Fundamentals and Potential of Quantum Computing

Les King
les@idug.org

May 2026

CCDUG – Toronto

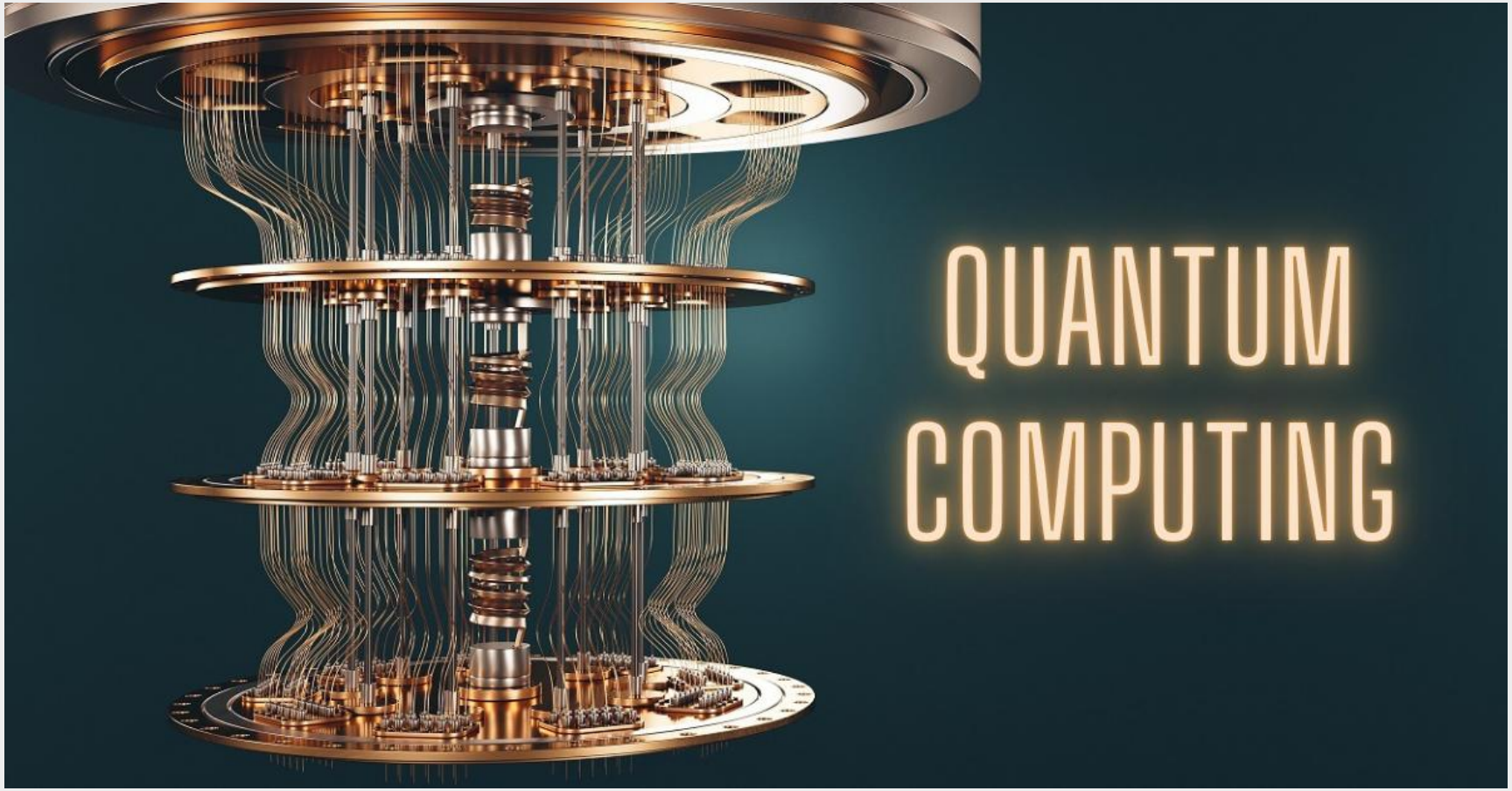
Session: ZMISC05

Quantum Computing

Concepts

Use Cases

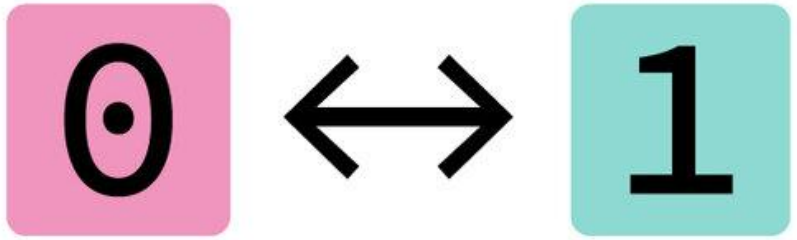
Challenges



Qubit

TRADITIONAL COMPUTERS

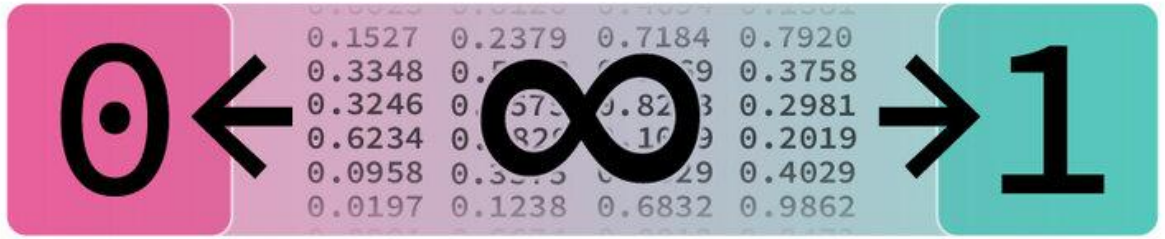
Technology based on ‘bits’



Bits have two states: 0 or 1

QUANTUM COMPUTERS

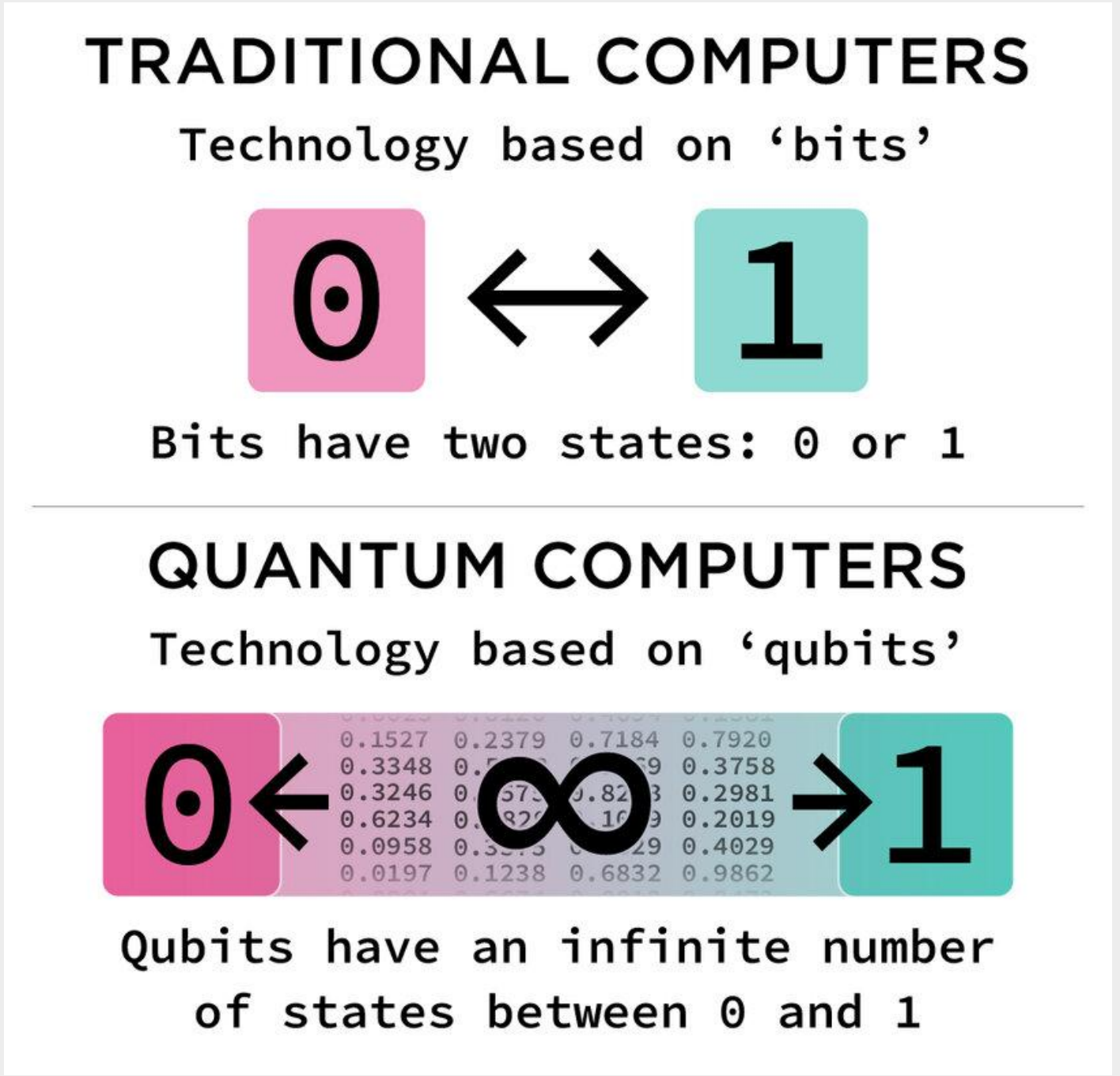
Technology based on ‘qubits’



Qubits have an infinite number of states between 0 and 1

Qubit

A Qubit is a physical **subatomic particle** such as **electron** or **proton** – usually a mix of **aluminum** and **niobium**

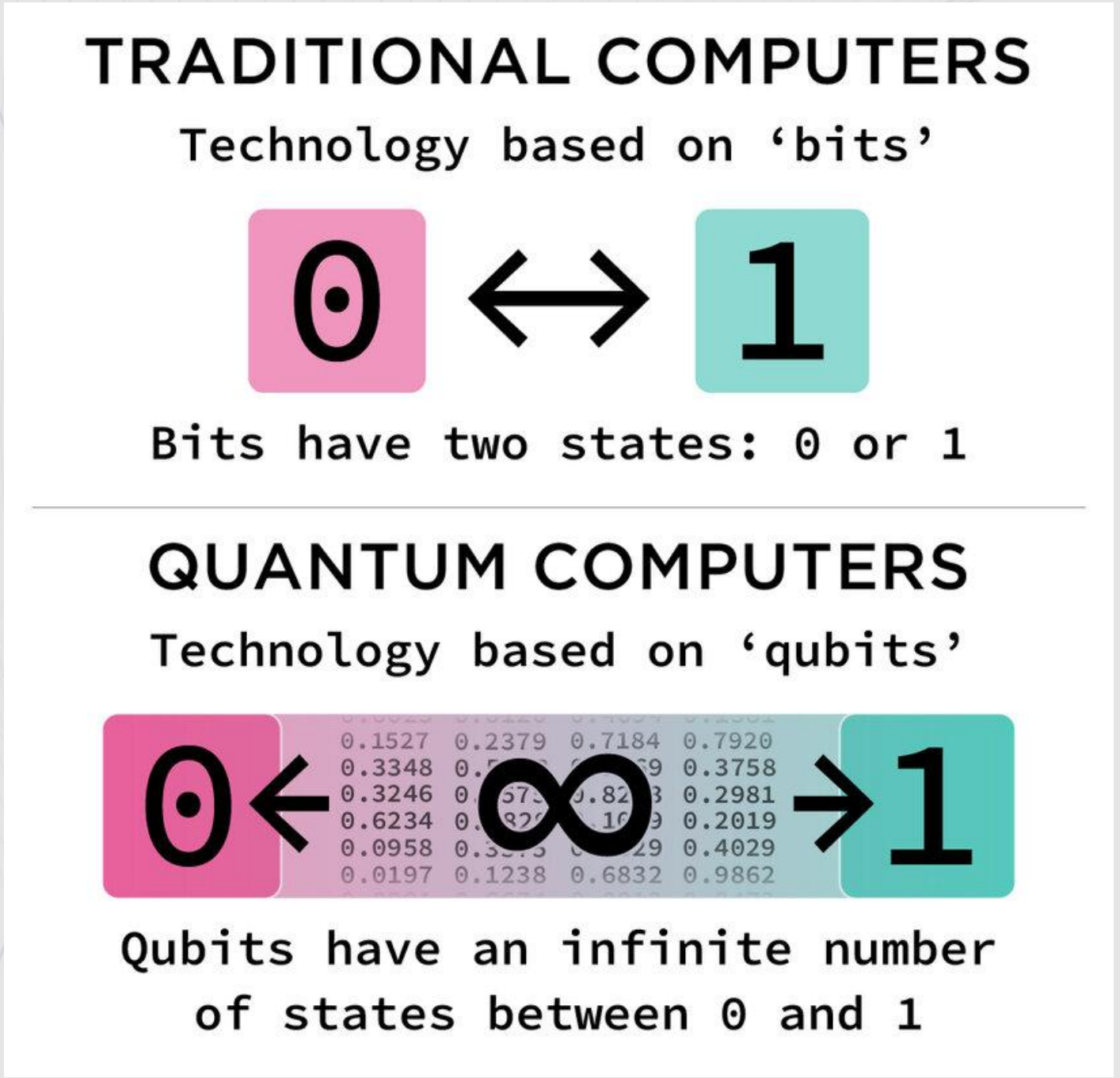


Qubit

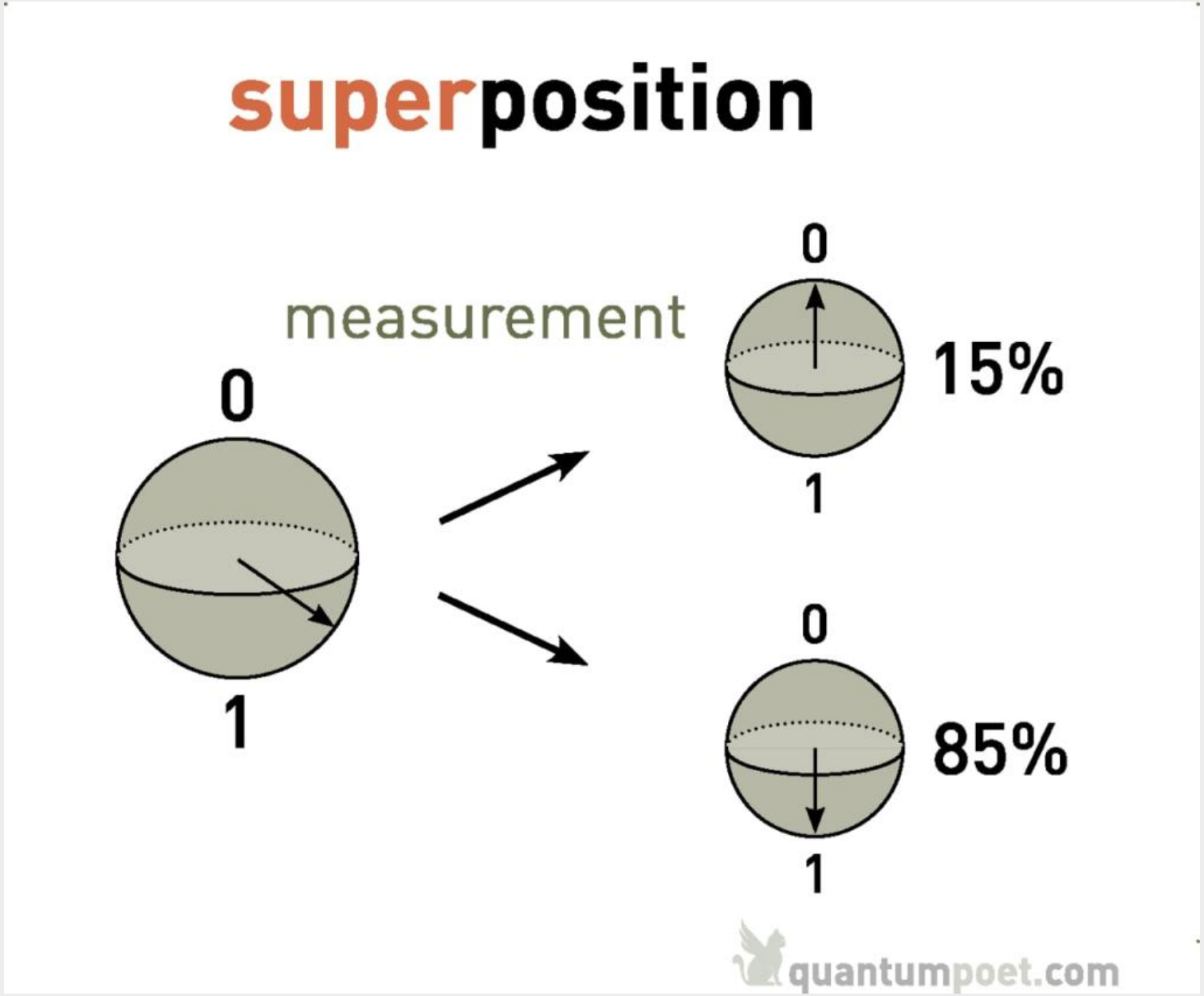
Qubits need to be kept at near **0 Kelvin** (-273.15C) in order for **improved stability**

The objective is to help maintain quantum states, minimize error rates, and enable **superconducting behavior**.

Qubits are extremely sensitive and prone to losing their quantum state (a process called **decoherence**) through interaction with their environment.



Concept 1: Superposition



Concept 1: Superposition

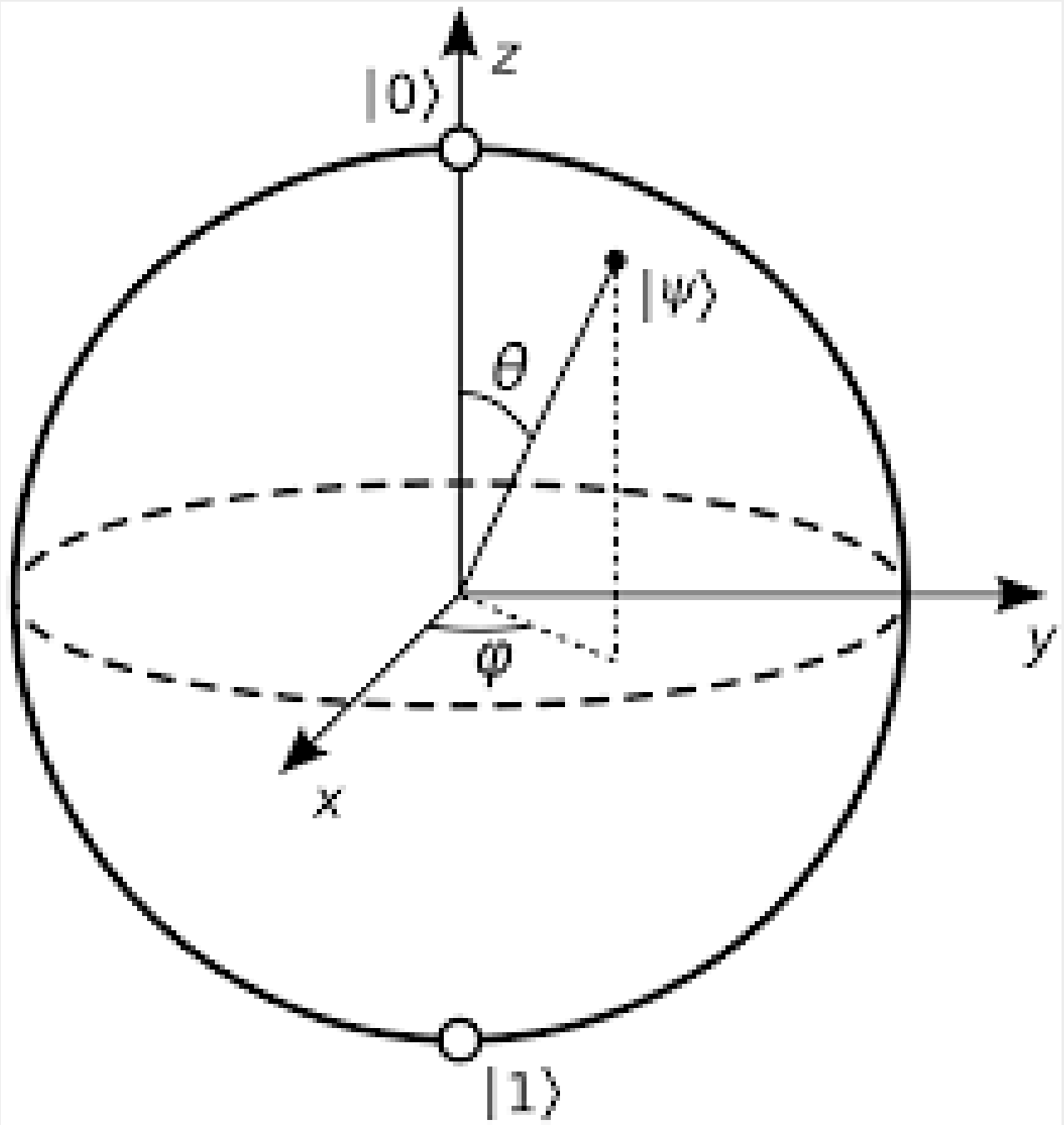
A single Qubit is best visualized with a **Bloch Sphere**

Why a sphere instead of a circle ?
Because a qubit is a **2-state system**

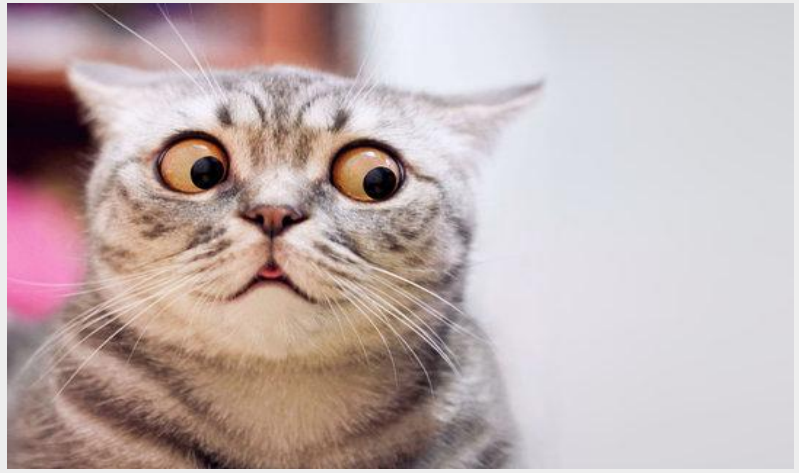
The arrow pointing straight down represents 1

The arrow pointing straight up it corresponds to 0

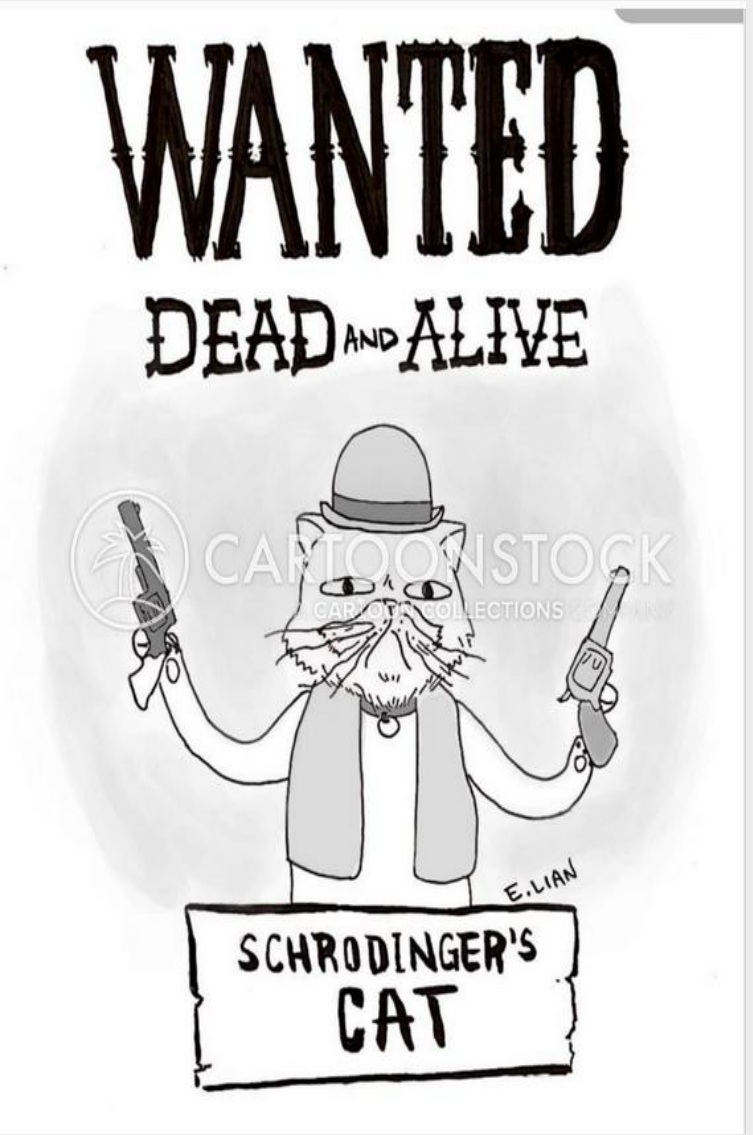
in any other position it represents a **superposition** of 0 and 1



Concept 1: Superposition - Schrodinger’s Cat



Schrödinger's Cat is **a famous thought experiment that demonstrates the idea in quantum physics that tiny particles can be in two states at once until they're observed**. It asks you to imagine a cat in a box with a mechanism that might kill it. Until you look inside, the cat is both alive and dead at the same time.



Concept 1: Superposition

A Qubit in its superposition state can have any of an infinite number of values between 0 and 1

It's **measured value** always resolves to 0 or 1

The measurement "collapses" the Qubit's quantum state

Can **never predict** a specific outcome

Can **calculate the probability** of a specific outcome

Concept 1: Superposition

Superposition states are unobservable – there's no actual value

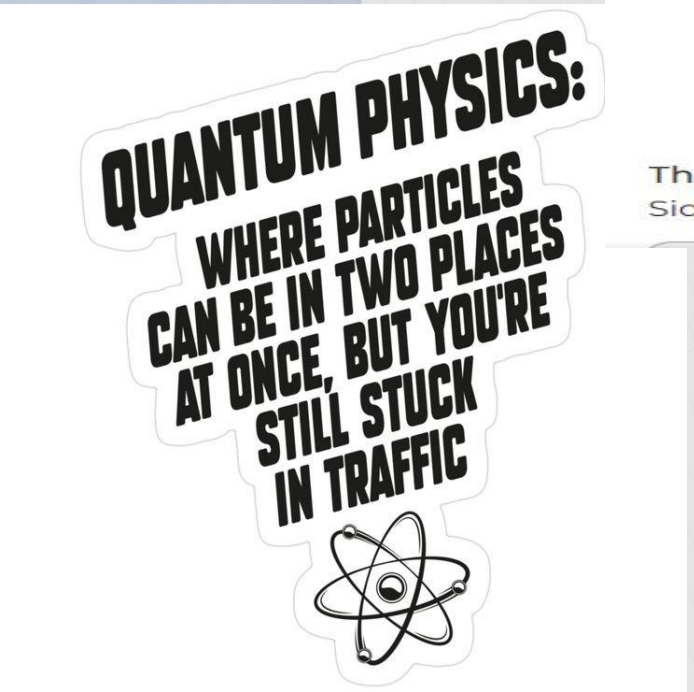
A measured stated – we can observe – a state of Spin Up or Spin Down is defined

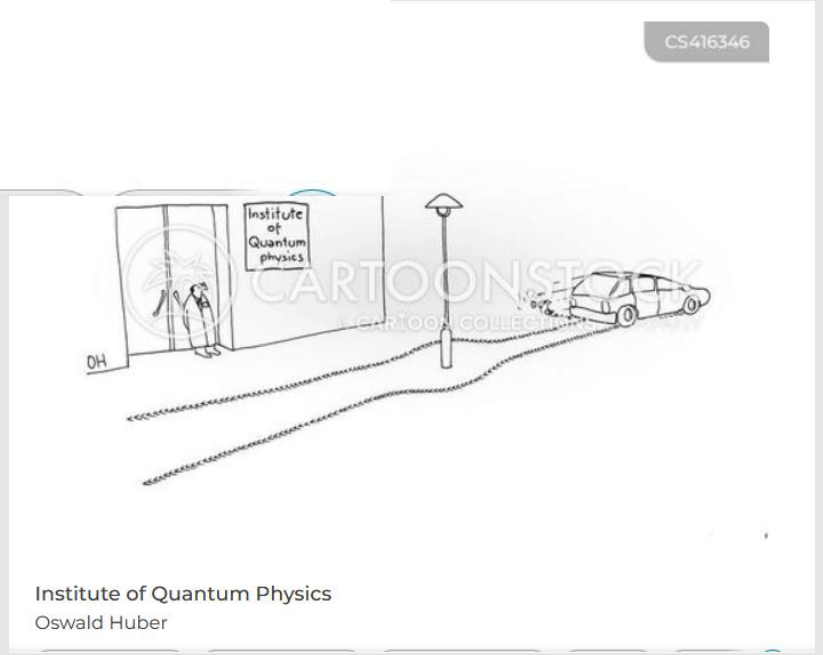
Spin Down = 0 – no energy applied to the electron or proton

Spin Up = 1 – energy applied to the electron or proton

Concept 1: Superposition

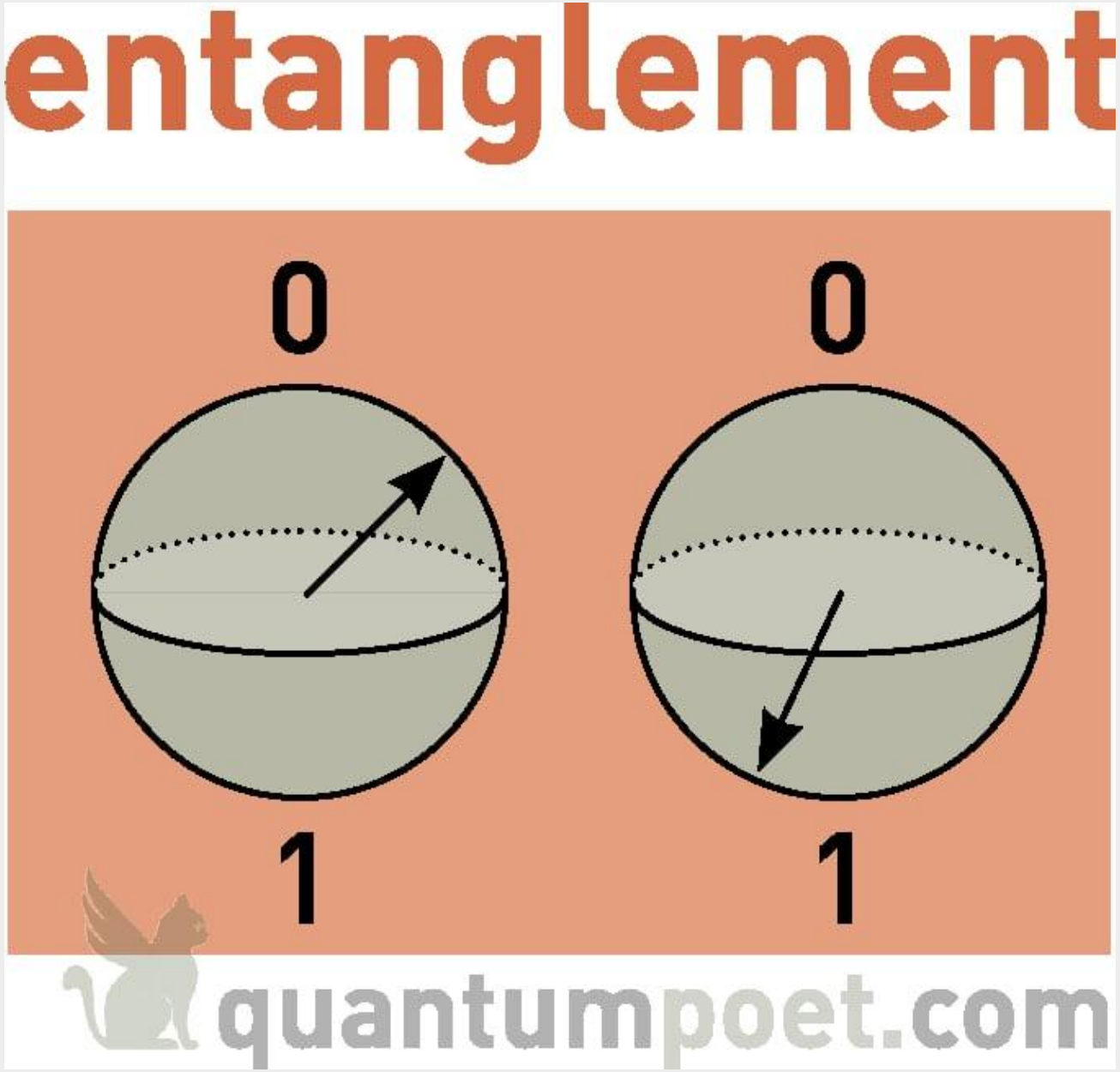
The Physiciatrist...
Sidney Harris



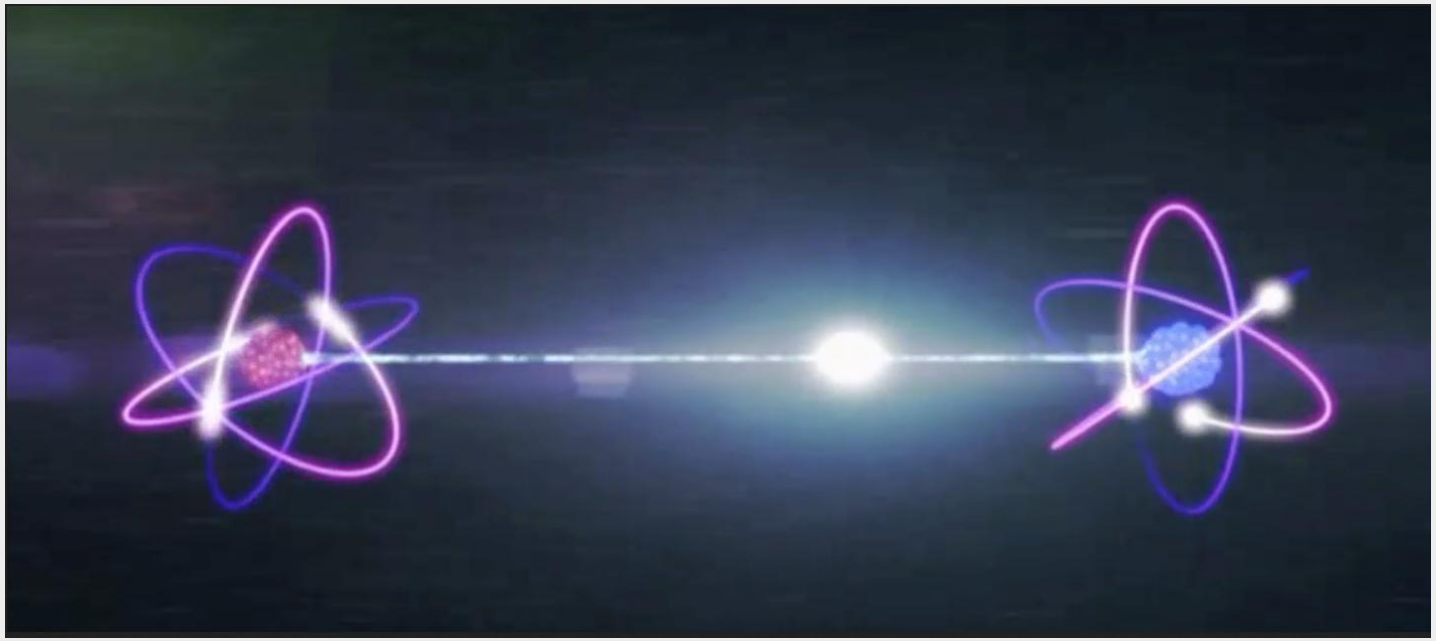


Institute of Quantum Physics
Oswald Huber

Concept 2: Entanglement



Concept 2: Entanglement



In quantum mechanics, entanglement occurs when, **minimally**, two particles pair up in such a way that the quantum state of one particle cannot be determined independently of the state of the other particle(s), irrespective of the distance between the two.

Concept 2: Entanglement

Why and how does entanglement occur ?

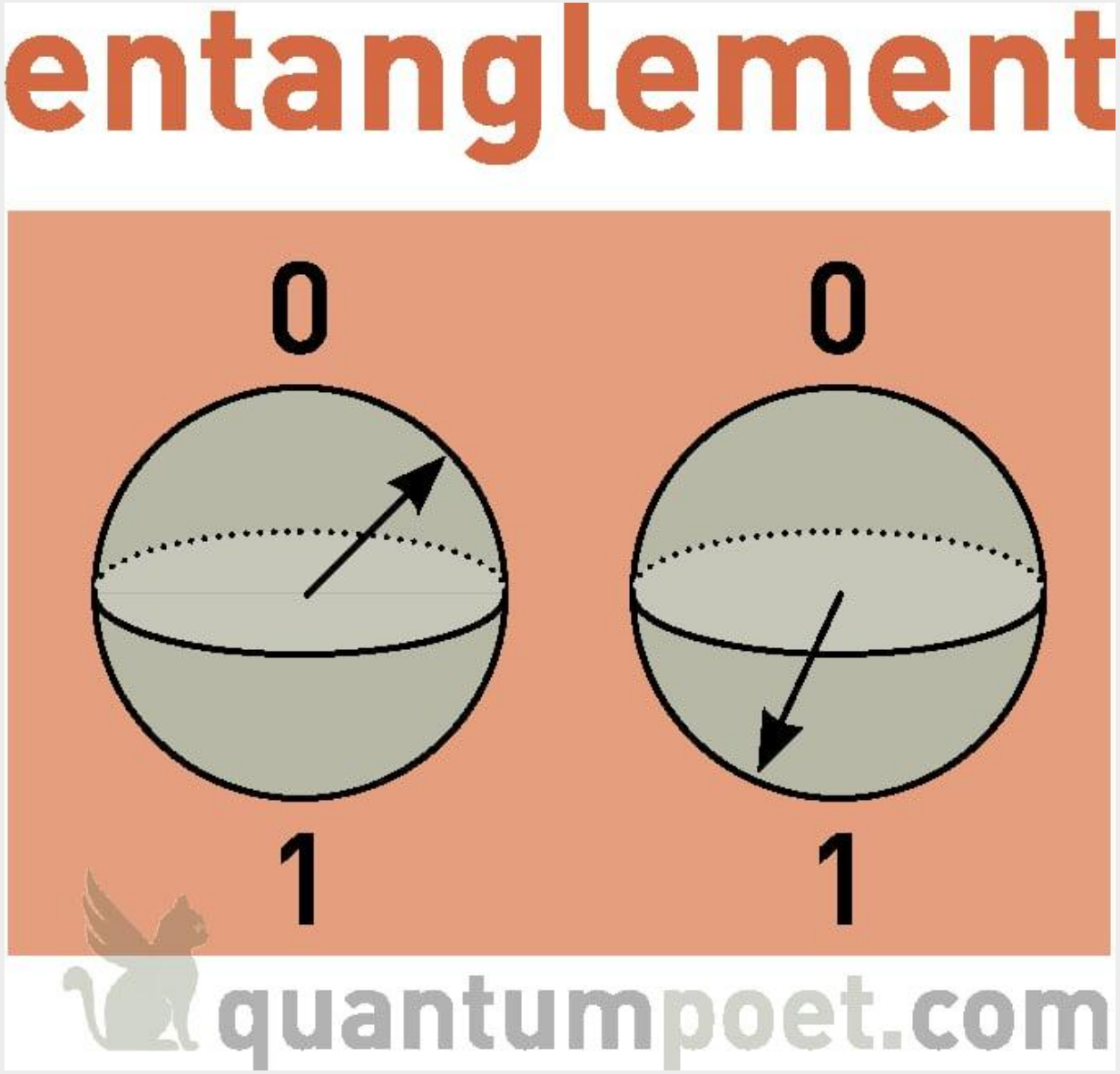
Concept 2: Entanglement

Can be harnessed by quantum computers

Two or more Qubits are entangled to create a **Single Quantum State**

Changing the state of one Qubit **instantaneously** changes the state of the other entangled Qubits

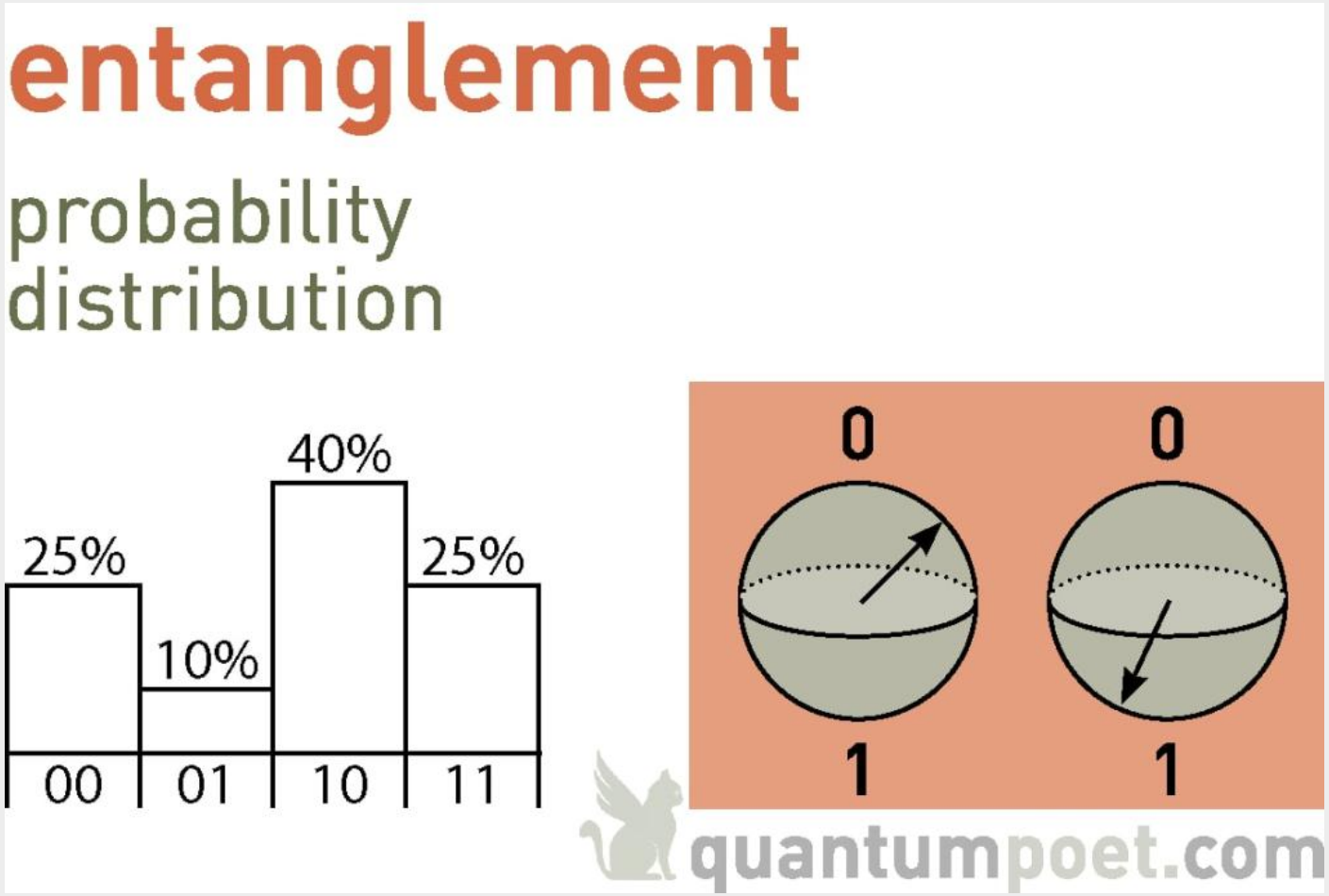
Entangling Qubits can be leveraged to provide "**quantum speed-up**" in quantum computing



Concept 2: Entanglement

Entangling Qubits can provide an **exponential speed-up** in quantum computing

Entangling Qubits can only be measured (remember “collapsing”) based on a **probability distribution** across the Qubits



Concept 2: Entanglement

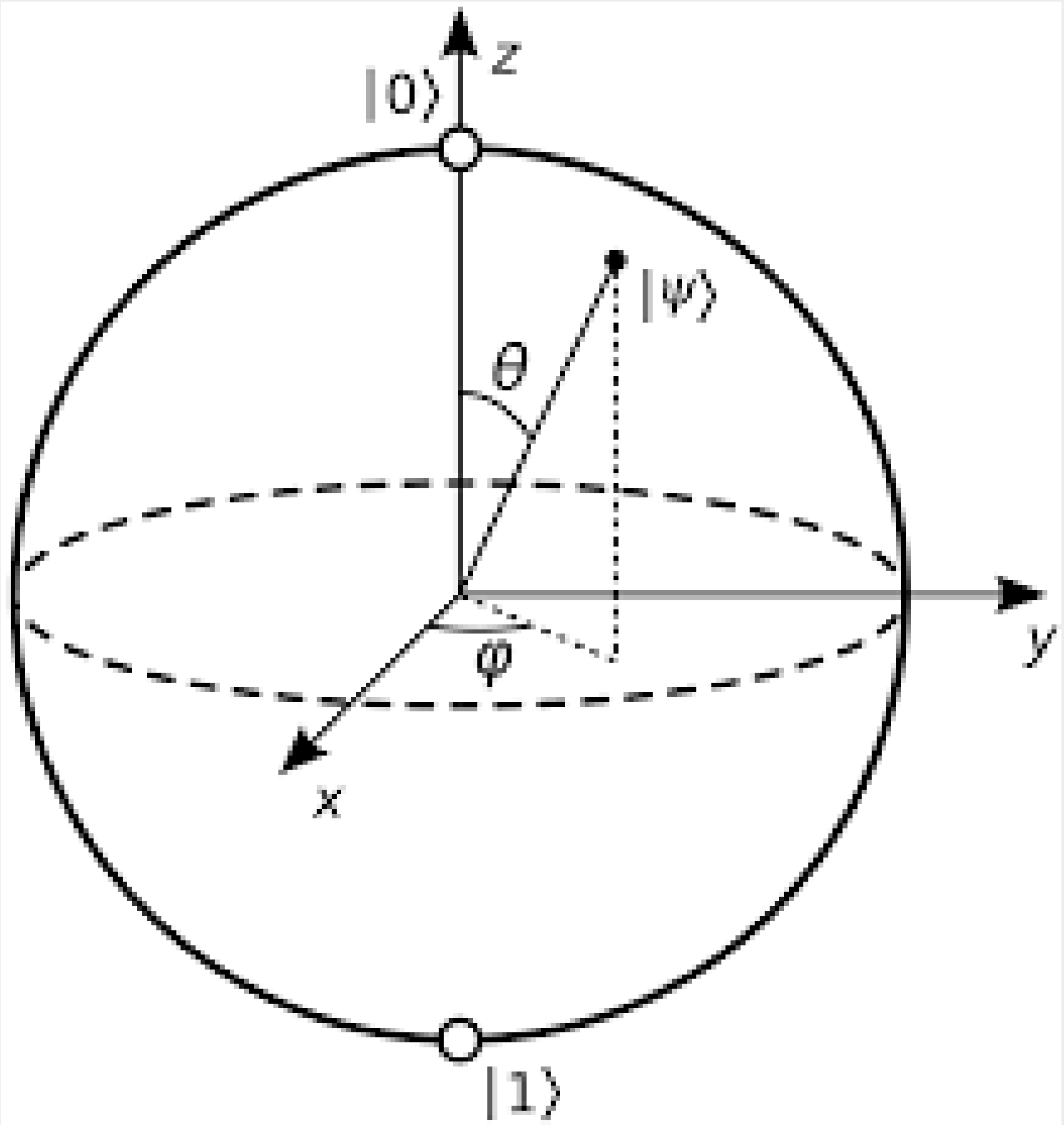
For **one qubit** we have a probability distribution over **two states**.

For **two qubits**, the probability distribution is over **four states**.

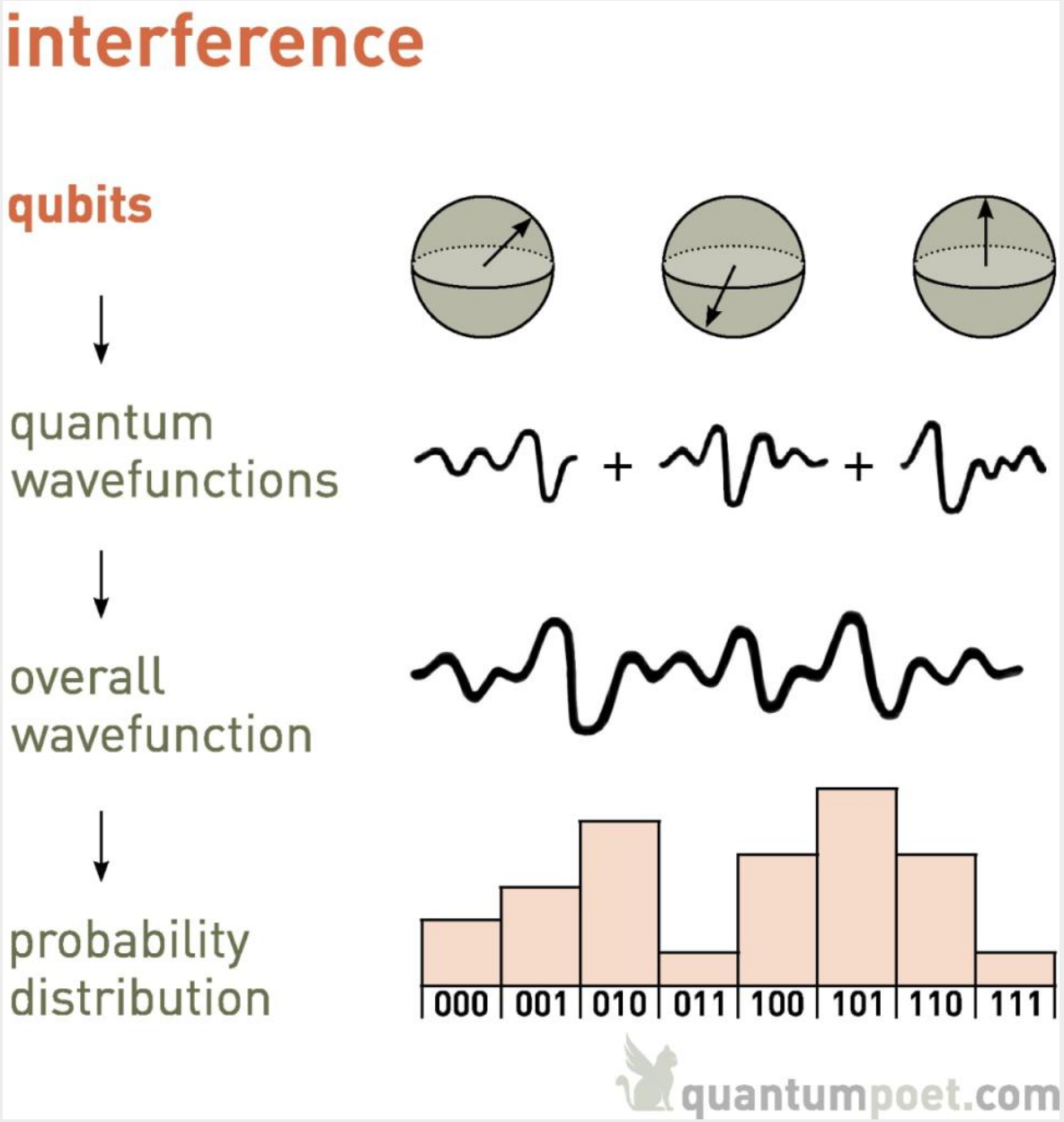
For **three qubits**, it is **eight states**.

…….

In general, for **N qubits**, the probability distribution is over **2^N states.**



Concept 3: Interference



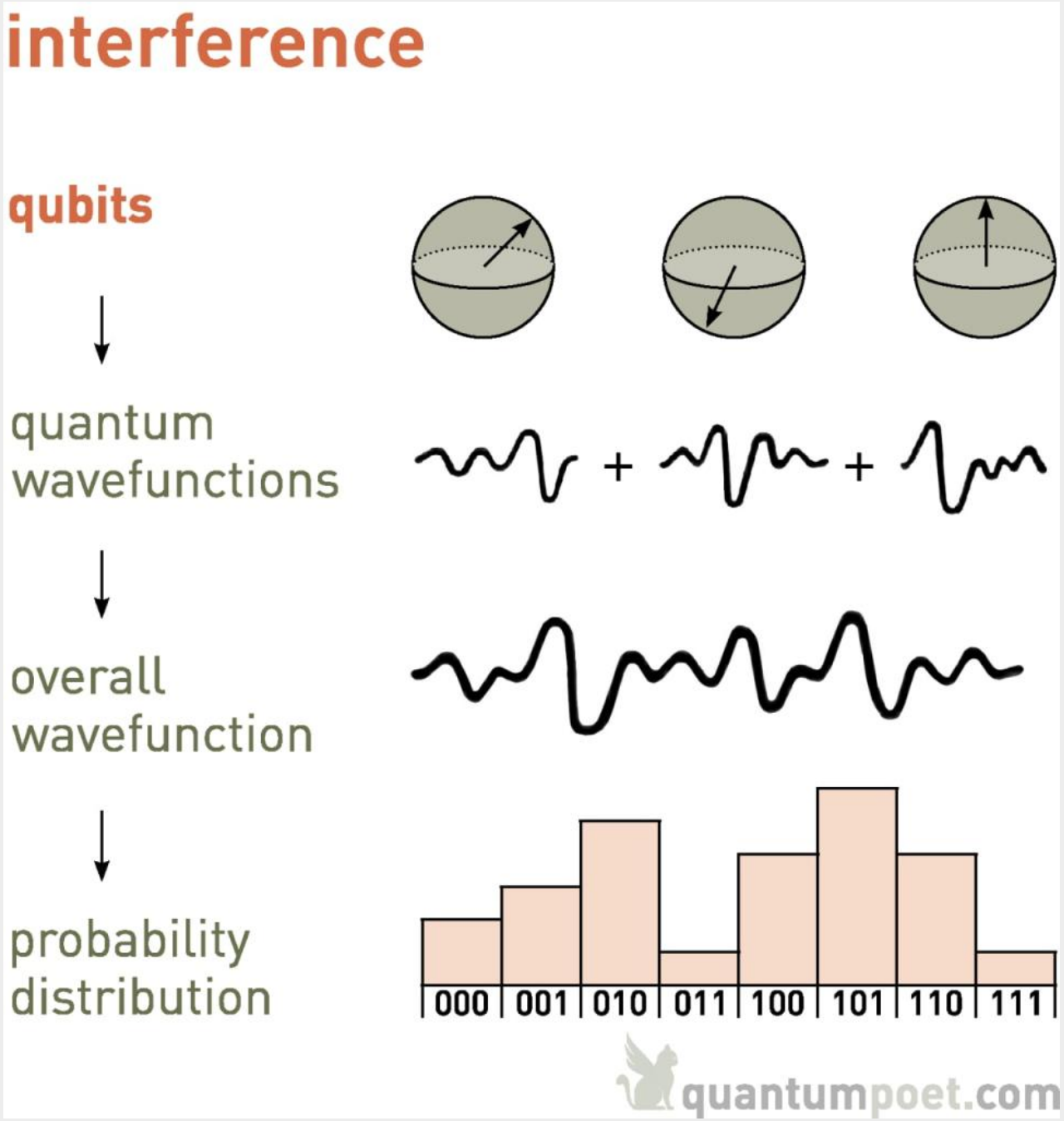
Concept 3: Interference

A **wave function** is the **basic mathematical description** of everything in quantum physics.

A wave function is generally expressed using **polynomials**

To measure the entangled qubits, we add the individual wave functions of each qubit, producing a **single wave function** of a single quantum state.

The adding together of the individual wave functions gives us the **interference pattern**.

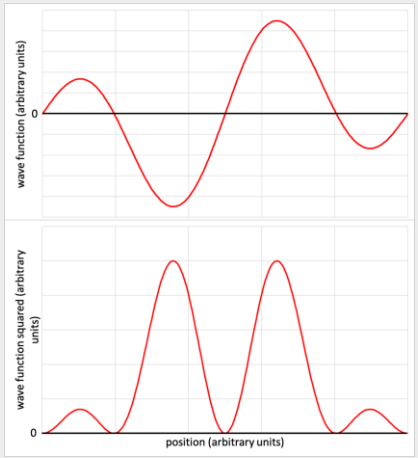


Concept 3: Interference

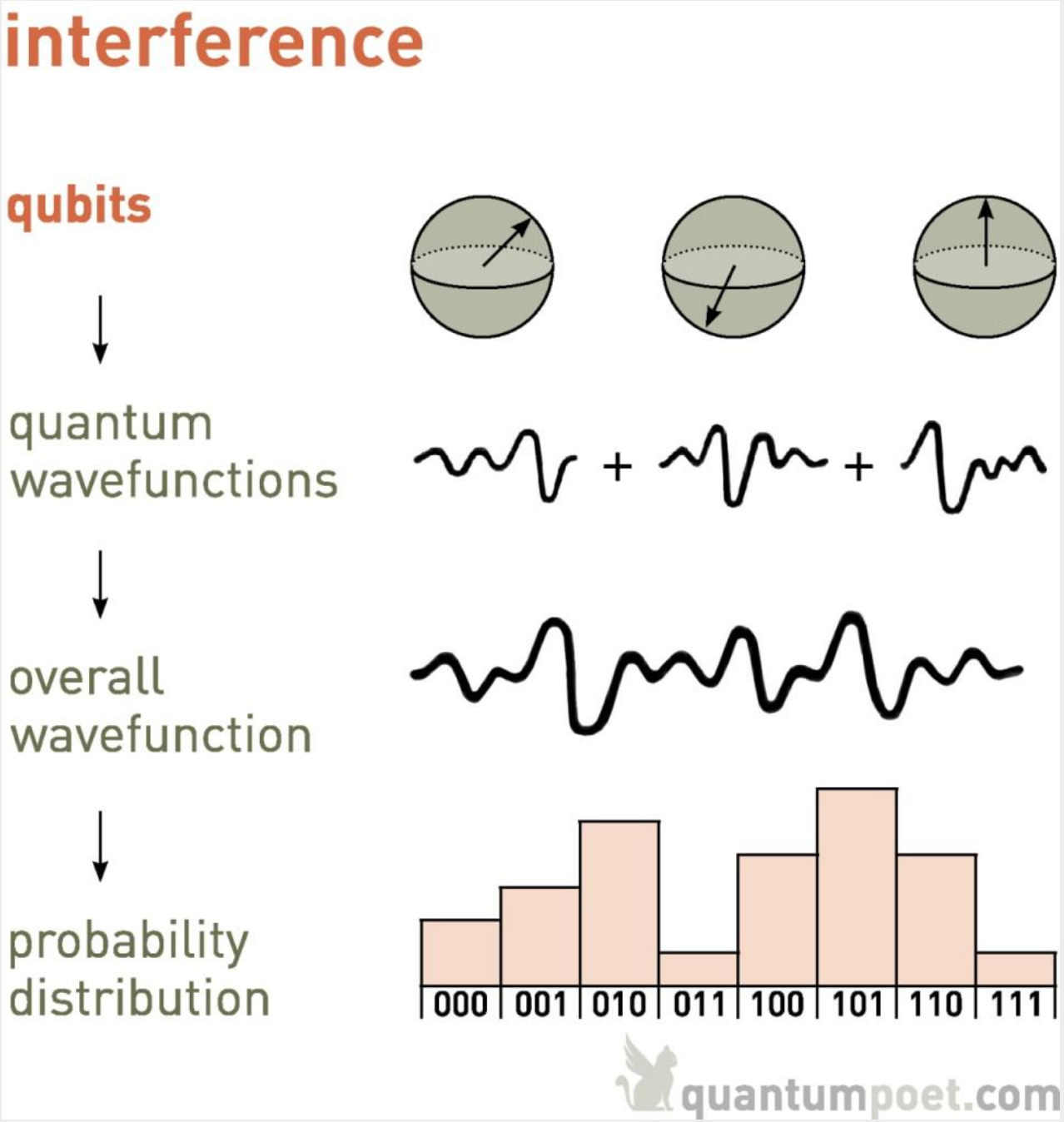
Schrodinger's Equation

$$-\frac{\hbar^2}{2m}\nabla^2\psi + V\psi = E\psi$$

$\Psi(x)$



$|\Psi|^2$ Probability of finding the location of an electron



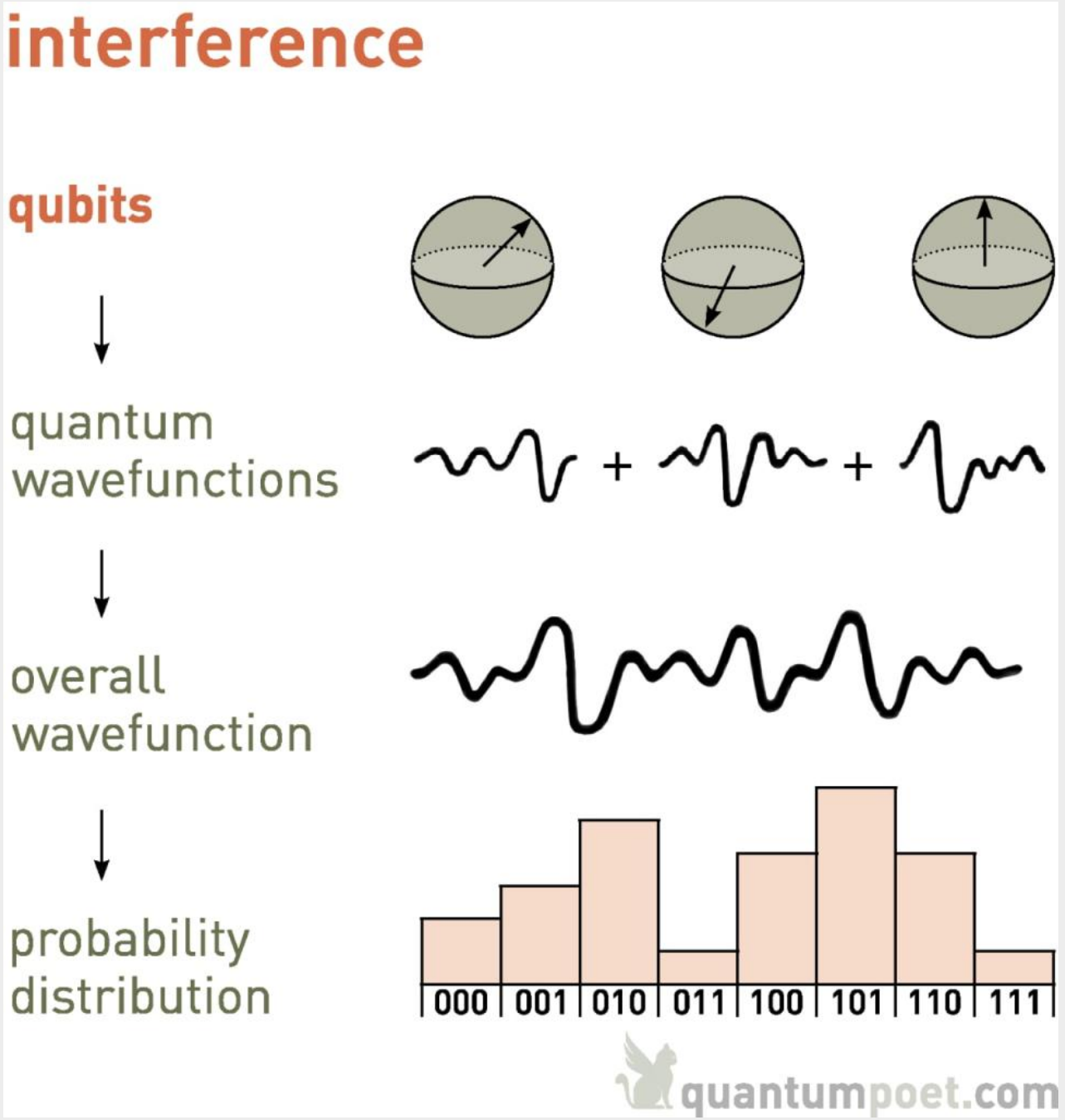
Concept 3: Interference

What is actually in a wave motion ?

Concept 3: Interference

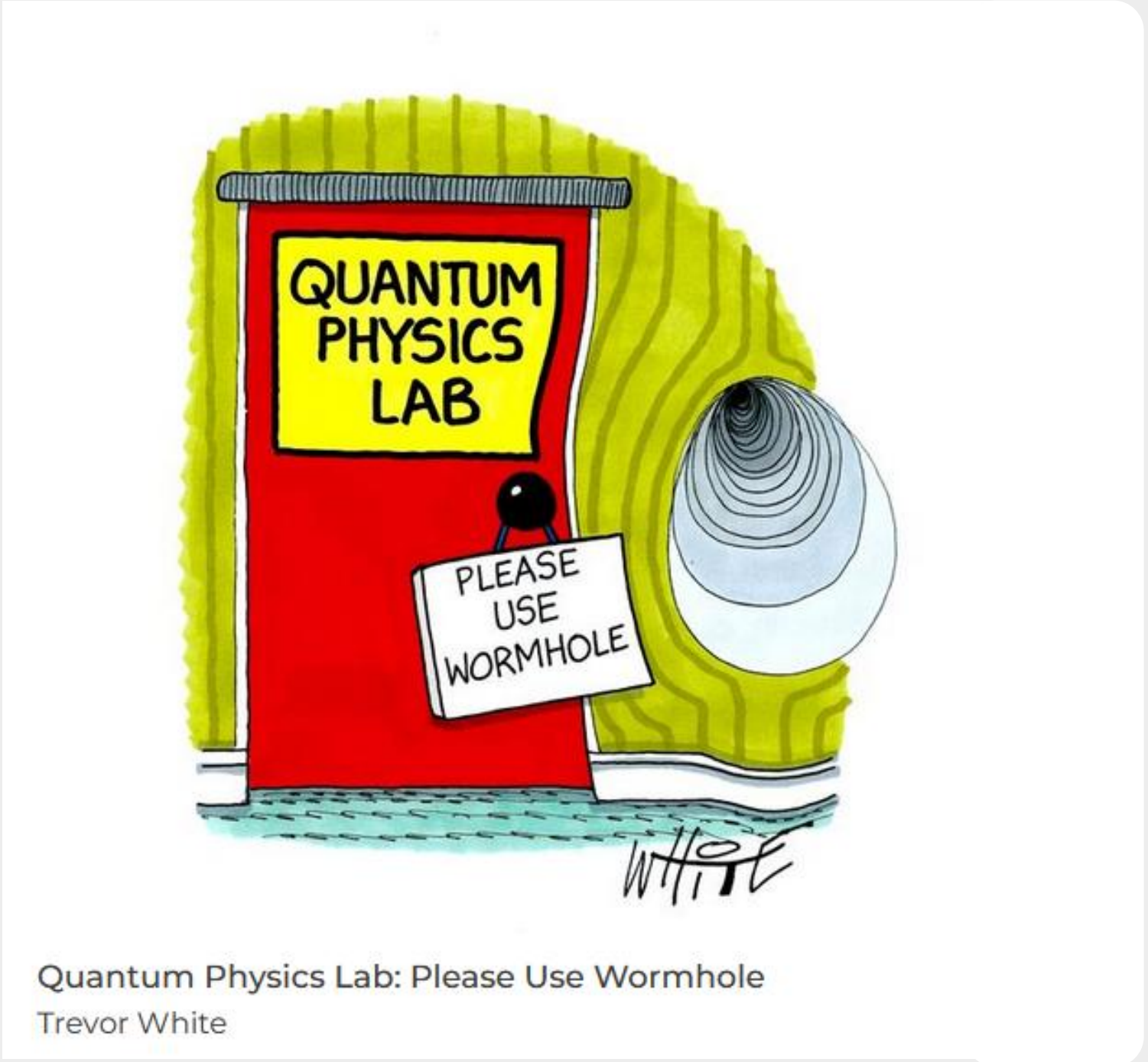
To **increase the probability** of the **correct answer**, leverage a **constructive interference** (where two wave crests add up, producing a larger wave).

To **decrease the probability** of an **incorrect answer**, leverage **destructive interference** (where two waves cancel each other out).



Concept 3: Interference

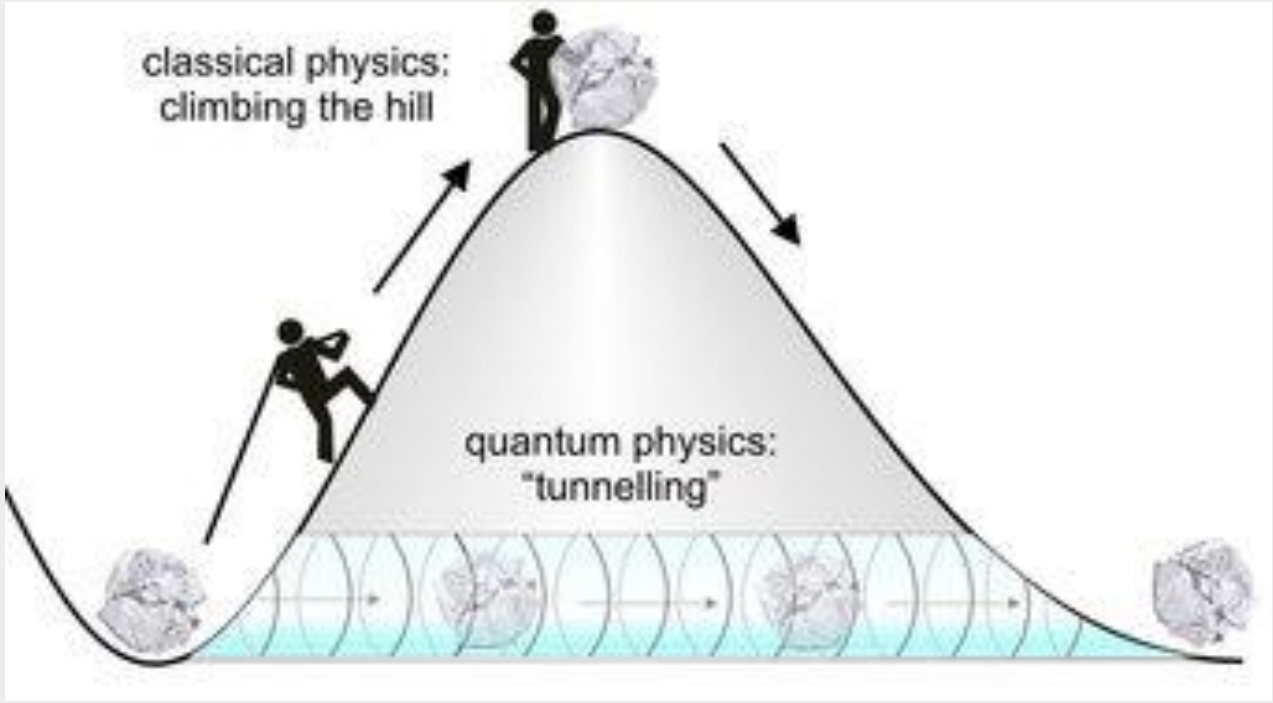
Concept 4: Tunneling



Quantum Physics Lab: Please Use Wormhole
Trevor White

Concept 4: Tunneling

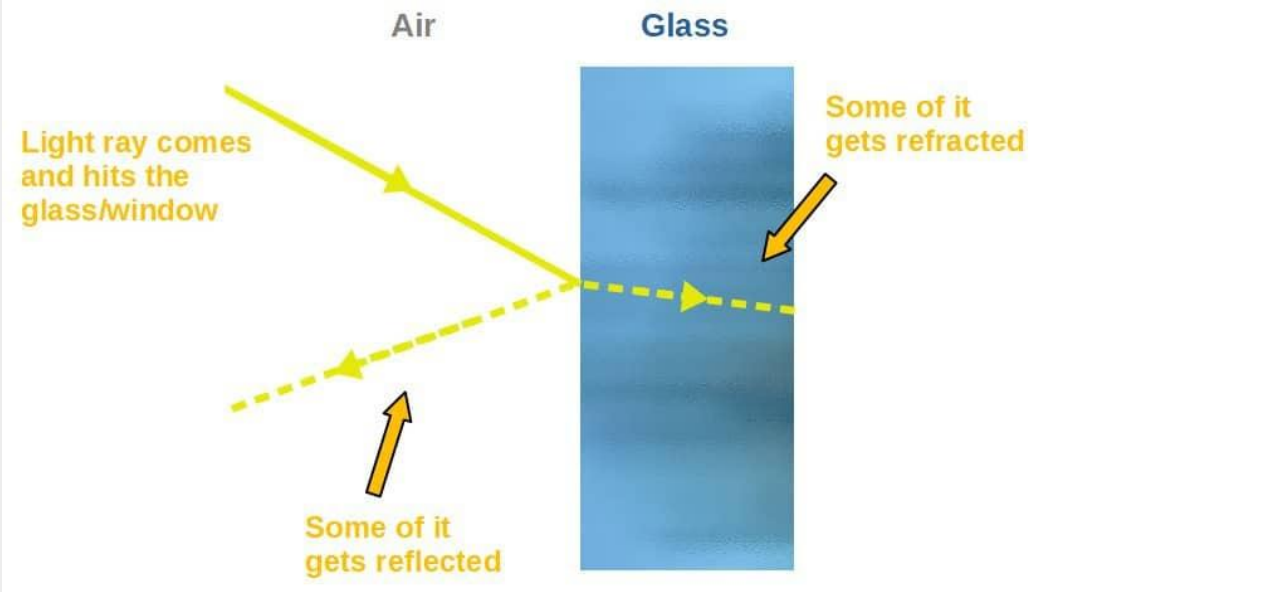
Phenomenon in which an object such as an electron **passes through** an **energy barrier** that, according classic mechanics, should not be passable due to the object **not having sufficient energy** to pass or surmount the barrier

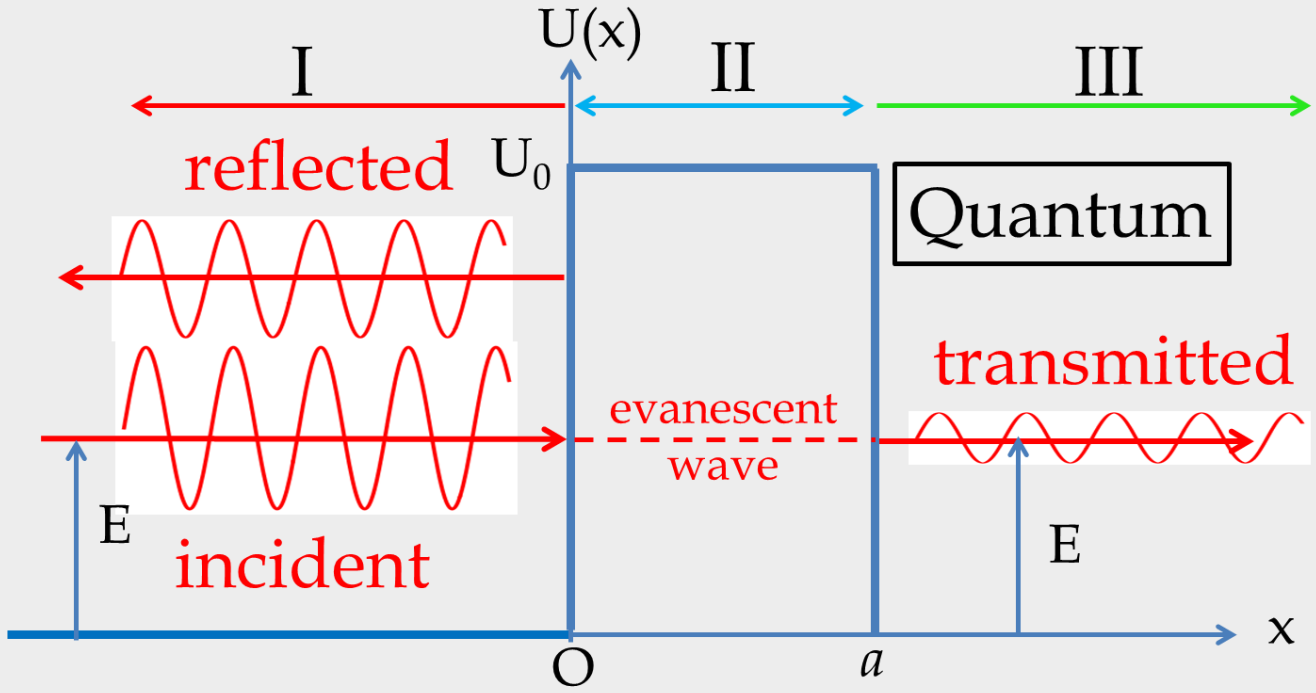


Concept 4: Tunneling

A lot of the power comes from this phenomenon

This drastically **reduces** the **energy** required to accomplish computing tasks





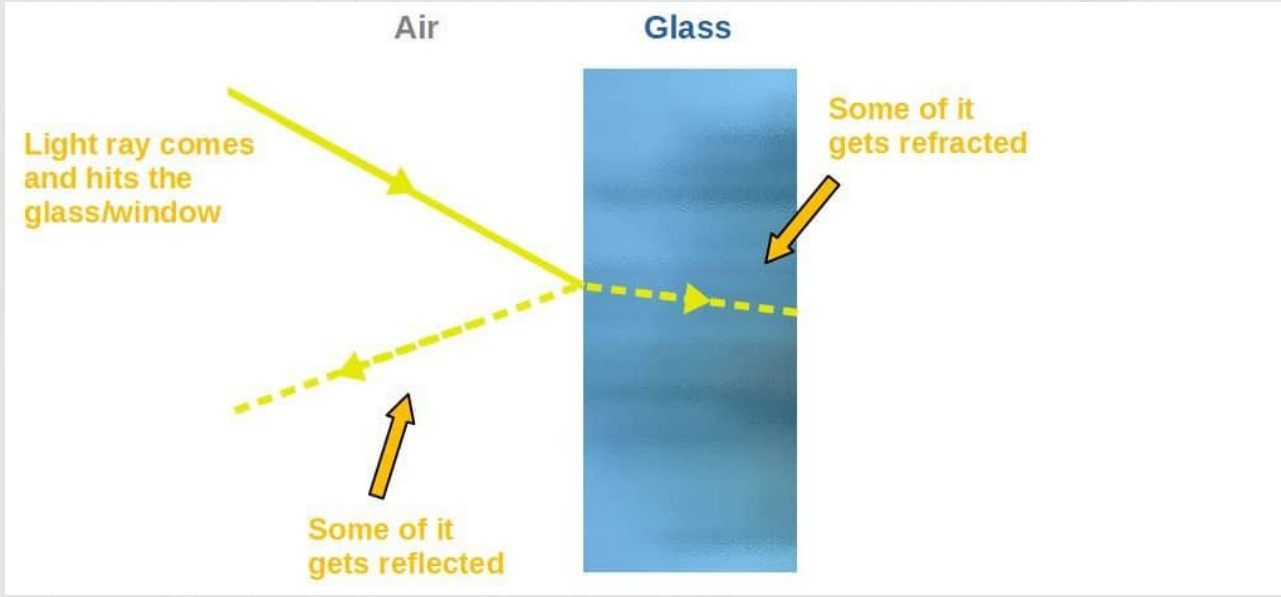
Concept 4: Tunneling

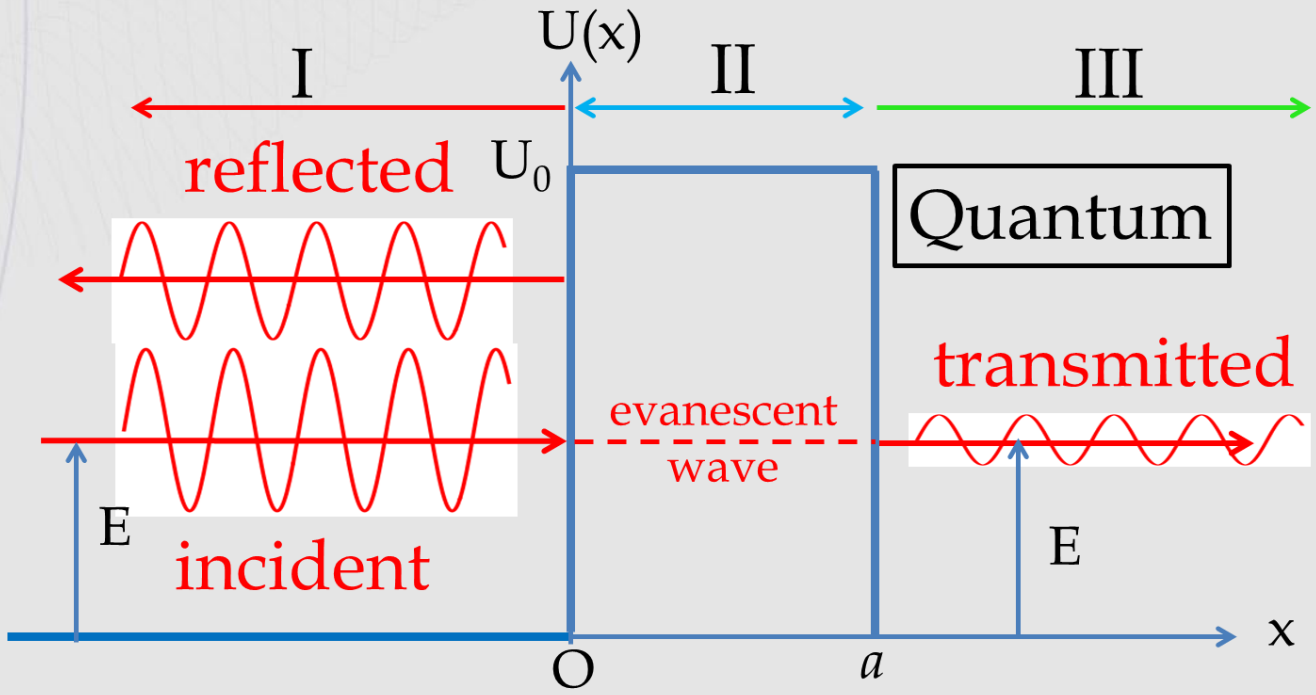
Nuclear Fusion in Stars: Tunnelling allows protons to overcome their electrostatic repulsion, allowing the Sun to produce energy.

Radioactive Decay: Alpha particles tunnel out of the nucleus.

Scanning Tunnelling Microscopy (STM): A tool that uses electron tunnelling to image surfaces at an atomic level.

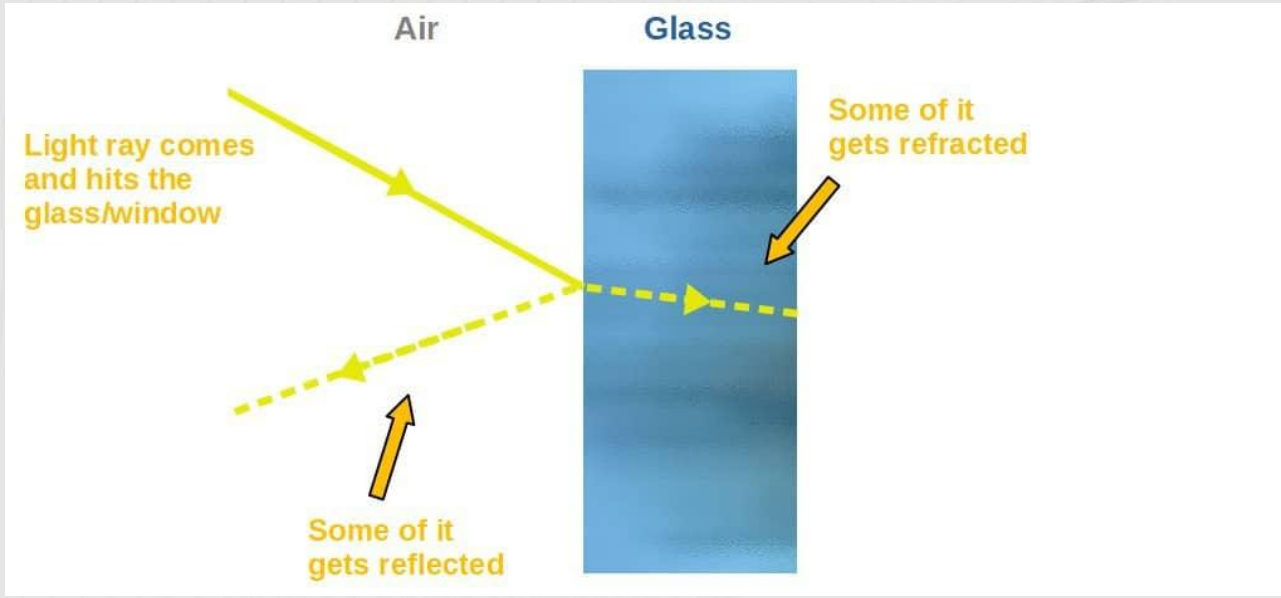
Electronics: Used in tunnel diodes and flash memory.

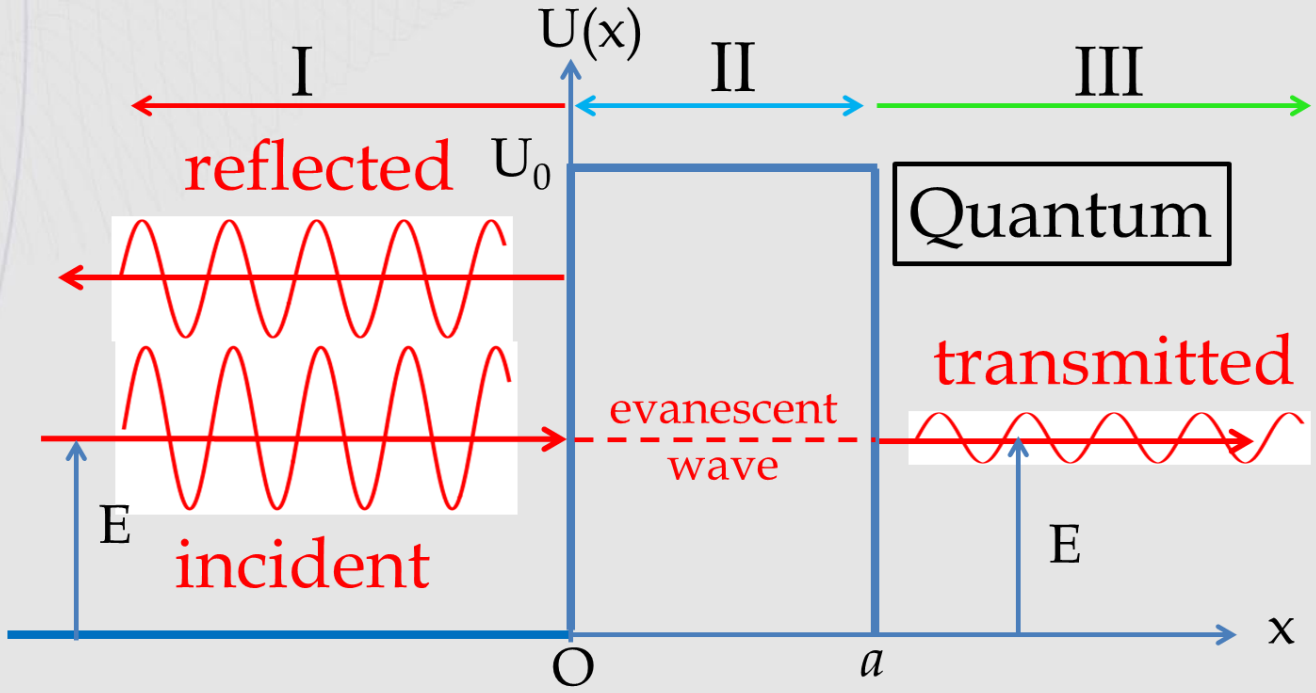




Concept 4: Tunneling

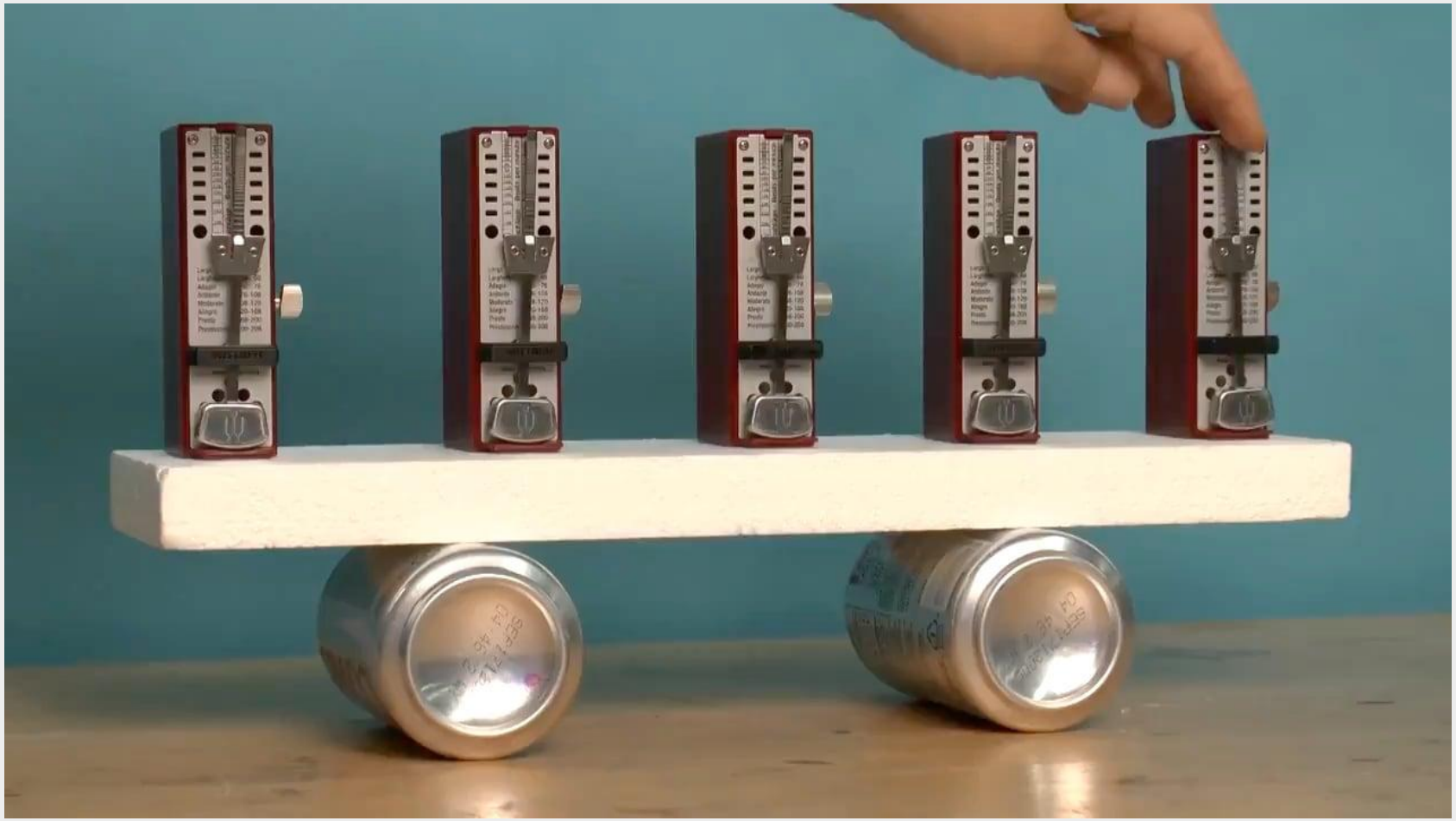
The **wave function** represents the **probability distribution** of **finding a particle**. When this wave function encounters a potential barrier, it doesn't drop to zero instantly but instead decays inside the barrier. If the barrier is thin enough, the wave function has a non-zero value on the other side, representing a chance that the particle will appear there.





Concept 4: Tunneling

Concept 5: Spontaneous Synchronization

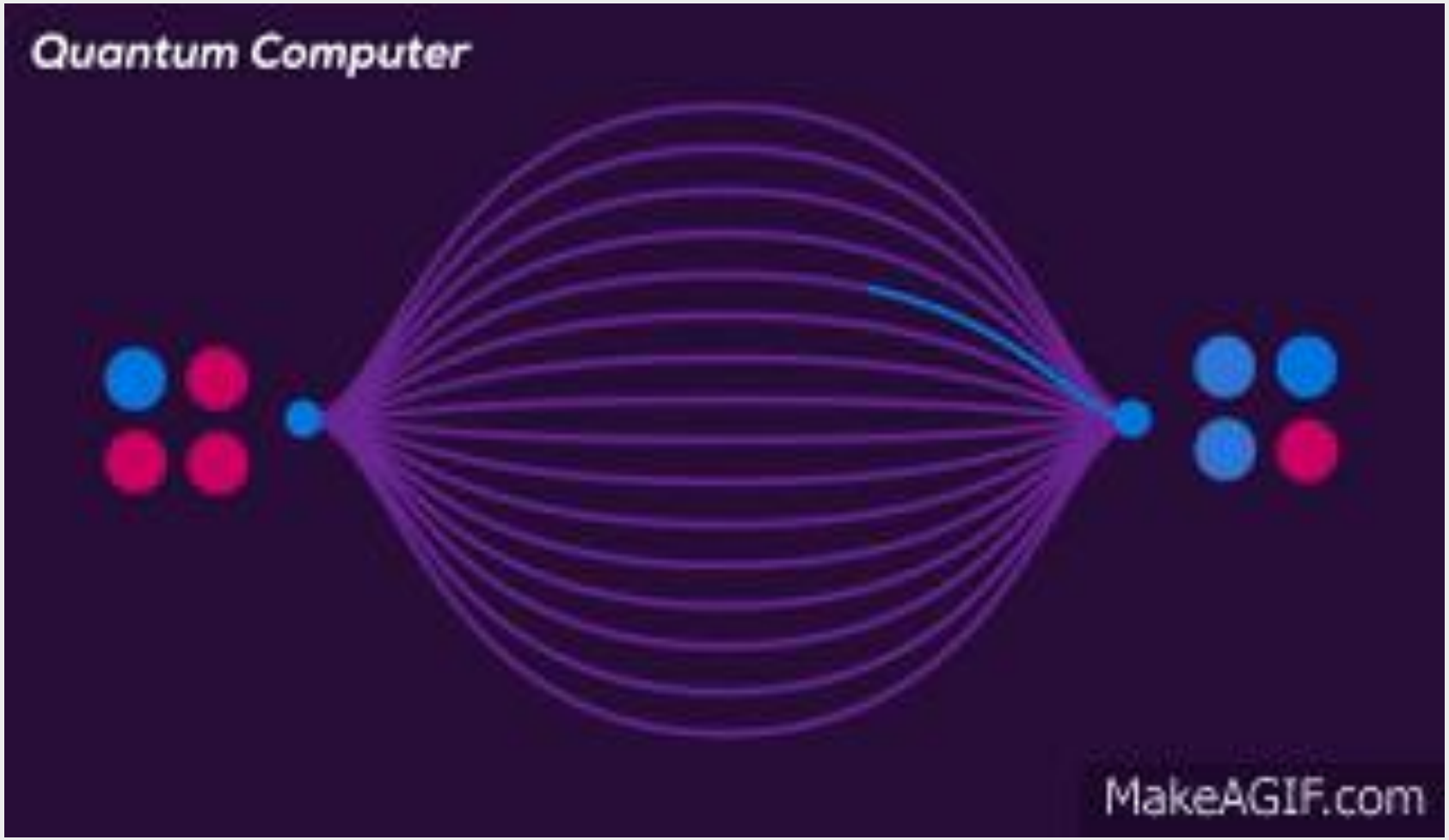


Concept 5: Spontaneous Synchronization

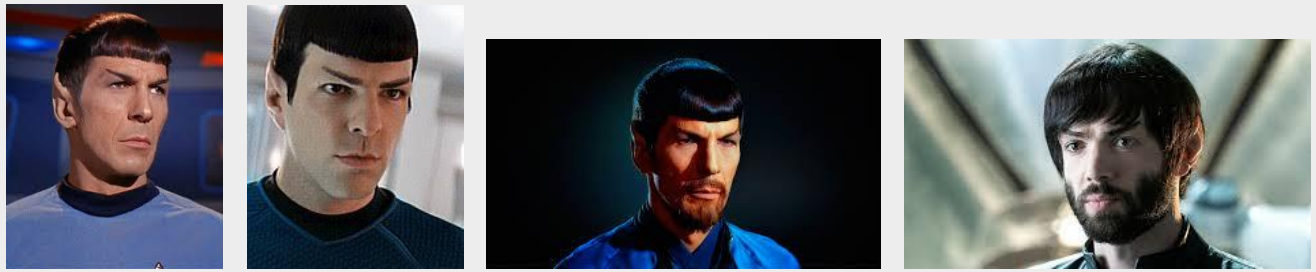
What happens when independent particles are incorporated into a single system

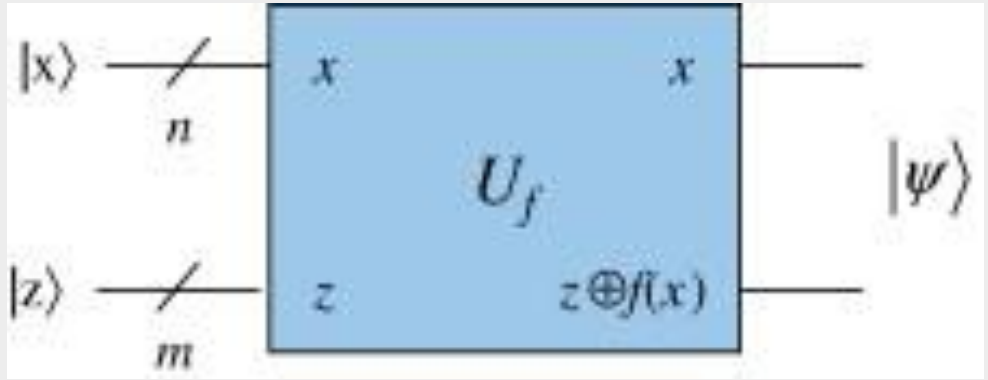
https://www.youtube.com/watch?v=Aaxw4zbULMs

Concept 6: Quantum Parallelization



Concept 6: Quantum Parallelization

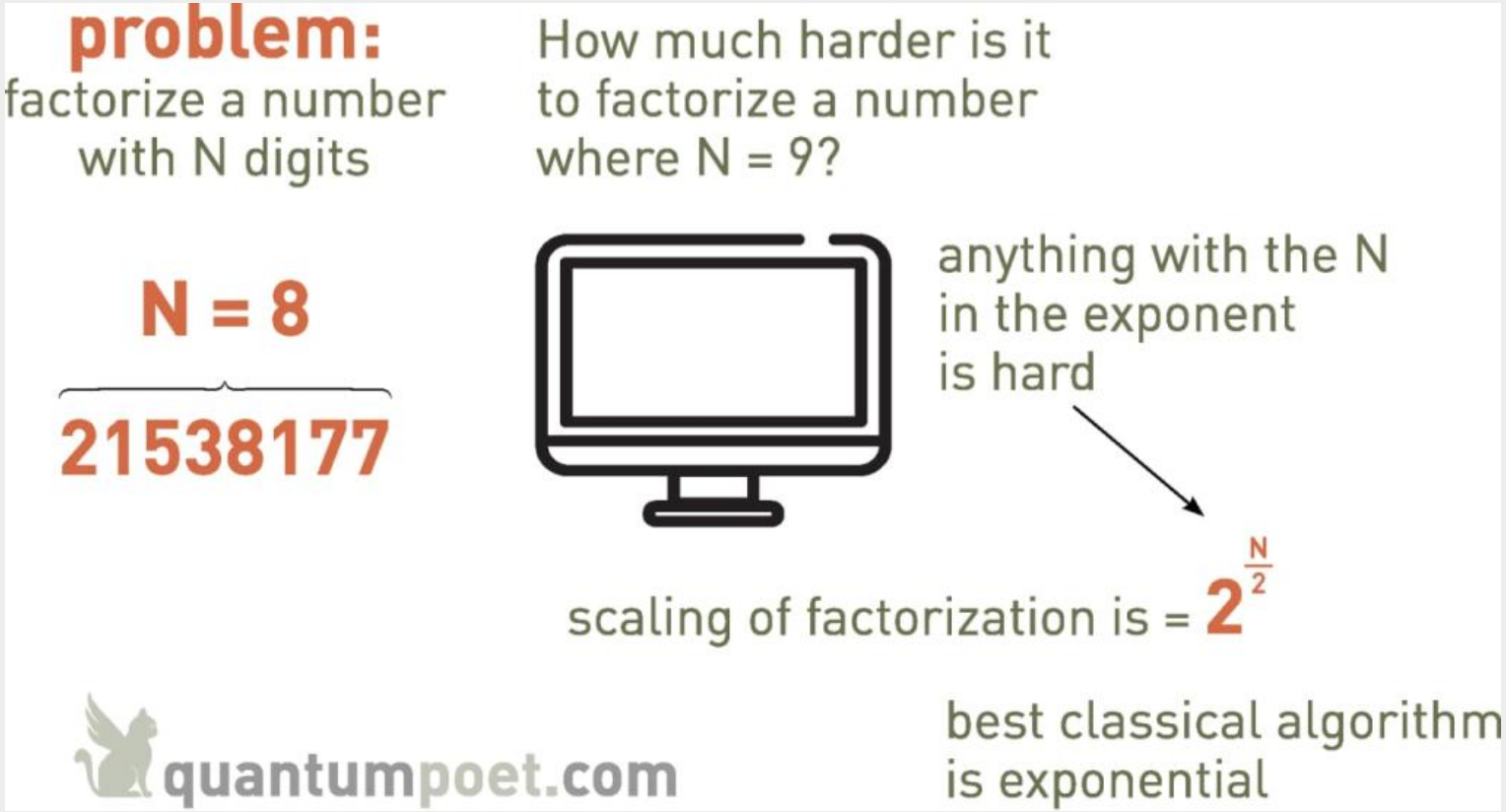




Think of having **N parallel universes** – all running whatever computation at the same time – however, there's a limitation – can only be in one universe at a time – Remember ! At the moment of observation – the qubit ends up in a "collapsed" state

The solution gets into "quantum" **chip level design** – where the second input becomes a "function" (or "influenced") by the first – and – whether the function f(x) is "balanced" or "constant"

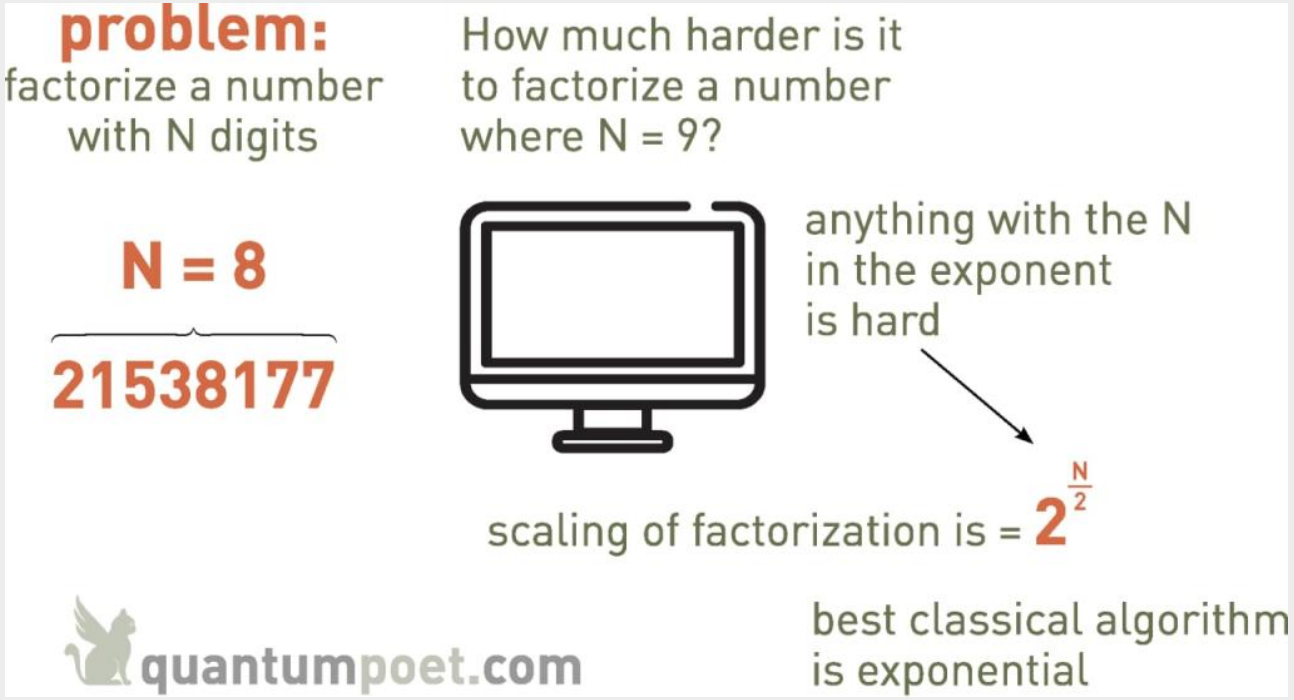
Concept 7: Algorithms

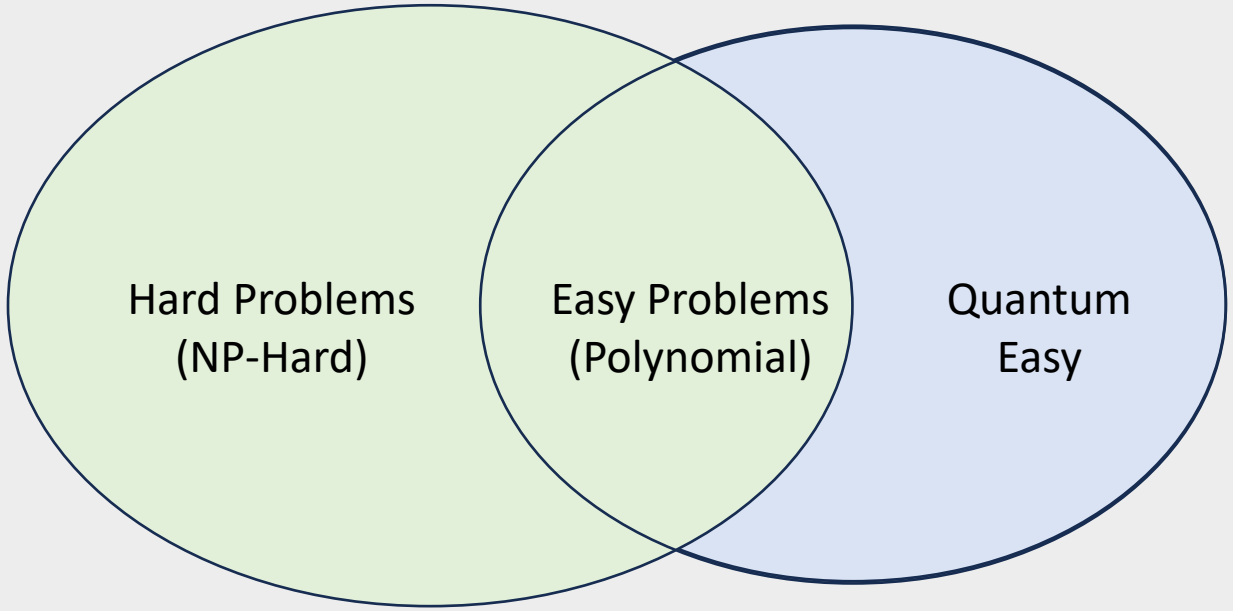


Concept 7: Algorithms

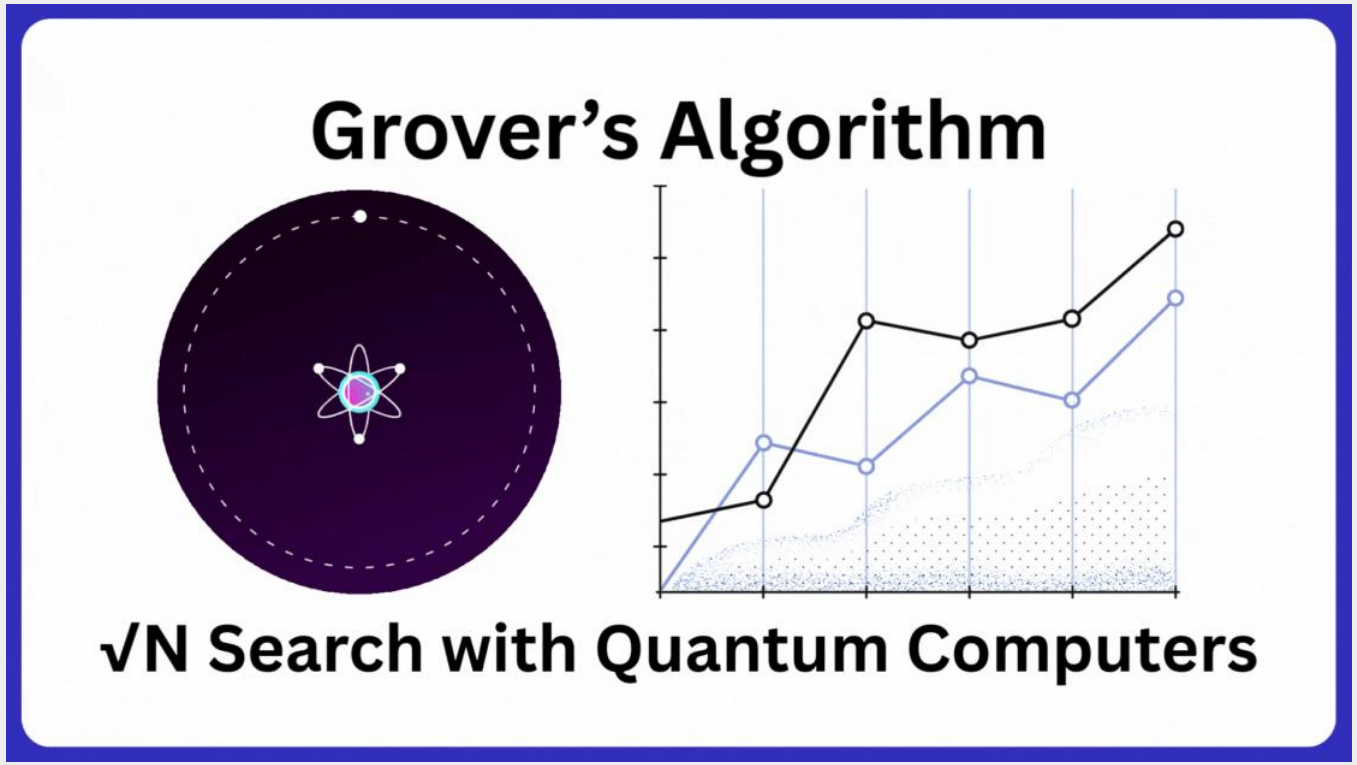
The objective is to develop **quantum algorithms** to **solve intractable problems** (problems which are unsolvable on classic computers) – NP and NP-Hard problems.

Prime factorization of very large numbers is an intractable problem because the search base of all possible integers is very large. Which is why prime factorization is used as the basis of present-day cybersecurity encryption.





Concept 7: Algorithms – Example: Grover's Operator



Quantum Search Algorithm

Allows for searches on **unstructured**, **unordered** data (O(sqrt{N})) queries instead of the (O(N)) expected from classical search methods.

Very good at "sweeping away" all incorrect answers

Pulling This Together

N Qubits

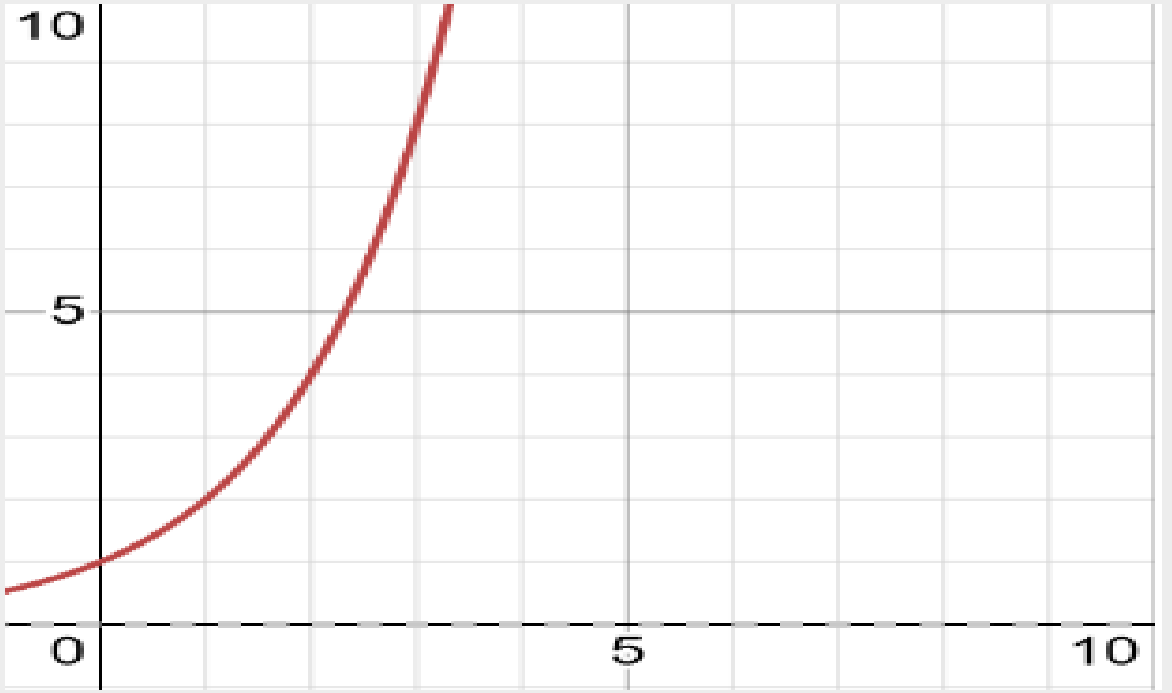
2^n Compressed Numbers

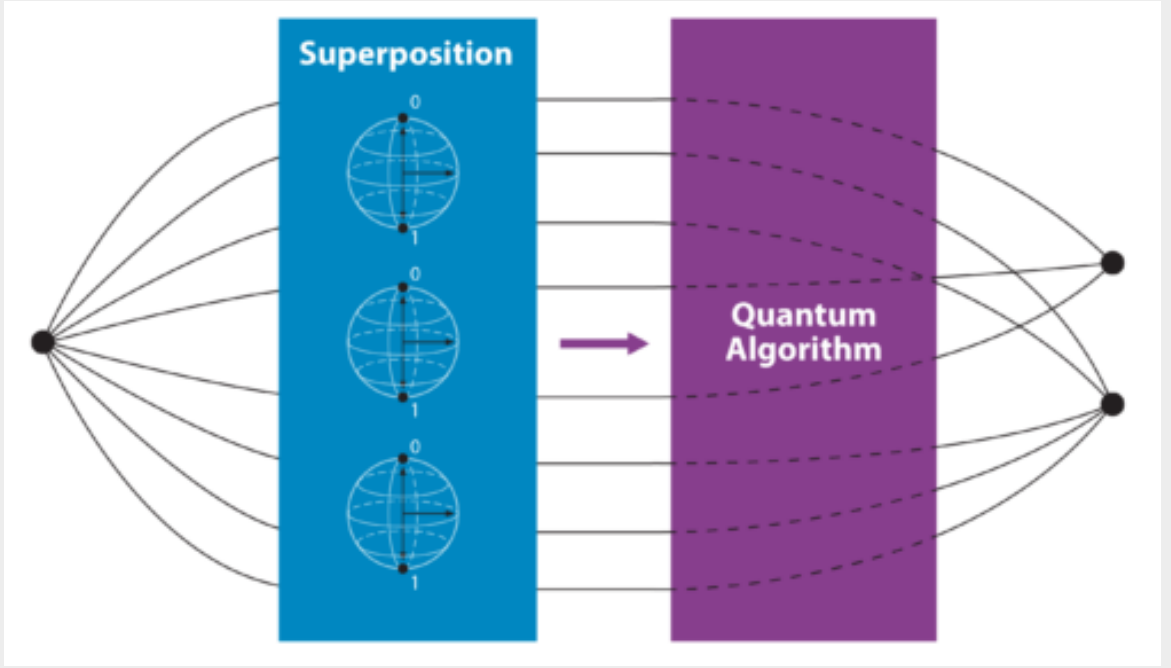
Think of a reasonable number of Qubits like N = 300

$2^{300} = \sim 10^{90}$

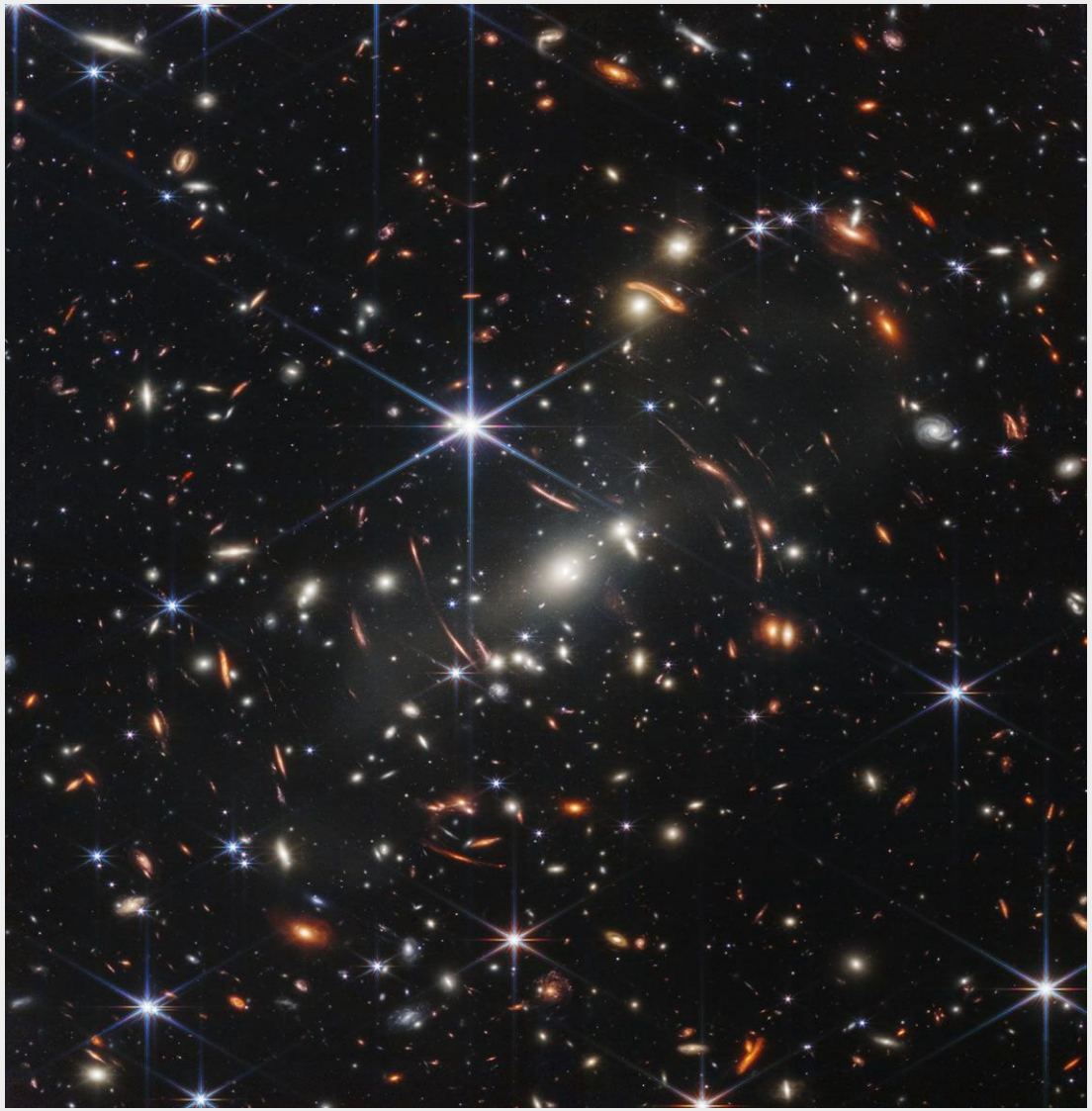
Leverage Linear Quantum Mechanics

Apply algorithms to Superposition





Perspective



Total Number of storage **bytes**
in the world **~10^{21}**

2^{300} = ~10^{90}

Total Number of **atoms**
in the universe **~10^{82}**

Use Cases – Why do we care ?

Use Cases – Traveling Salesman – Best Route

Ising Machine using Ising model

Partnership building the largest in the world

Caltech Department of Applied Physics and materials Science

NTT Research Physics & Informatics Lab

Use Cases – Traveling Salesman – Best Route

Nature likes to optimize energy naturally

Examples: Think of fish swimming or birds flying in a “V” formation or fireflies “blinking” at the same time

Spontaneous Synchronization

Ising Machine uses a collection of spinning particles – one particle for each city – eventually they will all synchronize on the most efficient path
They are calibrated to the distance (or any cost formula) between the cities

Drug Development

New classes of antibiotics to counter the emergence of multidrug resistant bacterial strains

Sustainability

Global Farming

Solar & Wind Power

Natural Resources

Weather

CERN

Use particle physics (quantum computing) to research particle physics

Entangled particles – don’t know why this happens

Start-up Issues

New discoveries nano-seconds after collision

AI

Combine the power of Quantum Computing with GenAI

Hardest Machine Learning problems

Ability to consider millions of options in parallel – in seconds

Quickly “sweep away” bad options

Self-learning programs – look at all learning paths – simultaneously – in seconds

Proactive not Reactive

Security Risk

Traditional Computer – Check one password at a time – could take millions of years

Quantum Computing – Check all passwords simultaneously – Use Grover's Operator to "sweep away" all incorrect results – takes seconds

What's left ? The correct password

Q-Day – 2030

Security Risk

Traditional Computer – Check one password at a time – could take millions of years

Quantum Computing – Check all passwords simultaneously – Use Grover's Operator to "sweep away" all incorrect results – takes seconds

What's left ? The correct password

Q-Day – 2030

There are **quantum-based technologies available today** to protect from the risk of quantum computing in the future. Post-Quantum Cryptography, for example, being integrated into Blockchain protocols today. This helps protect cryptocurrency, for instance.

Challenges


PAUL NOTH
"Well, your quantum computer is broken in every way possible simultaneously."


CG177162
YOU'RE SUPPOSED TO TURN IT OFF BEFORE YOU FIX THE PARTICLE ACCELERATOR, BOB.
©2019
COVERLY
SPEEDBUMP.COM
4-18 DIST. BY CREATORS

Challenges - Size

Size

Approximately 1.5m wide and 6m long – not very practical in personal devices or even in Commander Data

Challenges - Cost

Cost

$10K per Qubit

Starting Cost to manufacture: $5M

Realistically - $15M (D-Wave 2000Q)

$Bs depending on the size of system

Challenges - Technology

Technology

Circuit quality which allows Ks->Ms of gates

Running between 5K-10K now

Hoping Ms by 2030

Fault Tolerance Improvements

Concept of Logical Qubits

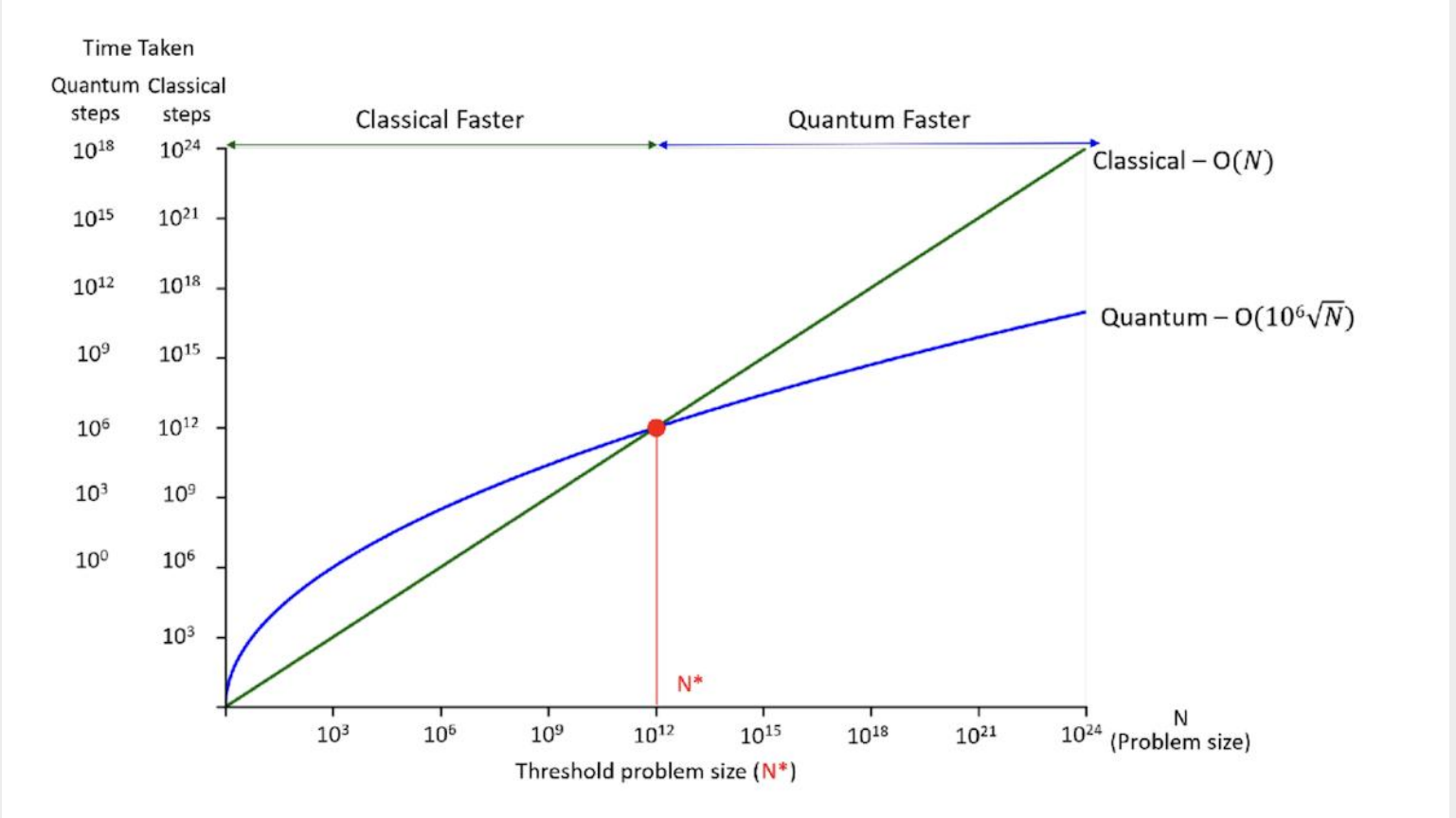
Q Day - 2030

Challenges – Workloads - Classic Computing vs Quantum Computing

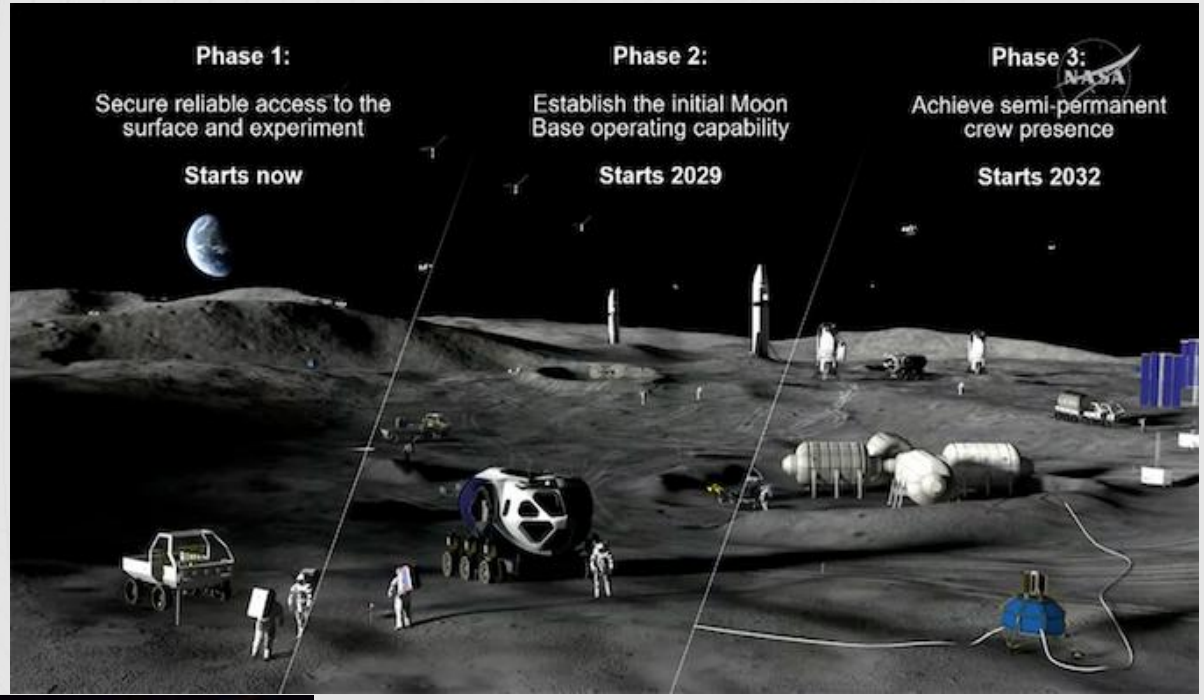
There are situations where quantum computers will be slower than traditional computers

Lots of variables and lots of steps are the sweet spot for a quantum computer

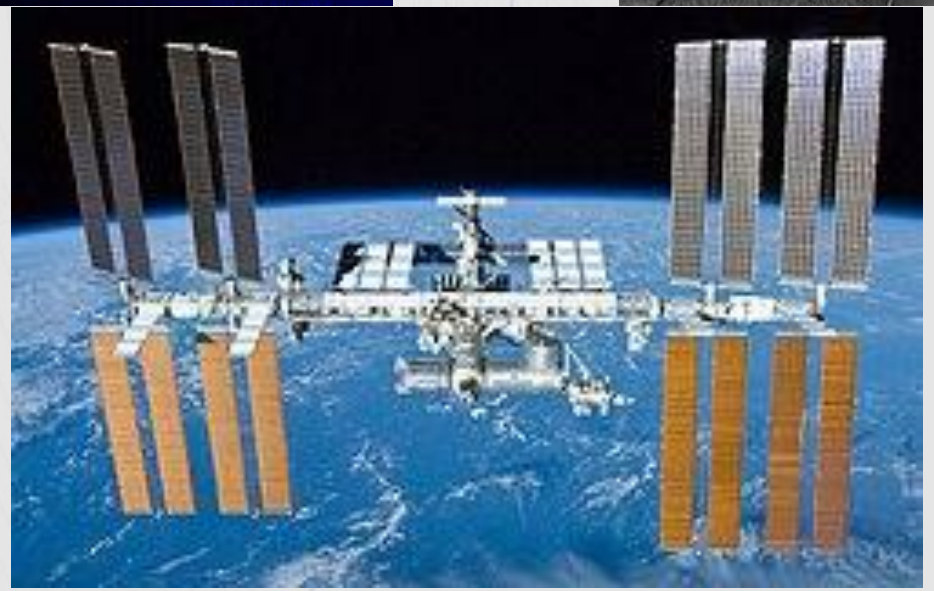
When do we use what ?



Potential Future Directions



NASA's Cold Atom Lab since 2018



Artemis 2 Mission in 2026

Photonic Quantum Processor launched in 2025

Fundamentals and Potential of Quantum Computing

Les King
les@idug.org
May 2026
CCDUG – Toronto
Session: ZMISC05