

Introduction To Quantum Computing



Introduction to Quantum Computing

Classical Physics and ADHOC hypothesis

Quantum Mechanics as Modern Theory

Quantum Systems

Distributed Quantum Computation





Classical Physics and **ADHOC** hypothesis

The Crisis of Classical Physics

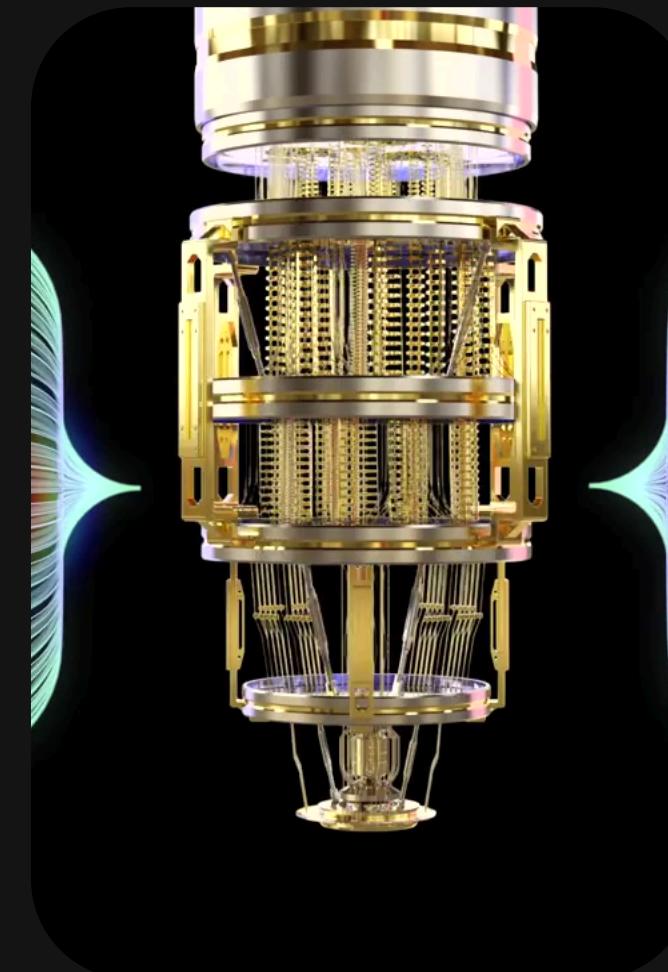
The Breakdown of Tradition

By the late 19th century, classical theories began predicting absurdities : physical impossibilities that the established laws of Newton and Maxwell couldn't explain.

The "Ad Hoc" Band-Aid

To prevent these theories from failing entirely, scientists introduced Ad Hoc Hypotheses:

- Definition: Auxiliary assumptions added to a theory specifically to save it from being falsified.
- Purpose: To bridge the gap between conflicting experimental data and existing theoretical frameworks.
- The Result: While these "quick fixes" kept classical physics afloat temporarily, they ultimately paved the way for the Quantum Revolution.



Classical physics hit a wall when it couldn't explain how light and energy behaved at extreme scales.

The Ultraviolet Catastrophe

The Luminiferous Aether



Classical Physics and **ADHOC** hypothesis

Classical physics hit a wall when it couldn't explain how light and energy behaved at extreme scales.





Quantum Mechanics as Modern Theory

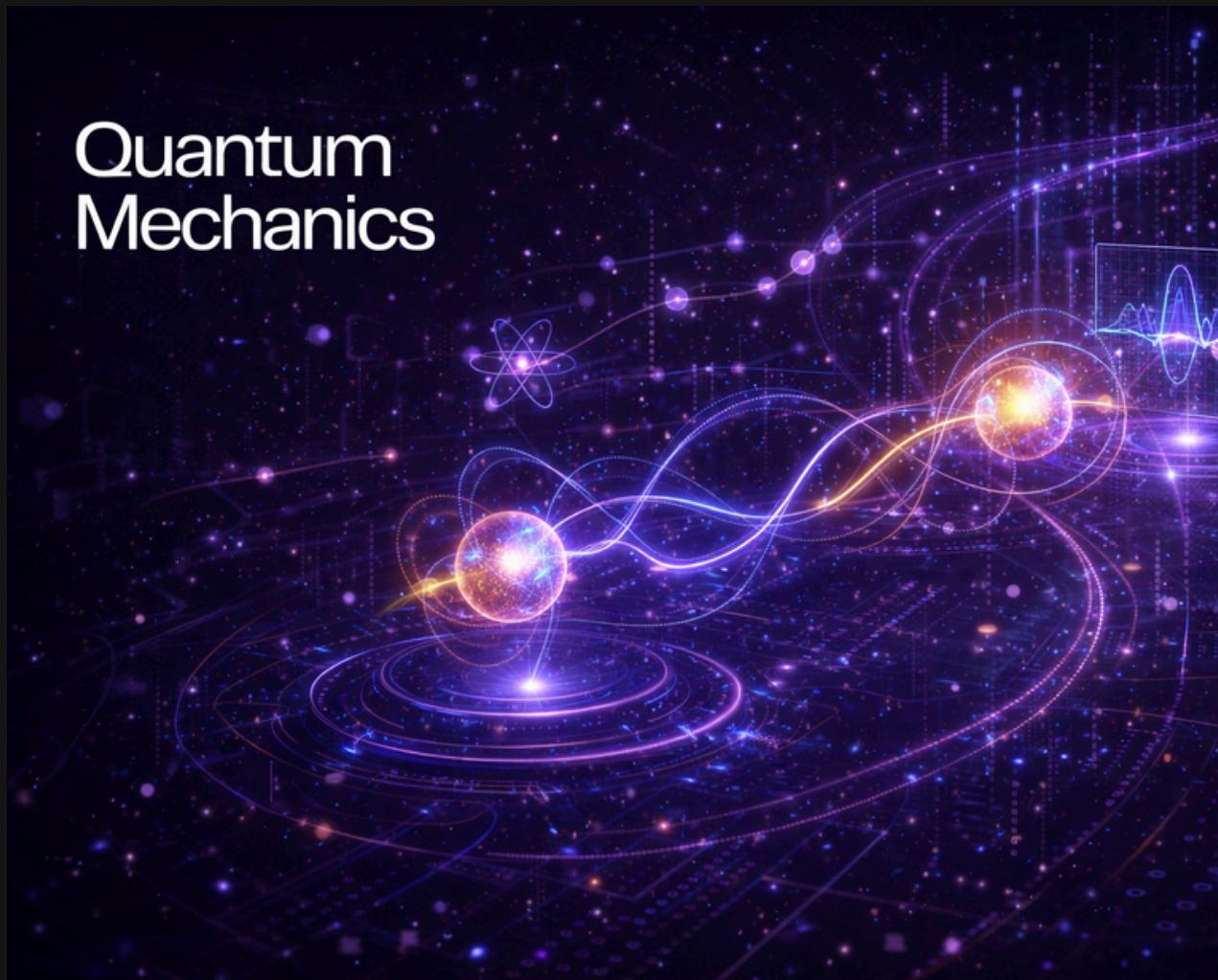
1920s: The Birth of a New Reality

From Crisis to Revolution

Since the 1920s, Quantum Mechanics (QM) has moved from a radical idea to an indispensable tool applied with enormous success to everything "under and inside the sun."

Defining Quantum Mechanics

A set of universal rules working under a rigorous mathematical framework for the construction of physical theories.



The Single Qubit (The Atom of Information)

a single qubit exists in a Superposition, represented mathematically as:

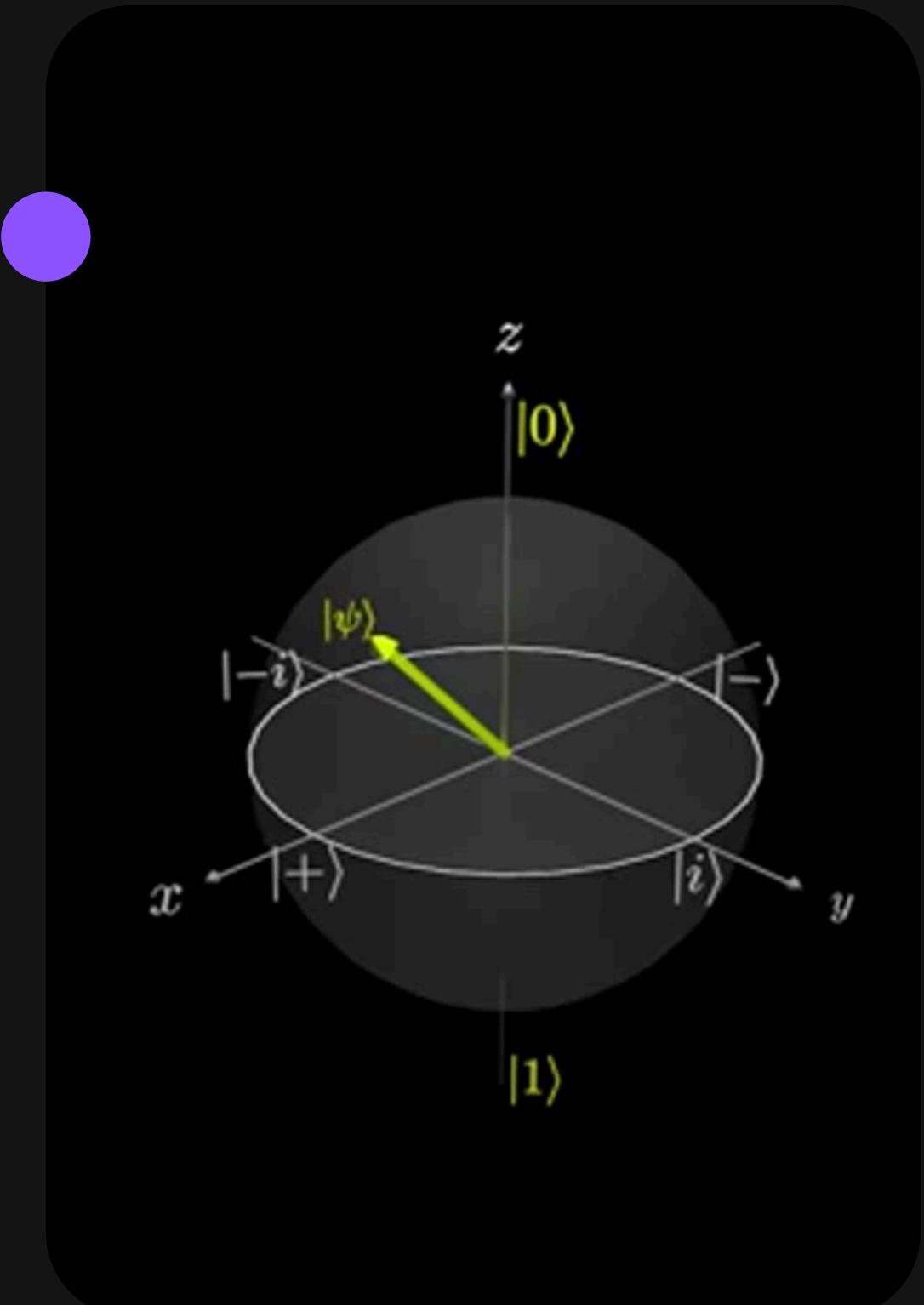
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- This means it carries the potential for both states simultaneously until measured.

The 2-Qubit System (Entanglement Emerges)

When we move to two qubits, we encounter Entanglement, what Einstein called "spooky action at a distance."

- The system can represent 4 states simultaneously (00, 01, 10, 11).



Quantum Systems

The New Frontier: Information & Computation

By applying the fundamental rules of the 1920s to information rather than just matter, we have entered a new frontier where quantum states redefine how data is processed and transmitted. This revolution utilizes principles like superposition and entanglement to power quantum computation, solving complex problems that remain impossible for classical systems.

The Single Qubit (The Atom of Information)

a single qubit exists in a Superposition, represented mathematically as:

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

- This means it carries the potential for both states simultaneously until measured.

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

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$$

Why this matters for Information ?

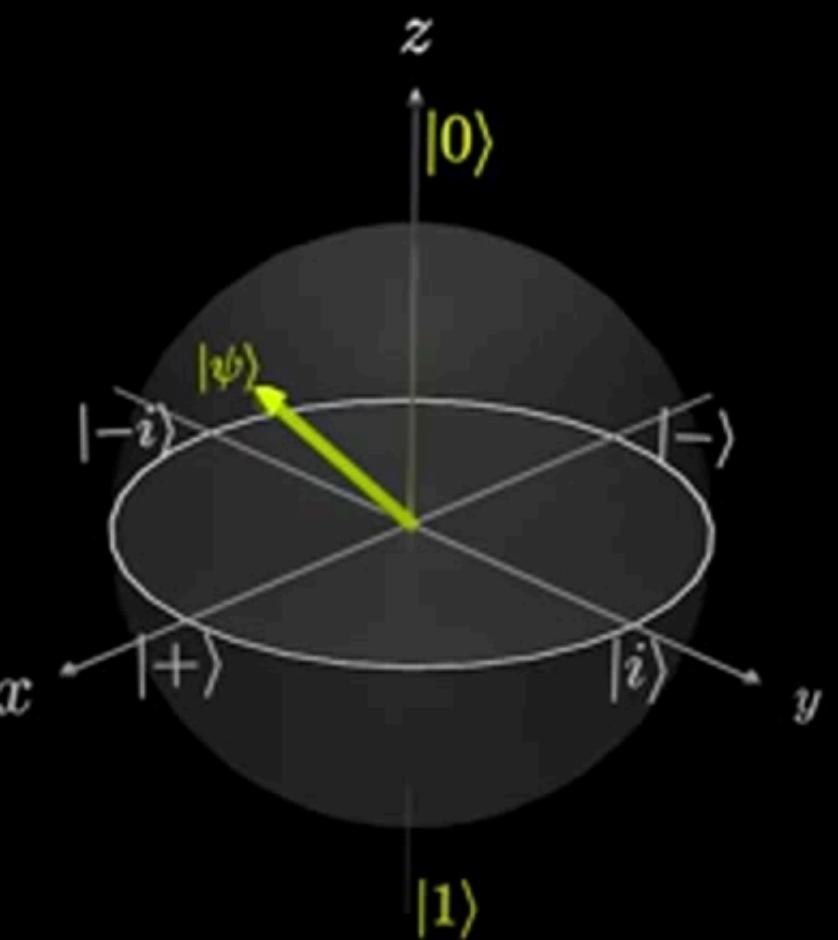
This representation reveals that "state" is relative to how you choose to look at the qubit.

While a classical bit is like a coin lying flat on a table (Heads or Tails), a qubit is like a coin spinning on the table. While it spins, it isn't just "Heads and Tails" it has a specific speed, an angle of tilt, and a direction of rotation.

- Classical bit: 1 bit of info.
- Quantum qubit: Two continuous complex coefficients.
- Until you measure it and stop the "spin," the qubit carries the "memory" of that entire spherical coordinate system.

Schrödinger cat

NATURE IS NOT DETERMINISTIC



Quantum System

The Information 8

By applying the fundamental principles of quantum mechanics, we can explore the frontier where quantum systems are processed and transmitted. These principles, like superposition and entanglement, make quantum computing possible and impossible for classical systems.

The 2-Qubit System (Entanglement Emerges)

The Single Qubit (The Atom of Information)

a single qubit exists in a Superposition, represented mathematically as:

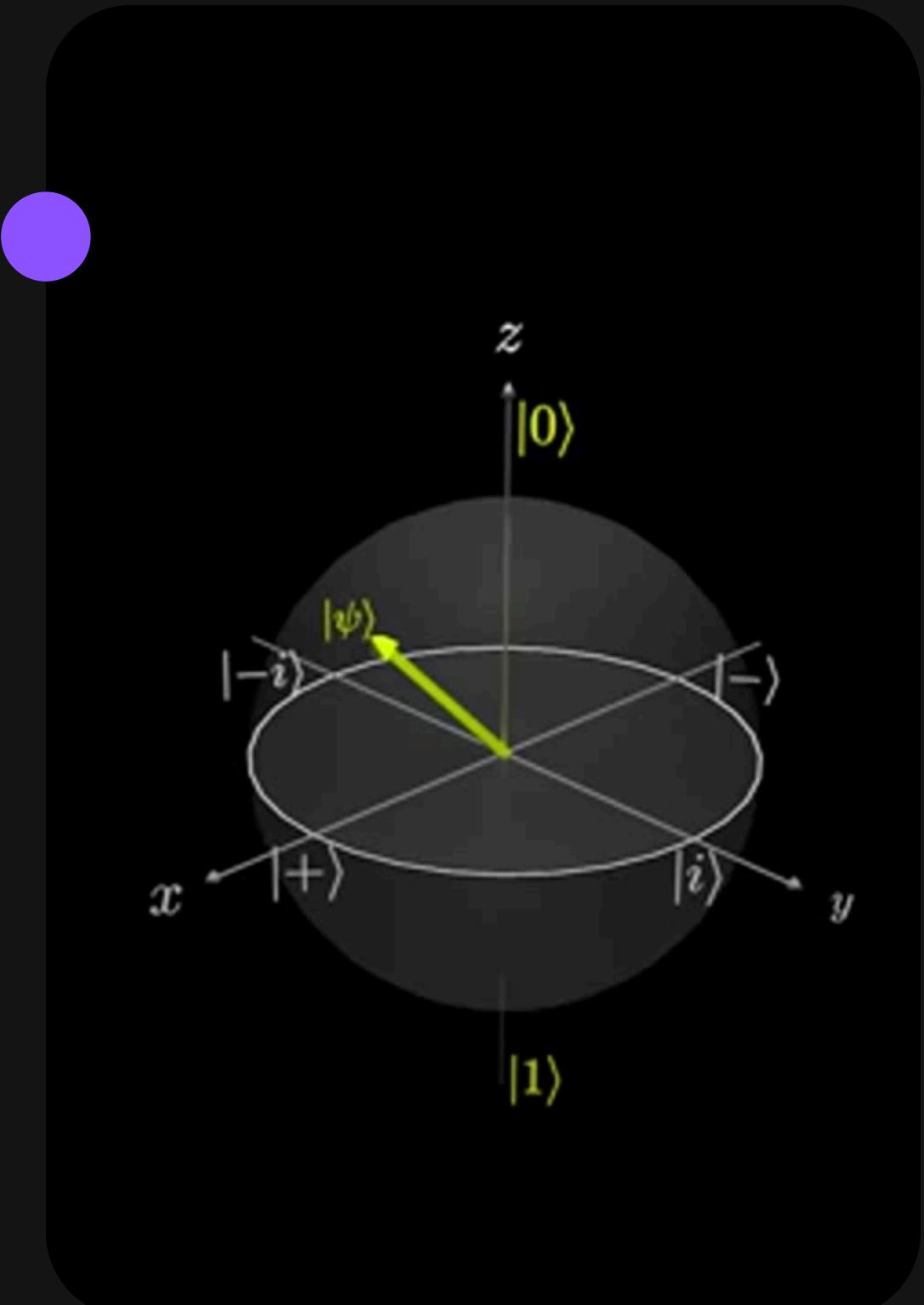
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- This means it carries the potential for both states simultaneously until measured.

The 2-Qubit System (Entanglement Emerges)

When we move to two qubits, we encounter Entanglement, what Einstein called "spooky action at a distance."

- The system can represent 4 states simultaneously (00, 01, 10, 11).



Quantum Systems

The New Frontier: Information & Computation

By applying the fundamental rules of the 1920s to information rather than just matter, we have entered a new frontier where quantum states redefine how data is processed and transmitted. This revolution utilizes principles like superposition and entanglement to power quantum computation, solving complex problems that remain impossible for classical systems.

The Single Qubit (The Atom of Information)

The 2-Qubit System (Entanglement Emerges)

When we move to two qubits, we encounter Entanglement, what Einstein called "spooky action at a distance."

- The system can represent 4 states simultaneously (00, 01, 10, 11).
- The qubits become "linked"; measuring one instantly determines the state of the other, regardless of distance. This is the foundation of Quantum Information Theory.

Scaling to 4 Qubits and Beyond

As we add qubits, the "computational space" grows exponentially, not linearly:

- 1 Qubit: 2 basis states
- 2 Qubits: 4 basis states
- 4 Qubits: 16 basis states
- n Qubits: 2^n basis states



Distribute Quantum Systems

Quantum Communication Channels

In a classical network, communication is limited by bandwidth and signal noise. In a quantum network, Entanglement acts as a "booster" for the channel's capacity.

Easy Communication: Entanglement makes synchronization "easy" because the parties are sharing a single correlated state, bypassing some of the statistical overhead required in classical packet-switching.



The Quantum Cryptosystem

The "rules" of the 1920s give us a new way to define Private and Public keys.

- Public Key: In classical systems (like RSA), the "Public Key" is a large number that is easy to multiply but hard to factor.
- Private Key: The "Private Key" is the secret factors of that number.
- The Quantum Difference: In a quantum network, we can use Quantum Key Distribution (QKD). Here, the "Private Key" is a string of quantum states. If an eavesdropper tries to look at the key, the Rule of Measurement ensures the state collapses, immediately alerting the two parties that the security is breached.

THANK YOU

