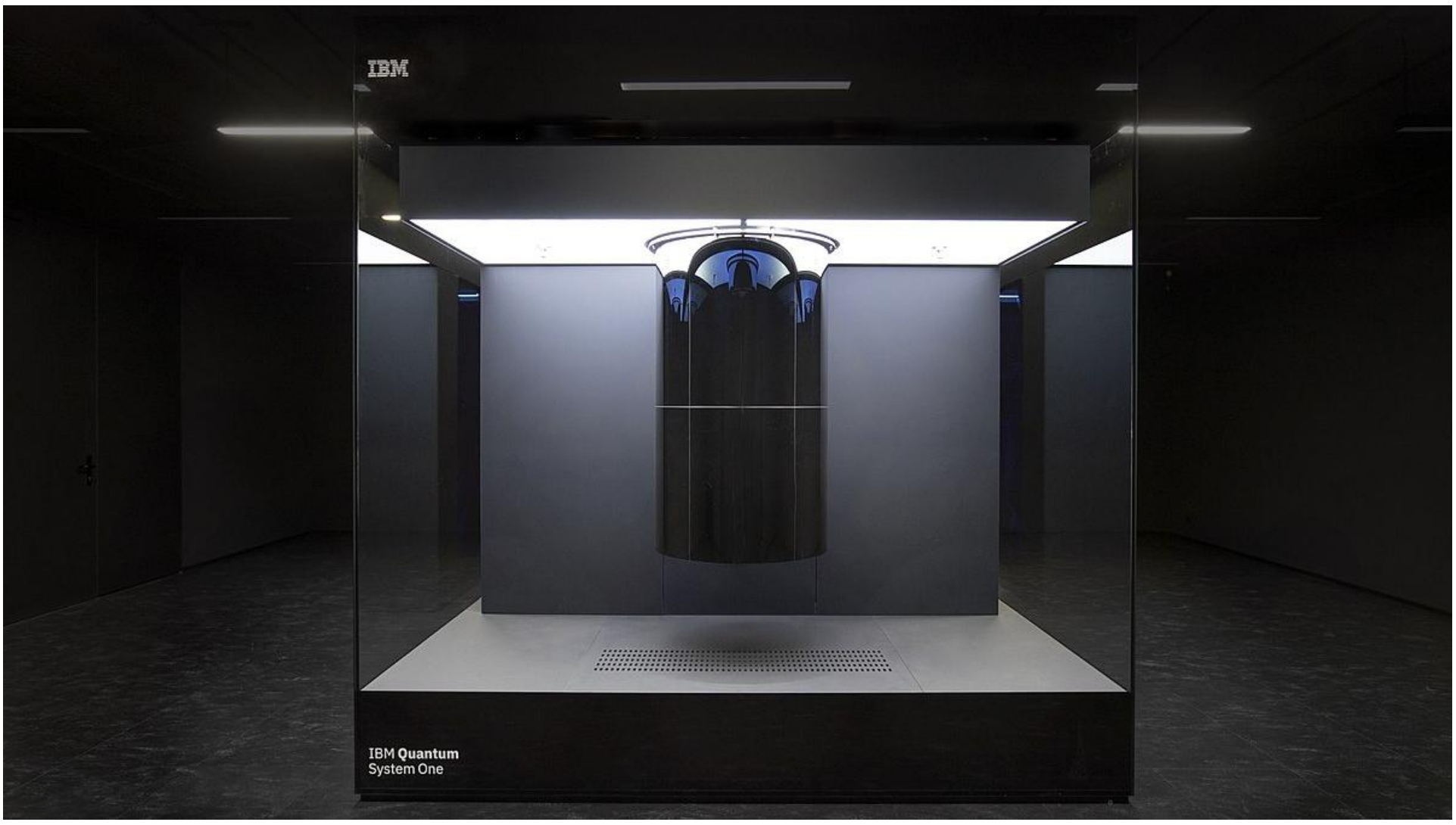
A beginner’s guide to quantum computing | Explained

Updated – December 29, 2024 10:53 am IST

TEJASRI GURURAJ



In 2019, IBM unveiled the world’s first circuit-based commercial quantum computer, Q System One | Photo Credit: IBM RESEARCH

Over the last decade or so, quantum computing has become the talk of computer town. Their potential to solve complex problems much faster than classical computers is an intriguing proposition that could benefit, if not transform, several industries.

The working of a quantum computer is based on the principles of quantum mechanics, an area of physics that deals with the smallest particles in the universe.

Physicist Richard Feynman proposed the idea of developing a computer to simulate quantum systems in 1982. He discussed the idea of a universal computer that could simulate all physics — both quantum and classical. Researchers realised classical computers, the computers of today, would struggle with the complexity of quantum systems and thus the idea of a quantum computer was born.

Since then, scientists have made significant progress in quantum computing.

Basics of quantum computing

Classical computers work on the principles of classical physics. Their fundamental computing unit is the bit: each bit represents one piece of information with two possible values, 0 or 1. It is possible to represent all types of information as a combination of 0s and 1s using the binary system.

Quantum computers rely on quantum bits or qubits to perform computations. Unlike classical bits, qubits can exist in the states 0, 1 or in a state that’s partly 0 and partly 1. In this context, state refers to all the possible values the qubit can have.

The ability of qubits to be in two states is known as superposition. Superposition is one of two fundamental principles that animate quantum computers.

Imagine a spinning coin. While the coin is spinning, it can be both heads or tails, and it isn't until the coin collapses that you can see which it is. A qubit is like a spinning coin that holds both values simultaneously.

When a qubit is measured, it collapses to one of the values, 0 or 1. This means while a classical bit holds one unit of information, a qubit can hold two. Because of this quantum computers can perform multiple computations simultaneously, with the measurement revealing one of the possible outcomes of the computations.

The second fundamental principle upon which quantum computers are based is called entanglement. This phenomenon allows qubits to be intrinsically linked no matter how far apart they physically are. Albert Einstein famously called it "spooky action at a distance".

So measuring the state of one of the qubits could immediately yield information about the state of the other. Say you have a pair of gloves. Each glove is put in a separate box and sent to different locations, and we don't know which box has which. But once a box is opened to reveal the left glove, we instantly know the other box has the right glove.

The instantaneous correlation between qubits allows shared information to be processed simultaneously, speeding up computations that would take far longer with classical computers.

Superposition and entanglement can't be described by classical theories of physics. They are exclusive to quantum mechanics — and central to the potential that quantum computers have to offer.

Significant milestones

Quantum computers are technologically superior but this doesn't automatically mean they will be better than classical computers at different tasks.

Over the years, experts have developed and honed specific tasks that prove quantum computers are capable of greater feats, and also show how.

In 1994, Bell Labs computer scientist Peter Shor created the famous Shor's algorithm. The algorithm could factorise (or find the factors of) large numbers in moments rather than the millions of years required by classical computers.

This has major implications for data security. Current methods to secure data involve locking the data and hiding the key to unlock it in the solution of a difficult mathematical problem.

Large-number factorisation is one such problem and classical computers require enormous amounts of resources to solve it. But using Shor's algorithm, a quantum computer could quickly solve the problem and open the locks.

The state of quantum computing came a long way in the next 25 years. In 2019, for example, IBM unveiled the world's first circuit-based commercial quantum computer Q System One. Circuit-based designs are believed to be the most versatile for general quantum-computing applications.

Q System One uses quantum circuits composed of quantum gates that manipulate qubits, analogous to how classical computers use logic gates.

In the same year, researchers at Google reported in a paper in *Nature* that their 53-qubit 'Sycamore' processor had achieved quantum supremacy.

A quantum computer achieves quantum supremacy when it can solve a problem that would take classical computers an unreasonable amount of time. The paper claimed Sycamore completed a task in 200 seconds that would take a supercomputer 10,000 years.

Earlier this month, in fact, Google unveiled a quantum chip called Willow, purportedly the world's first quantum processor in which error-corrected qubits improve as they scale.

Quantum states are easily prone to errors due to interactions with the environment. Quantum computers need error correction to hold information long enough to perform useful calculations with them.

Willow, Google has said, can finish a standard test in five minutes whereas the same calculation would take today’s best supercomputers 10 trillion trillion years.

Present limitations

The advancements are flying thick and fast but there are still many significant challenges to overcome before quantum computers can become (relatively) common.

The chief concern is that building quantum computers remains expensive and complex. Keeping many qubits stable is also difficult because of error rates and decoherence (when a qubit loses superposition because of noise from its surroundings).

The problems for which we really need quantum computers — like discovering new drugs or cracking mysteries in astronomy — also require millions of qubits.

All said, their potential to be useful is clear. This is why India launched the National Quantum Mission in 2023. The government has set aside ₹6,000 crore for the mission to be spent over eight years, among other things to develop quantum computers.

Tejasri Gururaj is a freelance science writer and journalist with a master’s degree in physics

Published – December 24, 2024 10:49 pm IST