CSS/ENG
ASSOCIATION

Presented by Sergi, Aren & Michal

Beyond Binary

Limits of Classical Computing

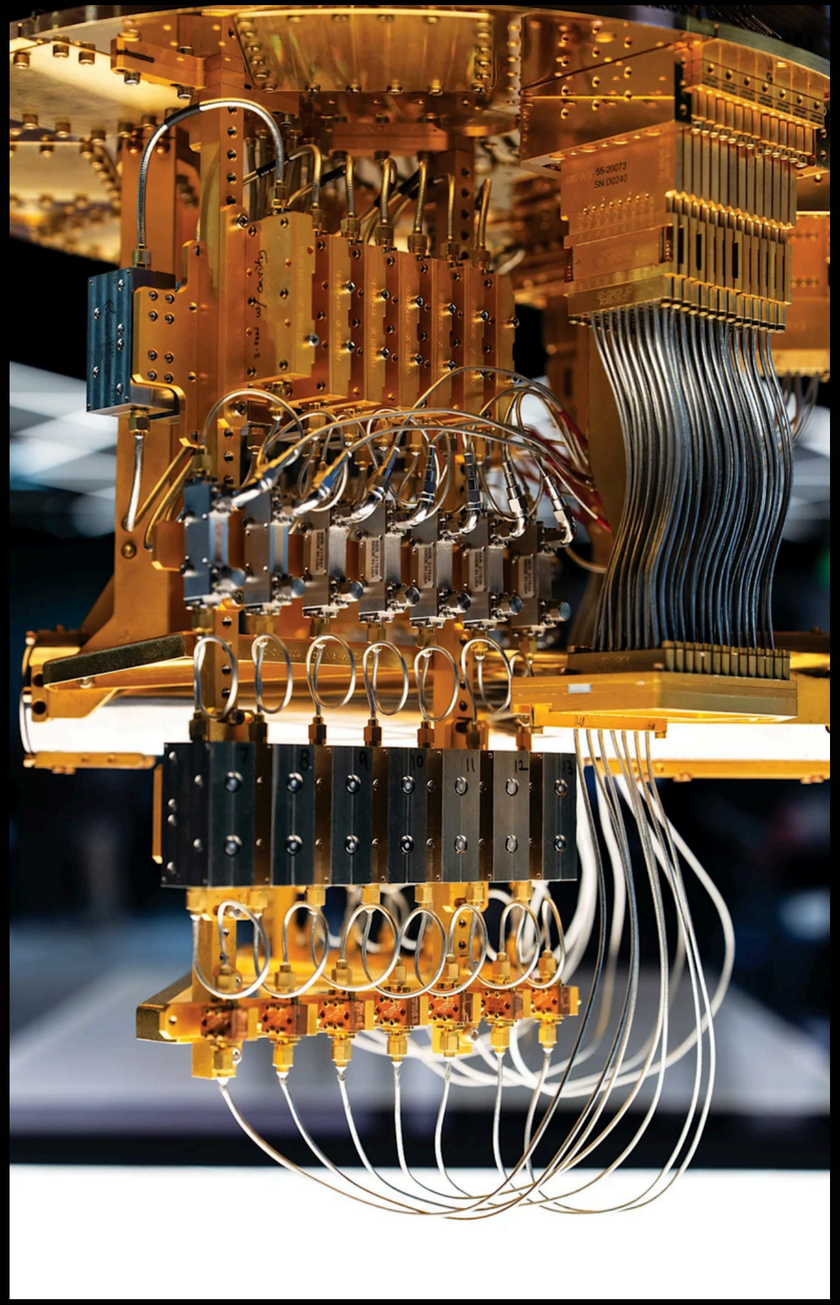
Classical computers operate using bits, which are strictly binary. They exist as either a zero or a one.

Every photograph, video game, and algorithmic calculation you have ever interacted with is built on this deterministic foundation.

When classical computers face highly complex probabilistic tasks, such as simulating molecular structures or factoring massive prime numbers, they are forced to calculate every possible outcome sequentially.

As the variables increase, the time required to brute force a solution scales exponentially, eventually requiring thousands of years of processing time.

Enter the Qubit



Quantum computing discards the standard bit in favour of the quantum bit, or qubit.

Instead of relying on standard electrical voltages, qubits are built using subatomic particles like electrons or photons.

By harnessing the principles of quantum mechanics, these particles are not restricted to existing as just a zero or a one.

They can exist in a fluid state representing a combination of both possibilities simultaneously until they are measured.

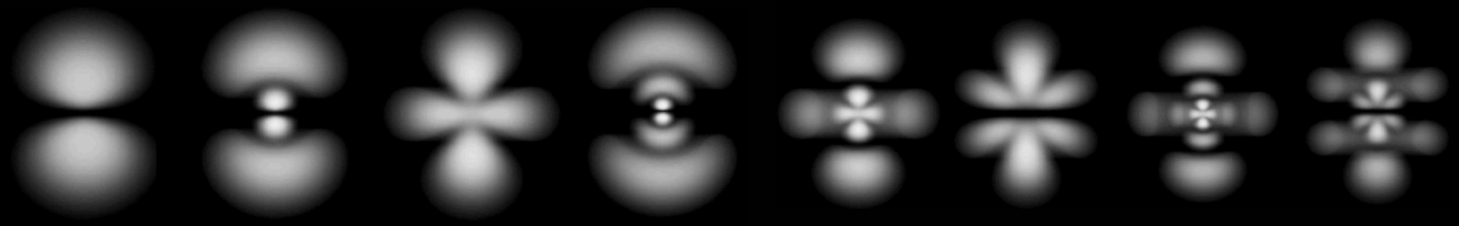
Superposition in Logic

This ability to exist in multiple states at once is called superposition.

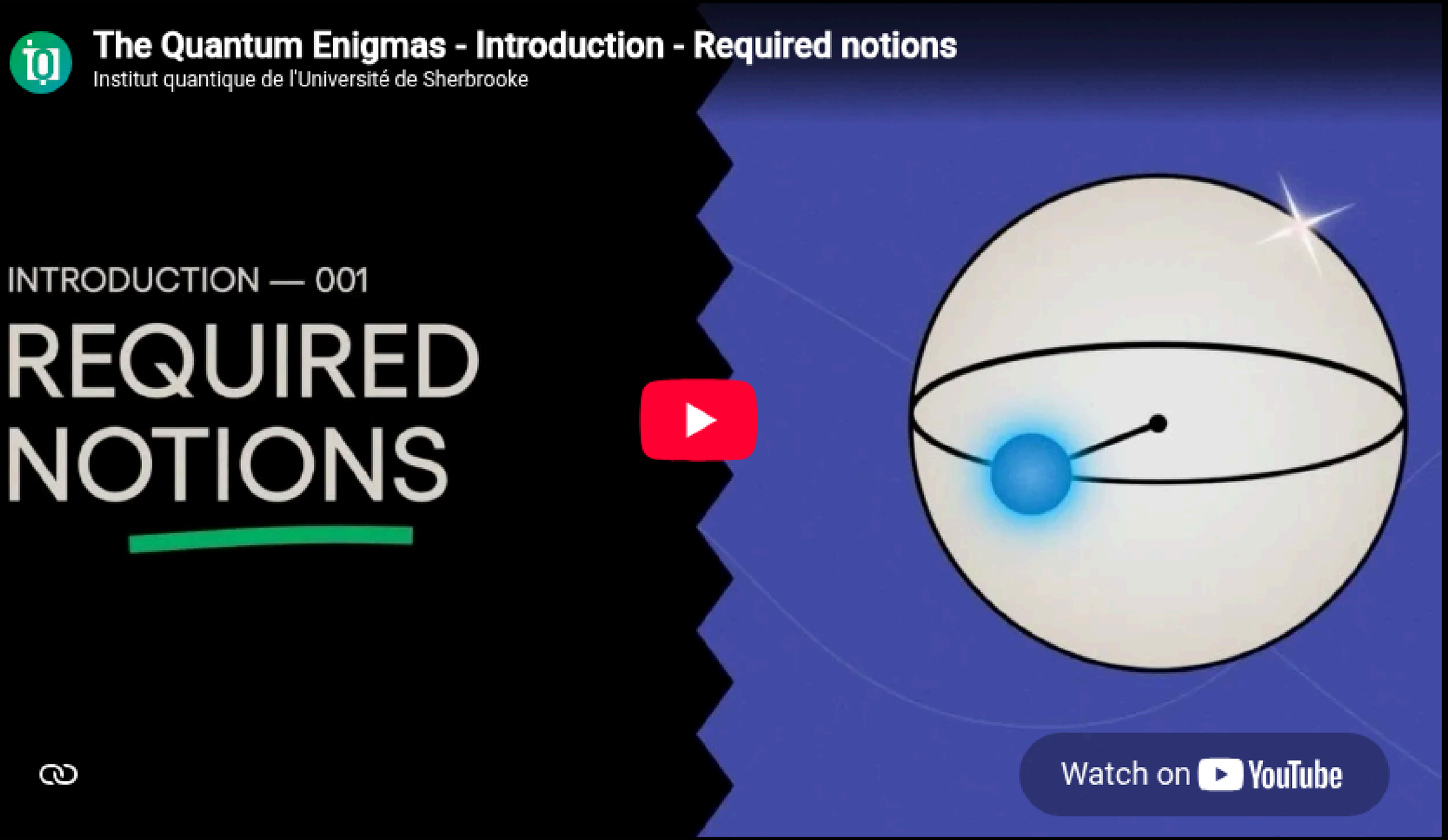
In formal mathematics, the state of a qubit is represented by the formula:

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle,$$
$$|1\rangle = \gamma|a\rangle + \delta|b\rangle.$$

where alpha and beta represent the probability amplitudes of measuring a zero or a one.
If you have two classical bits, they can only represent one of four possible states at any given moment (00, 01, 10, or 11).
Two qubits in superposition represent all four states simultaneously. Fifty qubits can represent over a quadrillion states at the exact same time, allowing for massive parallel calculations.



Visualising the Incomprehensible



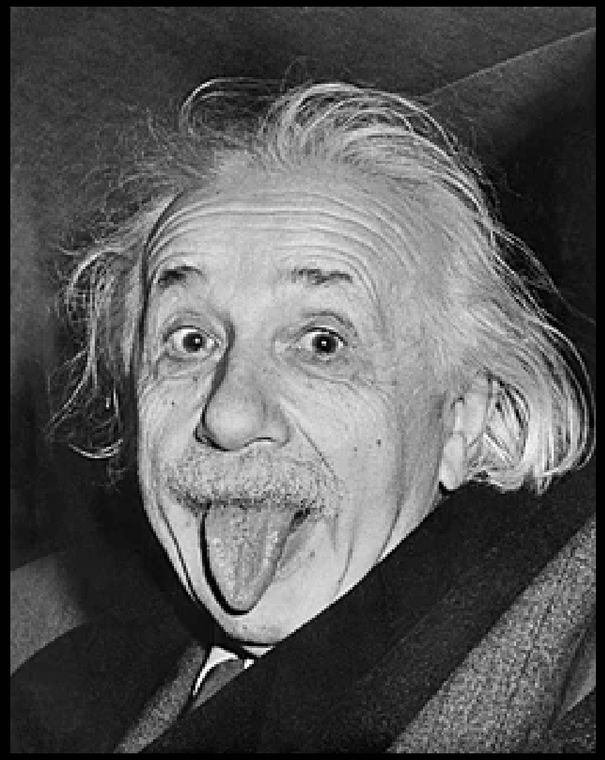
Entanglement

Einstein famously referred to this phenomenon as "spooky action at a distance."

When two qubits become entangled, their quantum states become mathematically linked, regardless of the physical distance separating them.

Measuring the state of one entangled qubit instantly dictates the state of its partner.

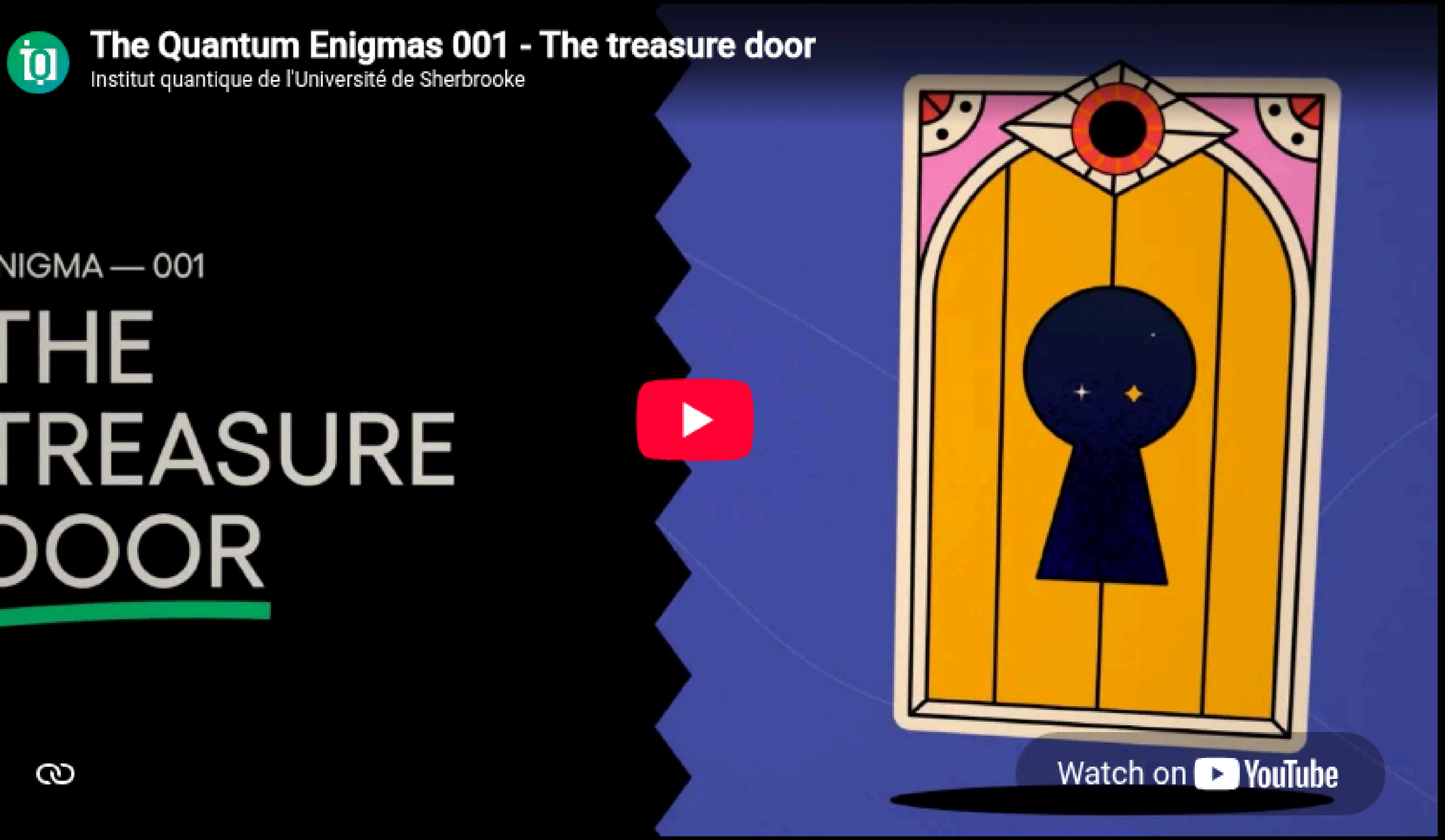
In computer science, this allows a quantum computer to process complex correlations between different pieces of data instantly, creating pathways for algorithms that are fundamentally impossible on classical hardware.



Quantum Inference

Simply holding multiple states at once is useless if you cannot extract the correct answer.
Quantum algorithms use interference to manipulate the probabilities of the qubits.
Similar to noise cancelling headphones, the algorithm is programmed to create destructive interference to cancel out the wrong answers.
Simultaneously, it creates constructive interference to amplify the correct answer, ensuring that when the superposition collapses upon measurement, the computer outputs the highly probable correct solution.

Programming a Quantum Circuit



Decoherence as a Nightmare

Building a physical quantum computer is one of the hardest engineering tasks in human history.

Qubits are incredibly fragile. The slightest change in temperature, a stray magnetic field, or even a single rogue photon can cause the superposition to collapse prematurely, destroying the calculation. This sensitivity is known as decoherence.

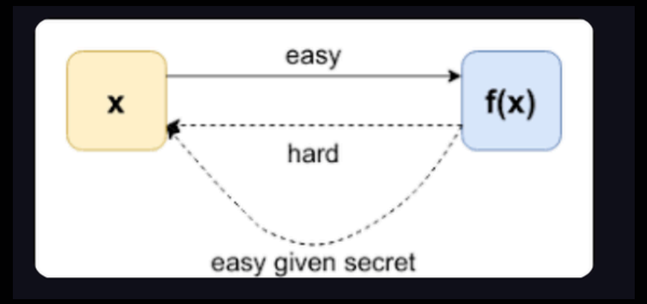
To combat this, the processors are suspended inside dilution refrigerators, cooling the superconducting circuits to roughly 15 millikelvins, which is significantly colder than the vacuum of deep space.

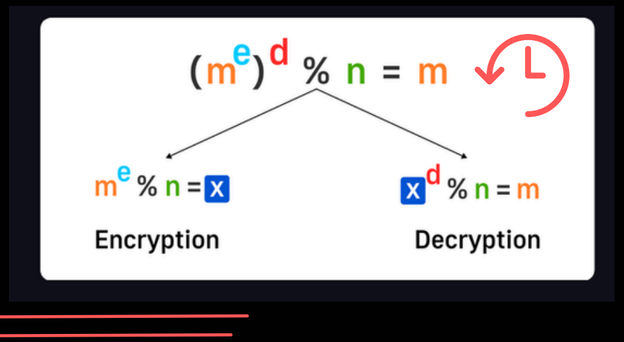
Real World Application

In Week 3, we discussed how RSA encryption protects the internet by relying on the fact that classical computers cannot efficiently factor massive prime numbers.

Shor's Algorithm is a quantum algorithm specifically designed to find the prime factors of an integer.

A sufficiently stable quantum computer running Shor's Algorithm could shatter modern RSA encryption in hours rather than millions of years, which is why institutions are actively developing post-quantum cryptography today.





Quantum computers are not designed to replace your laptop or run video games faster.

They excel at simulating nature at a molecular level, as nature itself operates on quantum mechanics.

Future applications include discovering new pharmaceutical drugs by accurately simulating protein folding, designing highly efficient battery chemistries, and optimising global supply chain logistics.

Thanks for coming!

Resources have been (should have been) posted on Teams, do take a look.

> The most disastrous thing that you can ever learn is your first programming language.



Presented by Aren, Michal, Sergi