Let's go

The bridge to possible

An Introduction to Quantum Network Technologies

What Every Network and Security Engineer Should Know About Quantum Technologies

Tim Szigeti, Principal Technical Marketing Engineer
Outshift by Cisco

Pre-Session Quiz

1) What are some use-cases for quantum networks?
2) What are some of the special properties of quantum bits (Qubits)?
3) What makes a quantum computer so fast?
4) What is Y2Q? And when do most experts expect it?
5) Can you transmit information faster than light with quantum teleporting?
6) Will quantum networks replace classical networks?
7) What is Cisco researching and developing in Quantum?

Agenda

- Why Build Quantum Networks?
- Intro to Quantum Mechanics
- Intro to Quantum Computing
  - Implications of Quantum Computing on Network Security
- Intro to Quantum Networking
- What is Cisco Doing?
- Summary & Next Steps

Why Build Quantum Networks?

Quantum Cryptography

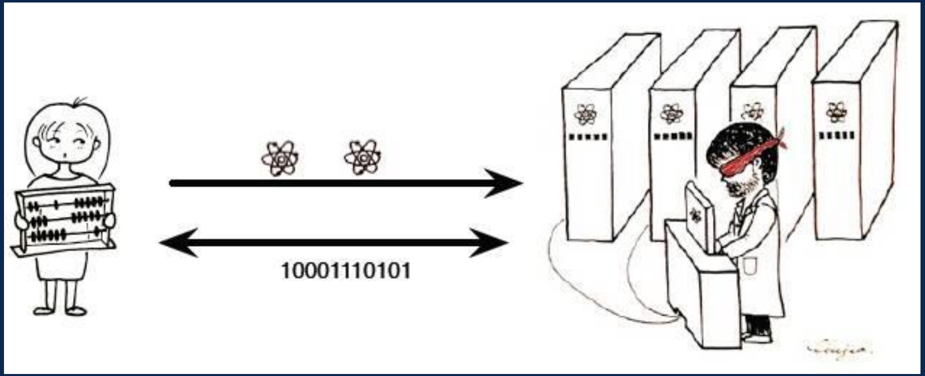
- Quantum networks can be used to securely exchange cryptographic keys, as these are mathematically proven to detect and prevent eavesdropping
- The most well-known method of this application is *Quantum Key Distribution (QKD)*

Distributed Quantum Computing

- Interconnecting geographically-dispersed quantum computers to realize benefits such as:
  - Increased Processing Power
  - Distributed Quantum Computing
  - Specialized Quantum Modules
  - Fault Tolerance
  - Hybrid Quantum-Classical Systems
  - Etc.

Blind Quantum Computing

- A privacy-preserving method in which a client can delegate a computation task to remote quantum computer(s) without disclosing the source data or algorithms
- The results of the computations would likewise be private



Network Clock Synchronization

- A world-wide set of high-precision clocks connected by quantum networks could achieve ultra precise clock signals
- Current accuracy: ≤ 30 ns
- Quantum accuracy: ≤1ps

https://www.gps.gov/systems/gps/performance/accuracy/
https://ieeexplore.ieee.org/document/9856607

Distributed Sensing

- Signals from distributed sensors can be combined via quantum networks to obtain higher-accuracy measurements than currently possible with classical network interconnections
- E.g. Deep Space Telescope Array
  - Classical precision: $\pm\ 1/\sqrt{N}$
  - Quantum precision: $\pm\ 1/N$

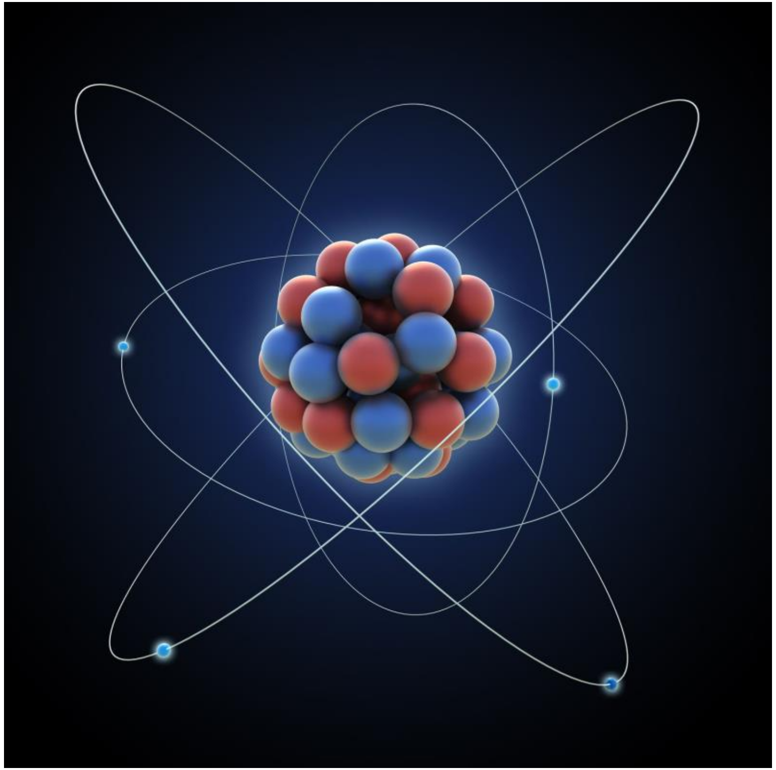
Quantum Money

- The main security requirement of money is unforgeability
- A quantum money scheme aims to fulfill by this requirement by exploiting the no-cloning property of the unknown quantum states

An Introduction to Quantum Mechanics

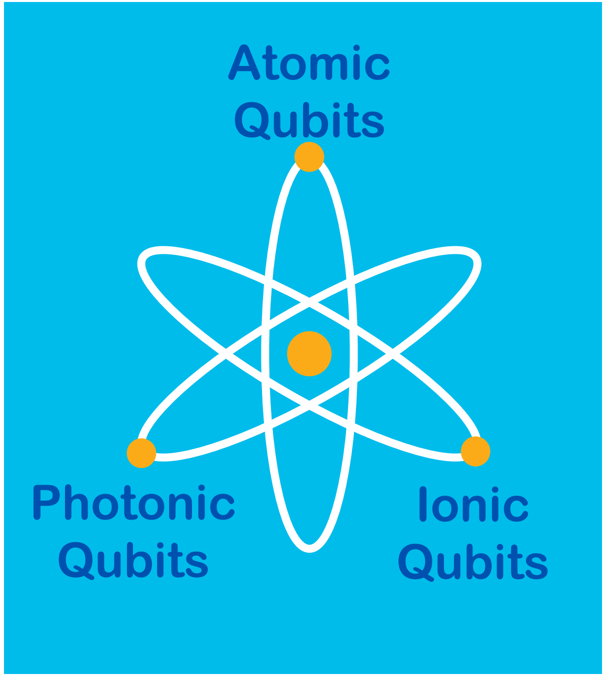
What is Quantum Mechanics?

- Quantum mechanics is the field of physics that explains how subatomic objects simultaneously have the characteristics of both:
  - **Particles**—tiny pieces of matter, and
  - **Waves**—variations that transfer energy



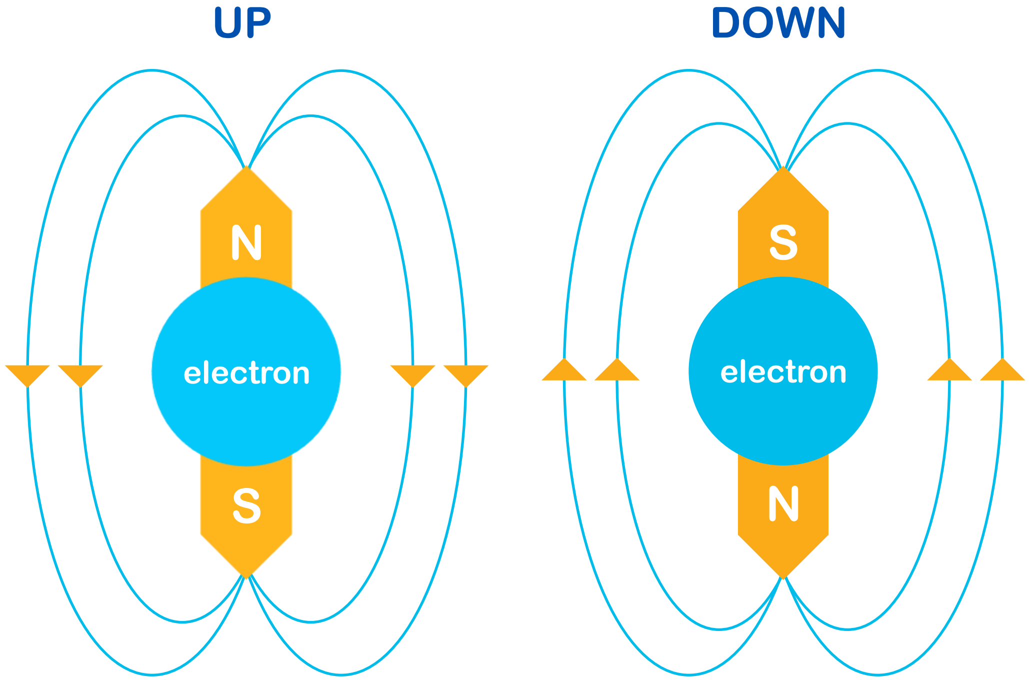
Quantum Bits (Qubits)

- Any quantum particle that can be measured in two discrete states, and as such, could be used to represent information
  - E.g. a 0 or 1



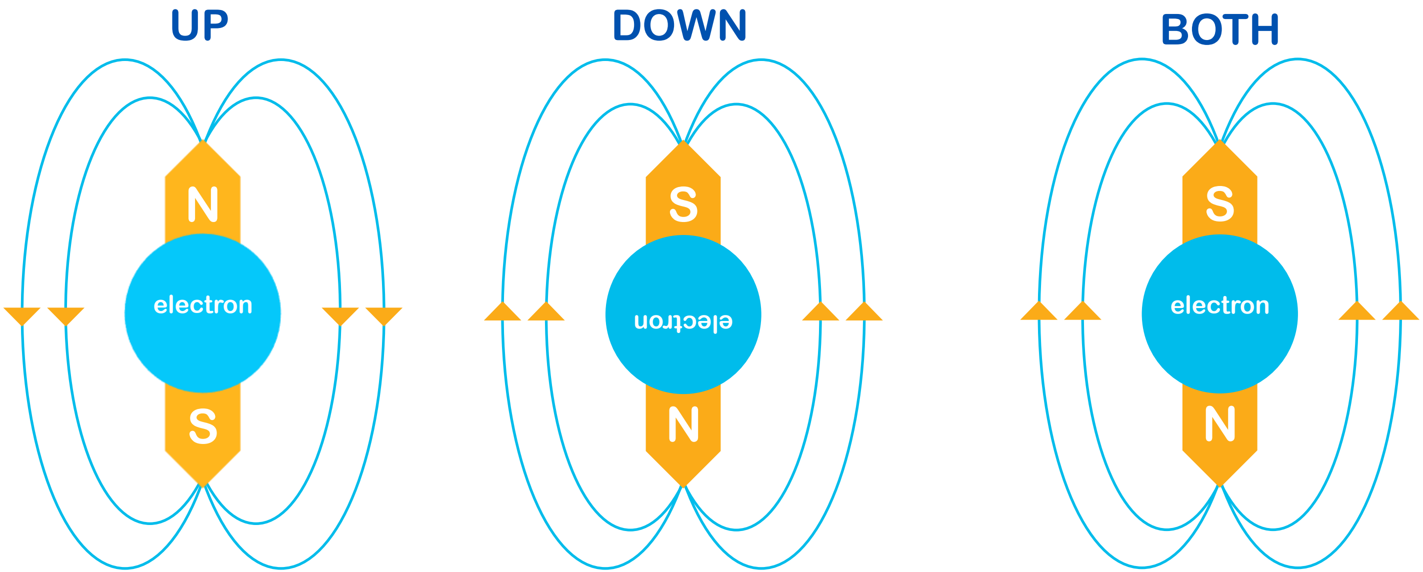
Qubit Example

- The spin of an electron can be used as a Qubit
- For example:
  - An upwards spin could be used represent a 0
  - A downward spin could be used to represent 1



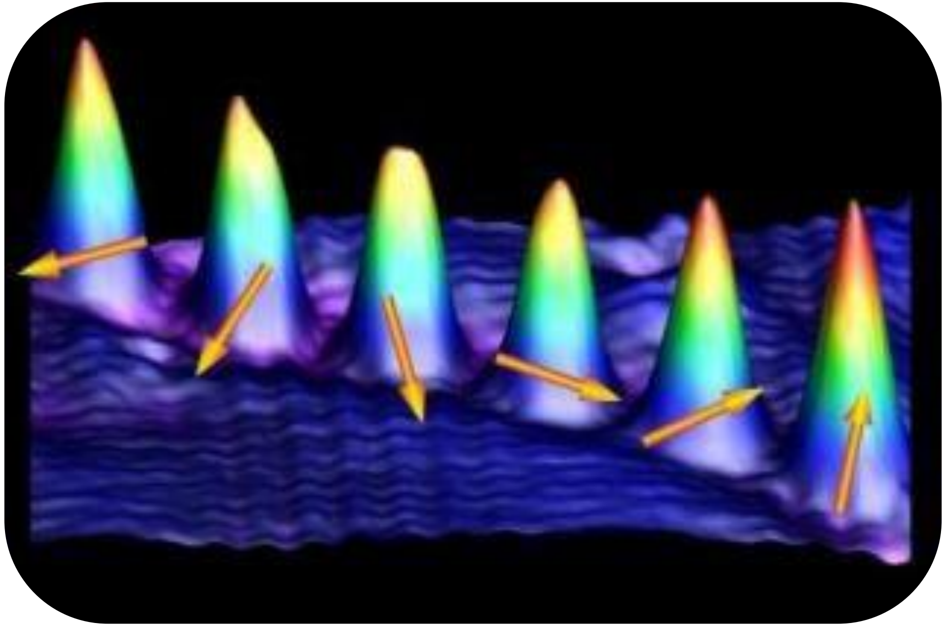
Angular Momentum

- The spin may not always be perfectly up or down, but angular
  - i.e. some *combination* of BOTH up-spin and down-spin



An Electron Microscope View Of Electron Spin

- The pointier the hat, the more upward the spin



General Quantum State Formula

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

Quantum State
represented by Psi

(Psi is the 23rd letter of the Greek alphabet)

Alpha Ket 0
Alpha represents the amplitude of state 0

(Alpha is the first letter of the Greek alphabet)

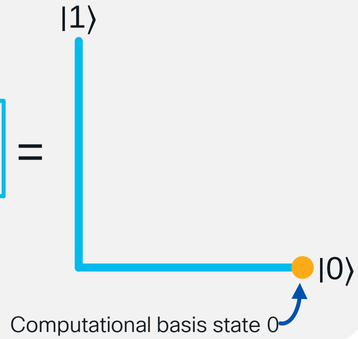
Beta Ket 1
Beta represents the amplitude of state 1

(Beta is the second letter of the Greek alphabet)

Quantum State and Vectors

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

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$



$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Vector 0

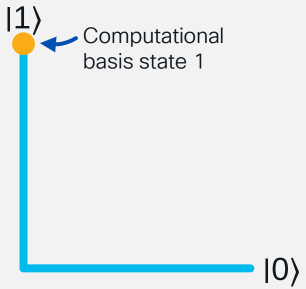
X-Axis Coordinate

Y-Axis Coordinate

$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Vector 1

$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} =$



Quantum State and Vectors

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

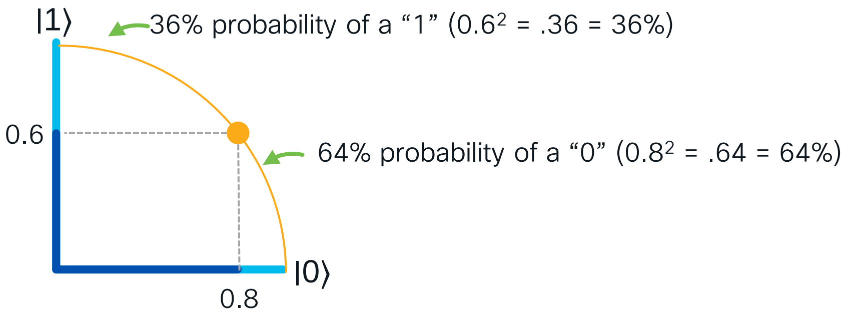
X-Axis Coordinate

Y-Axis Coordinate

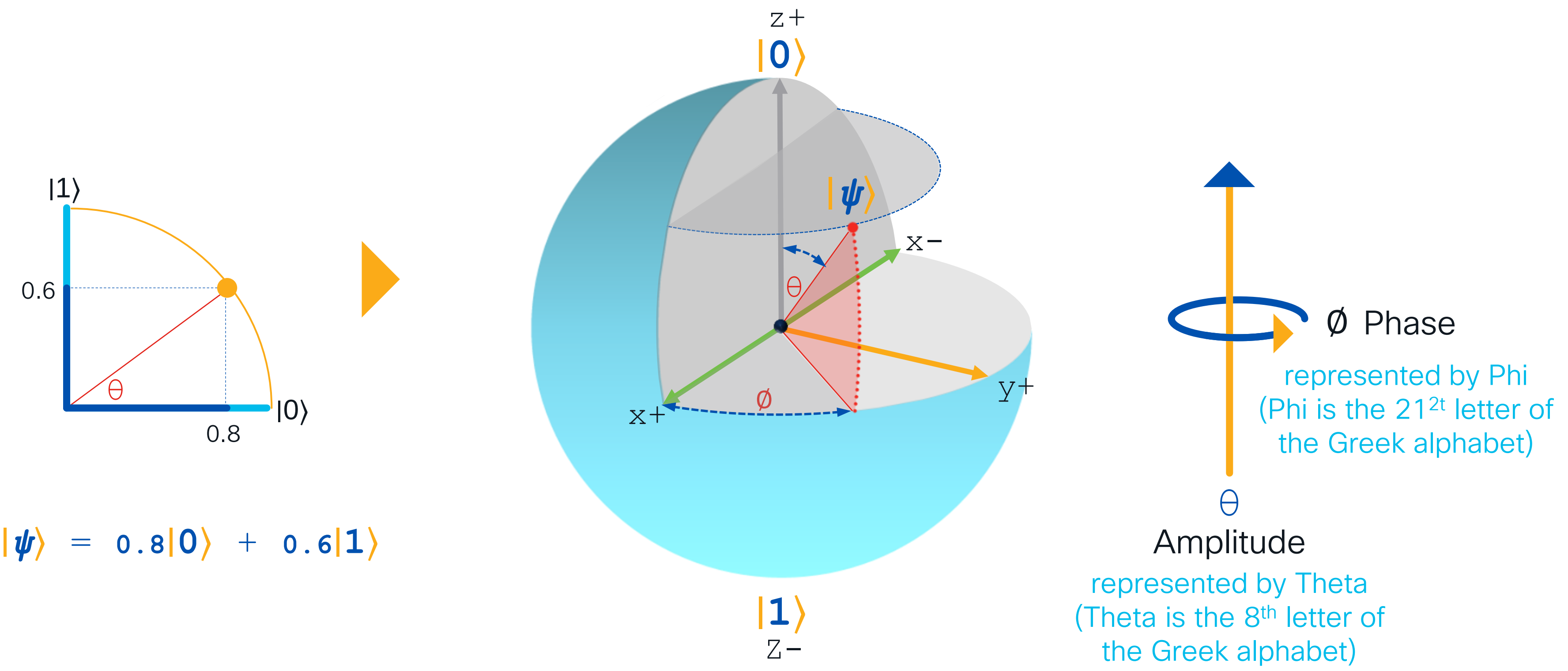
$$|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle = \begin{bmatrix} 0.8 \\ 0.6 \end{bmatrix} =$$

Sums of the squares of probabilities must equal 1

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



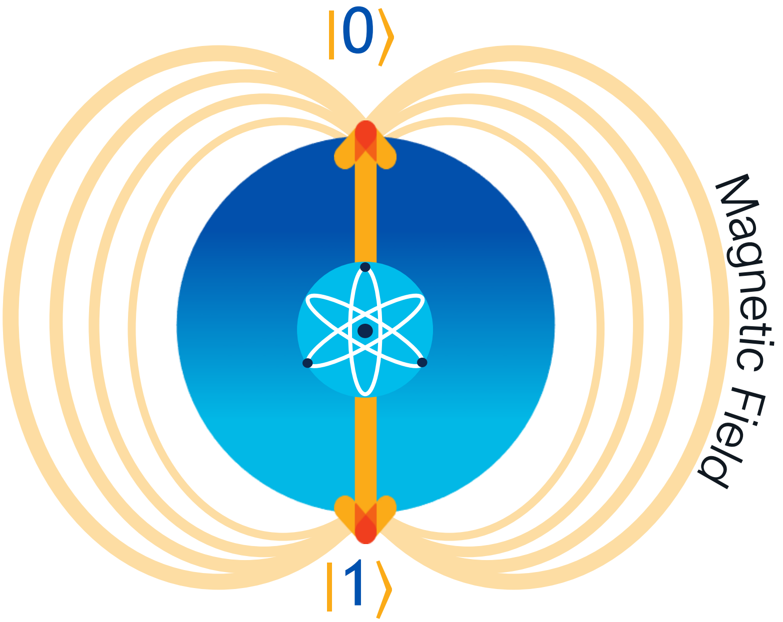
The Bloch Sphere: A 3D Qubit Representation



$$|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle$$

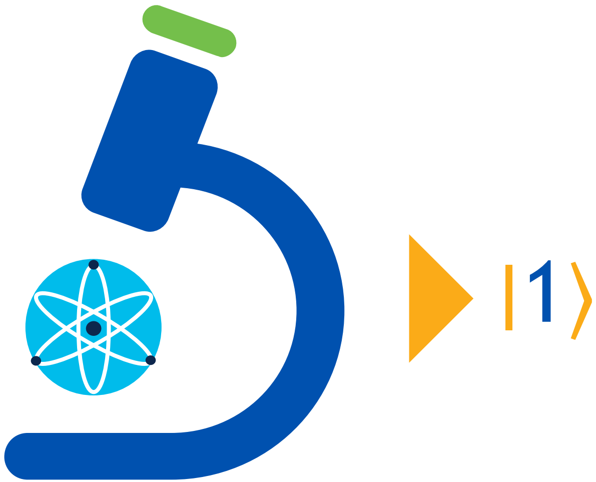
Quantum Special Property: Superposition

- As long a Qubit is unobserved (i.e. unmeasured) it is in a "Superposition" of probabilities for 0 and 1



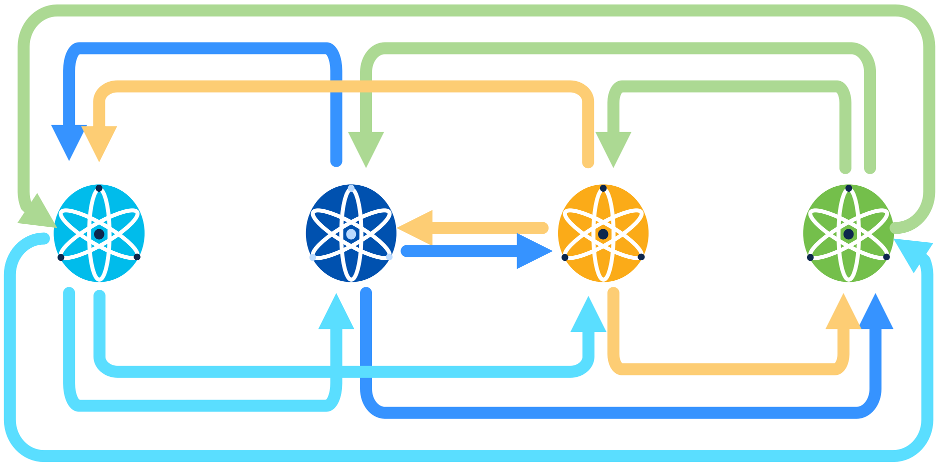
Quantum Special Property: Superposition

- As long a Qubit is unobserved (i.e. unmeasured) it is in a "Superposition" of probabilities for 0 and 1
- The instant a Qubit is measured, the superposition will collapse into one of the two discrete states



Quantum Special Property: Entanglement

- Entanglement is a physical relationship between Qubits where they react to a change in the other(s) state instantaneously regardless of how far they are apart
- Multiple qubits can become entangled with each other
  - The current record is 54



https://www.newscientist.com/article/2382022-record-breaking-number-of-qubits-entangled-in-a-quantum-computer/

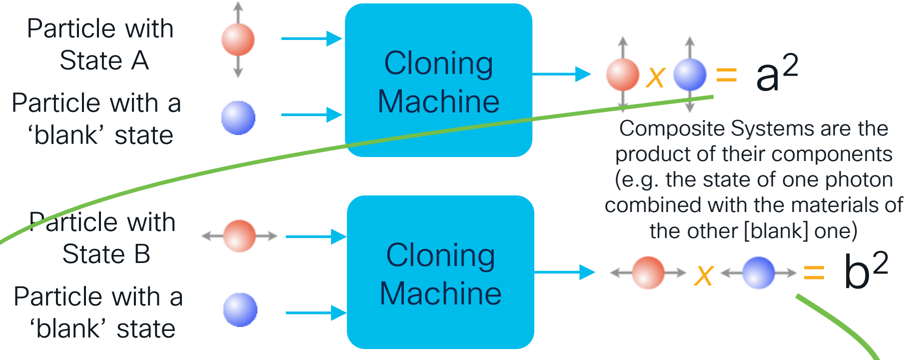
Quantum Special Property: Entanglement

- If an entangled qubit is measured, then entanglement is broken
- The discrete state of the entangled qubit will depend on the entanglement operation that was performed
  - the states may be the same, or
  - the states may be opposite (as shown in this example)
- The important point is that as one entangled qubit changes state, its counterpart(s) will instantaneously reflect that change

Quantum Special Property: No Cloning

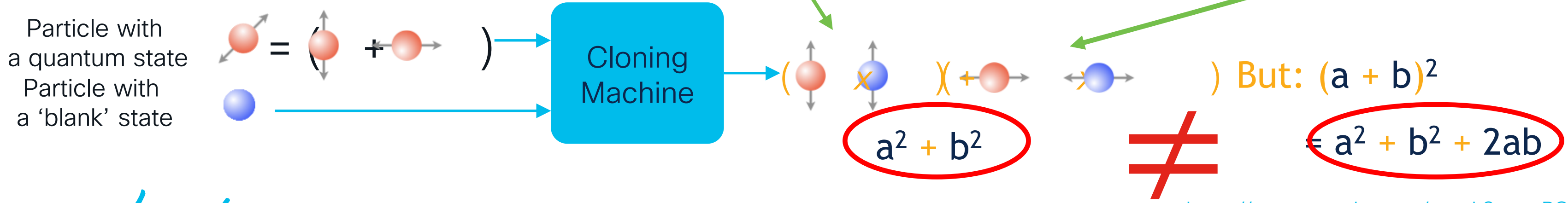
Given: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
Let $a = \alpha|0\rangle$ and $b = \beta|1\rangle$
$|\psi\rangle = (a + b)$

- It can be mathematically proven that it is impossible to clone a qubit
- The proof uses the logical method of "Proof by Contradiction"



For any given Transformation (T): T(a + b) = T(a) + T(b)
Let us assume the transformation is a cloning operation

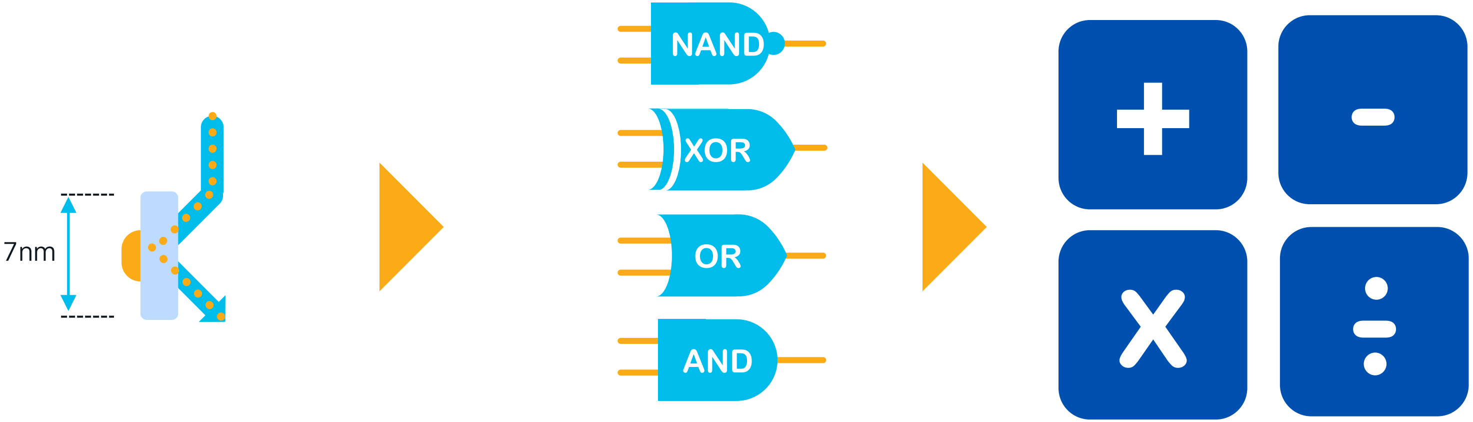
Quantum state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Simplified to: $|\psi\rangle = (a + b)$



https://www.youtube.com/watch?v=owPC60Ue0BE

An Introduction to Quantum Computing

Digital Circuits Quick Recap

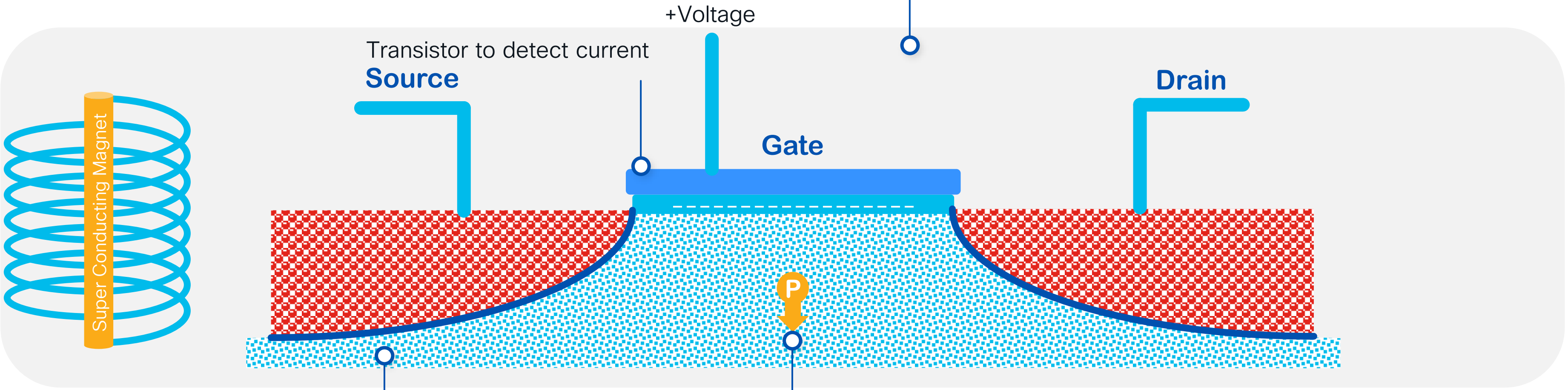


Transistors Logic Gates Circuits

Anatomy of a Compute Qubit

Low Energy State

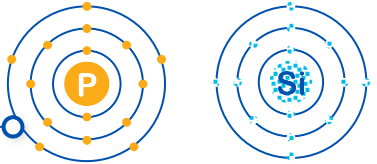
Qubit kept at -273c to minimize thermal energy interference



Bed made from Silicon-28 isotope. No nuclear spin as it is completely non-magnetic (Otherwise Si spin would interfere)

Outer electron in phosphorus atom will be in SPIN DOWN when no energy applied

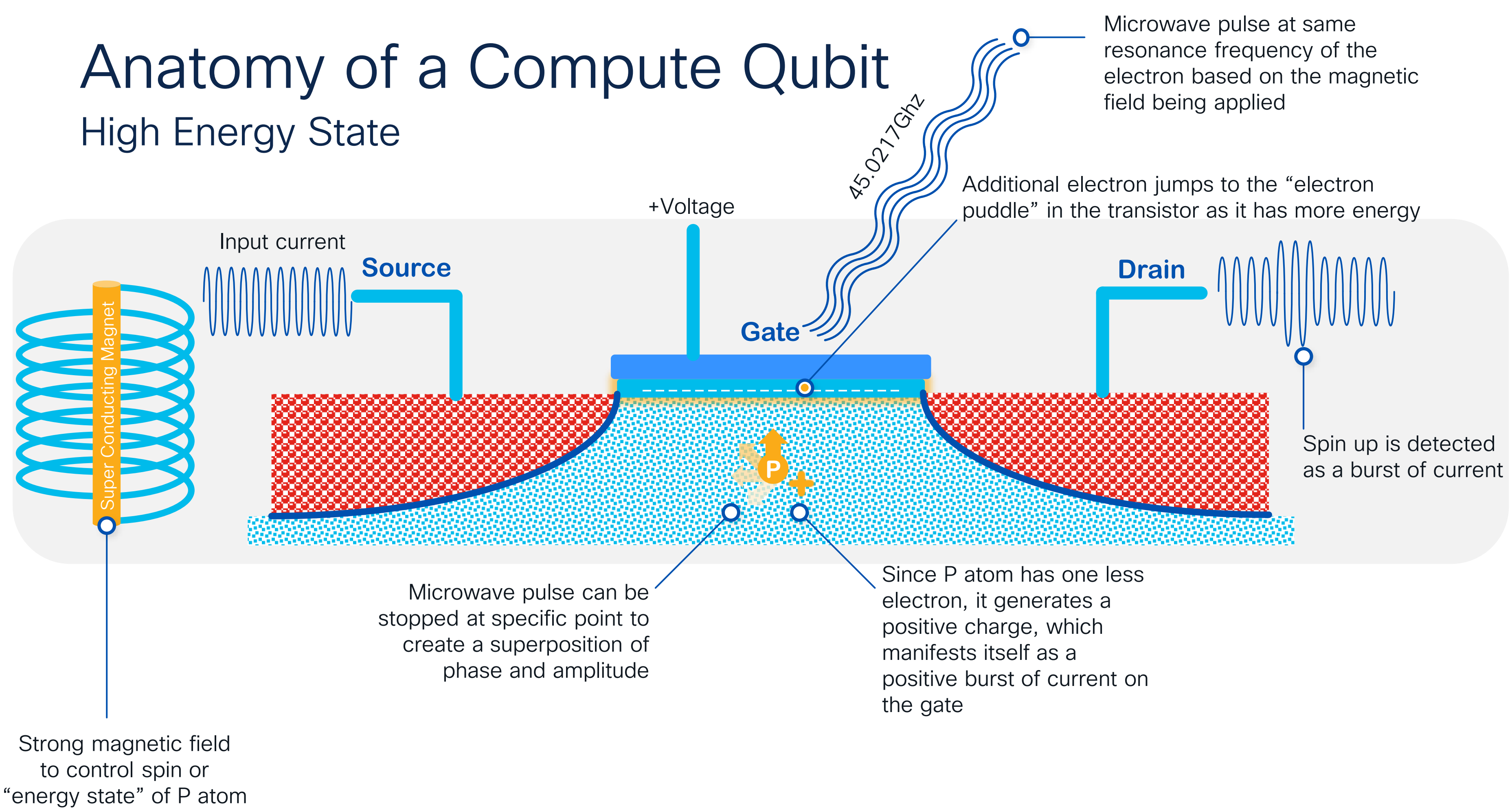
P atom has additional electron in outer shell compared to Si atom



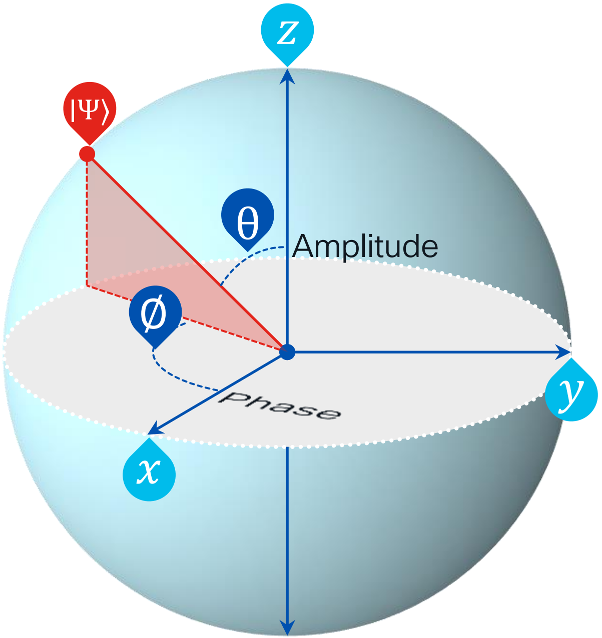
	Phosphorus Atom	Silicon Atom
Electrons	15	14
Protons	15	14
Neutrons	16	14

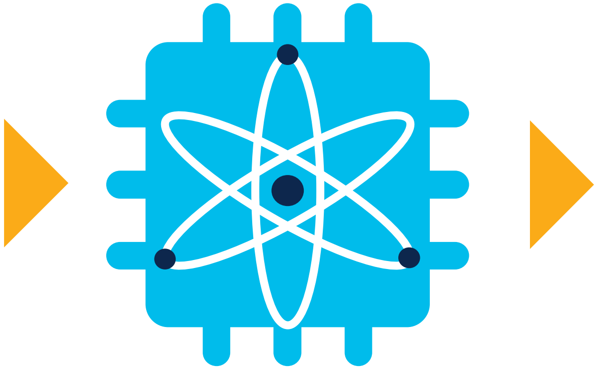
Anatomy of a Compute Qubit

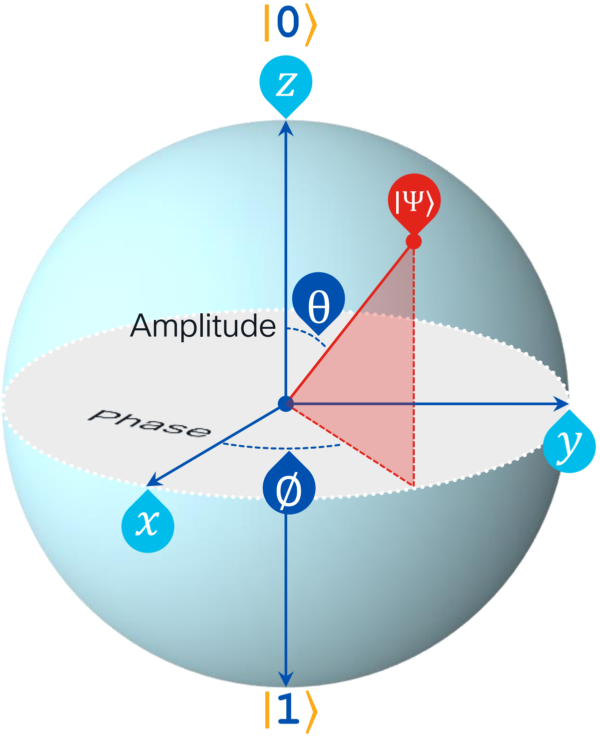
High Energy State



Quantum Gate Operation







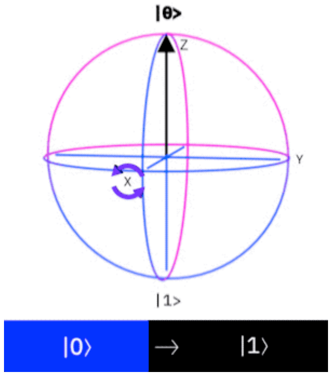
Quantum Gates :

- manipulate Amplitude θ and Phase Φ of the state vector
- take superpositions as inputs, rotate their probabilities, and produce *another* superposition as outputs

Quantum Gate Examples

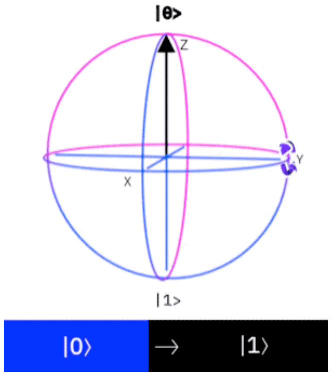
X

Pauli-X Gate is a NOT operation. It will turn a spin-up state to a spin-down and visa versa.



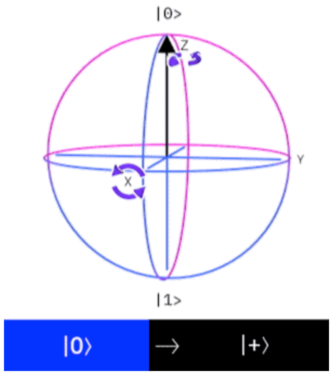
Y

Y-gate rotates around the Y-axis. It is similar to the X-gate but different in phase.



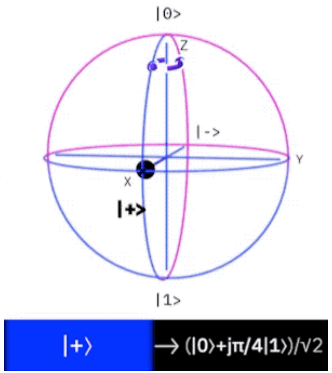
H

Hadamard Gate sets the qubit into a superposition state of a 50/50 chance that it will end up as |0> or |1>.



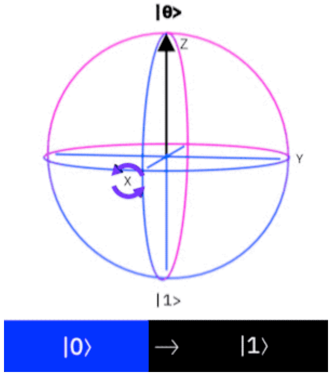
T

T gate rotates a qubit Π/4 around the z-axis.



Source: quantum.ibm.com

Quantum NOT Gate Example (Pauli-X Gate)



MATRIX

VECTOR

Row x Column

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

$$0 \; x \; 1 + 1 \; x \; 0 = 0$$

$$1 \; x \; 1 + 0 \; x \; 0 = 1$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

NOT Gate

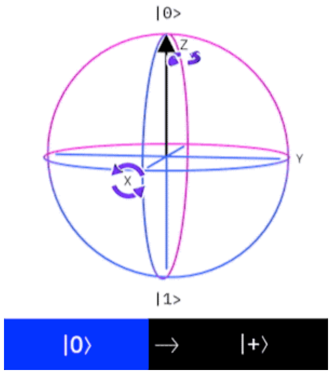
Basis State

$|0\rangle$

Basis State

$|1\rangle$

Hadamard Gate Example (Set to 50/50 State)



MATRIX | VECTOR

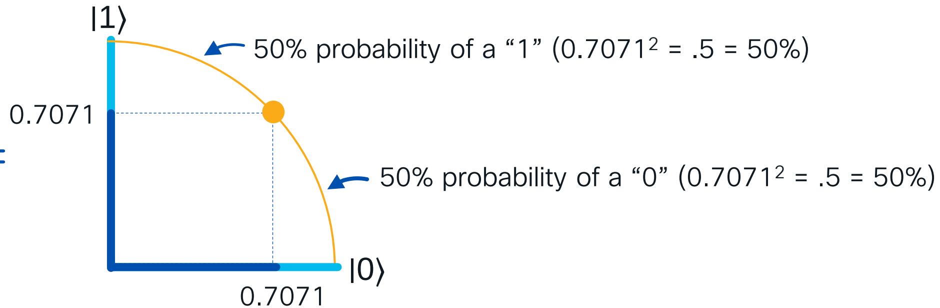
$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} .7071|0\rangle \\ .7071|1\rangle \end{bmatrix}$$

Hadamard Gate | Basis State 0 | Uniform Super Position

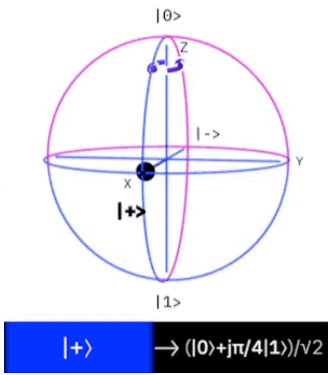
$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\psi\rangle = 0.7071|0\rangle + 0.7071|1\rangle =$$

Sums of the squares of probabilities must equal 1



T Gate Example (Rotate $\pi/4$ around the Z-axis)



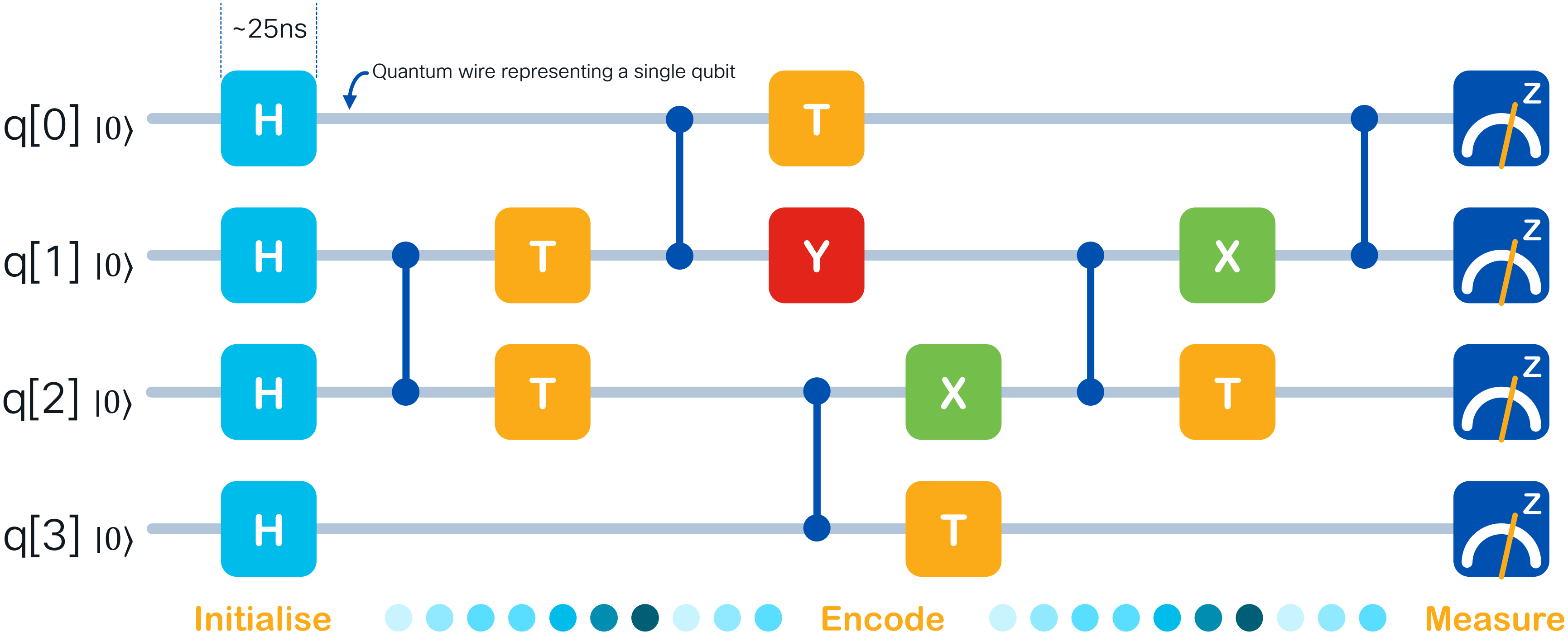
MATRIX | VECTOR

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \blacktriangleright \begin{bmatrix} \alpha|0\rangle \\ e^{i\pi/4}\beta|1\rangle \end{bmatrix}$$

T Gate | Basis State | Rotated position

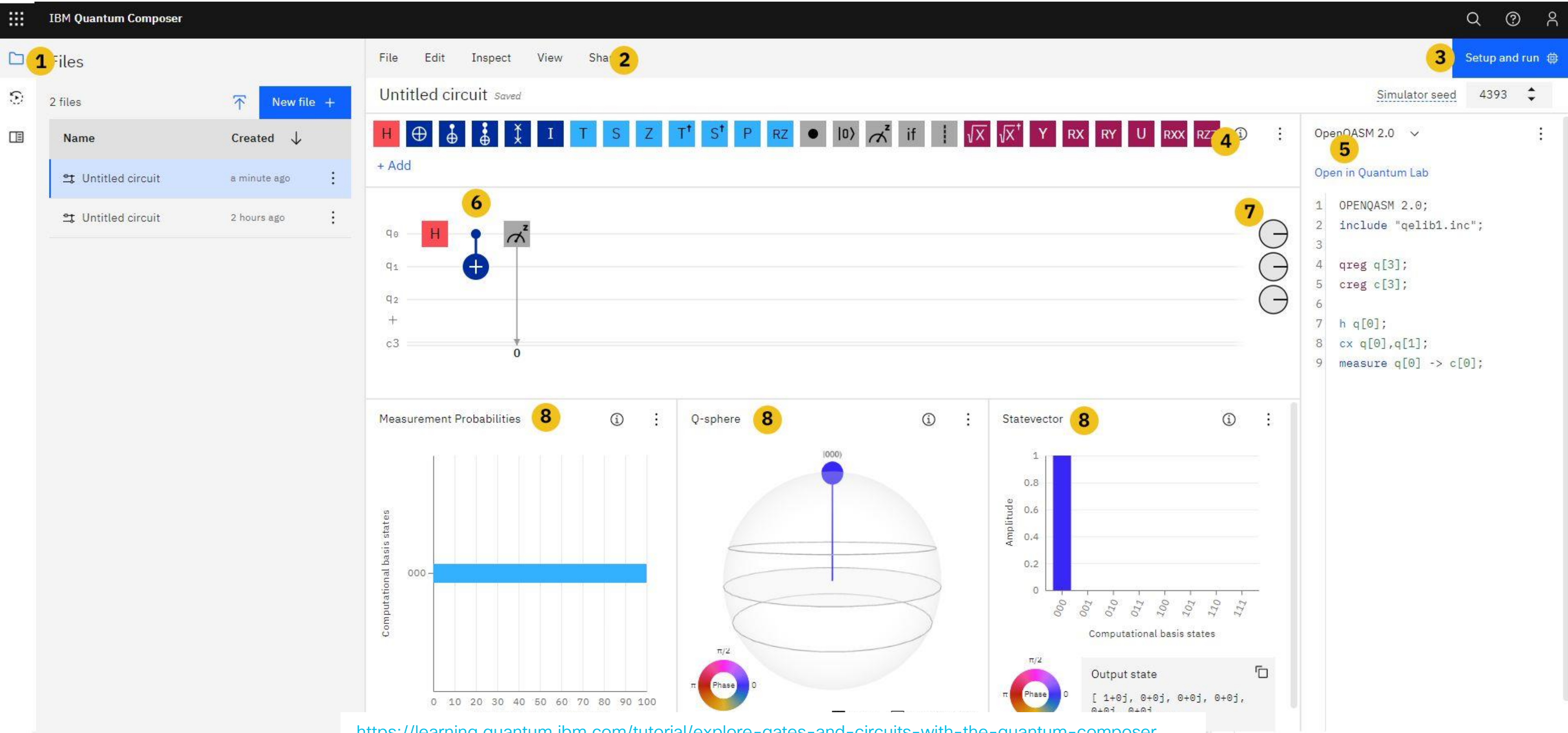
Quantum Circuits

Include Both Quantum Operators + Classical Computing



Number of input Qubits must match number of output Qubits

IBM Quantum Composer



https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer

Quantum Parallelism

QUBIT #1

Holds & operates on **values** of 0 and 1 *simultaneously*

QUBIT #1 | QUBIT #2

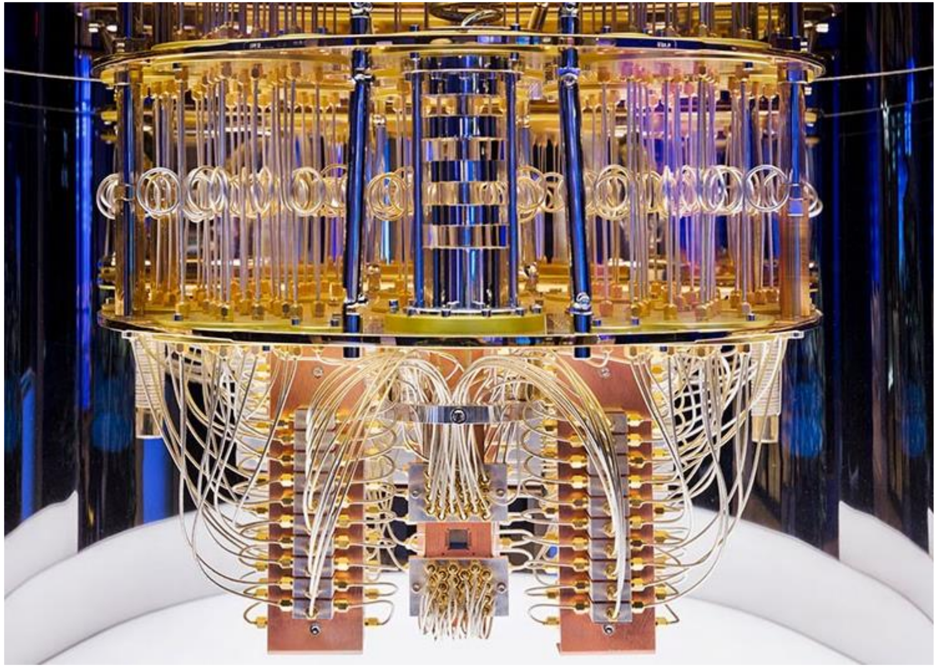
Holds & operates on **values** of 00, 01, 10, 11 *simultaneously*

QUBIT #1 | QUBIT #2 | QUBIT #3

Holds & operates on **values** of 000, 001, 010, 011, 100, 101, 110, 111 *simultaneously*

How Much Faster is a Quantum Computer?

- In 2021, the world's largest quantum computer had 127 Qubits
- This machine was 158M times faster than its classic counterpart
- Example Task Execution Times:
  - Classic Computer: 2,500 years
  - Quantum Computer: **1 minute**

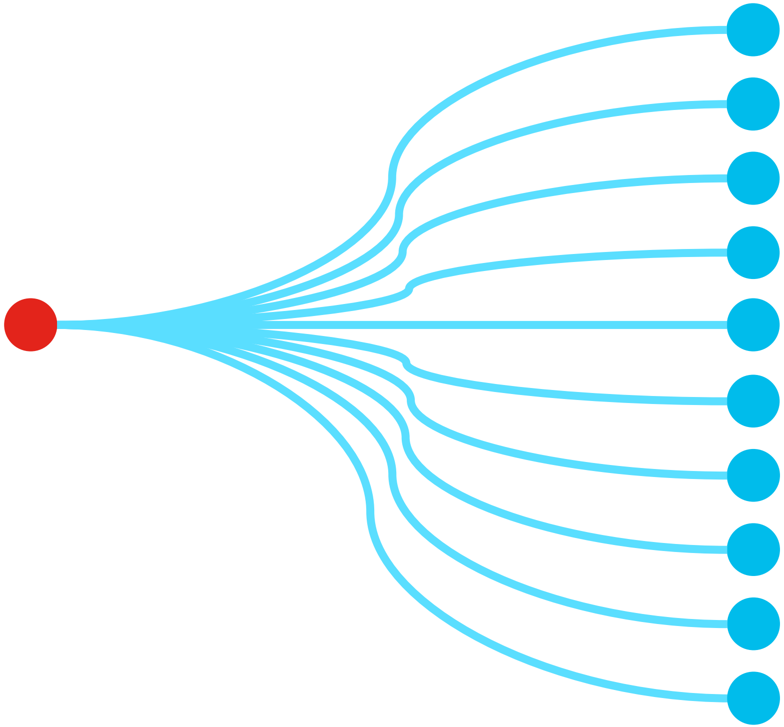


$2^{127} = 1.7 \times 10^{38}$ values

170,000,000,000,000,000,000,000,000,000,000,000,000

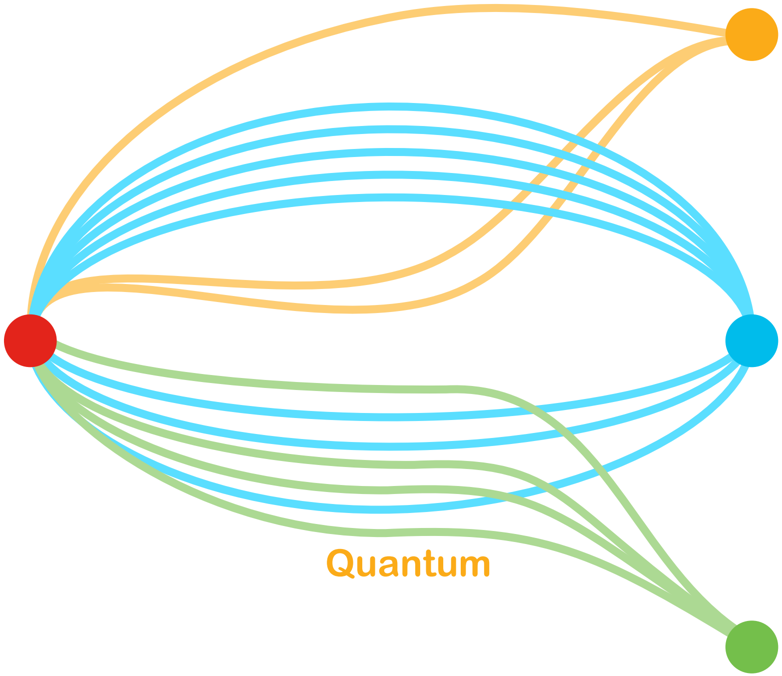
Classical Computing Problem Solving

- A classic computer needs to sequentially iterate through a problem until the correct result is found



Quantum Computing Problem Solving

- Quantum computing can provide a single or small number of answers with the highest probability of being correct, which narrows down the search for the correct solution



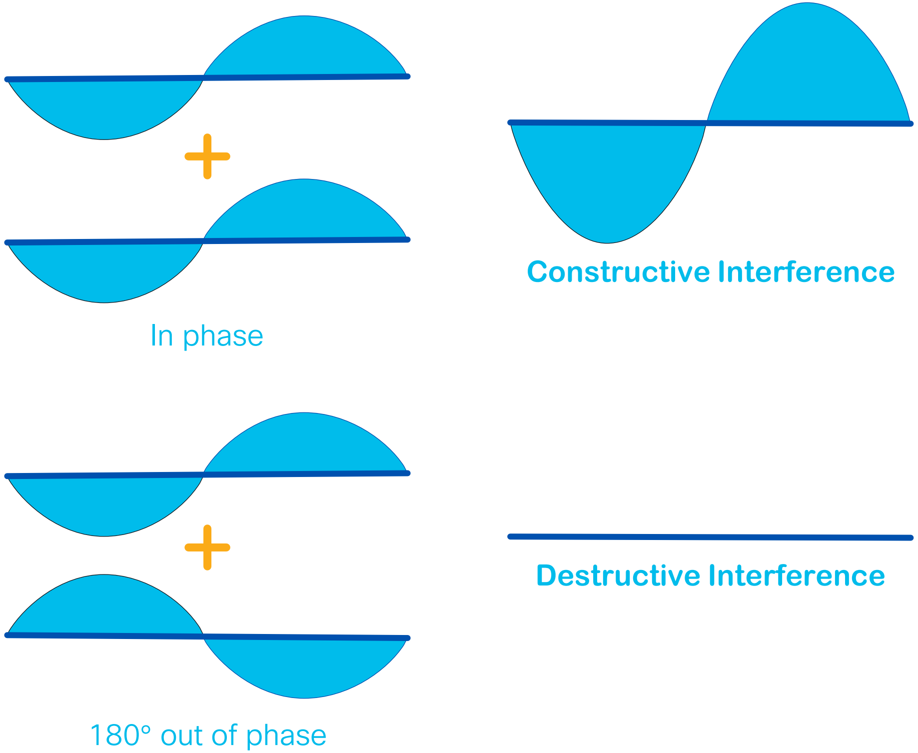
Interference Manipulation

- Another benefit that can be realized by quantum computing comes from manipulating interference
- Interference may be
  - constructive or
  - destructive
- Programmers of quantum algorithms (like Grover's and Shor's algorithms) endeavor to arrange qubits so that :
  - ***correct*** answers generate ***constructive interference***
  - ***incorrect*** answers generate ***destructive interference***
- Remember: Probability = Amplitude^2

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

Sums of the squares of probabilities must equal 1

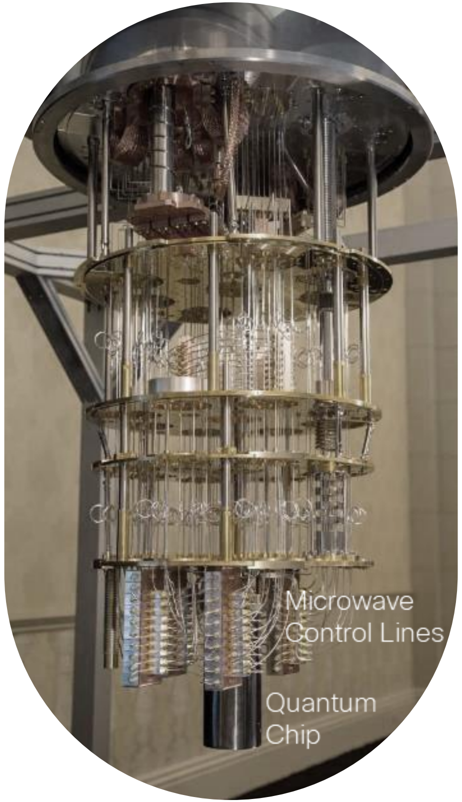
$$\alpha^2 + \beta^2 = 1$$



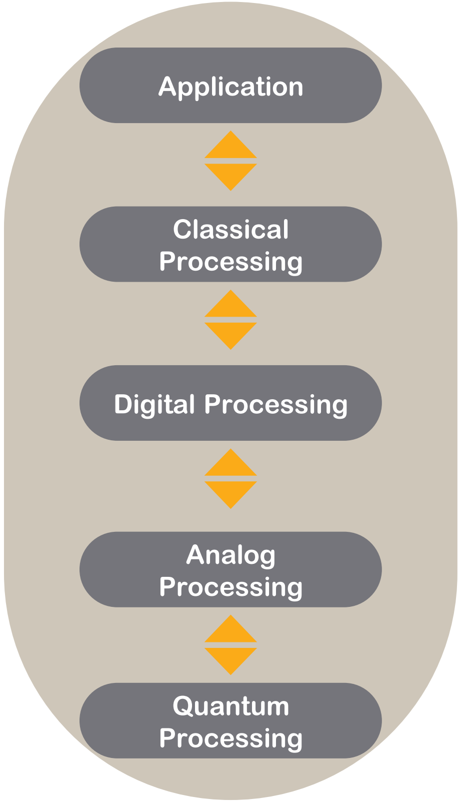
What Do Quantum Computers Look Like?

External (IBM)

External (IBM)



Internal (IBM)



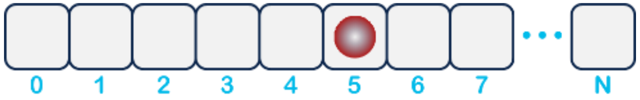
Functions

Implications of Quantum Computing on Network Security

Security-Concerning Quantum Algorithms

- Shor's Algorithm:
  - factorizes large numbers

  - with quantum compute, Shor's algorithm threatens the security of classical Public Key Infrastructure (PKI) including:
    - Diffie-Hellman (DH)
    - Elliptic Curve Cryptography (ECC), and
    - Elliptic Curve Diffie Hellman (ECDH)
  - The key exchange is at greatest risk
- Grover's Algorithm
  - searches an unstructured database (or an unordered list) for a specific result

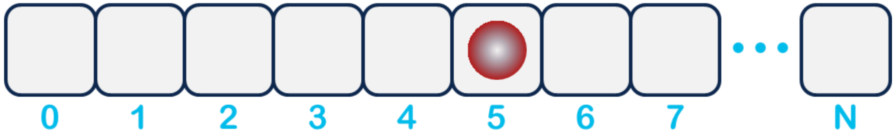


  - With quantum compute, Grover's algorithm will threaten the security of AES
  - Immediate recommendation is to increase key sizes

Y2Q, CRQC and SNDL

- **Years to Quantum (Y2Q)** refers to the unknown number of years before there is are **Cryptographically Relevant Quantum Computers (CRQC)**
- A CRQC can compute prime factorizations and discrete logarithms in polynomial time by Shor's algorithm, thereby rendering public key algorithms all but obsolete
- However, an adversary can capture network traffic *today* in the hopes of decrypting it *later* with a CRQC; this is a **Store Now, Decrypt Later (SNDL)** type of attack, and means that sensitive data is vulnerable *right now* to future quantum threats
  - Sometimes this method is also referred to as **Harvest Now Decrypt Later** (HNDL)

Grover’s Algorithm: Classic vs. Quantum



Classic Search

$f(\text{"}red\ ball\text{"})$ ▶ “Position 5”

Worst Case: $N\ searches$

Quantum Search

$f(\text{"}Pos\ 2?\text{"})$ ▶ “False”

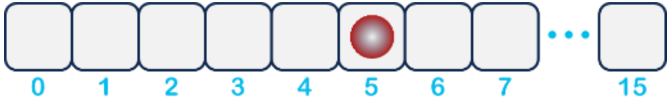
⋮

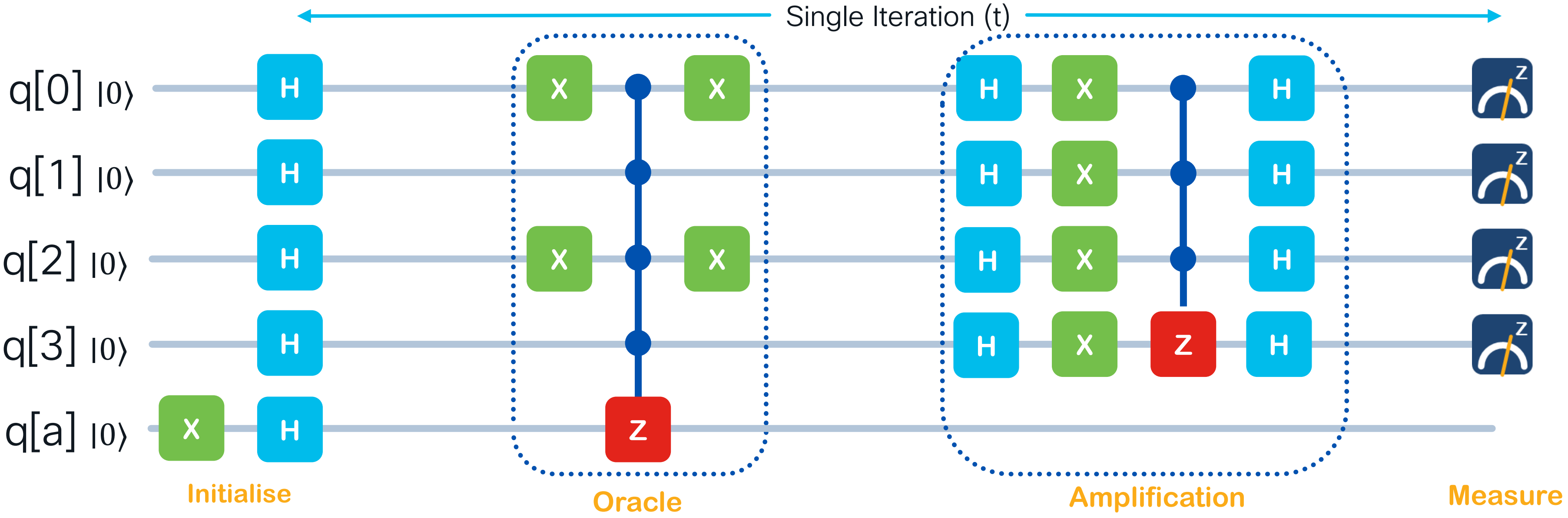
$f(\text{"}Pos\ 5?\text{"})$ ▶ “True”

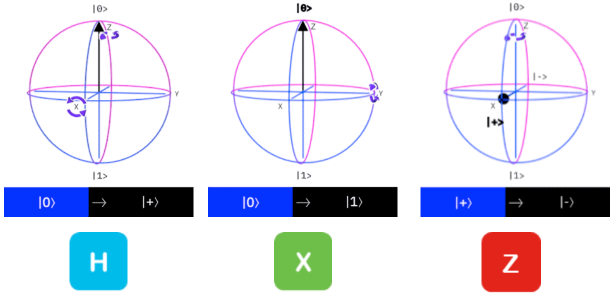
Worst Case: $\sqrt{N}\ searches$

- Grover’s algorithm uses amplitude amplification to return the correct result with high probability
- As such, with quantum parallelism and interference management, Grover’s algorithm becomes quadratically faster than a classical algorithm

Grover Quantum Circuit







https://www.techscience.com/jqc/v3n4/46224/pdf

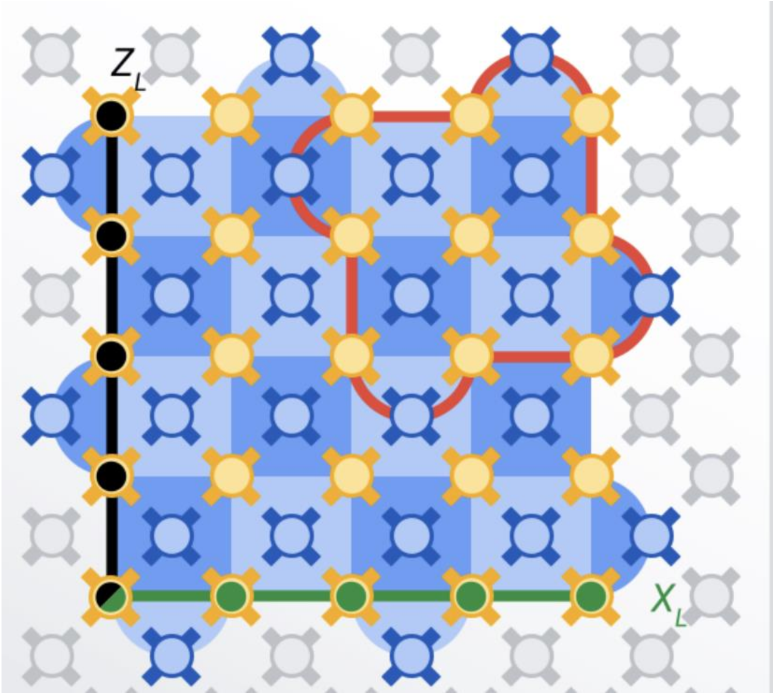
How many Qubits are required to Break RSA and AES?

- Experts estimate that:
  - RSA-2048 requires a quantum computer with 4,096 **logically-corrected qubits** to be broken
  - AES-256 requires a quantum computer with 6,681 **logically-corrected qubits** to be broken

https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

How Many Physical Qubits are Required to Produce a Logically-Corrected Qubit?

- Qubits are notoriously fragile and extremely sensitive to the environment and can easily lose coherence (state)
- The logical state of a qubit can be spread over many physical qubits to achieve **Quantum Error Correction**
- In March 2023, Google realized a logically-corrected qubit with just 49 physical qubits
- In December 2023, Harvard scientists achieved the same with just 48 qubits



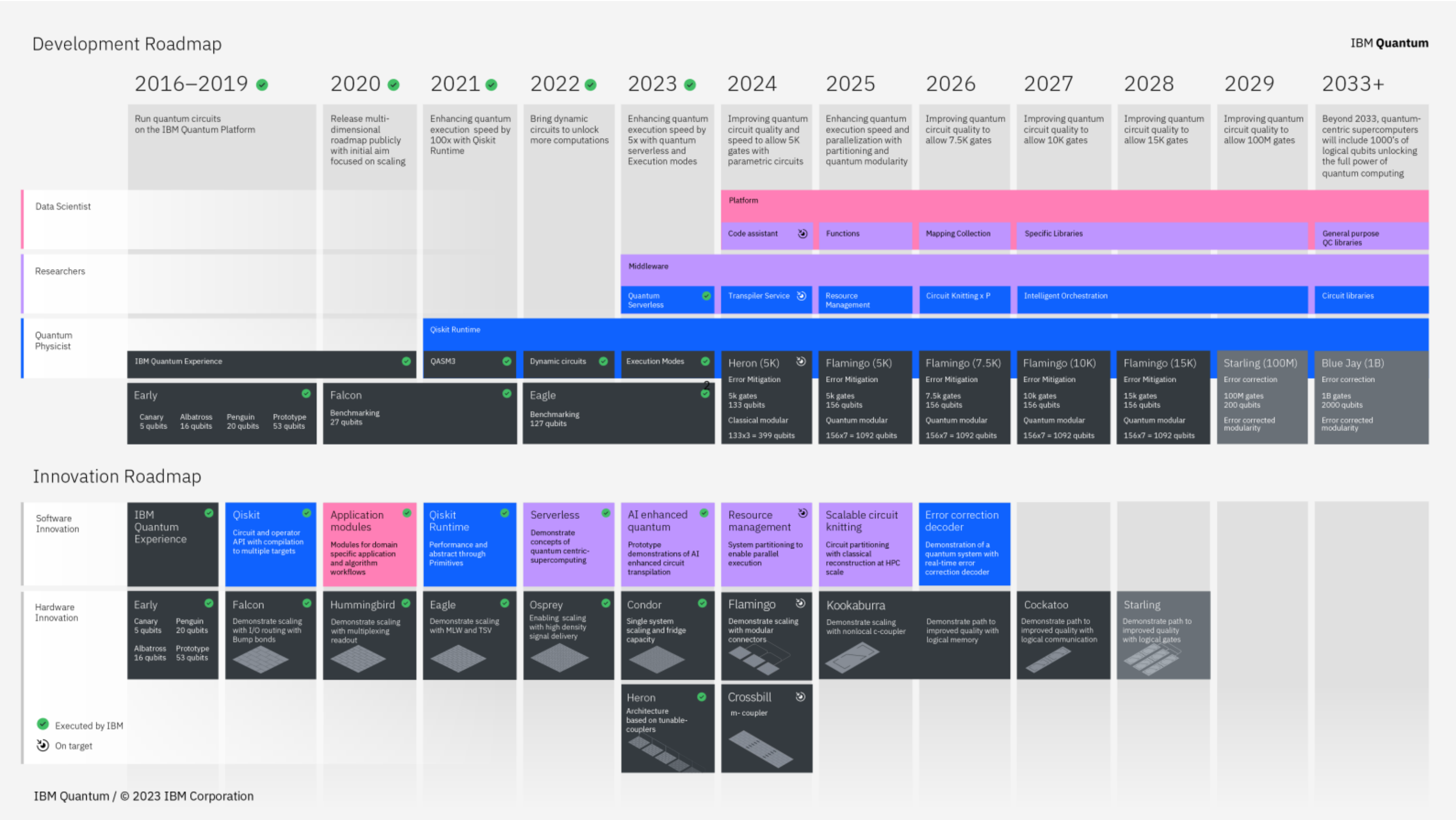
https://blog.google/inside-google/message-ceo/our-progress-toward-quantum-error-correction/
https://thequantumrecord.com/quantum-computing/breakthrough-in-quantum-error-correction/

So, really…
How many Qubits are required to Break RSA and AES?

- Let's assume 50 physical qubits for one logically-corrected qubit
- Experts estimate that:
  - RSA-2048 requires a quantum computer with 4,096 logically-corrected qubits to be broken
    - (4096 * ~50) 200,800 physical qubits
  - AES-256 requires a quantum computer with 6,681 logically-corrected qubits to be broken
    - (6681 * 334,050) 334,050 physical qubits
- But remember:
  - Quantum computers are *increasing* in size, while
  - Quantum Error Correction circuits are *decreasing* in size

https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

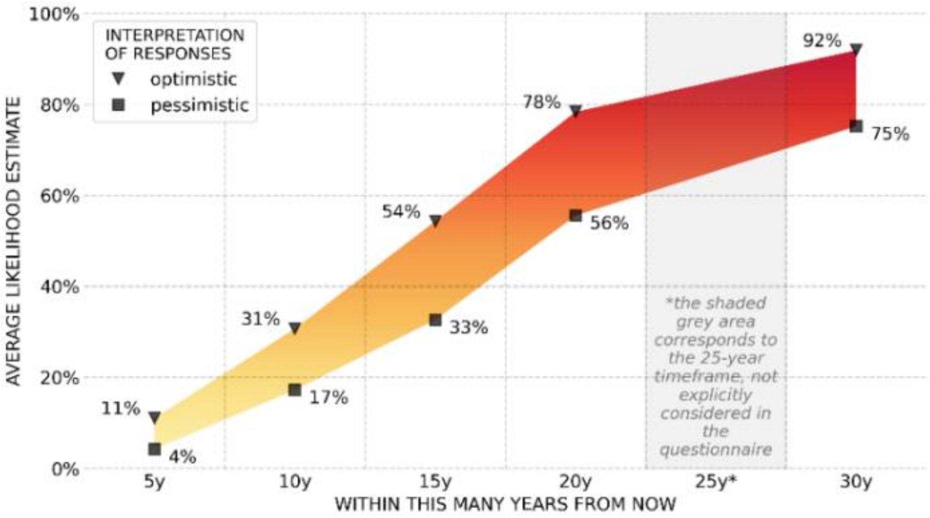
How Far Off Is That?



https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

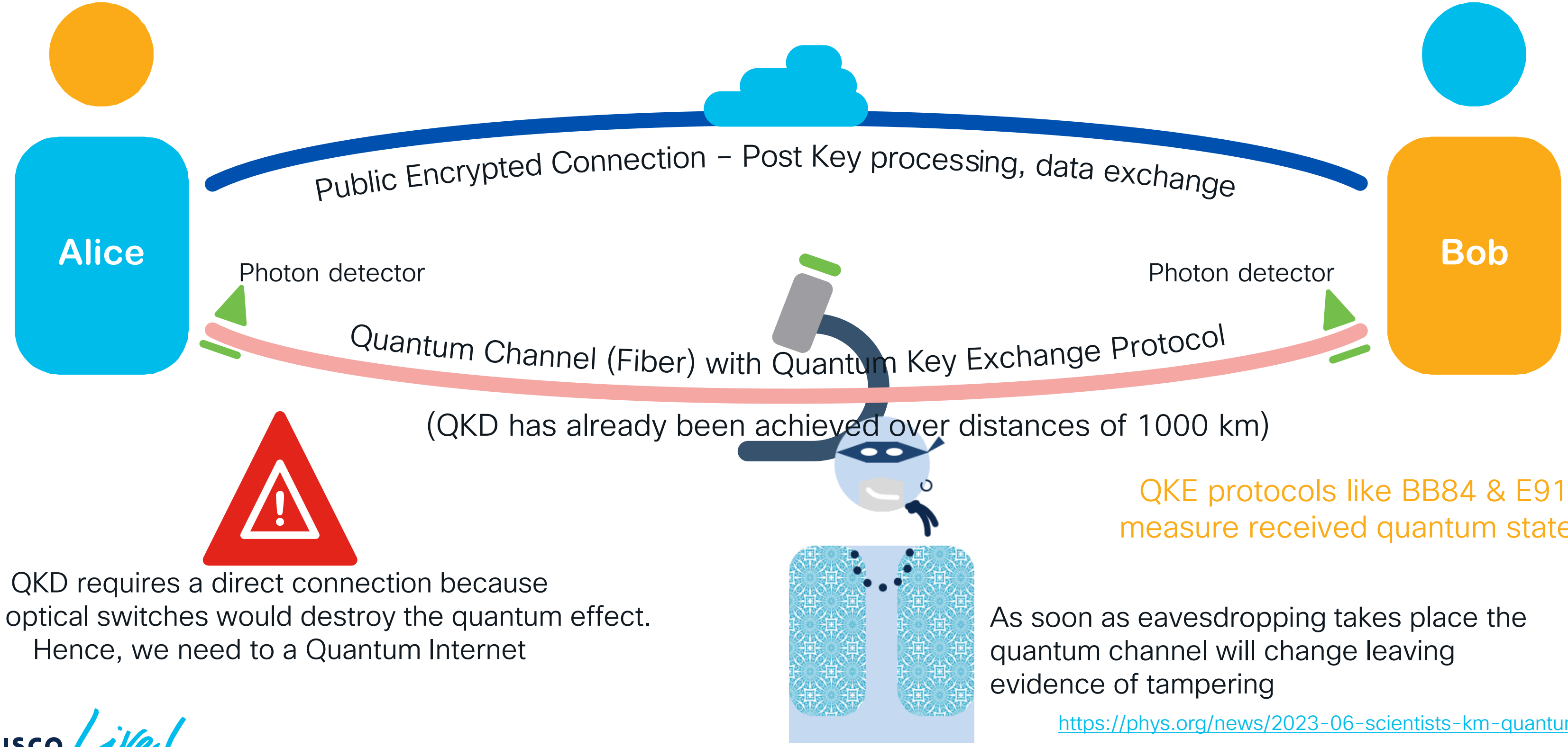
How Many Y2Q?

- Cloud Security Alliance:
  - April 14, 2030
- Global Risk Institute:
  - ~50% of experts predict 15 years
- White House / NIST
  - “in the not-too-distant future”



https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum/
https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

Quantum Key Distribution (QKD)



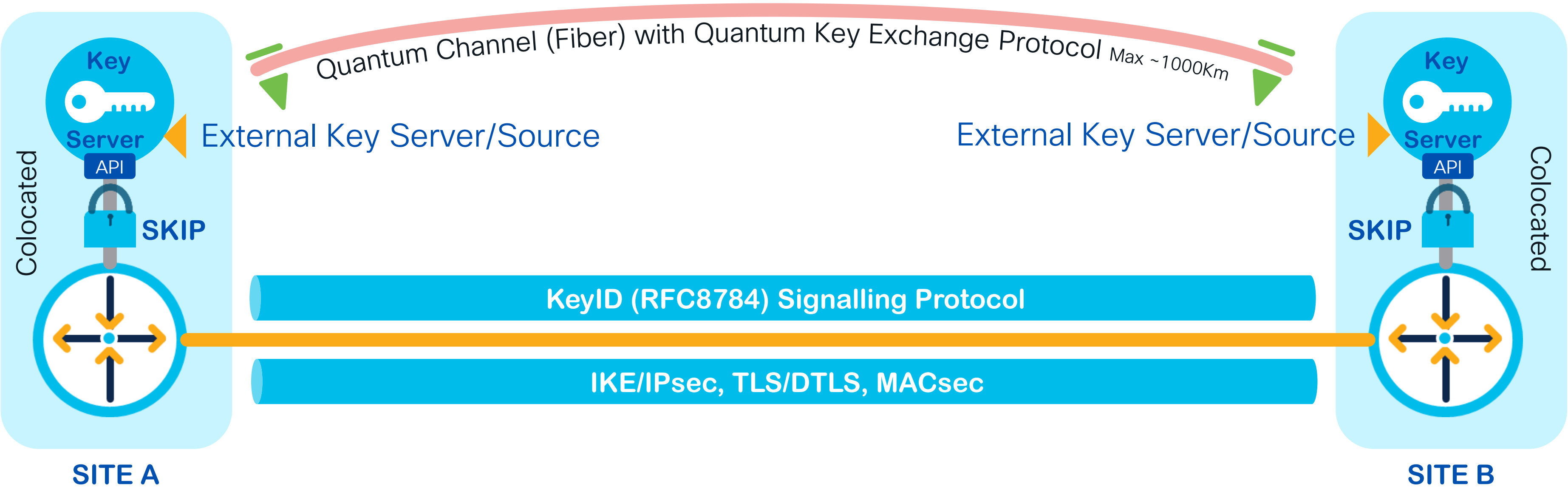
QKD requires a direct connection because
current optical switches would destroy the quantum effect.
Hence, we need to a Quantum Internet

QKE protocols like BB84 & E91
measure received quantum states

As soon as eavesdropping takes place the
quantum channel will change leaving
evidence of tampering

https://phys.org/news/2023-06-scientists-km-quantum-key.html

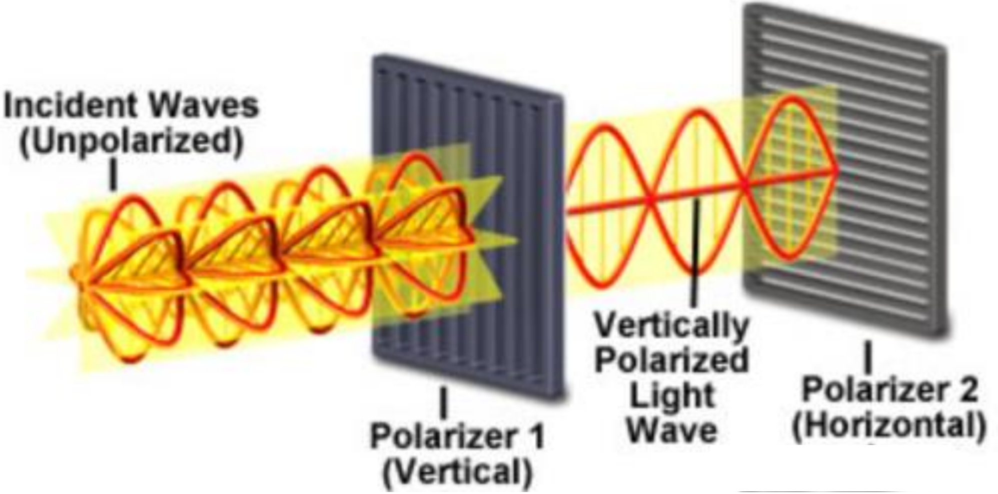
Secure Key Import Protocol (SKIP)



An Introduction to Quantum Networking

Photonic Qubits

- Photons can represent Qubits, as well as electrons
- Photons are more conducive to quantum networking than electrons
  - electrons are more conducive to computing
- The logical states of 0 or 1 are not determined by the spin of photons, but rather by their polarization
  - Horizontal Polarization |1⟩
  - Vertical Polarization |0⟩

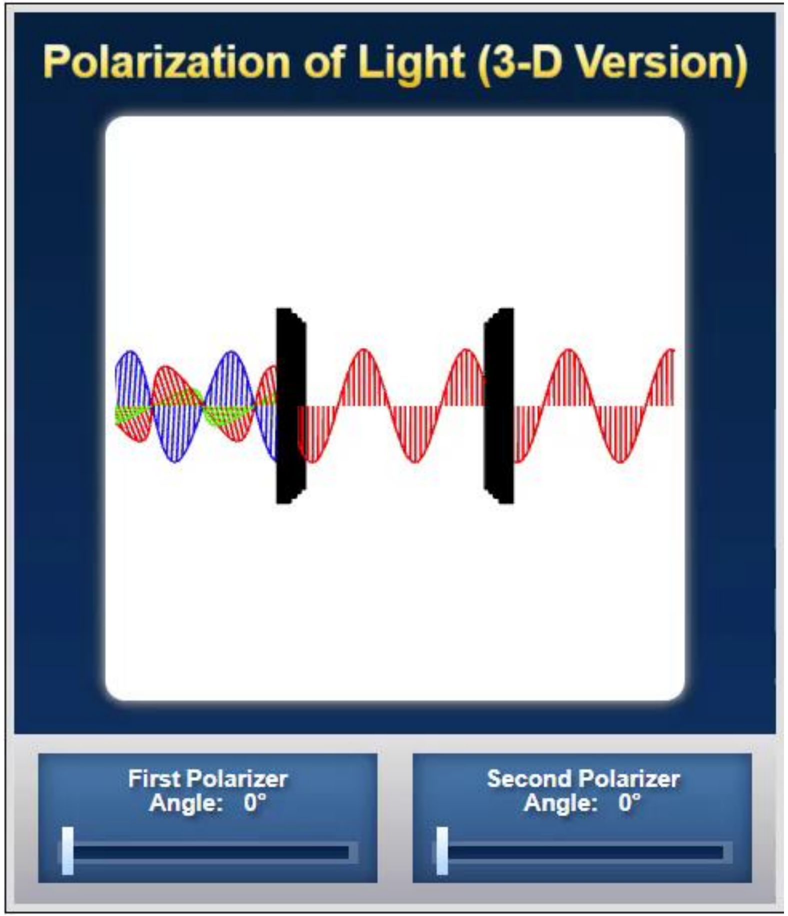


What Happens When Two Waves Intersect?

- When two waves intersect, the resulting displacement of the medium at any location is the *algebraic sum* of the displacements of the individual waves at that same location
- Therefore, another algebraic operation (specifically, a subtraction) can completely reverse the effects of the intersection

Photonic Qubits

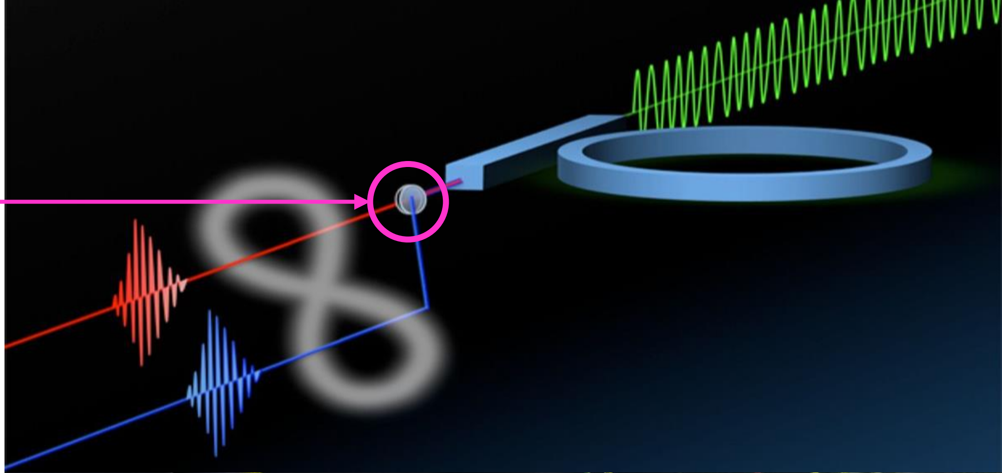
- Photons can represent Qubits, as well as electrons
- Photons are more conducive to quantum networking than electrons (which are more conducive to computing)
- Logical states of 0 or 1 are not determined by spin, but rather by polarization
  - Horizontal Polarization |1⟩
  - Vertical Polarization |0⟩

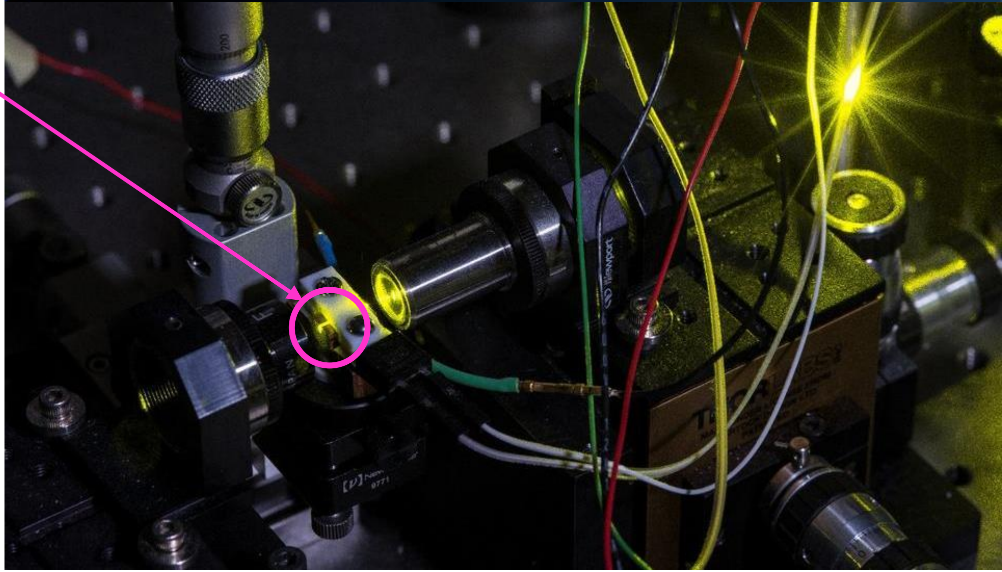


https://www.olympus-lifescience.com/en/microscope-resource/primer/java/polarizedlight/3dpolarized/

How Are Photons Entangled?

- The most common approach to generate entangled photons is via **Spontaneous Parametric Down-Conversion** (SPDC) in nonlinear crystals
- SPDC is an instant optical process that converts one photon of higher energy into a pair of photons of lower energy





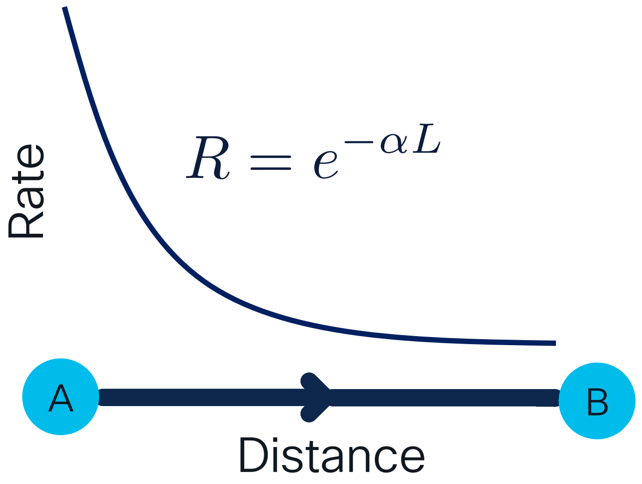
https://www.nature.com/articles/s41377-021-00537-2
https://spectrum.ieee.org/entanglement-on-a-chip
https://www.nist.gov/image/non-linear-crystal

Classical Optical Communication

Quantum Communication via Transporting

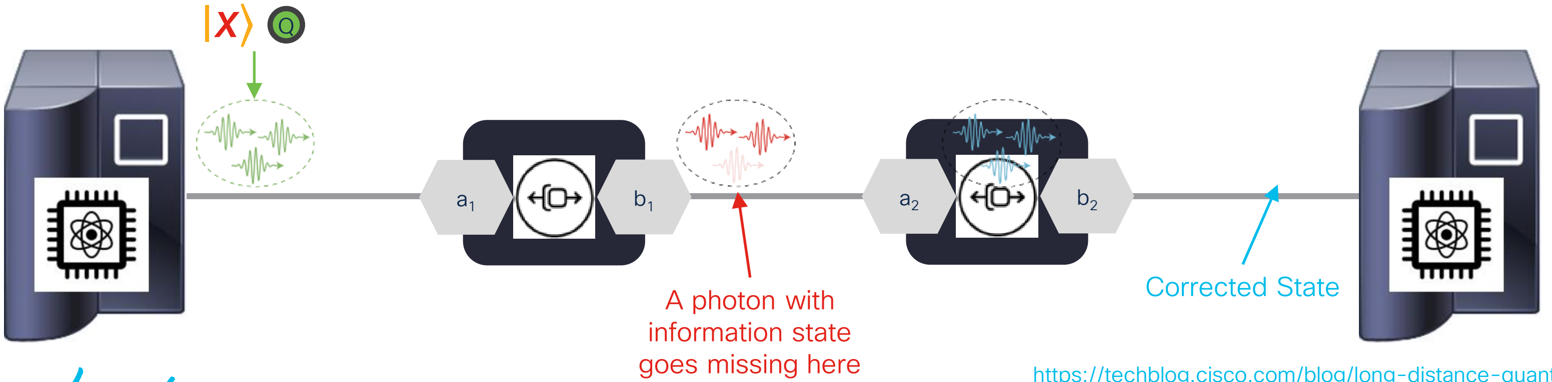
Primary Challenge to Quantum Transport

- Rate decays exponentially with distance
- Can we amplify the signal?
  - No, because of the No Cloning Theorem



(One-Way) Quantum Repeaters

- Quantum Repeaters leverage Quantum Error Correction, where encoded quantum information is transmitted in the form of multi-photon states
  - Parity information is included in the multi-photon state
- Intermediate repeater stations check the incoming state for errors and prepare a fresh encoded qubit as the output to be sent to the next repeater
- This does NOT violate the No Cloning Theorem, as quantum repeaters perform a multi-qubit measurement that does not disturb the quantum information in the encoded state, but rather, retrieves indirect information about a potential error



https://techblog.cisco.com/blog/long-distance-quantum-communication

(Two-Way) Quantum Communication via Teleporting

Initial State

Quantum Communication via Teleporting

Step 1: Entangle a Pair of Photons and Send One to the Receiver

Quantum Communication via Teleporting

Step 2: Perform Another Entanglement Operation at the Sender

Note: This step results in a teleportation of the *combination* of the states of qubits Q and A to qubit B

Quantum Communication via Teleporting

Step 3: Perform a Bell State Measurement at the Sender

Note: $\otimes$ is a mathematical notation for a tensor product; that is, a product of two quantum states, $|\psi\rangle$ and $|\Phi\rangle$

Note: The Bell State Measurement simultaneously:
- breaks the three-way entanglement,
- collapses the superpositions of qubits Q and A, and
- produces a result of 1 of 4 Bell States

The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00

$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01

$|\psi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10

$|\psi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11

Quantum Communication via Teleporting

Step 4: Send the Bell State Measurement Result over a Classical Channel

The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00

$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01

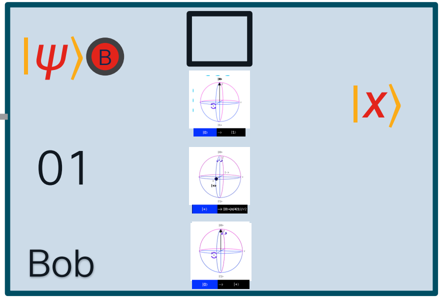
$|\psi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10

$|\psi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11

Quantum Communication via Teleporting

Step 5: Perform a Correction Operation on the Received Qubit (if necessary)

Note: $|x\rangle$ represents the original state of the qubit, which has now been received in its corrected form



The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00 → nothing to correct

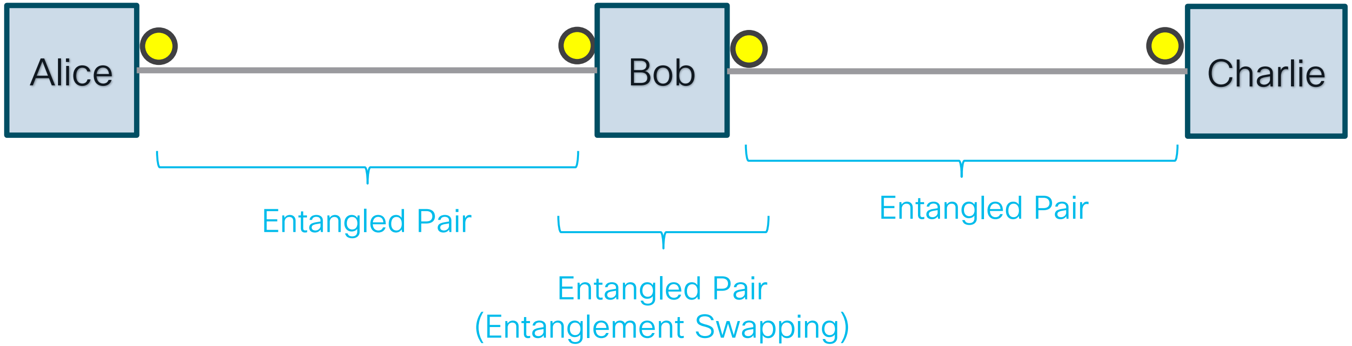
$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01 → correct x (only)

$|\psi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10 → correct z (only)

$|\psi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11 → correct (x and z)

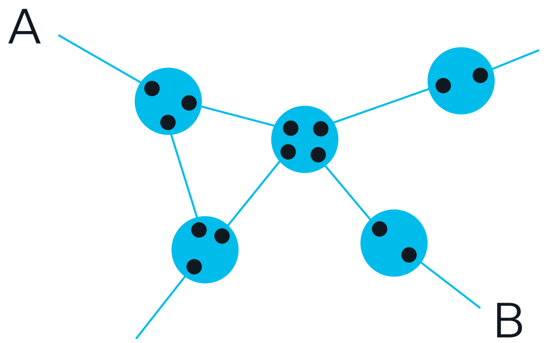
Refer to Bloch Sphere diagram for x,y and z axis

Extending Quantum Teleporting



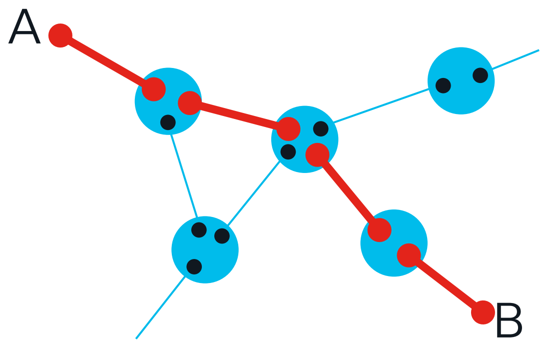
Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



Quantum Routers & Protocols

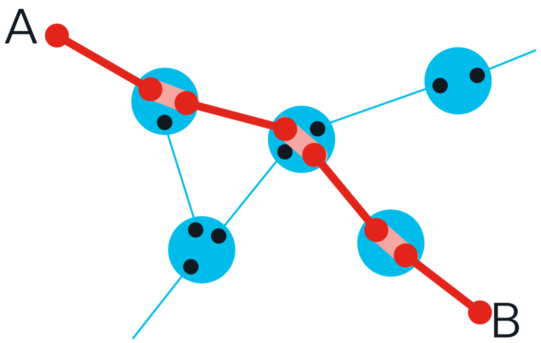
Two-Way Entanglement Distribution Network Example



Elementary link entanglement

Quantum Routers & Protocols

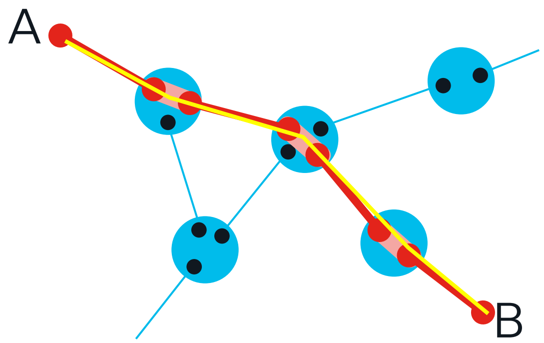
Two-Way Entanglement Distribution Network Example



Elementary swapping

Quantum Routers & Protocols

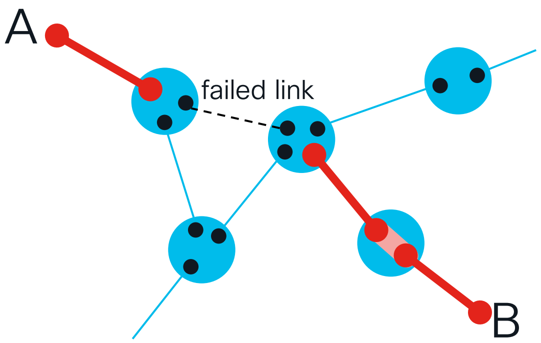
Two-Way Entanglement Distribution Network Example



End-to-end entanglement

Quantum Routers & Protocols

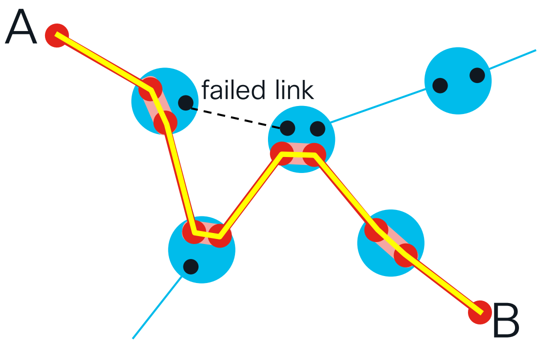
Two-Way Entanglement Distribution Network Example



Network failure event

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example

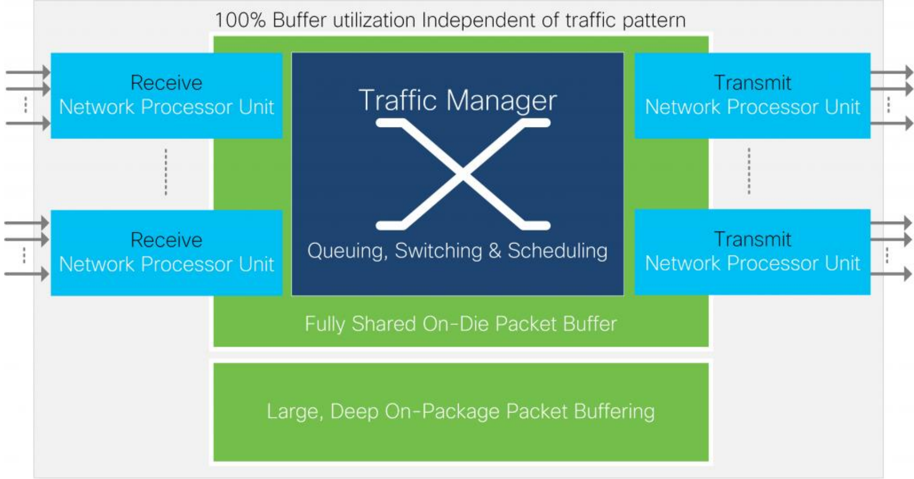


Reestablishing end-to-end entanglement

The Key Role of Memory in a Network Switch

- A major component of any network switch is memory
- Memory enables:
  - Ingress buffering and queuing
  - Switching
  - Egress buffering and queuing

Cisco Silicon One ASIC Architecture

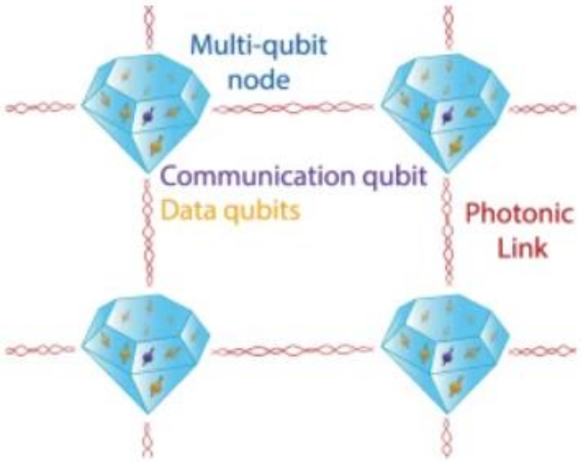


(everything shaded green represents memory)

Note: Cisco Silicon One is **NOT** an ASIC for a quantum switch, but rather is only being used as an example to illustrate how extensive memory is within switching architectures

Quantum Memory Methods and Storage Times

- Optical Quantum Memory
  - milliseconds to seconds.
- Superconducting Qubits
  - microseconds to milliseconds.
- Trapped Ions
  - seconds to minutes
- Note: techniques such as Quantum Error Correction may be employed to extend the effective storage times



An Example of Optical Quantum Memory Using Engineered Diamonds
https://www.nature.com/articles/s41534-022-00637-w

Quantum Networking Challenges by OSI Layer

Application	Cryptography, privacy-preserving computing, enhanced sensing, …
Transport	End-to-end (logical) quantum information transmission
Network Link Physical	Routing, Scheduling Quantum circuit switching Error correction, Purification Transporting/Teleporting qubits Photon loss, channel noise, hardware noise

What is Cisco doing?

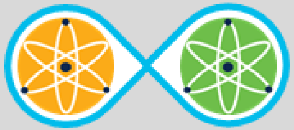
Key Engineering Challenges in Quantum Computing & Networking

1180

Developing Larger Quantum Computers
Current Record: 1180 qubits

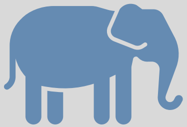
Achieving Longer Quantum Coherence
Current Record: 343 ms

Requiring Fewer Qubits for Error Correction
Current Record: 48

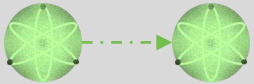


Extending Entanglement
Current Record: 248 km

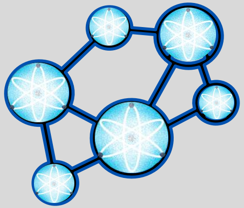
Raising Operating Temperatures



Achieving Longer Quantum Memory



Improving Quantum Transmission Fidelity



Planning & Modelling Quantum Networks

Developing Quantum Network Protocols

Lowering Costs

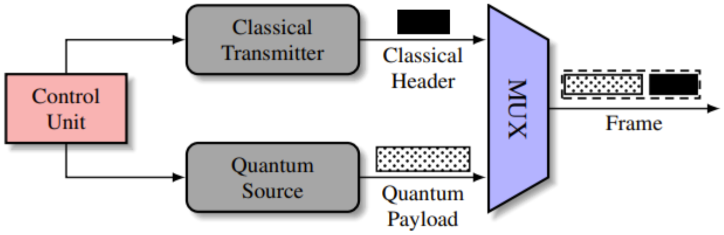
Steps to Building a Quantum Internet

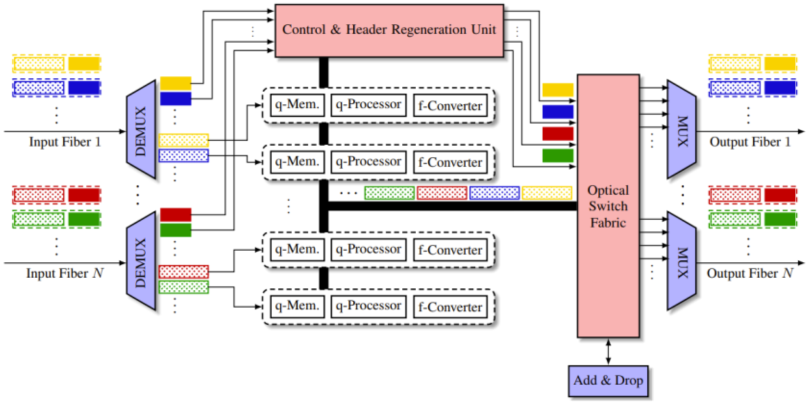
1) Research & Mathematical Modelling
2) Quantum Simulation
3) Lab testing

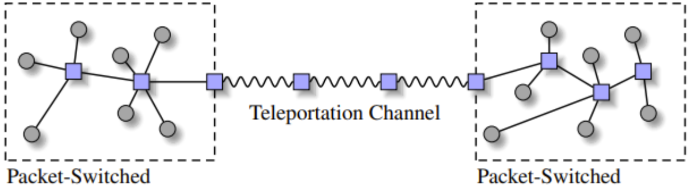
Modelling a Unified Classical & Quantum Internet

Research

- “We are now with Quantum Internet where we were with the classical Internet in the 1960s”
- The Cisco Research team has published a paper on how can we design a network that can serve thousands and eventually millions of end nodes





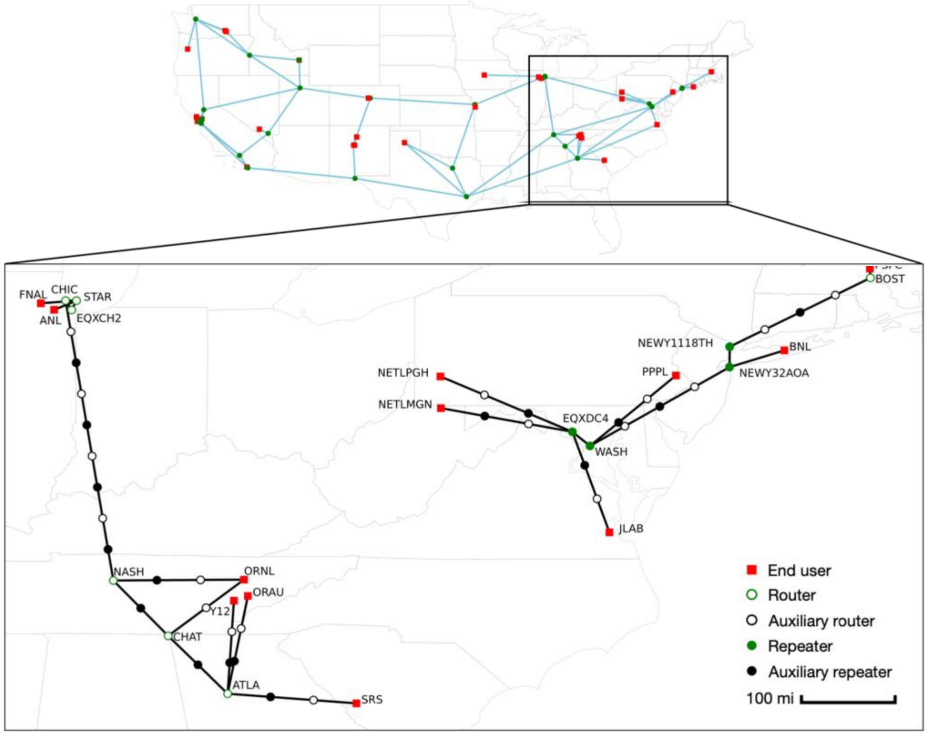


https://outshift.cisco.com/blog/making-a-quantum-ready-internet
https://arxiv.org/abs/2205.07507

Planning Quantum Networks Over Existing Fiber Networks

Research

- In another paper, the Cisco Research team developed a framework to guide the first steps of planning a quantum network using the existing optical network infrastructure
- This framework was formulated as an optimization problem
  - Specifically as an Integer Linear Programming (ILP) problem

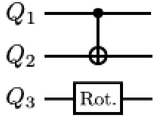


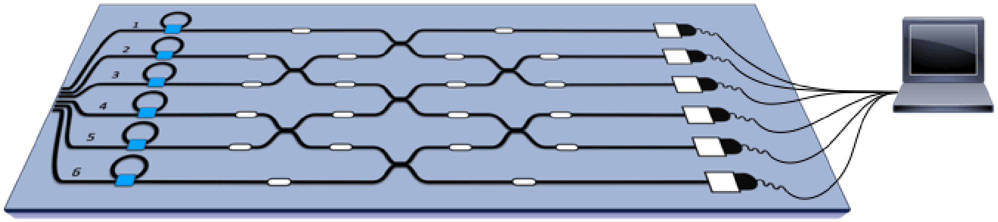
https://outshift.cisco.com/blog/first-steps-to-quantum-network-planning
https://arxiv.org/abs/2308.16264

Photonic Quantum Processors

Research

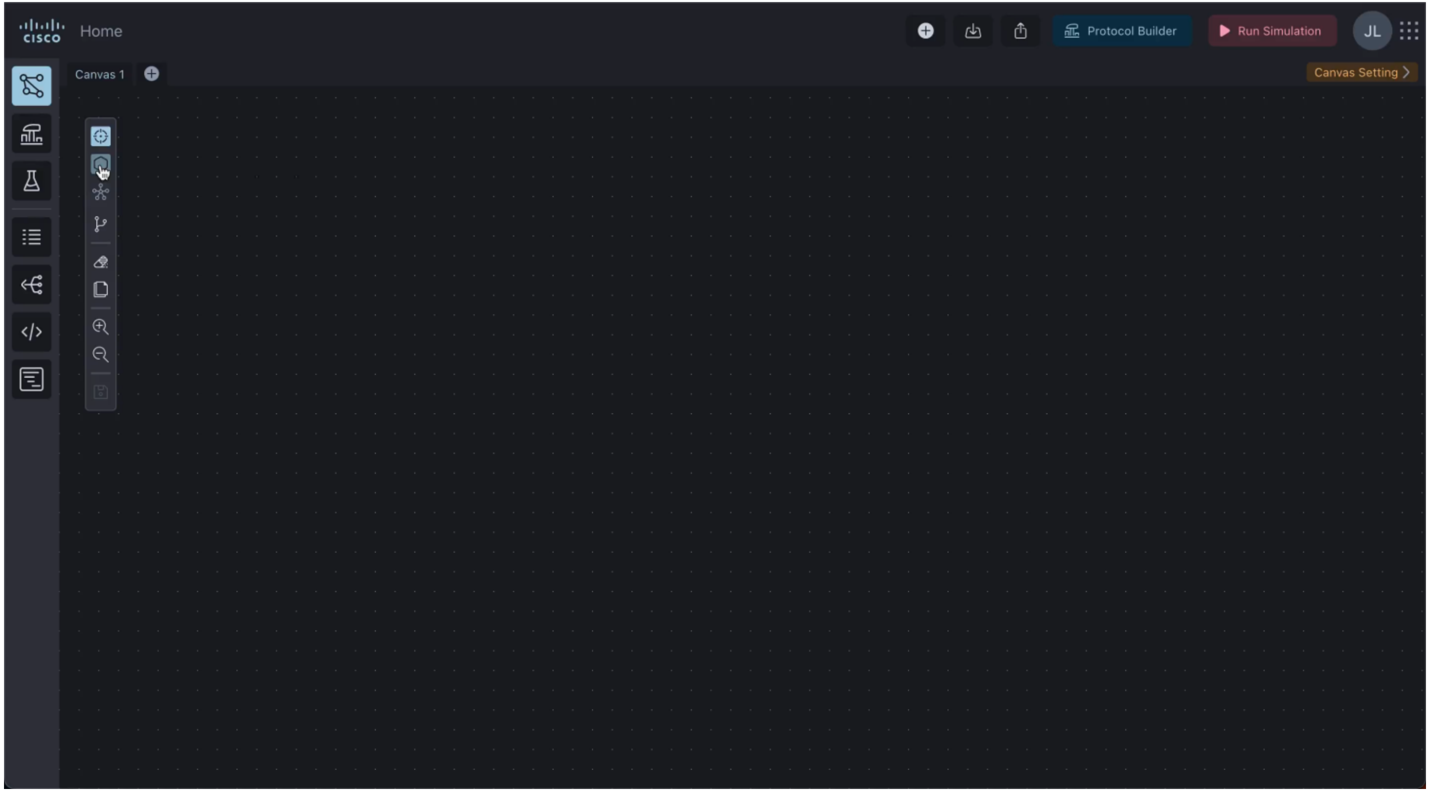
- Quantum photonics emerges as a promising platform for scalable quantum information processing
  - possibly at room temperature
- These directly enable quantum networking
  - by serving as a repeater for quantum error correction, or
  - as a server for distributed quantum computing resources





https://outshift.cisco.com/blog/how-powerful-are-photonic-quantum-processors

Quantum Network Design Kit (QDNK) Simulator

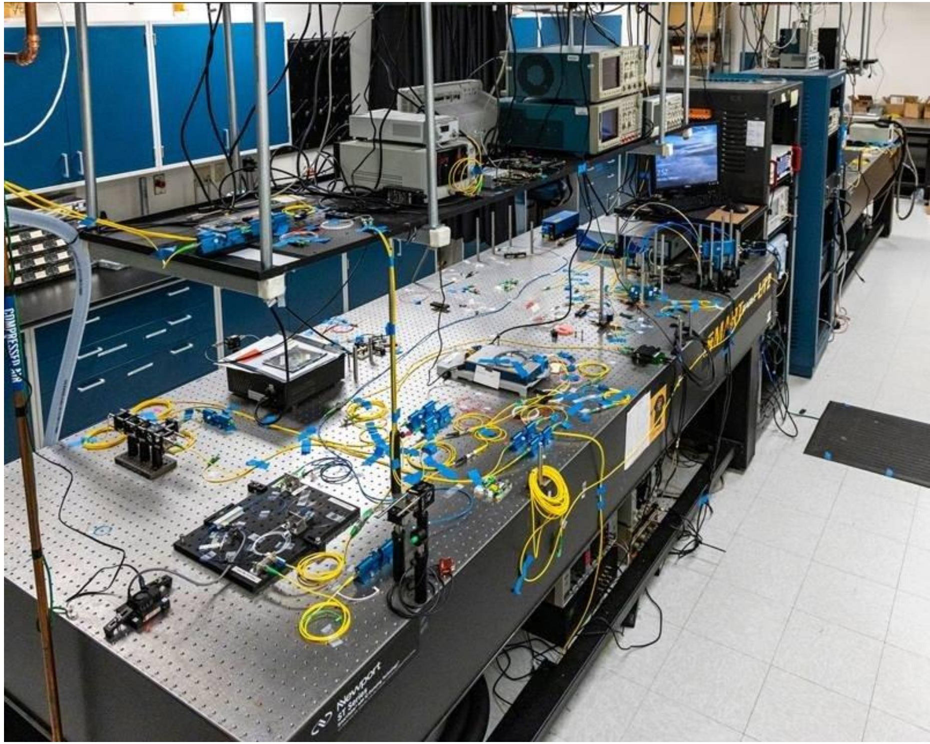


https://research.cisco.com/research-projects/qnet-lab

Cisco Quantum Research Lab

Testing

- Cisco announced the opening of a Quantum Research Lab in March 2023 in Santa Monica, CA



https://outshift.cisco.com/blog/quantum-research-lab-announcement

Summary & Next Steps

Pre-Session Quiz

1) What are some use-cases for quantum networks?
2) What are some of the special properties of quantum bits (Qubits)?
3) What makes a quantum computer so fast?
4) What is Y2Q? And when do most experts expect it?
5) Can you transmit information faster than light with quantum teleporting?
6) Will quantum networks replace classical networks?
7) What is Cisco researching and developing in Quantum?

Post Session Quiz / Summary

1) What are some use-cases for quantum networks?

Quantum Cryptography

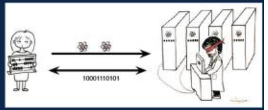
- Quantum networks can be used to securely exchange cryptographic keys, as these are mathematically proven to detect and prevent eavesdropping
- The most well-known method of this application is *Quantum Key Distribution (QKD)*

Distributed Quantum Computing

- Interconnecting geographically-dispersed quantum computers to realize benefits such as:
  - Increased Processing Power
  - Distributed Quantum Computing
  - Specialized Quantum Modules
  - Fault Tolerance
  - Hybrid Quantum-Classical Systems
  - Etc.

Blind Quantum Computing

- A privacy-preserving method in which a client can delegate a computation task to remote quantum computer(s) without disclosing the source data or algorithms
- The results of the computations would likewise be private



Network Clock Synchronization

- A world-wide set of high-precision clocks connected by quantum networks could achieve ultra precise clock signals
- Current accuracy: ≤ 30 ns
- Quantum accuracy: ≤1ps

https://www.gps.gov/systems/gps/performance/accuracy/
https://ieeexplore.ieee.org/document/9856607

Distributed Sensing

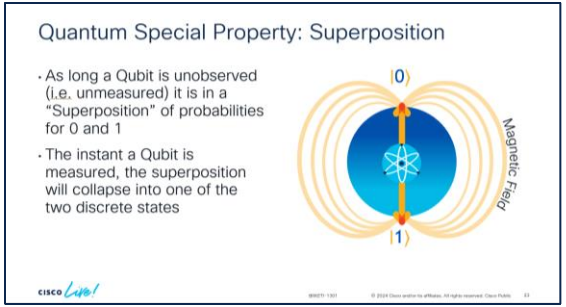
- Signals from distributed sensors can be combined via quantum networks to obtain higher-accuracy measurements than currently possible with classical network interconnections
- E.g. Telescope Array
  - Classical precision: $\pm 1/\sqrt{N}$
  - Quantum precision: $\pm 1/N$

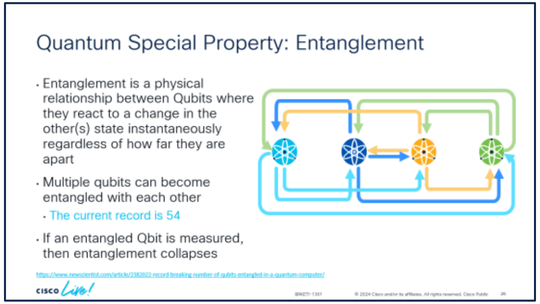
Quantum Money

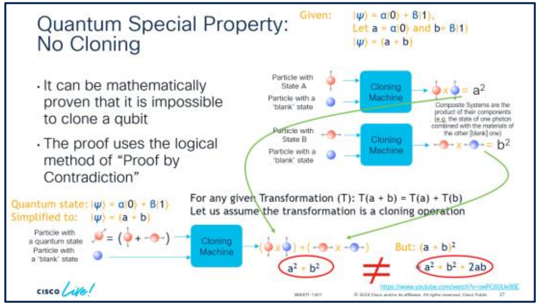
- The main security requirement of money is unforgeability
- A quantum money scheme aims to fulfill by this requirement by exploiting the no-cloning property of the unknown quantum states

Post Session Quiz / Summary

2) What are some of the special properties of quantum bits (Qubits)?

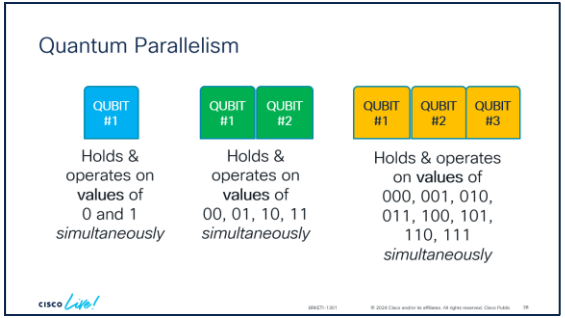


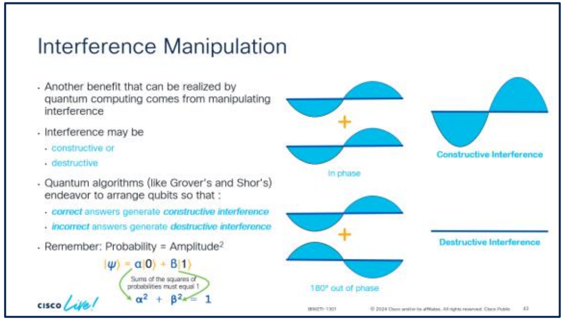




Post Session Quiz / Summary

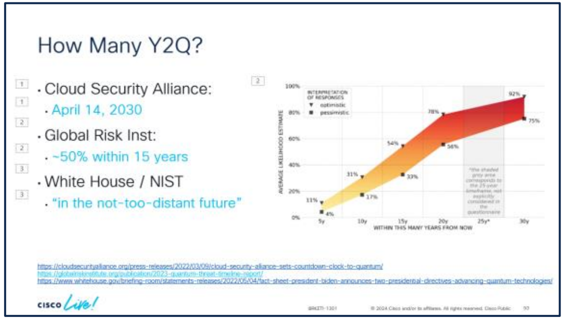
3) What makes a quantum computer so fast?





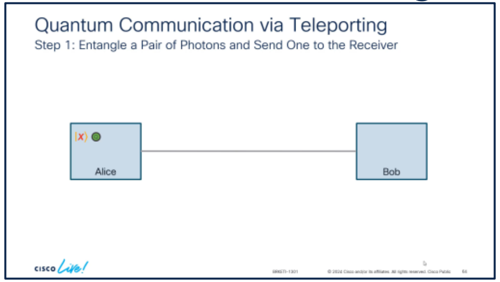
Post Session Quiz / Summary

4) What is Y2Q? And when do most experts expect it?

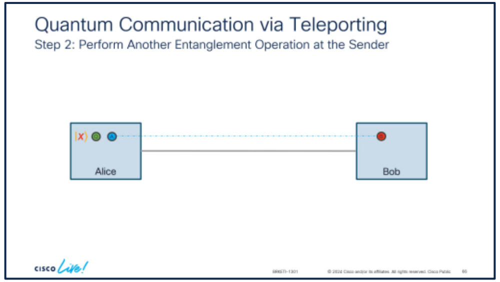


Post Session Quiz / Summary

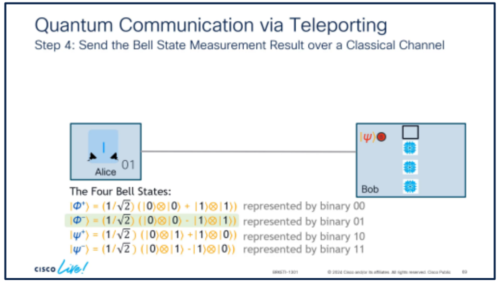
5) Can you transmit information faster than light with quantum teleporting?



Equivalent to sending (at least) one bit over a classical channel



Teleporting one of 4 random states does occur faster than light, but (strictly speaking) this not an information transfer on its own merit, since we cannot correctly interpret what has been sent without additional data



(At least) Two more bits of data are sent over a classic channel

Key Takeaway:
Quantum teleportation does NOT enable faster than light communication

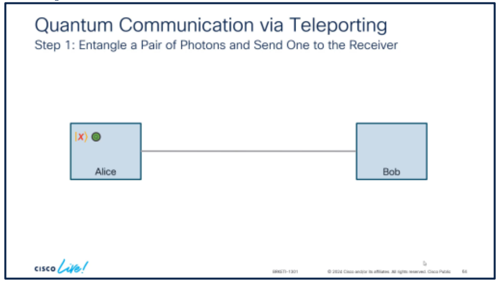
In fact, ***for every bit*** of information sent via ***quantum*** teleportation, ***at least 3 additional bits*** of data must be sent over ***classical*** channels

Post Session Quiz / Summary

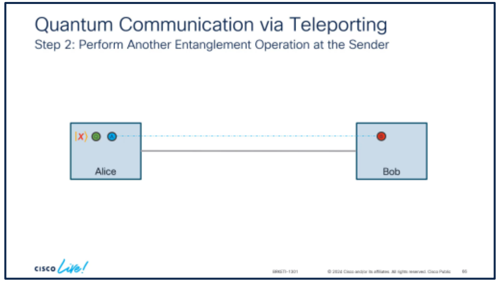
6) Will quantum networks replace classical networks?

Key Takeaway:
Quantum teleportation does NOT enable faster than light communication

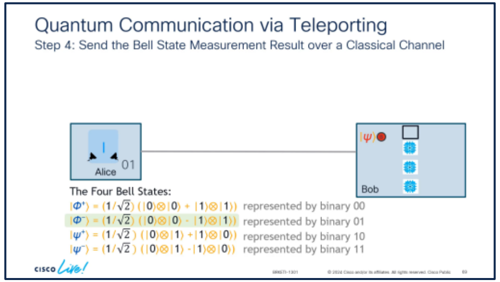
In fact, ***for every bit*** of information sent via ***quantum*** teleportation, ***at least 3 additional bits of data must be sent over classical channels***



Equivalent to sending (at least) one bit over a classical channel



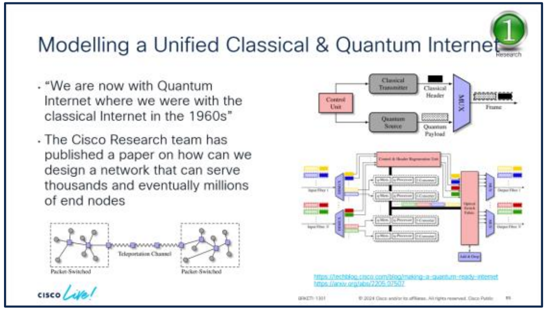
Teleporting one of 4 random states does occur faster than light, but (strictly speaking) this not an information transfer on its own merit, since we cannot correctly interpret what has been sent without additional data

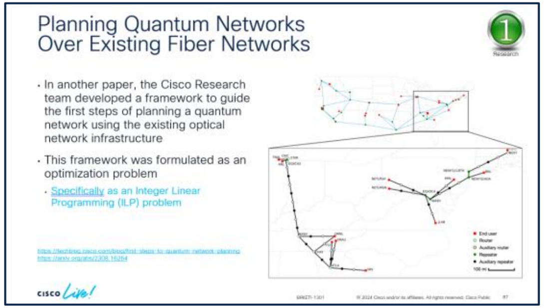


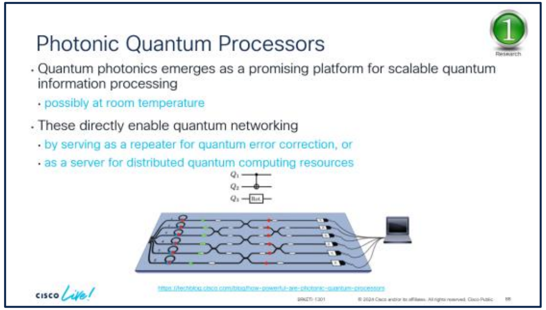
(At least) Two more bits of data are sent over a classic channel

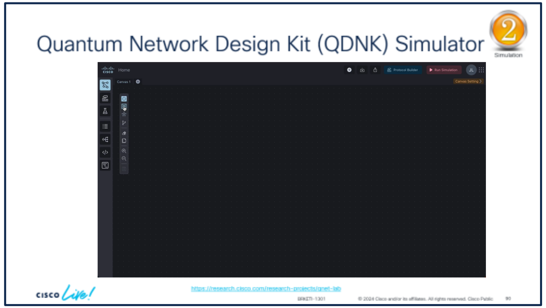
Post Session Quiz / Summary

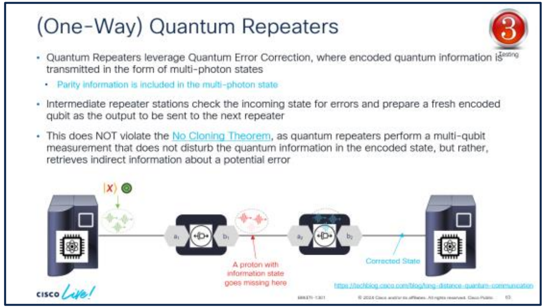
7) What is Cisco researching and developing in Quantum?











Acknowledgements

- Jeff Apcar
- Hassan Shapourian
- Stephen DiAdamo
- Peng Zhao

Continue the Discussion

- Come visit us in the Outshift booth in the Cisco World of Solutions (Booth D10)
- Book your one-on-one Meet the Engineer meeting
- See what’s coming by meeting with us in the Innovation Forum
- Book a meeting with us for an extended discussion on any Outshift area of research and development

Visit Outshift in the World of Solutions!

outshift by cisco

- Snap a picture of this slide and visit the Outshift Booth, D10.
- Get your badge scanned to be entered into our daily drawing* for €250 Cisco Store Gift Certificate.
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

**Winners will be notified via email*

The bridge to possible

Thank you

cisco Live!

Let's go