# Quantum Networking and Security

CS 518

Lecture 1

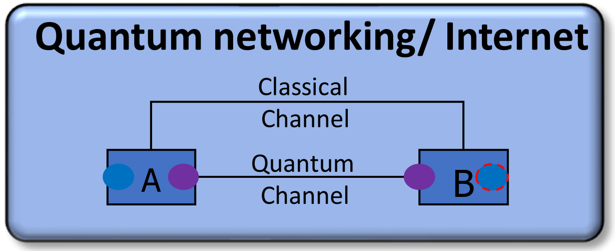
Prof M Rahman

# Overview- Quantum Networking: Teleportation

- “**Teleportation**” is a magic word, exotic and evocative, but it has been appearing in serious technical literature with increasing frequency.

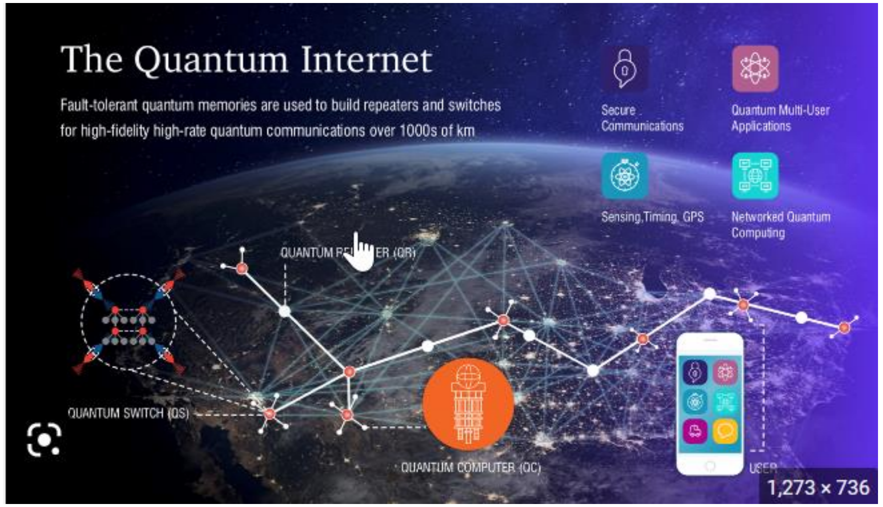
- Both theoretically fascinating and experimentally demonstrated, teleportation is the key to quantum networks

- **.Only the quantum state moves**



# Quantum Networking/Internet

- ❑ Basics
  - Quantum networks for computation
  - Quantum networks for communication
  - Overview of the elements of a quantum network
- ❑ Elements of a quantum network
  - End nodes: quantum processors
  - Communication lines: physical layer
    - Fiber optic networks
    - Free space network
  - Repeaters
    - Trusted repeaters
    - Quantum repeaters
    - Error correction
    - Entanglement purification



The Quantum Internet

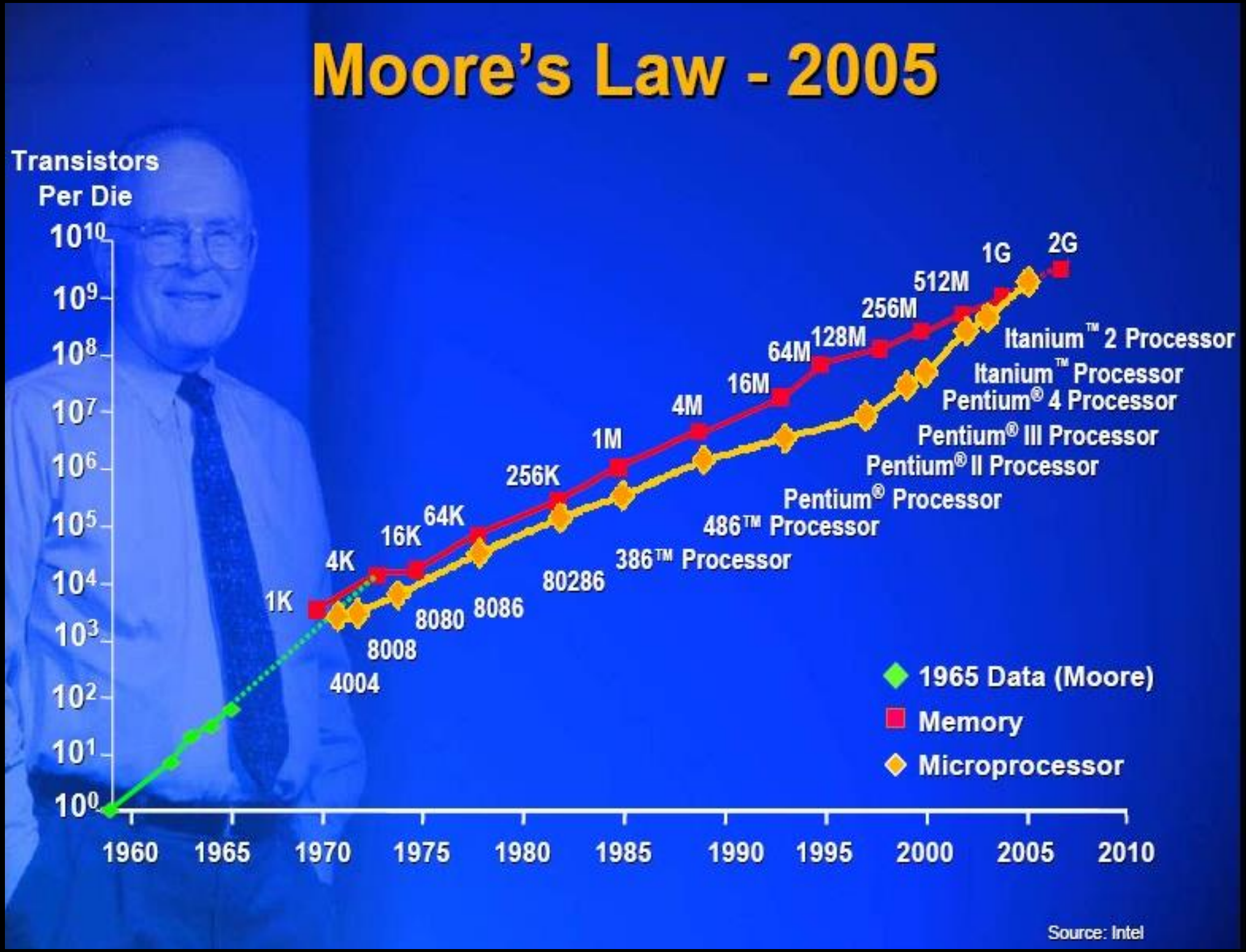
Fault-tolerant quantum memories are used to build repeaters and switches for high-fidelity high-rate quantum communications over 1000s of km

**Quantum network uses Quantum computers**

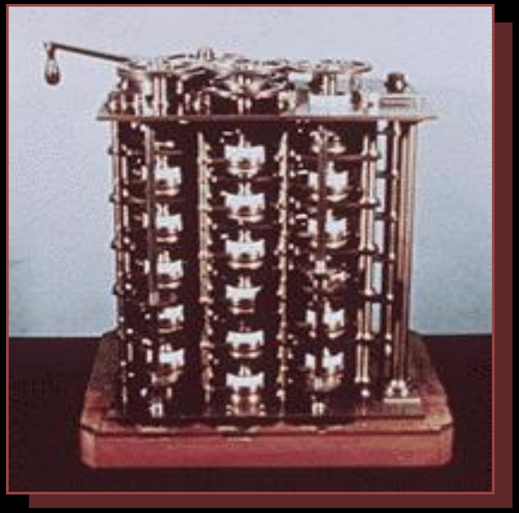
- ❑ Applications
  - Secure communications
- ❑ Current status
  - Quantum Internet
  - Quantum networks of computation
  - Experimental quantum models
  - Mobile quantum network
  - QKD networks

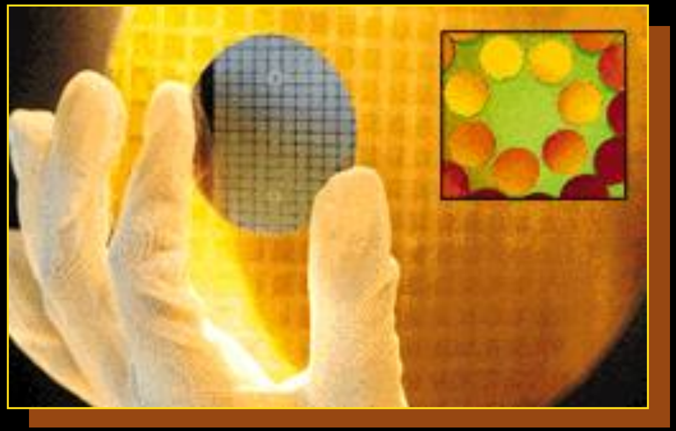
# Why Quantum Computing

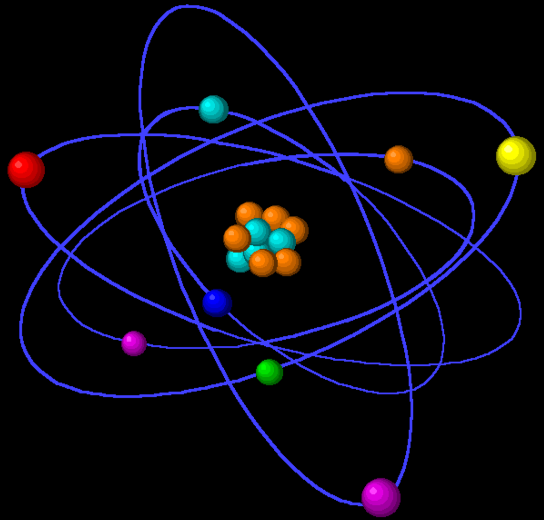
- Moore’s Law: transistors double every 2 year
- Slowing down
- Transistors cannot be made smaller – laws of quantum mechanics start to take over
- Post-silicon era



# Why Quantum Computing







Computer technology is making devices smaller and smaller…

…reaching a point where classical physics is no longer a suitable model for the laws of physics.

kT log(2)

# Limitations of Classical Computers

- RSA encryption (2048-bit)
  - 100,000 computers in parallel
  - 3 GHz processors
  - Factoring would take longer than the age of the universe

- Quantum simulation: inefficient with classical computers
  - Feynman: why not use quantum mechanics for computation?

# Quantum Computing Pioneers

- Yuri Manin (1937- ), mathematician
  - 1980: First to propose the idea of the quantum computer

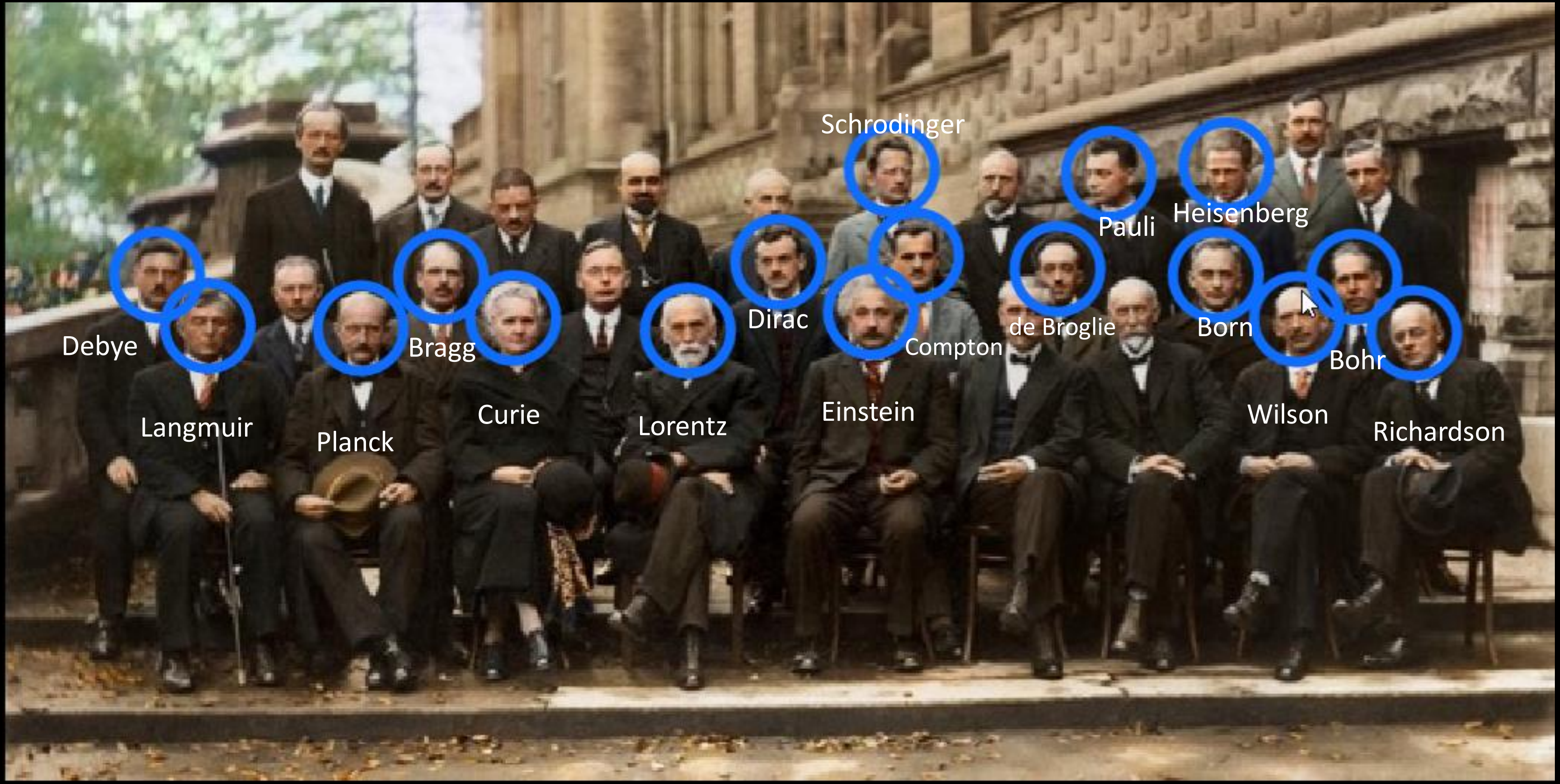
- Paul Benioff (1930- ), physicist
  - 1980: Described quantum mechanical models of computers

- Richard Feynman (1918-1988), physicist
  - 1981: Presented a logical quantum computer model
  - Demonstrated that a quantum system cannot be simulated with a classic computer
  - Demonstrated that the traditional approach to computer development would never lead to a revolution

# Quantum Mechanics developed in 1927 by the world’s greatest physicists

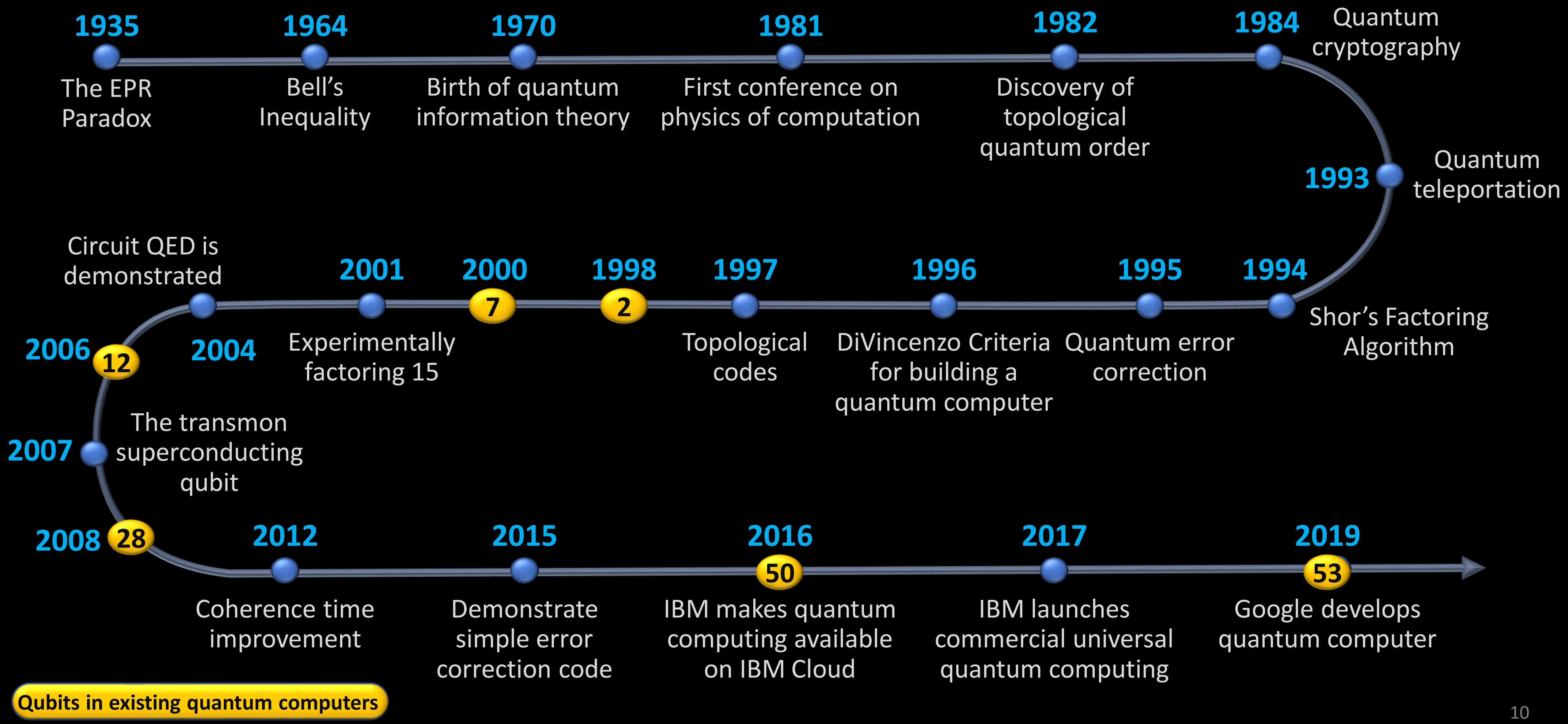
Solvay Conference 1927

# Quantum Mechanics developed in 1927 by the world's greatest physicists



Solvay Conference 1927

# A History of Quantum Computing



1935 The EPR Paradox

1964 Bell's Inequality

1970 Birth of quantum information theory

1981 First conference on physics of computation

1982 Discovery of topological quantum order

1984 Quantum cryptography

1993 Quantum teleportation

1994 Shor's Factoring Algorithm

1995 Quantum error correction

1996 DiVincenzo Criteria for building a quantum computer

1997 Topological codes

1998 2

2000 7

2001 Experimentally factoring 15

2004 Circuit QED is demonstrated

2006 12

2007 The transmon superconducting qubit

2008 28

2012 Coherence time improvement

2015 Demonstrate simple error correction code

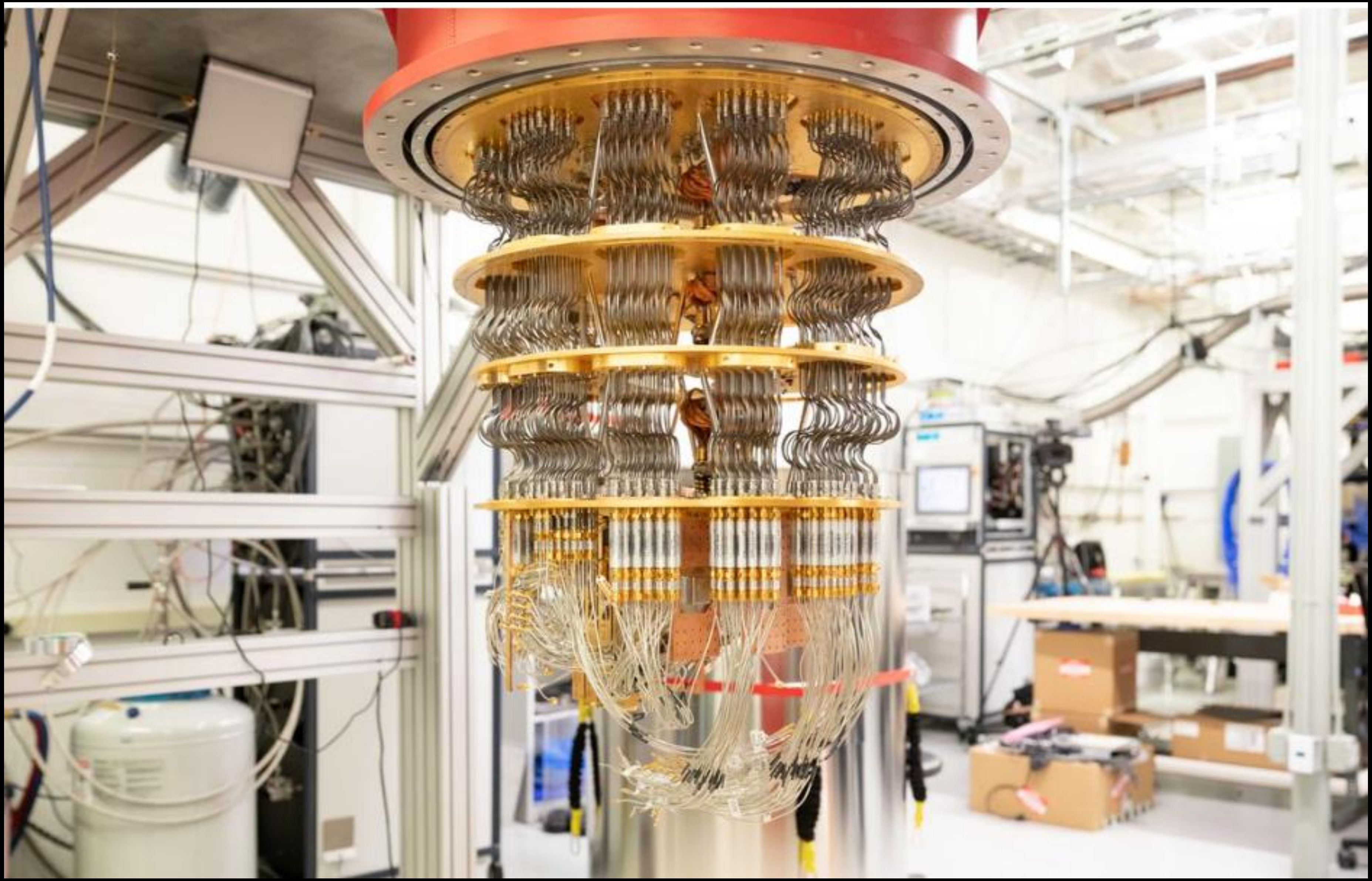
2016 50 IBM makes quantum computing available on IBM Cloud

2017 IBM launches commercial universal quantum computing

2019 53 Google develops quantum computer

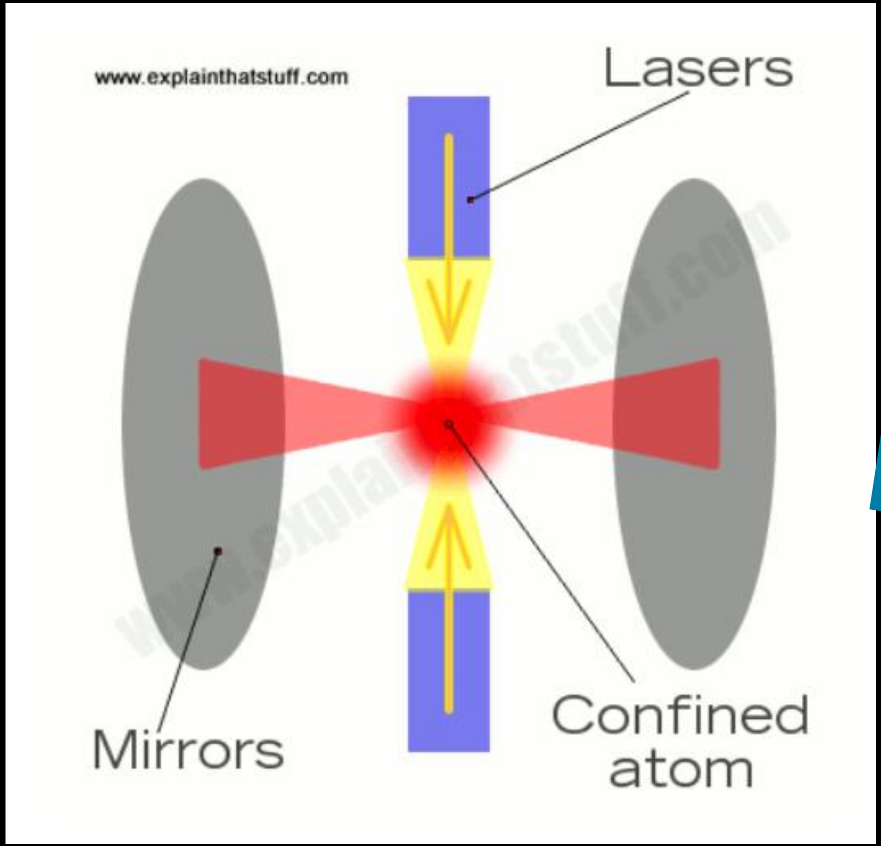
Qubits in existing quantum computers

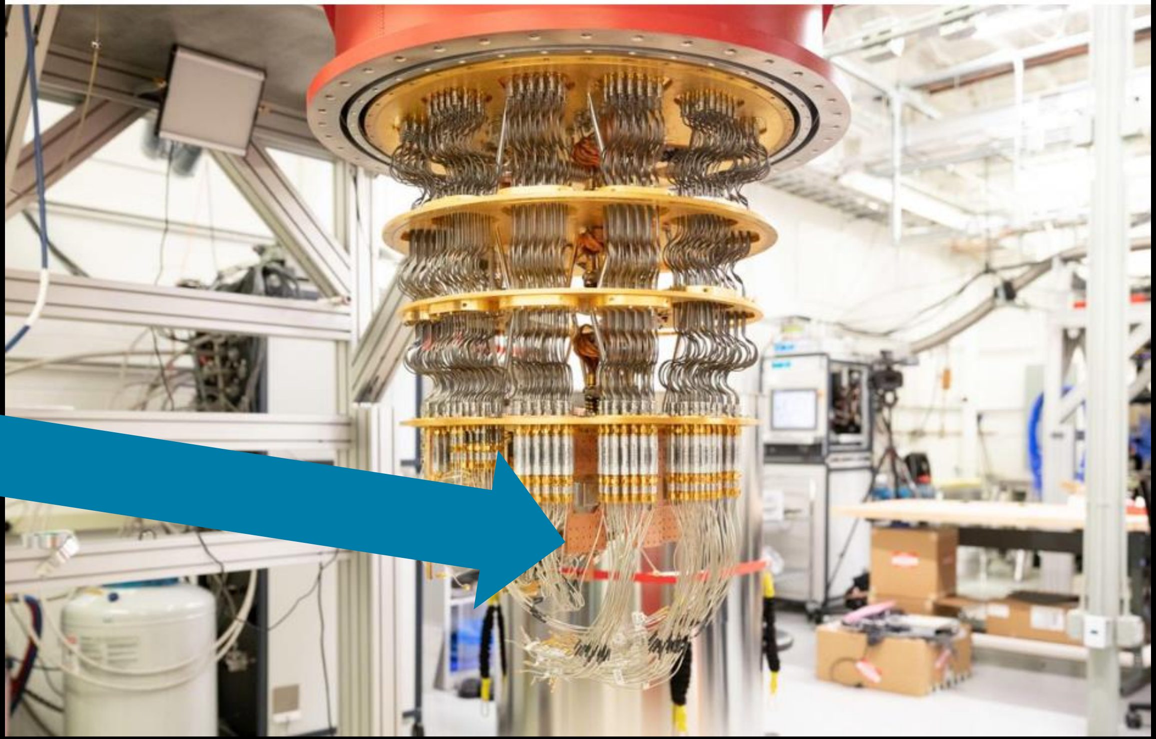
# 53 qubit Google’s Sycamore Quantum Computer



53 qubit Google’s Sycamore Quantum Computer ; 23 Oct , 2019

# Google’s Quantum Supremacy

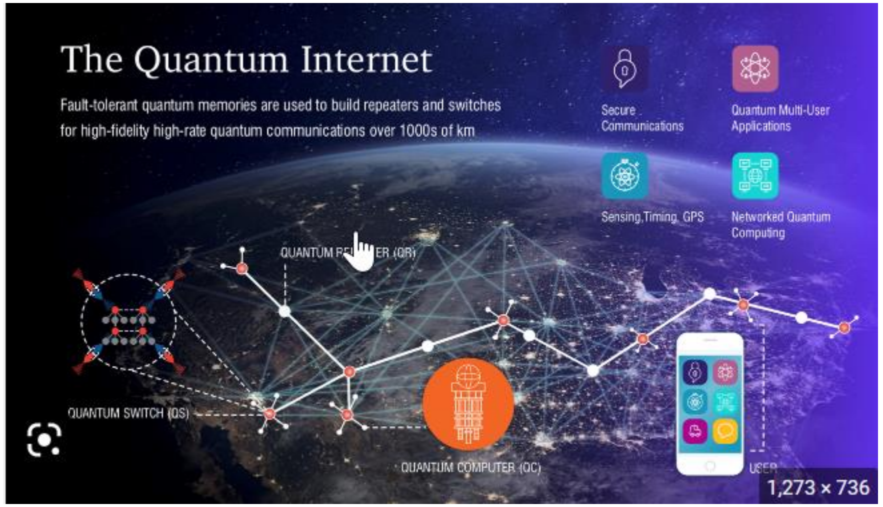




53 qubit Google’s Sycamore Quantum Computer ; 23 Oct , 2019

# Quantum Networking/Internet

- ❑ **Basics**
  - **Quantum networks for computation**
  - **Quantum networks for communication**
  - **Overview of the elements of a quantum network**
- ❑ **Elements of a quantum network**
  - **End nodes: quantum processors**
  - **Communication lines: physical layer**
    - **Fiber optic networks**
    - **Free space network**
  - **Repeaters**
    - **Trusted repeaters**
    - **Quantum repeaters**
    - **Error correction**
    - **Entanglement purification**

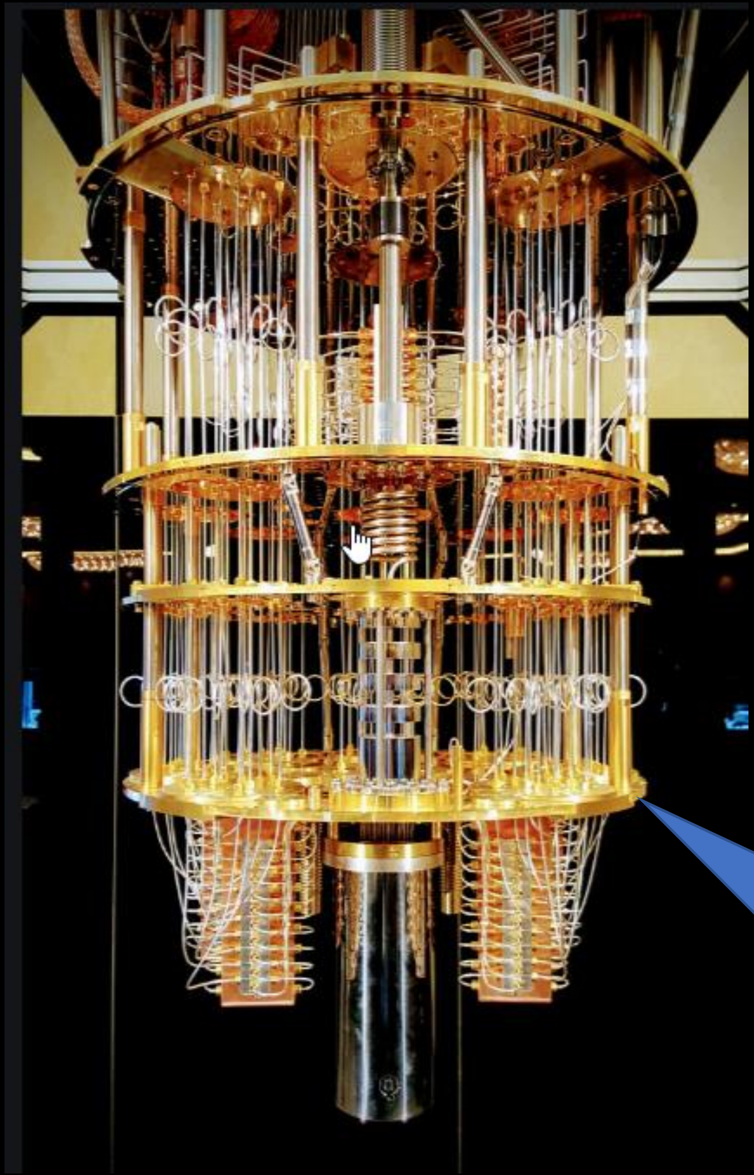


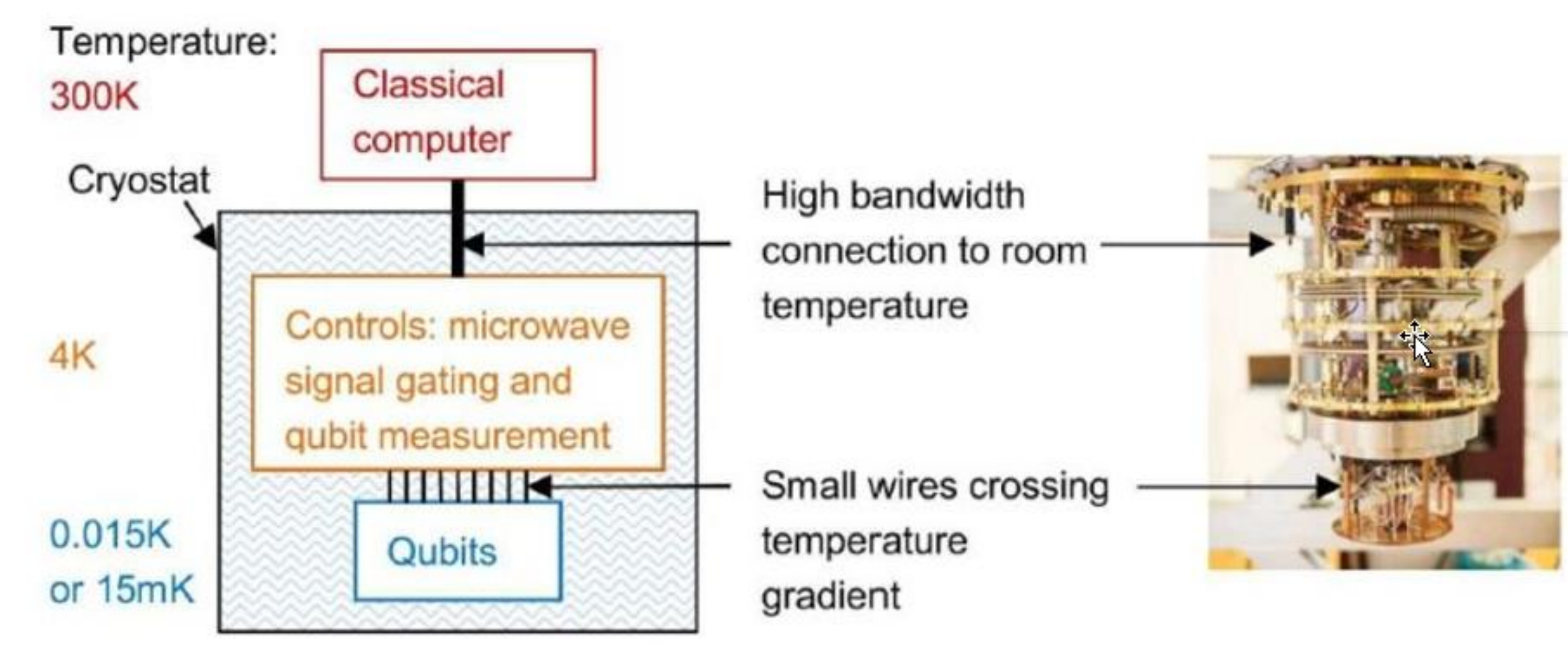
The Quantum Internet

Fault-tolerant quantum memories are used to build repeaters and switches for high-fidelity high-rate quantum communications over 1000s of km

**Quantum network uses Quantum computers**

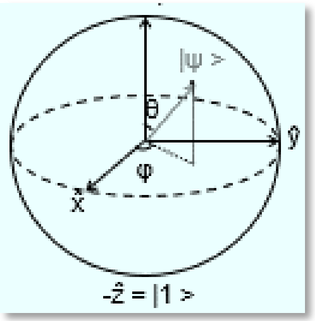
- ❑ **Applications**
  - **Secure communications**
- ❑ **Current status**
  - **Quantum Internet**
  - **Quantum networks of computation**
  - **Experimental quantum models**
  - **Mobile quantum network**
  - **QKD networks**




Temperature:
300K
Cryostat
4K
0.015K
or 15mK
Classical computer
Controls: microwave signal gating and qubit measurement
Qubits
High bandwidth connection to room temperature
Small wires crossing temperature gradient

From top to bottom, the system gradually cools from four Kelvin -- liquid-helium temperatures -- to 800 milliKelvin, 100 milliKelvin and, finally, 10 milliKelvin. Inside the canister where the chip is, that's 10 thousandths of a degree above absolute zero

# Technical Summary

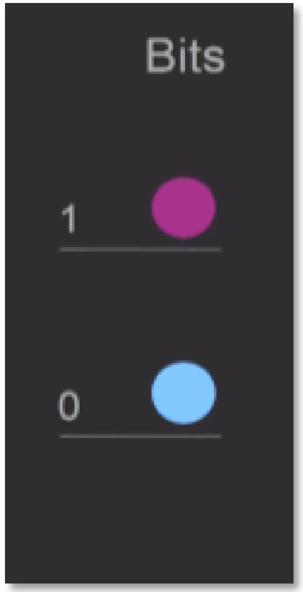


## Classical

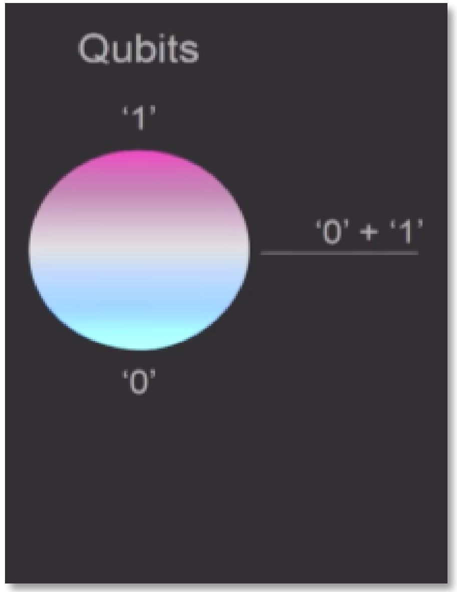
## Quantum Computing Essential Ingredients

## Quantum Networking

### Bit



### Qubit



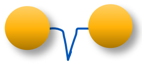
### Superposition

**Quantum computers (quantum bits)**

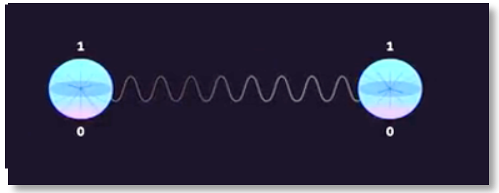
**"0" and "1" state**

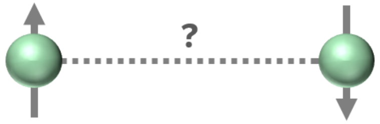
**Superposition**

### Entanglement



EPR Qubit Pair

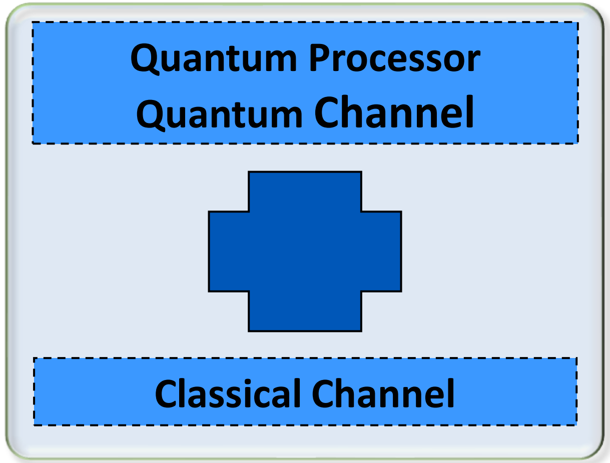




**observed "here"**

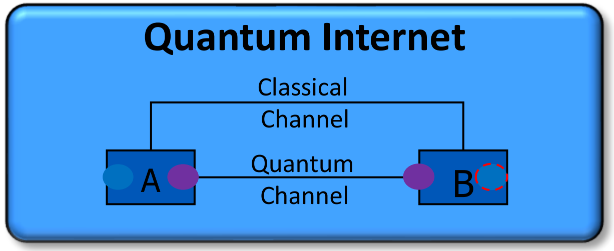
**affected "over there"**

### Teleportation



**Quantum Processor**
**Quantum Channel**

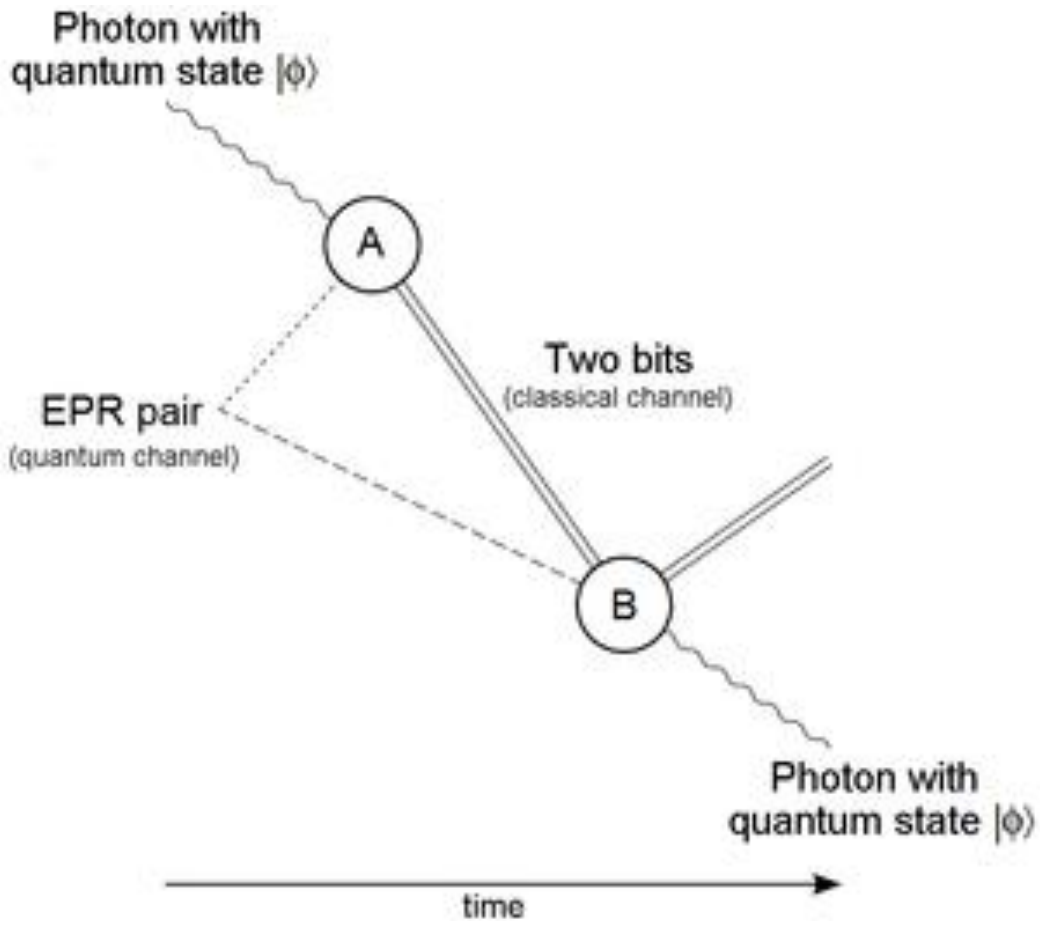
**Classical Channel**



**Quantum Internet**

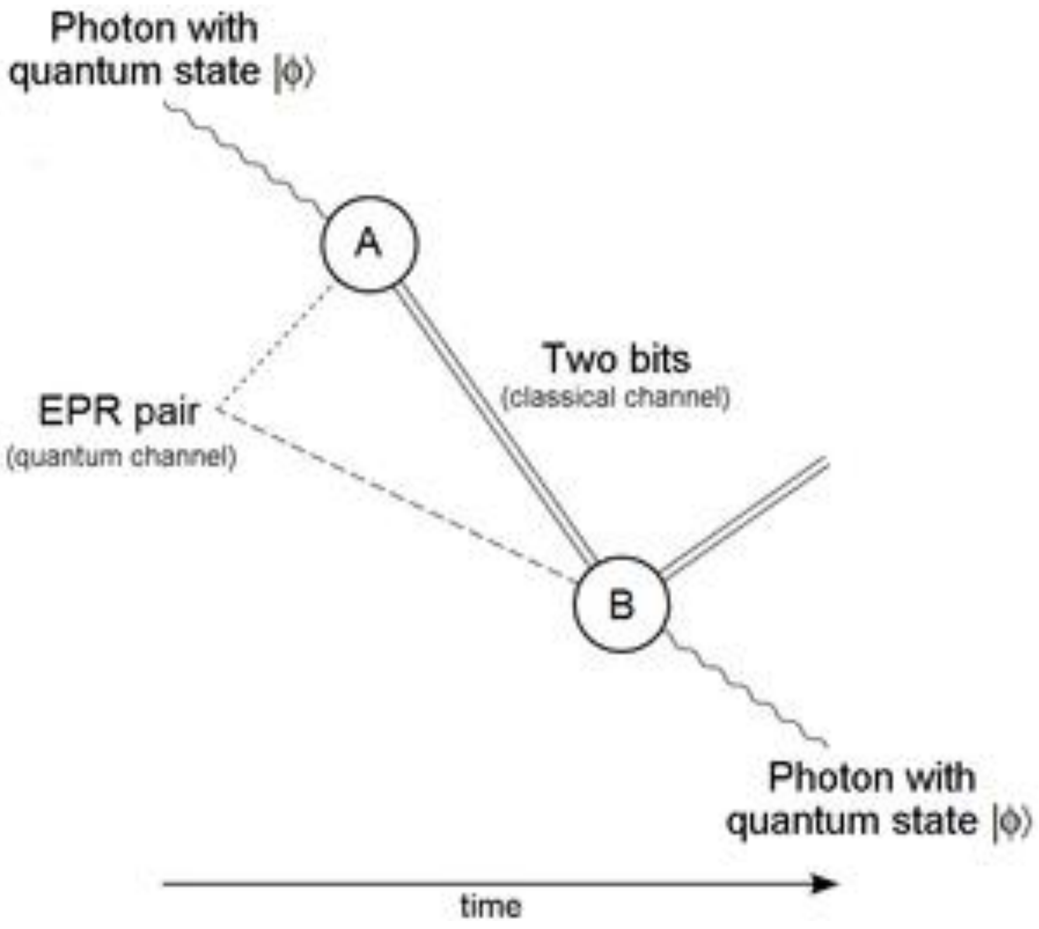
# Overview- Quantum Networking: Teleportation

- “**Teleportation”** is a magic word, exotic and evocative, but it has been appearing in serious technical literature with increasing frequency.
- Both theoretically fascinating and experimentally demonstrated, teleportation is the key to quantum networks
- When used in discussions about quantum information, teleportation refers not to Captain Kirk stepping into a machine on the starship Enterprise, dissolving and reappearing on a planet’s surface, but to an operation in which a quantum variable dissolves here and reappears there, on a different physical device. **Only the quantum state moves**; the electron or other physical device remains where it was, and the receiver can in fact be a very different form of physical device than the sender. The quantum state is destroyed at the sender in the process.
- Classical networks communicate by physically **copying data** and transmitting the copy, but the rules of quantum mechanics **forbid** the creation of independent copies of an unknown, arbitrary quantum state. Instead of risking the loss of valuable, fragile quantum data by directly transmitting our only copy, networks will prepare generic states that are used to teleport data or to perform teleportation-derived operations on the data.

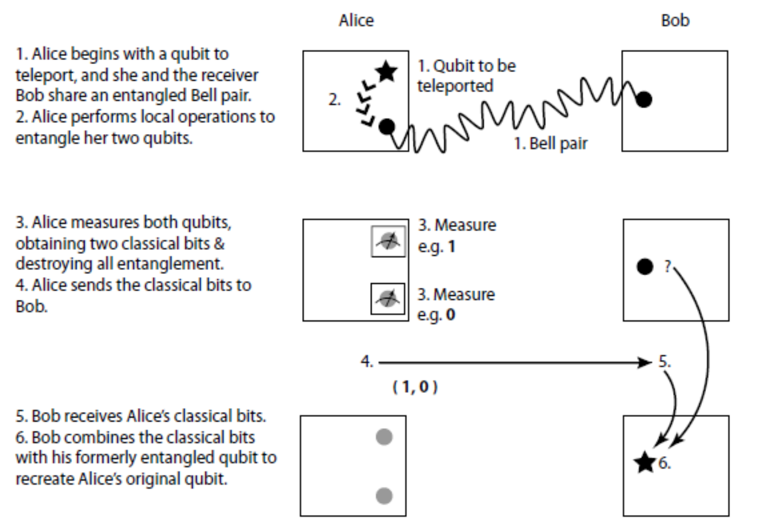

Photon with quantum state $|\phi\rangle$
A
Two bits
(classical channel)
EPR pair
(quantum channel)
B
Photon with quantum state $|\phi\rangle$
time

# Overview- Quantum Networking: Teleportation

- Quantum networks bring new capabilities to communication systems. Quantum physical effects can be used to detect eavesdropping, to improve the share sensitivity of separated astronomical instruments or to create distributed states that will enable numerical quantum computation over a distance using teleportation.
- Quantum communication is the exchange of quantum states over a distance, generally requiring the support of substantial classical communication.
- The quantum states that are exchanged may be "standalone" states, an individual element of quantum data. They may also be part of a larger quantum state, spanning devices or even network nodes in a way no shared classical state can. These latter states we refer to as entangled states, which we will study extensively in this course



# Quantum Networking- Teleportation

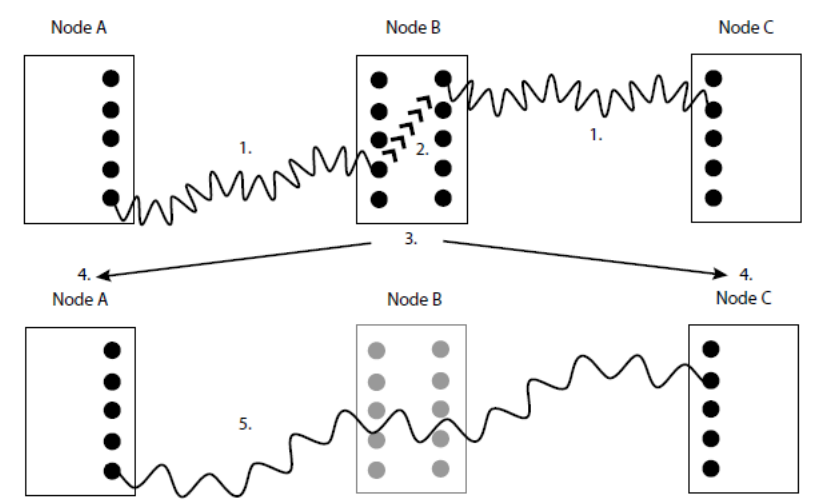


1. Alice begins with a qubit to teleport, and she and the receiver Bob share an entangled Bell pair.
2. Alice performs local operations to entangle her two qubits.

3. Alice measures both qubits, obtaining two classical bits & destroying all entanglement.
4. Alice sends the classical bits to Bob.

5. Bob receives Alice's classical bits.
6. Bob combines the classical bits with his formerly entangled qubit to recreate Alice's original qubit.

**Figure 1.1.** *Operations in teleporting a qubit from Alice to Bob*



1. Nodes begin with two entangled pairs, AB and BC.
2. Node B selects pairs to teleport, performs local operations, measures one qubit of each pair.
3. B communicates measurement results and new entanglement status to A and C.
4. Receive partner's measurement result and new entanglement status, including node/qubit addresses.
5. Result is single lower-fidelity, longer-distance Bell pair.

**Figure 1.2.** *Teleportation can lengthen one Bell pair using another*

# Quantum Networking

1. Nodes begin with two entangled pairs.
2. Select pairs to purify, perform local operations, measure one pair.
3. Communicate measurement result.
4. Receive partner's measurement result, decide to keep or discard.
5. Result is either single higher-fidelity Bell pair, or no entanglement.

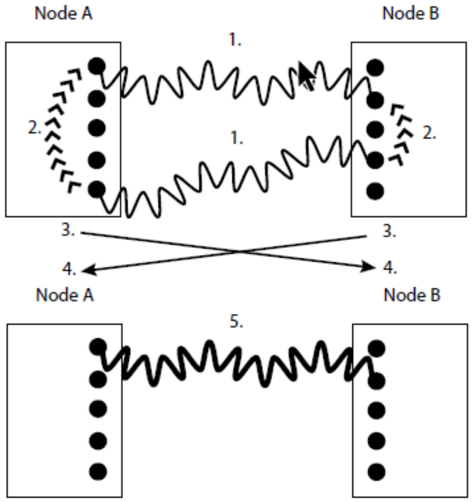


**Figure 1.3.** *Steps involved in purification of Bell pairs*

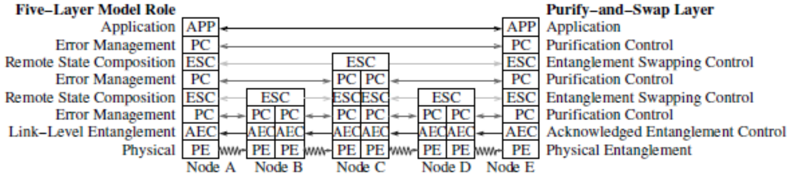


**Figure 1.4.** *Protocol layers and their interaction in purify-and-swap repeaters, in a five-node, four-hop chain. The labels on the left indicate the model layer represented, and the labels in the boxes and on the right indicate the protocol name for purify-and-swap repeaters. Double-headed arrows indicate bidirectional classical communication is required. The only quantum portion of the stack is the physical layer, shown with all links propagating left to right*

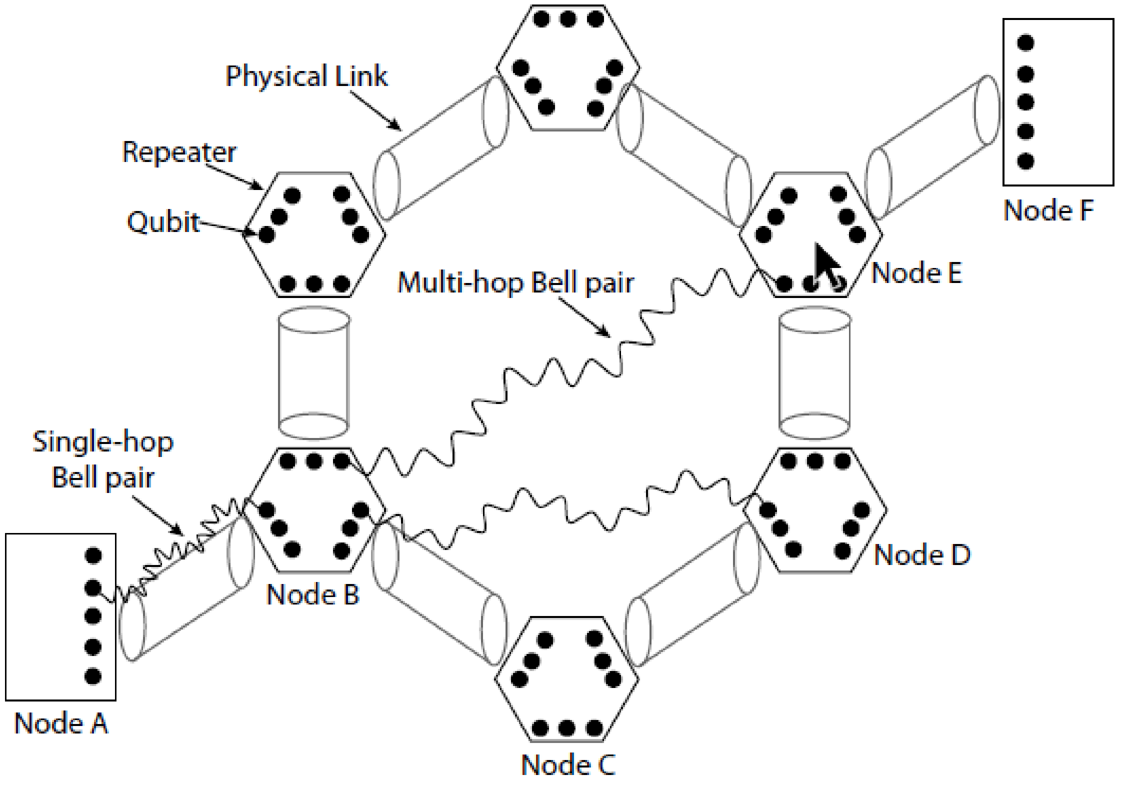
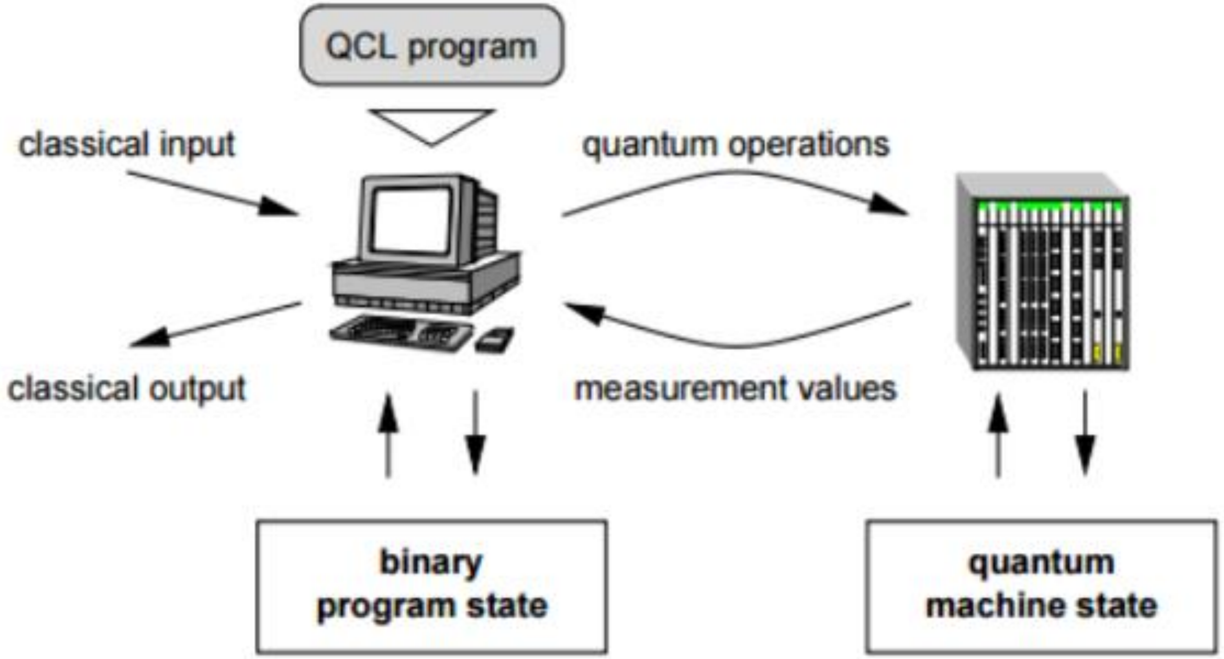


**Figure 1.5.** *Even when Node B knows that A is trying to build a Bell pair with F, B may be uncertain whether its Bell pair connected to Node D or Node E is "closer" to the destination*

# Overview (Cont..)

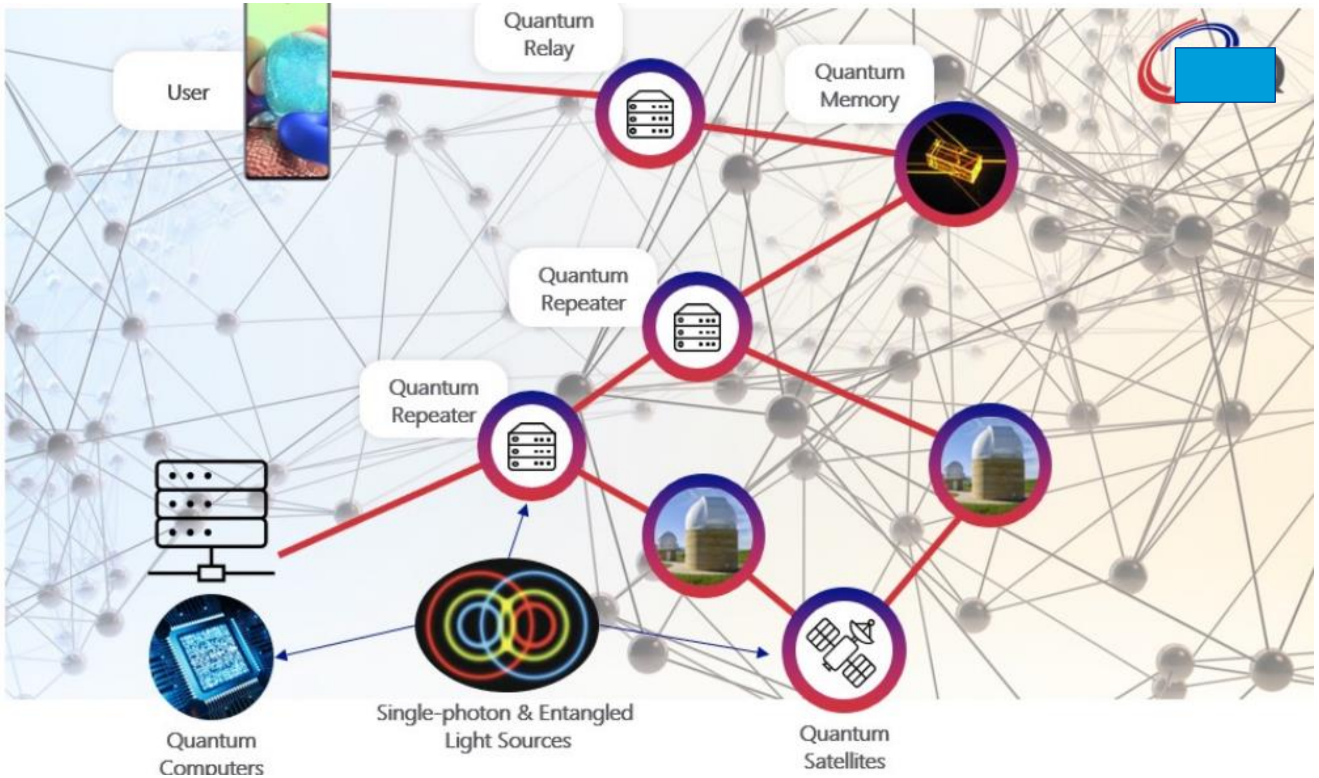


- **Applications running on classical computers** will use these quantum states to accomplish one of the above tasks. **The classical computer is connected to a quantum device**, which may do no more than measure the quantum states to find a classical value (such as a bit of a secret key), or may store them for use in more complex quantum computers.
- **A classical computer will treat a quantum computer as a type of coprocessor**; likewise, the classical computer will see the quantum network through the eyes of a separate device.
- **Because quantum data is fragile and some quantum operations are probabilistic**, errors and distributed calculations must be managed aggressively and perhaps cooperatively among nodes. Solutions to these problems will have both similarities to and differences from purely classical networks.
- **Architectures for large-scale quantum networking and internetworking are in development**, paralleling theoretical and experimental work on physical layers and low-level error management and connection technologies. Unentangled quantum networks have already been deployed, starting in the early 2000s; as of early 2014, entangled networks are not yet deployed, but may appear within the next few years and will form a vibrant research topic in the coming decade.

# Quantum Internet/Networking

❖ **The quantum internet**- **a network interconnecting remote quantum devices through quantum links in synergy with classical ones –is envisioned as the final stage of the quantum revolution, opening fundamentally new communications and computing capabilities.**

- **Quantum networks** form an important element of quantum computing and quantum communication systems.
- Quantum networks facilitate the transmission of information in the form of quantum bits, also called qubits, between physically separated quantum processors.
- A quantum processor is a small quantum computer being able to perform quantum logic gates on a certain number of qubits.
- Quantum networks work in a similar way to classical networks. The main difference is that quantum networking, like quantum computing, is better at solving certain problems, such as modeling quantum systems.



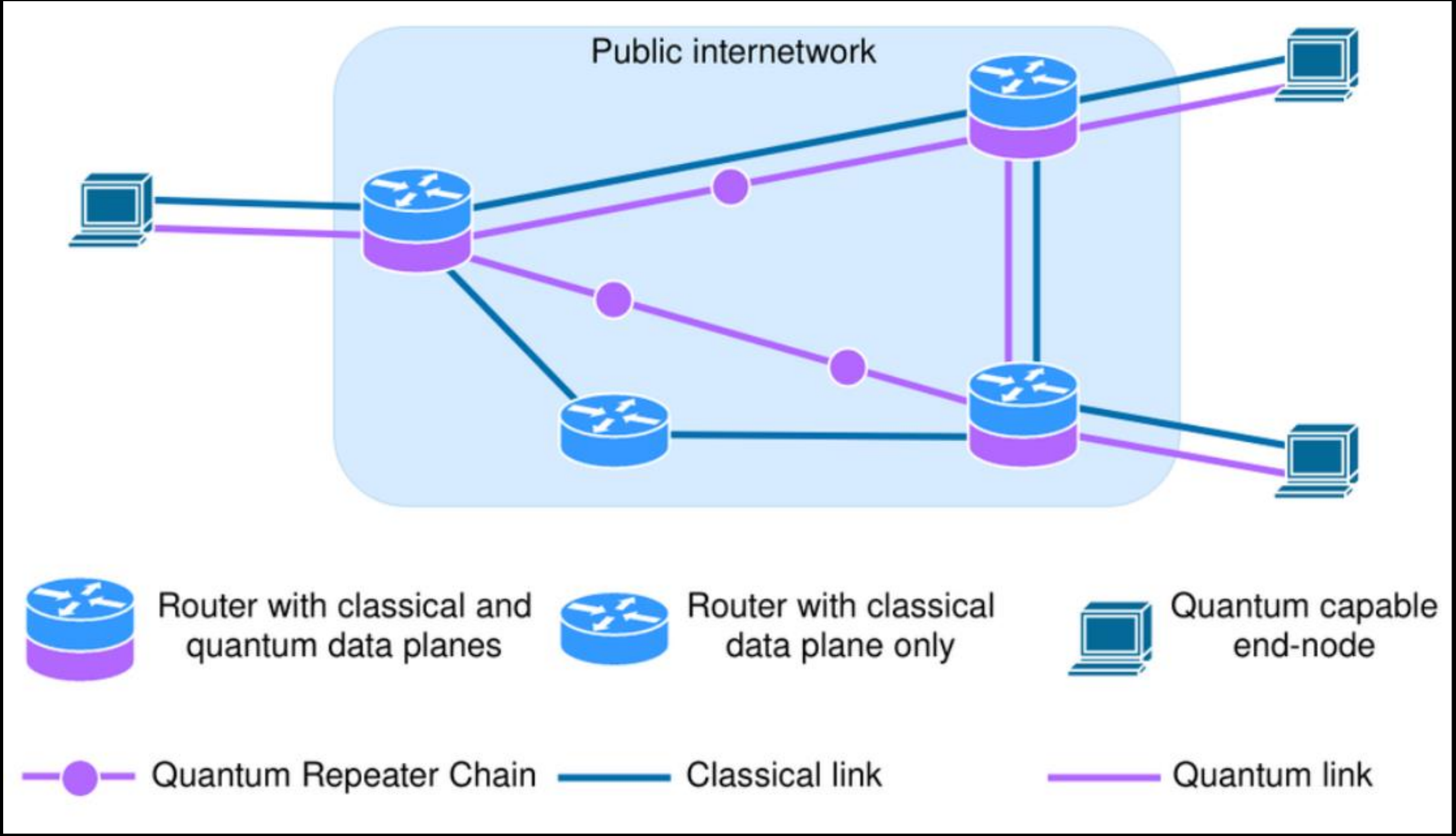
# Quantum networks for computation

- Quantum networks for computation
  - Networked quantum computing or distributed quantum computing[1][2] works by linking multiple quantum processors through a quantum network by sending qubits in between them
  - Doing this creates a quantum computing cluster and therefore creates more computing potential. Less powerful computers can be linked in this way to create one more powerful processor.
  - This is analogous to connecting several classical computers to form a computer cluster in classical computing
  - Like classical computing, this system is scalable by adding more and more quantum computers to the network
  - Currently, quantum processors are only separated by short distances.

# Quantum Communication

- In the realm of quantum communication, one wants to send qubits from one quantum processor to another over long distances.[3]
- This way, local quantum networks can be intra-connected into a quantum internet.
- A quantum internet[1] supports many applications, which derive their power from the fact that by creating quantum entangled qubits, information can be transmitted between the remote quantum processors.
- Most applications of a quantum internet require only very modest quantum processors. For most quantum internet protocols, such as quantum key distribution in quantum cryptography, it is sufficient if these processors are capable of preparing and measuring only a single qubit at a time.
- This is in contrast to quantum computing where interesting applications can only be realized if the (combined) quantum processors can easily simulate more qubits than a classical computer (around 60[4]).
- Quantum internet applications require only small quantum processors, often just a single qubit, because quantum entanglement can already be realized between just two qubits.
- A simulation of an entangled quantum system on a classical computer cannot simultaneously provide the same security and speed.

# Quantum Internet/Networking



- The Quantum Internet – a network interconnecting remote quantum devices through quantum links in synergy with classical ones
- The quantum internet is a network that lets quantum devices exchange information within an environment that harnesses the weird laws of quantum mechanics.

➢ **Quantum network uses Quantum computers**

# Quantum Networking

- Unsurprisingly, qubits cannot be used to send the kind of data we are familiar with, like emails and WhatsApp messages.
- But the strange behavior of qubits is opening up huge opportunities in other, more niche applications.

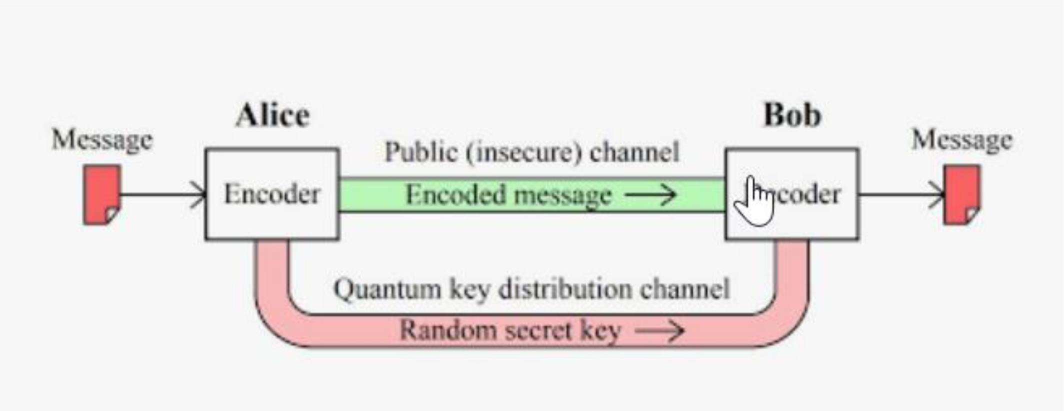
- **QUANTUM (SAFER) COMMUNICATIONS**
  - One of the most exciting avenues that researchers, armed with qubits, are exploring, is security.
  - When it comes to classical communications, most data is secured by distributing a shared key to the sender and receiver and then using this common key to encrypt the message. The receiver can then use their key to decode the data at their end.

# Quantum Networking: QKD

- Measuring causes the state of the qubit to collapse, but it is the value that is read out during the measurement process that is important. The qubit, in a way, is only there to transport the key value.

- More importantly, QKD means that it is easy to find out whether a third party has eavesdropped on the qubits during the transmission since the intruder would have caused the key to collapse simply by looking at it.

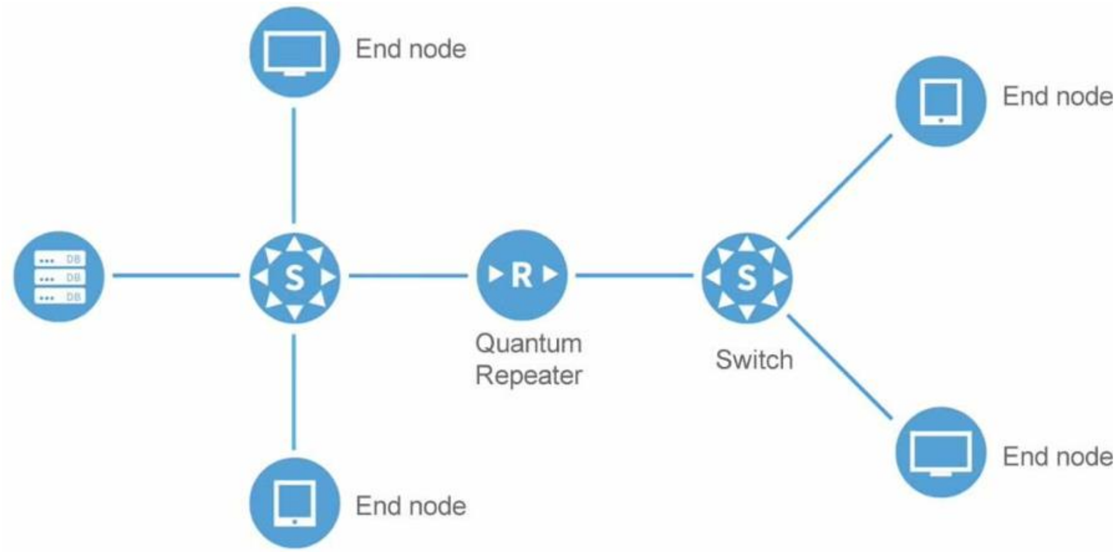
- If a hacker looked at the qubits at any point while they were being sent, this would automatically change the state of the qubits. A spy would inevitably leave behind a sign of eavesdropping – which is why cryptographers maintain that QKD is "provably" secure.



# Quantum Networking: QKD

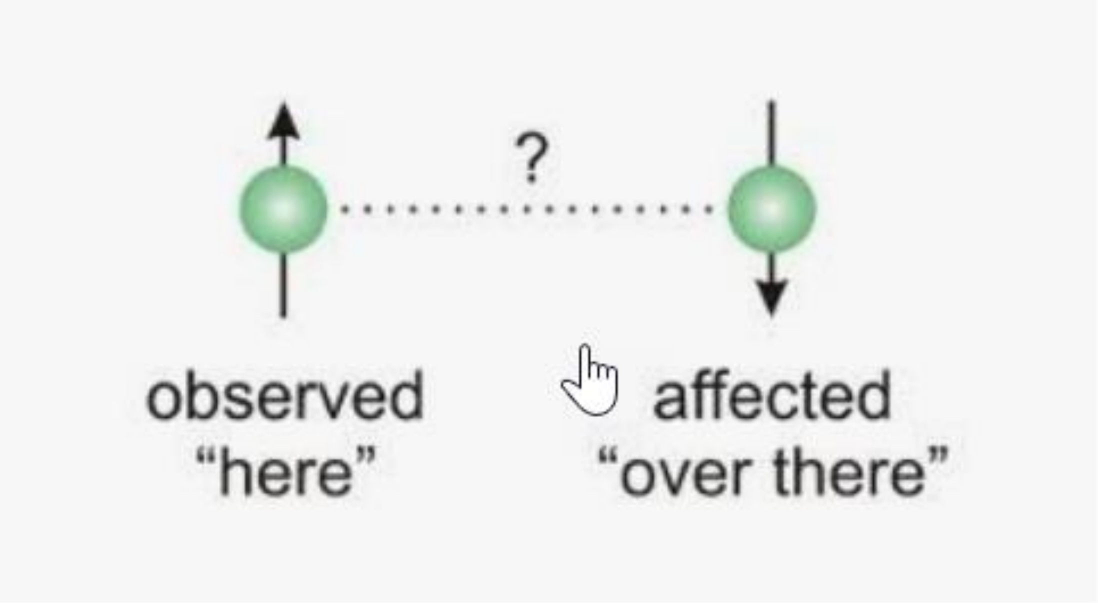
- **SO, WHY A QUANTUM INTERNET?**

- QKD technology is in its very early stages. The "usual" way to create QKD at the moment consists of sending qubits in a one-directional way to the receiver, through optic-fiber cables; but those significantly limit the effectiveness of the protocol.
- Qubits can easily get lost or scattered in a fiber-optic cable, which means that quantum signals are very much error-prone, and struggle to travel long distances. Current experiments, in fact, are limited to a range of hundreds of kilometers.
- There is another solution, and it is the one that underpins the quantum internet: to leverage another property of quantum, called entanglement, to communicate between two devices.
- When two qubits interact and become entangled, they share particular properties that depend on each other.
  - While the qubits are in an entangled state, any change to one particle in the pair will result in changes to the other, even if they are physically separated.
  - The state of the first qubit, therefore, can be "read" by looking at the behavior of its entangled counterpart. That's right: even Albert Einstein called the whole thing "spooky action at a distance".
- And in the context of quantum communication, entanglement could in effect, teleport some information from one qubit to its entangled other half, without the need for a physical channel bridging the two during the transmission.



# Quantum Networking: Entanglement

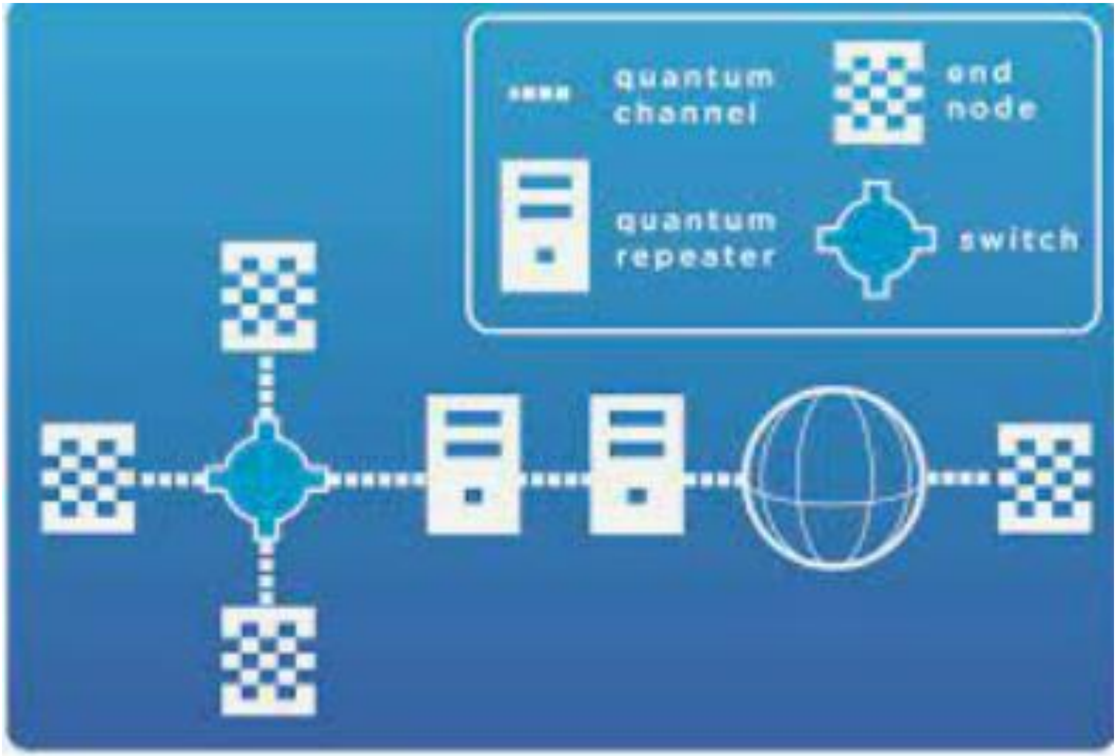
- **HOW DOES ENTANGLEMENT WORK?**
  - The very concept of teleportation entails, by definition, the lack of a physical network bridging between communicating devices. But it remains that entanglement needs to be created in the first place, and then maintained.
  - To carry out QKD using entanglement, it is necessary to build the appropriate infrastructure to first create pairs of entangled qubits, and then distribute them between a sender and a receiver. This creates the "teleportation" channel over which cryptography keys can be exchanged.
  - Specifically, once the entangled qubits have been generated, you have to send half of the pair to the receiver of the key. An entangled qubit can travel through networks of optic fiber, for example; but those are unable to maintain entanglement after about 60 miles.
  - Qubits can also be kept entangled over large distances via satellite, but covering the planet with outer-space quantum devices is expensive.
  - There are still huge engineering challenges, therefore, to building large-scale "teleportation networks" that could effectively link up qubits across the world. Once the entanglement network is in place, the magic can start: linked qubits won't need to run through any form of physical infrastructure anymore to deliver their message.
  - During transmission, therefore, the quantum key would virtually be invisible to third parties, impossible to intercept, and reliably "teleported" from one endpoint to the next. The idea will resonate well with industries that deal with sensitive data, such as banking, health services or aircraft communications. And it is likely that governments sitting on top secret information will also be early adopters of the technology.



# Quantum Networking: Entanglement and Repeaters

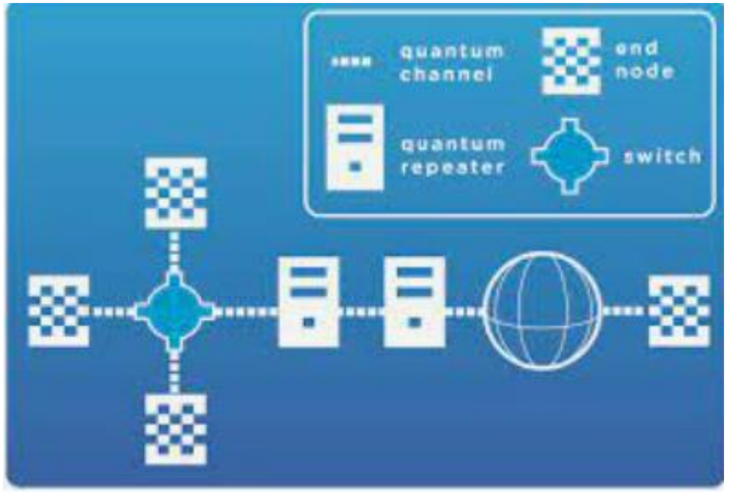
- **WHAT ELSE COULD WE DO WITH THE QUANTUM INTERNET?**

- 'Why bother with entanglement?' you may ask. After all, researchers could simply find ways to improve the "usual" form of QKD.
  - Quantum repeaters, for example, could go a long way in increasing communication distance in fiber-optic cables, without having to go so far as to entangle qubits.
- That is without accounting for the immense potential that entanglement could have for other applications. QKD is the most frequently discussed example of what the quantum internet could achieve because it is the most accessible application of the technology.
  - But security is far from being the only field that is causing excitement among researchers.
- The entanglement network used for QKD could also be used, for example, to provide a reliable way to build up quantum clusters made of entangled qubits located in different quantum devices.
- Researchers won't need a particularly powerful piece of quantum hardware to connect to the quantum internet – in fact, even a single-qubit processor could do the job.
  - But by linking together quantum devices that, as they stand, have limited capabilities, scientists expect that they could create a quantum supercomputer to surpass them all.

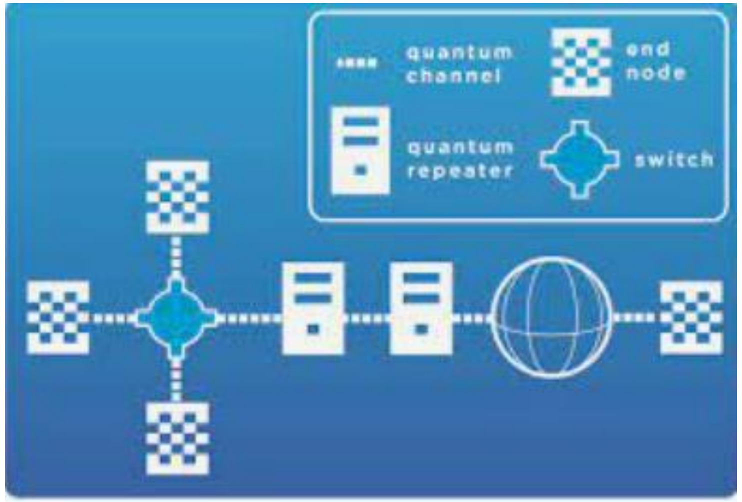


# Quantum Networking: Advanced Quantum Computers

- By connecting many smaller quantum devices together, therefore, the quantum internet could start solving the problems that are currently impossible to achieve in a single quantum computer.
    - This includes expediting the exchange of vast amounts of data and carrying out large-scale sensing experiments in astronomy, materials discovery, and life sciences.
    - For this reason, scientists are convinced that we could reap the benefits of the quantum internet before tech giants such as Google and IBM even achieve quantum supremacy – the moment when a single quantum computer will solve a problem that is intractable for a classical computer.
- Google and IBM's most advanced quantum computers currently sit around 50 qubits, which, on its own, is much less than is needed to carry out the phenomenal calculations needed to solve the problems that quantum research hopes to address.
- On the other hand, linking such devices together via quantum entanglement could result in clusters worth several thousand of qubits.
    - For many scientists, creating such computing strength is in fact the ultimate goal of the quantum internet project.



# Quantum Networking



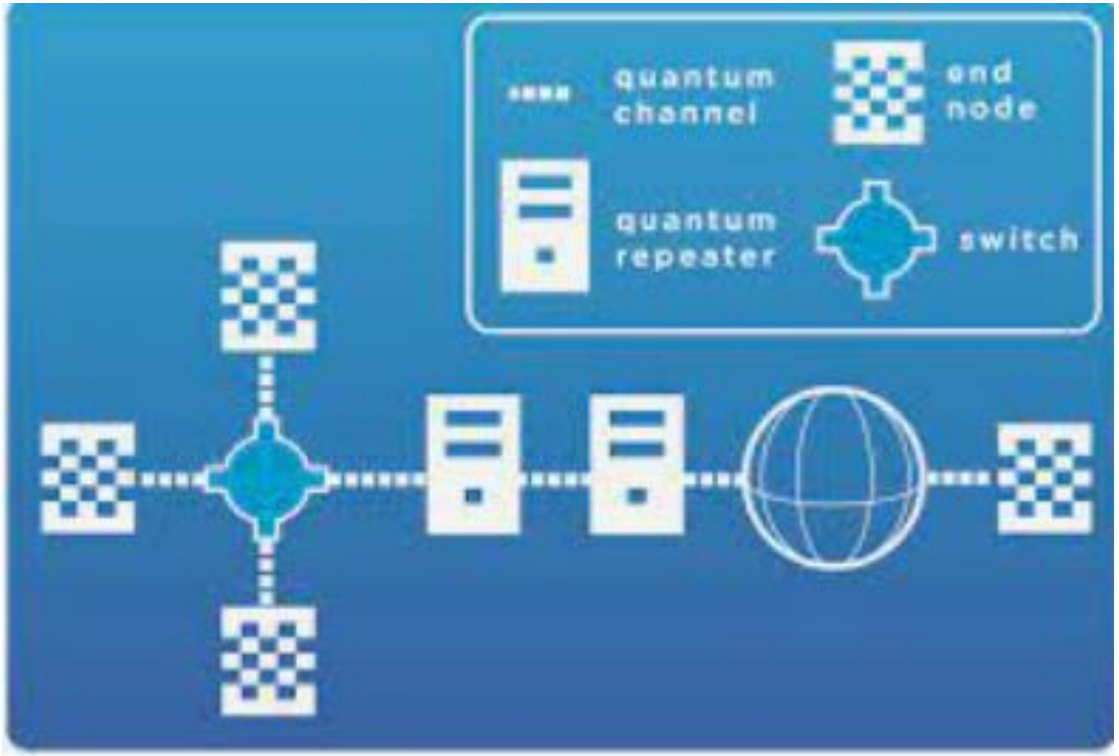
- **WHAT COULDN'T WE DO WITH THE QUANTUM INTERNET?**
- For the foreseeable future, the quantum Internet could not be used to exchange data in the way that we currently do on our laptops.
- Imagining a generalized, mainstream quantum internet would require anticipating a few decades (or more) of technological advancements. As much as scientists dream of the future of the quantum internet, therefore, it is impossible to draw parallels between the project as it currently stands, and the way we browse the web every day.
- A lot of quantum communication research today is dedicated to finding out how to best encode, compress and transmit information thanks to quantum states.
    - Quantum states, of course, are known for their extraordinary densities, and scientists are confident that one node could teleport a great deal of data.
- But the type of information that scientists are looking at sending over the quantum internet has little to do with opening up an inbox and scrolling through emails.
    - And in fact, replacing the classical internet is not what the technology has set out to do.
- Rather, researchers are hoping that the quantum internet will sit next to the classical Internet, and would be used for more specialized apps.
    - The quantum internet will perform tasks that can be done faster on a quantum computer than on classical computers, or which are too difficult to perform even on the best supercomputers that exist today.

# Quantum Networking

- **SO, WHAT ARE WE WAITING FOR?**

- Scientists already know how to create entanglement between qubits and have even been successfully leveraging entanglement for QKD.
- China, a long-time investor in quantum networks, has broken records on satellite-induced entanglement. Chinese scientists recently established entanglement and achieved QKD over a record-breaking 745 miles.
- The next stage, however, is scaling up the infrastructure. All experiments so far have only connected two endpoints. Now that point-to-point communication has been achieved, scientists are working on creating a network in which multiple senders and multiple receivers could exchange over the quantum internet on a global scale.
- Essentially, the idea is to find the best ways to churn out many entangled qubits on demand, over long distances, and simultaneously between many different points. This is much easier said than done: for example, maintaining the entanglement between a device in China and one in the US would probably require an intermediate node, on top of new routing protocols.

- And countries are opting for different technologies when it comes to establishing entanglement in the first place. While China is picking satellite technology, optical fiber is the method favored by the US DoE, which is now trying to create a network of quantum repeaters that can augment the distance that separates entangled qubits.



# Quantum Networking: Optical Fiber

- In the US, particles have remained entangled through optical fiber over a 52-mile "quantum loop" in the suburbs of Chicago, without the need for quantum repeaters.
  - The network will soon be connected to one of the DoE's laboratories to establish an 80-mile quantum testbed.

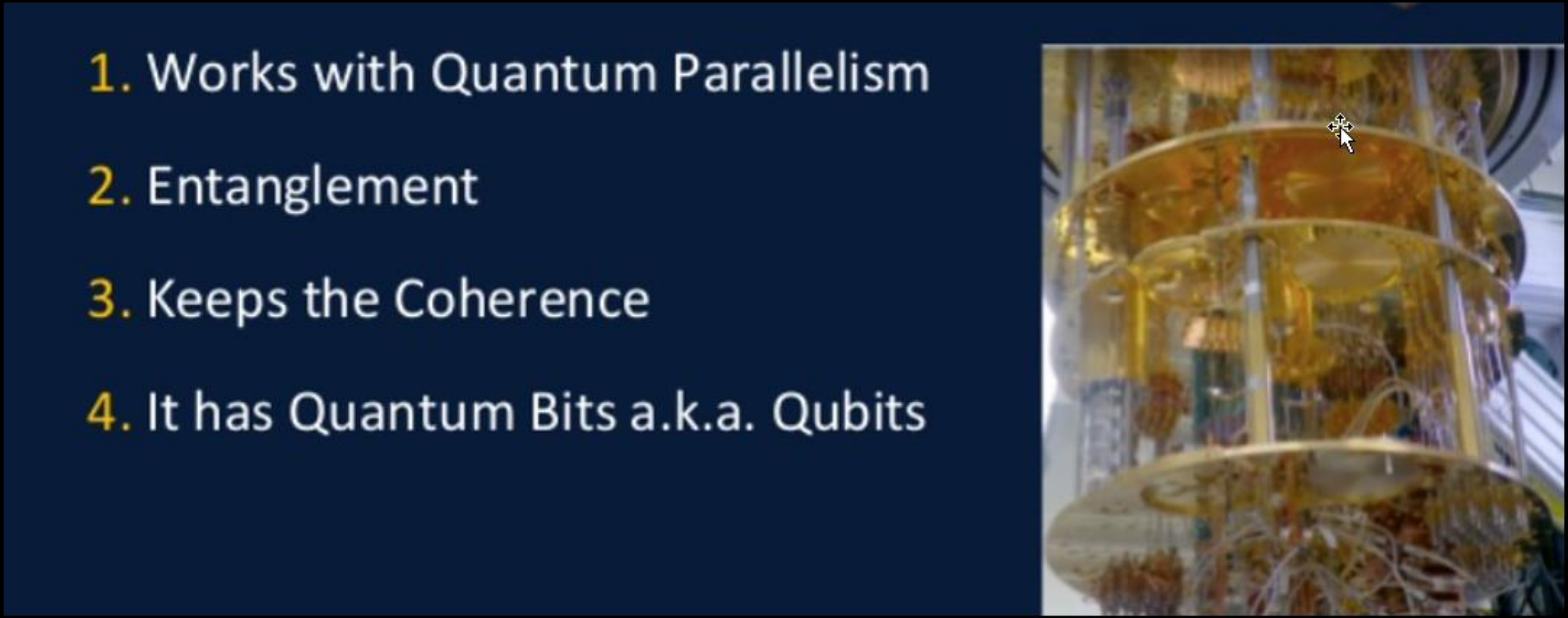
- In the EU, the Quantum Internet Alliance was formed in 2018 to develop a strategy for a quantum internet and demonstrated entanglement over 31 miles last year.
- For quantum researchers, the goal is to scale the networks up to a national level first, and one day even internationally.

- The vast majority of scientists agree that this is unlikely to happen before a couple of decades
  - The quantum internet is without a doubt a very long-term project, with many technical obstacles still standing in the way.
- But the unexpected outcomes that the technology will inevitably bring about on the way will make for an invaluable scientific journey, complete with a plethora of outlandish quantum applications that, for now, cannot even be predicted.

# Quantum Computers

- Quantum computers use atoms to perform calculations
- Computation depends on principles of quantum theory
  - Qubit: quantum bit
  - Superposition of Qubit
  - Entanglement of Qubit

# Features of Quantum Computers



1. Works with Quantum Parallelism
2. Entanglement
3. Keeps the Coherence
4. It has Quantum Bits a.k.a. Qubits

# Classical bit and Qubit

- The ***bit*** is the fundamental concept of classical computation and classical information.

- Quantum computation and quantum information are built upon an analogous concept, the *quantum bit*, or ***qubit*** for short.

- What is a qubit?
  - We're going to describe qubits as *mathematical objects* with certain specific properties.
  - 'But hang on', you say, 'I thought qubits were physical objects.'
    - It's true that qubits, like bits, are realized as actual physical systems, and we describe in detail how this connection between the **abstract mathematical** point of view and **real systems** is made.
    - However, for the most part, we treat qubits as **abstract mathematical objects**.
  - The beauty of treating qubits as abstract entities is that it gives us the freedom to construct a general theory of quantum computation and quantum information which does not depend upon a specific system for its realization.

# Classical bit and Qubit (Cont.)

- **A classical bit is a** data element with two values, 0 and 1:
  - It can be represented using an almost endless array of physical phenomena; classical computers typically use charge in active CMOS circuits or the direction of a tiny magnetic field on a disk drive.

- **A qubit is the quantum** equivalent of a bit:
  - It is represented using either a true two-level system, such as the direction of polarization of a photon or the direction of spin of an electron, or a pseudo-two-level system, such as two energy levels of an atom that can be treated as a two-level system.
  - Of course, an electron spins in either the “up” or “down” direction, not zero and one; therefore, we chose to label the two states as our zero and one states, much as we choose e.g. +5 volts to be a logical one and ground to be a logical zero in classical circuits.

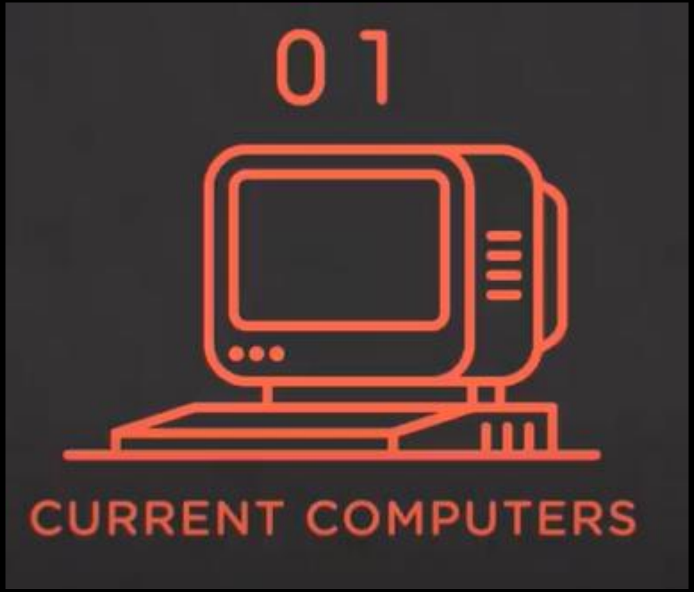
$|\psi>$

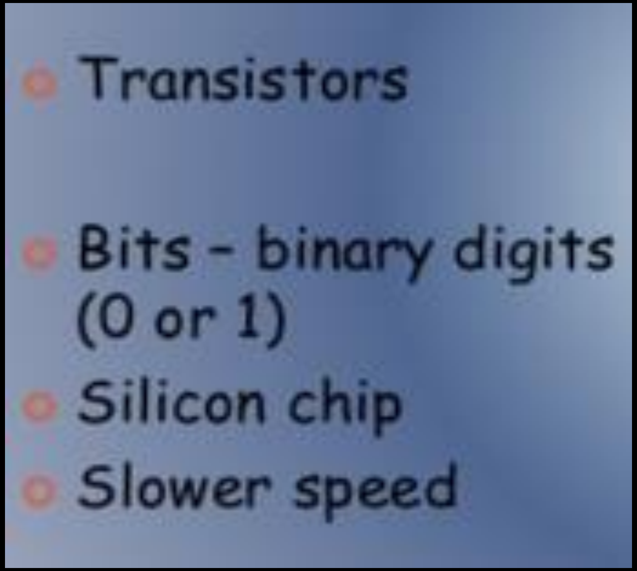
- **The difference between** a classical bit and a qubit is that a **qubit can be in a superposition** of the two states; it can be partially zero and partially one. The state of a qubit can be written as

$$|\psi> = \alpha|0> + \beta|1>$$

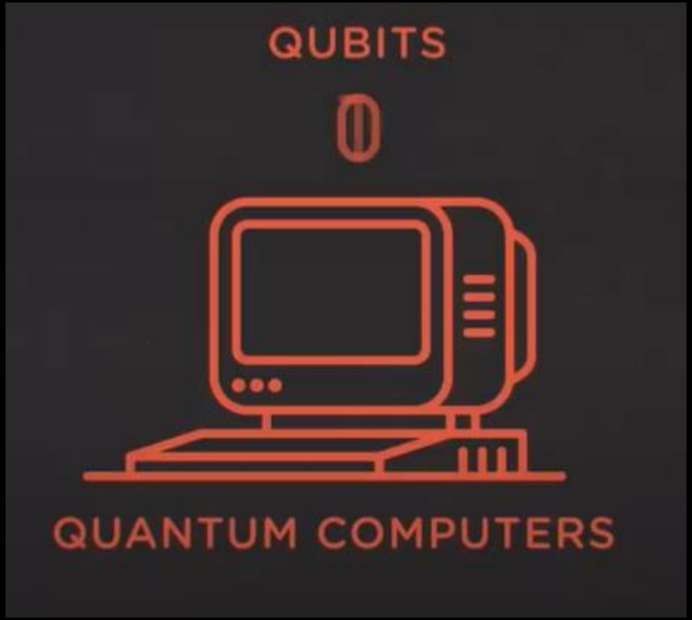
where $\alpha$ and $\beta$ are complex numbers, $|\alpha|2$ is the probability of finding the qubit in the state 0, and $|\alpha|2 + |\beta|2 = 1$: the qubit must be found to be in one state or the other.

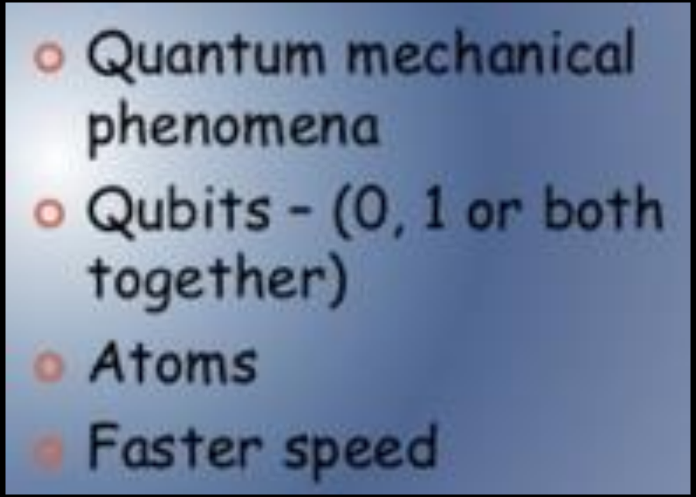
# Classical vs. Quantum Computer





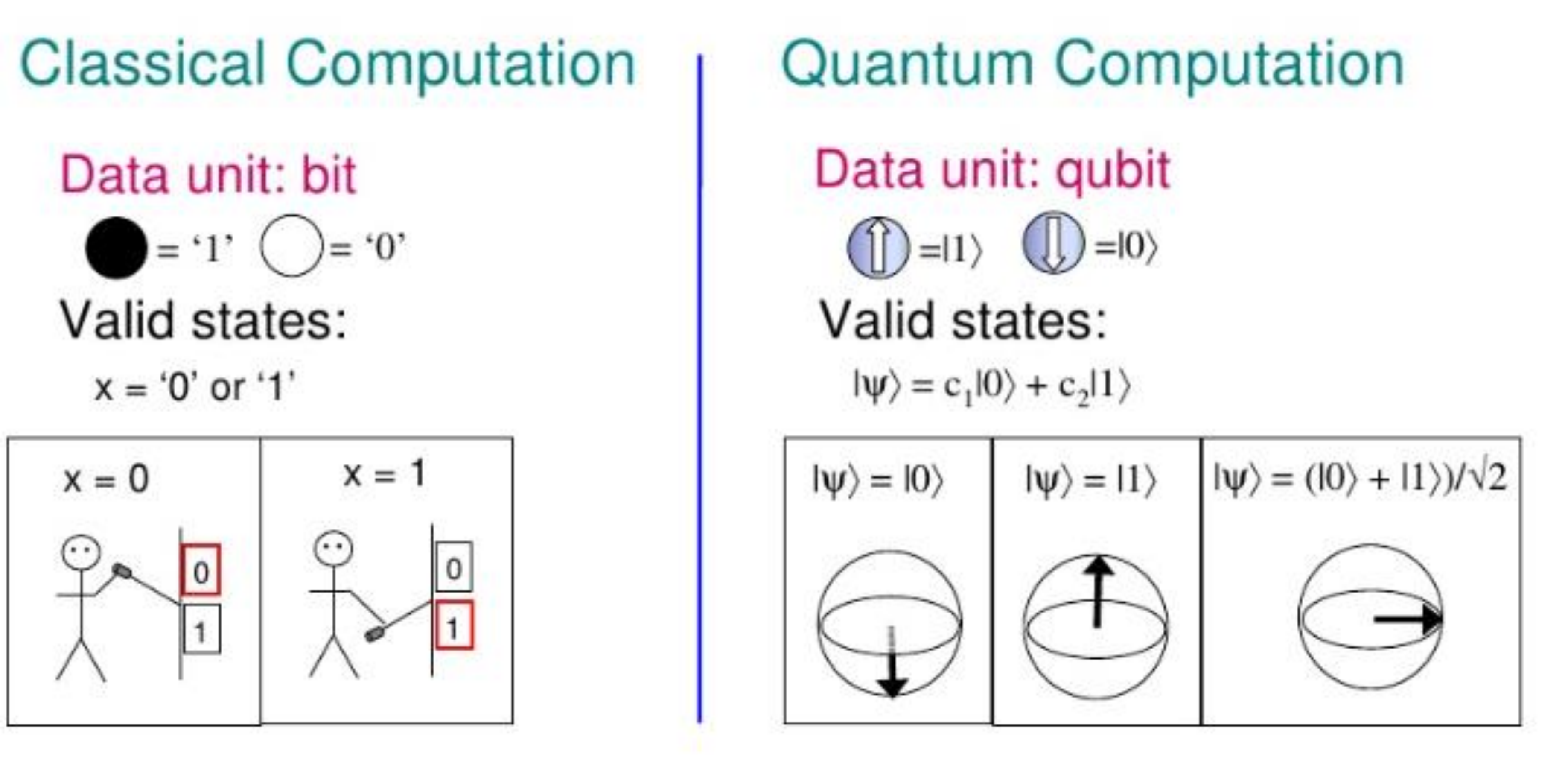
- Transistors
- Bits – binary digits (0 or 1)
- Silicon chip
- Slower speed





- Quantum mechanical phenomena
- Qubits – (0, 1 or both together)
- Atoms
- Faster speed

# Classical Computation vs. Quantum Computation



## Classical Computation

Data unit: bit

● = '1' ○ = '0'

Valid states:

x = '0' or '1'

x = 0

x = 1

## Quantum Computation

Data unit: qubit

⇧ $=|1\rangle$ ⇩ $=|0\rangle$

Valid states:

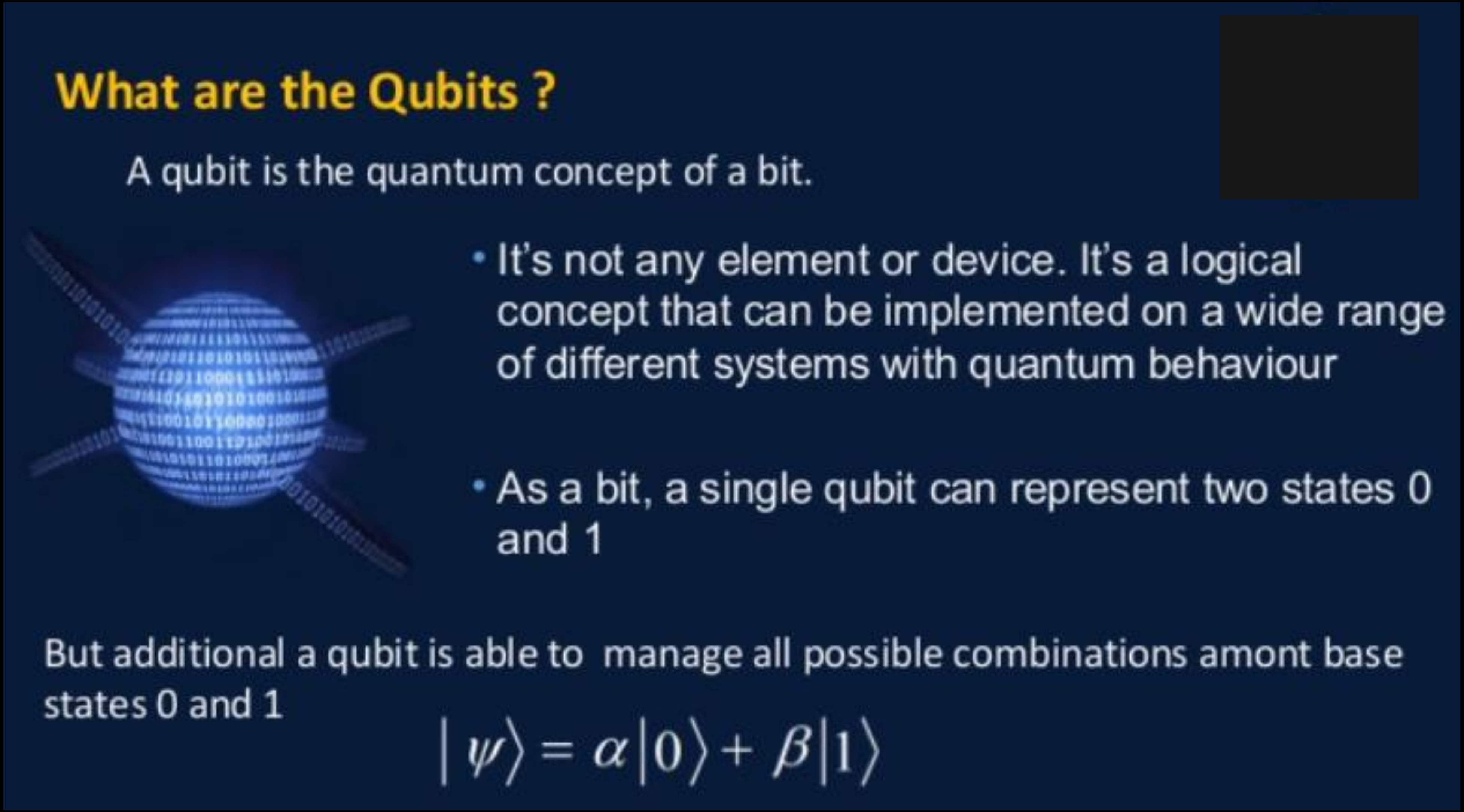
$|\psi\rangle = c_1|0\rangle + c_2|1\rangle$

$|\psi\rangle = |0\rangle$

$|\psi\rangle = |1\rangle$

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

# Qubits



## What are the Qubits ?

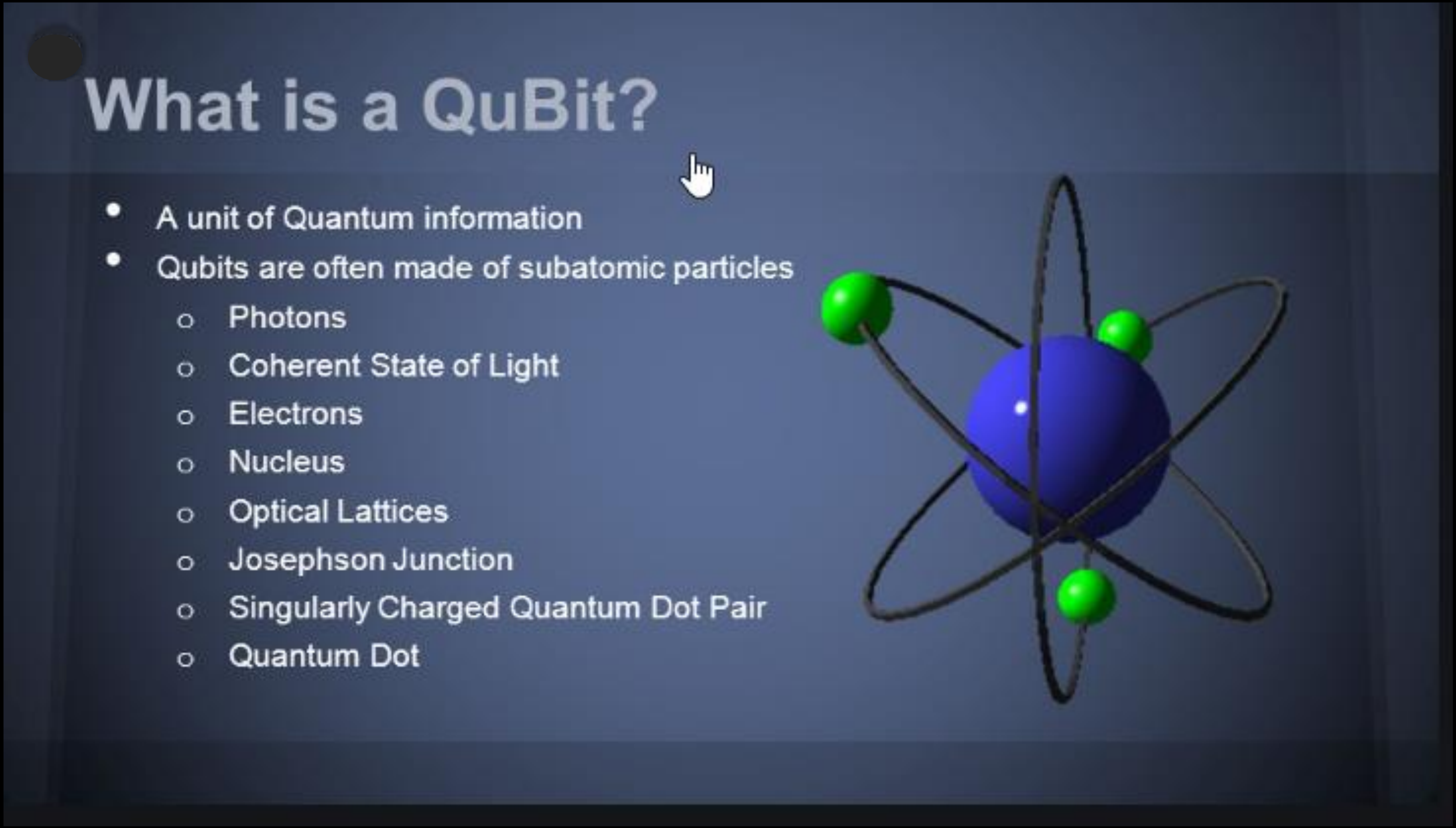
[redacted]

A qubit is the quantum concept of a bit.

- It's not any element or device. It's a logical concept that can be implemented on a wide range of different systems with quantum behaviour
- As a bit, a single qubit can represent two states 0 and 1

But additional a qubit is able to  manage all possible combinations amont base states 0 and 1

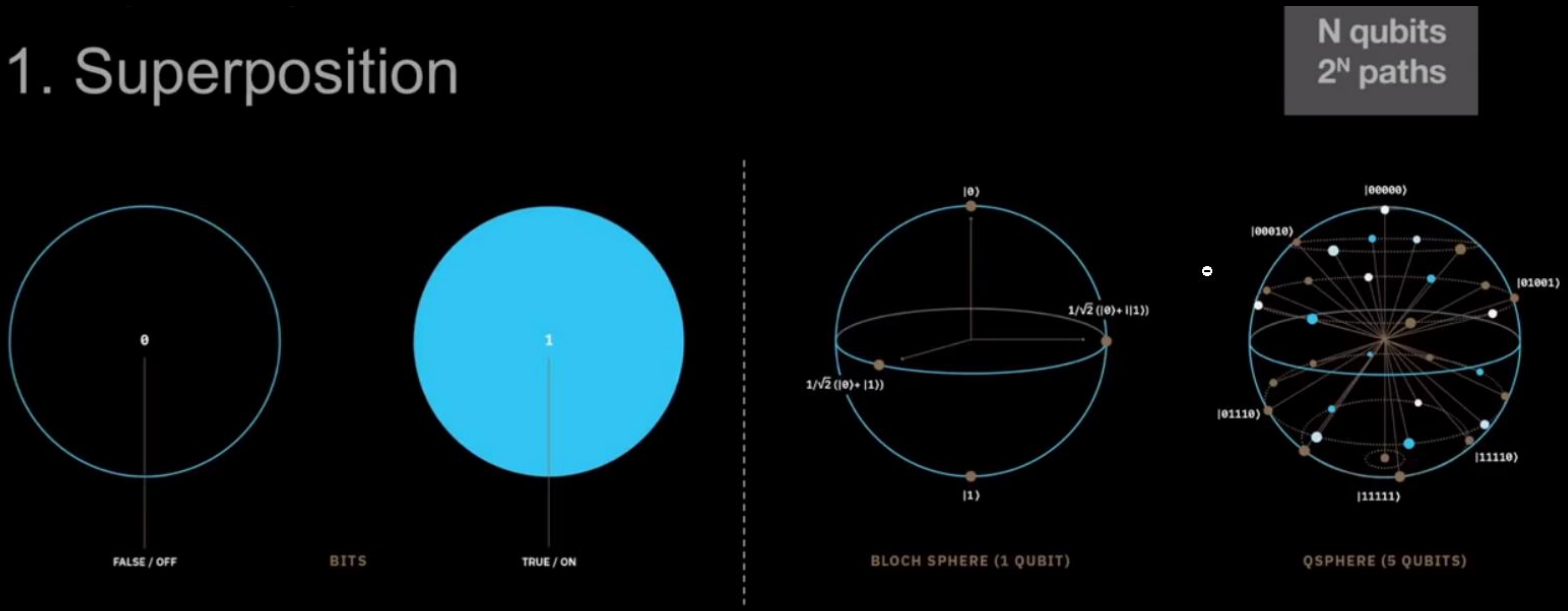
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



# What is a QuBit?

- A unit of Quantum information
- Qubits are often made of subatomic particles
    - Photons
    - Coherent State of Light
    - Electrons
    - Nucleus
    - Optical Lattices
    - Josephson Junction
    - Singularly Charged Quantum Dot Pair
    - Quantum Dot

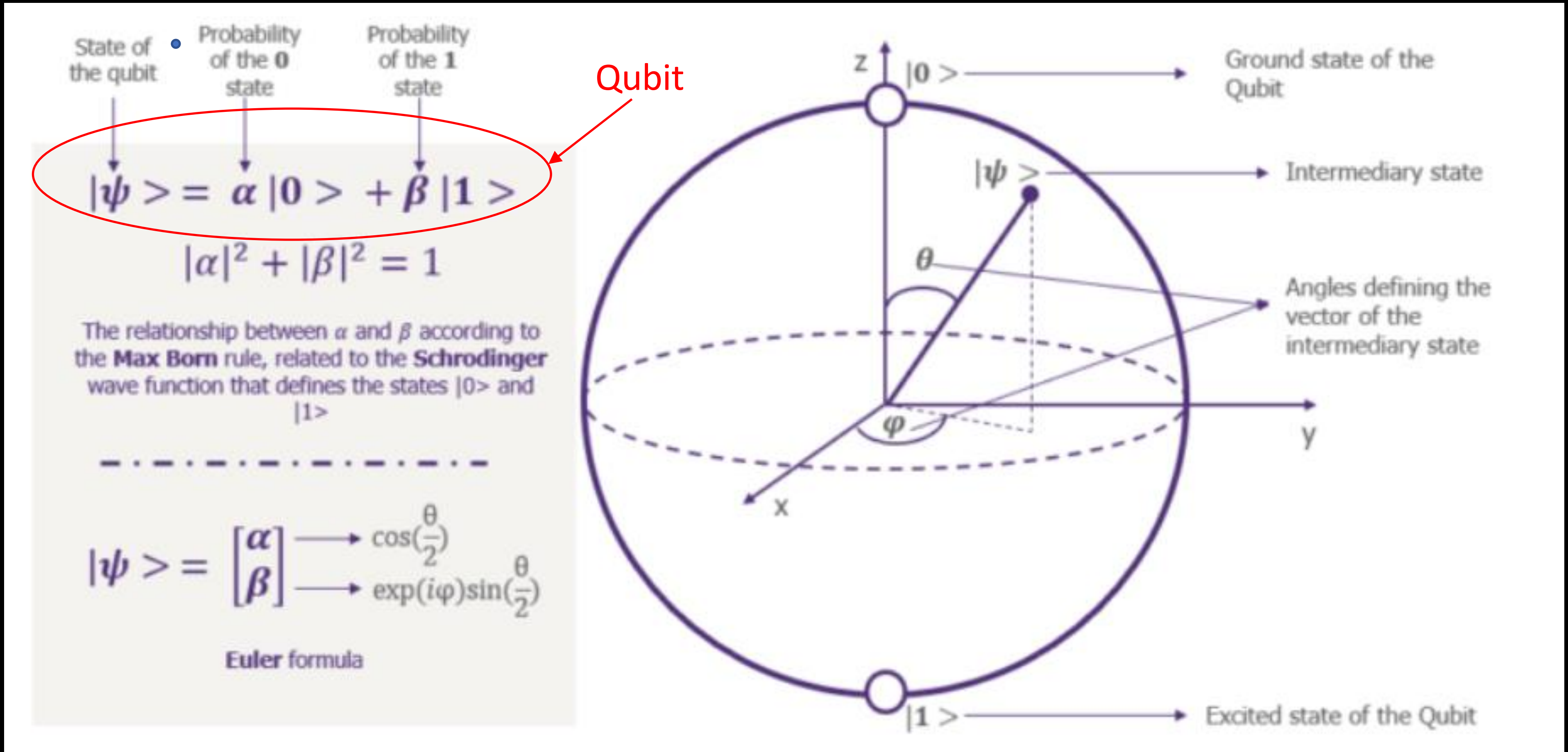
# Qubits Representation in Bloch sphere



1. Superposition

N qubits
$2^N$ paths

# Mathematical Model of Qubit



State of the qubit

Probability of the **0** state

Probability of the **1** state

Qubit

$$|\psi> = \alpha\,|0> + \beta\,|1>$$

$$|\alpha|^2 + |\beta|^2 = 1$$

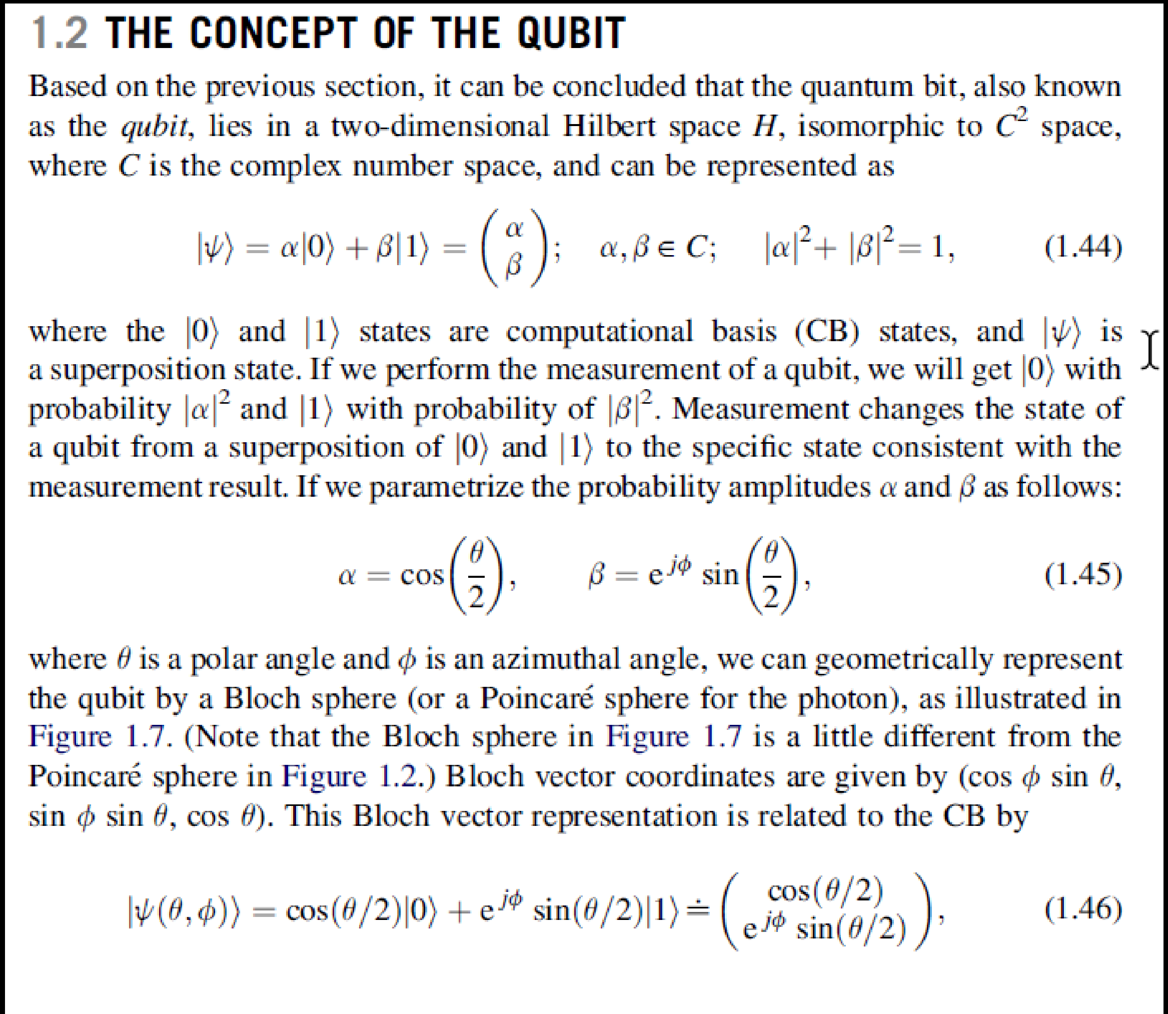
The relationship between $\alpha$ and $\beta$ according to the **Max Born** rule, related to the **Schrodinger** wave function that defines the states |0> and |1>

$$|\psi> = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{matrix} \longrightarrow \cos(\frac{\theta}{2}) \\ \longrightarrow \exp(i\varphi)\sin(\frac{\theta}{2}) \end{matrix}$$

**Euler** formula

z
|0 >
Ground state of the Qubit
|ψ >
Intermediary state
θ
Angles defining the vector of the intermediary state
φ
x
y
|1 >
Excited state of the Qubit

# Concept of Qubit



## 1.2 THE CONCEPT OF THE QUBIT

Based on the previous section, it can be concluded that the quantum bit, also known as the *qubit*, lies in a two-dimensional Hilbert space $H$, isomorphic to $C^2$ space, where $C$ is the complex number space, and can be represented as

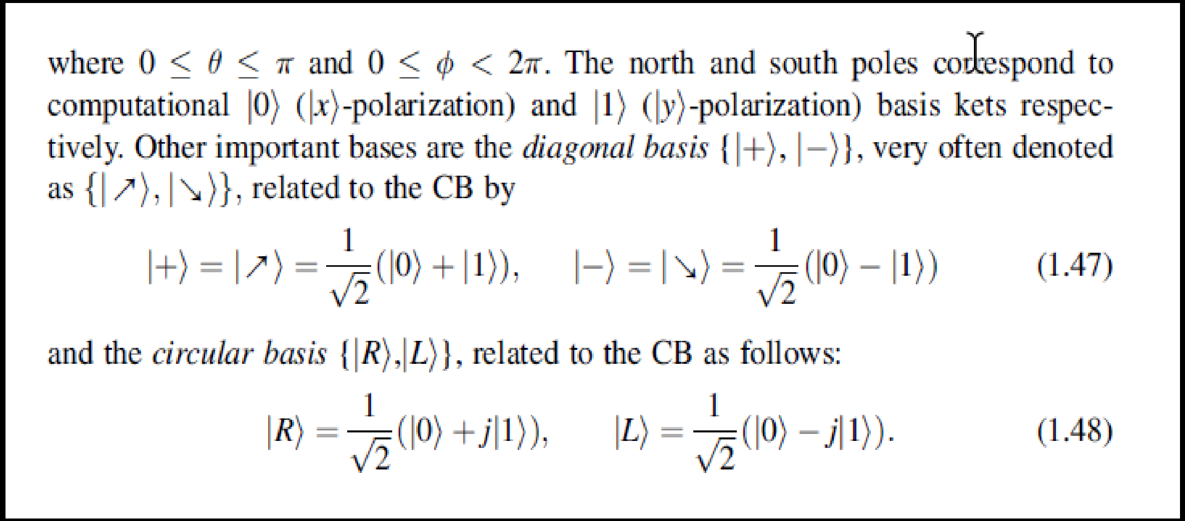
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \quad \alpha, \beta \in C; \quad |\alpha|^2 + |\beta|^2 = 1, \tag{1.44}$$

where the $|0\rangle$ and $|1\rangle$ states are computational basis (CB) states, and $|\psi\rangle$ is a superposition state. If we perform the measurement of a qubit, we will get $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability of $|\beta|^2$. Measurement changes the state of a qubit from a superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the measurement result. If we parametrize the probability amplitudes $\alpha$ and $\beta$ as follows:

$$\alpha = \cos\left(\frac{\theta}{2}\right), \qquad \beta = e^{j\phi} \sin\left(\frac{\theta}{2}\right), \tag{1.45}$$

where $\theta$ is a polar angle and $\phi$ is an azimuthal angle, we can geometrically represent the qubit by a Bloch sphere (or a Poincaré sphere for the photon), as illustrated in Figure 1.7. (Note that the Bloch sphere in Figure 1.7 is a little different from the Poincaré sphere in Figure 1.2.) Bloch vector coordinates are given by ($\cos\phi \sin\theta$, $\sin\phi \sin\theta$, $\cos\theta$). This Bloch vector representation is related to the CB by

$$|\psi(\theta,\phi)\rangle = \cos(\theta/2)|0\rangle + e^{j\phi}\sin(\theta/2)|1\rangle \doteq \begin{pmatrix} \cos(\theta/2) \\ e^{j\phi}\sin(\theta/2) \end{pmatrix}, \tag{1.46}$$

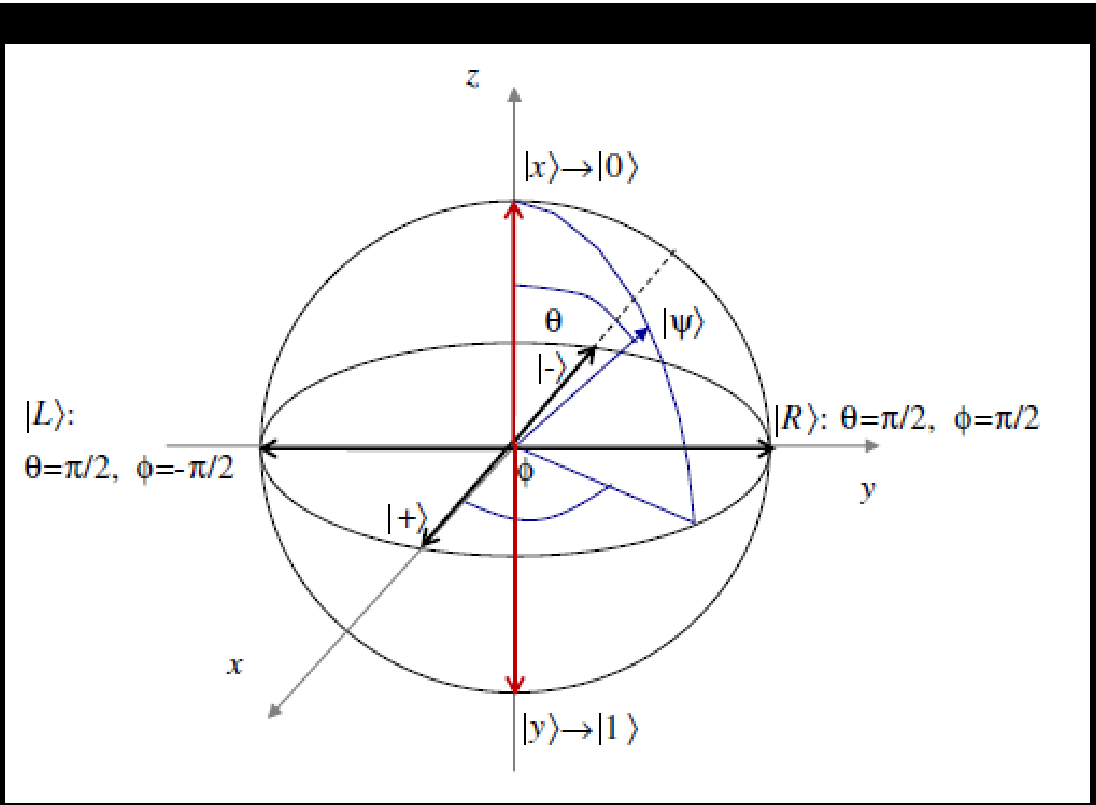


where $0 \le \theta \le \pi$ and $0 \le \phi < 2\pi$. The north and south poles correspond to computational $|0\rangle$ ($|x\rangle$-polarization) and $|1\rangle$ ($|y\rangle$-polarization) basis kets respectively. Other important bases are the *diagonal basis* $\{|+\rangle, |-\rangle\}$, very often denoted as $\{|\nearrow\rangle, |\searrow\rangle\}$, related to the CB by

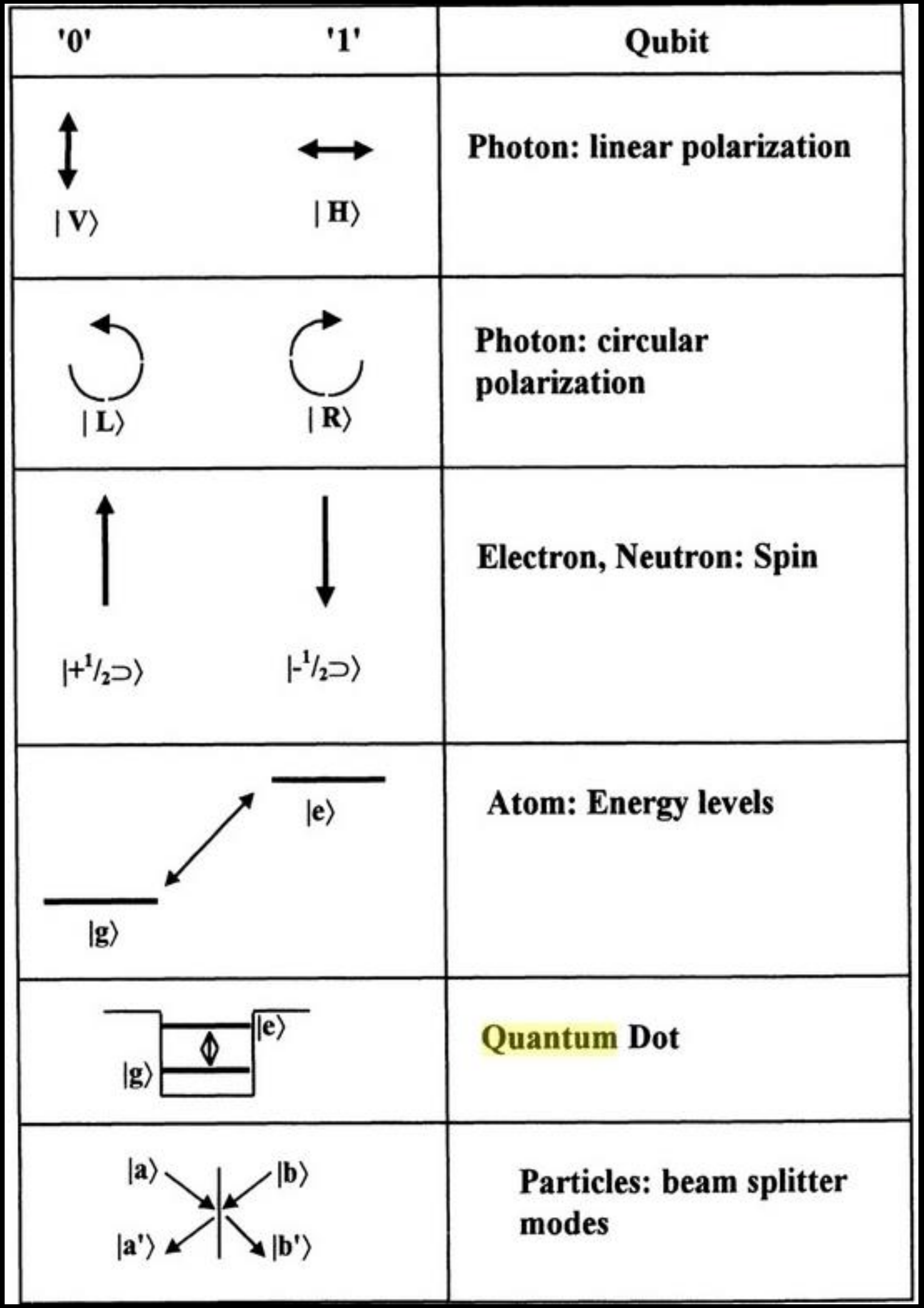
$$|+\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.47}$$

and the *circular basis* $\{|R\rangle, |L\rangle\}$, related to the CB as follows:

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + j|1\rangle), \qquad |L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - j|1\rangle). \tag{1.48}$$



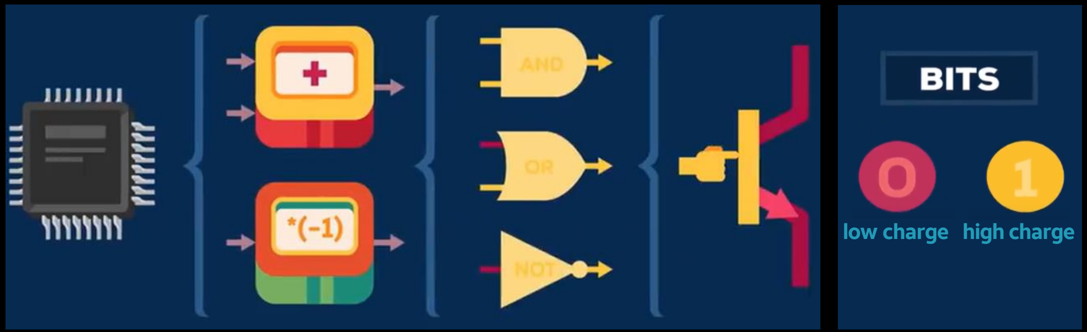
# Physical Realizations of Qubits



| '0' | '1' | Qubit |
|---|---|---|
| $\lvert V\rangle$ | $\lvert H\rangle$ | **Photon: linear polarization** |
| $\lvert L\rangle$ | $\lvert R\rangle$ | **Photon: circular polarization** |
| $\lvert +{}^1/_2\supset\rangle$ | $\lvert -{}^1/_2\supset\rangle$ | **Electron, Neutron: Spin** |
| $\lvert g\rangle$ | $\lvert e\rangle$ | **Atom: Energy levels** |
| $\lvert g\rangle$ | $\lvert e\rangle$ | **Quantum Dot** |
| $\lvert a\rangle$<br>$\lvert a'\rangle$ | $\lvert b\rangle$<br>$\lvert b'\rangle$ | **Particles: beam splitter modes** |

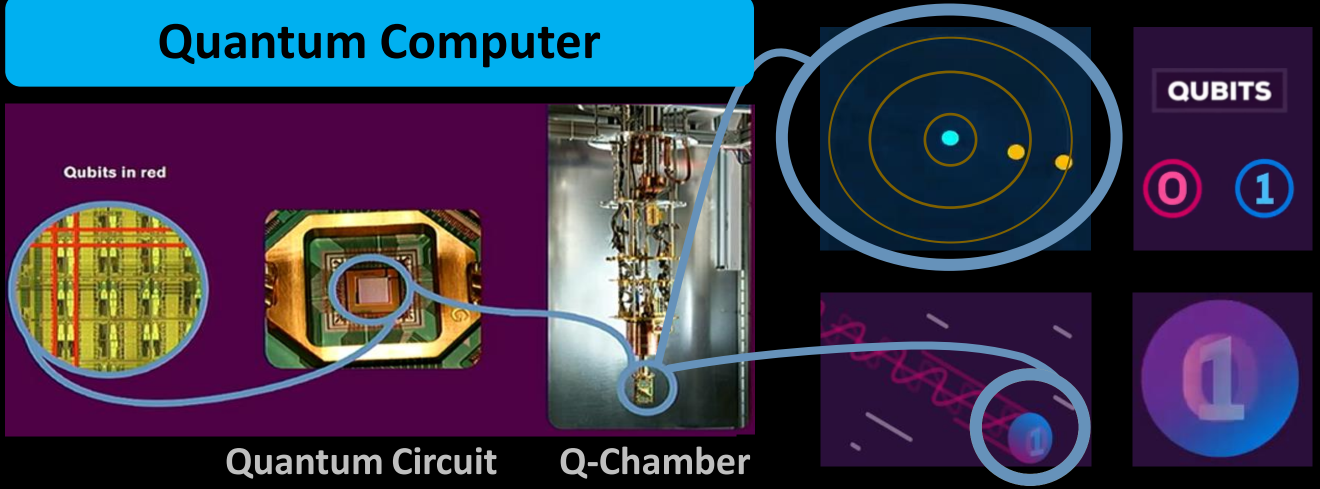
# Classical vs. Quantum Computers Basics

## Classical Computer



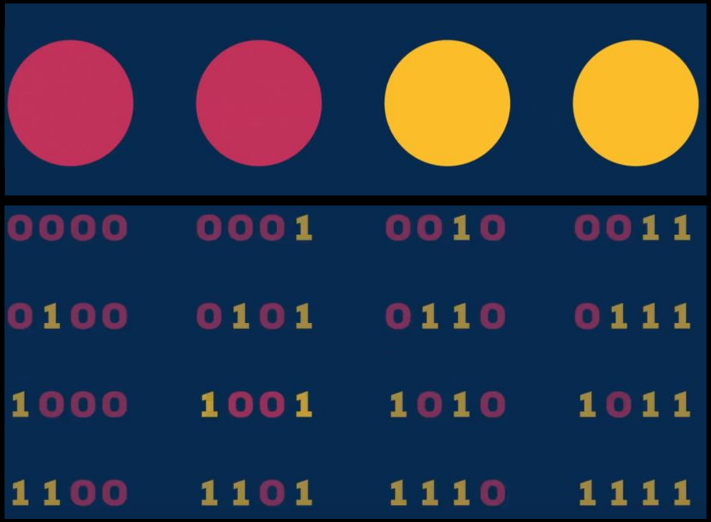
IC Circuit Module Logic gates Transistor

## Quantum Computer



Quantum Circuit Q-Chamber

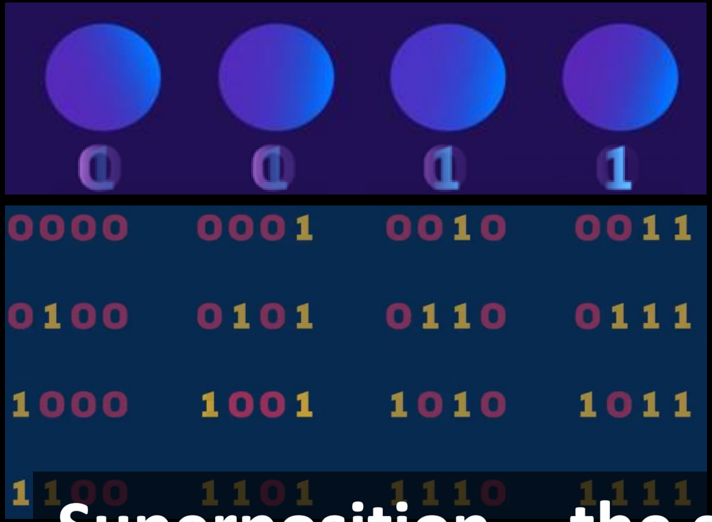
## 4-bit Classical Register



| | | | |
|---|---|---|---|
| 0000 | 0001 | 0010 | 0011 |
| 0100 | 0101 | 0110 | 0111 |
| 1000 | 1001 | 1010 | 1011 |
| 1100 | 1101 | 1110 | 1111 |

- One number from 0 to 15 at a time

## 4-qubit Register



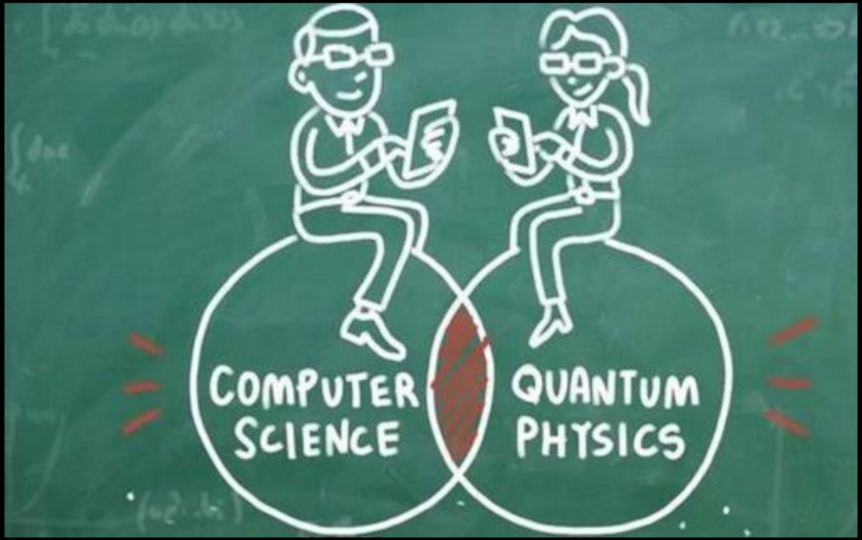
| | | | |
|---|---|---|---|
| 0000 | 0001 | 0010 | 0011 |
| 0100 | 0101 | 0110 | 0111 |
| 1000 | 1001 | 1010 | 1011 |
| 1100 | 1101 | 1110 | 1111 |

- All 16 numbers in a superposition allowing truly parallel computation
- Exponential growth with addition of each qubit:

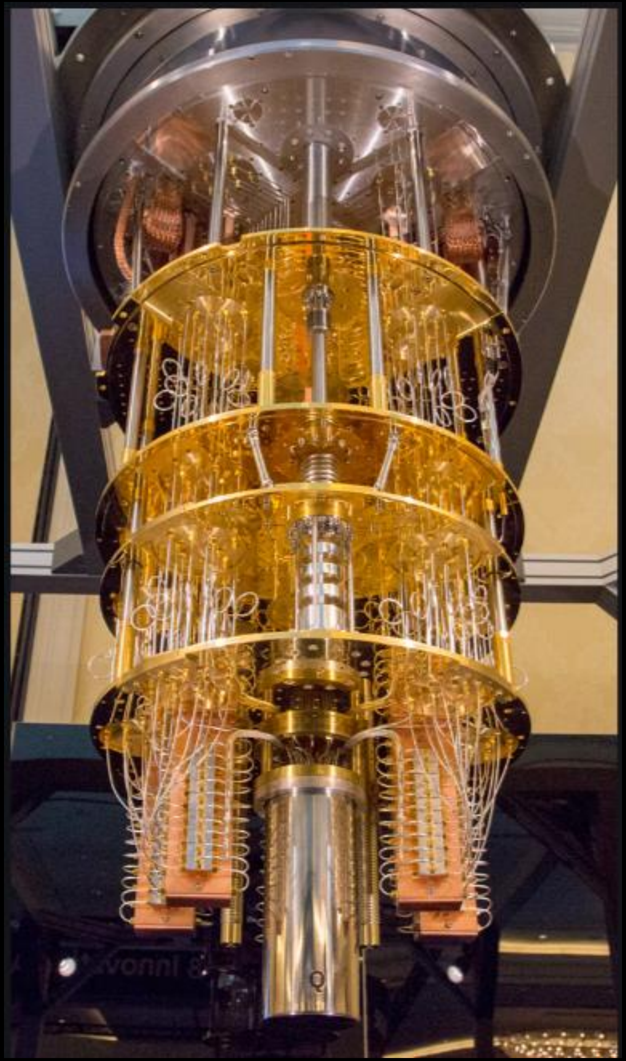
$2^{20} = 1{,}048{,}576$

**Superposition -- the game changer**

# What is Quantum Computing?



**Quantum + Computing = Quantum Computing**



A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the *sub-atomic* level