UNC
INFORMATION
TECHNOLOGY SERVICES

Introduction to Quantum Computers

Shubin Liu, Ph.D.
Research Computing Center
University of North Carolina at Chapel Hill
Chapel Hill, NC 27599-3420

Objectives & Prerequisites

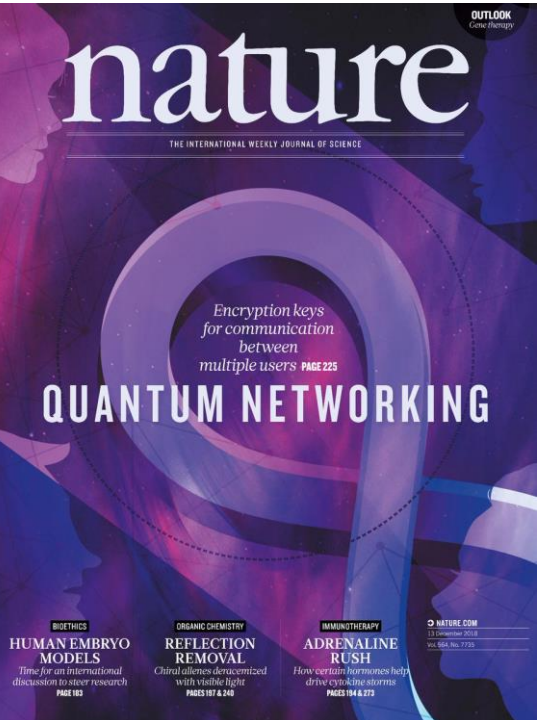
- After this workshop, you should be
  - Familiar with basics and general trends of quantum computers
  - Able to understand simple quantum circuits
  - Ready to build and run simple quantum computing tasks with QISKit
- We assume that you know
  - Basic knowledge of linear algebra and statistics, but not mandatory
  - No prior knowledge of quantum mechanics required
  - **Recommendation**: An account @ IBM Quantum Experience

    https://quantum-computing.ibm.com

UNC INFORMATION TECHNOLOGY SERVICES

Agenda

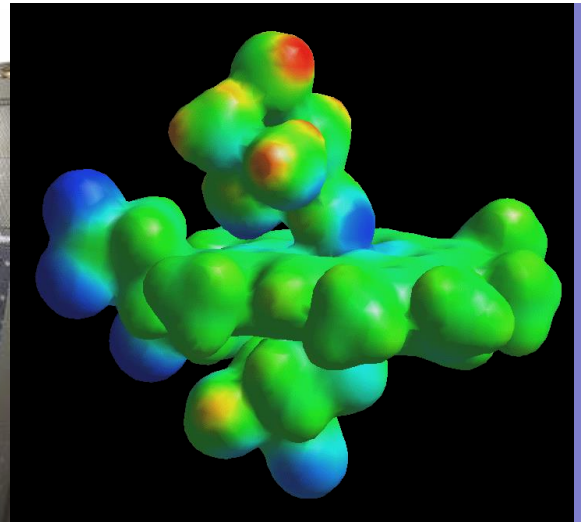
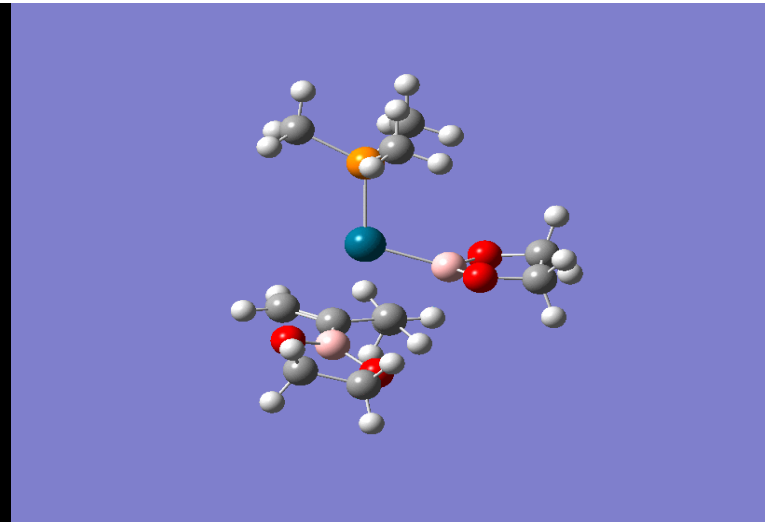
- **What is a Quantum Computer?**
  - Brief history, quantum mechanics, current status
- **Basic Concepts of Quantum Computers**
  - Qubit, superposition, entanglement, decoherence, measurement
  - Quantum gates, quantum circuits, quantum algorithm
- **How does a Quantum Computer work?**
  - Requirements of quantum computer
  - Quantum computer design & roadmap
- **Applications of Quantum Computers**
  - Quantum optimization
  - Quantum chemistry and materials
  - Quantum communication
  - Case studies: cryptography, Shor algorithm, variational quantum eigensolver
- **DEMO: Quantum Computing with QISKit**



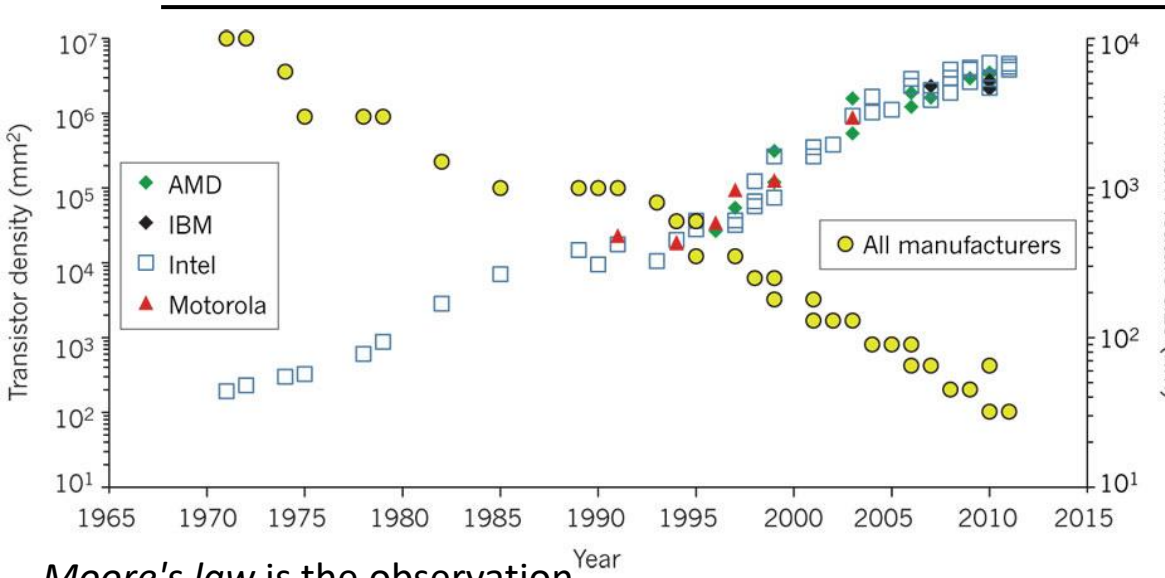
About Myself

- Ph.D. degree, quantum chemist by training, UNC-CH Chemistry
- Senior Computational Scientist @ Research Computing Center, UNC-CH
- Engagement group, training, collaboration, etc. https://shubin.web.unc.edu/
- Research Interests: Development of density functional theory and its applications in biology, energy and drug design (using HPC/HTC clusters)



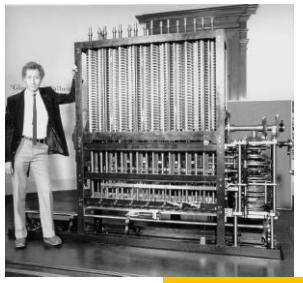



Moore's law & Future of Computers

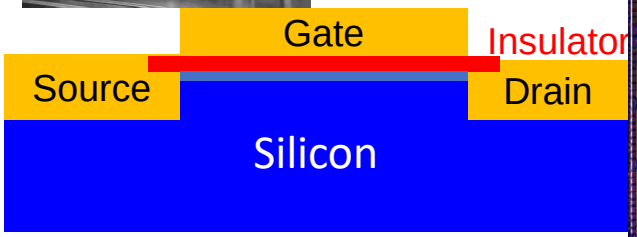


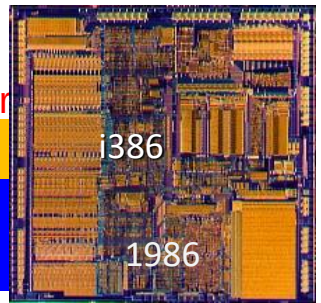
Moore's law is the observation that the number of transistors in a dense integrated circuit doubles about every two years.

Moore's law will soon run into major physical constraints!

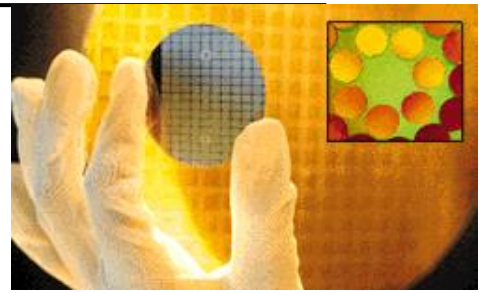


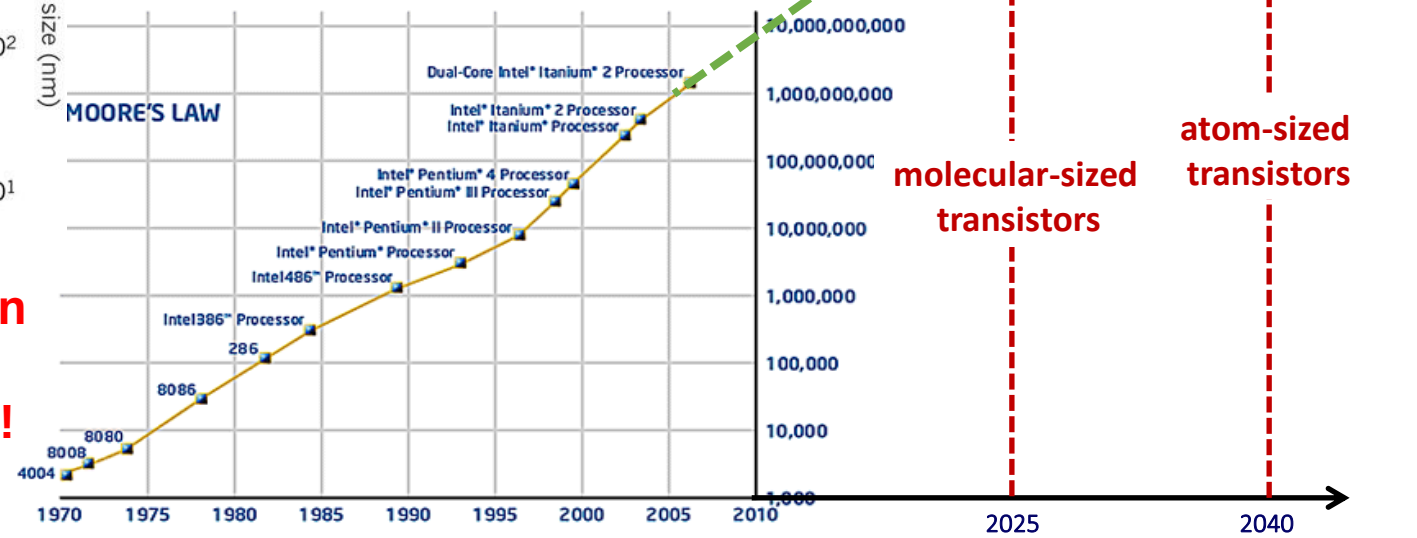
Moore, G. E. *Electronics* **8**, 114–117 (1965).
Image from: Ferain, I. *et al.*, *Nature* **479**, 310–316 (2011).





Richard Feynman





"There's Plenty of Room at the Bottom" (1959)

"When we get to the very, very small world – say circuits of seven atoms – we have a lot of new things that would happen that represent **completely new opportunities for design**. *Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics…"*

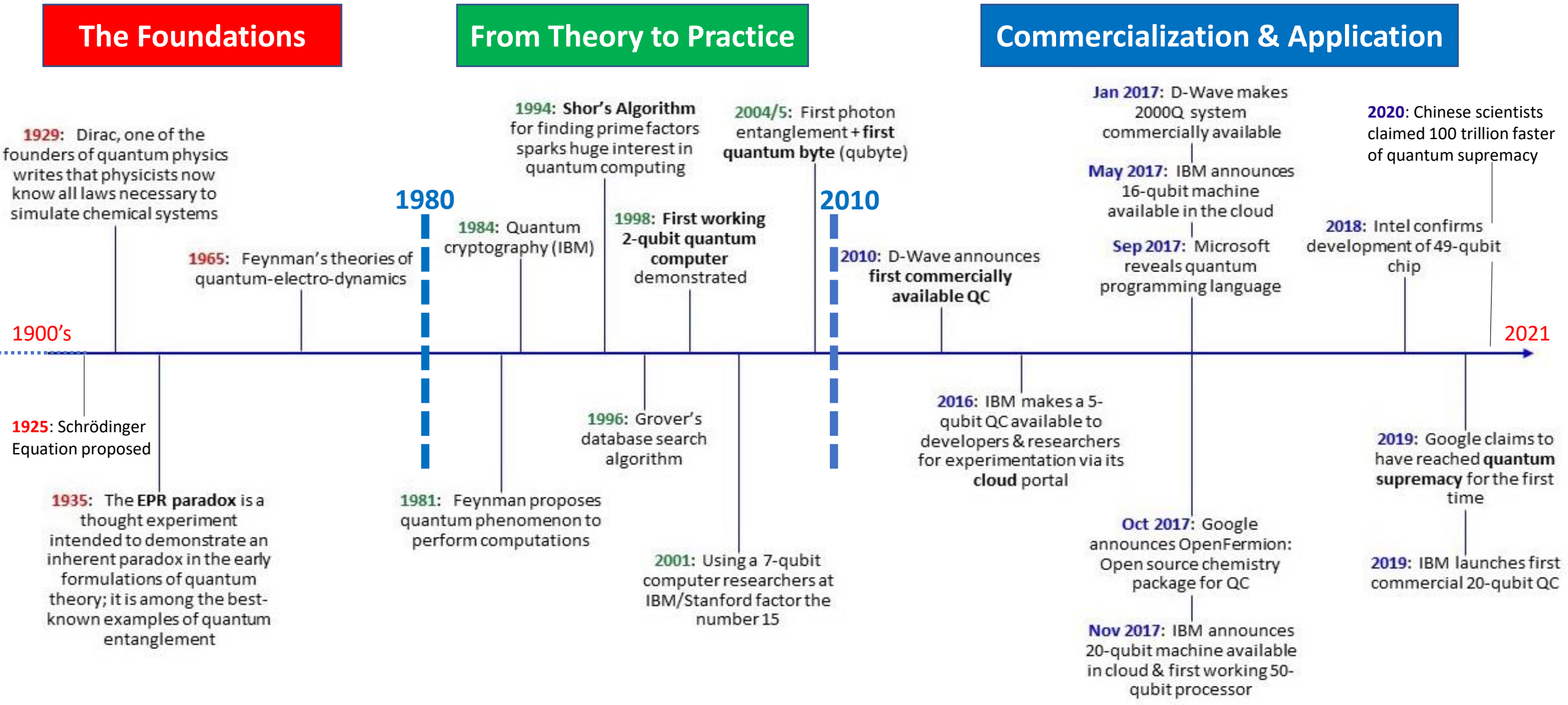
What is a quantum computer?

- Quantum Computer
  - A computer that uses laws of quantum mechanics to perform massively parallel computing through superposition, entanglement, and decoherence.

- Classical Computer
  - A computer that uses voltages flowing through circuits and gates, which can be controlled and manipulated entirely by classical mechanics.

UNC INFORMATION TECHNOLOGY SERVICES

Evolution of Quantum Theory & Quantum Technology



Brief History of Quantum Computers

- 1981: Richard Feynman proposed to use quantum computing to model quantum systems. He also describe theoretical model of quantum computer
- 1985: David Deutsch described first universal quantum computer
- 1994: Peter Shor developed the first algorithm for quantum computer (factorization into primes)
- 1995 Schumacher proposed “Quantum bit” or “qubit” as physical resource
- 1996: Lov Grover developed an algorithm for search in unsorted database
- 1998: the first quantum computers on two qubits, based on NMR (Oxford; IBM, MIT, Stanford)
- 2000: quantum computer on 7 qubits, based on NMR (Los-Alamos)
- 2001: 15 = 3 x 5 on 7- qubit quantum computer by IBM
- 2005-2006: experiments with photons; quantum dots; fullerenes and nanotubes as "particle traps"

UNC
INFORMATION
TECHNOLOGY SERVICES

Brief History of Quantum Computers

- 2007: D-Wave announced the creation of a quantum computer on 16 qubits
- 2012: D-Wave claimed a quantum computation using 84 qubits
- 2017: D-Wave Systems Inc. announced the D-Wave 2000Q quantum annealer with 2000 qubits
- 2017: Microsoft revealed Q Sharp with 32 qubits
- 2018: Google announced the creation of a 72-qubit quantum chip
- 2019: Google claimed quantum supremacy with 54 qubits to perform operations in 200 seconds that would take a supercomputer about 10,000 years to complete
- 2019: IBM revealed 53 qubits
- 2020: Chinese researchers claimed to have achieved quantum supremacy using a photonic 76-qubit system at 100 trillion times the speed of classical supercomputers
- 2020: IBM will build 1121-qubit quantum computer in 2023, and 1 million-qubit quantum computer in 2030.

UNC
INFORMATION
TECHNOLOGY SERVICES

Quantum Mechanics

Quantum mechanics is the theory that describes the behavior of microscopic systems, such as photons, electrons, atoms, molecules, etc.

Nobody understands quantum mechanics!

“No, you’re not going to be able to understand it.... You see, my physics students don’t understand it either. That is because I don’t understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with an experiment. So I hope that you can accept Nature as She is – absurd”

--Richard Feynman

UNC INFORMATION TECHNOLOGY SERVICES

Classical vs. Quantum Mechanics

Classical Mechanics

- It deals with macroscopic particles
- It is based on Newton's laws of motion and Maxwell's electromagnetic wave theory
- Any amount of energy may be emitted or absorbed continuously
- The state of a system is defined exactly by specifying their positions and velocities
- The future state can be predicted with certainty

Quantum Mechanics

- It deals with microscopic particles
- It is based on the Schrödinger equation
- In Planck's postulation, only discrete values of energy are emitted or absorbed – origin of "quantum"
- Because of Heisenberg's uncertainty principle and de Broglie hypothesis dual nature of matter (both particle & wave), the state of a system cannot be specified exactly
- It gives probabilities of finding particles at various locations in space

UNC INFORMATION TECHNOLOGY SERVICES

Quantum Mechanics

- Quantum states, represented by Dirac's ket, $|\psi\rangle$, evolve in time according to the Schrödinger equation:

$$d|\psi\rangle/dt = -i\hat{H}(t)|\psi\rangle/\hbar,$$

- which implies that time evolution is described by unitary transformations:

$$|\psi\rangle \rightarrow \hat{U}|\psi\rangle.$$

$$d\hat{U}(t)/dt = -i\hat{H}(t)\hat{U}(t)/\hbar.$$

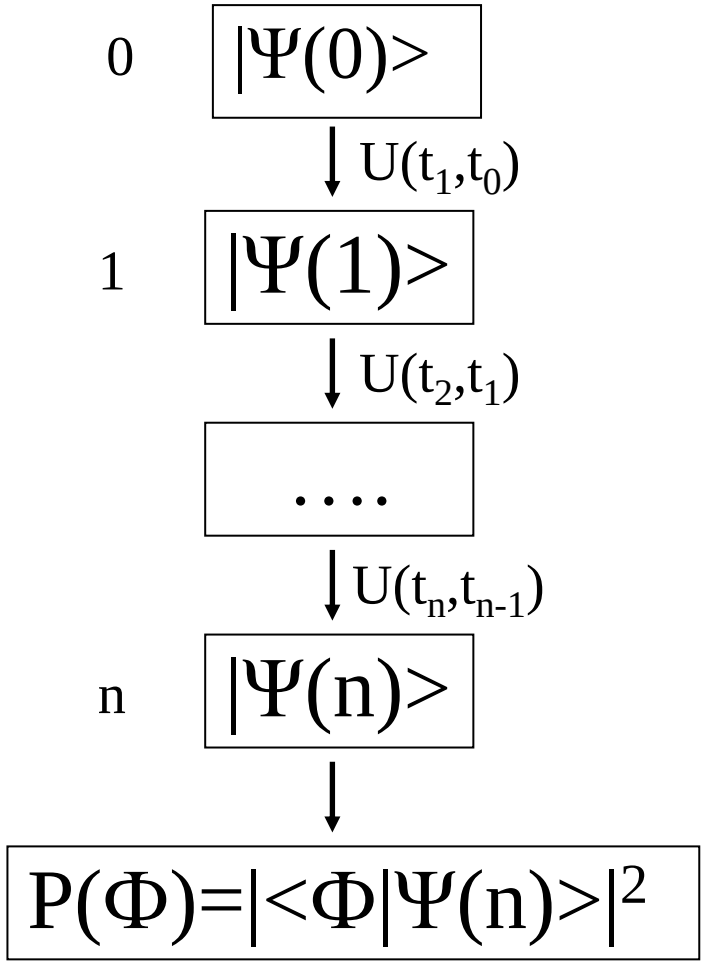
- where $|\psi\rangle$ is the quantum state (wavefunction) and H is Hamiltonian

- This theory, which has been extensively tested by experiments, is probabilistic in nature. The outcomes of measurements on quantum systems are not deterministic.

- Between measurements, quantum systems evolve according to linear equations (the Schrödinger equation). This means that solutions to the equations obey a superposition principle: *linear combinations of solutions are still solutions*.

UNC INFORMATION TECHNOLOGY SERVICES

Unitary Transformation as Quantum Computing



PREPARATION:

The initial preparation of the state defines a wave function at time $t_0=0$.

STATE EVOLUTION:

Evolved by a sequence of unitary operations

....

MEASUREMENT:

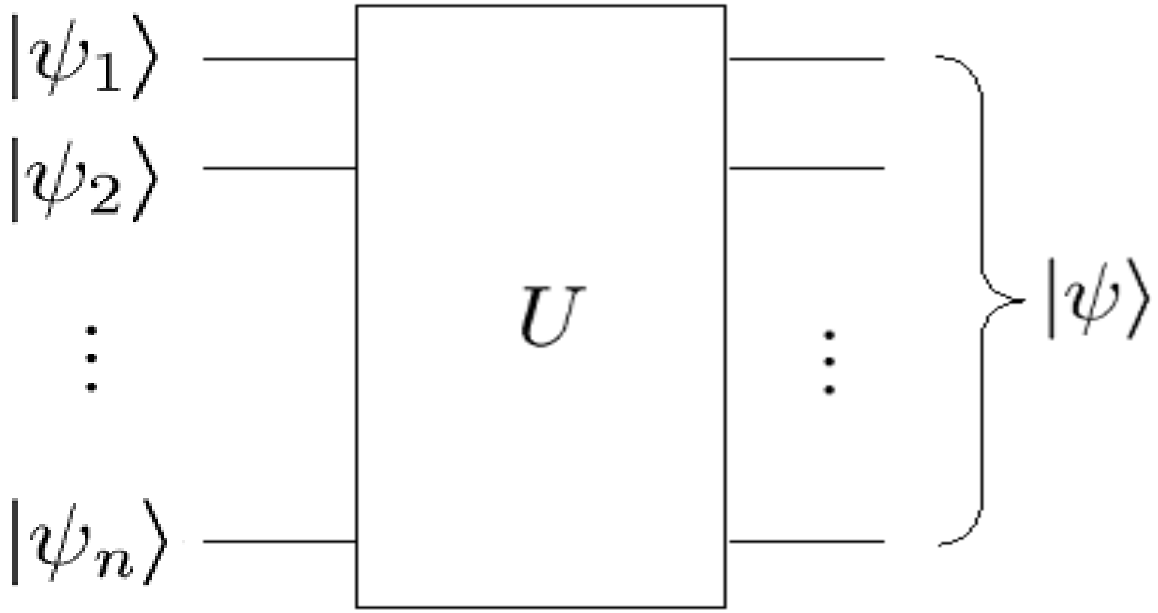
Quantum measurement is projective.

Collapsed by measurement of the state

UNC INFORMATION TECHNOLOGY SERVICES

Classical Computing Approach using Flow Chart

Unitary Transformation as Quantum Computing



On a quantum computer, programs are executed by unitary evolution of an input that is given by the state of the system, $|\psi_n>$, which can in either 0 or 1 state. Since all unitary operators are invertible, we can always reverse or 'uncompute' a computation on a quantum computer.

What does a quantum computer look like?

Chinese 76-qubit photon-based quantum computer

IonQ, ion-trap-based 32-qubit quantum computer

IBM 53-qubit superconductor-based quantum computer

Quantum Computing Race - Corporations

R&D investments reach $10.7 billion by 2024

THE EUROPEAN QUANTUM COMPUTING STARTUP LANDSCAPE

YEAR 2020

Hardware

Computing

OQC, Alice & Bob, AQT, IQM, ORCA Computing, Oxford Ionics, Universal Quantum, eleQtron, the nQn project, Quantum Motion, NextGenQ

Components & Materials

AegiQ, QBLOX, quantum technology supersensors, kiutra, nu Quantum, MIRAEX, Qnami, Delft Circuits, Hardware for quantum engineers, QDevil, Quandela, TORIDION, The Quantum Computing People

Software

Operating Systems

QBaltic, Quantum Machines, QUANTASTICA, RIVERLANE, ParityQC

Applications

Security & Encryption

QUSIDE, PHASECRAFT, QuBalt, InfiniQuant, Quantumz.io, QuantLR, Quantum Impenetrable, Crypta Labs, Kronus, ArQit, Dawn Data Technologies, QuantiCor, PQSHIELD, Crypto Quantique, KETS, Quantum Base, CRYPTONEXT SECURITY, QUANTOPTICON

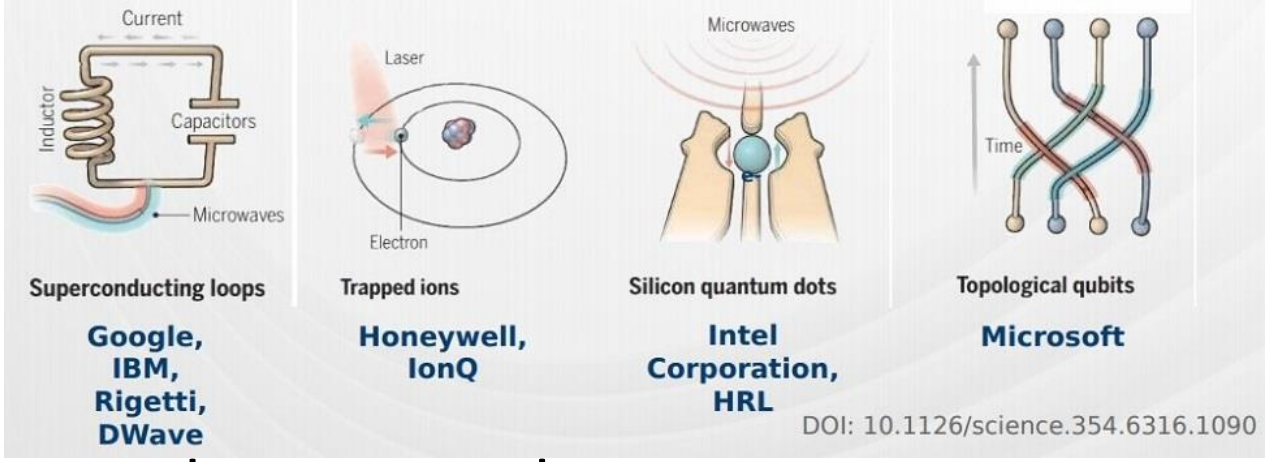
Chemistry & Pharma

HQS Quantum Simulations, KUANO, rahko, CQC Cambridge Quantum Computing, Ketita, APEXQUBIT, ChemAlive, Qu & Co, Pharmacelera, Creative Quantum

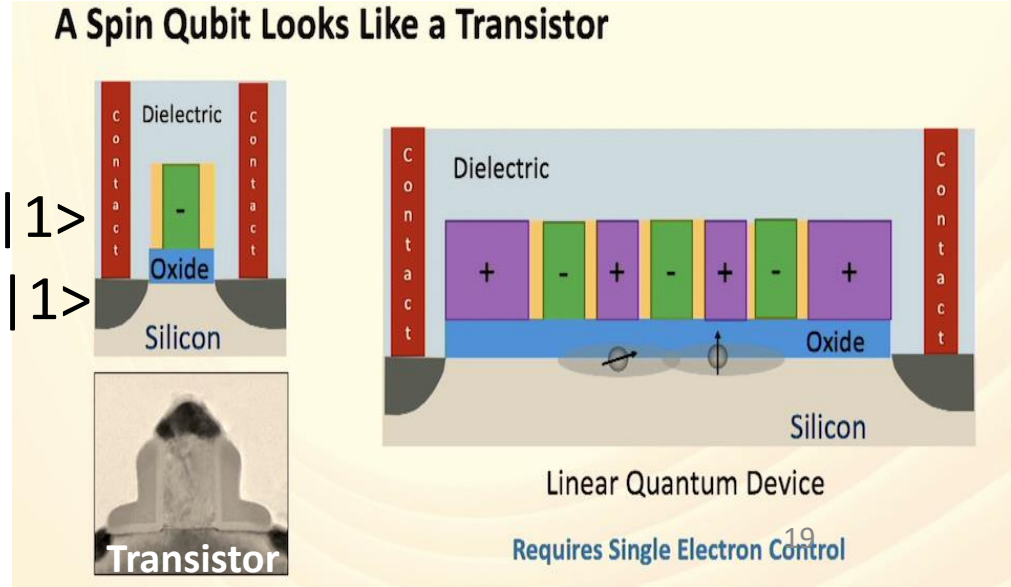
Others

⟨b| e⟩, VeriQloud, |n⟩, AVANETIX, QuantFi, Multiverse Computing, JoS QUANTUM, Terra Quantum, shyn

Quantum Bit - Qubit



- The smallest unit of information in a quantum computer
- It represents the state of the wavefunction $|\psi\rangle$ in Schrödinger equation
- A qubit may be in the "on" (1) state or in the "off" (0) state
- Many ways to implement a qubit:
  - Nuclear spin in NMR: ↑ = |0>, ↓ = |1>.
  - Photons in a cavity: 0 photon = |0>, 1 photon = |1>
  - Energy states of an atom: g.s. |0>, excited state |1>
  - Polarization of photon, many others….



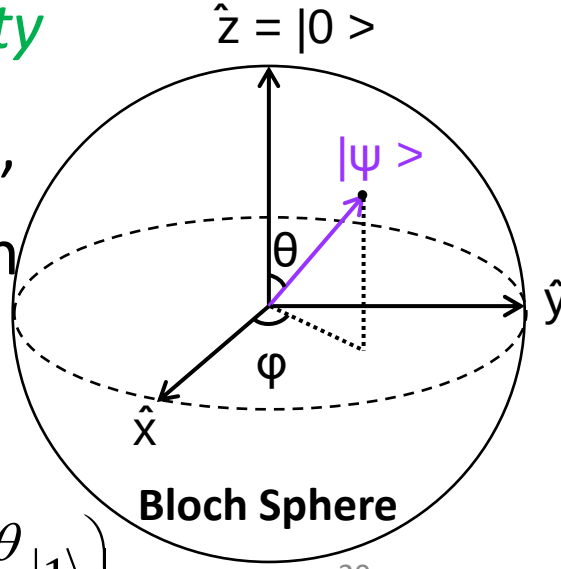
Quantum Bit - Qubit

- Since quantum systems evolve according to linear equations (the Schrödinger equation), linear combinations of solutions are also solutions. So, for the state of a qubit|0> and |1>, its superposition also describes the same state
- The general form of a qubit state can be represented by:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

where α_0 and α_1 are complex numbers that specify the *probability amplitudes* of the corresponding states.

- $|\alpha_0|^2$ gives the probability that you will find the qubit in the "off" (0) state; $|\alpha_1|^2$ gives the probability that you will find the qubit in the "on" (1) state.
- Normalization condition: $|\alpha_0|^2 + |\alpha_1|^2 = 1$



$$|\Psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

UNC INFORMATION TECHNOLOGY SERVICES

Classical Bit vs. Quantum Bit

CLASSICAL BITS:

- can be in two distinct states, 0 and 1
- can be measured completely
- are not changed by measurement
- can be copied
- can be erased

QUANTUM BITS:

- can be in state |0> or in state |1> or in any other state that is a linear combination of the two states
- can be measured partially with given probability
- are changed by measurement
- cannot be copied
- cannot be erased

UNC INFORMATION TECHNOLOGY SERVICES

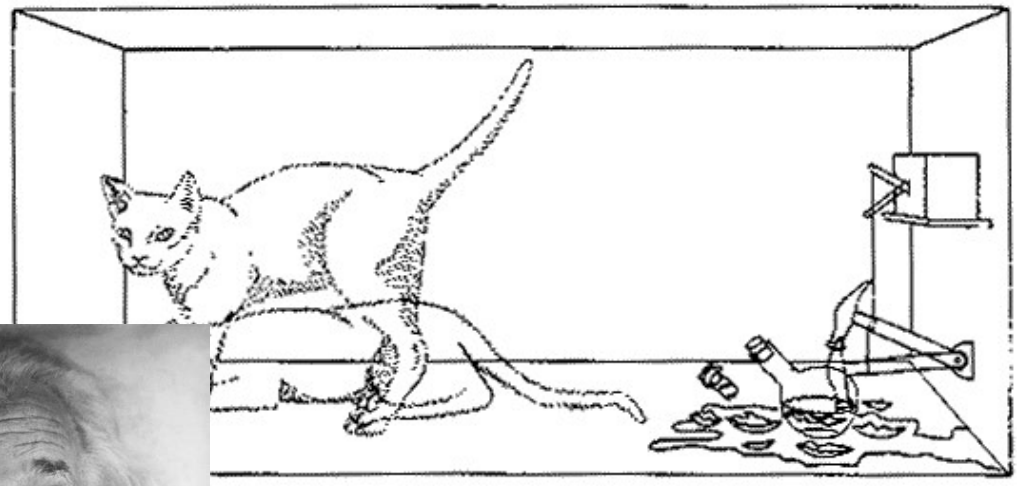
Advantages of Qubits & Enormous Quantum Power

- Adding qubits increases storage exponentially
  - Quantum computer doubles the power with every added qubit
    - To double the power of a digital computer 32bits -> 64 bits
    - To double the power of a quantum computer 32qubits -> 33 qubits
- Can do operations on all superpositions…like massively parallel computation
  - One math operation on 2^n numbers encoded in classical computers with n bits requires 2^n steps or parallel processors, but the same operation on 2^n numbers encoded by n qubits takes 1 step
    - A 64-bit computer can perform manipulation on 64-bit binary numbers at a time.
    - A 64-qubit quantum computer operates in a space of 2^{64} dimensions, or roughly 16,000,000,000,000,000,000 ($16*10^{18}$) numbers to specify the state of the quantum system.
- This makes complex problems much easier to solve by quantum computer

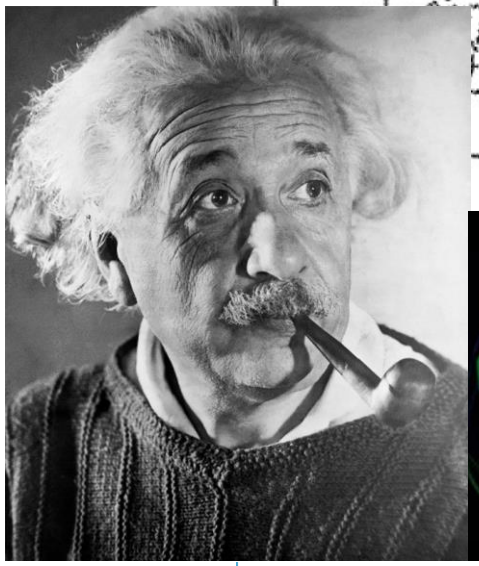
UNC INFORMATION TECHNOLOGY SERVICES

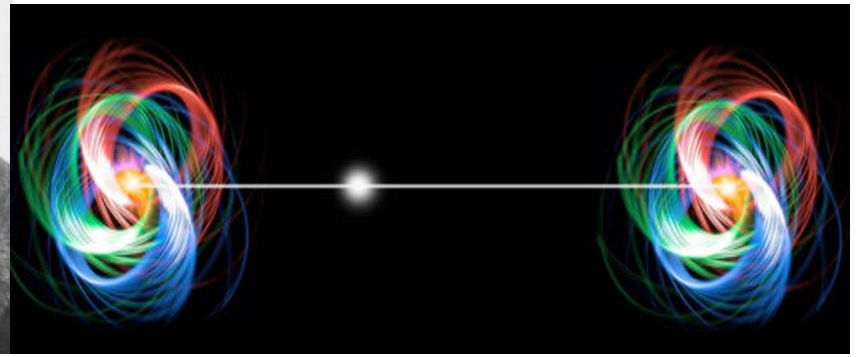
However, Quantum Systems are SPOOKY!

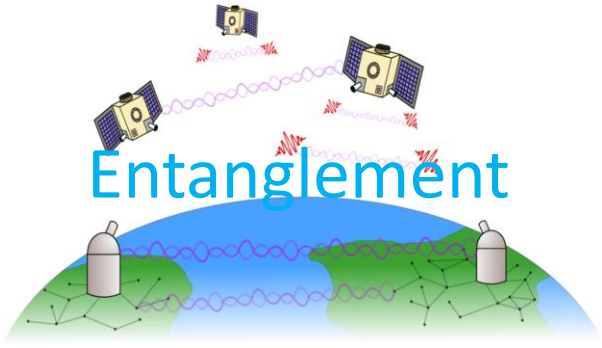
Schrödinger's Cat: Superposition



Schrödinger's Cat in a black box







UNC INFORMATION TECHNOLOGY SERVICES

"I cannot seriously believe in [the quantum theory] because it cannot be reconciled with the idea that physics should represent a reality in time and space, free from spooky actions at a distance." *Albert Einstein, March 1947.*

Superposition

- Every quantum state can be represented as a sum of two or more other distinct states. Mathematically, it refers to a property of solutions to the Schrödinger equation; since the Schrödinger equation is linear, any linear combination of solutions will also be a solution.
- A single qubit can be forced into a superposition of the two states denoted by the addition of the state vectors:

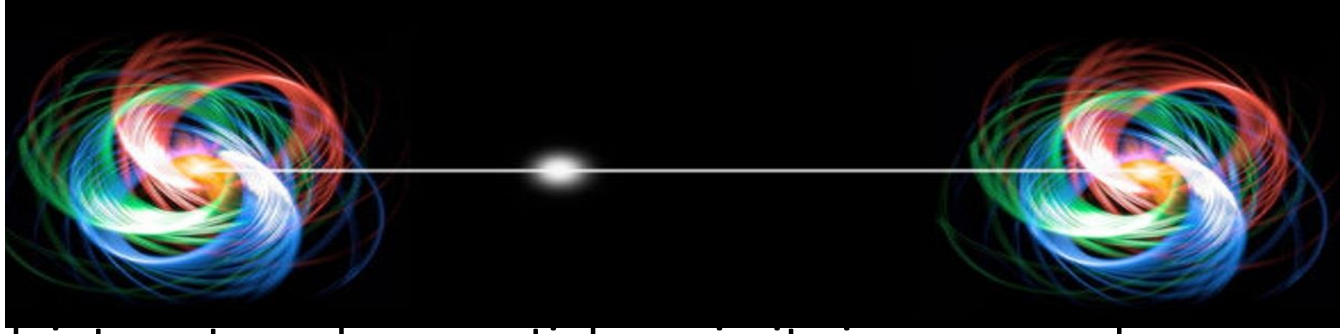
$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

Where α_0 and α_1 are complex numbers and $|\alpha_0|^2 + |\alpha_1|^2 = 1$

- A qubit in superposition is in both of the states $|1\rangle$ and $|0$ at the same time
- If this state is measured, we see only one or the other state (live or dead) with some probability.
- The classic example of superposition is Schrödinger's Cat in a black box. Since both a living and dead cat are obviously valid solutions to the laws of quantum mechanics, a superposition of the two should also be valid. Schrödinger described a thought experiment that could give rise to such a state.
- Consider a 3-qubit register. An equally weighted superposition of all possible states would be denoted by:

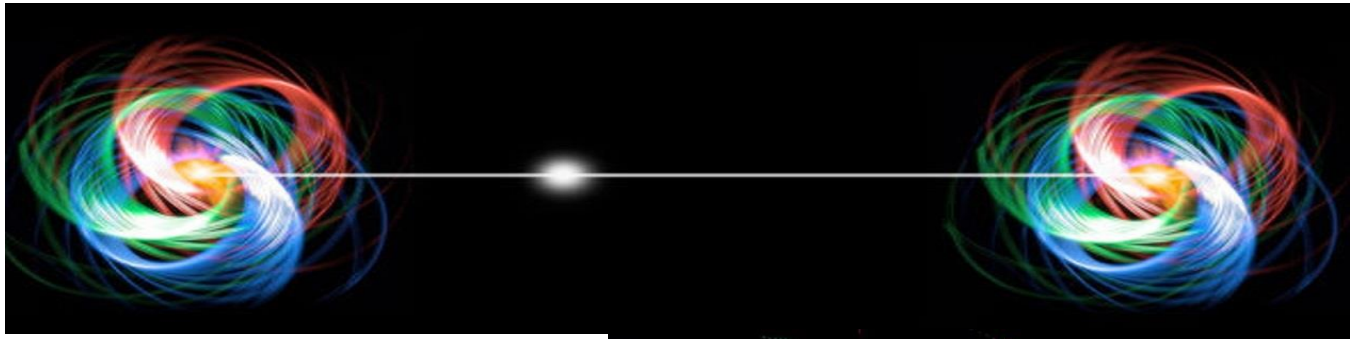
$$|\psi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \ldots + \frac{1}{\sqrt{8}}|111\rangle$$

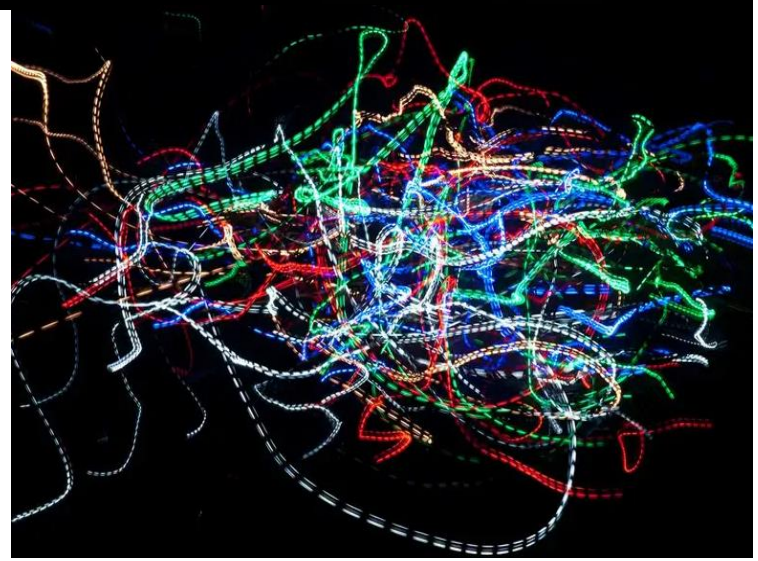
Entanglement



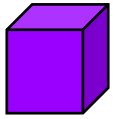
- When a pair or group of particles is generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the others, even when the particles are separated by a large distance.
- An entangled pair is a single quantum system in a superposition of equally possible states. The entangled state contains no information about the individual particles, only that they are in opposite states.
- If the state of one is changed, the state of the other is ***instantly*** adjusted to be consistent with quantum mechanical rules.
- If a measurement is made on one, the other will ***automatically*** collapse.
- Quantum entanglement is at the heart of the disparity between classical and quantum physics: *entanglement is a primary feature of quantum mechanics lacking in classical mechanics*.
- Entanglement is a joint characteristic of two or more quantum particles.
- Einstein called it "**spooky actions at a distance**"

Entanglement

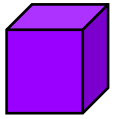




Suppose that two qubits are in states:



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



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

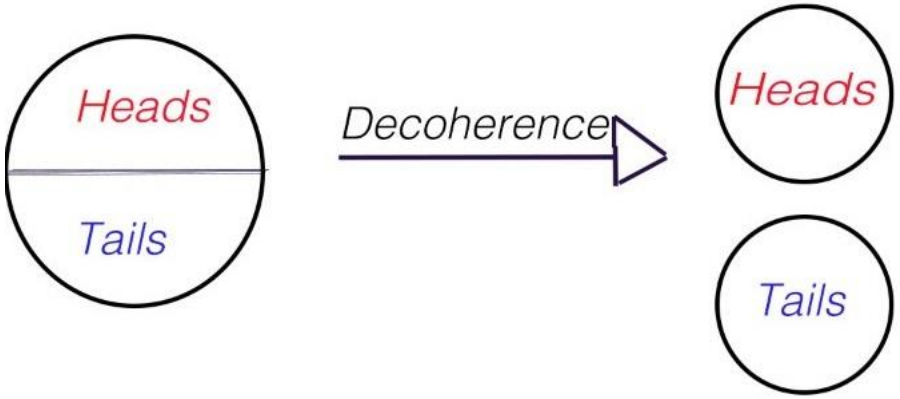
The state of the combined system is their ***tensor product***:

$$(\alpha|0\rangle+\beta|1\rangle)(\alpha'|0\rangle+\beta'|1\rangle)=\alpha\alpha'|00\rangle+\alpha\beta'|01\rangle+\beta\alpha'|10\rangle+\beta\beta'|11\rangle$$

Question: what are the states of the individual qubits for

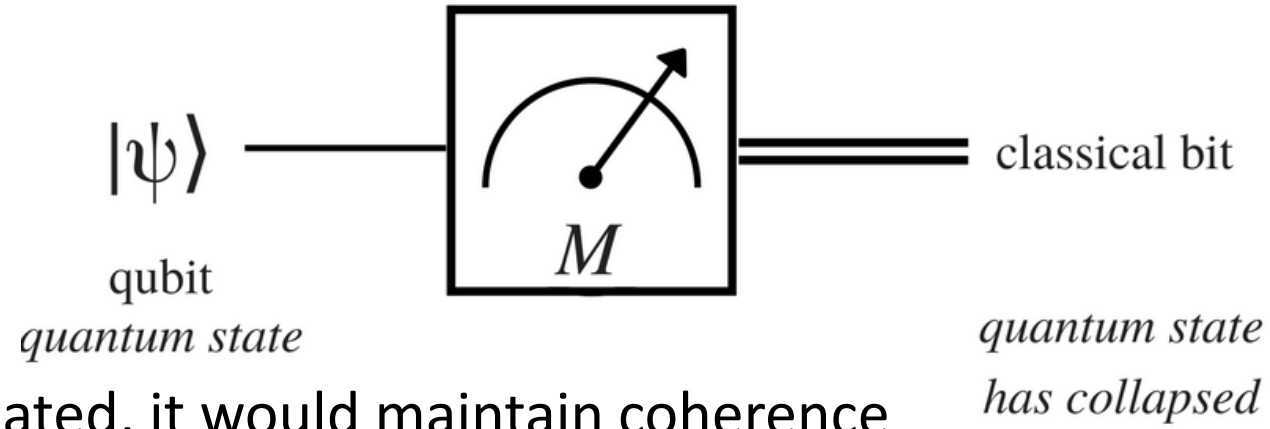
1. $\frac{1}{2}|00\rangle+\frac{1}{2}|01\rangle-\frac{1}{2}|10\rangle-\frac{1}{2}|11\rangle$ an ***independent*** state
2. $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$ an ***entangled*** state

Decoherence



- Quantum decoherence is the loss of superposition, because of the spontaneous interaction between a quantum system and its environment.
- Decoherence can be viewed as the loss of information from a system into the environment.
- The reason why quantum computers still have a long way to go because superposition and entanglement are extremely fragile states.
- Preventing decoherence remains the biggest challenge in building quantum computers.

Measurement



- If a quantum system were perfectly isolated, it would maintain coherence indefinitely, but it would be impossible to manipulate or investigate it.
- A quantum measure is a decoherence process.
- When a quantum system is measured, the wave function $|\psi\rangle$ collapses to a new state according to a probabilistic rule.
- If $|\psi> = \alpha_0 |0> + \alpha_1 |1>$, after measurement, either $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$, and these alternatives occur with certain probabilities of $|\alpha_0|^2$ and $|\alpha_1|^2$ with $|\alpha_0|^2 + |\alpha_1|^2 = 1$.
- A quantum measurement never produces $|\psi\rangle = \alpha_0 |0> + \alpha_1 |1>$.
- *Example*: Two qubits: $|\psi> = 0.316|00\rangle + 0.447|01\rangle + 0.548|10\rangle + 0.632|11\rangle$
  The probability to read the rightmost bit as 0 is $|0.316|^2 + |0.548|^2 = 0.4$

Quantum Gate

- A **quantum gate** (or **quantum logic gate**) is a basic quantum circuit operating on qubits.
- They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits
- Due to the normalization condition every gate operation *U* has to be unitary: $UU^* = I$
- The number of qubits in the input and output of the gate must be equal; a gate which acts on n qubits is represented by 2^n x 2^n unitary matrix
- Unlike many classical logic gates, quantum gates are reversible.

UNC INFORMATION TECHNOLOGY SERVICES

Unitary Matrix

- In linear algebra, a complex square matrix ***U*** is unitary if its conjugate transpose U^* is also its inverse, that is, if

$$U^*U = UU^* = I,$$

where *I* is the identity matrix.

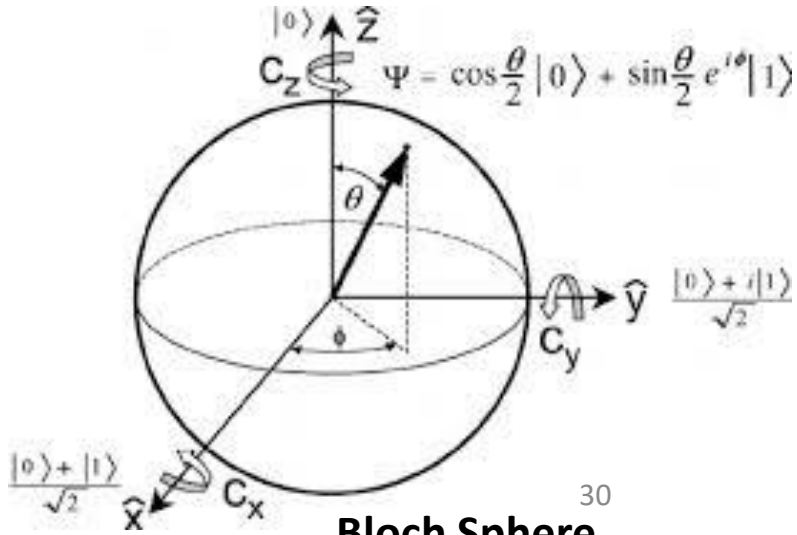
$$\begin{bmatrix} x' \\ y' \\ z' \\ w' \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ p_{31} & p_{32} & p_{33} & p_{34} \\ p_{41} & p_{42} & p_{43} & p_{44} \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

- Unitary transformations are linear transformations that preserve vector norm; In 2 dimensions, linear transformations preserve unit circle (rotations and reflections).
- Examples:

$$U = \begin{bmatrix} a & b \\ -e^{i\varphi}b^* & e^{i\varphi}a^* \end{bmatrix}, \qquad |a|^2 + |b|^2 = 1,$$

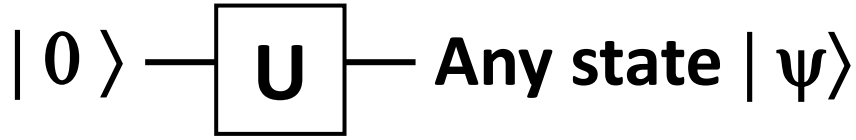
$$U = e^{i\varphi/2} \begin{bmatrix} e^{i\varphi_1}\cos\theta & e^{i\varphi_2}\sin\theta \\ -e^{-i\varphi_2}\sin\theta & e^{-i\varphi_1}\cos\theta \end{bmatrix},$$

which depends on parameters *a*, *b*, φ and θ.



Bloch Sphere

Single Qubit Gate



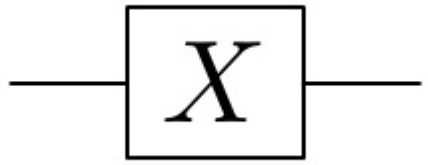
- **Pauli-X gate**

$$|0\rangle \rightarrow |1\rangle, \quad |1\rangle \rightarrow |0\rangle$$

Dirac notation

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Matrix representation



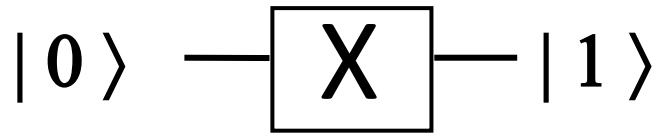
Circuit representation

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Rightarrow X\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0\cdot 1 + 1\cdot 0 \\ 1\cdot 1 + 0\cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow X\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0\cdot 0 + 1\cdot 1 \\ 1\cdot 0 + 0\cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- Acting on pure states becomes a **classical *NOT*** gate

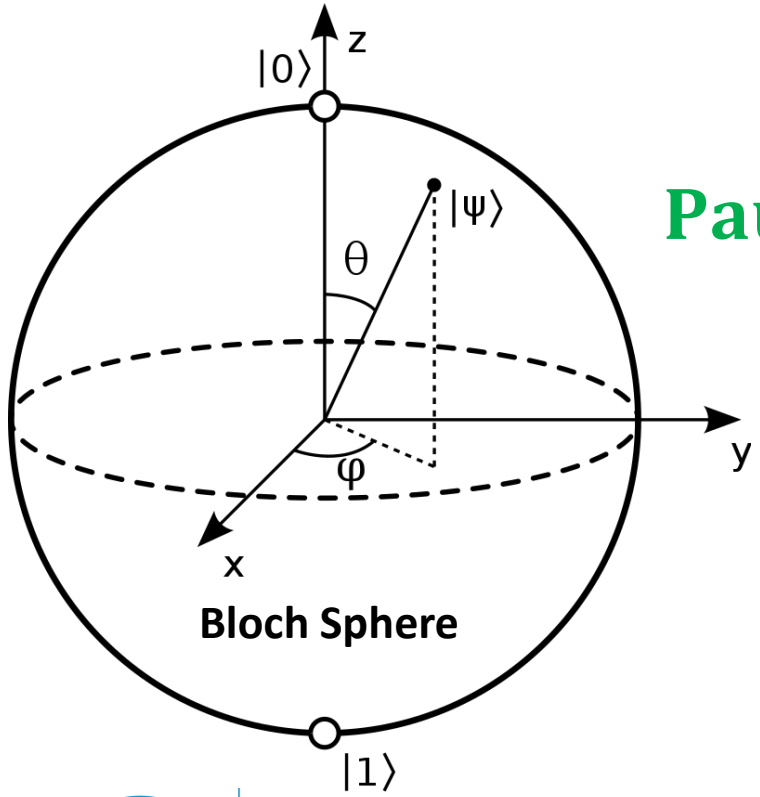
UNC INFORMATION TECHNOLOGY SERVICES



Single Qubit Gates

Dirac notation *Matrix representation* *Circuit representation*

Pauli Y – Gate $|0\rangle \rightarrow i|1\rangle, \quad |1\rangle \rightarrow -i|0\rangle$ $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$



…another gate with no classical equivalence

Pauli Z – Gates: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

S S

=

S Z

Phase **π/8 (T) gate** $P^2 = Z$

Hadamard Gate

- Acts on a single qubit
  - Corresponding to the Hadamard transform leading to *superposition*

Dirac notation

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$(|0\rangle + |1\rangle)/\sqrt{2} \rightarrow |0\rangle$$

$$(|0\rangle - |1\rangle)/\sqrt{2} \rightarrow |1\rangle$$

Unitary matrix

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Circuit representation

no classical equivalent!

UNC INFORMATION TECHNOLOGY SERVICES

The Amazing H-Gate

- After a qubit in state $|0\rangle$ or $|1\rangle$ has been acted upon by a *H* gate, the state of the qubit is an equal superposition of $|0\rangle$ and $|1\rangle$. Thus, the qubit goes from a deterministic state to a truly random state, i.e., if the qubit is now measured, we will measure $|0\rangle$ or $|1\rangle$ with equal probability.
- We see that *H* is its own inverse, that is, $H^{-1} = H$ or $H^2 = I$. Therefore, by applying *H* twice to a qubit we change nothing. This is amazing!
- By applying a randomizing operation to a random state produces a deterministic outcome!
- **One of the most important gates in quantum computing!**

UNC INFORMATION TECHNOLOGY SERVICES

CNOT Gate

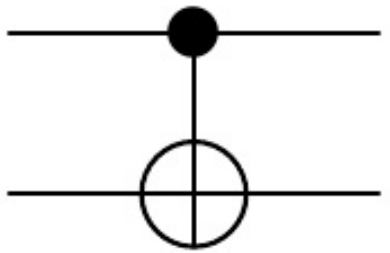
- ***C**ontrolled **NOT*** gate
- Acts on two qubits
  - If the control qubit is set to 0, target qubit is the same
  - If the control qubit is set to 1, target qubit is flipped

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

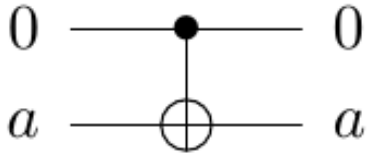
Matrix representation

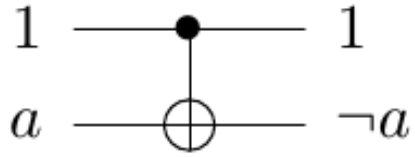
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Circuit representation



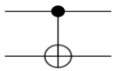
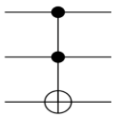
- Equivalent to classical gate operation XOR



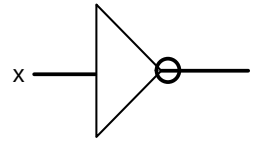


The output is “true” if and only if exactly one of the operands has a value of “true”.

Quantum vs. Classic Gates

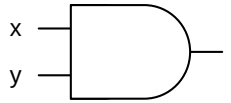
Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

NOT gate



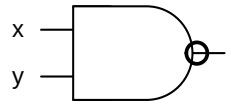
x	y
0	1
1	0

AND gate



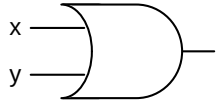
x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

NAND gate



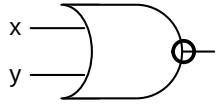
x	y	z
0	0	1
0	1	1
1	0	1
1	1	0

OR gate



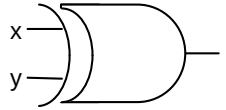
x	y	z
0	0	0
0	1	1
1	0	1
1	1	1

NOR gate



x	y	z
0	0	1
0	1	0
1	0	0
1	1	0

XOR gate

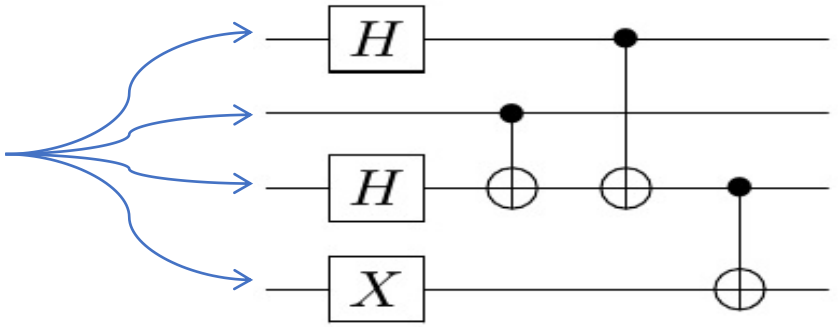


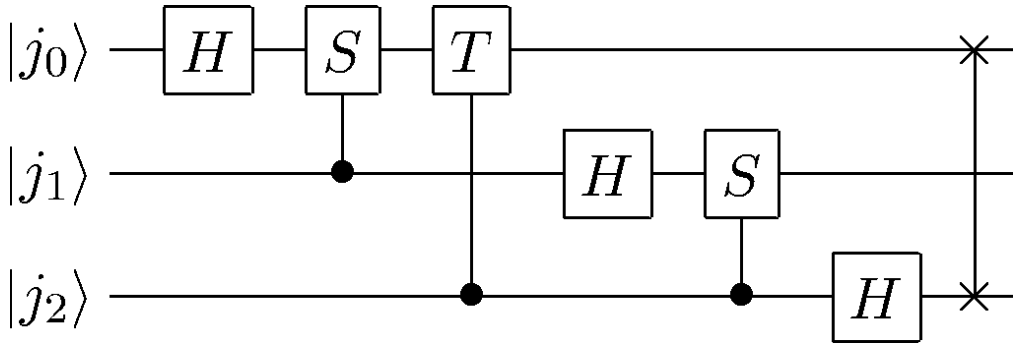
x	y	z
0	0	0
0	1	1
1	0	1
1	1	0

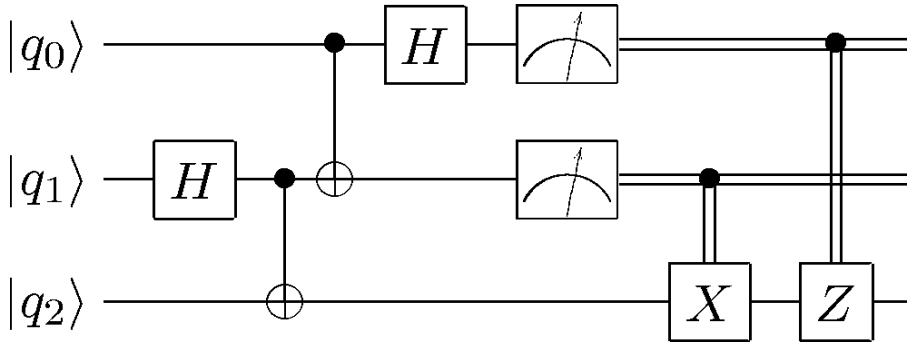
Quantum Circuit

- A quantum circuit is a model for quantum computation in which a computation is a sequence of quantum gates with *n*-qubit register linked by “wires”
- The circuit has fixed “width” corresponding to the number of qubits being processed

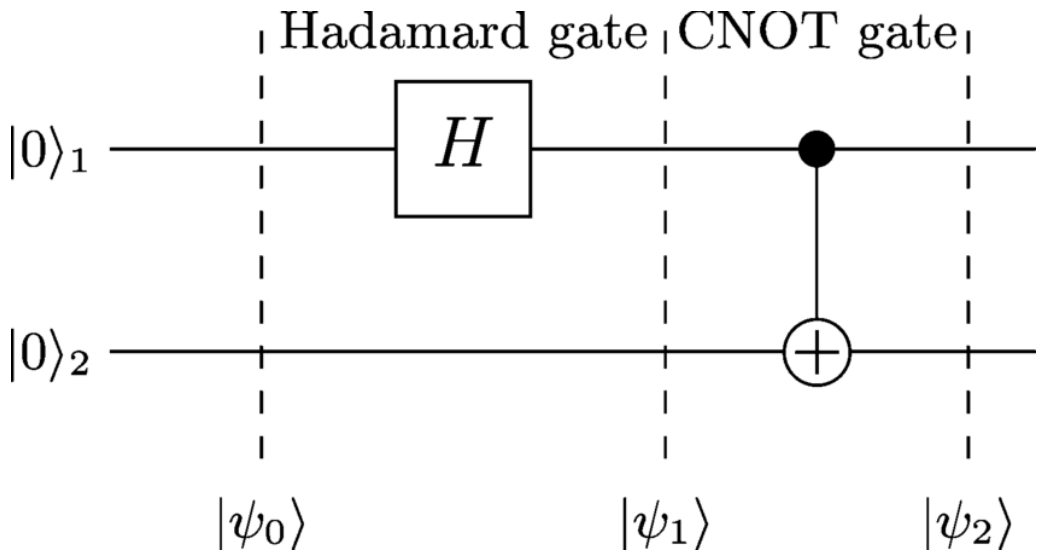
Unlike classical circuits, the same number of wires is going throughout the circuit

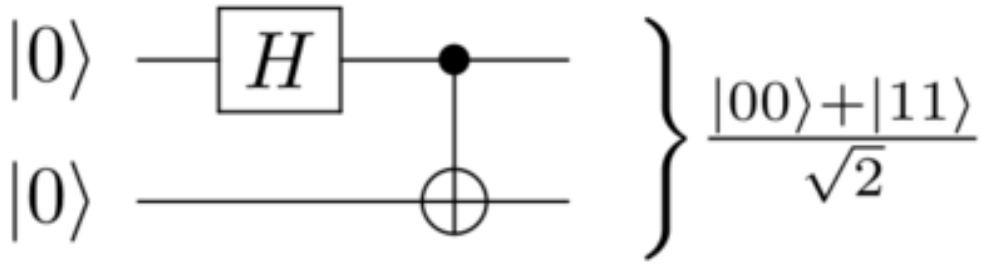






Bell State – How to Generate Entanglement?

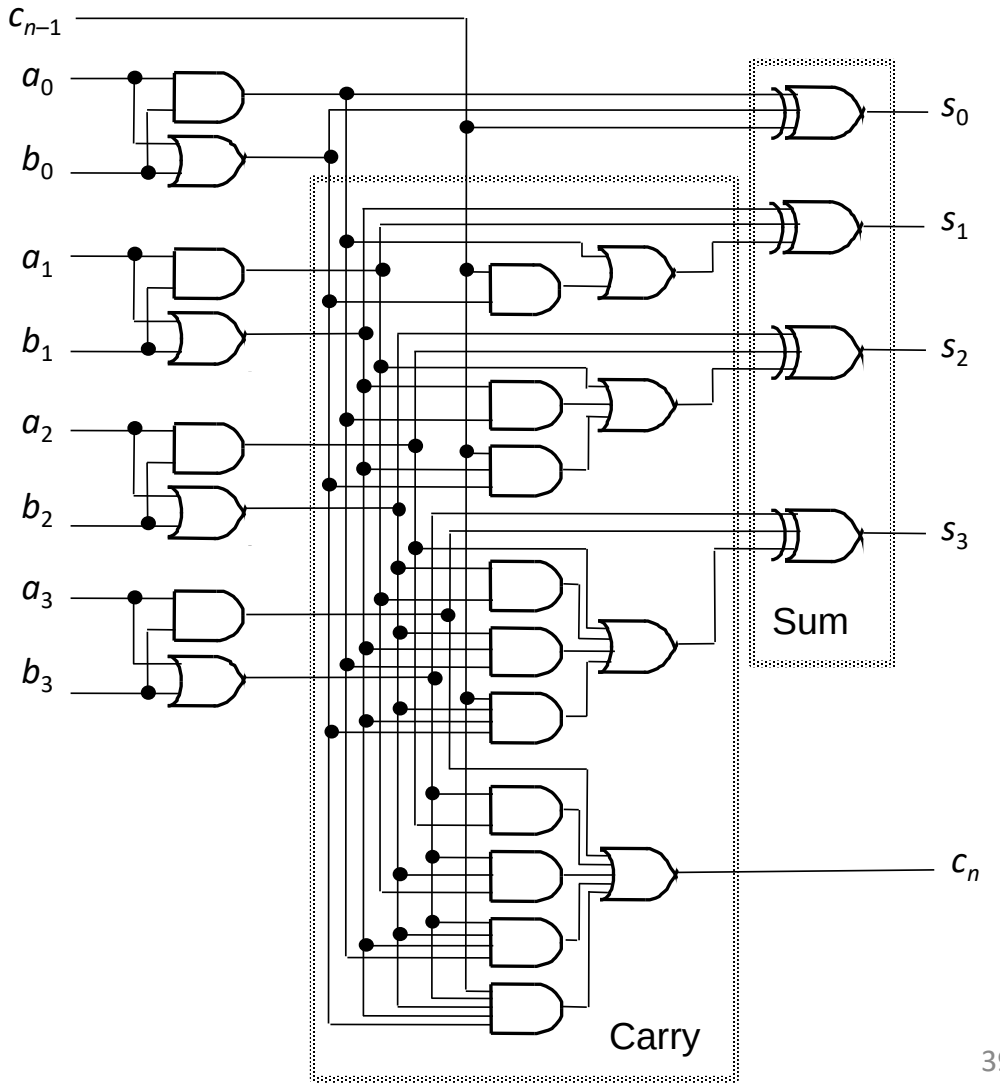




Using two qubits to generate an entanglement state, also called Bell state, with a Hadamard gate and a CNOT gate

Quantum vs. Classical Circuits

- Classical Logic Circuits
  - Circuit behavior is governed implicitly by classical physics
  - Signal states are simple bit vectors, e.g. *X* = 01010111
  - Operations are defined by Boolean Algebra
  - No restrictions exist on copying or measuring signals
  - Small well-defined sets of universal gate types, e.g. {NAND}, {AND,OR,NOT}, {AND,NOT}, etc.
  - Well developed CAD methodologies exist
  - Circuits are easily implemented in fast, scalable and macroscopic technologies such as CMOS

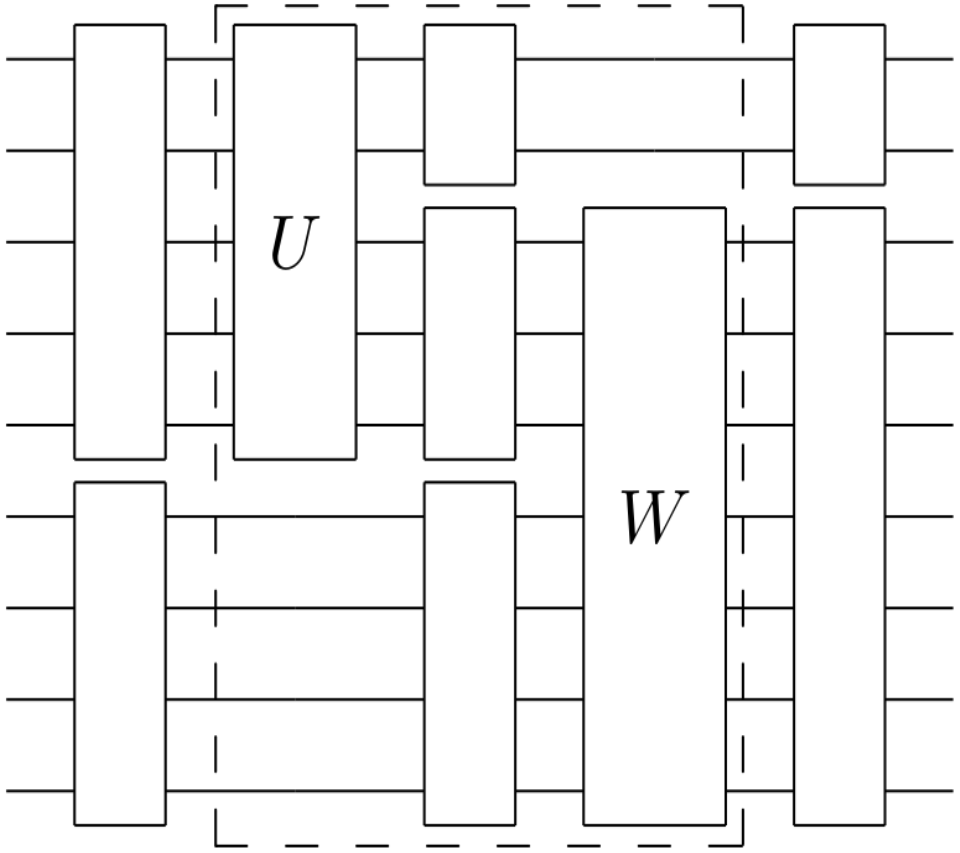


Quantum vs. Classical Circuits

- Quantum Logic Circuits
  - Circuit behavior is governed explicitly by quantum mechanics
  - Signal states are vectors interpreted as a superposition of binary "qubit" vectors with complex-number coefficients

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} c_i |i_{n-1} i_{n-1} \ldots i_0\rangle$$

  - Operations are defined by linear algebra over Hilbert Space and can be represented by unitary matrices with complex elements
  - Severe restrictions exist on copying and measuring signals
  - Many universal gate sets exist but the best types are not obvious
  - Circuits must use microscopic technologies that are slow, fragile, and not yet scalable, e.g., NMR



Quantum Algorithms

- It may be possible to solve a problem on a quantum system much faster (i.e., using fewer steps) than on a classical computer
- Factoring and searching are examples of problems where quantum algorithms are known and are faster than any classical ones
- Implications for cryptography, information security
- What makes a quantum algorithm potentially faster than any classical one?
  - **Quantum parallelism:** by using superpositions of quantum states, the computer is executing the algorithm on all possible inputs at once
  - **Dimension of quantum Hilbert space:** the "size" of the state space for the quantum system is exponentially larger than the corresponding classical system
  - **Entanglement capability:** different subsystems (qubits) in a quantum computer become entangled, exhibiting nonclassical correlations

UNC INFORMATION TECHNOLOGY SERVICES

Famous Quantum Algorithms

Algorithms	Classical steps	quantum logic steps
Fourier transform e.g.: - Shor's prime factorization - discrete logarithm problem - Deutsch Jozsa algorithm	$N \log(N) = n 2^n$ $N = 2^n$ - n qubits - N numbers	$\log^2(N) = n^2$ - hidden information! - Wave function collapse prevents us from directly accessing the information
Search Algorithms	N	$\sqrt{N}$
Quantum Simulation	c^N bits	kn qubits

UNC INFORMATION TECHNOLOGY SERVICES

Algebraic and Number Theoretic Algorithms	Factoring	Solving Exponential Congruences
	Discrete log	Matrix elements of Group Representations
	Principal Ideal	Verify Matrix Products
	Unit Group	Subset- sum
	Class Group	Decoding
	Gauss Sums	Constraint Satisfaction
		Quantum Cryptanalysis
Oracular Algorithms	Searching	Graph Collision
	Abelian Hidden Subgroup	Matrix Commutativity
	Non-Abelian Hidden Subgroup	Group Commutativity
	Bernstein-Vazirani	Hidden Nonlinear Structures
	Deutsch-Jozsa	Center of Radial Function
	Formula Evaluation	Group Order and Membership
	Gradients, Structured Search, and Learning Polynomials	Group Isomorphism
	Hidden Shift	Statistical Difference
	Polynomial interpolation	Finite Rings and Ideals
	Pattern matching	Counterfeit Coins
	Linear Systems	Matrix Rank
	Ordered Search	Matrix Multiplication over Semirings
	Graph Properties in the Adjacency Matrix Model	Subset Finding
	Graph Properties in the Adjacency List Model	Search and Wildcards
	Welded Tree	Network flows
	Collision Finding and Element Distinctness	Electrical Resistance
		Machine Learning
		Junta Testing and Group Testing
Approximation and Simulation Algorithms	Quantum Simulation	Semidefinite Programming
	Knot Invariants	Zeta Functions
	Three-manifold Invariants	Weight Enumerators
	Partition Functions	Simulated Annealing
	Adiabatic Algorithms	String Rewriting
	Quantum Approximate Optimization	Matrix Powers

Quantum Algorithm Zoo: https://quantumalgorithmzoo.org/

More Quantum Algorithms

Class	Problem/Algorithm	Paradigm Used
Inverse Function	Grover's Algorithm	GO
	Bernstein-Vazirani	n.a
Number-theoretic Applications	Shor's Factoring Algorithm	QFT
Algebraic Applications	Linear Systems	HHL
	Matrix Element Group Representations	QFT
	Matrix Product Verification	GO
	Subgroup Isomorphism	QFT
	Persistent Homology	GO,QFT
Graph Applications	Graph Properties Verification	GO
	Minimum Spanning Tree	GO
	Maximum Flow	GO
	Approximate Quantum Algorithms	SIM
Learning Applications	Quantum Principal Component Analysis (PCA)	QFT
	Quantum Support Vector Machines (SVM)	QFT
	Partition Function	QFT
Quantum Simulation	Schrodinger Equation Simulation	SIM
	Transverse Ising Model Simulation	VQE
Quantum Utilities	State Preparation	n.a
	Quantum Tomography	n.a.
	Quantum Error Correction	n.a.

Quantum Programming

- There is already a number of programming languages adapted for quantum computing
- The purpose of quantum programming languages is to provide a tool for researchers, not a tool for programmers
- QCL is an example of such language
- IBM QISKit (Quantum Information Science Kit) is another example

UNC
INFORMATION
TECHNOLOGY SERVICES

Quantum Programming

- **QCL** (**Q**uantum **C**omputation **L**anguage)

```
/* Remove "//" if starting interpreter with -n option */
// extern operator H(qureg q);

procedure FlipCoin() {
  qureg q[1]; int x;

  reset;
  H(q);
  measure q, x;
  if x == 1  { print "Heads"; }
  if x == 0  { print "Tails"; }
  reset;
}
```

C-like syntax

allows combining of quantum and classical code

http://tph.tuwien.ac.at/~oemer/qcl.html

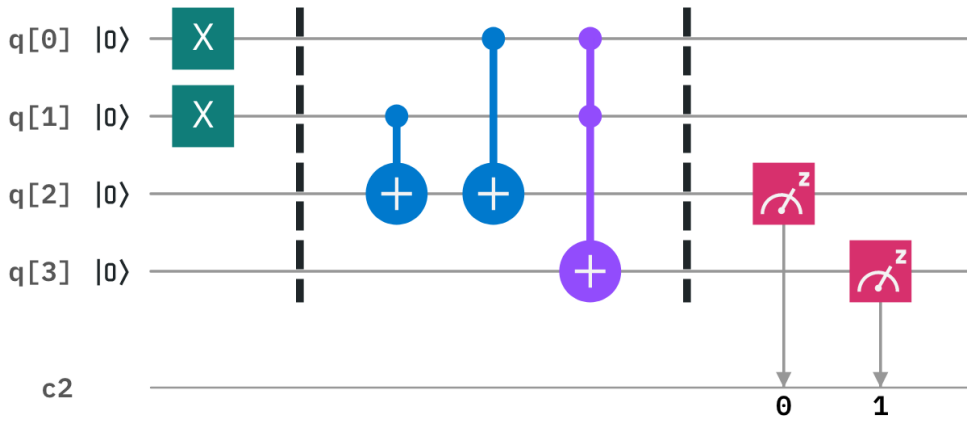
UNC INFORMATION TECHNOLOGY SERVICES

Quantum Programming

Qiskit
Elements for building a quantum future

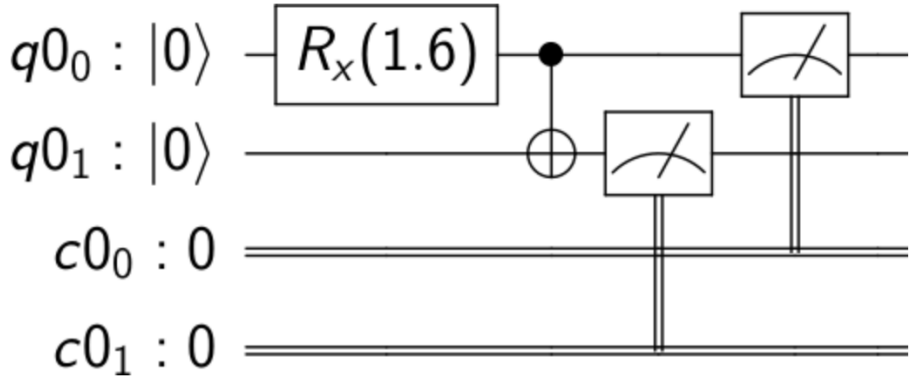
- **QISKit** (**Q**uantum **I**nformation **S**cience **Kit**)

Qiskit is an open-source framework for quantum computing. It provides tools for creating and manipulating quantum programs and running them on prototype quantum devices on IBM Quantum Experience over Cloud-based access




```
In [7]: from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
        from qiskit.tools.visualization import circuit_drawer
        import numpy as np

        qr = QuantumRegister(2)
        cr = ClassicalRegister(2)
        qp = QuantumCircuit(qr,cr)

        qp.rx( np.pi/2,qr[0])
        qp.cx(qr[0],qr[1])

        qp.measure(qr,cr)

        circuit_drawer(qp)
```

Out[7]:



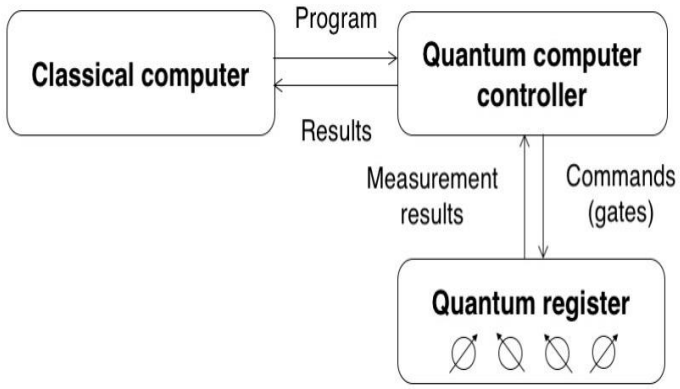

```
In [1]: from qiskit import *

In [2]: qr = QuantumRegister(2)
        cr = ClassicalRegister(2)

In [3]: c = QuantumCircuit(qr, cr)    # c = QuantumCircuit(2,2)
```

Name	Tagline	Programming language	Licence	Supported OS
Cirq	Framework for creating, editing, and invoking Noisy Intermediate Scale Quantum (NISQ) circuits.	Python	Apache-2.0	Windows, Mac, Linux
Cliffords.jl	Efficient calculation of Clifford circuits in Julia.	Julia	MIT	Windows, Mac, Linux
dimod	Shared API for Ising/quadratic unconstrained binary optimization samplers.	Python	Apache-2.0	Windows, Linux, Mac
dwave-system	Basic API for easily incorporating the D-Wave system as a sampler in the D-Wave Ocean software stack.	Python	Apache-2.0	Linux, Mac
FermiLib	Open source software for analyzing fermionic quantum simulation algorithms.	Python	Apache-2.0	Windows, Mac, Linux
Forest (pyQuil & Grove)	Simple yet powerful toolkit for writing hybrid quantum-classical programs.	Python	Apache-2.0	Windows, Mac, Linux
OpenFermion	The electronic structure package for quantum computers.	Python	Apache-2.0	Windows, Mac, Linux
ProjectQ	An open source software framework for quantum computing.	Python, C++	Apache-2.0	Windows, Mac, Linux
PyZX	Python library for quantum circuit rewriting and optimisation using the ZX-calculus.	Python	GPL-3.0	Windows, Mac, Linux
QGL.jl	A performance orientated QGL compiler.	Julia	Apache-2.0	Windows, Mac, Linux
Qbsolv	Decomposing solver that finds a minimum value of a large quadratic unconstrained binary optimization problem by splitting it into pieces.	C	Apache-2.0	Windows, Linux, Mac
Qiskit Terra & Aqua	Quantum Information Science Kit for writing experiments, programs, and applications.	Python, C++	Apache-2.0	Windows, Mac, Linux
Qiskit Tutorials	A collection of Jupyter notebooks using Qiskit.	Python	Apache-2.0	Windows, Mac, Linux
Qiskit.js	Quantum Information Science Kit for JavaScript.	JavaScript	Apache-2.0	Windows, Mac, Linux
Qrack	Comprehensive, GPU accelerated framework for developing universal virtual quantum processors.	C++	GPL-3.0	Linux, Mac
Quantum Fog	Python tools for analyzing both classical and quantum Bayesian networks.	Python	BSD-3-Clause	Windows, Mac, Linux
Quantum++	A modern C++11 quantum computing library.	C++, Python	MIT	Windows, Mac, Linux
Qubiter	Python tools for reading, writing, compiling, simulating quantum computer circuits.	Python, C++	BSD-3-Clause	Windows, Mac, Linux
Quirk	Drag-and-drop quantum circuit simulator for your browser to explore and understand small quantum circuits.	JavaScript	Apache-2.0	Windows, Mac, Linux
reference-qvm	A reference implementation for a Quantum Virtual Machine in Python.	Python	Apache-2.0	Windows, Mac, Linux
ScaffCC	Compilation, analysis and optimization framework for the Scaffold quantum programming language.	C++, Objective C, LLVM	BSD-2-Clause	Linux, Mac
Strawberry Fields	Full-stack library for designing, simulating, and optimizing continuous variable quantum optical circuits.	Python	Apache-2.0	Windows, Mac, Linux
XACC	eXtreme-scale Accelerator programming framework.	C++	Eclipse PL-1.0	Windows, Mac, Linux
XACC VQE	Variational quantum eigensolver built on XACC for distributed, and shared memory systems.	C++	BSD-3-Clause	Windows, Mac, Linux

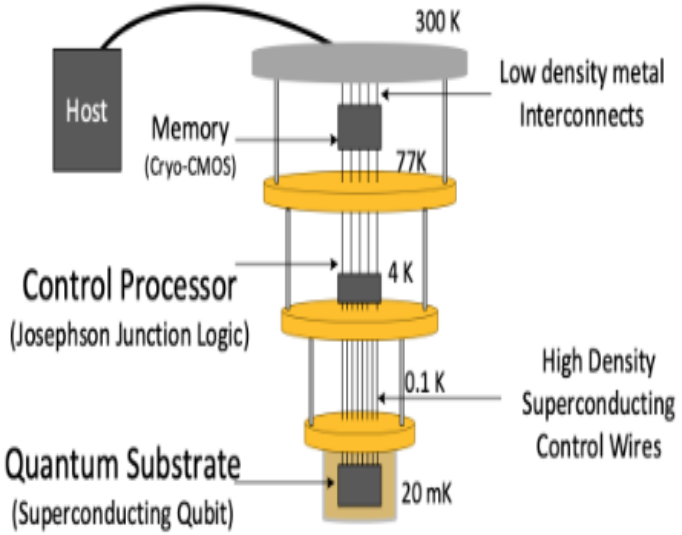
https://doi.org/10.1371/journal.pone.0208561.t001

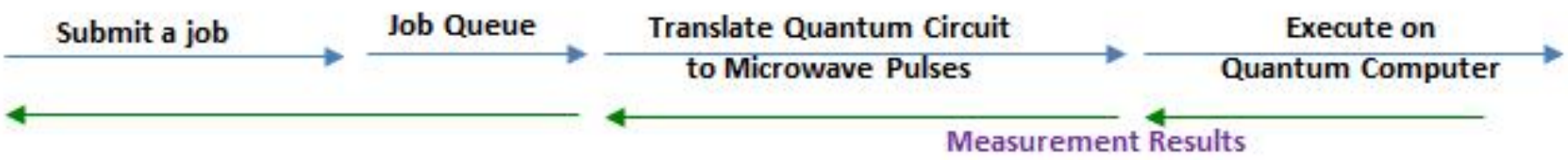
Quantum Programming Languages

How does a quantum computer work?



Quantum Computer Architecture

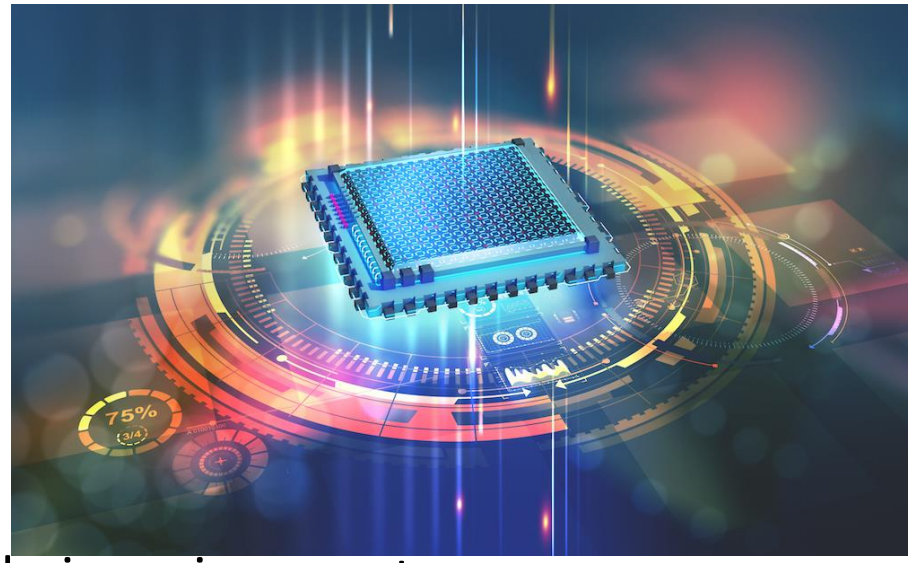


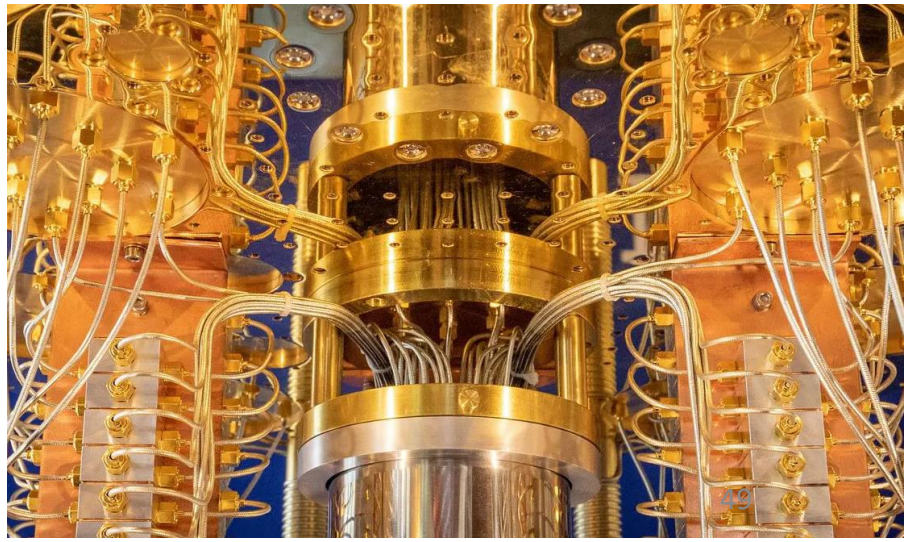


The flow of submitting a job from a classical computer to a quantum computer, executing the job, and returning quantum measurement results to the classical computer.

Design of Quantum Computer

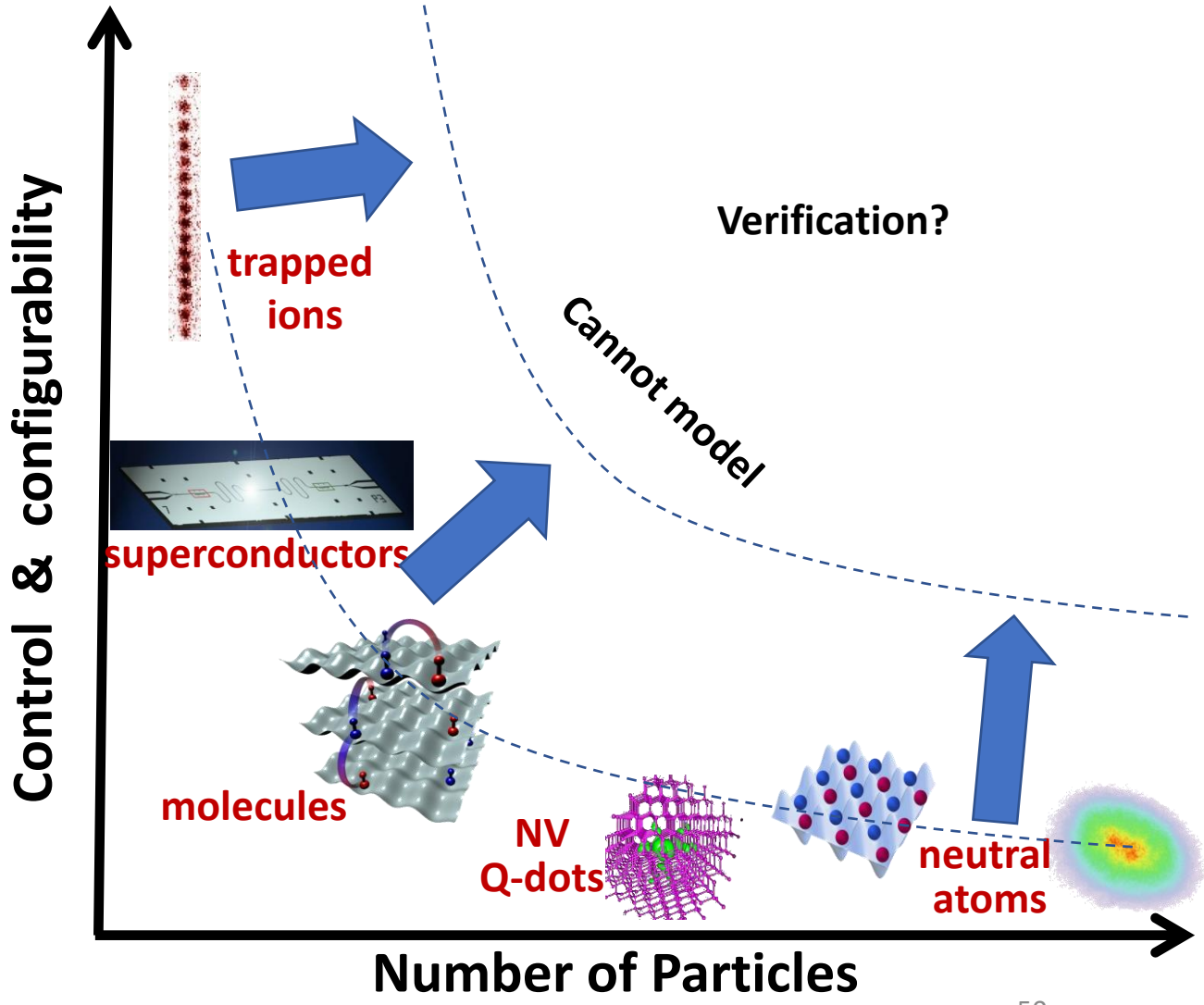
- Requirements
  - Qubit implementation itself;
  - Control of unitary evolution;
  - Initial state preparation (qubits);
  - Measurement of the final state(s).
- Other Considerations
  - Systems have to be almost completely isolated from their environment
  - The coherent quantum state has to be preserved
  - Decoherence times have to be very long
  - Performing operations on several qubits in parallel
  - Physical system with two uniquely addressable states
  - A universal set of quantum gates
  - Ability to entangle two qubits





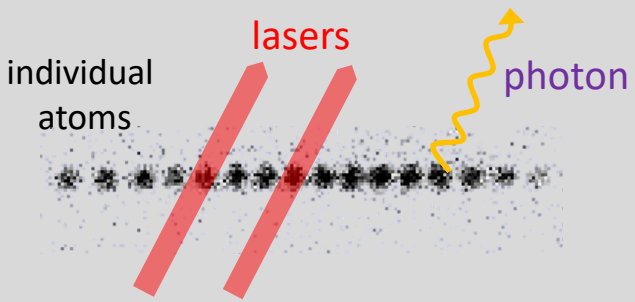
Implementation of Quantum Hardware

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atom
- Linear optics
- Nitrogen vacancies in diamond
- Electrons in liquid He
- Superconducting Josephson junctions
  - charge qubits; flux qubits; phase qubits
- Quantum Hall qubits
- Coupled quantum dots
  - spin, charge, excitons
- Spin spectroscopies, impurities in semiconductors



Leading Quantum Computer Hardware Candidates

Trapped Atomic Ions



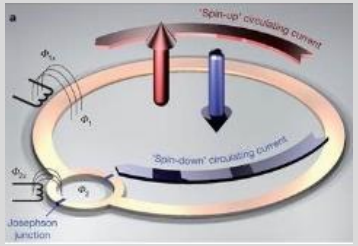
Atomic qubits connected through laser forces on motion or photons

FEATURES & STATE-OF-ART
- very long (>>1 sec) memory
- 5-20 qubits demonstrated
- **atomic qubits all identical**
- **connections reconfigurable**

CHALLENGES
- lasers & optics
- high vacuum
- 4K cryogenics
- **engineering needed**

Investments:	IARPA	Lockheed
	DoD	Honeywell
	Sandia	UK Gov't

Superconducting Circuits



Superconducting qubit: right or left current

FEATURES & STATE-OF-ART
- connected with wires
- fast gates
- 5-10 qubits demonstrated
- **printable circuits and VLSI**

CHALLENGES
- short (10^{-6} sec) memory
- 0.05K cryogenics
- **all qubits different**
- **not reconfigurable**

LARGE Investments:	IARPA	Lincoln Labs
	DoD	Intel/Delft
	Google/UCSB	IBM

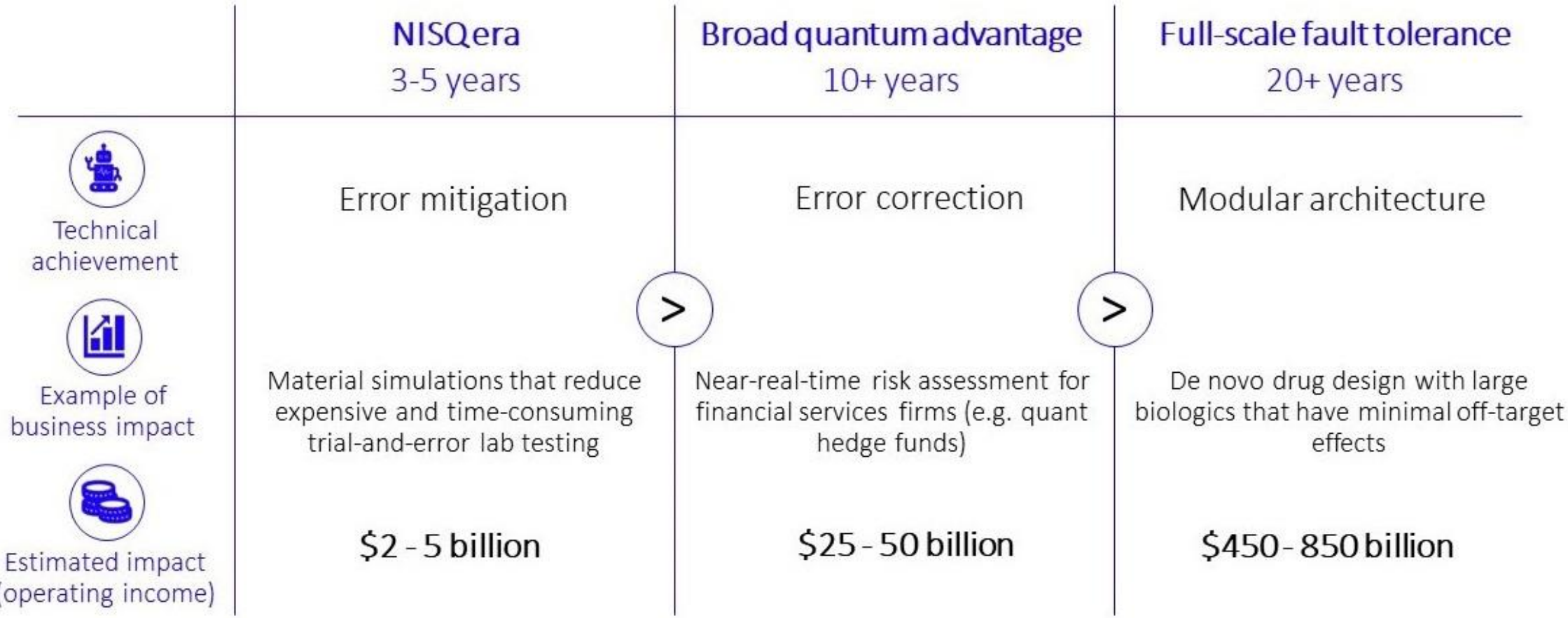
- NV-Diamond and other solid state "atoms"
- Atoms in optical lattices
- Semiconductor gated quantum dots

NISQ – Noisy Intermediate-Scale Quantum Era

- John Preshill of CalTech introduced this terminology in 2018
  - https://arxiv.org/abs/1801.00862
- Quantum computers can do things that classical computers can’t
- But they won't be big enough to provide fault-tolerant implementations of the algorithms we know about.
- Noisy because we don't have enough qubits to spare for error correction, and so we'll need to directly use the imperfect qubits at the physical layer.
- And 'Intermediate-Scale' because of their small (but not too small) qubit number (50-100 qubits).

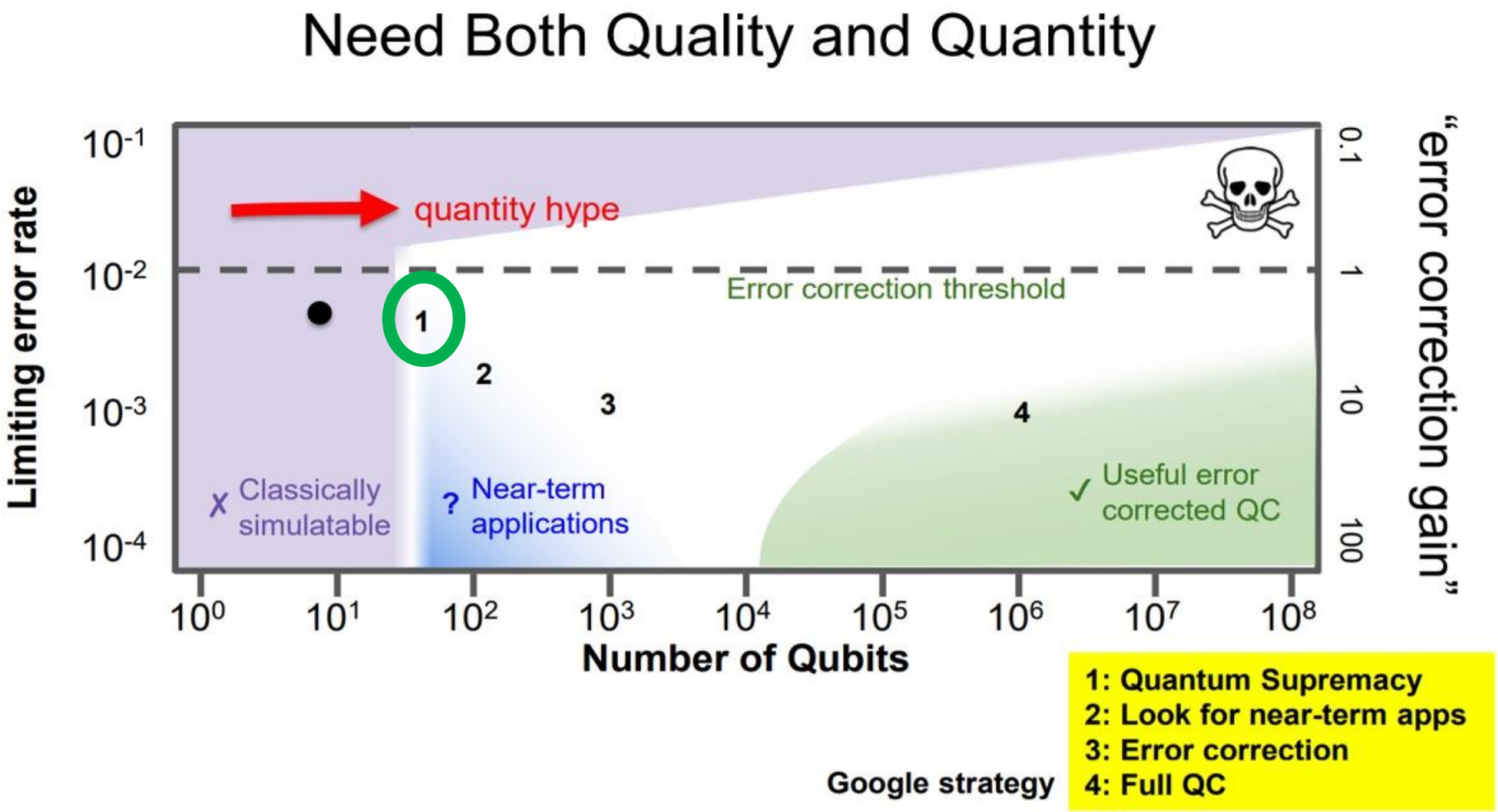
UNC
INFORMATION
TECHNOLOGY SERVICES

NISQ – Noisy Intermediate-Scale Quantum Era



UNC INFORMATION TECHNOLOGY SERVICES

Roadmap of Quantum Computers



Quantum Volume

- **Quantum volume V_Q** is a metric that measures the capabilities and error rates of a quantum computer.
- Defined by Nikolaj Moll *et al. Quantum Sci. Technol.* **3**, 030503 (2018).
- It depends on the number of qubits *N* as well as the number of steps that can be executed, the circuit depth *d*: $\tilde{V}_Q = \min[N, d(N)]^2$.
- IBMs modified the quantum volume definition: $\log_2 V_Q = \arg\max_{n \leq N} \{\min[n, d(n)]\}$

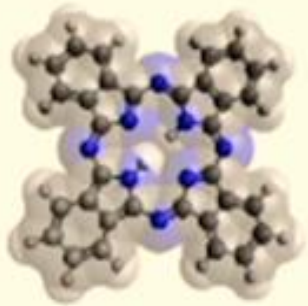
Date	Quantum volume (circuit size)	Manufacturer	Notes
2020, January	32 (5×5)	IBM	"Raleigh" (28 qubits)
2020, June	64 (6×6)	Honeywell	6 qubits
2020, August	64 (6×6)	IBM	27 qubits
2020, November	128 (7×7)	Honeywell	"H1" (10 qubits)

Applications of Quantum Computers

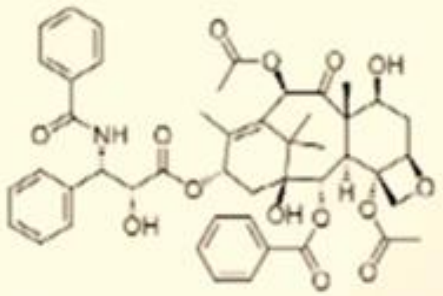
TIME

"Quantum Will Change Everything"

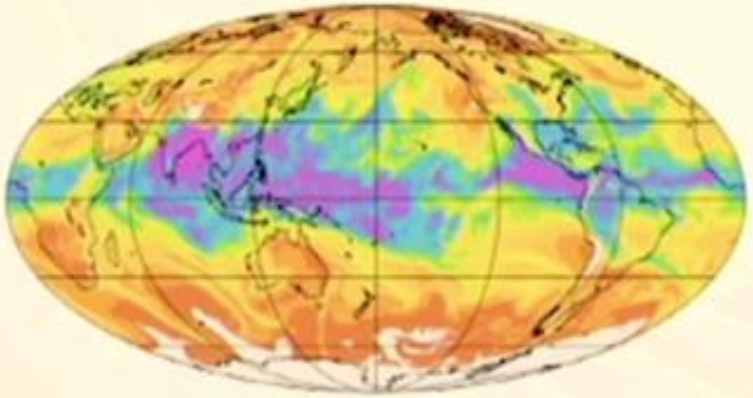
Travel & Logistics



Chemistry



Pharmacology



Climate Modeling

Financial Analysis

Cryptography

Application 1. Quantum Factoring

P. Shor (1994)

A quantum computer can factor numbers **exponentially faster** than classical computers

15 = 3 × 5 (…easy)

3864788462100938762143232563 1 = ? × ?

Importance: cryptanalysis

public key cryptography relies on inability to factor large numbers

Best classical algorithm:	Shor's quantum algorithm:
10^{24} steps	10^{10} steps
On classical THz computer:	On quantum THz computer:
150,000 years	<1 second

Application 2: Quantum Search

L. Grover (1997)

A quantum computer can find a marked entry in an unsorted database **quadratically faster** than classical computers

(e.g., given a phone number, finding the owner's name in a phonebook)

Importance: "satisfiability" problems

- fast searching of big data
- inverting complex functions
- determining the median or other global properties of data
- pattern recognition; machine vision

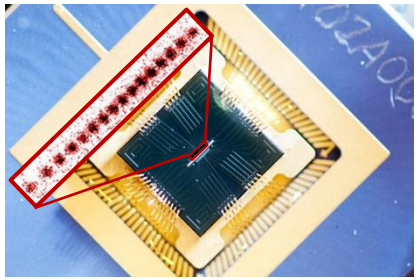
UNC INFORMATION TECHNOLOGY SERVICES

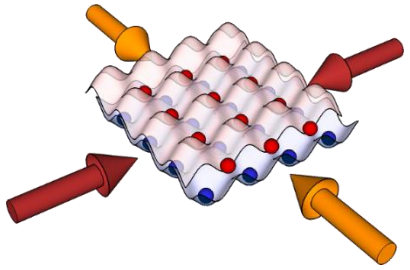
Application 3: Quantum Simulation

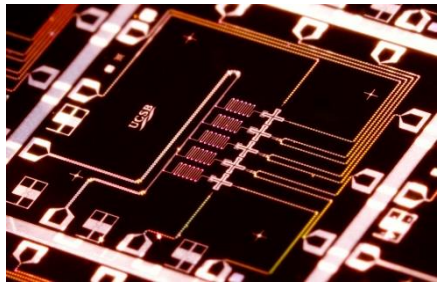
Quantum modelling is hard: *N* quantum systems require solution to 2^N coupled eqns

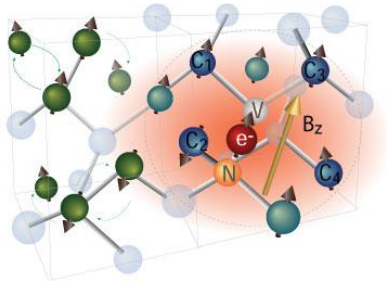
$$i\hbar\frac{\partial\Psi}{\partial t} = H\Psi$$

Alternative approach: Implement model of interacting system on a ***quantum simulator***, or "standard" set of qubits with programmable interactions


Atomic ions

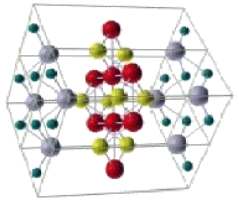

Trapped atoms

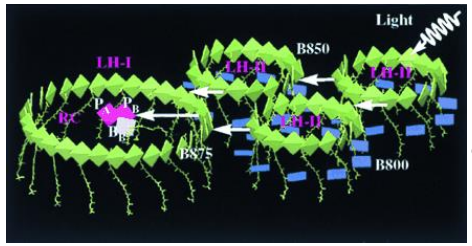

Superconductors



NV-diamond

Quantum Material Design Understand exotic material properties or design new quantum materials from the bottom up





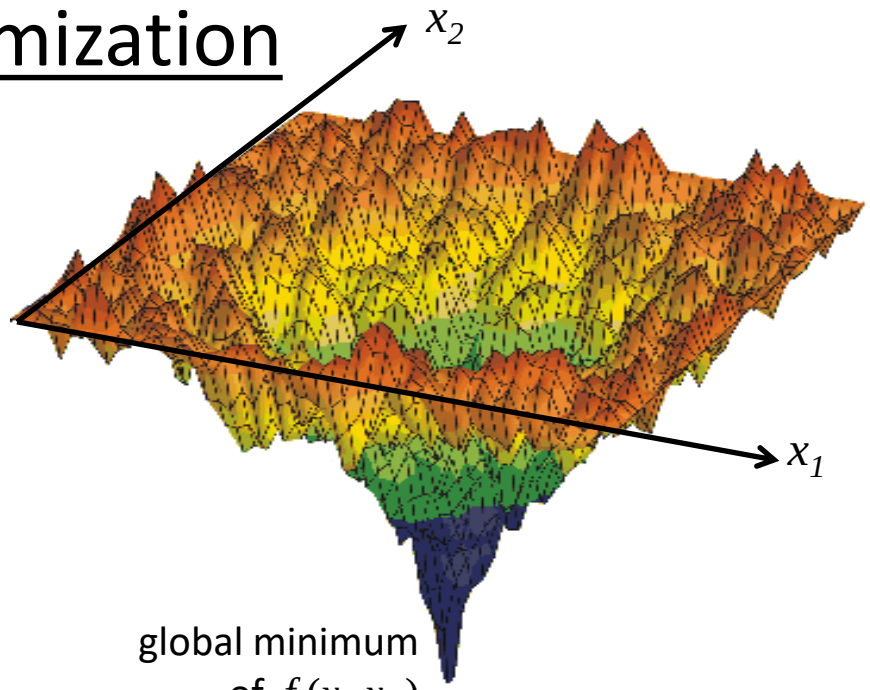
Energy and Light Harvesting Use quantum simulator to program QCD lattice gauge theories, test ideas connecting cosmology to information theory (AdS-CFT etc..)

Quantum Field Theories Program QCD lattice gauge theories, test ideas connecting cosmology to information theory (AdS-CFT etc..)

Application 4: Quantum Optimization

Minimizing complex (nonlinear) functions by "simultaneously sampling" entire space through quantum superposition

Relevant to
- Logistics
- Operations Research
- VLSI design
- Finance



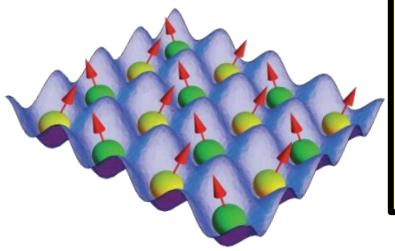
global minimum of $f(x_1,x_2)$

Example: quadratic optimization

Minimize

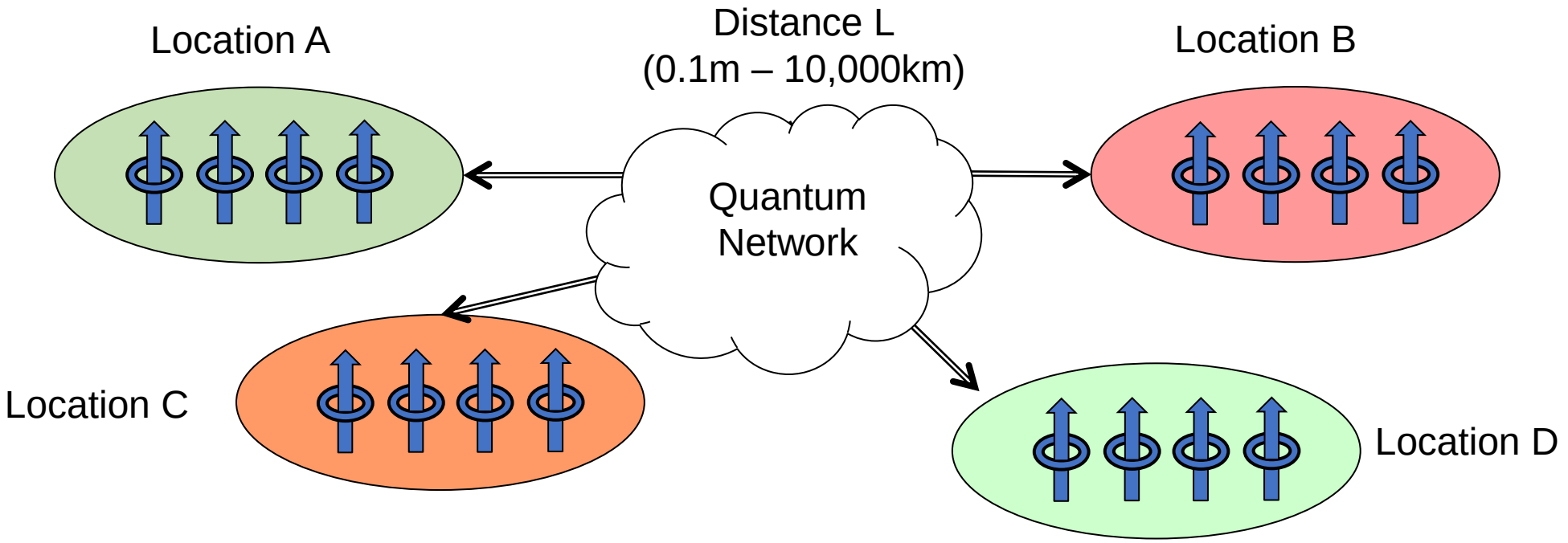
$$f(x_1, x_2, \ldots) = \sum_{i<j} q_{ij} x_i x_j + \sum_i c_i x_i$$

this function maps to energy of quantum magnetic network



Killer Application?
- could crack a large class of intractable problems: factoring, "traveling salesman" problem, etc..
- BUT not known if there is always a quantum speedup

Application 5: Quantum Networks



Uses of a quantum network

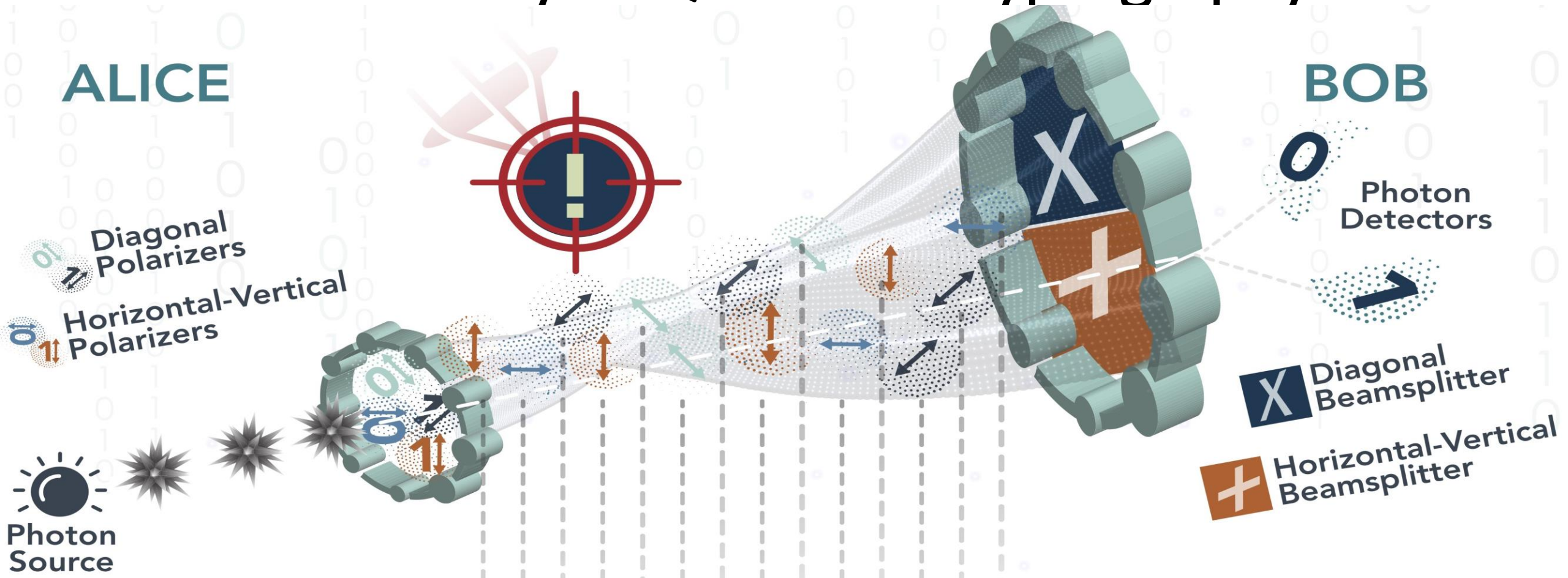
- Secret key generation: cryptography
- Certifiable random number generation
- Quantum repeaters (“amplifiers”)
- Distributed quantum entanglement for optimal decision making
- *Large-scale quantum computing*

Case Study 1: Quantum Cryptography

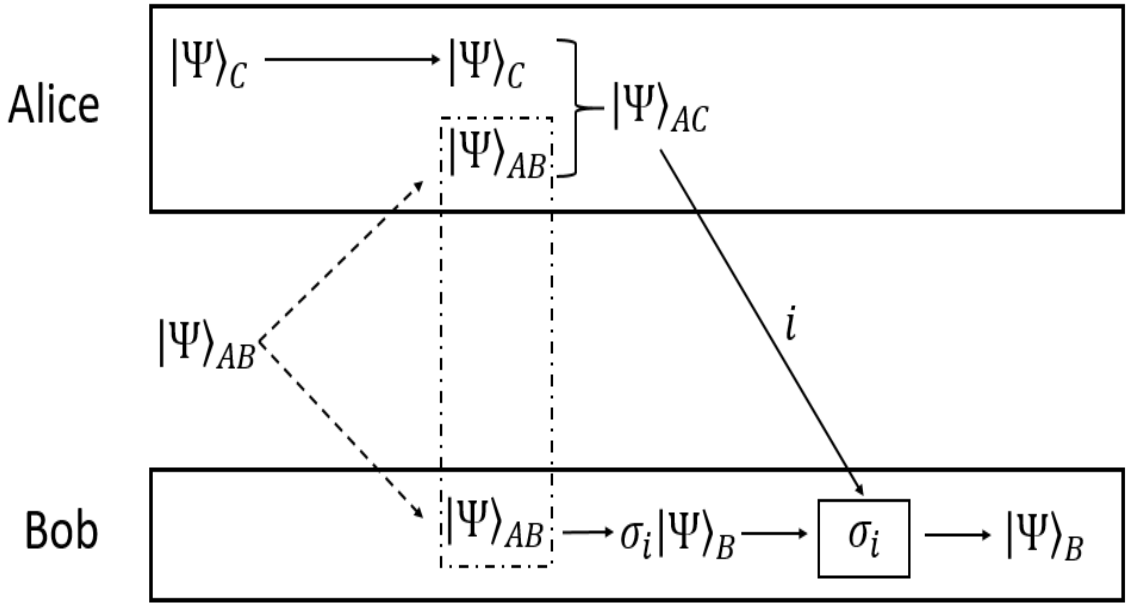
- Alice and Bob wish to establish a secret key, but the communication lines between them may be compromised. Alice sends random q-bits to Bob. For each one, she picks either basis {|0>,|1>} or {|0>±|1>}.
- Bob randomly chooses a basis to measure the bit in. If he guesses wrong, he gets a random bit.
- If an eavesdropper Eve tries to intercept the q-bits, she doesn't know (any more than Bob) the basis in which they were prepared. If she guesses wrong, the bit she passes on to Bob will have been disturbed.
- After N bits have been sent, Alice and Bob compare notes as to which bases they used. All bits where their bases didn't match are discarded. The remainder should be perfectly correlated.

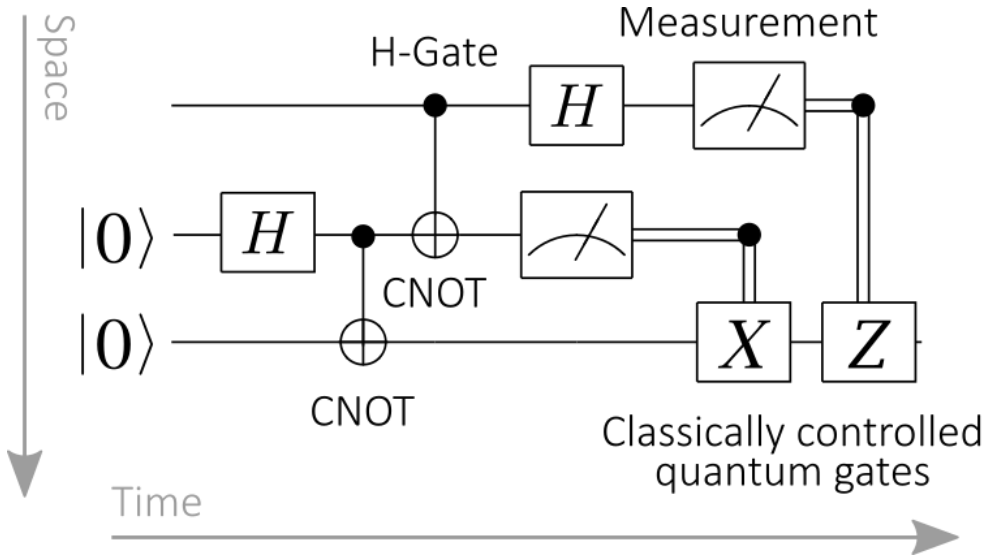
UNC INFORMATION TECHNOLOGY SERVICES

Case Study 1: Quantum Cryptography



Alice's Bit Sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0		
	+	X	+	+	X	X	+	+	X	+	X	X	+	+	Bob's Detection	
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob's Measurements	
Sifted Key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted Key	





Quantum Teleportation Explained

- Alice's measurement disentangles A and B and entangles A and C. Depending on what particular entangled state Alice sees, Bob will know exactly how B was disentangled, and can manipulate B to take the state that C had originally. Thus, the state C was "teleported" from Alice to Bob, who now has a state that looks identical to how C originally looked.
- It is important to note that state C is not preserved in the processes: the **no-cloning** and **no-deletion** theorems of quantum mechanics prevent quantum information from being perfectly replicated or destroyed.
- Bob receives a state that looks like C did originally, but Alice no longer has the original state C in the end, since it is now in an entangled state with A.

1) Generate an entangled pair of electrons with spin states A and B, in a particular Bell state
2) Separate the entangled electrons, sending A to Alice and B to Bob.
3) Alice measures the "Bell state" (described below) of A and C, entangling A and C.
4) Alice sends the result of her measurement to Bob via some classical method of communication.
5) Bob measures the spin of state B along an axis determined by Alice's measurement

Case Study 2: Shor Algorithm of Factoring

- Theorem of Number Theory
  - If $a \neq \pm b \pmod{N}$ but $a^2 \equiv b^2 \pmod{N}$, then gcd(*a*+*b*,*N*) is a factor of *N*.

- To Factor N on a quantum computer:
  - Select *x* coprime to *N*
  - Use QFT on quantum computer to find the period of
    $$f(s) = x^s \bmod N$$
  - Use order of *x* to compute possible factors of N.
  - Check if they work; If not, rerun.
- Best classical algorithm takes time $O(\exp(n^{1/3}))$

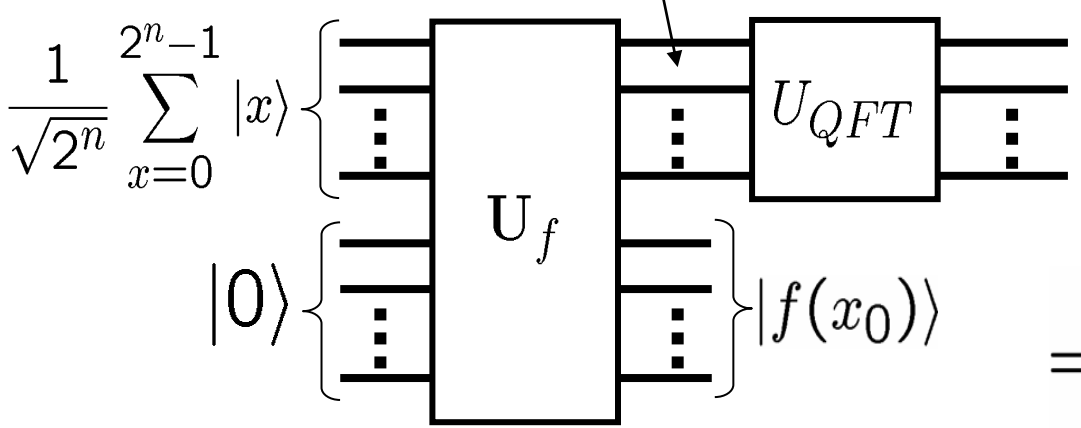
  But Shor's quantum algorithm takes time $O(n^3 \log n)$

Peter Shor 1994

Quantum Fourier Transform (QFT)

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \omega_N^{xy} |y\rangle\langle x| \qquad U_{QFT}^{\dagger} = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \omega_N^{-xy} |x\rangle\langle y|$$

$$|\psi(x_0)\rangle = \frac{1}{\sqrt{2^n/l}} \sum_{j=0}^{2^n/l-1} |x_0 + jl\rangle$$



$$\frac{1}{\sqrt{2^{2n}/l}} \sum_{p=0}^{2^n-1} \sum_{j=0}^{2^n/l-1} \exp\left(\frac{2\pi i p(x_0 + jl)}{2^n}\right) |p\rangle$$

$$= \frac{1}{\sqrt{l}} \sum_{p=0|pl=0 \bmod 2^n}^{2^n-1} e^{\frac{2\pi i p x_0}{2^n}} |p\rangle$$

$$f(s) = x^s \bmod N$$

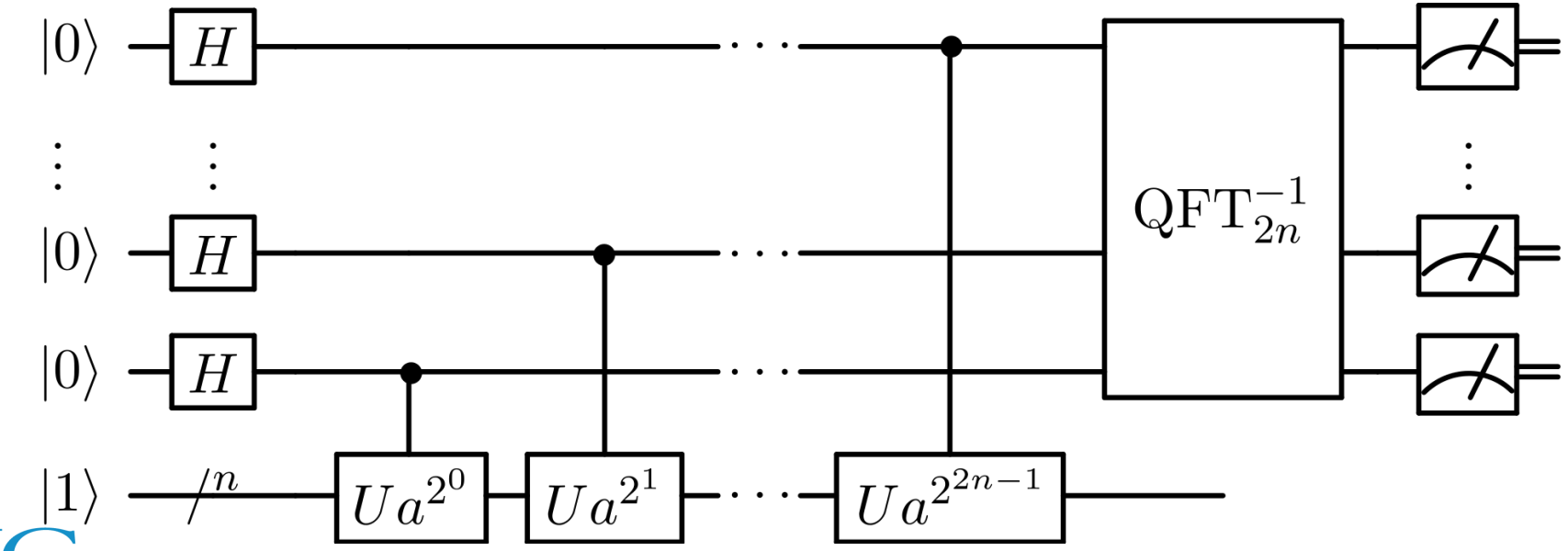
Case Study 2: Shor Algorithm of Factoring

188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

=

3980750864240649373971255005503864911990643623425267084063851895759463889572617685833172777214610743530253623071973048224632914695302097116459852171130520711256363590397527

×



UNC INFORMATION TECHNOLOGY SERVICES

Case Study 3: Variational Quantum Eigensolver

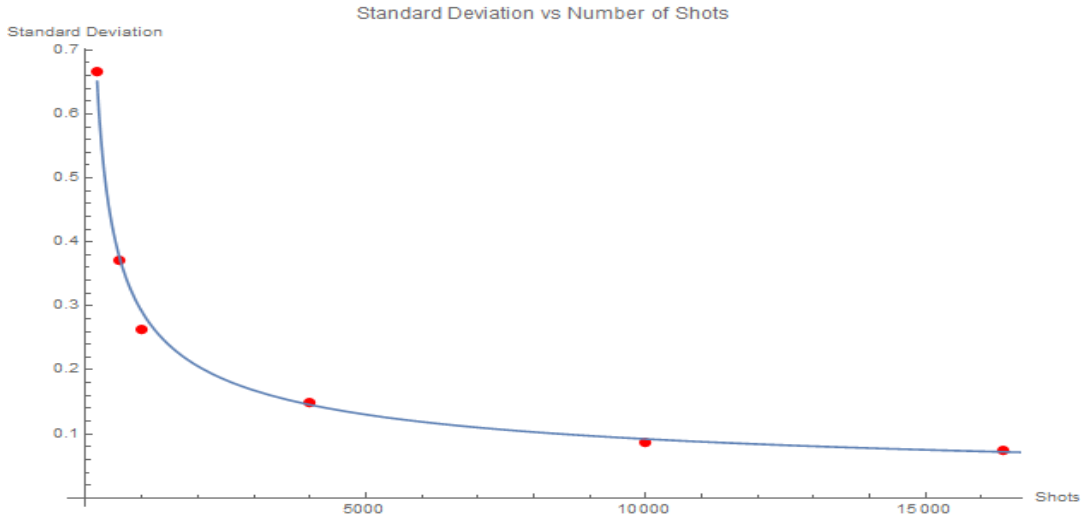
- VQE is a quantum/classical hybrid algorithm that can be used to find eigenvalues of a matrix H.
- When VQE is used in quantum simulations, H is typical the Hamiltonian of an electronic system.
- It is run inside of a classical optimization loop.
- The quantum part has two fundamental steps:
  - Prepare the quantum states $|\psi>$, often called the ansatz;
  - Measure the expectation value $<\psi|H|\psi>$
- The classical optimization loop does two tasks:
  - Use a classical non-linear optimizer to minimize the expectation value by varying ansatz parameters
  - Iterate until convergence is reached.

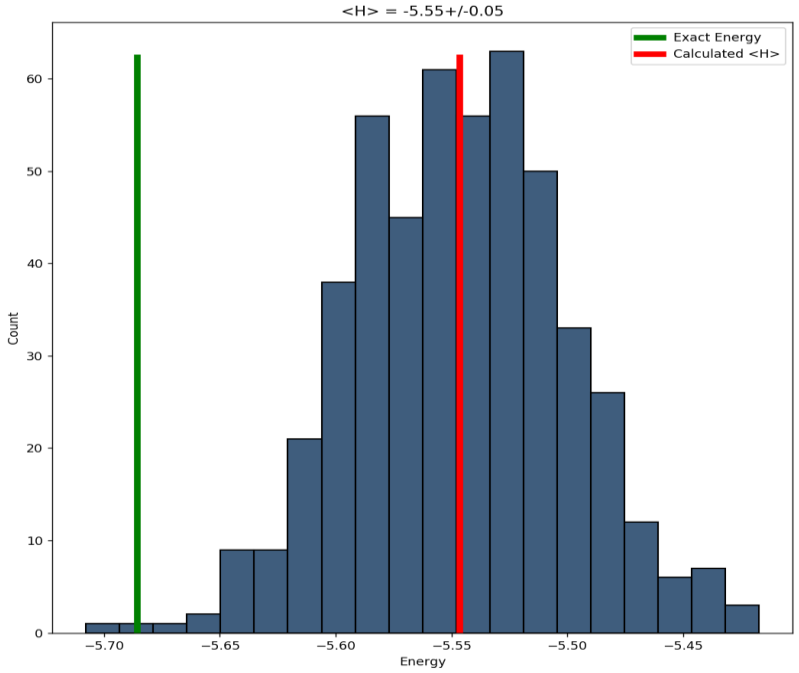
UNC INFORMATION TECHNOLOGY SERVICES

Nature Communications, 5, 4213, (2014).
New J. Phys. 18, 023023 (2016).

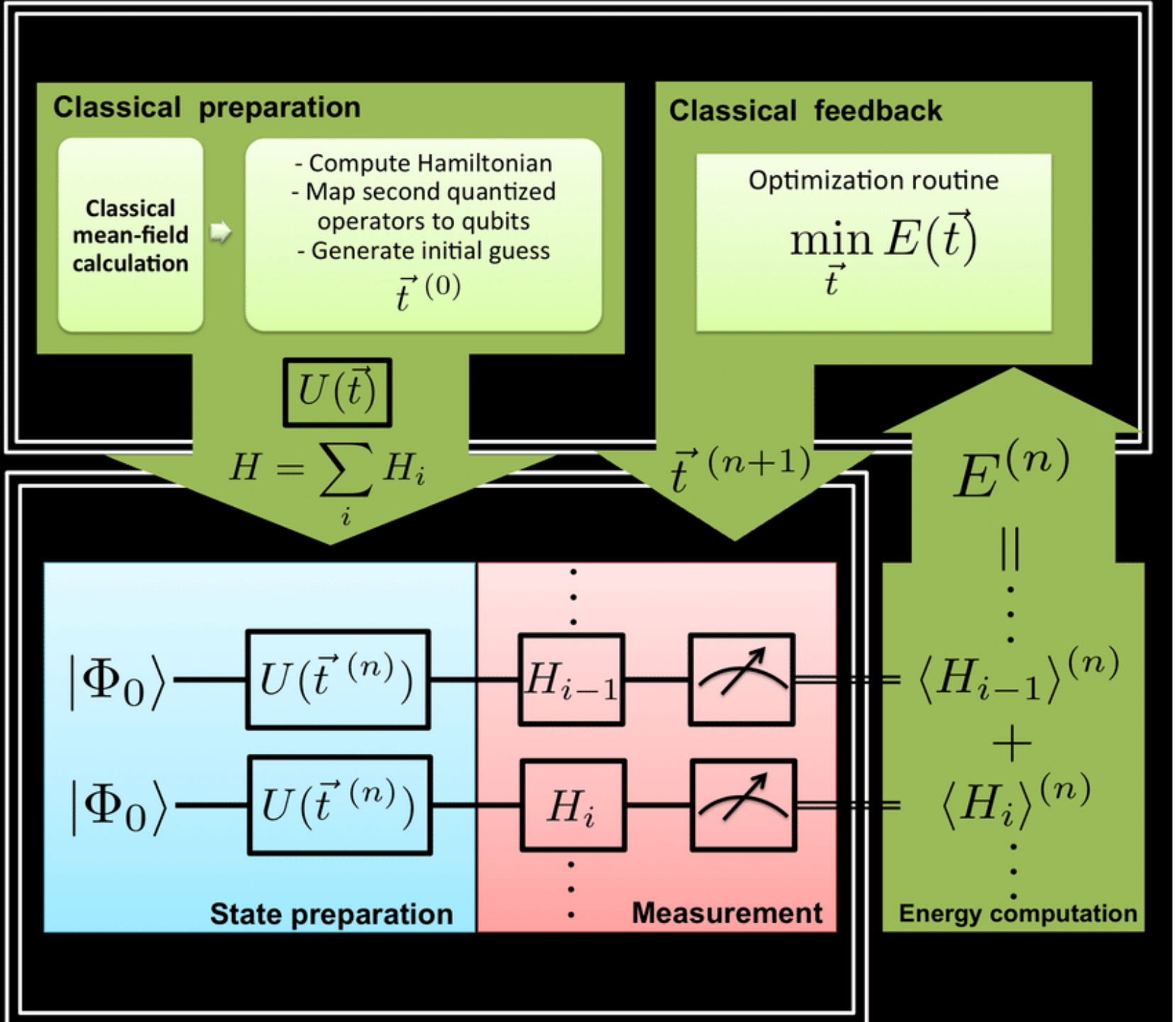
VQE Procedures

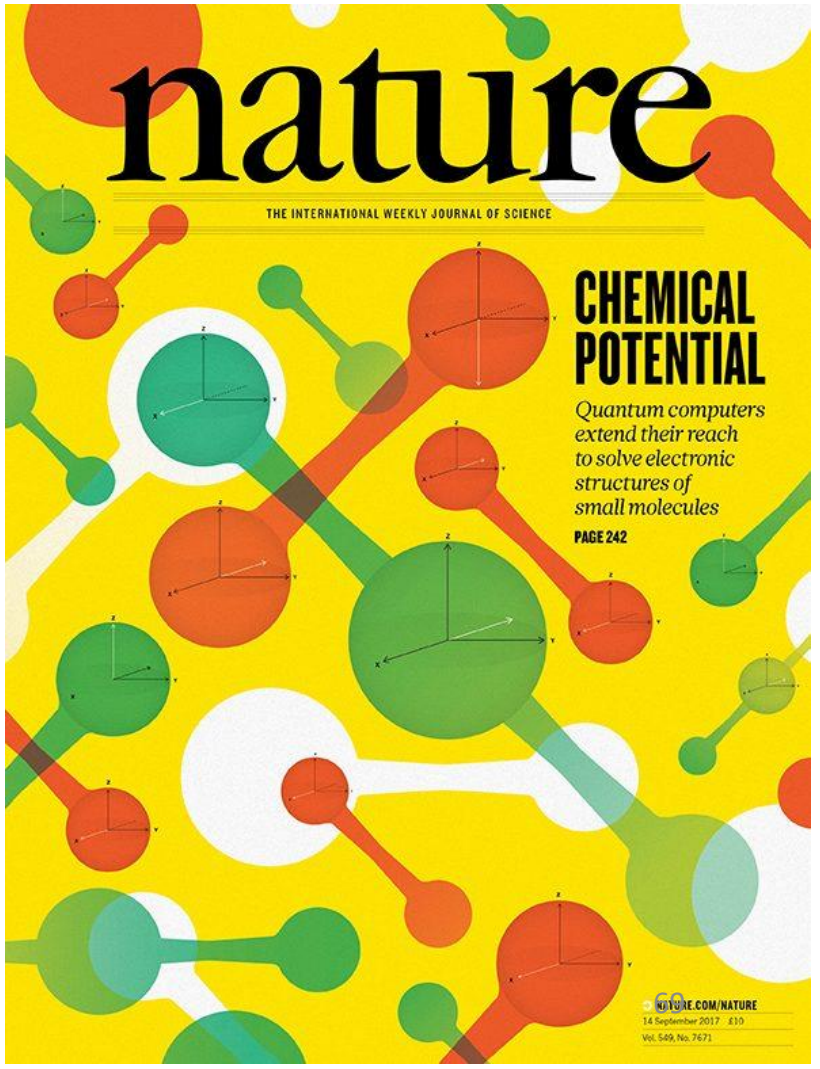
- The Hamiltonian of the system is mapped to a qubit Hamiltonian
- A trial wavefunction is picked
- A quantum circuit is applied to prepare the desired state. The quantum circuit used in the variational eigensolver is a Hadamard gate applied to each qubit to create a superimposed state, followed by a y and z rotation (R_y , R_z)
- The energy of the trial state is estimated by a classic optimizer
- Varies the parameters of the state to redo the loop
- Loops until the energy minimization condition is met



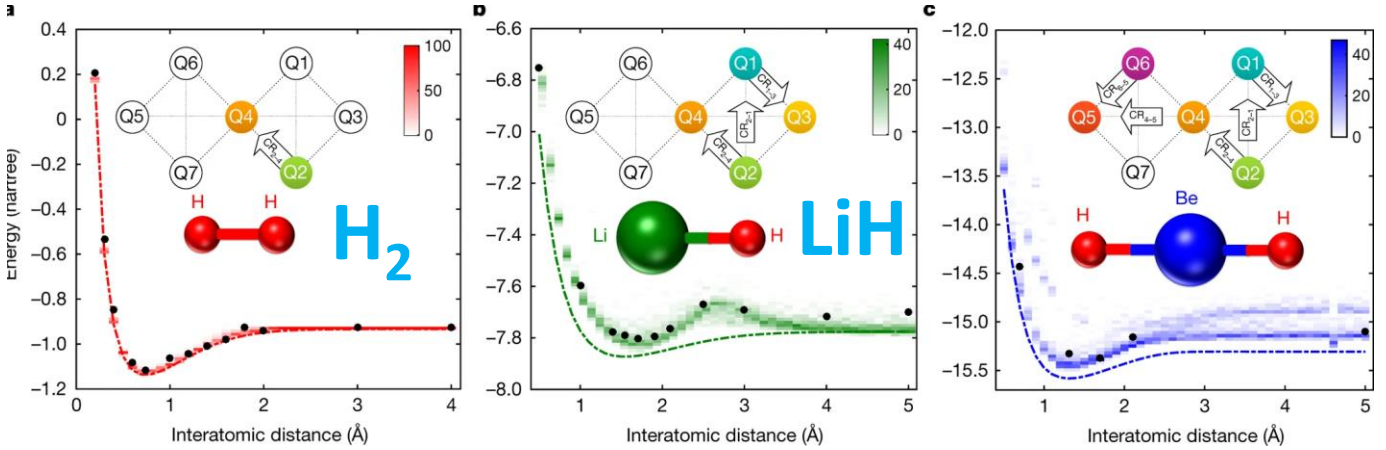


Case Study 3: Variational Quantum Eigensolver



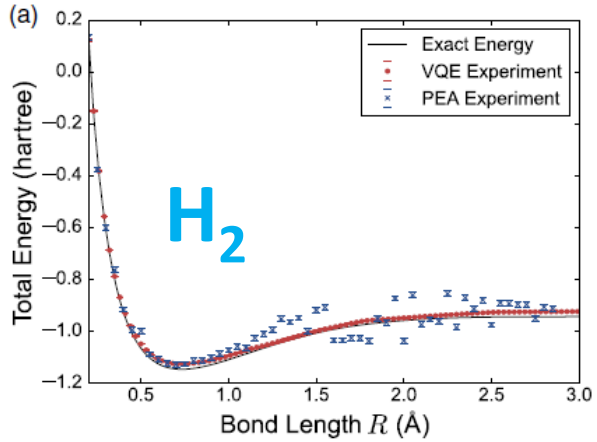


Case Study 3: Variational Quantum Eigensolver



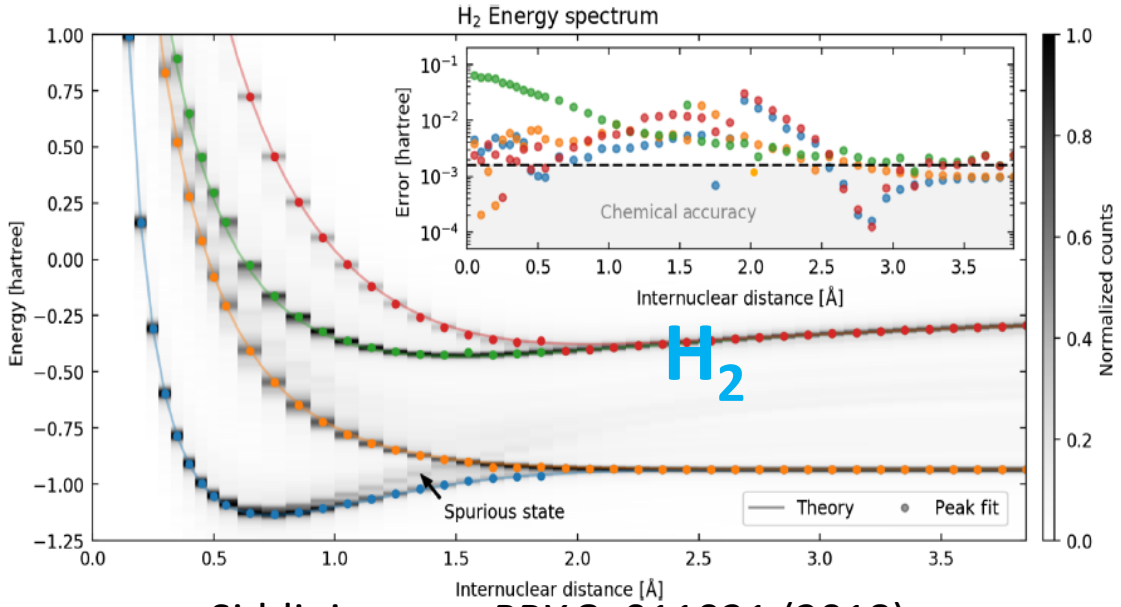
H_2 LiH BeH_2

IBM group, *Nature* **549**, 242 (2017)



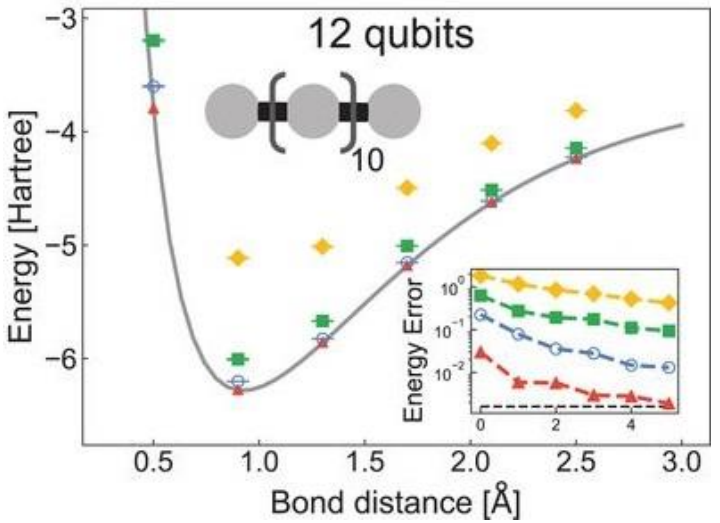
H_2

Google group, *PRX* **6**, 031007 (2016)



H_2

Siddiqi group, *PRX* **8**, 011021 (2018)



H_{12}

Google group, *Science* **369**, 1084 (2020)

Post-Quantum World

There is a good chance that quantum computers will be able to crack RSA-2048 within five-ten years (need about 8,000 qubits in a universal computer to do this).
Some encrypted data has a shelf-life of more than ten years. It may take ten years to cut over to a new encryption scheme, so companies and governments are scrambling to figure out what to do.

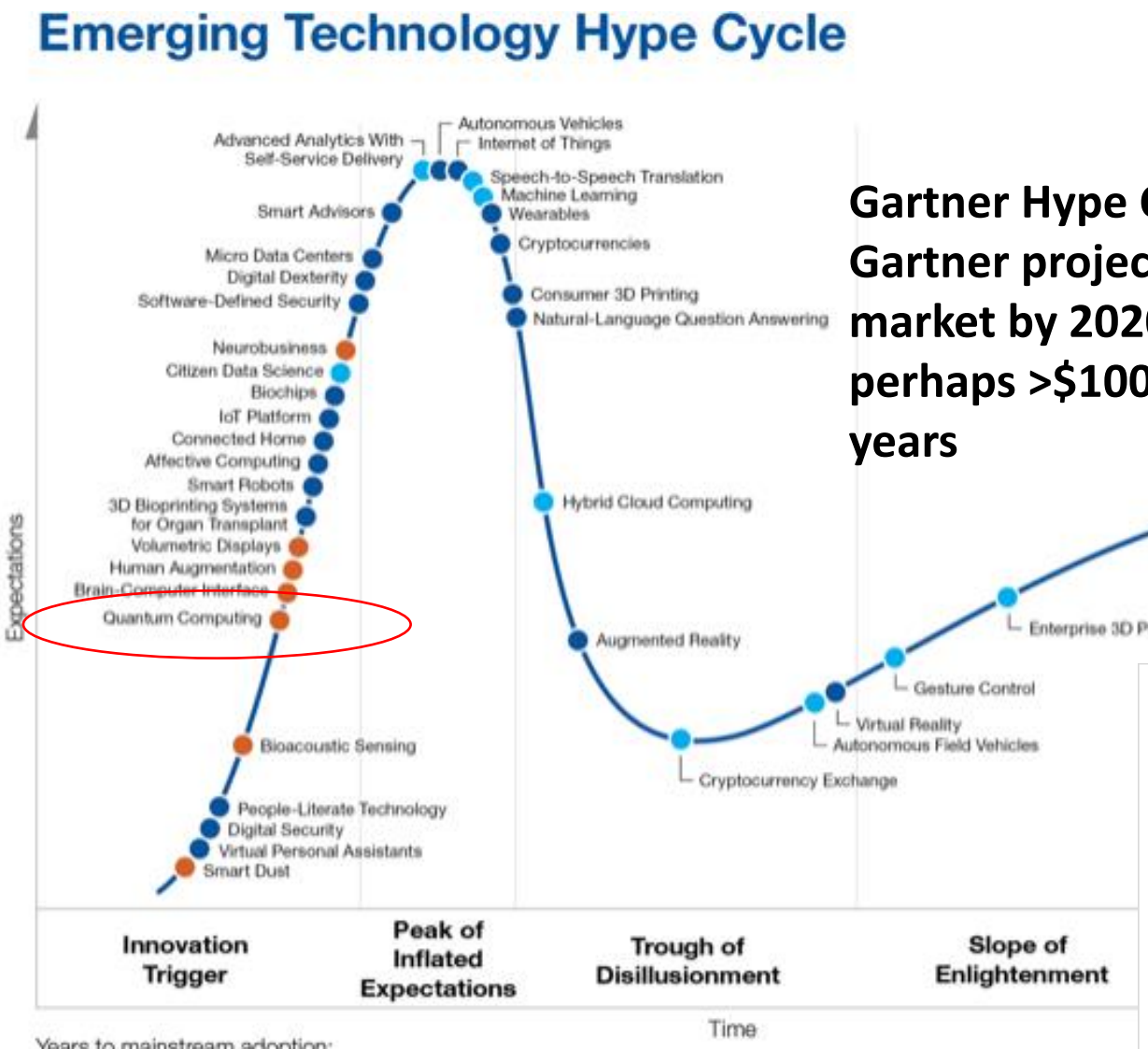
Most encryption used today is not safe in a quantum world.
If someone has been recording a https session, say, they may not be able to decrypt it now, but a few years from now, who knows.

There are encryption algorithms that are safe:
Secure communications will move to symmetric encryption or hash algorithms, or perhaps lattice algorithms.

QKD (Quantum Key Distribution) will likely be more popular for the most sensitive communications
Some governments and banks are already starting to use “Quantum Safe” algorithms, and this is expected to increase over the next decade.

UNC
INFORMATION
TECHNOLOGY SERVICES

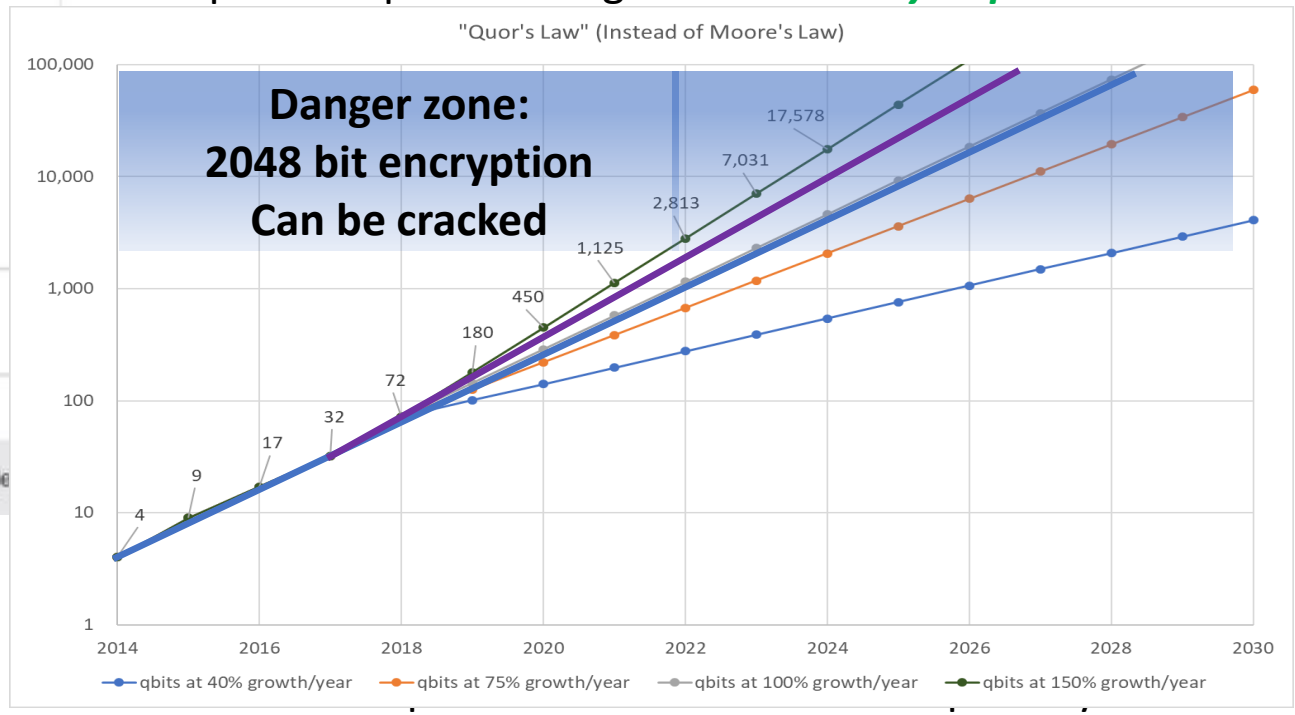
Future of Quantum Computers



Gartner Hype Cycle. Gartner projects a $5B market by 2020 worth perhaps >$100B in ten years

Qubit count of general-purpose quantum computers will double roughly every one to two years, or roughly every 18 months on average.

Neven's Law, named after Hartmut Neven, the director of Google's Quantum Artificial Intelligence Lab, stated that quantum processors grow at a ***doubly-exponential rate***.



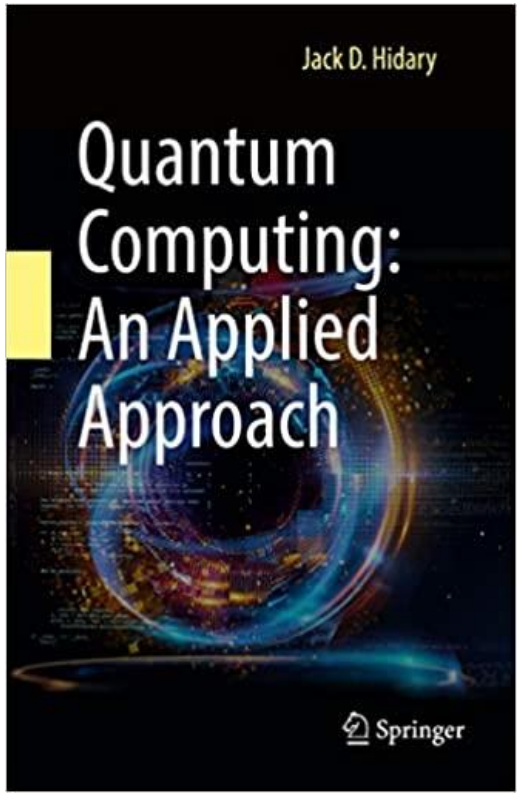
UNC INFORMATION TECHNOLOGY SERVICES

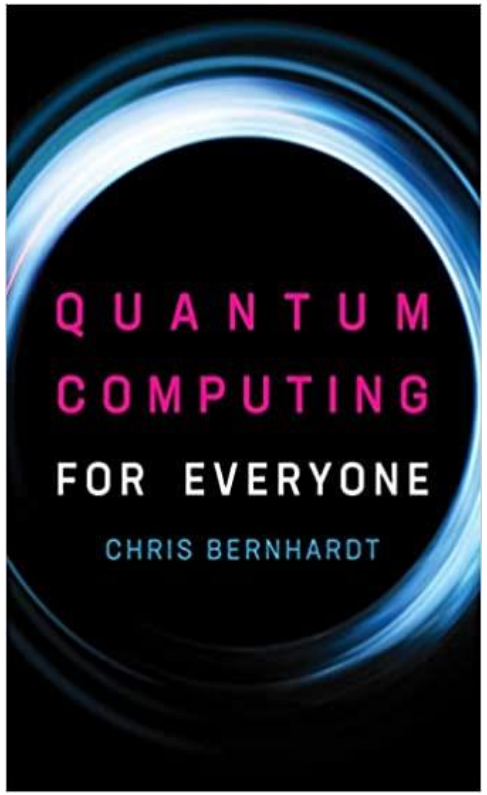
Problems with Quantum Computers

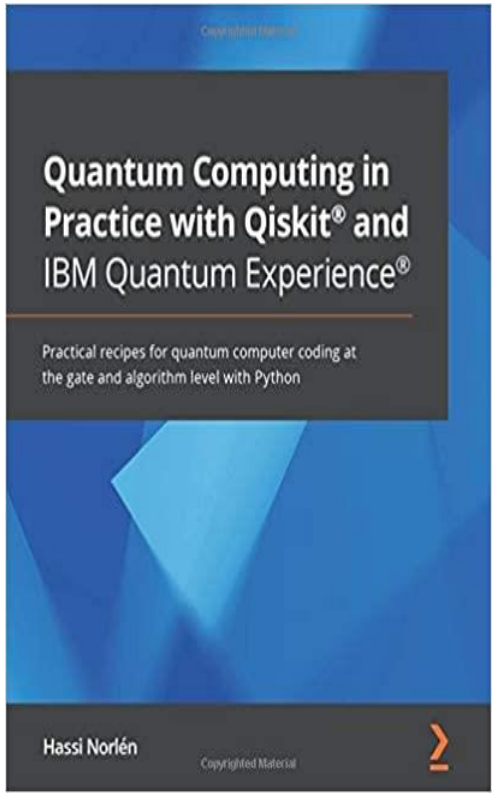
- Decoherence
  - Quantum system is extremely sensitive to external environment, so it should be safely isolated
  - It is hard to achieve the decoherence time that is more than the algorithm running time
- Error correction (requires more qubits!)
- Physical implementation of computations
- New quantum algorithms to solve more problems
- Entangled states for data transfer
- Running time increases exponentially with matrix size

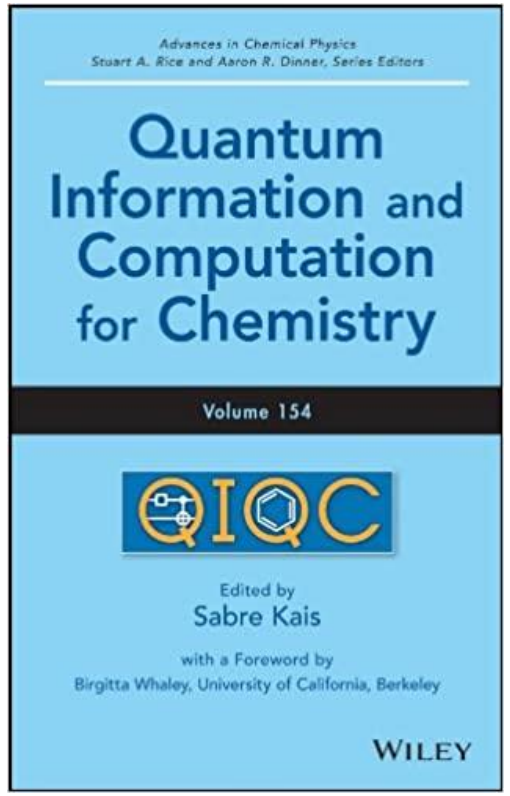
UNC
INFORMATION
TECHNOLOGY SERVICES

Further Reading









https://en.wikipedia.org/wiki/Talk:Quantum_computing/Further_Reading

UNC INFORMATION TECHNOLOGY SERVICES

Future Short-Courses in Planning

Two more short courses on quantum computing are under consideration:

- Intermediate Level – Quantum Algorithms and Applications
  - Deutsch–Jozsa algorithm
  - Bernstein–Vazirani algorithm
  - Simon's algorithm
  - Quantum phase estimation algorithm
  - Grover's algorithm
  - Shor’s Algorithm
  - Quantum Fourier Transform
- Advanced Level – Applications of Quantum Computers in Chemistry
  - Variational quantum eigensolver
  - QAOA (quantum approximate optimization algorithm)

UNC INFORMATION TECHNOLOGY SERVICES

Credit, Citation and Acknowledgment

- https://arnaldogunzi.medium.com/nisq-era-3b45b71bb11a
- https://www.geeksforgeeks.org/introduction-of-logic-gates/
- https://en.wikipedia.org/wiki/Quantum_logic_gate
- https://www.hpcwire.com/2020/08/19/intel-connects-the-quantum-dots-in-accelerating-quantum-computing-effort/
- https://medium.com/uvc-partners-news/the-european-quantum-computing-startup-landscape-a115ffe84ad8
- https://industry40marketresearch.com/product/quantum-computing-market-technologies/
- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication
- https://www.yaabot.com/31345/quantum-computing-neural-chips-moores-law-future-computing/
- https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat
- https://www.newscientist.com/article/mg23030710-500-thats-odd-quantum-entanglement-mangles-space-and-time/
- https://blogs.umass.edu/Techbytes/2016/10/18/quantum-computing/
- https://www.fonow.com/view/267479.html
- https://science.sciencemag.org/content/356/6343
- https://www.nature.com/nature/volumes/574/issues/7779
- https://www.ibm.com/blogs/research/2017/09/quantum-molecule/
- https://phys.org/news/2020-10-ionq-next-generation-quantum.html
- https://www.advancedsciencenews.com/researchers-claim-quantum-supremacy-with-new-computer/
- https://www.cnet.com/news/quantum-computer-makers-like-their-odds-for-big-progress-soon/
- https://medium.com/faun/hello-many-worlds-in-quantum-computer-524fe90b833b
- https://www.epiqc.cs.uchicago.edu/hybrid-quantum-classical-computing
- https://brilliant.org/wiki/quantum-teleportation/
- https://www.youtube.com/watch?v=yprDIC-9D0k
- https://www.youtube.com/watch?v=QuR969uMICM

DEMO: Quantum Computing with IBM QISKit

- IBM QISKit (Quantum Information Science Kit) API, a Cloud-enabled Python interface to quantum computer:
  - What is QISKit?
  - How to obtain an account? How to login?
  - How to build simple quantum circuits?
  - How to run quantum circuits on IBM quantum computers?
  - How to monitor jobs and visualize results?
  - How to find online tutorials and documentations?

QISKit DEMO

Questions & Comments???

Please direct comments/questions about research computing to

E-mail: research@unc.edu

Please direct comments/questions pertaining to this presentation to

E-Mail: shubin@email.unc.edu

The PPT file of this presentation is available here:
http://its2.unc.edu/divisions/rc/training/scientific/short_courses/Quantum_Computer.ppt

UNC INFORMATION TECHNOLOGY SERVICES