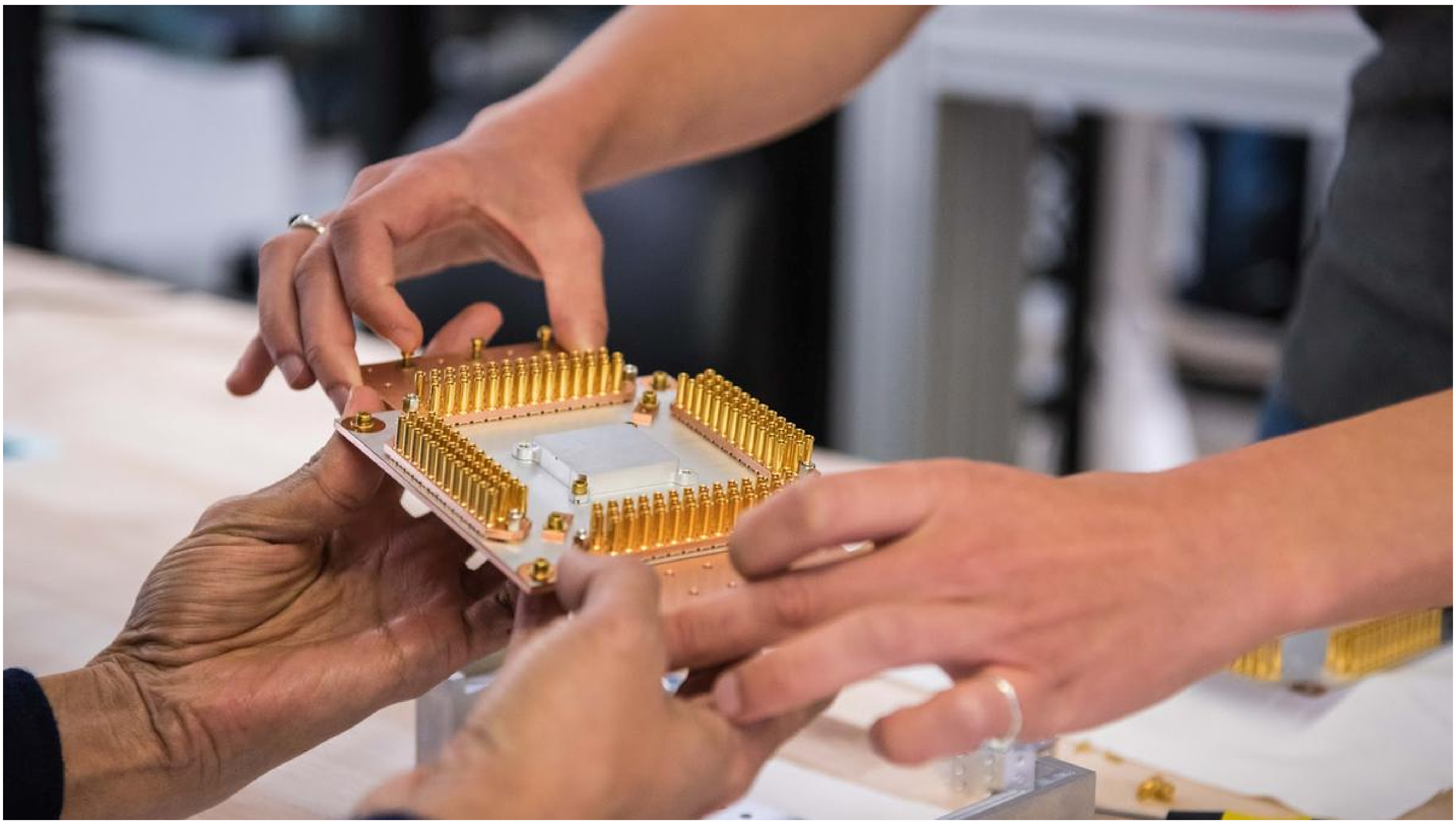
Explained | The challenges of quantum computing

What do quantum computers do that classic computers cannot? What are the elements that need to be in place before practical quantum computers become a reality? How long will it take to gain quantum supremacy?

Updated – December 22, 2022 11:41 am IST

VASUDEVAN MUKUNTH



A component of Google's Quantum Computer. | Photo Credit: Reuters

The story so far: The allure of quantum computers (QC) is their ability to take advantage of quantum physics to solve problems too complex for computers that use classical physics. The 2022 Nobel Prize for physics was awarded for work that rigorously tested one such 'experience' and paved the way for its applications in computing – which speaks to the contemporary importance of QCs. Several institutes, companies and governments have invested in developing quantum-computing systems, from software to solve various problems to the electromagnetic and materials science that goes into expanding their hardware capabilities. In 2021 alone, the Indian government launched a National Mission to study quantum technologies with an allocation of ₹8,000 crore; the army opened a quantum research facility in Madhya Pradesh; and the Department of Science and Technology co-launched another facility in Pune. Given the wide range of applications, understanding what QCs really are is crucial to sidestep the misinformation surrounding it and develop expectations that are closer to reality.

How does a computer use physics?

A macroscopic object – like a ball, a chair or a person – can be at only one location at a time; this location can be predicted accurately; and the object's effects on its surroundings can't be transmitted faster than at the speed of light. This is the classical 'experience' of reality.

For example, you can observe a ball flying through the air and plot its trajectory according to Newton's laws. You can predict exactly where the ball will be at a given time. If the ball strikes the ground, you will see it doing so in the time it takes light to travel through the atmosphere to you.

Quantum physics describes reality at the subatomic scale, where the objects are particles like electrons. In this realm, you can't pinpoint the location of an electron. You can only know that it will be present in a given volume of space, with a probability attached to each point in the volume – like 10% at point A and 5% at point B. When you probe this volume in a stronger way, you might find the electron at point B. If you repeatedly probe this volume, you will find the electron at point B 5% of the time.

There are many interpretations of the laws of quantum physics. One is the 'Copenhagen interpretation', which Erwin Schrödinger popularised using a thought-experiment he devised in 1935. There is a cat in a closed box with a bowl of poison. There is no way to know whether the cat is alive or dead without opening the box. In this time, the cat is said to exist in a superposition of two states: alive and dead. When you open the box, you force the superposition to collapse to a single state. The state to which it collapses depends on the probability of each state.

Similarly, when you probe the volume, you force the superposition of the electrons' states to collapse to one depending on the probability of each state. (Note: This is a simplistic example to illustrate a concept.)

The other 'experience' relevant to quantum-computing is entanglement. When two particles are entangled and then separated by an arbitrary distance (even more than 1,000 km), making an observation on one particle, and thus causing its superposition to collapse, will instantaneously cause the superposition of the other particle to collapse as well. This phenomenon seems to violate the notion that the speed of light is the universe's ultimate speed limit. That is, the second particle's superposition will collapse to a single state in less than three hundredths of a second, which is the time light takes to travel 1,000 km. (Note: The 'many worlds' interpretation has been gaining favour over the Copenhagen interpretation. Here, there is no 'collapse', automatically removing some of these puzzling problems.)

How would a computer use superposition?

The bit is the fundamental unit of a classical computer. Its value is 1 if a corresponding transistor is on and 0 if the transistor is off. The transistor can be in one of two states at a time – on or off – so a bit can have one of two values at a time, 0 or 1.

The qubit is the fundamental unit of a QC. It's typically a particle like an electron. (Google and IBM have been known to use transmons, where pairs of bound electrons oscillate between two superconductors to designate the two states.) Some information is directly encoded on the qubit: if the spin of an electron is pointing up, it means 1; when the spin is pointing down, it means 0.

But instead of being either 1 or 0, the information is encoded in a superposition: say, 45% 0 plus 55% 1. This is entirely unlike the two separate states of 0 and 1 and is a third kind of state.

The qubits are entangled to ensure they work together. If one qubit is probed to reveal its state, so will some of or all the other qubits, depending on the calculation being performed. The computer's final output is the state to which all the qubits have collapsed.

One qubit can encode two states. Five qubits can encode 32 states. A computer with N qubits can encode 2N states – whereas a computer with N transistors can only encode 2 × N states. So a qubit-based computer can access more states than a transistor-based computer, and thus access more computational pathways and solutions to more complex problems.

How come we're not using them?

Researchers have figured out the basics and used QCs to model the binding energy of hydrogen bonds and simulate a wormhole model. But to solve most practical problems, like finding the shape of an undiscovered drug, autonomously exploring space or factoring large numbers, they face some fractious challenges.

A practical as well as reliable QC needs at least 1,000 qubits. The current biggest quantum processor has 433 qubits. There are no theoretical limits on larger processors; the barrier is engineering-related.

Qubits exist in superposition in specific conditions, including very low temperature (~0.01 K), with radiation-shielding and protection against physical shock. Tap your finger on the table and the states of the qubit sitting on it could collapse.

Material or electromagnetic defects in the circuitry between qubits could also 'corrupt' their states and bias the eventual result. Researchers are yet to build QCs that completely eliminate these disturbances in systems with a few dozen qubits.

Error-correction is also tricky. The no-cloning theorem states that it's impossible to perfectly clone the states of a qubit, which means engineers can't create a copy of a qubit's states in a classical system to sidestep the problem. One way out is to entangle each qubit with a group of physical qubits that correct errors. A physical qubit is a system that mimics a qubit. But reliable error-correction requires each qubit to be attached to thousands of physical qubits.

Researchers are also yet to build QCs that don't amplify errors when more qubits are added. This challenge is related to a fundamental problem: unless the rate of errors is kept under a certain threshold, more qubits will only increase the informational noise.

Practical as well as reliable QCs will require at least lakhs of qubits, operating with superconducting circuits that we're yet to build – apart from other components like the firmware, circuit optimisation, compilers and algorithms that make use of quantum-physics possibilities. Quantum supremacy itself – a QC doing something a classical computer can't – is thus at least decades away.

The billions being invested in this technology today are based on speculative profits, while companies that promise developers access to quantum circuits on the cloud often offer physical qubits with noticeable error rates.

The interested reader can build and simulate rudimentary quantum circuits using IBM's 'Quantum Composer' in the browser.

> The allure of quantum computers (QC) is their ability to take advantage of quantum physics to solve problems too complex for computers that use classical physics.
>
> Quantum physics describes reality at the subatomic scale, where the objects are particles like electrons. In this realm, you can't pinpoint the location of an electron. You can only know that it will be present in a given volume of space, with a probability attached to each point in the volume.
>
> Researchers have figured out the basics and used QCs to model the binding energy of hydrogen bonds and simulate a wormhole model. But to solve most practical problems, like finding the shape of an undiscovered drug, autonomously exploring space or factoring large numbers, they face some fractious challenges.

Published – December 18, 2022 01:38 am IST