## Implementations:

## Building a Quantum Computer

## Why build a quantum computer?

- Grover's algorithm
  - Provides a quadratic speed-up over best possible classical algorithms
- Shor's algorithm
  - Provides an exponential speed-up over best known classical algorithms
- Quantum simulations
- Moore's law
  - Shrinking transistors will eventually mean quantum effects will dominate classical devices

## Why NOT build a quantum computer?

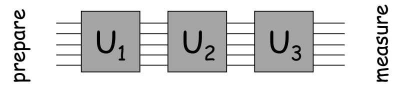
- Extremely difficult
- Impossible?
  - Does not contradict any law of physics

## Implications of building a quantum computer

- Most of the world's sensitive data is encrypted using public-key encryption systems such as RSA
- A quantum computer gives the owner the ability to crack these encryption systems
- We need to know if a quantum computer can be built, and who could build a quantum computer
- A quantum computer in the hands of terrorists could cause anarchy

## Why is building a quantum computer so difficult?

- Intuitively: the world appears classical




- We need excellent control in order to prepare qubits, apply exactly the right sequence of operations and then measure the qubits.
- However, the second postulate of quantum mechanics states that <u>only</u> closed quantum systems evolve unitarily.

## DiVincenzo's criteria

1. A scalable physical system with well characterized qubits.
2. The ability to initialize the state of the qubits to a simple basis state.
3. Long (relative) decoherence times, much longer than the gate-operation time.
4. A universal set of quantum gates.
5. A qubit-specific measurement capability.

**<u>QC Networkability</u>**

6. The ability to interconvert stationary and flying qubits.
7. The ability to faithfully transmit flying qubits between specific locations.

## Decoherence

- We say that a quantum system decoheres when it starts acting in a classical fashion rather than as predicted by quantum mechanics.
- Decoherence is due to unwanted and uncontrolled interactions of a system with its environment.
- The ket formalism is ideal for the study of completely quantum systems.
- When classical probabilities are involved we need to use the density matrix formalism.

## Decoherence

- We have seen that an arbitrary pure state of a qubit can be written as

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

- What if we want to describe a system which is either in the state |0> or |1> ?
- We write pure states as matrices of the form

$$|\psi\rangle\langle\psi|$$

- We write mixed states as convex combinations of pure states, for example

$$0.7|\psi\rangle\langle\psi| + 0.3|\phi\rangle\langle\phi|$$

## Decoherence

- Imagine we have the pure state

$$\tfrac{1}{2}|00\rangle\langle 00| + \tfrac{1}{2}|00\rangle\langle 11| + \tfrac{1}{2}|11\rangle\langle 00| + \tfrac{1}{2}|11\rangle\langle 11|$$

- If we measure the second qubit and obtain the result 0, then we know the first qubit is in the pure state

$$|0\rangle\langle 0|$$

- If "somebody else" measures the second qubit, and doesn't tell us the result, then we have the mixed state

$$0.5|0\rangle\langle 0| + 0.5|1\rangle\langle 1|$$

- Which is quite different from the state

$$\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|0\rangle\langle 1| + \tfrac{1}{2}|1\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|$$

## Schemes for implementing a quantum computer

Spectral hole burning

Nuclear Magnetic Resonance

Optical

Quantum dots

Trapped Ion

Neutral Atom

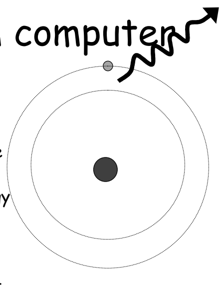
e-Helium

Superconducting

Gated qubits

Doped silicon

## Ion trap quantum computer

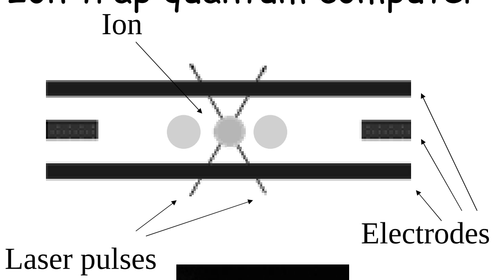


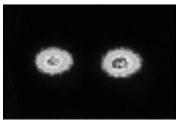
- Consider a hydrogen atom
  - Composed of a proton
  - And an electron
  - The energy levels of the electron are quantized
  - The electron can move down an energy level by releasing a photon
  - Or up an energy level by absorbing a photon
  - If we called the ground state (lowest energy level) |0>, and the first excited state |1>, we'd have a qubit
  - There are many reasons why using hydrogen as a qubit would be impractical

## Ion trap quantum computer

- Instead, we use elements such as beryllium.
- Ionize the atoms.
- Contain the ions in an electromagnetic field, such as a linear Paul trap

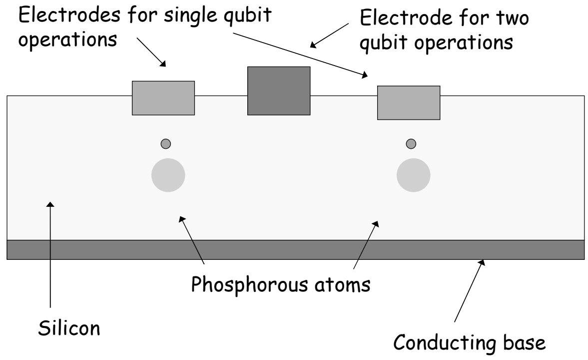
# Ion trap quantum computer



Two $Be^{+}$ ions in an ion trap (picture courtesy of NIST)

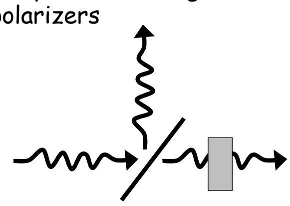
# Silicon based quantum computer




# Optical quantum computer

- Uses the presence or absence of a single photon to represent a |0> or |1>.
- Carry out single qubit operations using beam splitters and polarizers

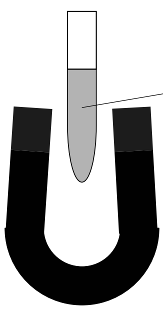
$$|0\rangle \rightarrow \alpha|0\rangle + e^{i\theta}\beta|1\rangle$$

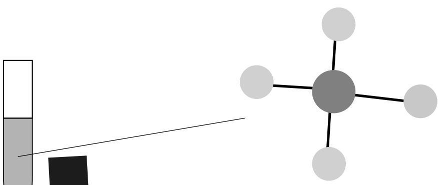


# Optical quantum computer

- In order to do two-qubit operations it is necessary to combine non-deterministic measurements with a quantum phenomenon known as quantum teleportation
- Has many hurdles associated with it such as:
  - Need for single photon sources
  - Need for single photon detectors
  - Need for a means of storing photons

# NMR quantum computer





- Uses the nuclear spin of the atoms in certain molecules as qubits
- Performs operations by applying radio-frequency pulses to the liquid
- Acts on millions of molecules at the same time, effectively perform "ensemble" computing

# Summary

- Currently many different schemes are being pursued to implement a quantum computer.
- All of these methods are in the very early stages of development
- Each scheme tends to have it's own specific "problem" area, which is insurmountable using <u>current</u> technology
- Not possible to give an accurate estimate of when (or even if) a large scale quantum computer will be built