GROUP 163
CAPSTONE PROJECT

REVIEW 1

FROM BITS TO QUBITS

Classical v/s Quantum Computing

Our Team

Supervised By:
Dr. Lokesk Malviya Sir

Shubham Singh
21BCE10456

Sheikh Mohd Shoaib
21BCE11346

Dewanshi Joshi
21BCE11627

Ajinkya Fulpatil
21BCE11160

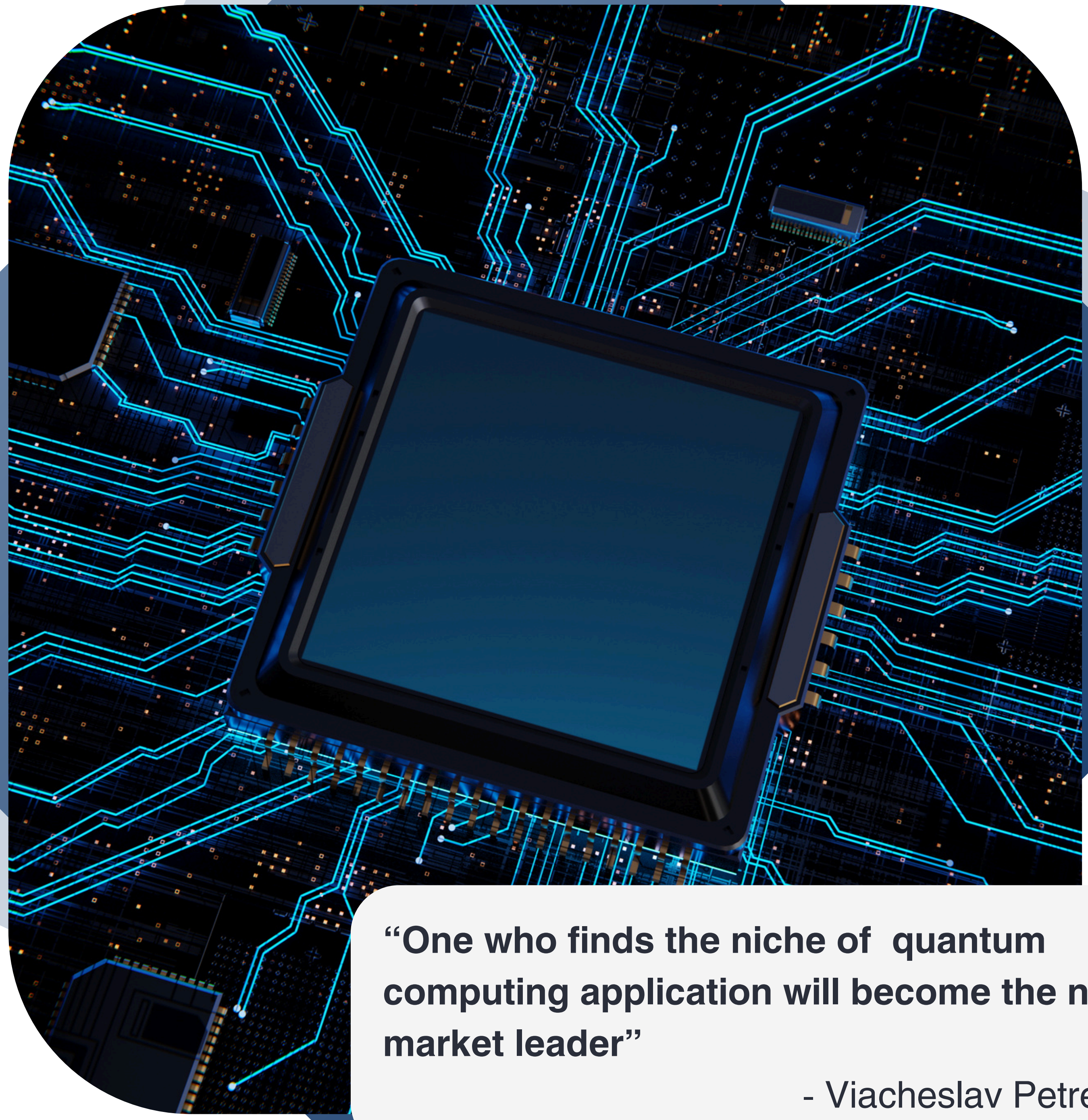
Harshita Nimje
21BCE10524

Agenda

OBJECTIVE

The Race for Quantum Supremacy

- The paper compares quantum computing and classical computing, focusing on quantum's ability to handle complex problems that classical systems can't efficiently solve.
- It examines advancements in quantum algorithms and explores how both systems may coexist, shaping future computational advancements in fields like cryptography and optimization and many more.



"One who finds the niche of quantum computing application will become the new market leader"

- Viacheslav Petrenko

What’s our MOTIVATION?

- Imagine a computer that can process information in ways we never thought possible. What if instead of just handling data as 0s and 1s, a computer could use both at the same time?
- This is the power of quantum computing! Unlike classical computers that use bits, quantum computers use qubits, allowing them to exist in multiple states at once—mind-blowing, right? Have you heard about Google’s Sycamore processor?
- It solved a problem in 200 seconds that would take even the fastest supercomputers thousands of years.
- Can you imagine what this means for fields like cryptography or drug discovery?

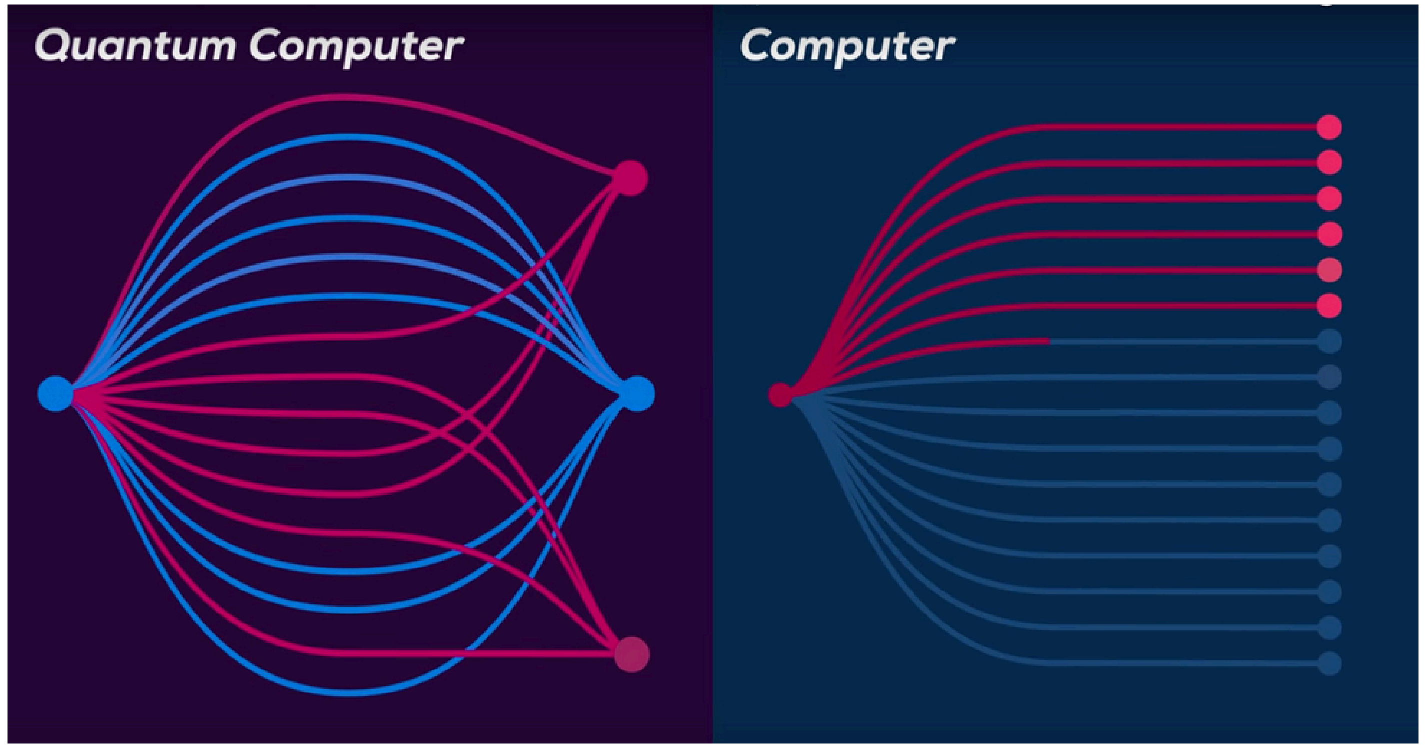
Significance

Quantum computing holds the potential to revolutionize various industries and fields by solving complex problems that are currently intractable for classical computers. Its significance lies in several key areas:

- Exponential Speedup in Problem Solving
- Revolutionizing Cryptography
- Optimization Problems
- Quantum Simulation
- Scientific Discovery and Research

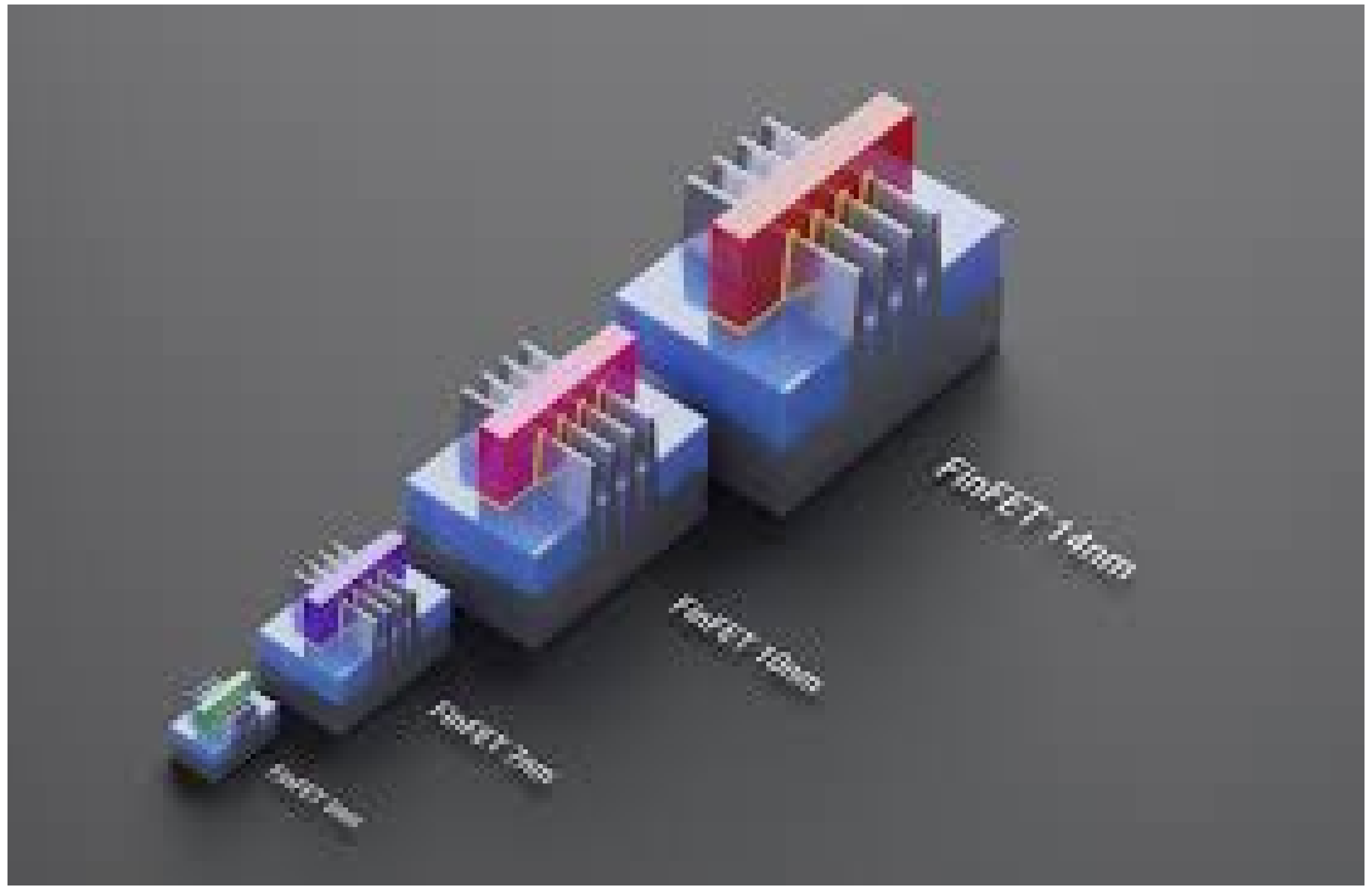
Limitations of classical computing

- **Processing Speed:** Classical computers struggle with complex problems (like factoring large numbers) due to their sequential processing, leading to longer computation times.
- **Memory Constraints:** Classical bits limit memory efficiency, as they can only represent one state (0 or 1) at a time, resulting in significant overhead for large datasets.
- **Inability to Exploit Quantum Phenomena:** Classical computers cannot utilize quantum phenomena such as superposition and entanglement, restricting their ability to solve certain problems more efficiently than quantum computers.



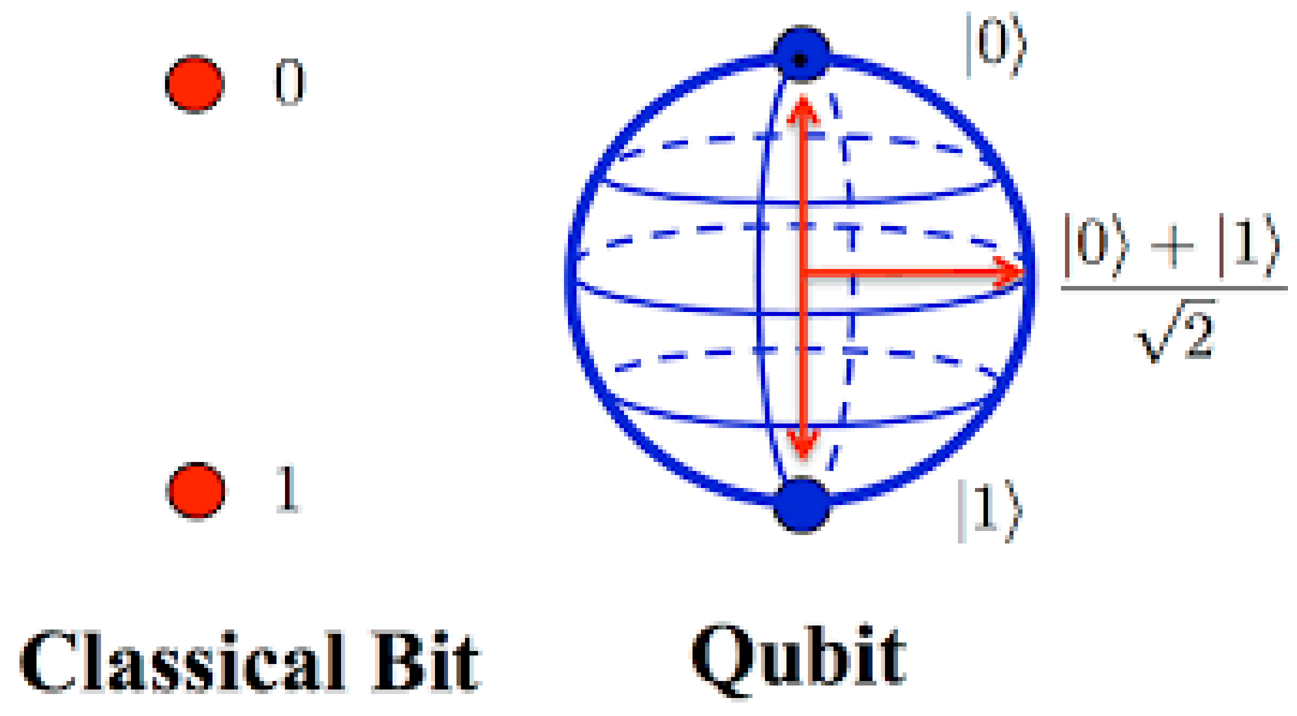
Moore's Law

- **Transistor Density:** Moore's Law predicts that the number of transistors on a microchip doubles approximately every two years, leading to increased processing power and performance.
- **Cost Efficiency:** As transistor density increases, the cost per transistor decreases, making computing technology more affordable and accessible over time.
- **Technological Advancement:** Moore's Law has driven innovation in semiconductor technology, influencing the design and development of faster, smaller, and more efficient electronic devices.



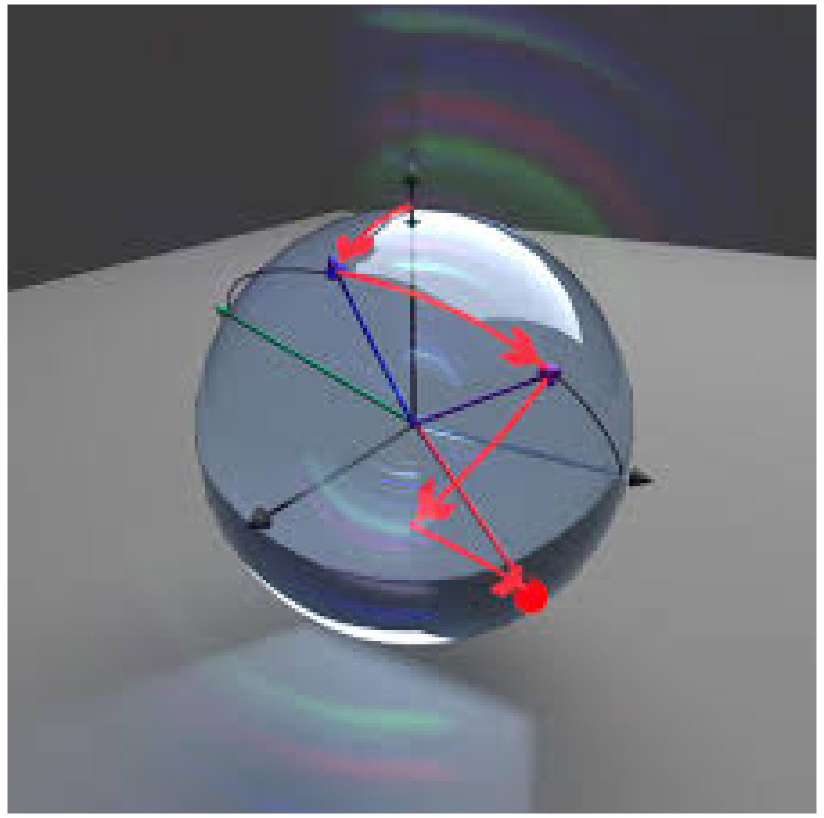
Superposition

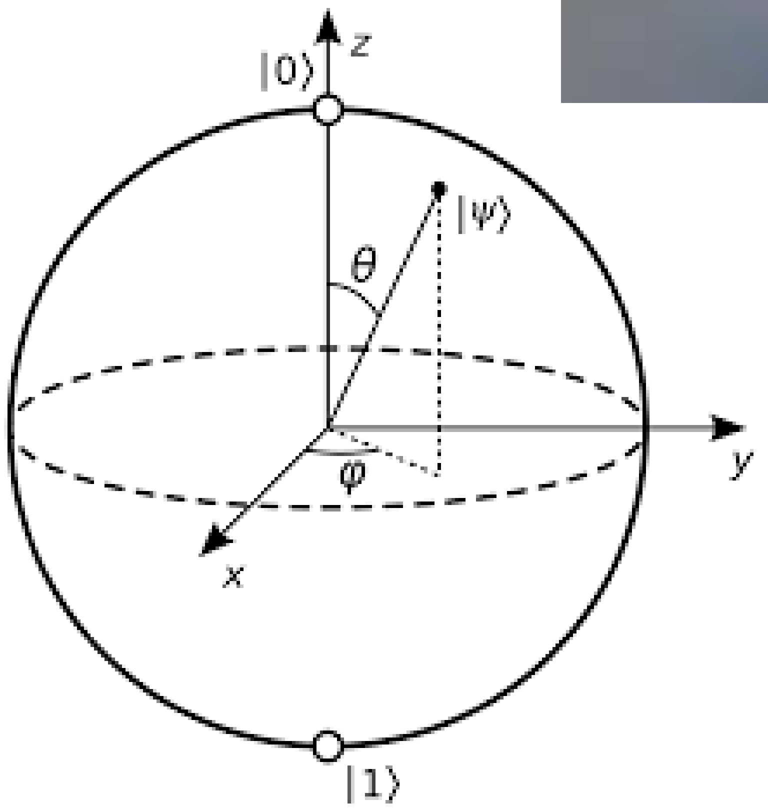
- **Multiple States:** A qubit can be in both 0 and 1 states at the same time.
- **Faster Processing:** This allows quantum computers to perform many calculations at once, speeding up problem-solving.
- **Interference:** Superposition helps in combining outcomes to improve the chances of getting the right answer.



Bloch sphere

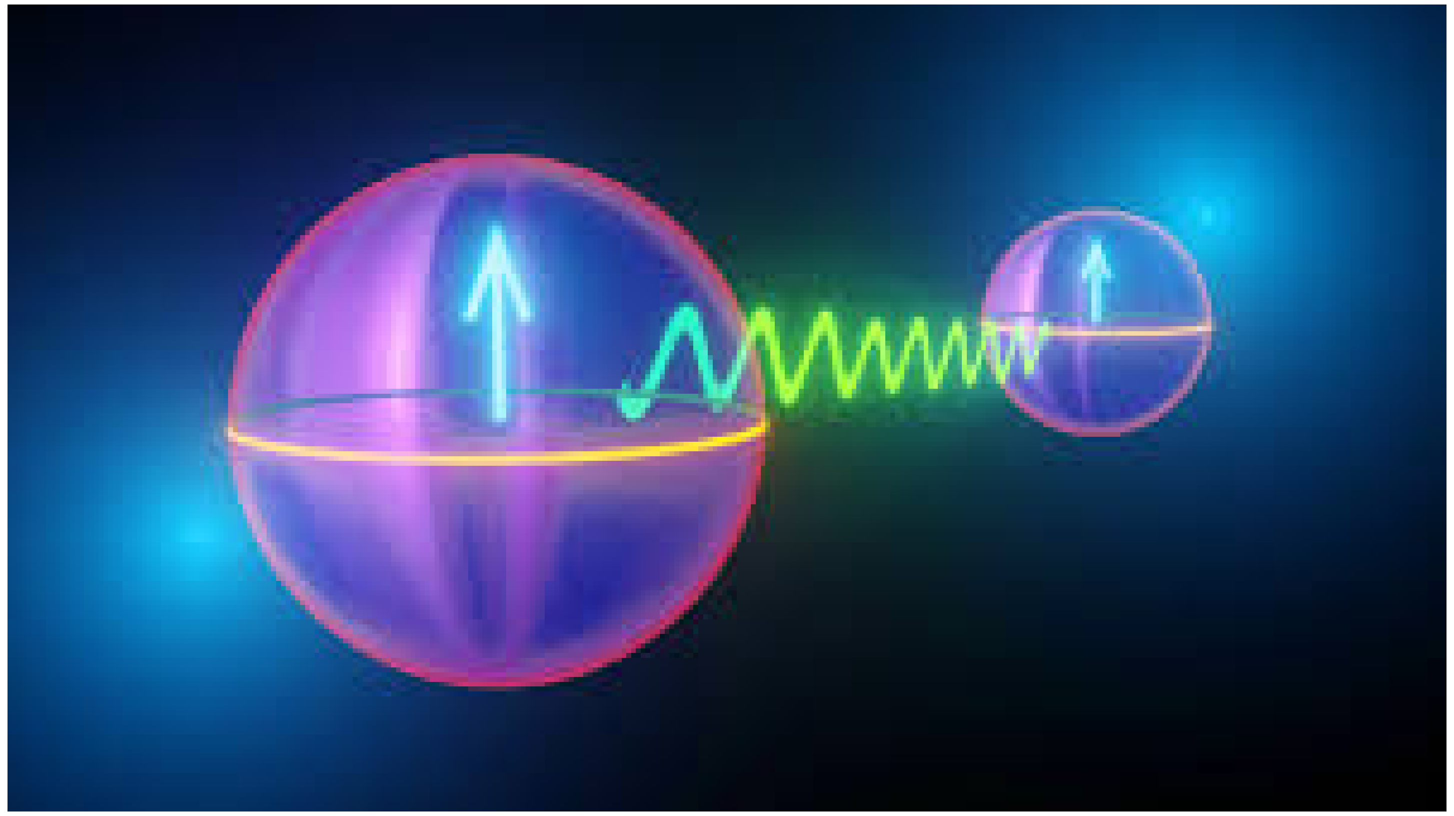
- **Visual Representation of Qubits:** The Bloch sphere is a 3D model used to represent the state of a single qubit, with $|0\rangle$ at the north pole and $|1\rangle$ at the south pole.
- **Qubit Superposition:** Any point on the surface of the sphere represents a qubit's superposition between the states $|0\rangle$ and $|1\rangle$, allowing visualization of both probability and phase.
- **Quantum Gates and Rotations:** Rotations around the Bloch sphere illustrate quantum gate operations, which modify the qubit's state for quantum computations.





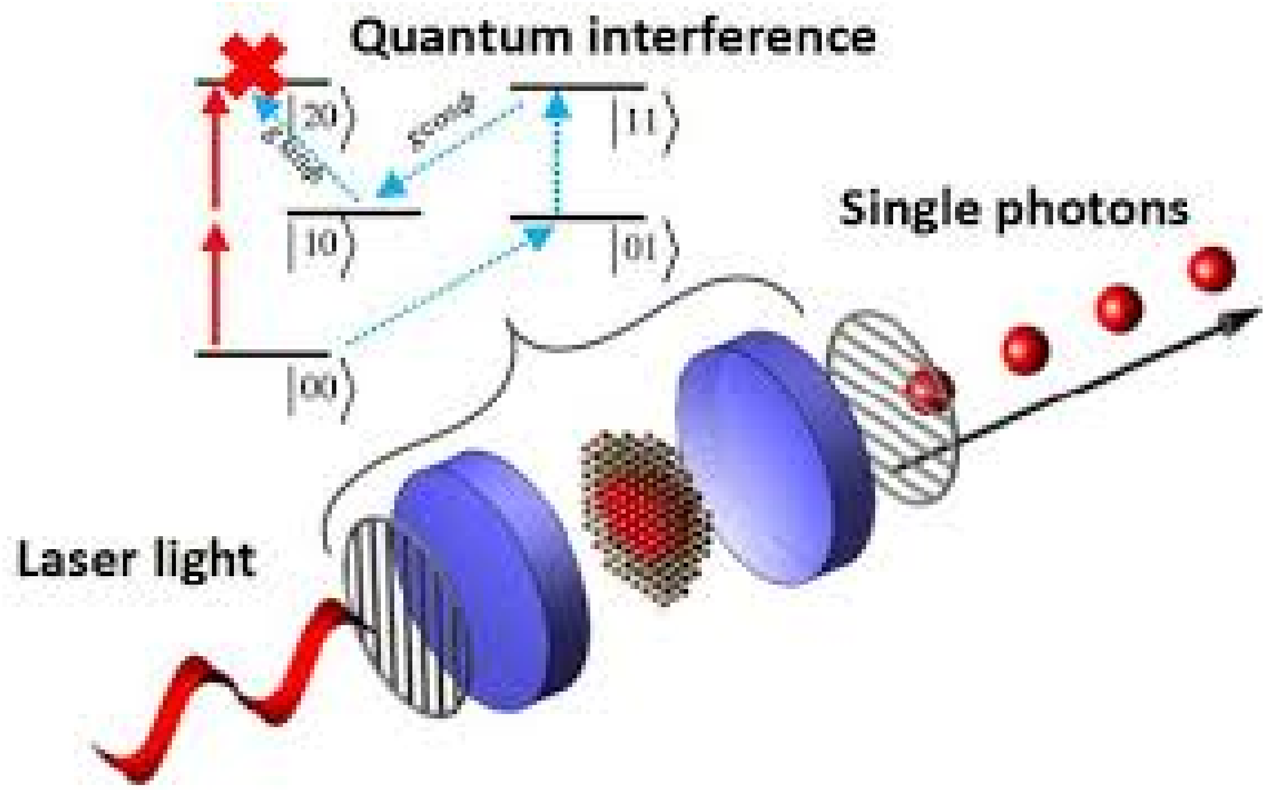
Entanglement in Quantum Computing

- **Definition:** Phenomenon that occurs when 2 or more qubits become interconnected in a way that the state of 1 qubit is directly related to the state of other, regardless of the distance between them.
- These **non-local connections** between qubits allows quantum computers to perform highly coordinated operations that are impossible for classical computing.
- **Solves Complexity:** Entangled qubits can process and exchange info instantaneously, enabling QC to solve complex, correlated problems efficiently.
- **Example:** The concept of entanglement is a key driver behind quantum cryptography



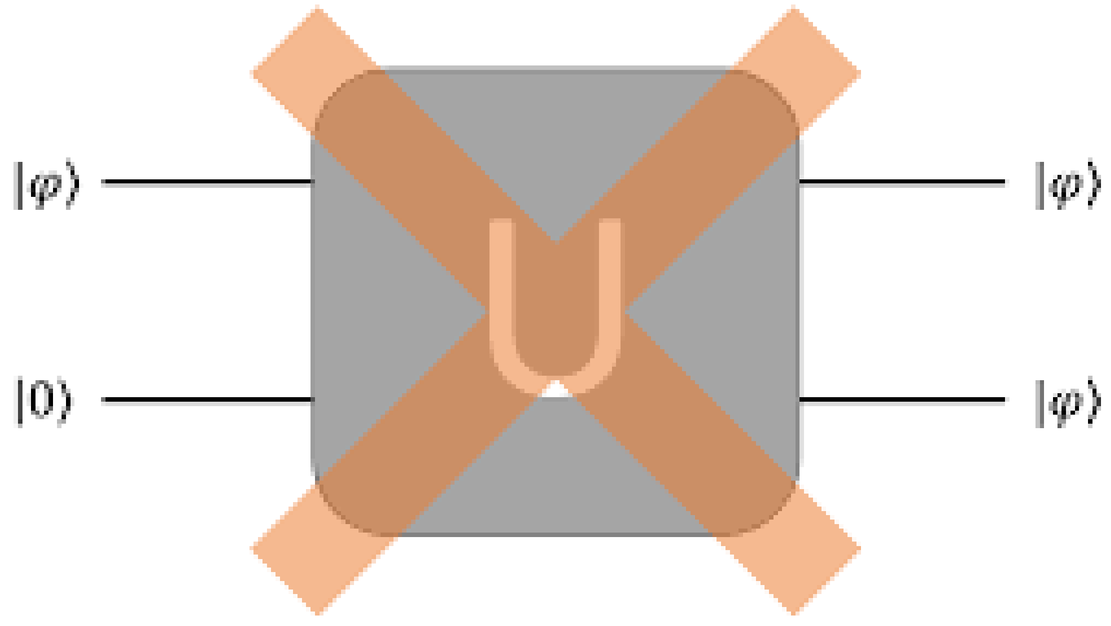
Quantum Interference

- **Definition:** Quantum interference occurs when probability amplitudes add up or cancel out based on their phase, affecting the outcomes of quantum processes.
- **Types: Constructive Interference:** Amplifies the probability of certain outcomes. **Destructive Interference:** Suppresses incorrect outcomes.
- **Distinct from Classical Probability:** Classical probabilities simply add, whereas quantum probabilities interfere.
- **Example:** In algorithms like Grover's Search, interference is leveraged to converge on the correct solution faster by amplifying the correct state and diminishing incorrect ones.



No-Cloning Theorem

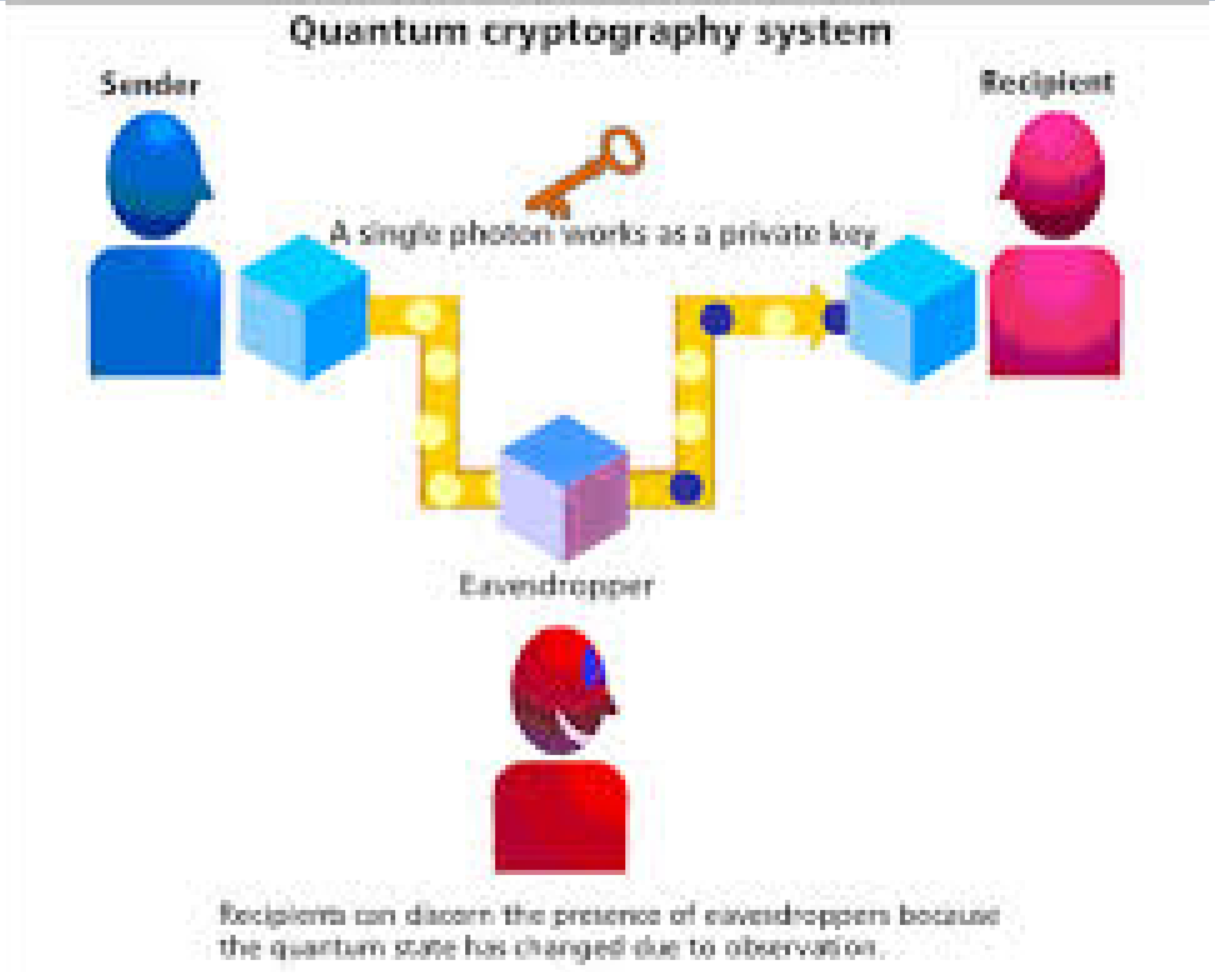
- **Impossibility of Cloning:** An unknown quantum state cannot be copied exactly.
- **Measurement Disturbance:** Attempting to measure a quantum state alters it, preventing cloning.
- **Implications for Security:** Ensures the integrity and security of quantum information, crucial for quantum communication.



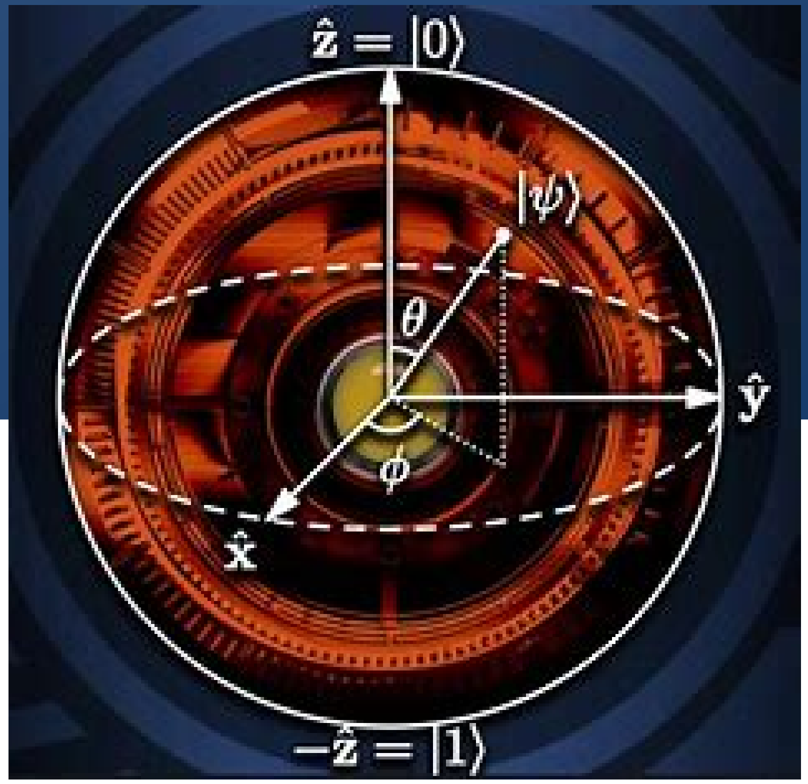
No-Cloning Theorem

Significant Implications

- **Quantum Cryptography:** Enhances the security of communication by preventing eavesdropping since quantum states can't be copied without detection.
- **Data Integrity:** Ensures that quantum information remains unique and untampered, vital for quantum computing and secure data transfer.
- **Quantum Key Distribution (QKD):** Plays a crucial role in protocols like QKD, where secure keys can be shared without fear of duplication.



Measurement of Qubits



In quantum computing, measurement is a crucial process where the state of a qubit (quantum bit) is observed, and it collapses from a superposition (where it can exist in multiple states) to a definite classical state — either 0 or 1.

Before Measurement: Superposition

A qubit can exist in a superposition of the two classical states, meaning it can be in a combination of both 0 and 1. The state of a qubit is typically represented as:

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

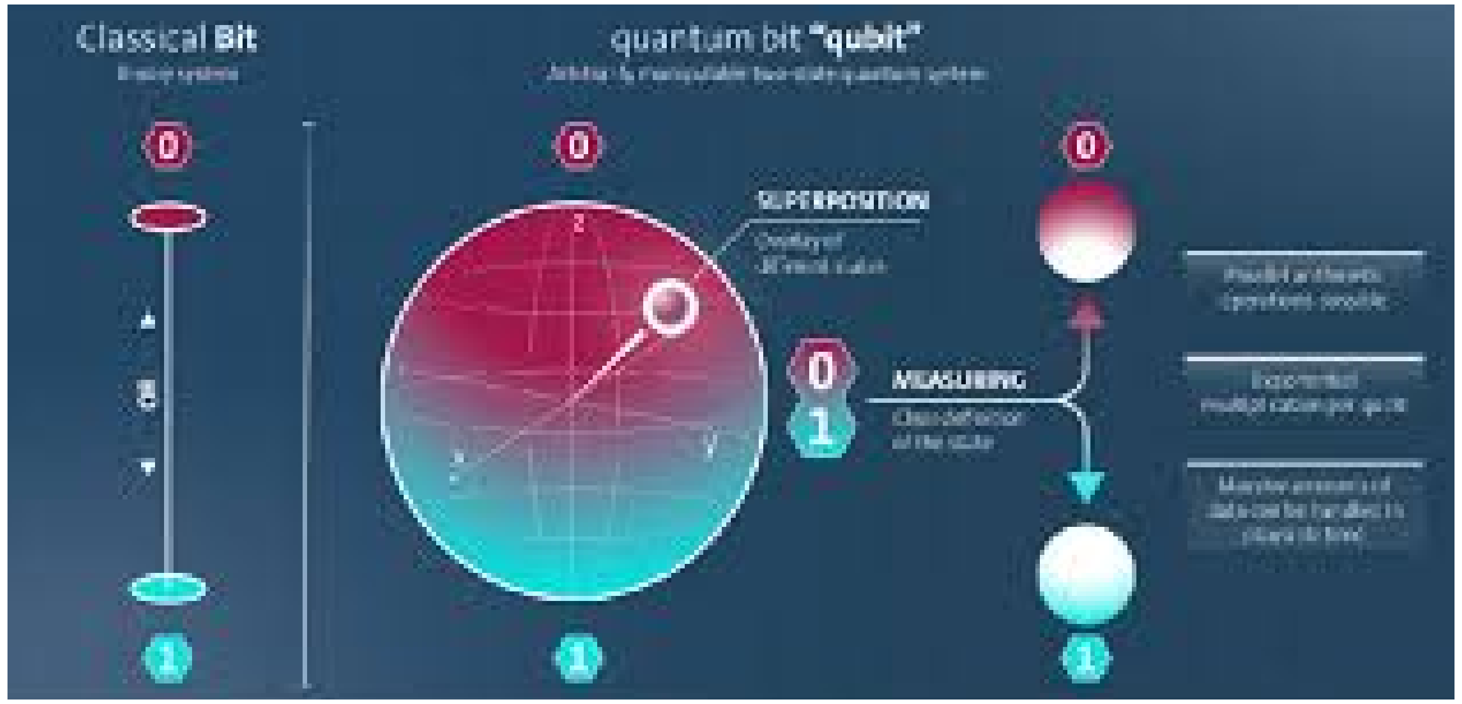
The Measurement Process

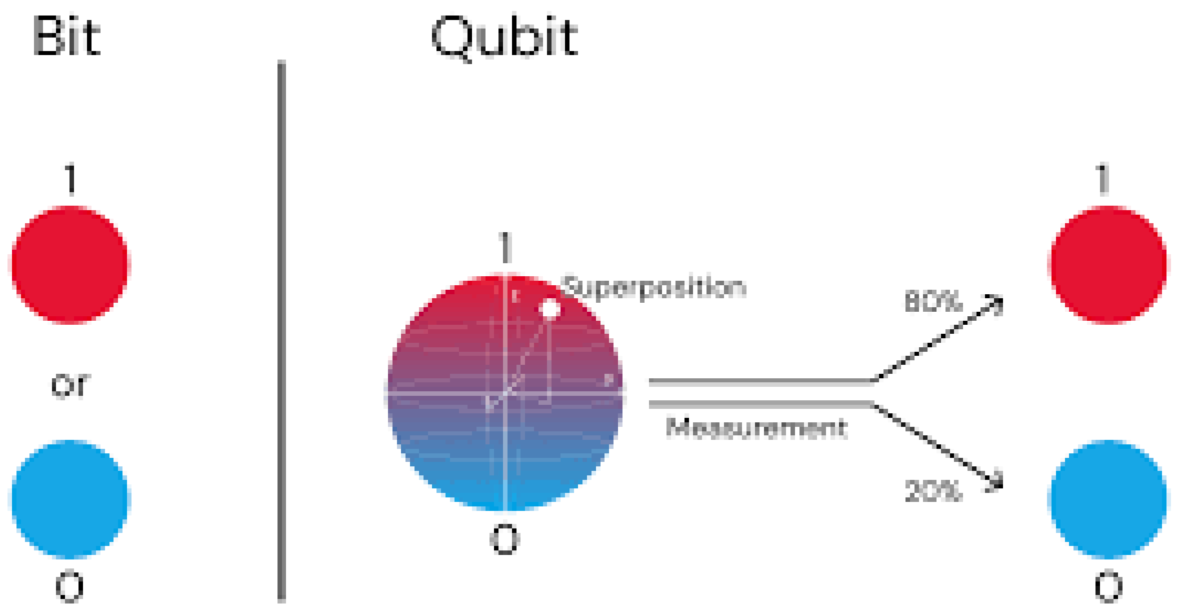
When you measure a qubit, you are forcing it to "collapse" from its superposition state to either 0 or 1, and the result is probabilistic:

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

Comparison with classical bit

- **State Representation:** Classical bits can be either 0 or 1, while qubits can exist in superpositions of both states simultaneously (0, 1, or any combination).
- **Information Capacity:** A qubit can represent more information than a classical bit due to its ability to exist in multiple states, enabling parallel processing.
- **Entanglement:** Qubits can be entangled, allowing them to be correlated in ways classical bits cannot, leading to faster and more secure computations.





THANK YOU!