

# Introduction to Quantum Computing

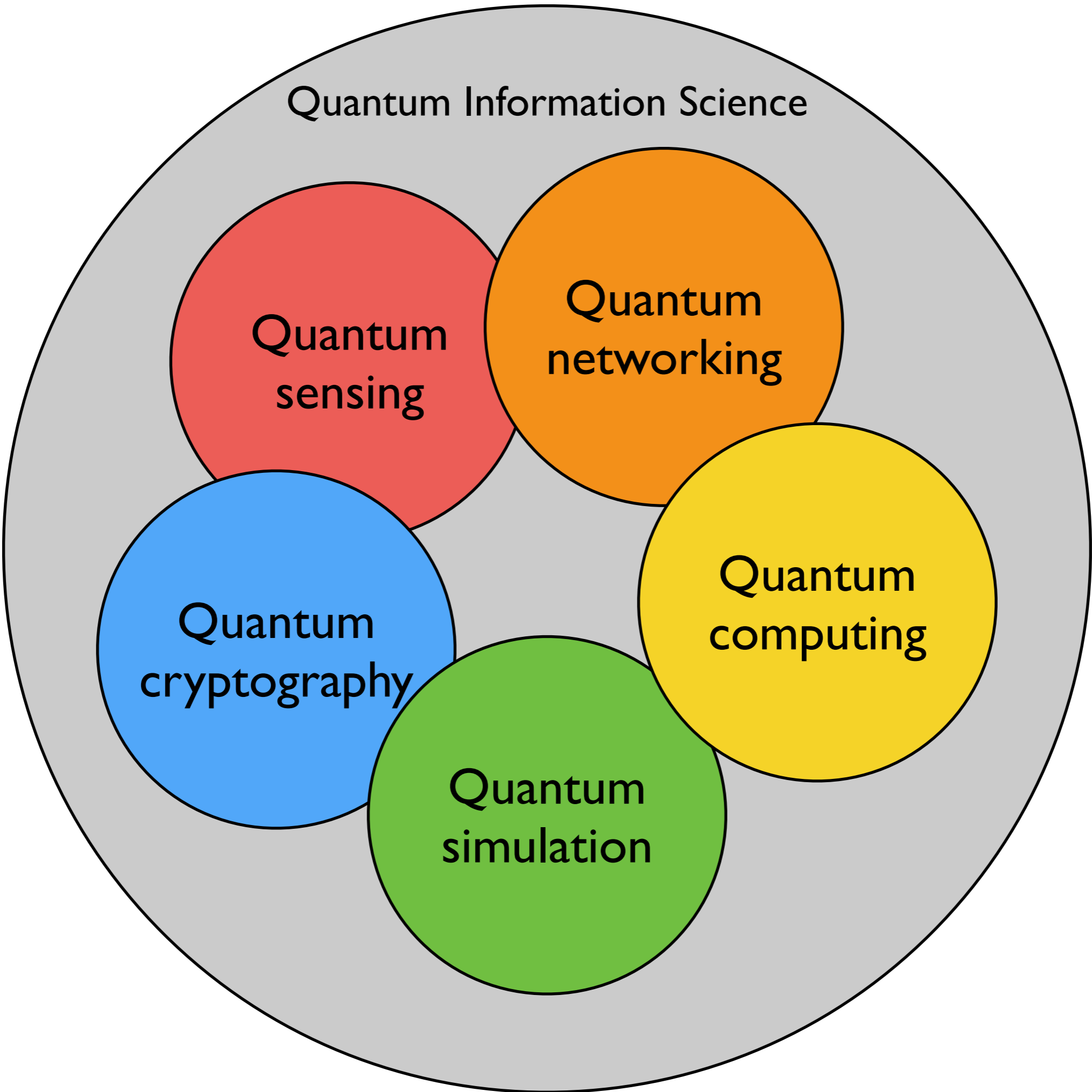
## Lecture I: Fundamentals

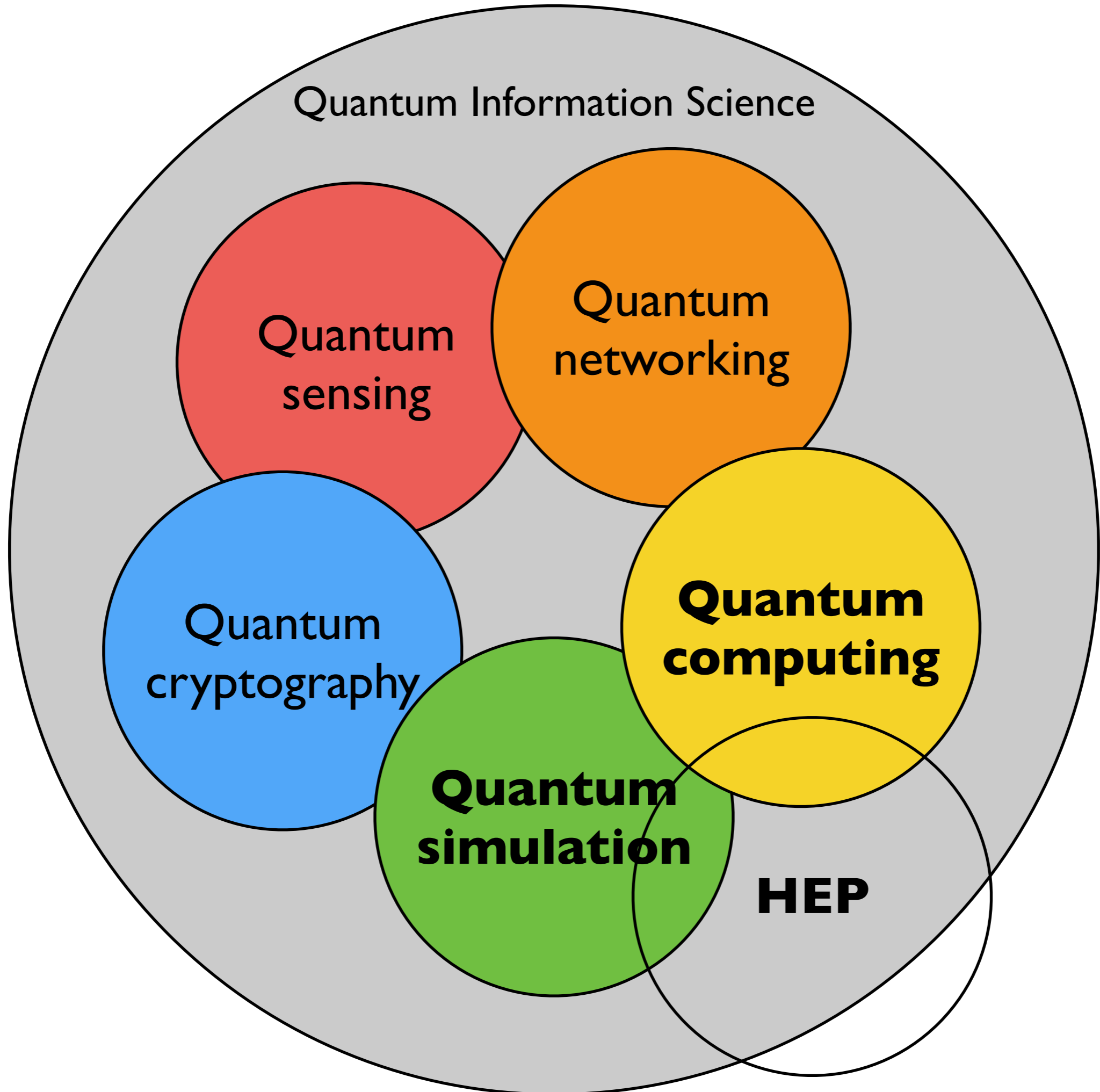
---

Heather M. Gray  
UC Berkeley/LBNL

*Many thanks to Umesh Varizani and Irfan Siddiqi for  
material used in these slides*

CERN Academic Training, March 2021





# Outline for the lectures

- **Lecture 1: Fundamentals**

- A brief history, qubits, quantum circuits, qubit technologies

- **Lecture 2: Quantum computers and quantum algorithms**

- Quantum computers today, quantum algorithms, error correction, quantum advantage

- **Lecture 3: Applications of quantum computing in HEP**

- Applications of quantum computing to HEP: simulation, reconstruction and physics analysis; including quantum machine learning



# Outline for the lectures

- **Lecture 1: Fundamentals**

- A brief history, qubits, quantum circuits, qubit technologies

- **Lecture 2: Quantum computers and quantum algorithms**

- Quantum computers today, quantum algorithms, error correction, quantum advantage

- **Lecture 3: Applications of quantum computing in HEP**

- Applications of quantum computing to HEP: simulation, reconstruction and physics analysis; including quantum machine learning

# Early Ideas

## The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines

Paul Benioff<sup>1,2</sup>

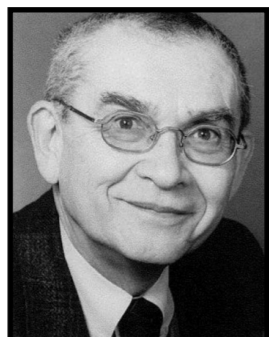
*Received June 11, 1979; revised August 9, 1979*

In this paper a microscopic quantum mechanical model of computers as represented by Turing machines is constructed. It is shown that for each number  $N$  and Turing machine  $Q$  there exists a Hamiltonian  $H_N^Q$  and a class of appropriate initial states such that if  $\Psi_Q^N(0)$  is such an initial state, then  $\Psi_Q^N(t) = \exp(-iH_N^Q t) \Psi_Q^N(0)$  correctly describes at times  $t_3, t_6, \dots, t_{3N}$  model states that correspond to the completion of the first, second, ...,  $N$ th computation step of  $Q$ . The model parameters can be adjusted so that for an arbitrary time interval  $\Delta$  around  $t_3, t_6, \dots, t_{3N}$ , the "machine" part of  $\Psi_Q^N(t)$  is stationary.

**KEY WORDS:** Computer as a physical system; microscopic Hamiltonian models of computers; Schrödinger equation description of Turing machines; Coleman model approximation; closed conservative system; quantum spin lattices.



P. Benioff, 1979



Yuri Manin, Steklov Institute, "Computable and Uncomputable", 1980 (in Russian)

## Simulating Physics with Computers

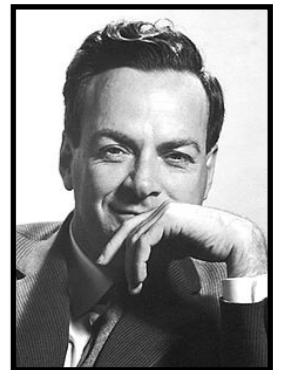
Richard P. Feynman

*Department of Physics, California Institute of Technology, Pasadena, California 91107*

*Received May 7, 1981*

### 1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain.



R. Feynman, 1981

# The Algorithms

## Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor  
AT&T Bell Labs  
Room 2D-149  
600 Mountain Ave.  
Murray Hill, NJ 07974, USA

### Abstract

*A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)*

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as

## P. Shor, 1994

The invention of quantum algorithms dramatically increased interest in quantum computers

## A fast quantum mechanical algorithm for database search

Lov K. Grover  
3C-404A, Bell Labs  
600 Mountain Avenue  
Murray Hill NJ 07974  
[lkgrover@bell-labs.com](mailto:lkgrover@bell-labs.com)

### Summary

Imagine a phone directory containing  $N$  names arranged in completely random order. In order to find someone's phone number with a probability of  $\frac{1}{2}$ , any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of  $\frac{N}{2}$  names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only  $O(\sqrt{N})$  steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing  $N$  items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of  $\frac{N}{2}$  items before finding the desired item.

## L. Grover, 1996

### Grover Algorithm with zero theoretical failure rate

G. L. Long<sup>1,2,3,4</sup>

<sup>1</sup>Department of Physics, Tsinghua University, Beijing 100084, P.R.China

<sup>2</sup>Key Laboratory for Quantum Information and Measurements, Ministry of Education, Beijing 100084, P. R. China

<sup>3</sup>Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing, 100080, P. R. China

<sup>4</sup>Center of Atomic, Molecular and Nanosciences, Tsinghua University, Beijing 100084, P. R. China  
(October 24, 2018)

In standard Grover's algorithm for quantum searching, the probability of finding the marked item is not exactly 1. In this Letter we present a modified version of Grover's algorithm that searches a marked state with full successful rate. The modification is done by replacing the phase inversion by two phase rotation through angle  $\phi$ . The rotation angle is given analytically to be  $\phi = 2 \arcsin\left(\frac{\sin\left(\frac{\pi}{4J+6}\right)}{\sin\beta}\right)$ , where  $\sin\beta = \frac{1}{\sqrt{N}}$ ,  $N$  the number of items in the database, and  $J$  an integer equal to or greater than the integer part of  $(\frac{\pi}{2} - \beta)/(2\beta)$ . Upon measurement at  $(J+1)$ -th iteration, the marked state is obtained with certainty.

PACS numbers: 03.67.Lx, 89.70.+c, 89.80.+h

Grover's quantum search algorithm [1] is an important development in quantum computation. It achieves square-root speedup over classical algorithms in unsorted database searching. It has extensive applications, because many problems, for instance deciphering the DES encryption scheme, can be reduced to this problem [2]. Starting from an evenly distributed state, Grover algorithm searches the database with

## G. Long, 2001

# Early Computers

## First quantum computers used existing NMR techniques

### Implementation of a Quantum Algorithm to Solve Deutsch's Problem on a Nuclear Magnetic Resonance Quantum Computer

J. A. Jones

Oxford Centre for Molecular Sciences, New Chemistry Laboratory, South Parks Road, Oxford OX1 3QT, UK, and Centre for Quantum Computing, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK

M. Mosca

Centre for Quantum Computing, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK, and Mathematical Institute, 24-29 St Giles', Oxford, OX1 3LB, UK

Correspondence should be addressed to J. A. Jones at the New Chemistry Laboratory.

Email: jones@bioch.ox.ac.uk

#### Abstract

Quantum computing shows great promise for the solution of many difficult problems, such as the simulation of quantum systems and the factorisation of large numbers. While the theory of quantum computing is well understood, it has proved difficult to implement quantum computers in real physical systems. It has recently been shown that nuclear magnetic resonance (NMR) can be used to implement small quantum computers using the spin states of nuclei in carefully chosen small molecules. Here we demonstrate the use of an NMR quantum computer based on the pyrimidine base cytosine, and the implementation of a quantum algorithm to solve Deutsch's problem (distinguishing between constant and balanced functions). This is the first successful implementation of a quantum algorithm on any physical system.

**2 qubit**

J. Jones and M. Mosca, 30 April 1998

### Experimental Implementation of Fast Quantum Searching **2 qubit**

Isaac L. Chuang,<sup>1,\*</sup> Neil Gershenfeld,<sup>2</sup> and Mark Kubinec<sup>3</sup>

<sup>1</sup>IBM Almaden Research Center K10/D1, 650 Harry Road, San Jose, California 95120

<sup>2</sup>Physics and Media Group, MIT Media Lab, Cambridge, Massachusetts 02139

<sup>3</sup>College of Chemistry, D7 Latimer Hall, University of California, Berkeley, Berkeley, California 94720-1460

(Received 21 November 1997; revised manuscript received 29 January 1998)

Using nuclear magnetic resonance techniques with a solution of chloroform molecules we implement Grover's search algorithm for a system with four states. By performing a tomographic reconstruction of the density matrix during the computation good agreement is seen between theory and experiment. This provides the first complete experimental demonstration of loading an initial state into a quantum computer, performing a computation requiring fewer steps than on a classical computer, and then reading out the final state. [S0031-9007(98)05850-5]

PACS numbers: 89.70.+c, 03.65.-w

The study of computation in quantum systems began with the recognition of the theoretical possibility [1–3]. This was followed by a series of results leading up to proofs that a quantum computer requires fewer operations than a classical computer for problems including factoring [4] and searching [5,6]. Appreciation of the power of quantum computing was quickly tempered by the realization that preserving quantum coherence made the implementation of practical quantum computers appear to be unlikely [7–9].

is  $9/4 = 2.25$ . With a quantum computer using Grover's algorithm, this is reduced to a *single* evaluation. We have experimentally implemented this case using molecules of chloroform as a quantum computer, and confirmed the periodic behavior expected of the algorithm.

The algorithm works by representing  $x$  as a pair of two-state quantum systems. We take these to be the spins of the carbon and hydrogen nuclei, writing  $|\uparrow\rangle = |1\rangle$  and  $|\downarrow\rangle = |0\rangle$ . The function  $f(x)$  is implemented as a unitary transform that flips the phase of the  $x_0$  element.

## Chuang, Gershenfeld and Kubinec, 13 April 1998

### Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M.K. Vandersypen<sup>†,\*</sup>, Matthias Steffen<sup>\*,†</sup>, Gregory Breyta<sup>†</sup>, Costantino S. Yannoni<sup>†</sup>, Mark H. Sherwood<sup>†</sup> and Isaac L. Chuang<sup>\*,†</sup>

<sup>†</sup> IBM Almaden Research Center,  
San Jose, CA 95120

<sup>\*</sup> Solid State and Photonics Laboratory,  
Stanford University,  
Stanford, CA 94305-4075

**7 qubit**

Vandersypen et al, 2001

Timeline on wikipedia

# Promises of Quantum Computation

- Exponential information storage
  - Information is encoded through entanglement
- Solutions to unsolved (classical) problems
- Revolutionize cryptography
  - Threaten existing cryptographic algorithms
  - New algorithms from quantum cryptography, quantum networking
- Brings foundational quantum mechanics to the fore
  - e.g. entanglement; exponential power
- Perhaps new insights into complex algorithms and even complexity theory

*“Art of making use of the resources that quantum mechanics gives us”*

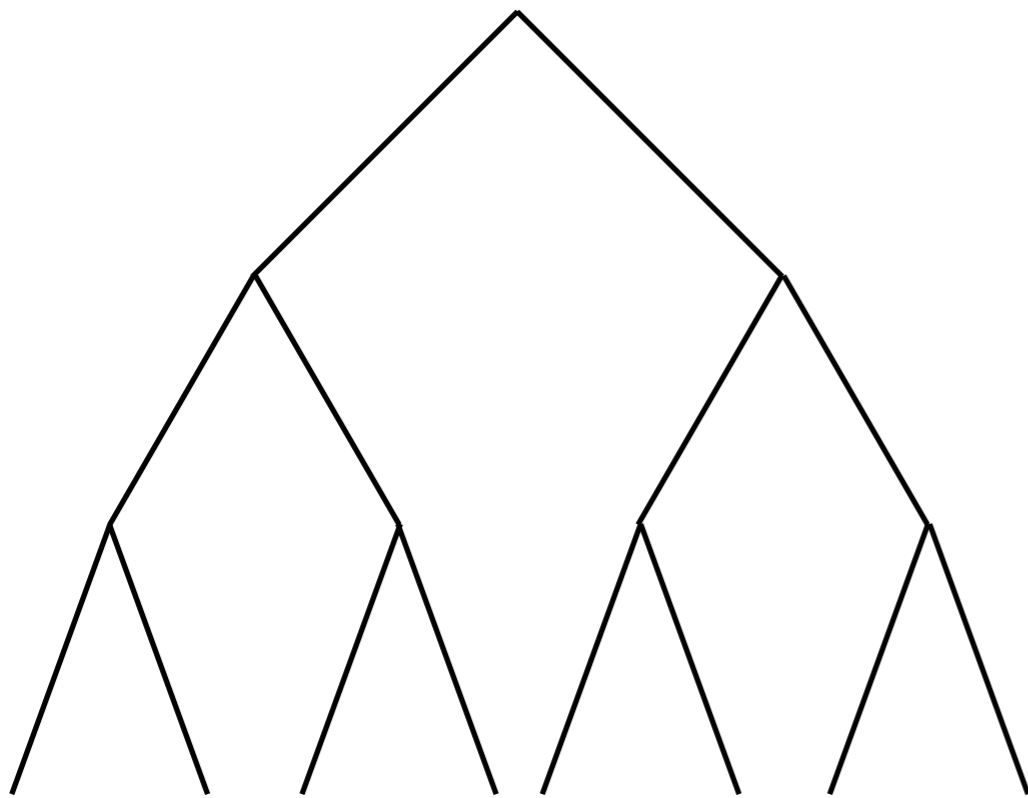
# Challenges of Quantum Computation

- Measurement always intrinsically disturbs the quantum system
  - Quantum systems need to be totally isolated
- But
  - System needs to be controlled
  - Data needs to be input and output
  - Qubits within the system need to (strongly) interact with each other
- Quantum computers today suffer from
  - Decoherence
  - Noise
- Must be mitigated through quantum error correction techniques



# Quantum Computing in the Popular Press

- Quantum computer as a "massively parallel" classical computer
- There is the potential for exponentially many answers
  - BUT, we can only observe one of them
- Speed gains must come through using interference to increase the probability of the correct answer



## The coldest computers in the world

By Chris Baraniuk  
Technology of Business reporter

7 August 2020

## *This Week in Tech: What on Earth Is a Quantum Computer?*

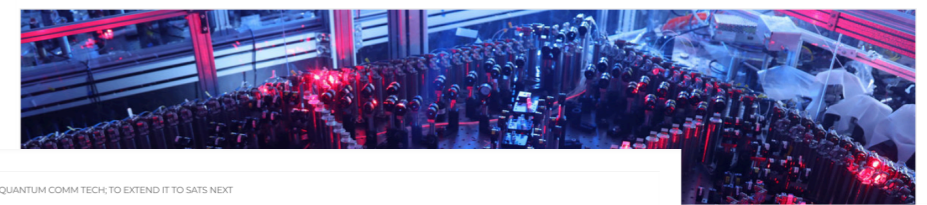
The question isn't so easy to answer. Also, Google's founders stepped away just as their company enters a turbulent adulthood.



• Home / China / Innovation

## Quantum computer created

By ZHANG ZHIHAO in Beijing and ZHU LIXIN in Hefei | China Daily | Updated: 2020-12-05 07:17



NEWS / INDIA NEWS / ISRO DEMONSTRATES QUANTUM COMM TECH; TO EXTEND IT TO SATS NEXT

## Isro demonstrates quantum comm tech; to extend it to Sats next

Chethan Kumar / TNN / Updated: Mar 23, 2021, 06:34 IST



UP NEXT



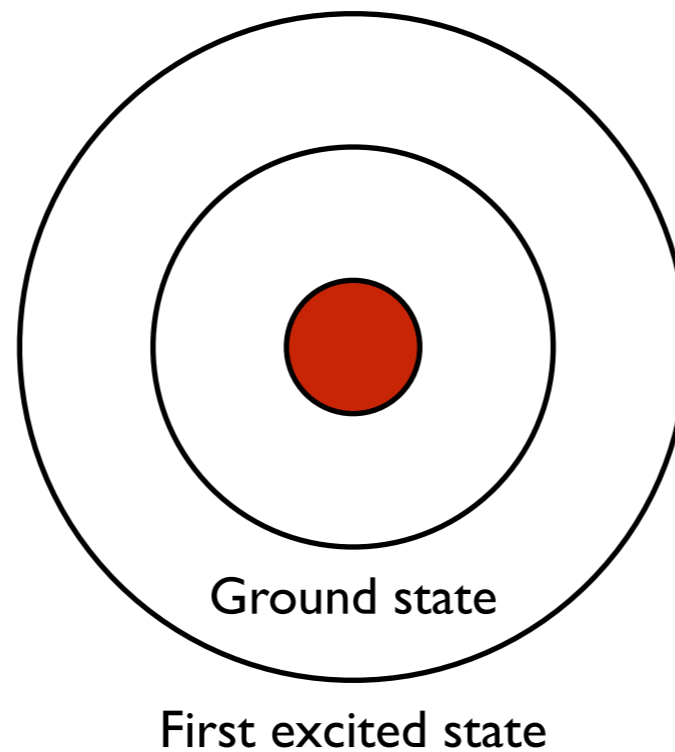
# Building Blocks of Quantum Computation

Qubits  
Quantum Gates  
Quantum Circuits



# Qubits

- Qubits are the basic unit of quantum computation
  - Quantum analog of bits
- Simple example: hydrogen atom
  - Ground state = 0
  - First excited state = 1

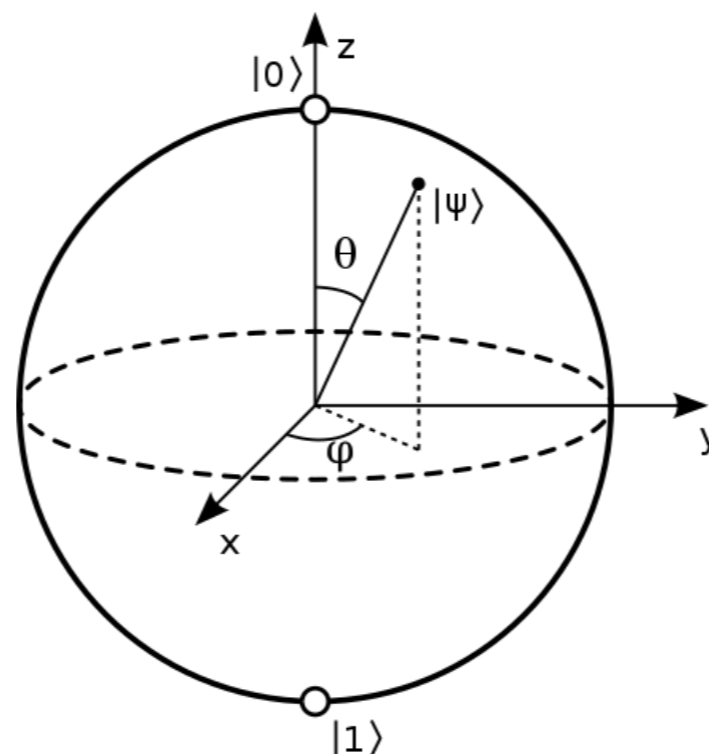


# Qubits (2)

- More generally, can be any quantum state ( $\alpha, \beta$  complex)
  - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Unit vector in a Hilbert space (2D complex space)
- When we measure the qubit
  - $|0\rangle$  with probability  $|\alpha|^2$
  - $|1\rangle$  with probability  $|\beta|^2$
- Many different ways to realize qubits: photon polarization, spin

Measurement disturbs the state:  
cannot determine both  $\alpha$  and  $\beta$  in a  
single measurement

Bloch sphere



# Bases

- Qubits can be expressed (or measured) in terms of any orthogonal bases
  - e.g.  $|\psi\rangle = \alpha'|v\rangle + \beta'|w\rangle$
- Common choices

- Standard basis:  $|0\rangle, |1\rangle$

- Sign basis:  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

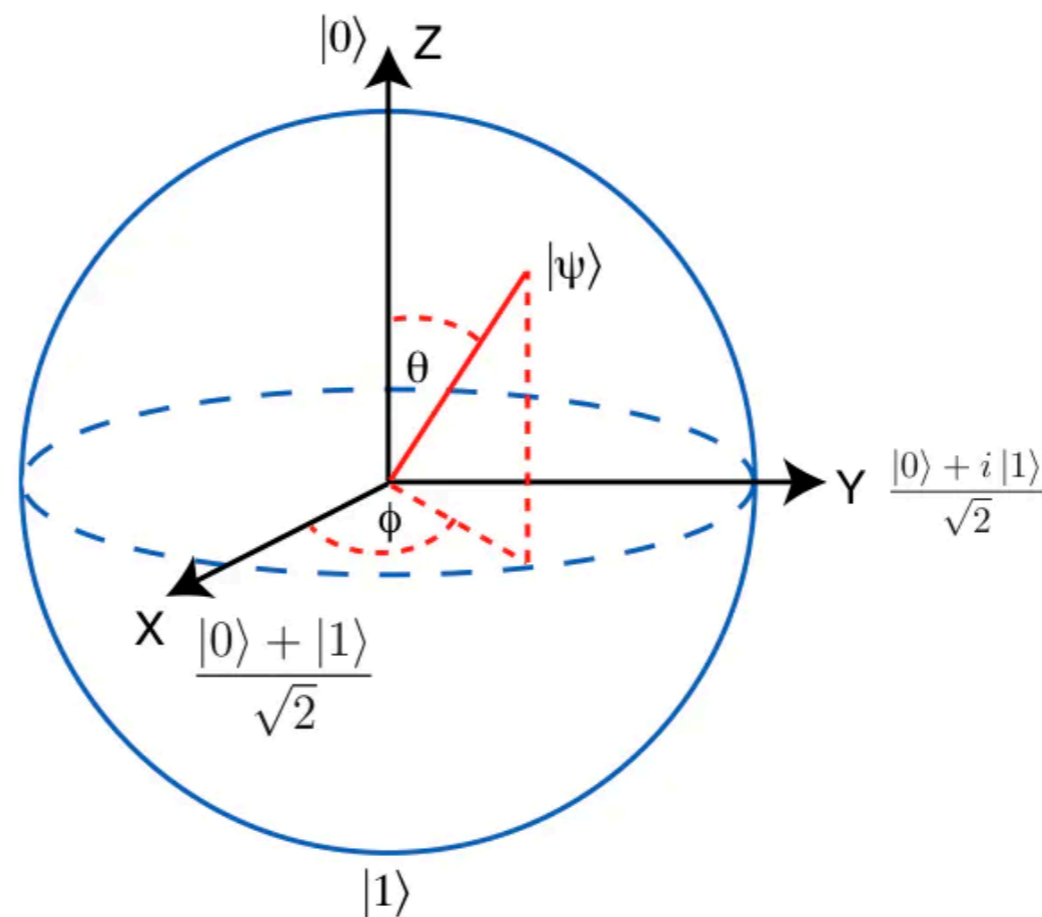


Image Credit

# Larger systems of qubits

- Easily generalize to a two qubit system using tensor product:

$$\bullet \quad |\psi\rangle = \sum_{i=0}^{k-1} \sum_{j=0}^{l-1} \gamma_{ij} |ij\rangle = |i\rangle \otimes |j\rangle$$

$$\bullet \quad \mathbb{C}^n \otimes \mathbb{C}^n = \mathbb{C}^{n^2}$$

- Generalise to n qubits:  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$

- Consider a two qubit system, e.g. two electrons in a hydrogen atom

- Four states, 2 bits of classical information

$$\bullet \quad |\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

- How much information?

- Two bits of information

- rest inaccessible to measurement

- Can extend qubits to qutrits (or qudits)

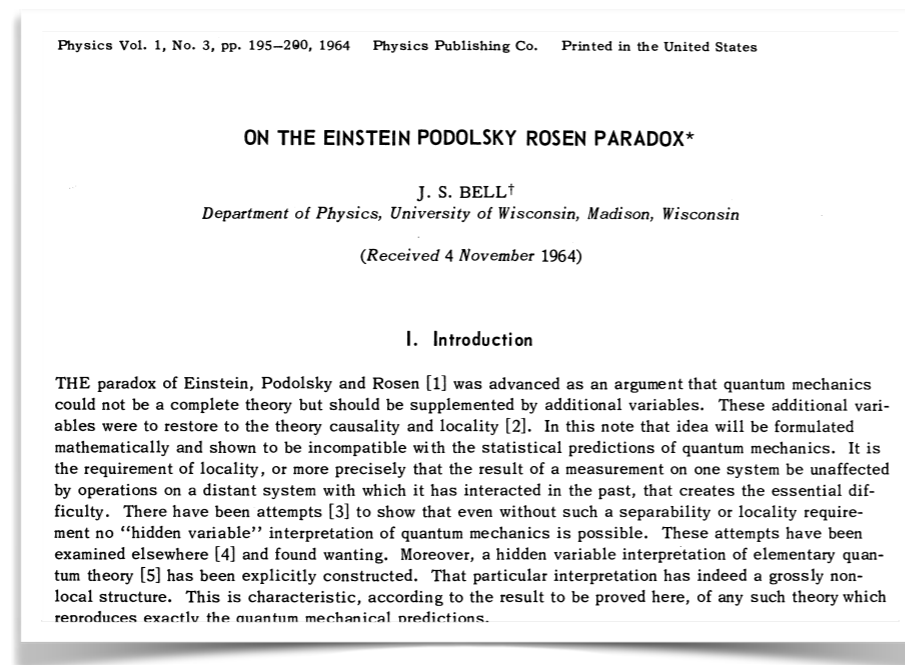


# Entangled Quantum Systems

- Reminder: not all two qubit systems can be decomposed into pairs of qubit states

- e.g.  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  (Bell state)

- Measure either qubit;  $P(1/2) = 0$
- If first measurement is 0; second measurement is always 0
- True in any orthonormal basis



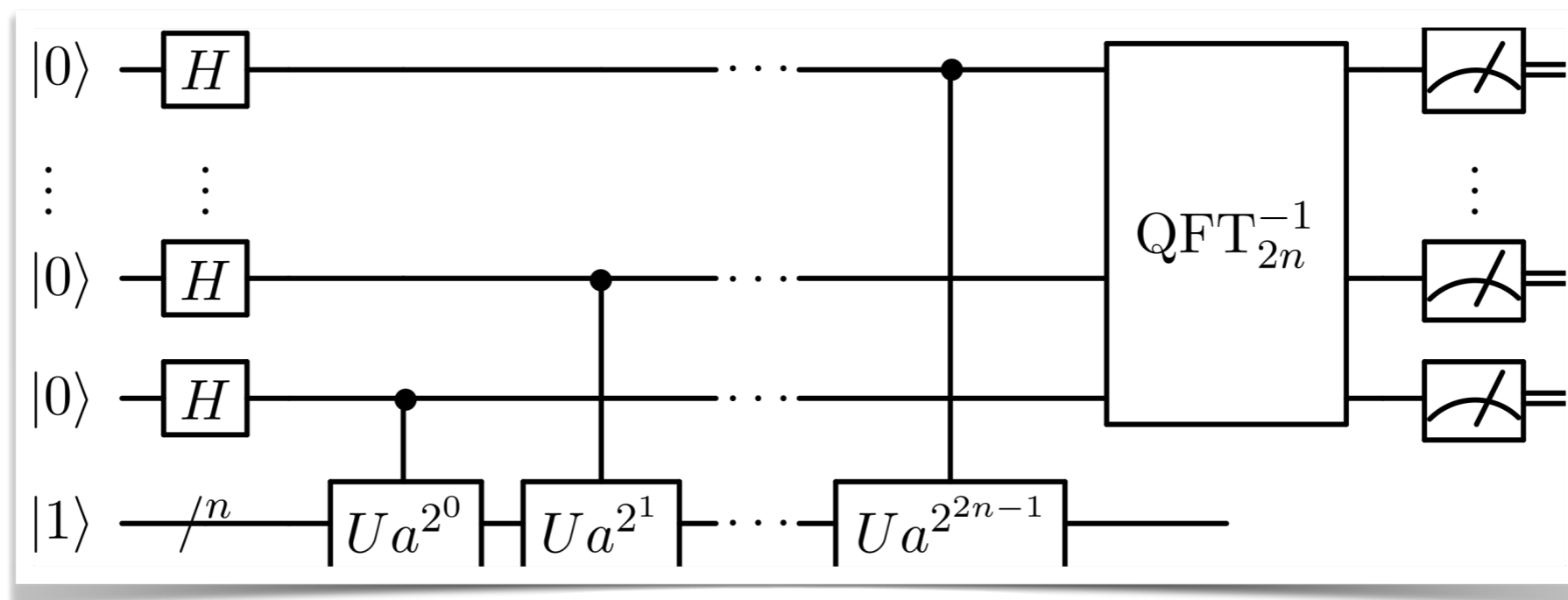
J.S. Bell, 1964

# No Clone Theorem

- No cloning theorem: impossible to make a (separable) copy of an unknown quantum state
- Proofs can be quite fun
  - e.g. Would enable communication at a speed faster than the speed of light
- Does not mean that a reproduce a specific state cannot be reproduced
  - Only that we cannot make a copy of an unknown state
- Does the no clone theorem mean that it's impossible to store quantum information?
- Or that it's impossible to correct errors?
- More later, but the answer is no. Although we cannot copy qubits, we can spread the information from a single qubit onto multiple qubits

# Quantum Gates

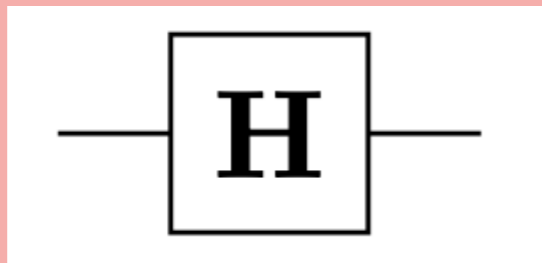
- Quantum gates are used to manipulate quantum information
  - i.e. operate on qubits
- Reminder: evolution of quantum systems is unitary
- Quantum gates = unitary operators
- Quantum gates will be combined to produce quantum circuits



# Quantum Gates for Single Qubits

## Hadamard

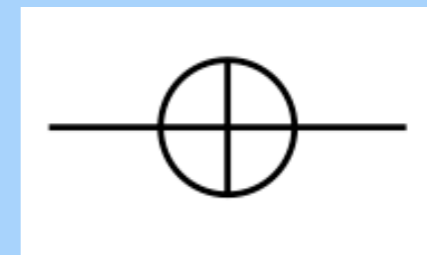
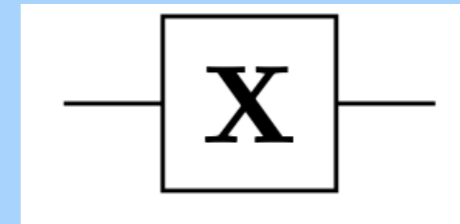
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Rotation by  $\pi$   
around  $\pi/8$  axis in  
complex plane  
Maps  $|0\rangle, |1\rangle$  to  
 $|+\rangle, |-\rangle$  basis

## NOT/Pauli-X

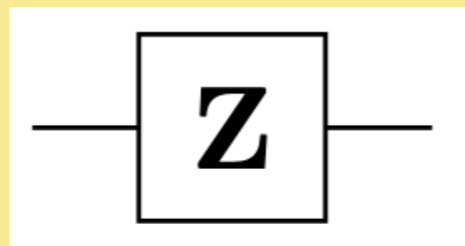
$$NOT = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



Real and symmetric  $\rightarrow$   
 $H = H^\dagger$

## Phase Flip (Z-gate)

$$Z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



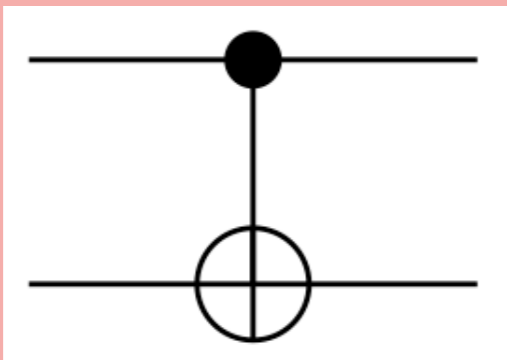
NOT gate in  
the  $|+\rangle, |-\rangle$   
basis

... and many more

# Quantum Gates for Two Qubit Systems

## CNOT

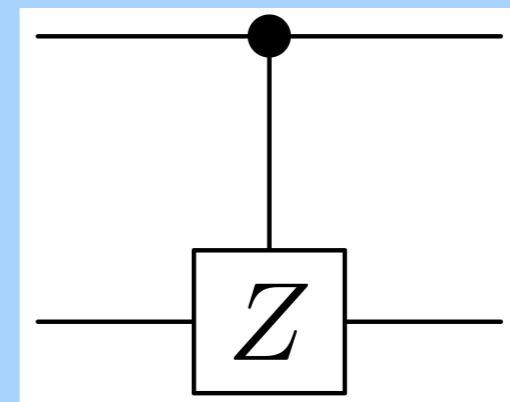
$$CNOT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Flips 2nd (target) qubit iff the first qubit is  $|1\rangle$

## Controlled Z

$$CZ = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

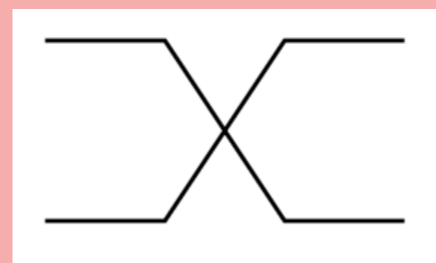
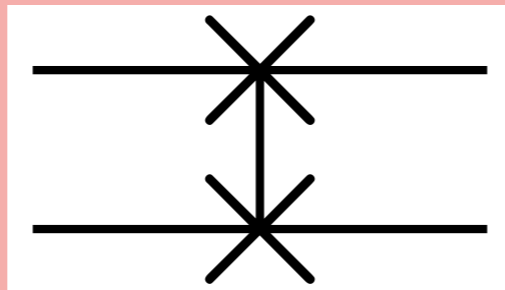


Applies Z-gate to 2nd qubit iff the first qubit is  $|1\rangle$

# Quantum Gates for Two Qubit Systems 2

## SWAP

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

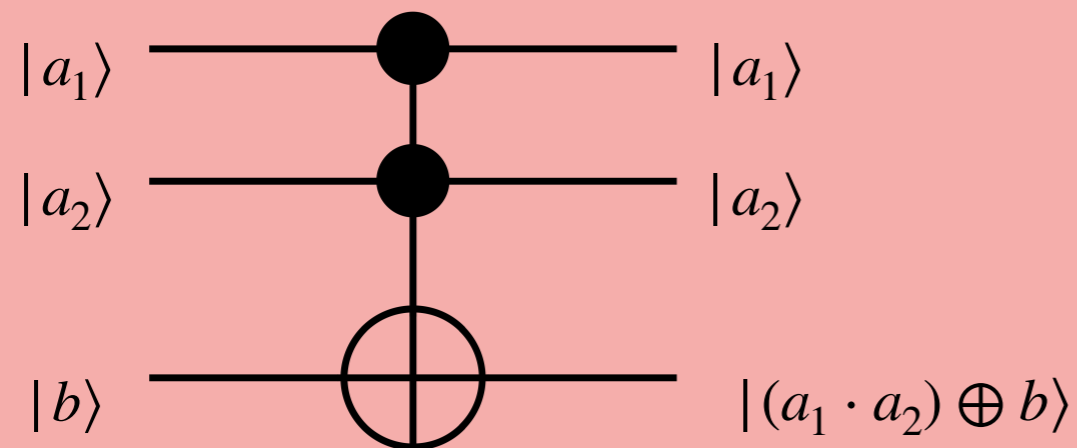


Swaps two qubits



# Toffoli and Fredkin Gates

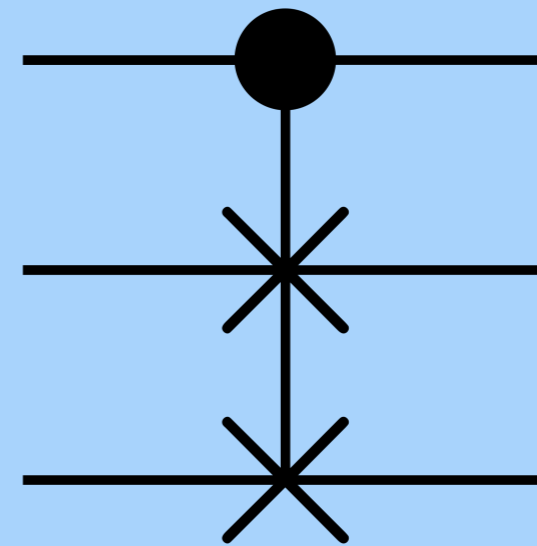
## Toffoli or CCNOT



If the first two bits are 1, the third bit is inverted  
Can be generalized to an n-bit version

Toffoli

## Fredkin or CSWAP



If the first bit is 1, swap the 2nd and 3rd bits

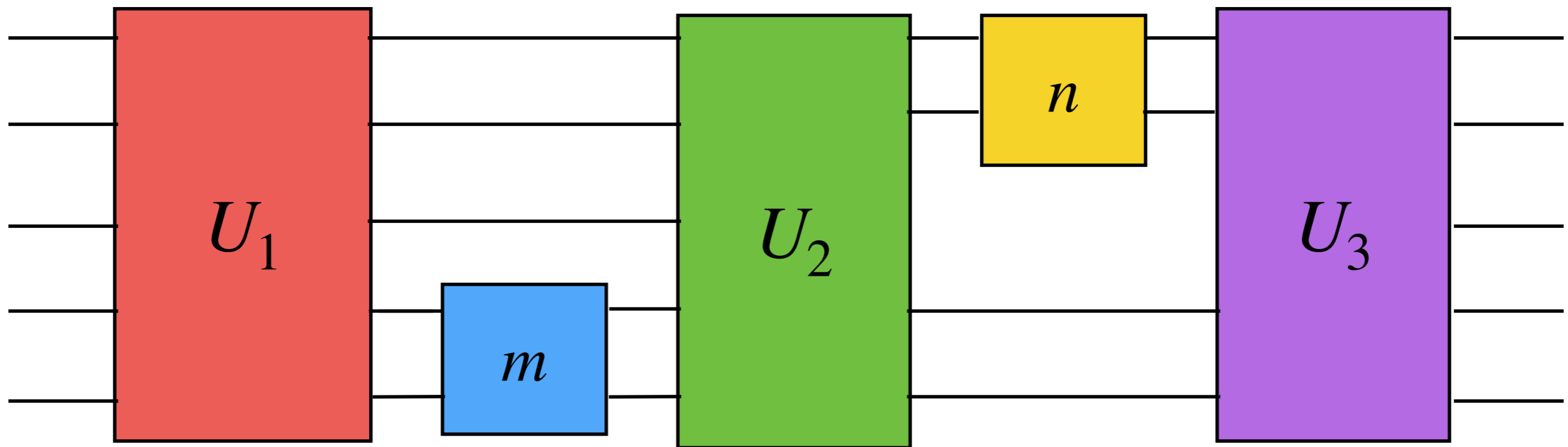
Fredkin

# Universal Gate Sets

- If we want to build a programmable quantum computer, we need it to be able to do any series of quantum operations
- Set of **universal** quantum gates
  - Iff any unitary operation can be approximated to an arbitrary level of accuracy by a finite quantum circuit using only those gates
  - Almost any unitary transformation on a two qubit system can be approximate by a sequence of CNOT and single qubit gates
  - Number of gates =  $O(d^2 \log^3 1/\epsilon)$  (Solovay-Kitaev Theorem)
- Sets of universal quantum gates
  - Phase + Rotation + CNOT
  - Toffoli + Hadamard
  - CNOT + Hadamard+ Phase Flips
- Sets of universal classical gates
  - NAND

# Quantum Circuits

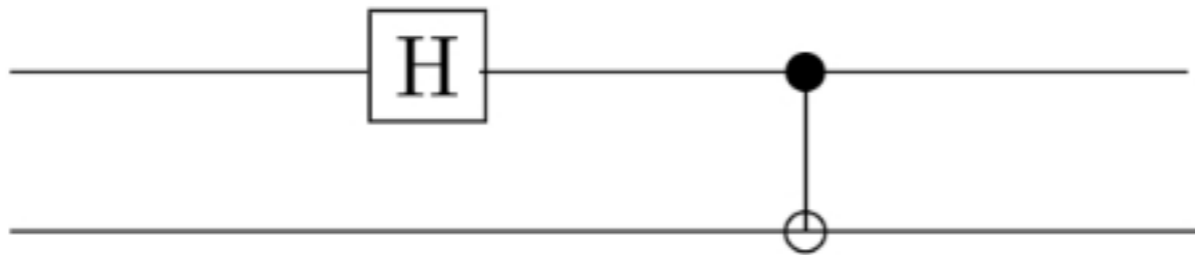
- Qubits and quantum gates can be combined to produce quantum circuits
- Logic flows from left to right
- Qubits are indicated by lines; quantum gates by boxes (or symbols)



# Example: Generate the Bell State

- Generate one of the Bell states

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



- Example: Consider input of  $|0\rangle \otimes |0\rangle$ ?

- Solution:

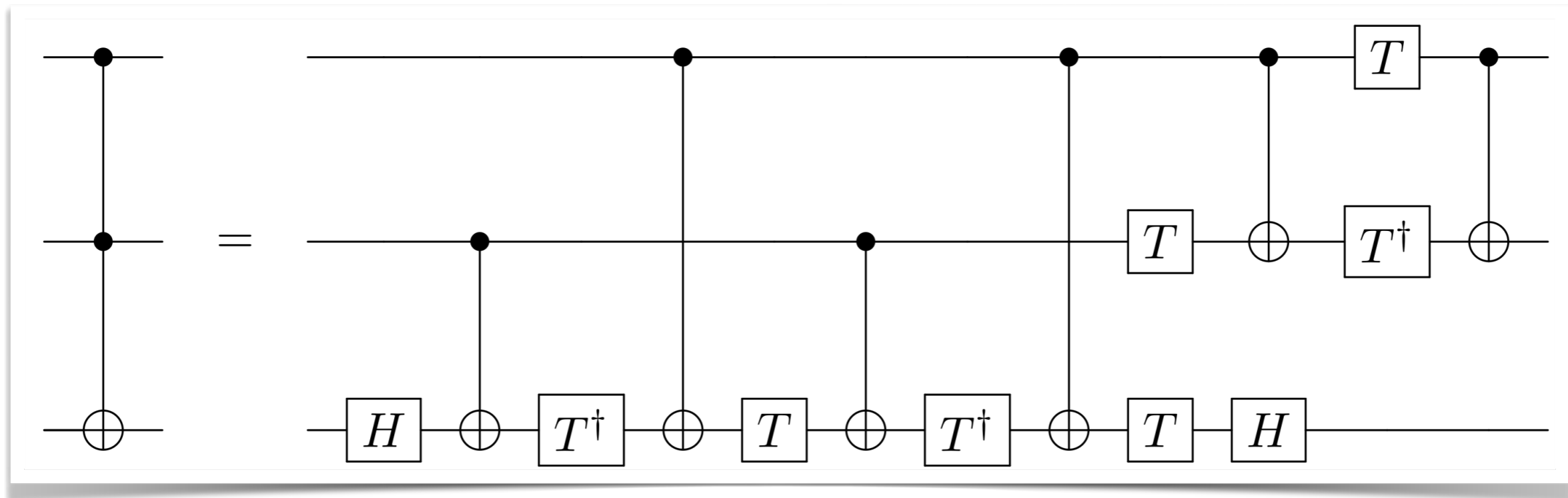
- Step 1:  $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

- Step 2:  $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = |\Phi^+\rangle$

CNOT gate  
entangles the  
qubits

# Construction of Toffoli Gate

*Example circuit constructing the Toffoli gate from single qubit gates*



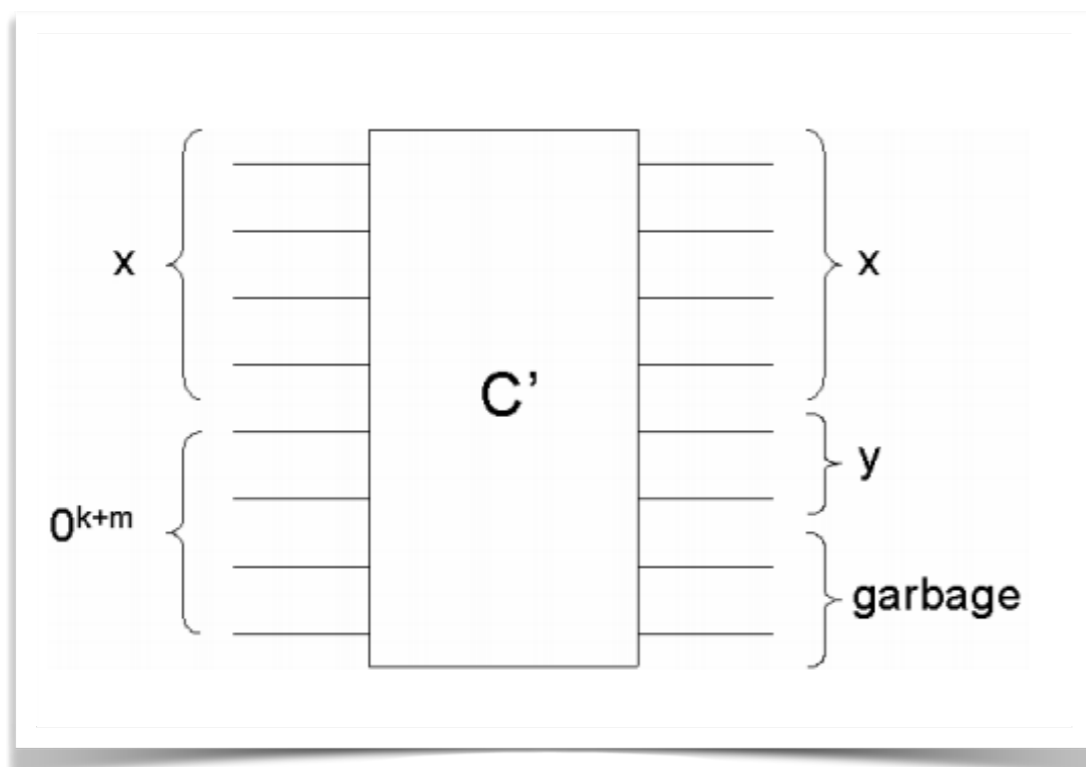
Proof of min gates

Image Credit

# Aside: Reversible Computation

- All quantum evolution is unitary
  - Initially there were concerns that this put constraints on the capabilities of quantum computation
- It turns out, that a reversible circuit can be constructed for any nonreversible circuit
- Example for a circuit  $C$ , where  $y = C(x)$

## Reversible Circuit



## Clean Reversible Circuit

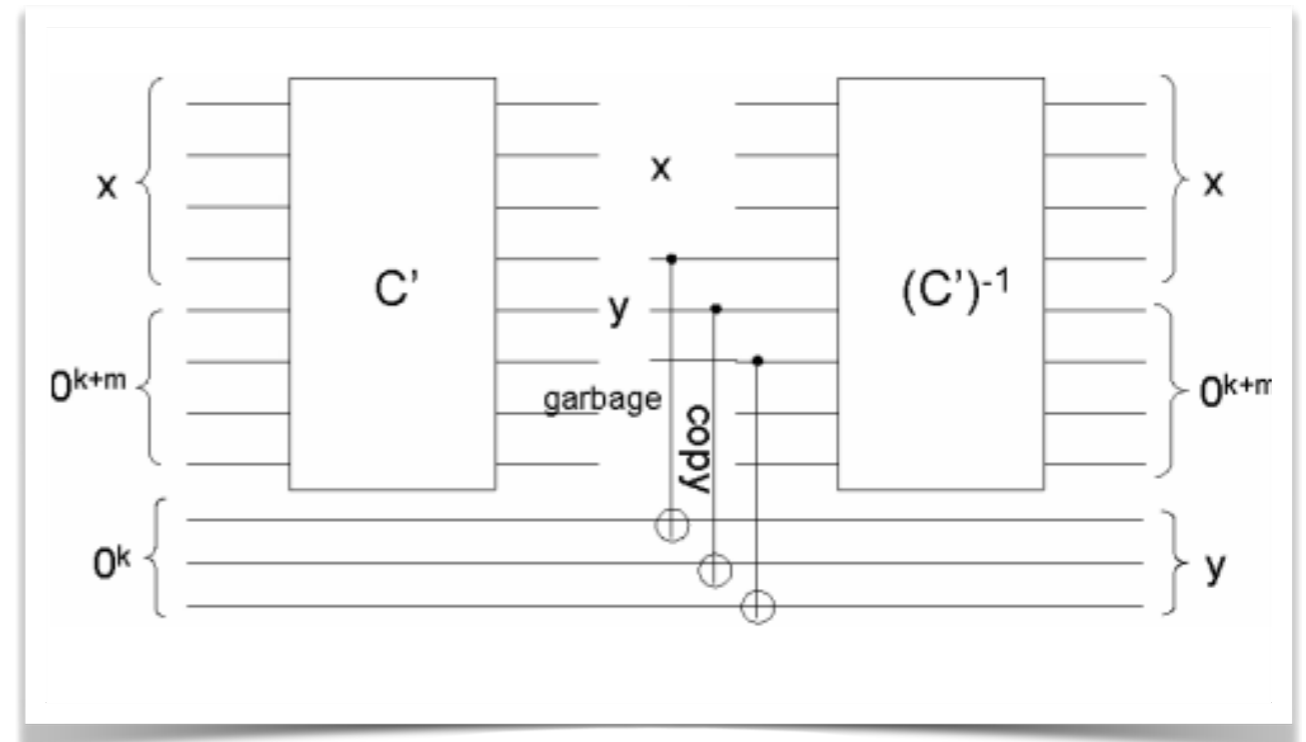
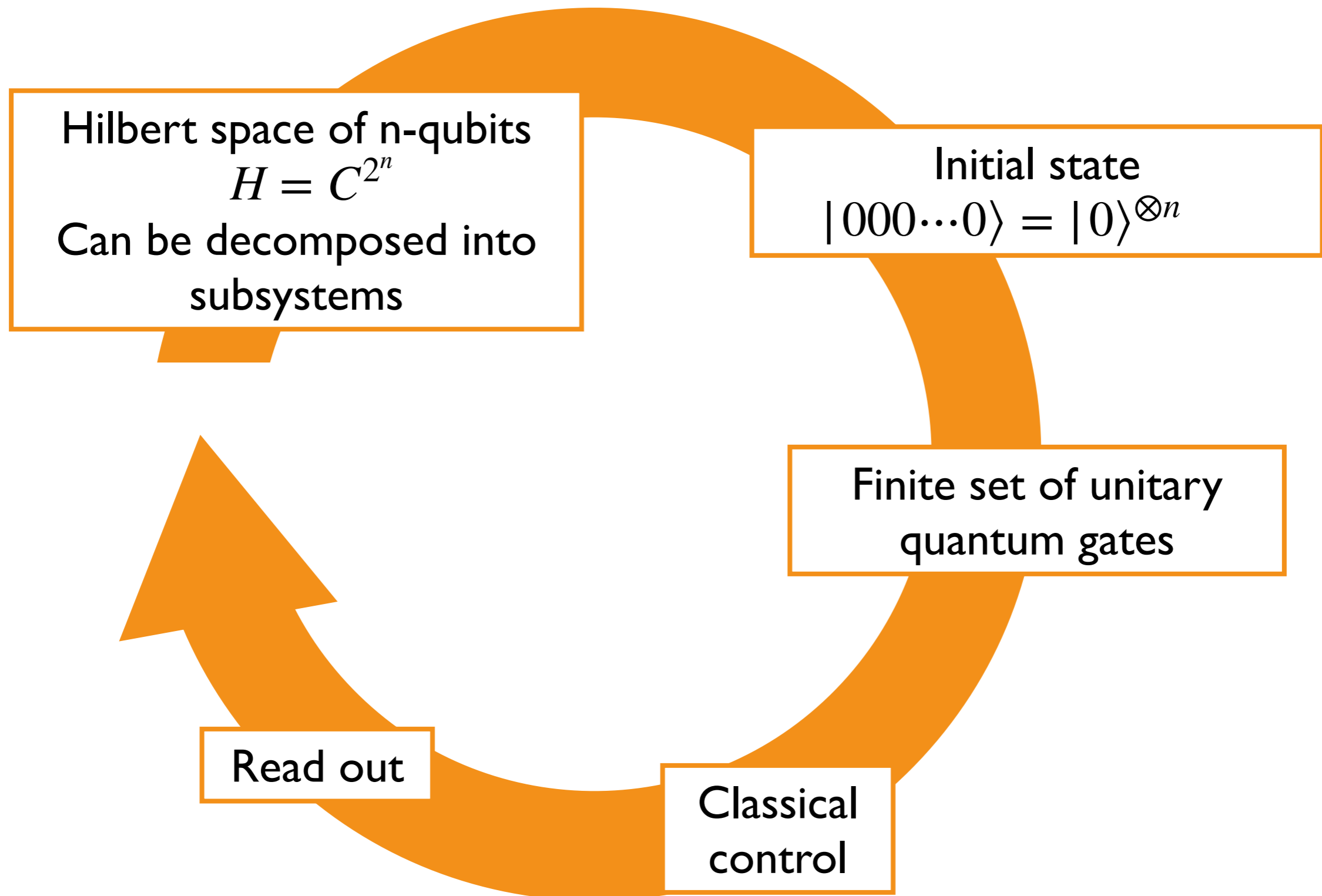


Image Credit: Umesh Varizani



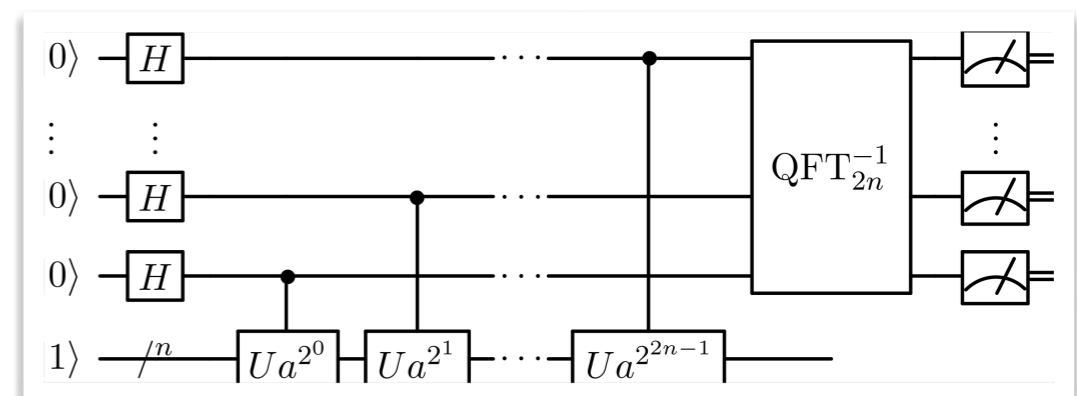
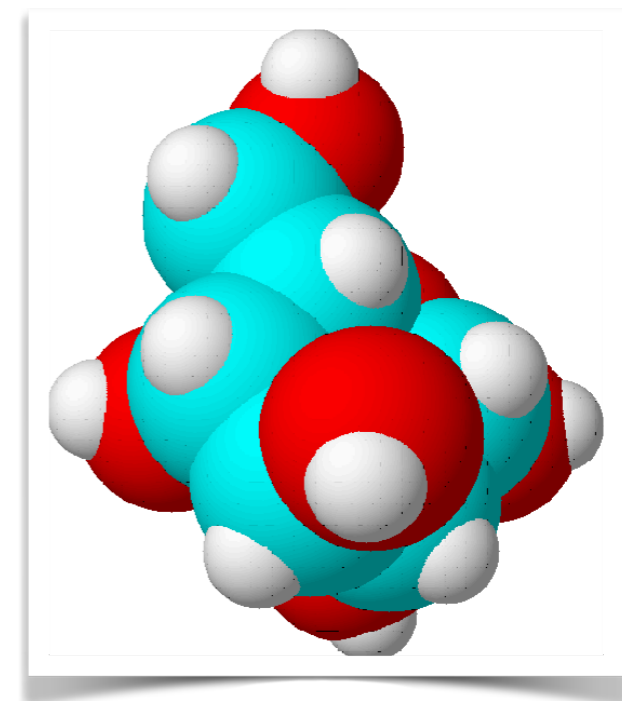
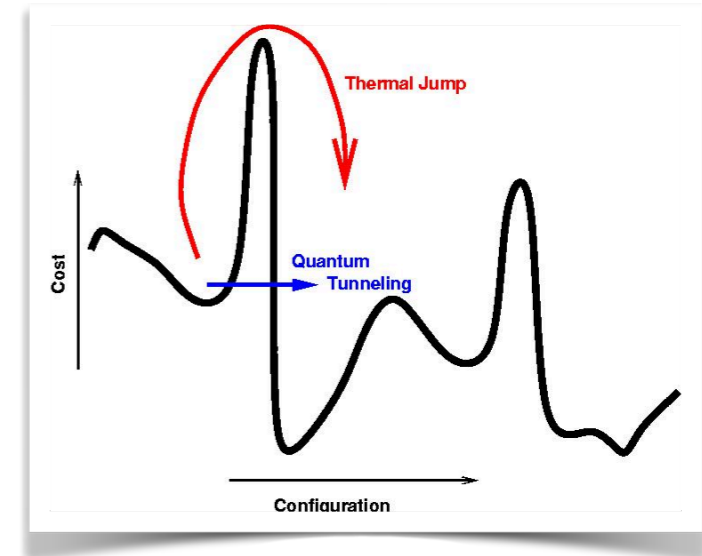
# Circuit Model for a Quantum Computer



# **Building Quantum Computers**

# Types of Quantum Computers

- Analog quantum computers
  - Initialise a quantum state
  - Directly control the Hamiltonian to evolve the state to solve a problem
  - Examples include quantum annealing, adiabatic quantum computing and direct quantum simulation
- Digital quantum computers (or gate based quantum computers)
  - Problems are broken down into primitive operations (gates)
  - Digital outcomes for certain input states
  - Much more similar concept to classical computers



# Analog Quantum Computers

- System of qubits in an initial quantum state
- Change the Hamiltonian to encode the problem in the final Hamiltonian
- Final state is the answer
  - System remains in ground state: adiabatic quantum computing
  - Otherwise: quantum annealing
- For highly complex Hamiltonians, AQC is equivalent in computational power to gate based quantum computers
- However, existing quantum annealers have limited choices for the Hamiltonian
- Direct simulation: set Hamiltonian to that of the system of interest
  - Evolution models that system

# Building gate-based quantum computers

- DiVincenzo criteria to quantify how to build a gate-based QC
  - Quantum **two-level system** that can be employed as qubits
  - Ability to **initialize qubits**
  - Sufficient **decoherence time** to complete computation
  - Set of **universal quantum gates**
  - Ability to **measure** quantum bits
- Next, let's briefly review some examples of current technologies that have been used or considered to build quantum computers

# Types of Qubit

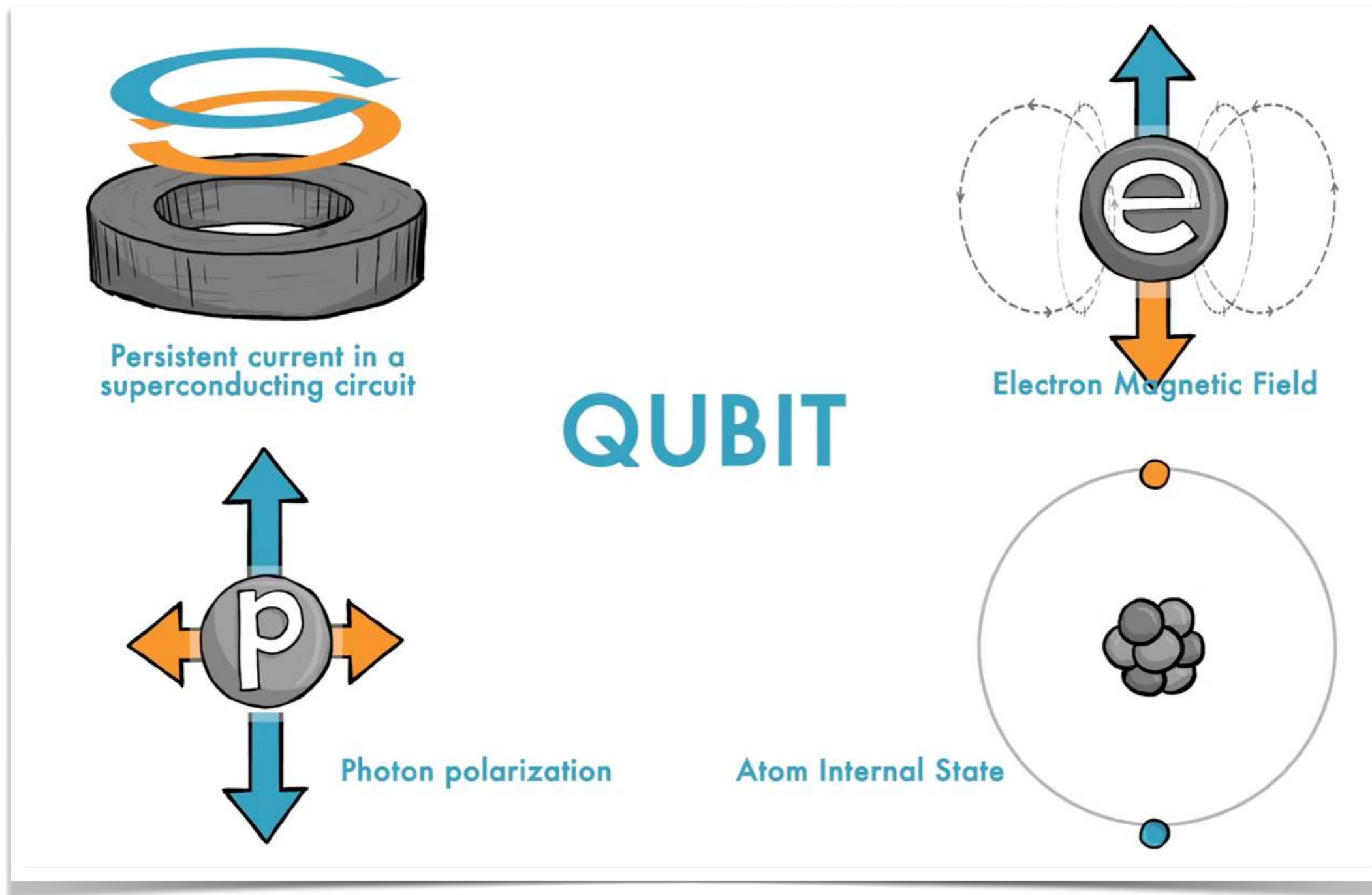


Image Credit: John Preskill

# Types of Qubits

EXHIBIT 7 | Overview of Leading Quantum Computing Technologies During the NISQ Era

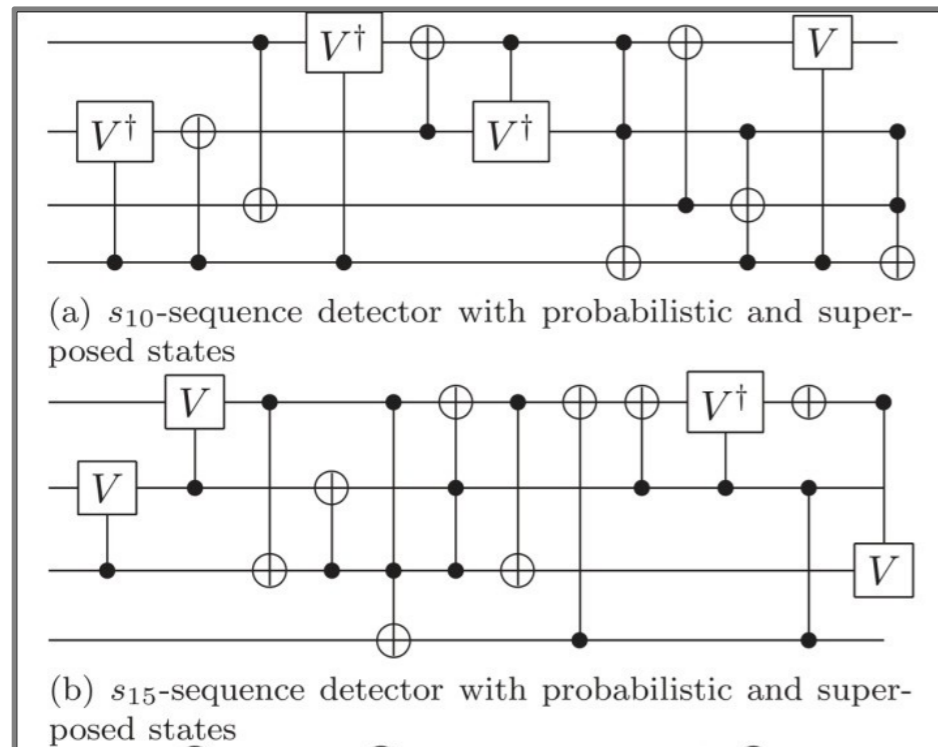
	Leading technologies in NISQ era <sup>1</sup>		Candidate technologies beyond NISQ		
	Superconducting <sup>2</sup>	Trapped ion	Photonic	Silicon-based <sup>3</sup>	Topological <sup>8</sup>
Qubit type or technology					
Description of qubit encoding	Two-level system of a superconducting circuit	Electron spin direction of ionized atoms in vacuum	Occupation of a waveguide pair of single photons	Nuclear or electron spin or charge of doped P atoms in Si	Majorana particles in a nanowire
Physical qubits <sup>4,5</sup>	IBM: 20, Rigetti: 19, Alibaba: 11, Google: 9	Lab environment: AQT <sup>6</sup> : 20, IonQ: 14	6×3 <sup>9</sup>	2	target: 1 in 2018
Qubit lifetime	~50–100 μs	~50 s	~150 μs	~1–10 s	target ~100 s
Gate fidelity <sup>7</sup>	~99.4%	~99.9%	~98%	~90%	target ~99.9999%
Gate operation time	~10–50 ns	~3–50 μs	~1 ns	~1–10 ns	–
Connectivity	Nearest neighbors	All-to-all	To be demonstrated	Nearest neighbor	–
Scalability	No major road-blocks near-term	Scaling beyond one trap (>50 qb)	Single photon sources and detection	Novel technology potentially high scalability	?
Maturity or technology readiness level	TRL <sup>10</sup> 5	TRL 4	TRL 3	TRL 3	TRL 1
Key properties	Cryogenic operation Fast gating Silicon technology	Improves with cryogenic temperatures Long qubit lifetime Vacuum operation	Room temperature Fast gating Modular design	Cryogenic operation Fast gating Atomic-scale size	Estimated: Long lifetime High fidelities

Any two state quantum system

**Sources:** BCG analysis; expert interviews.  
<sup>1</sup>Noisy Intermediate-Scale Quantum devices era.  
<sup>2</sup>Currently only technology with external cloud access; several forms (charge, flux, phase) of qubits exist but most pursue a less noise-sensitive charge-based qubit (transmon).  
<sup>3</sup>Additional approaches include Si and SiGe quantum dots.  
<sup>4</sup>Demonstrated ability to perform single and two-qubit gates.  
<sup>5</sup>Announcements of next-generation qubit architecture: Intel: 49, IBM: 50, Google: 72, Rigetti: 128 (all superconducting qubits), IonQ: 50 (trapped ion), Hefei University: 50 (photonic).  
<sup>6</sup>Alpine Quantum Technologies.  
<sup>7</sup>Two-qubit fidelity.  
<sup>8</sup>Microsoft roadmap to build first quantum computer in 2023.  
<sup>9</sup>18 qubits were encoded with six photons using three degrees of freedom.  
<sup>10</sup>Technology readiness level.

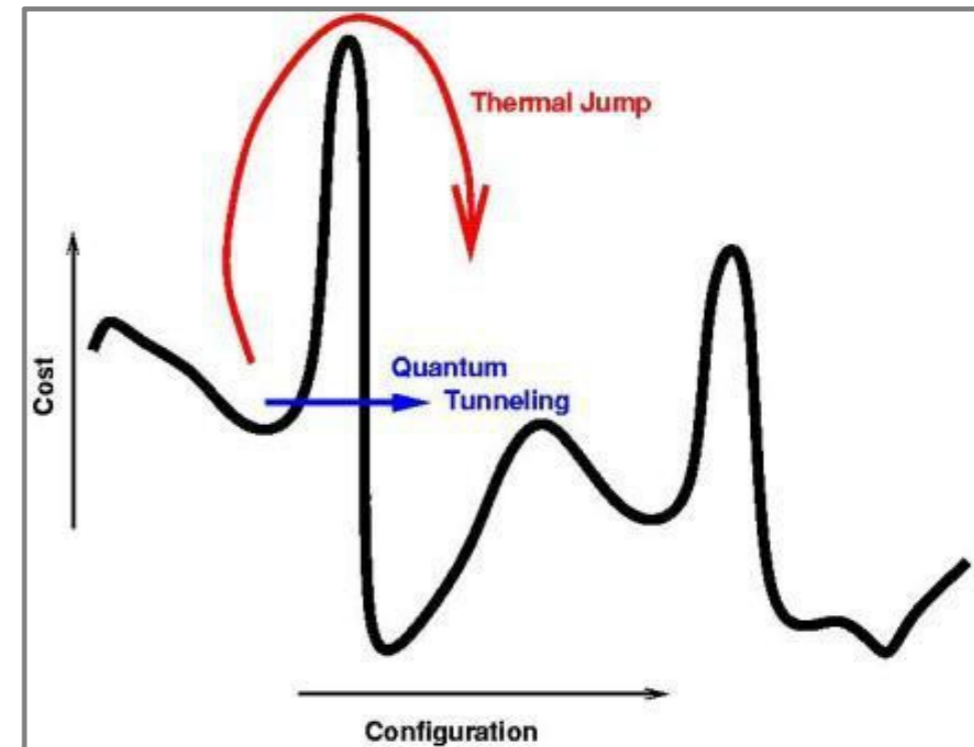
# Qubit and qubit

## Universal quantum computers vs quantum annealers



### Quantum Circuits

Series of quantum gates operating on a set of quantum states.



### Quantum Annealing

Evolution of a quantum system to a low T Gibbs state  
**That's D-Wave !**



# Trapped Ion

- One of the earliest types of quantum computers
- Strip atoms of their outer electron
  - Positively charged ions are controlled by electric fields in ion traps
- Contained in ultra-high vacuum chambers
- Lasers cool the ions to very low temperatures (e.g. 0.1 - 1 mK)
- Ion states are controlled using laser pulses or microwave radiation
  - Can couple ions together

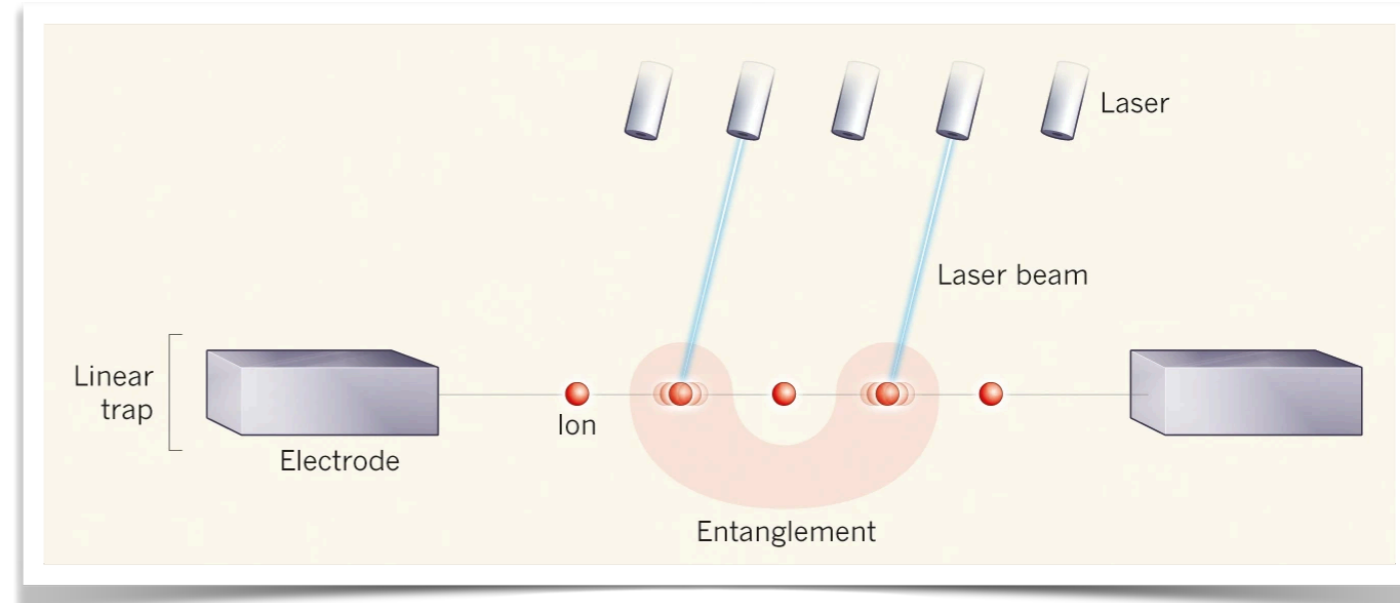


Image Credit

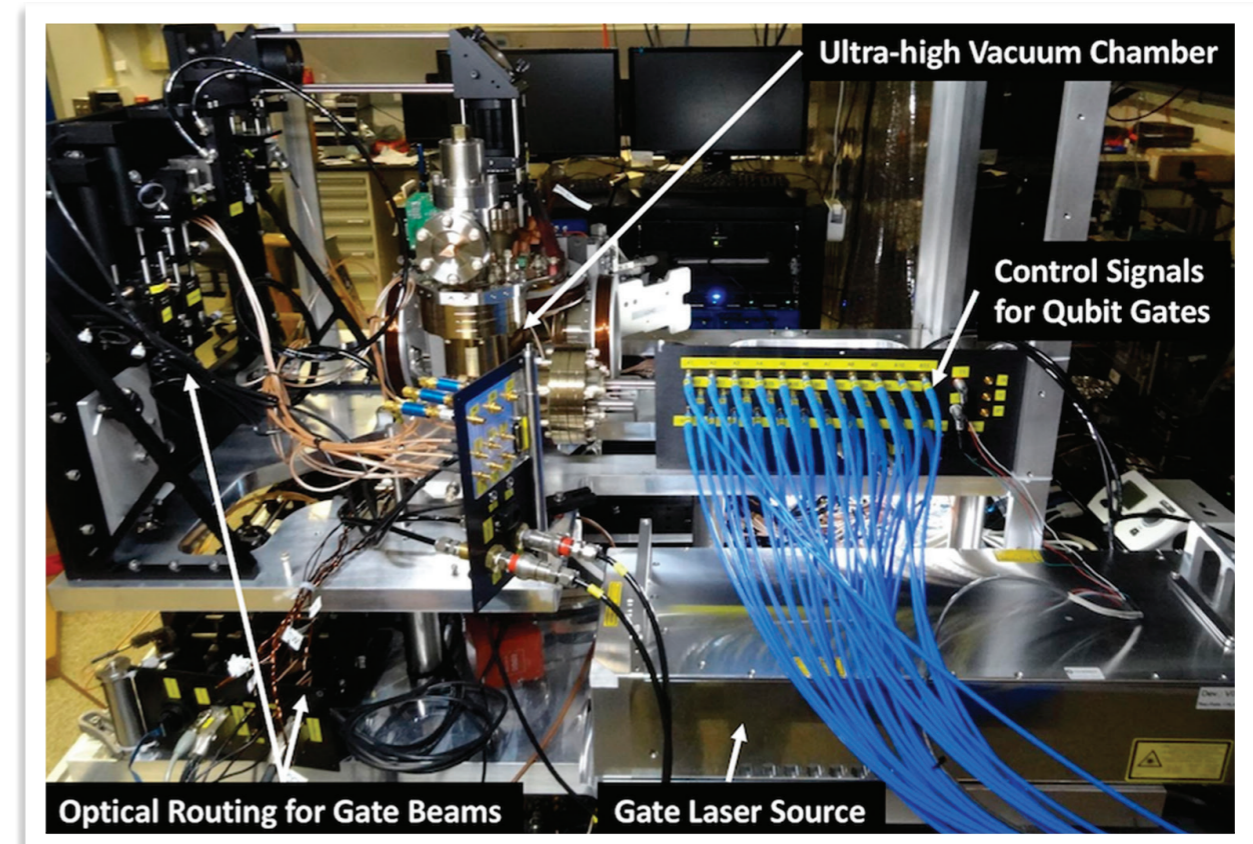


Image Credit

# Superconducting Qubits

- Currently one of the most commonly used technologies for NISQ computers
- Create an artificial atom using superconducting materials
  - Josephson junction
- Build arrays using similar process to manufacturing ICs
- Manipulate states using microwave radiation
- Cool in dilution refrigerators below 100 mK
- Types: phase, charge and flux qubits

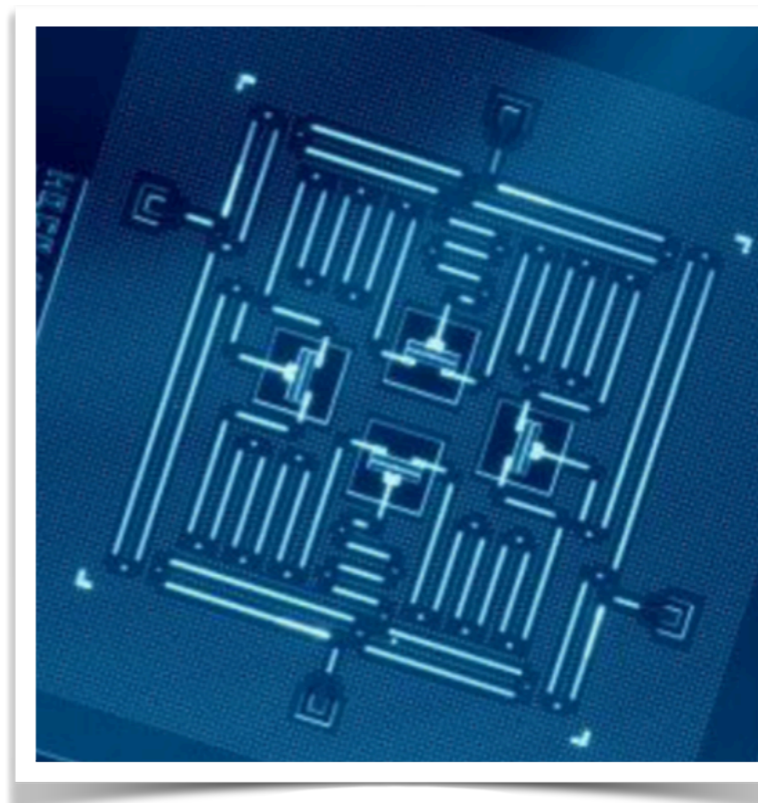
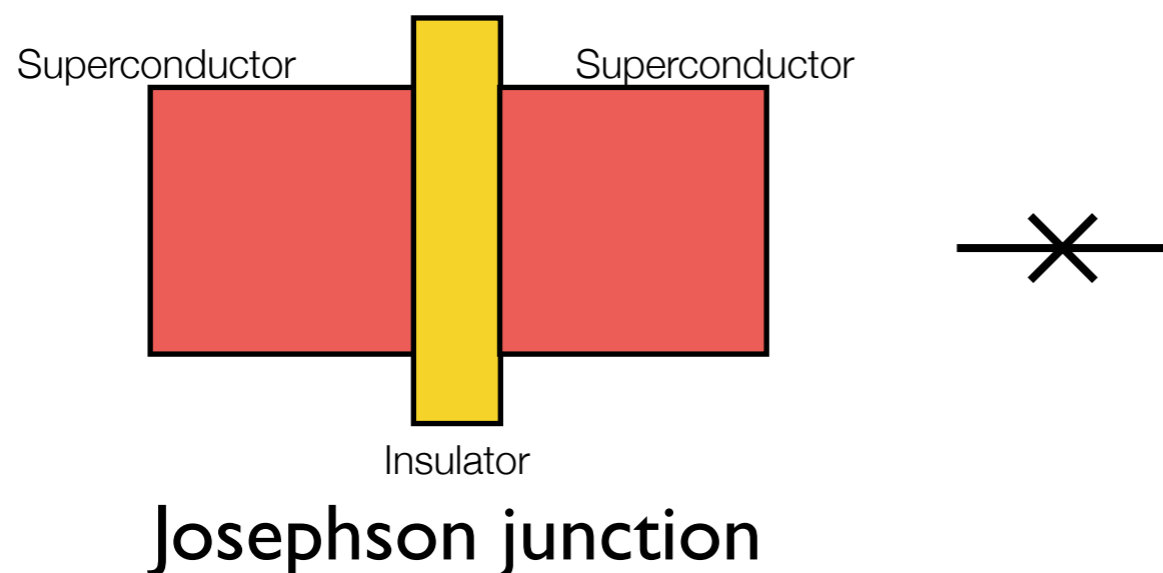
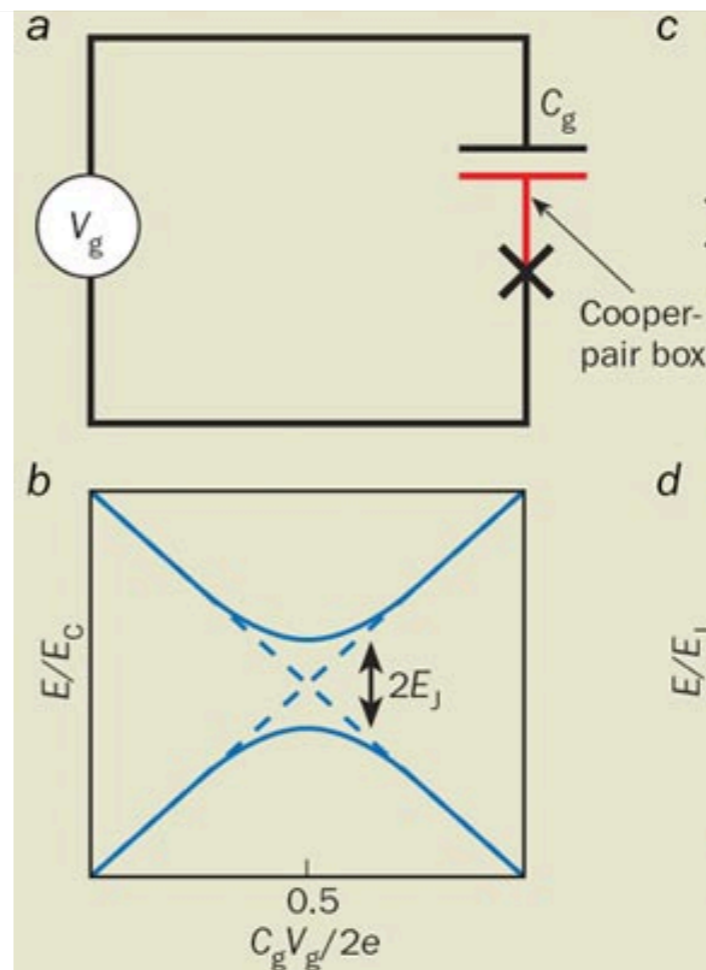


Image Credit

# Superconducting qubits

- Charge qubit
  - Josephson junction, capacitor and voltage
  - Cooper pair box (red)
    - Superposition of zero or one extra pairs in box
- Flux qubit
  - Loop of Josephson junctions, external magnetic flux
  - Superposition of currents circulating clockwise or anti clockwise
- Phase qubit
  - Single Josephson junction
  - Quantum oscillations of phase difference between electrodes

## Charge qubit



## Flux qubit

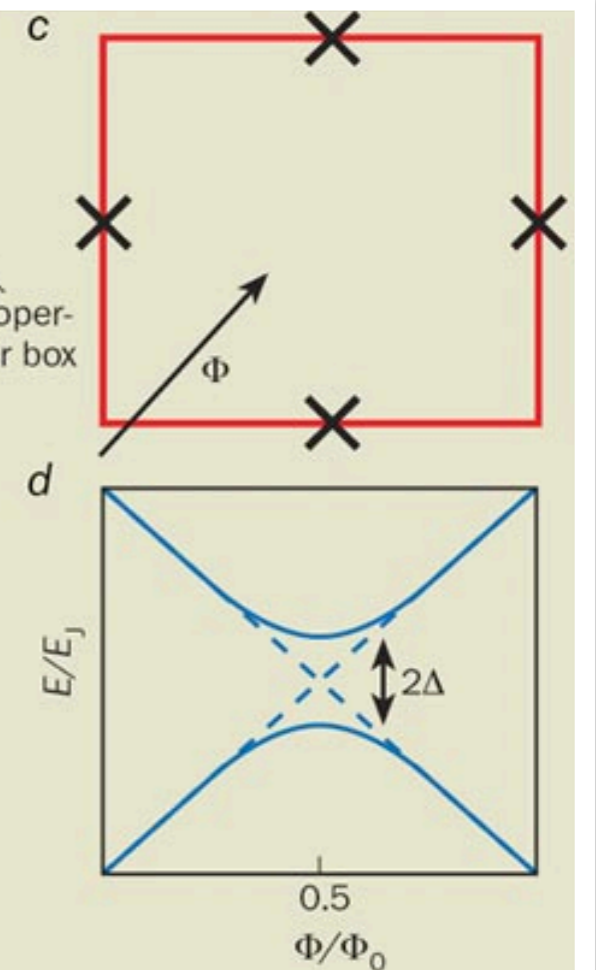
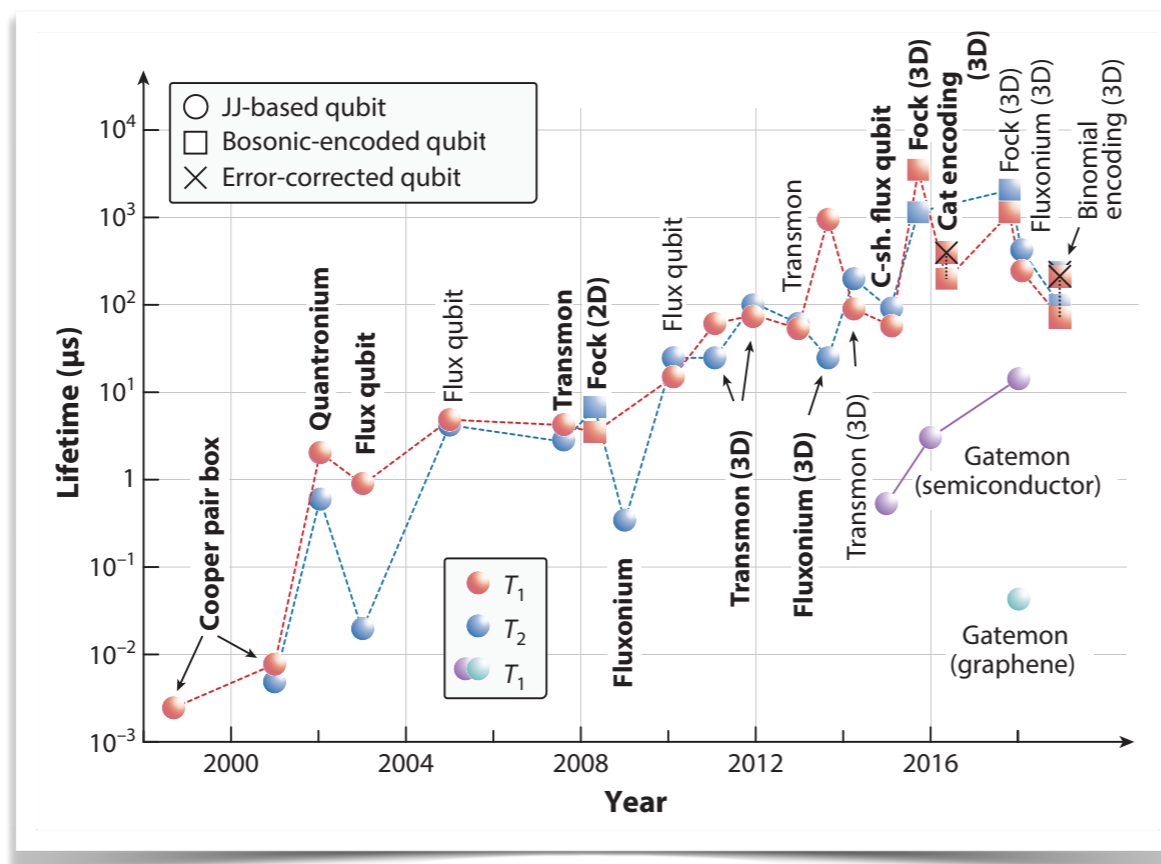
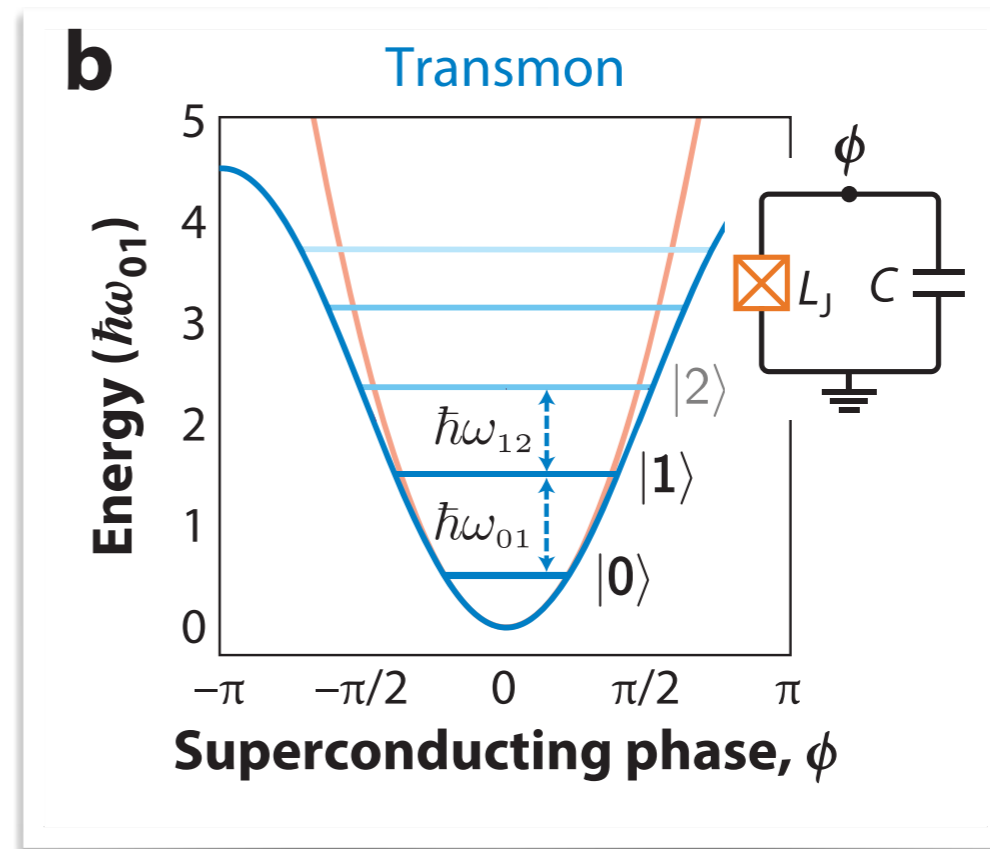
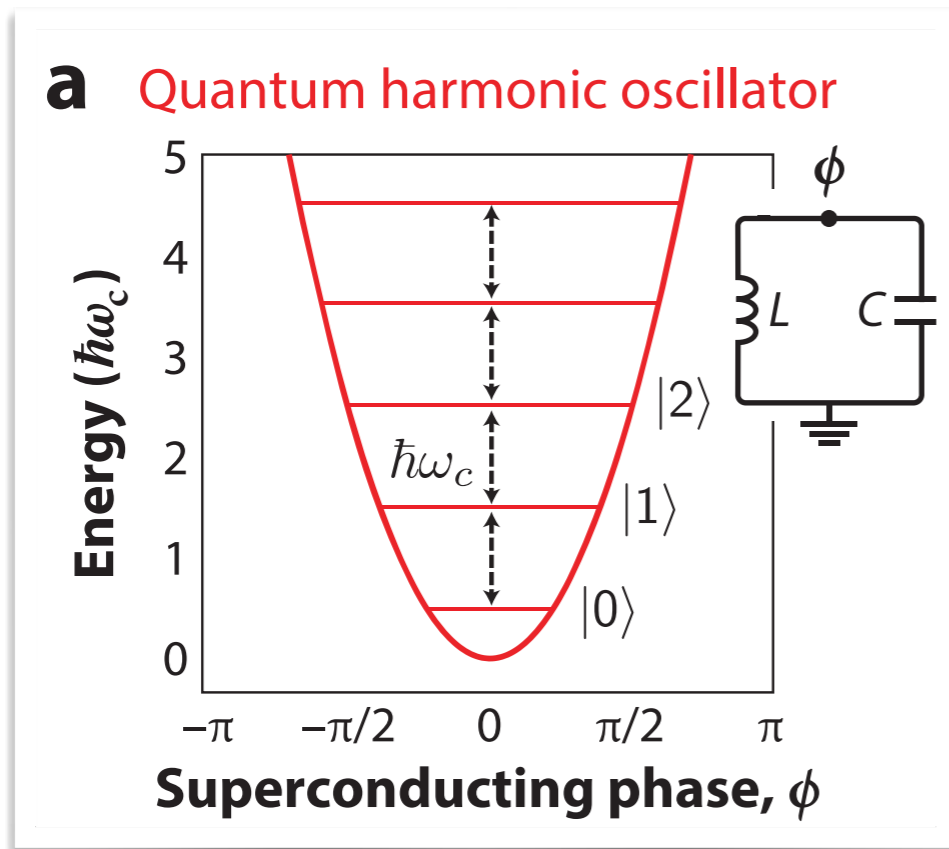


Image Credit



# Transmon charge qubits



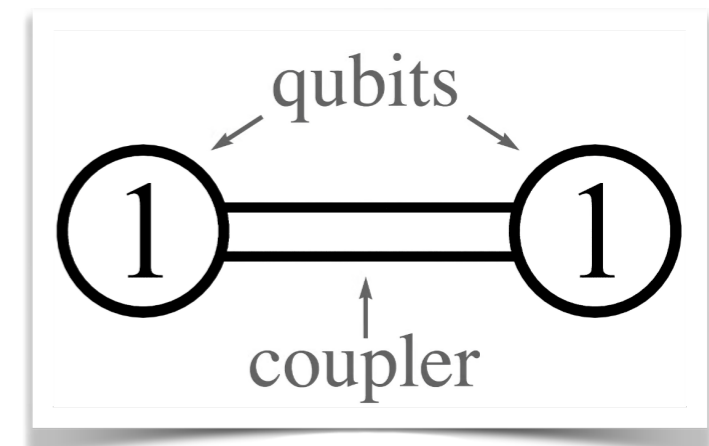
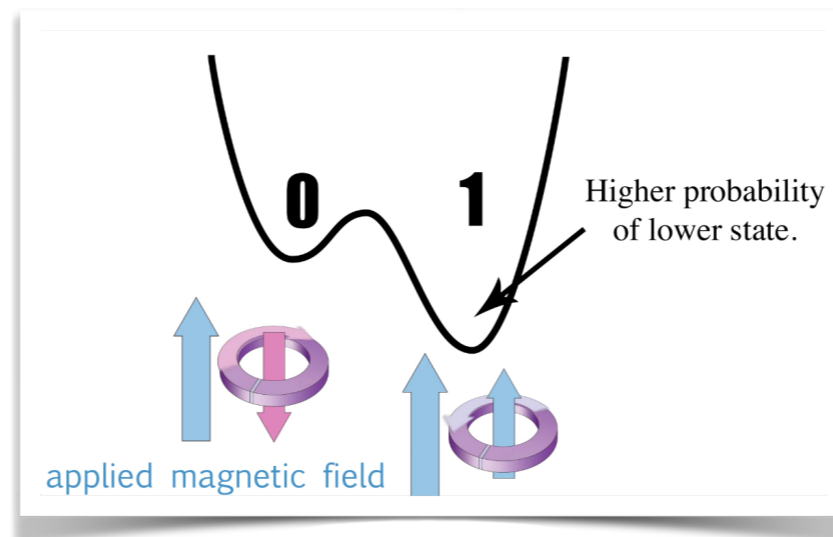
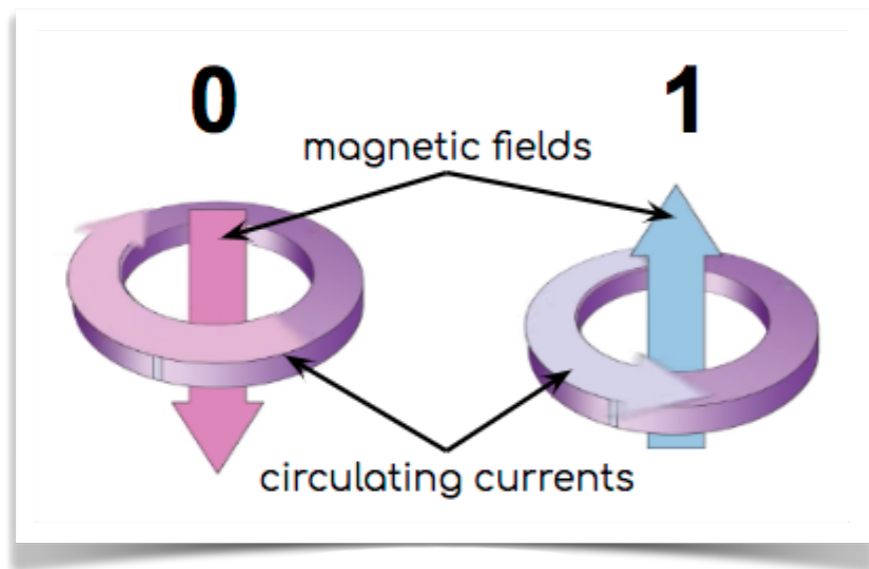
Transmon=transmission  
line shunted plasma  
oscillation qubit

Annu. Rev. Condens. Matter Phys.  
2020. 11:369–95

Transmon qubits

# Quantum Annealers

source: [dwavesys on YouTube](#)



qubits  $\Rightarrow q_i$

bias weights  $\Rightarrow$

$a_i$

coupling strength  
 $\Rightarrow b_{ij}$

$$O(a; b; q) = \sum_{i=1}^N a_i q_i + \sum_i \sum_j b_{ij} q_i q_j \quad q_i \in \{0, 1\}$$

QUBO

Quadratic  
Unconstrained  
Binary Optimisation



*Don't expect speed up over classical computation with quantum annealers*

Slide credit: L. Linder

# Photonic

- Also known as boson sampling, quantum computer using photons
- Circuit constructed from squeezed photons, beam splitters and photon counters

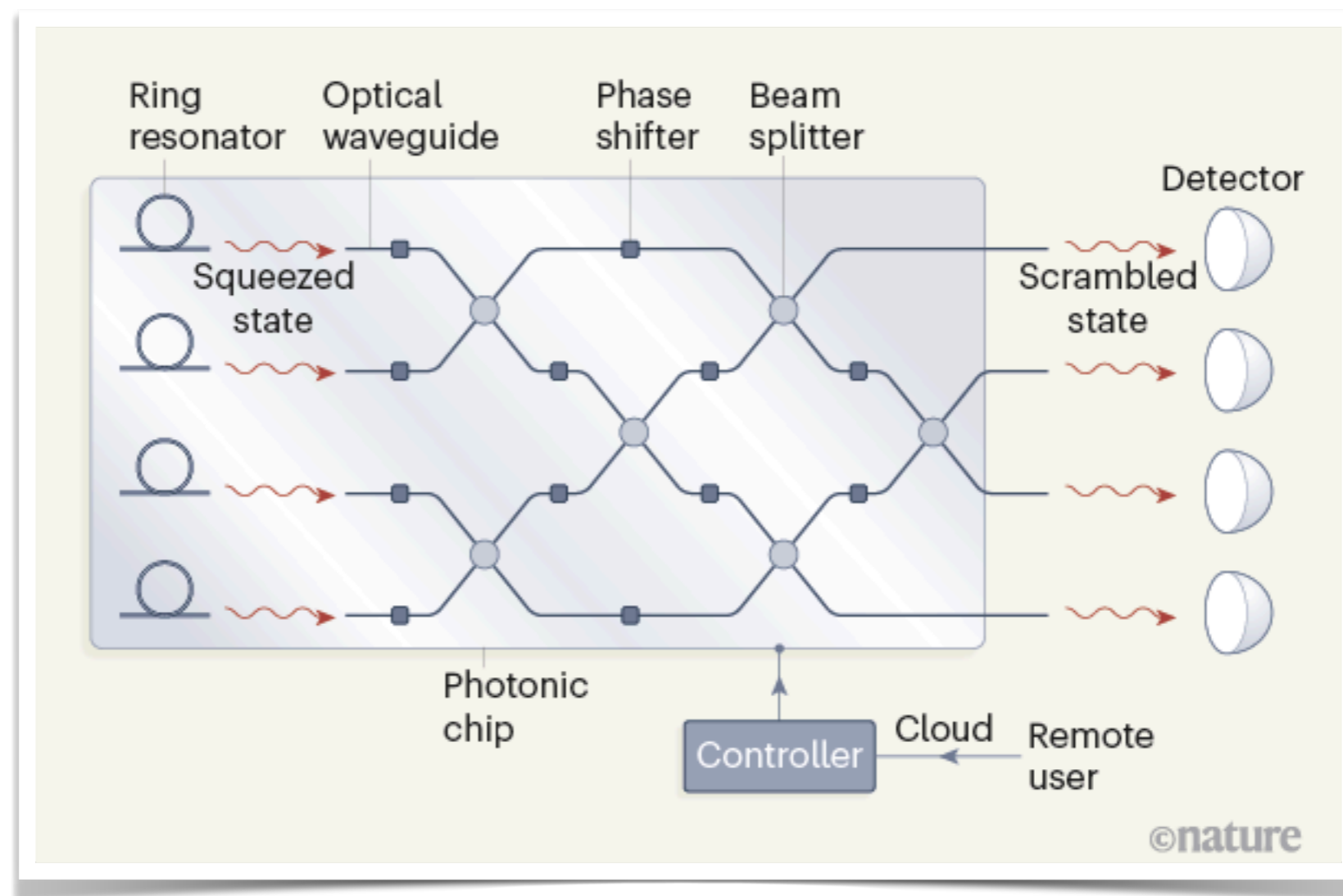


Image Credit

# Silicon-based

- Original idea for silicon-based quantum computers in 1998
- Store qubits in nuclear spins in phosphorus atoms in silicon
- Demonstrations of one (2012) and two (2019) qubit operations using phosphorus
- Alternatively, one can use quantum dots

Illustration of a circuit to realize a spin qubit

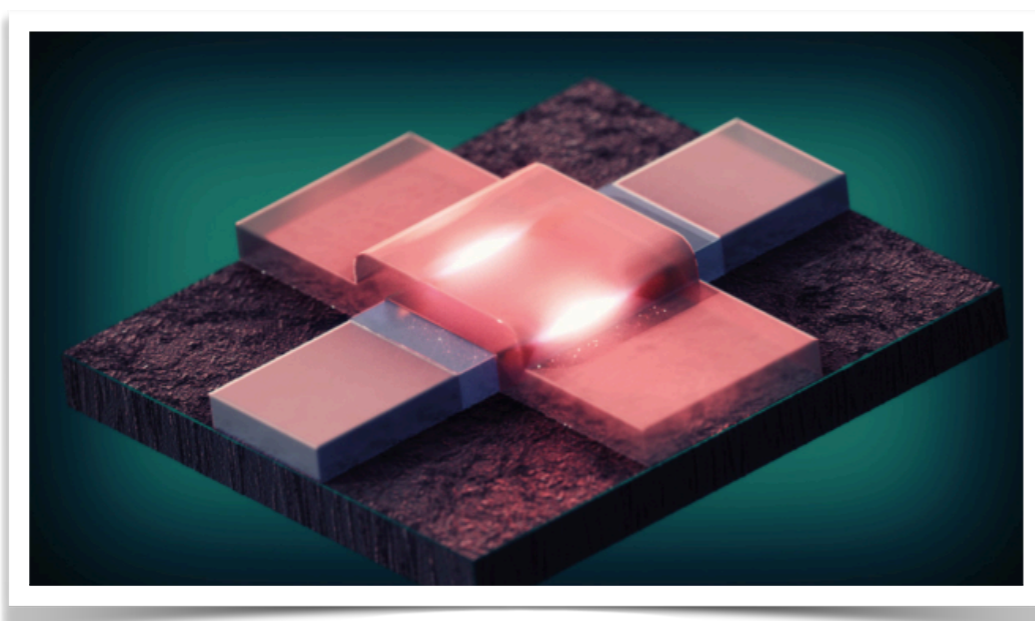


Image Credit

## Manipulating electron spins

A schematic of the two-electron-trap sample used by Zajac *et al.* is shown. Negatively biased electrostatic gates (gray) form tunnel barriers, whereas positively biased gates (brown) accumulate electron reservoirs or exactly two electrons in the double-dot potential. Each electron spin qubit can be separately set in quantum superposition state, or the two qubits can be entangled with the microwave and voltage pulses.

**1** Stray field from micromagnet couples electron spins to the electric field.

**2** Strain in Si layer vertically confines electrons.

**3** Potential created by metal gates laterally confines electrons.

**4** Spin alignment of the electrons is controlled with microwaves and voltage pulses.

**5** Tunnel coupling through the barrier between the two electrons (blue) causes an exchange interaction between the two spins, which drives entanglement.

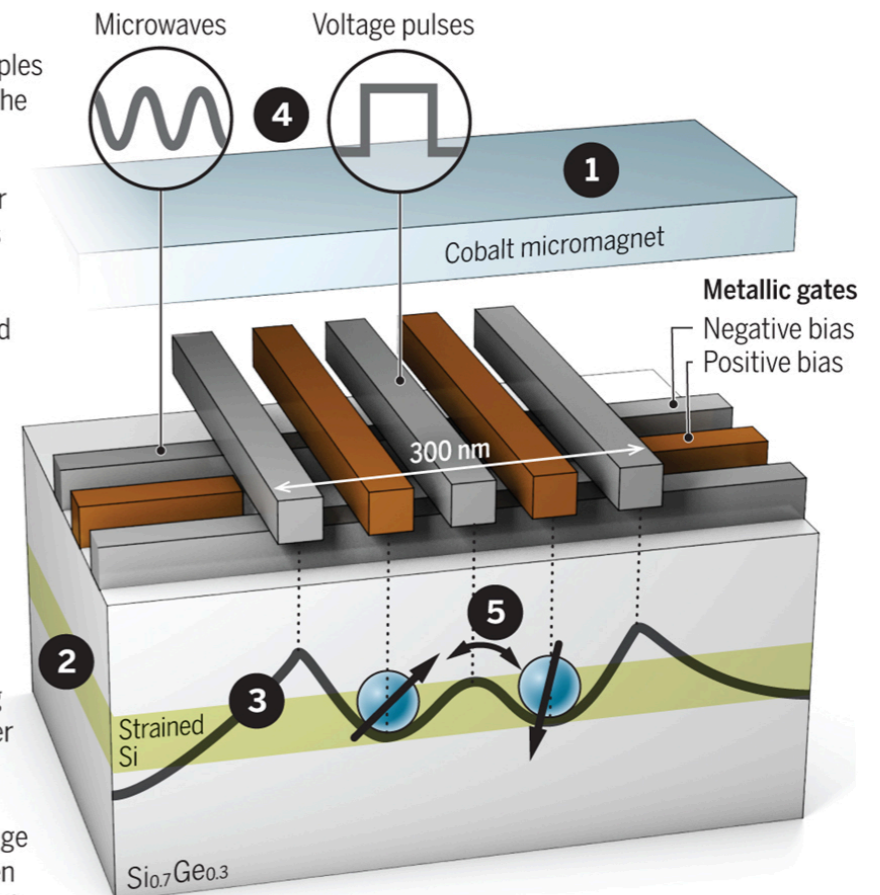
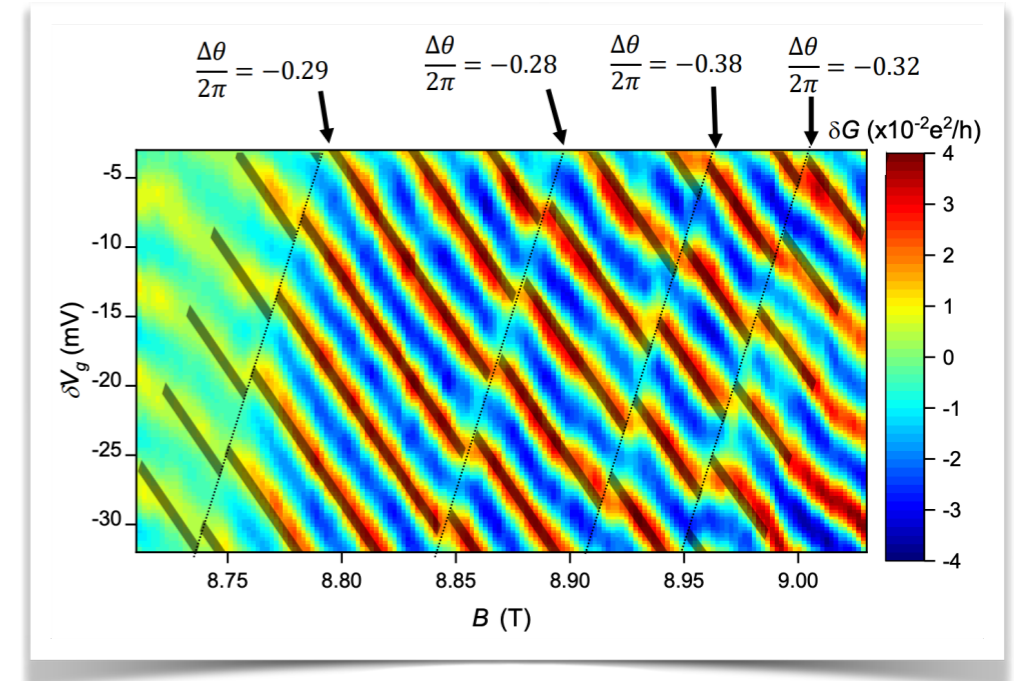


Image Credit



# Topological Quantum Computers

- Exploit topology to build quantum computers that are more robust to outside interference and noise, ref: Kitaev
- Qubits would be anyons (quasiparticles with statistics interpolating between fermions and bosons)
- A potential route to topological quantum computers would use Majorana particles
  - Form two Majorana particles (~half electrons) on both ends of a semiconductor wire wrapped with a superconductor
  - Qubit is made by encoding information by swapping the positions of the particles on the wire
  - Strategy pursued by Microsoft
- Claimed observation of Majorana zero modes: paper, retraction



arXiv:2006.14115



# Conclusion

- Quantum computers hold exceptional promise to transform computation
  - Their realization requires overcoming many significant challenges
- Brief introduction to the historical development of the field of quantum information and quantum computing
- Qubits are the basic units of quantum computation
  - Wide range of possible realizations: trapped ions, superconducting, to photons and topological quantum computers
- Quantum gates operate on qubits to change their states
- Quantum gates are combined into quantum circuits to perform quantum algorithms (more tomorrow)
- A wide range of technologies are being explored to produce qubits
  - Superconductors, trapped ion, photonic, silicon based
- Tomorrow, we'll bring this together by discussing some current quantum computers, quantum algorithms, quantum advantage and quantum error correction

# Further Reading

- Online resources
  - Scott Aaronson's blog
  - Umesh Varizani's introductory course
  - John Preskill's graduate course, lecture notes, youtube playlist
- Books
  - Nielsen and Chuang
  - Kitaev, Shen and Vyalyi
  - Aaronson
  - Watrous
  - Wilde