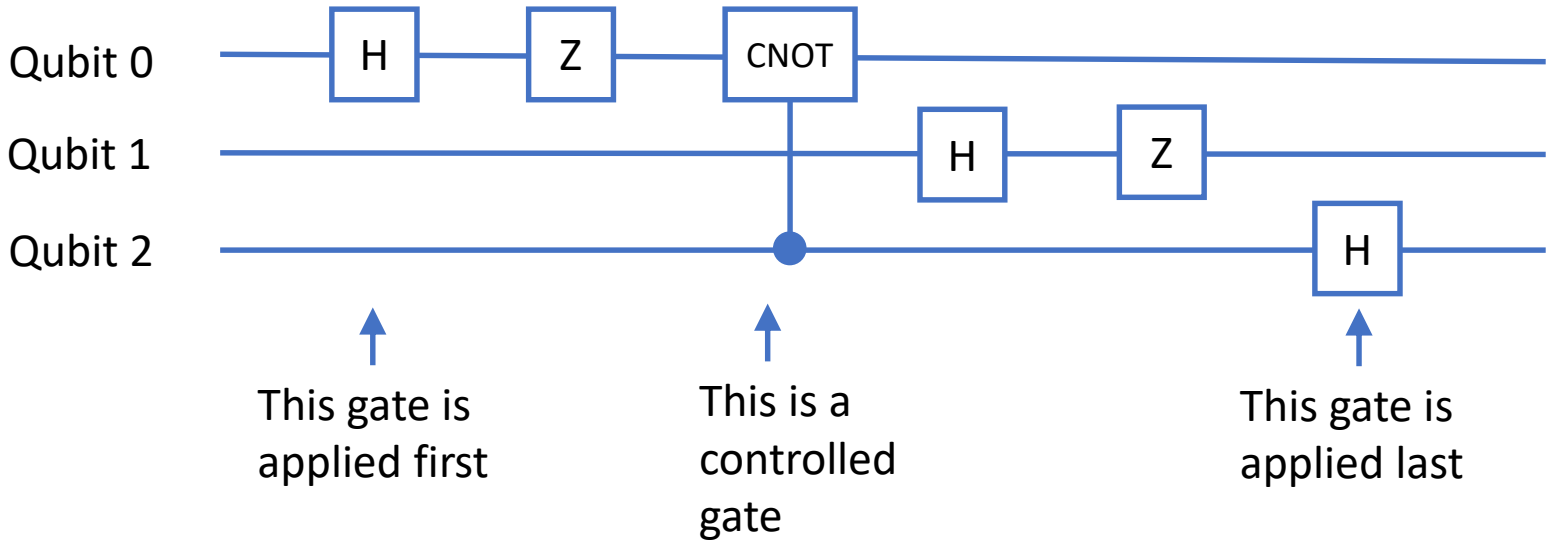


Quantum

NOT (Pauli-X)	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT (Controlled NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

QUANTUM CIRCUITS

A quantum circuit is a sequence of quantum gates applied to a register of qubits. It is usually written in a sort-of guitar string notation, which makes it easier to follow the control flow.



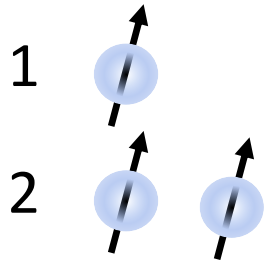
Single qubit gates:

Hadamard gate: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Pauli-Z gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

CNOT gate: $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

THE POWER OF QUANTUM COMPUTING: EXPONENTIAL COMPLEXITY



$$|0\rangle, |1\rangle$$

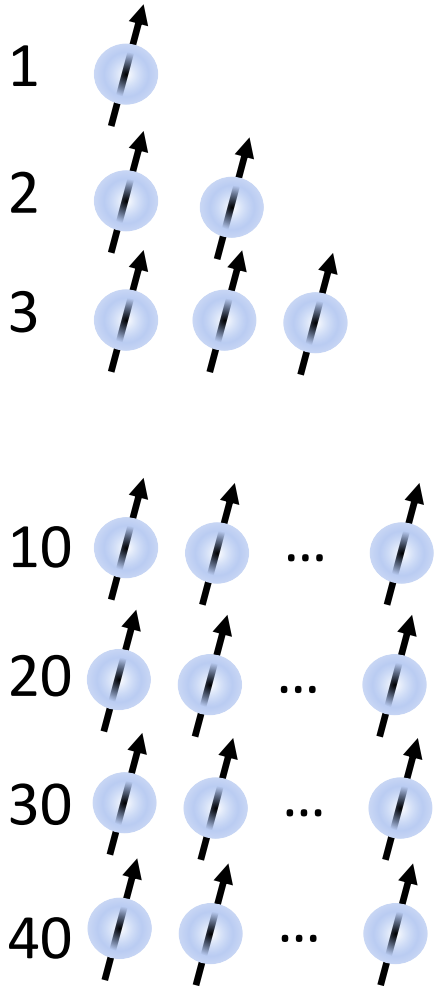
$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

$$\alpha_{00} * |00\rangle + \alpha_{01} * |01\rangle + \alpha_{10} * |10\rangle + \alpha_{11} * |11\rangle$$

- 2 qubits can be in 4 states at the same time!
- We need 4 parameters to describe the states

$$4 = 2^2$$

THE POWER OF QUANTUM COMPUTING: EXPONENTIAL COMPLEXITY



$|0\rangle, |1\rangle$ → $2 = 2^1$

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$ → $4 = 2^2$

$|000\rangle, |001\rangle, |010\rangle, ..., |111\rangle$ → $8 = 2^3$

$|00...\rangle, |00...1\rangle, ..., |11...1\rangle$ → $1k = 2^{10}$

$|00...\rangle, |00...1\rangle, ..., |11...1\rangle$ → $1M = 2^{20}$

$|00...\rangle, |00...1\rangle, ..., |11...1\rangle$ → $1G = 2^{30}$

$|00...\rangle, |00...1\rangle, ..., |11...1\rangle$ → $1T = 2^{40}$

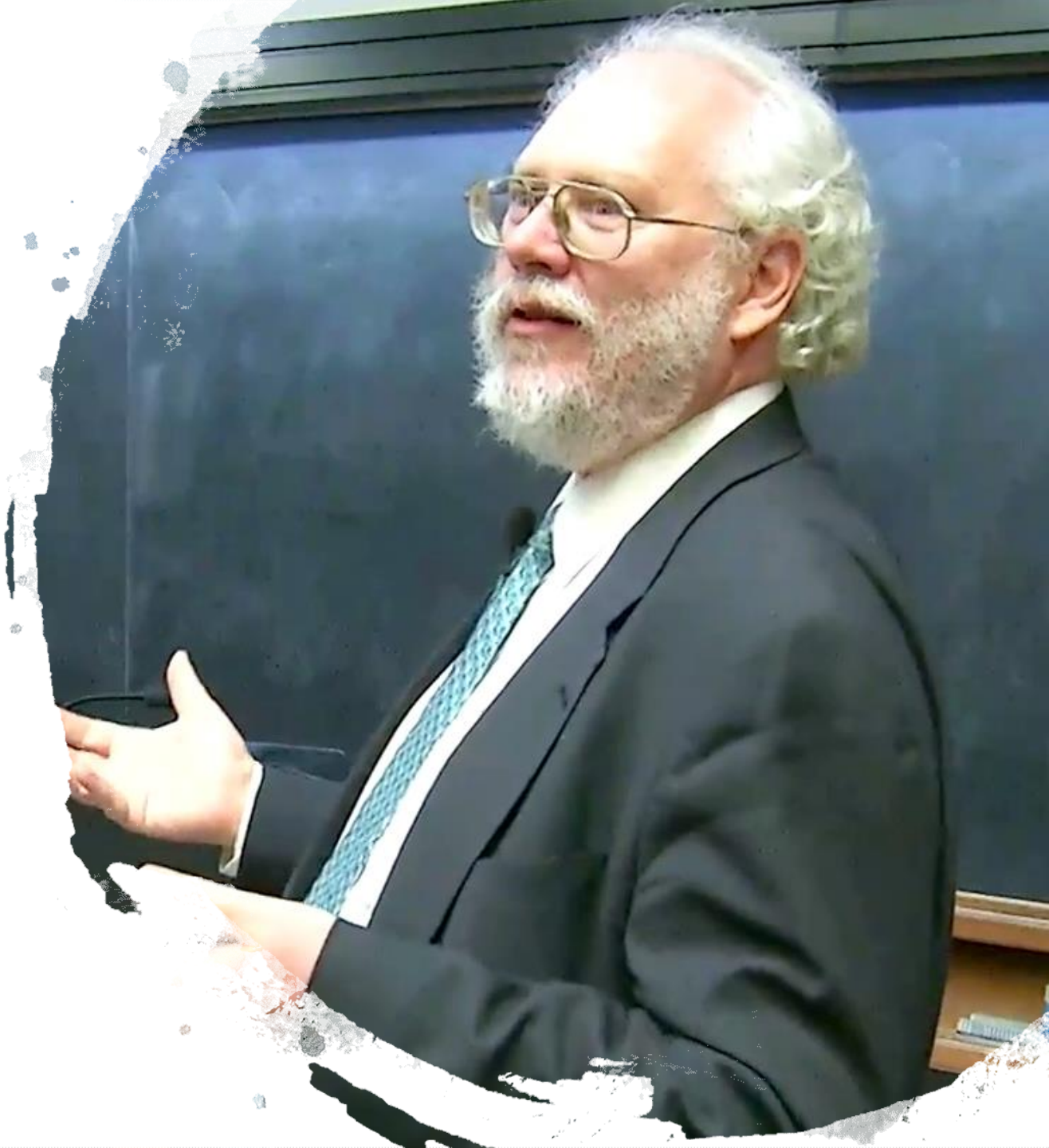
WHAT IS A QUANTUM COMPUTER?

- Qubits: any 2-level physical system which is controlled by the quantum mechanical rules. The memory of a quantum computer is a quantum register, consisting of a set of qubits.
- Gates: represent unitary transformation of single and double qubits
- Measurements: this lead to a probability distribution

WHY QUANTUM COMPUTATION?

Shor’s factoring algorithm (1994)

- **Quantum computers can factor n-digits integers in *polynomial time***
- **This is the base of our cryptography system**
- **Quantum computer can solve hard problems that might not be solved with a classical machine**



WHAT CAN WE DO WITH QUANTUM COMPUTING?

Cryptanalysis	Breaking the RSA crypto-system with Shor's algorithm
Quantum Search	Quantum database search with Grover's algorithm
Quantum Simulation	The simulation of new materials is based on the same second-quantization approach we used here. Exploiting qubits for the simulation is straight forward

Augmenting the Traditional HPC Systems

~50+ Qubits: Proof of concept

- Computational power exceeds supercomputers
- Learning test bed for quantum “system”

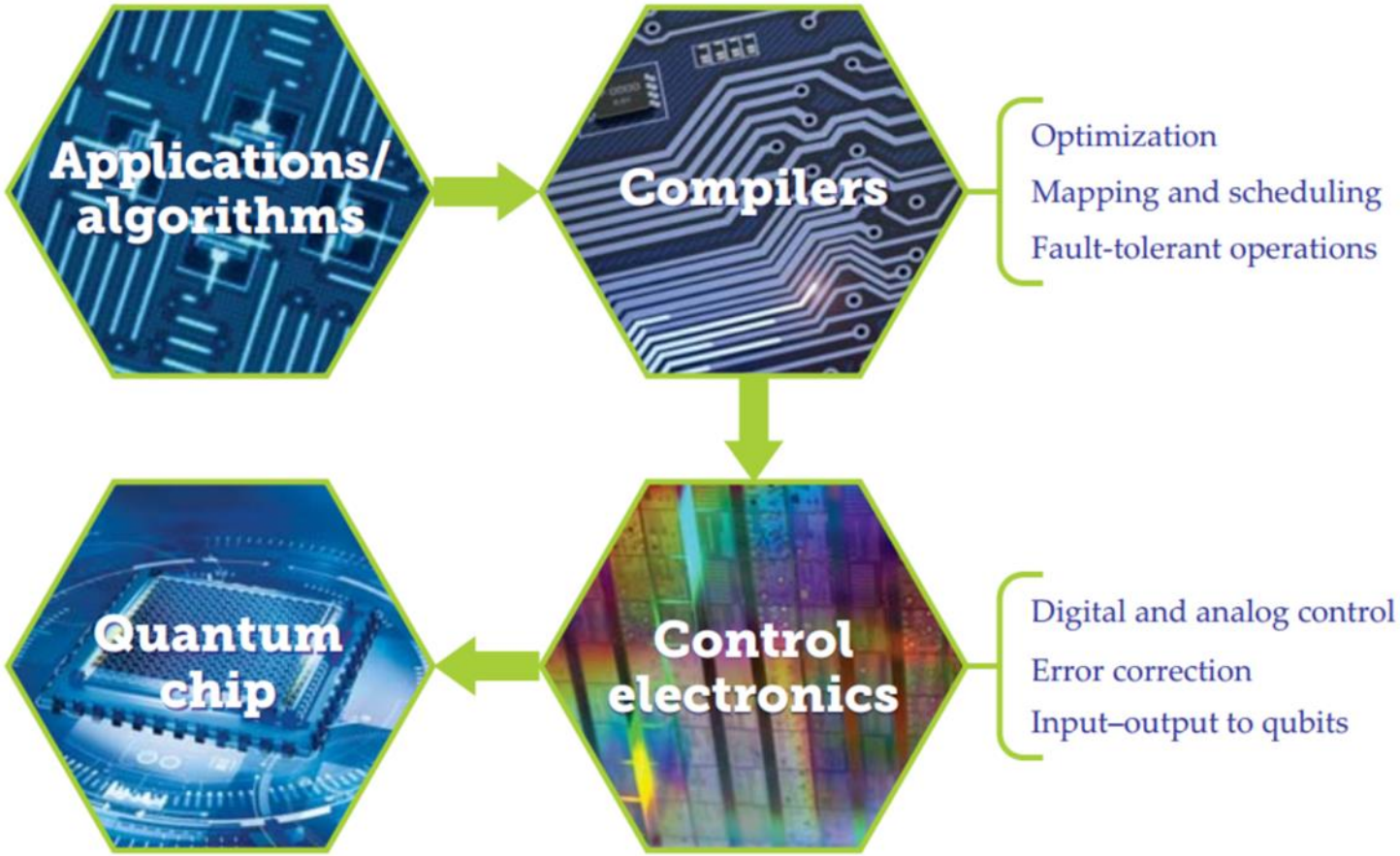
~1000+ Qubits: Small problems

- Limited error correction
- Chemistry, material design
- Optimization

~1M+ Qubits: Commercial scale

- Fault tolerant operation
- Cryptography
- Machine Learning

Functionalities Necessary for a Quantum Computer



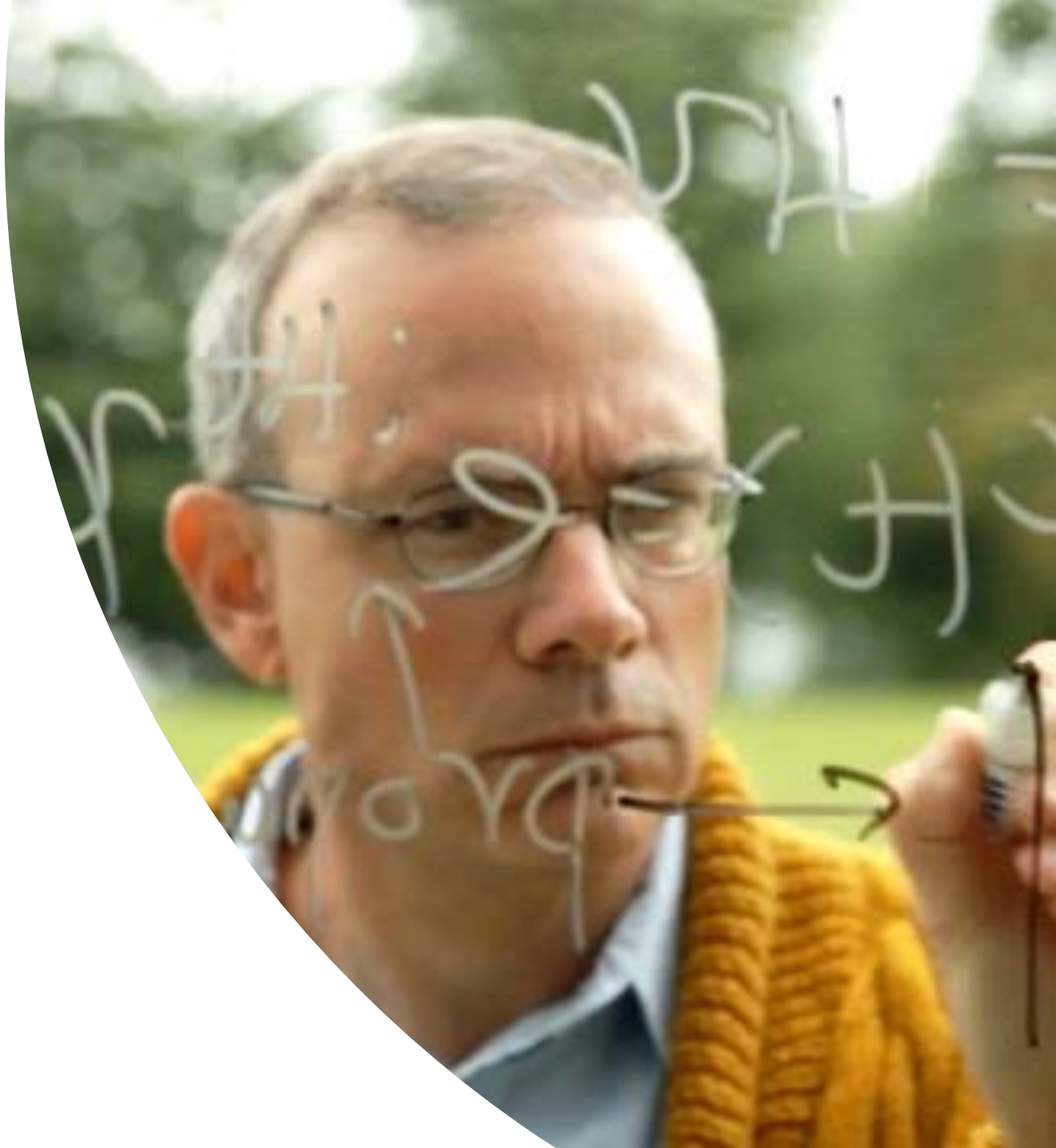
How does one create a quantum computing system that takes a quantum algorithm as input and automatically performs a computation on qubits?

A systems perspective of quantum computing: https://doi.org/10.1063/PT.3.4163

HOW DO WE CREATE AND OPERATE A QUANTUM COMPUTER?

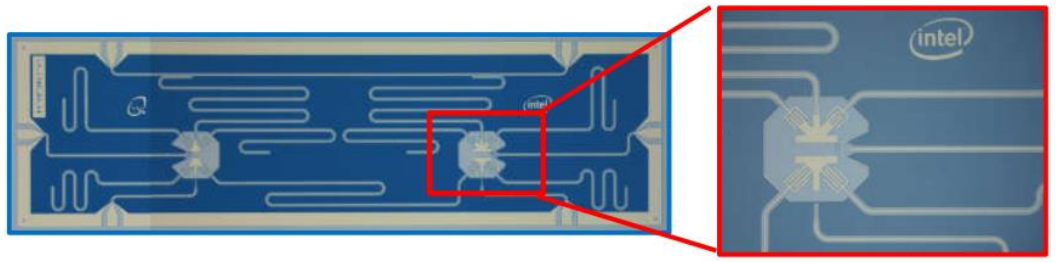
DiVincenzo’s criteria for building a quantum computer (2000)

- *A scalable physical system with well characterized qubit*
- *The ability to initialize the state of the qubits to a simple fiducial state*
- *Long relevant decoherence times*
- *A "universal" set of quantum gates*
- *A qubit-specific measurement capability*



BUILDING QUBITS

Superconducting Qubits



Qubit
Two Level System (TLS)

ε_1

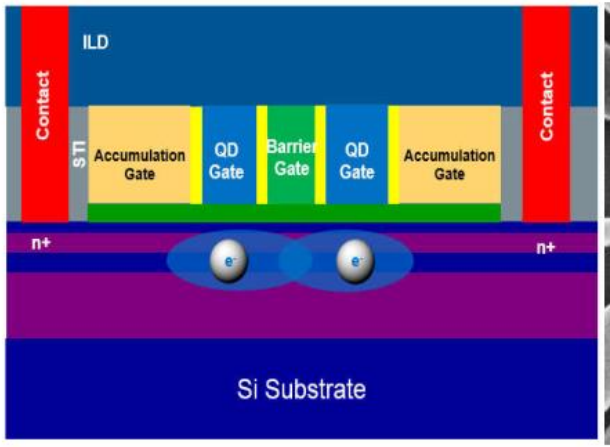
$E_z = \varepsilon_1 - \varepsilon_0$

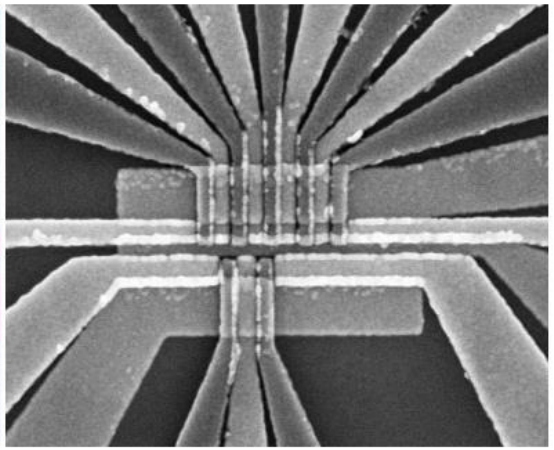
ε_0

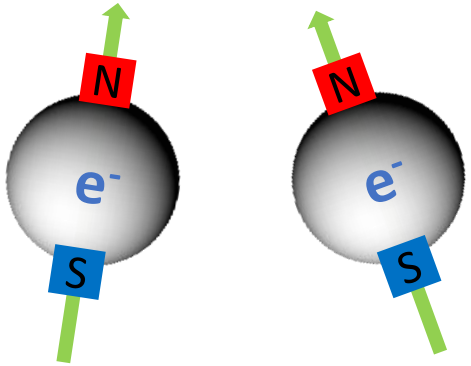
$\hbar\omega_0 = \delta\varepsilon_{01}$

ω ~ GHz
μwave

Spin Qubits in Silicon

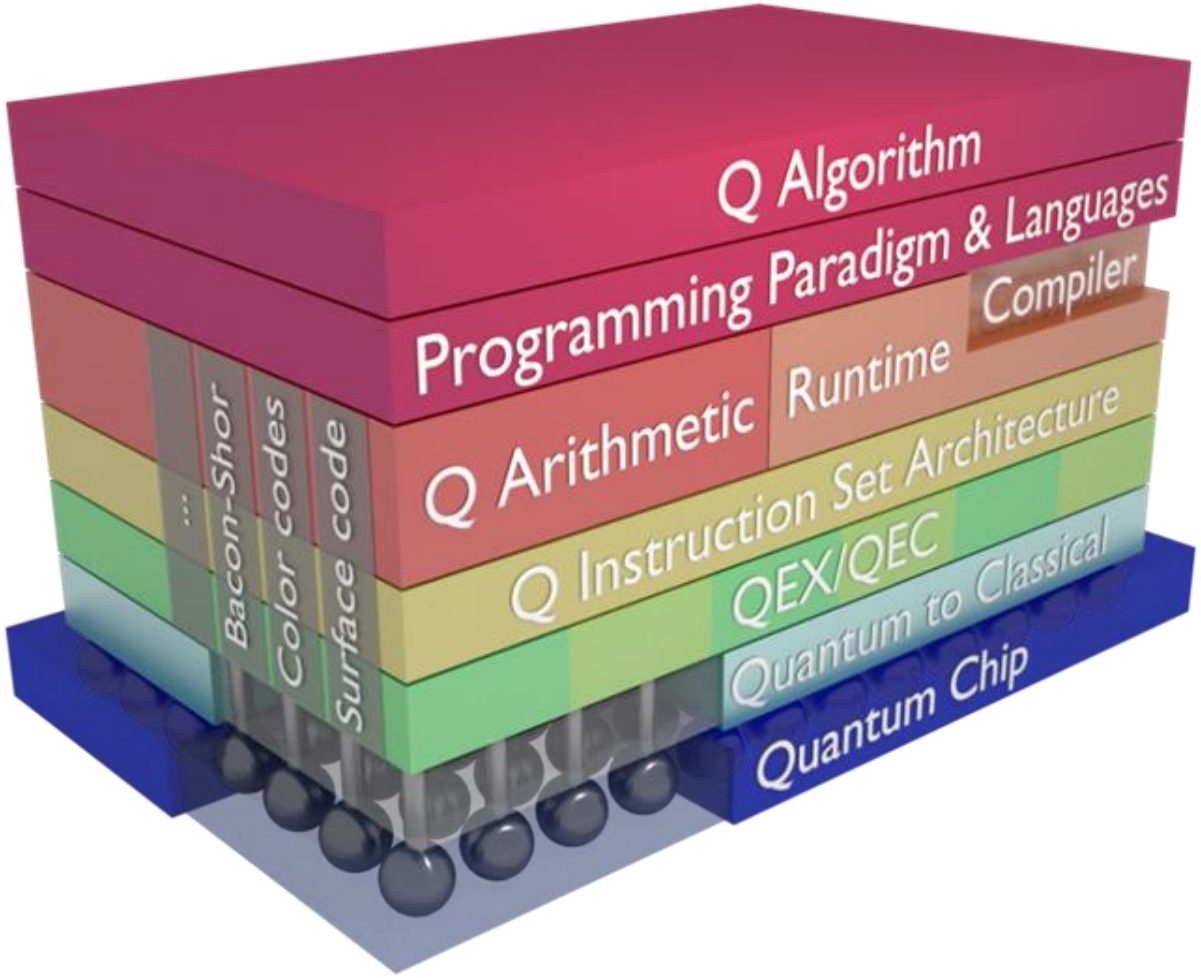






Single electron transistor

QUANTUM COMPUTING SYSTEM STACK



Many challenges when building a large-scale quantum system

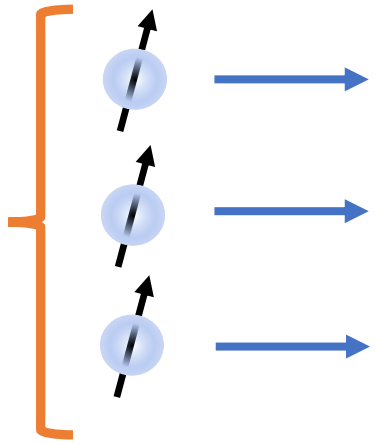
- Quantum applications and algorithms
- Programming languages
- Mapping to the quantum chip:
  - Instruction set definition
  - Compiler technology
  - Gate optimization

WHAT CAN WE DO NOW? SIMULATING QUANTUM ALGORITHMS ON CURRENT SYSTEMS

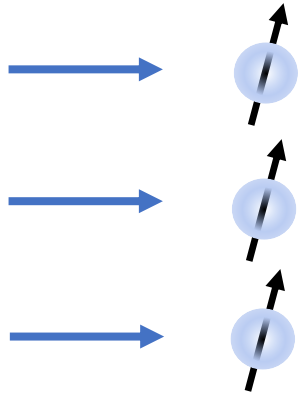
QUANTUM ALGORITHM

Physically

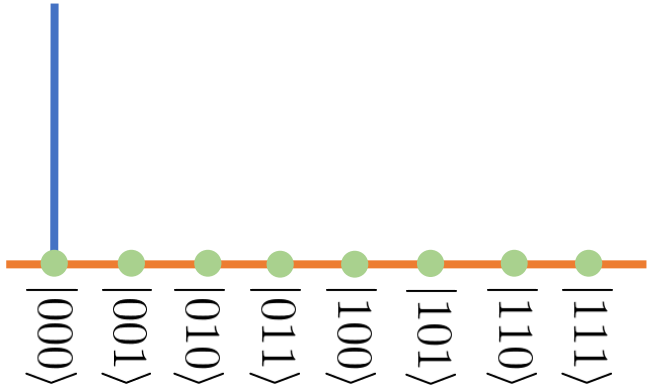
N input qubit



Sequence physical signals and pulses to manipulate the quantum register

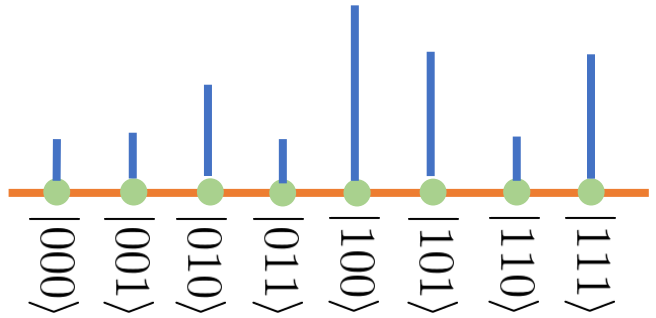


Practically



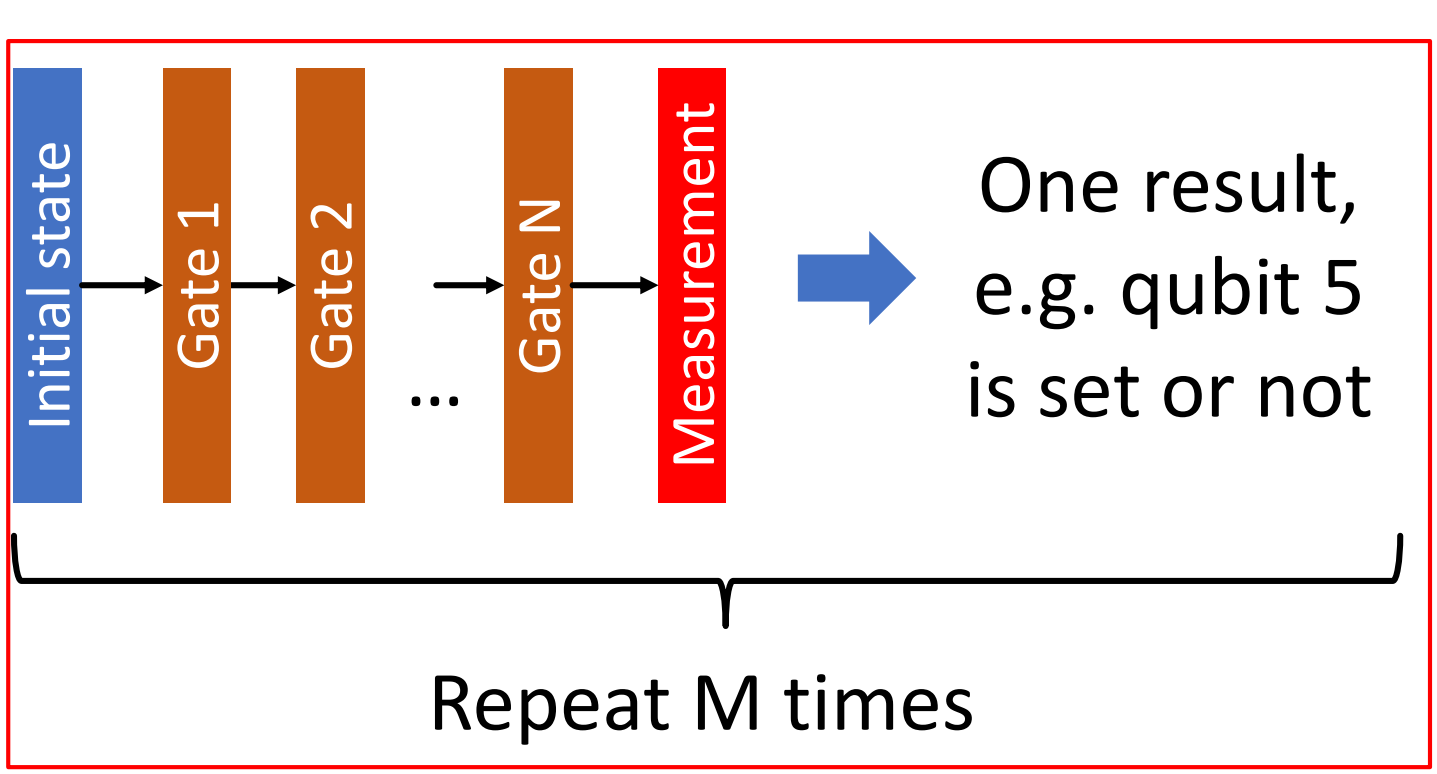
Probability distribution over the classical states

Sequence of Quantum Gates



Maximizing the probability of the good solution

QUANTUM COMPUTING – SPEED UP



many results, e.g. qubit 5 is set
In 75% of the cases

The number of gates times the number of repetitions determines the execution time, not necessarily the size of the problem!

INTEL QUANTUM SIMULATOR

The **Intel® Quantum Simulator** is a single node or distributed high-performance implementation of a quantum simulator that can simulate general single-qubit gates and two-qubit controlled gates

We collaborate with different partners to explore the potential of the quantum computing exploring new algorithms

- Quantum Natural Language Processing

- Quantum Neural Network Perceptron

https://github.com/intel/intel-QS

CONCLUSIONS

- The quantum computer started from a very simple idea of computing like the Nature does, but the ***Nature speaks Quantum***
- The potential of quantum computing is enormous and all the excitement started from the idea of ***Shor's factorization algorithm***
- Having a commercial system is not enough, knowledge of ***new quantum algorithms*** and applications is required

THANK YOU!


intel
experience
what's inside™