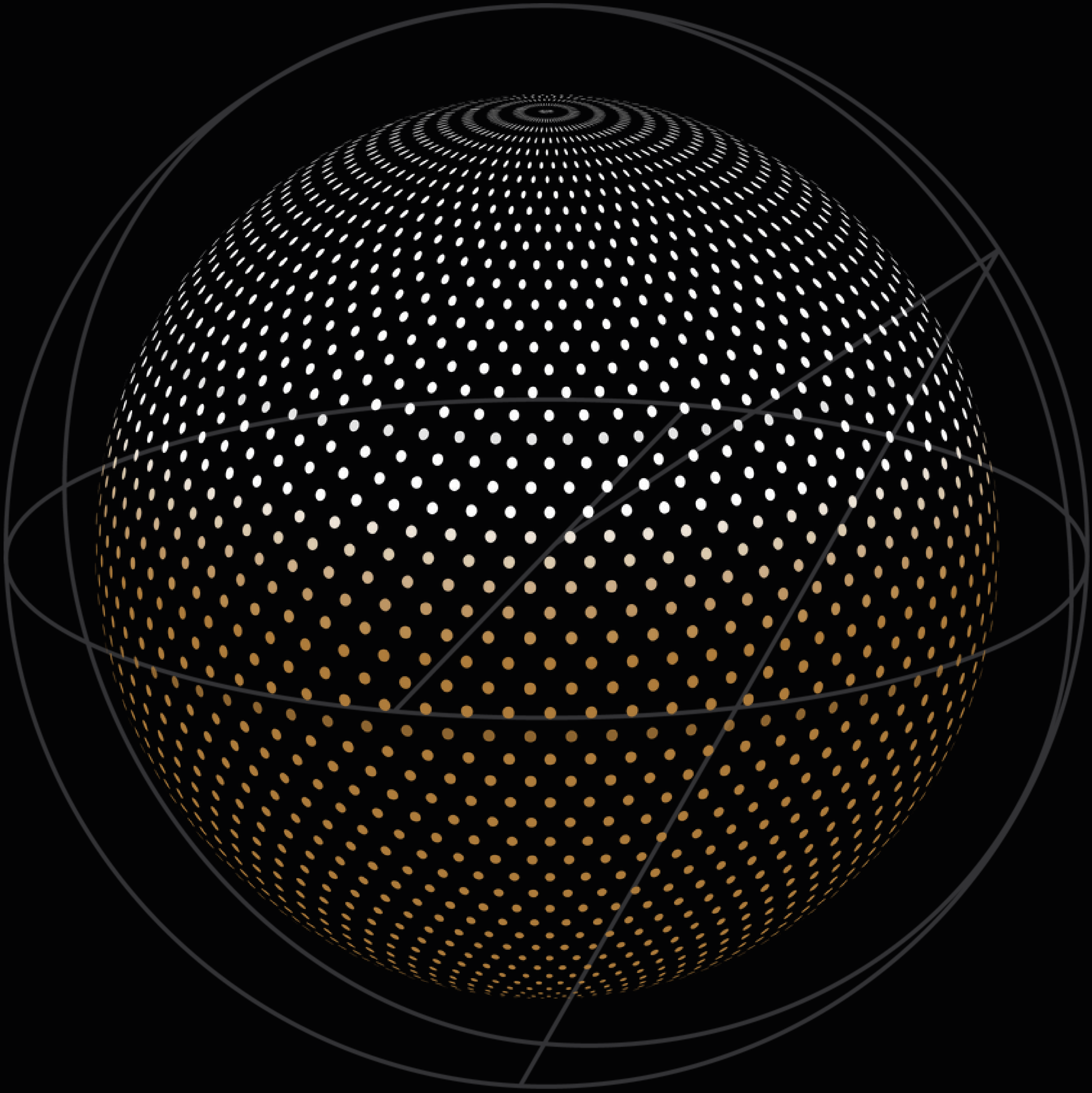


# What is quantum computing?

## A BEGINNERS GUIDE

OQC

@OQC_TECH

OQC.TECH

## Quantum computers are a new generation of problem solving machines which operate according to completely new rules.

This new kind of computing will make entirely new forms of information processing possible, which will help to generate breakthrough discoveries in a variety of industries. Quantum computing uses the principles of quantum mechanics to perform certain tasks much faster than classical computers, as well as running certain tasks that classical supercomputers can't do. It has the potential to revolutionise sectors such as financial services, pharmaceuticals, operations and logistics, and security amongst others through faster and more nuanced information processing.

BY 2025, EVERY CONNECTED PERSON IN THE WORLD WILL HAVE, ON AVERAGE, A DIGITAL DATA ENGAGEMENT OVER 4,900 TIMES PER DAY – THAT'S ABOUT 1 DIGITAL INTERACTION EVERY 18 SECONDS

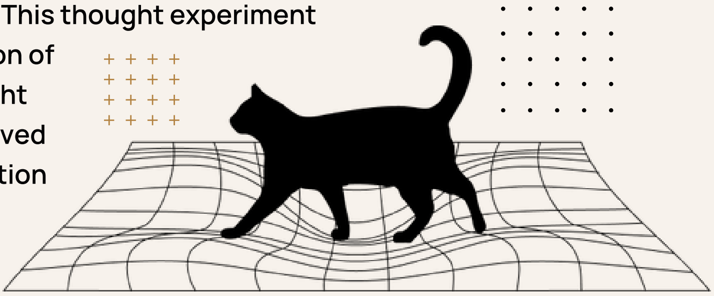
SOURCE: INTERNATIONAL DATA CORPORATION

To put this into perspective, imagine you have an unsorted dataset with 1 million records and you wanted to find a specific record based on certain criteria. A classical computer would need to search each record 1 by 1. To check the entire dataset, it would need to take on average 500,000 steps. This is time consuming, costly, and energy intensive. Comparatively, a quantum computer can run algorithms that can find this record thousands of times faster: this reduces time, cost, and is much more energy efficient. This is known as Grover's algorithm. Leading organisations have already started investing in their quantum capabilities and there is a risk of being left behind for businesses who do not start integrating quantum.

There are a few fundamental elements of quantum computing that make its complex nature easier to understand. In this article, we will explain superposition, entanglement, qubits, quantum chips, quantum software, and more!

## WHAT IS SHRÖDINGER'S CAT?

**Simply put, Schrödinger's cat is a thought experiment or paradox, of quantum superposition. The theory states that if you seal a cat in a box with something that could kill it, you won't know if the cat is alive or dead until you open the box. Therefore, until you open the box and observe the cat, the cat is simultaneously dead and alive. This thought experiment explored the problems with the Copenhagen interpretation of quantum mechanics and was initially conceived to highlight issues with interpreting quantum mechanics, but also served as a useful example to grasp the behaviour and its distinction from classical mechanics.**



# A brief quantum timeline

**1890-1999**

## THEORETICAL FOUNDATIONS

| | |
|---|---|
| 1899 | Sir Ernest Rutherford discovered alpha particle decay |
| 1900 | German physicist Max Plancks hypothesised black body radiation |
| 1905 | Einstein published his paper on the photoelectric effect |
| 1920 | The phrase ‘quantum mechanics’ was coined in University of Göttingen paper |
| 1922 | Otto Stern and Walther Gerlach performed the two slit experiment |
| 1926 | Schrödinger’s wave equation was discovered |

$$i\hbar\frac{\partial}{\partial t}\Psi = \hat{H}\Psi$$

| | |
|---|---|
| 1935 | The EPR paradox was proposed |
| 1973 | The Holevo theory is published |
| 1976 | Roman Stanislaw publish his seminal paper ‘Quantum Information Theory’ |
| 1980 | Yuri Manin began theorising quantum computing potential |
| 1982 | Richard Feynman published a paper on simulating physics with computers |
| 1984 | Charles Bennett and Gilles Brassard produced a pioneering quantum cryptography system |
| 1985 | David Deutsch published the concept of a ‘universal quantum computer’ |

1985-2001

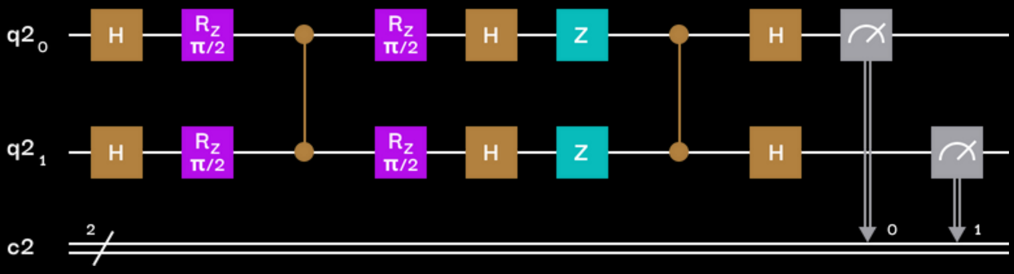
## DEVELOPMENT OF QUANTUM ALGORITHMS

⟶ **1985** British physicist David Elieser Deutsch, from the University of Oxford proposes the first quantum algorithm

⟶ **1994** Shor's algorithm is developed

⟶ **1995** Shor published the first quantum error correction paper

⟶ **1996** Grover's Algorithm was developed



⟶ **1996** Seth Lloyd proposed an algorithm which can simulate quantum-mechanical systems

⟶ **1998** Jonathan A. Jones and Michele Mosca demonstrated the first quantum algorithm on real hardware

⟶ **1999** Geordie Rose founded D-Wave Systems

⟶ **2001** IBM and Stanford University publish the first implementation of Shor's algorithm

2000-2021

## RACE TO BUILD QUANTUM COMPUTERS

⟶ **2000** David P. DiVincenzo proposed the DiVincenzo criteria

⟶ **2006** Microsoft develops its first quantum computing group, Station Q

⟶ **2007** Yale University develop a superconducting qubit variant, the Transmon

⟶ **2013** Rigetti Computing is founded

⟶ **2014** Quantinuum is founded

⟶ **2016** OQC's Coaxmon technology is patented by Peter Leek at Oxford University

⟶ **2017** OQC is founded out of Oxford University

2000-2024

## OUT OF THE LAB & QUANTUM ADVANCEMENTS

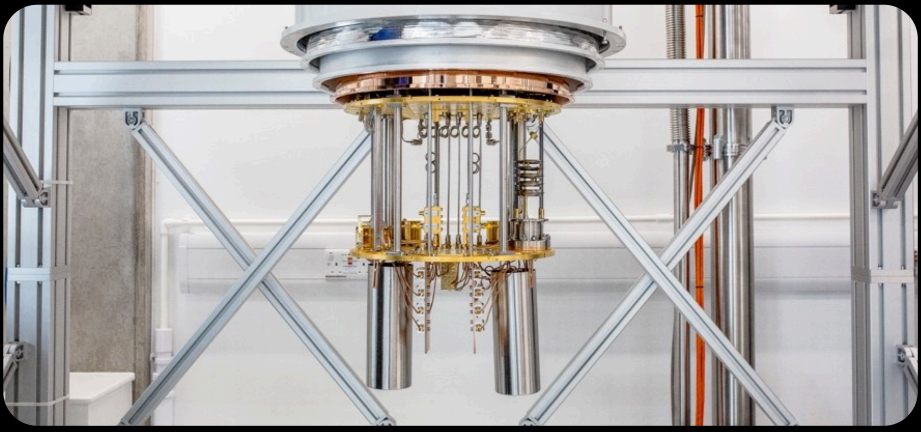
⟶ **2006** Oxford University demonstrate quantum "bang-bang" error correction

⟶ **2016** IBM launches their IBM Quantum Experience Platform

⟶ **2019** Google claims the demonstration of quantum supremacy

⟶ **2021**

OQC Lucy launches



→ **2022** OQC Lucy becomes available on AWS

→ **2023**

OQC
Toshiko
launches

→ **2023** OQC install quantum hardware into Equinix's TY11 Tokyo International Business Exchange™ (IBX®) data centre

→ **2023** Harvard University publish research on accelerating the development of quantum error correction in neutral atom technologies

→ **2024** OQC demonstrate a hardware efficient error-detection method

→ **2024** OQC publish findings on electron-beam annealing of Josephson junction to offer precise control over qubit frequencies post-fabrication

## IN THE 1920S AND 1930S, GREAT ADVANCEMENTS WERE MADE IN THE DEVELOPMENT OF QUANTUM PHYSICS THEORIES BY:

**NIELS BOHR**

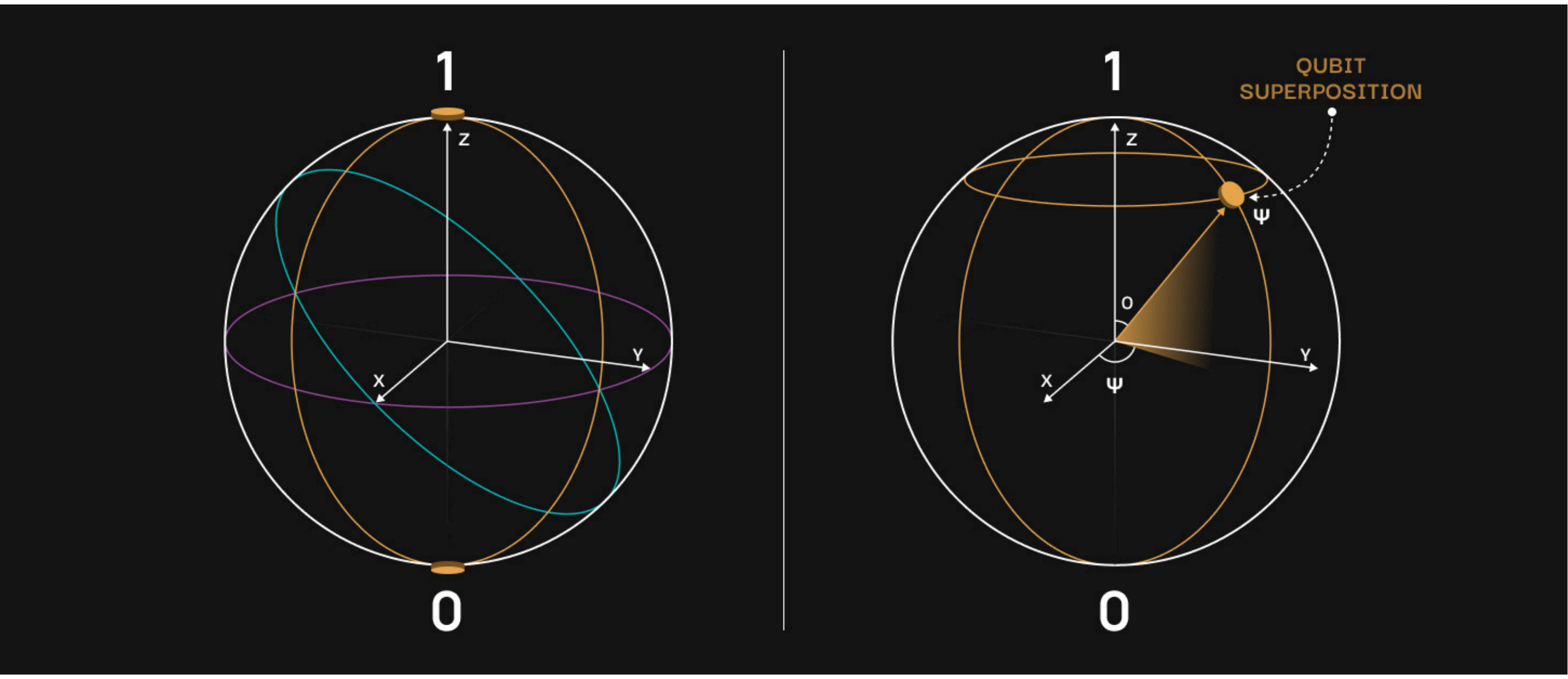
**WERNER HEISENBERG**

**ERWIN SCHRÖDINGER**

# Superposition & Entanglement

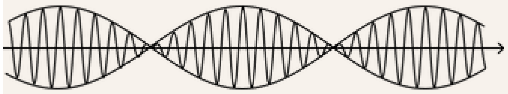
Superposition and entanglement are two fundamental principles of quantum mechanics that give quantum computing its unique advantage. Understanding the basics of these two elements help provide clarity on how quantum computing differs from its predecessor.

In classical compute, a ‘bit’ can either be in a 0 or a 1, but a qubit can be a 0,1 or any linear combination of the two. Their ability to be in multiple states simultaneously is what is called superposition: the mathematical combination of both 0 and 1.



However, the power of superposition comes from researchers transitioning away from the idea of everything being equatable to binary computation and thinking about our computational power as being a generalisation of probability theory. In this generalisation we do not just have probabilities of states occurring, we have amplitudes and phases. Just like the two-slit experiment mentioned above, these negative and positive amplitudes interfere with one another, and cancel out answers we don’t want.

**SUPERPOSITION**
IS THE ABILITY FOR A QUANTUM BIT TO BE THE LINEAR COMBINATION OF MULTIPLE STATES. THIS TAKES US AWAY FROM THE CLASSICAL IDEA OF A PIECE OF DATA BEING BINARY AND TOWARDS THE IDEA OF A DISTRIBUTION OF POSSIBILITIES.



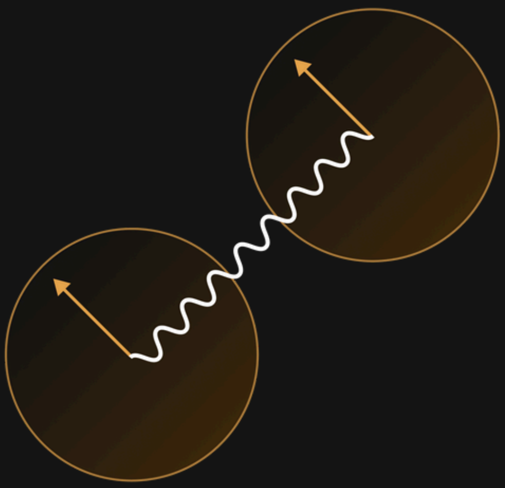
This is the art of quantum algorithm design: crafting good states to be positively amplified and bad states to be constructively interfered away. Don’t worry, when we take repeated measurements to construct a probability distribution to see what our computation is doing, the amplitude is converted into a regular probability so we can understand the output.

**ENTANGLEMENT:**

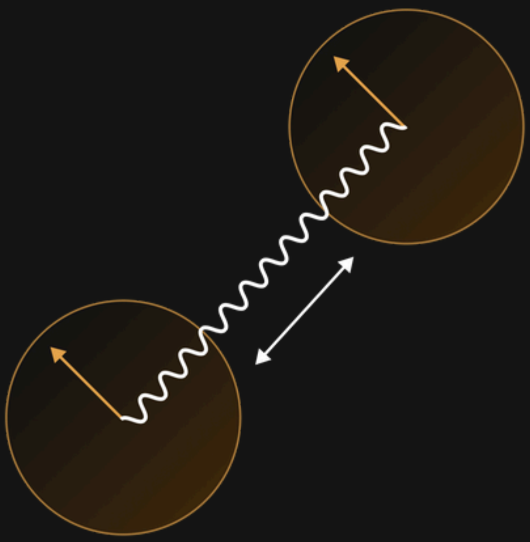
A GROUP OF PARTICLES BEING GENERATED, INTERACTING, OR SHARING SPATIAL PROXIMITY IN SUCH A WAY THAT THE QUANTUM STATE OF EACH PARTICLE OF THE GROUP CANNOT BE DESCRIBED INDEPENDENTLY OF THE STATE OF THE OTHERS, EVEN WHEN SEPARATED BY DISTANCE.

**A** TWO QUBITS

**B** ENTANGLEMENT OCCURS



**C** ONCE LINKED, THE MEASUREMENT OF ONE INSTANTLY GIVES INFORMATION ABOUT THE OTHER

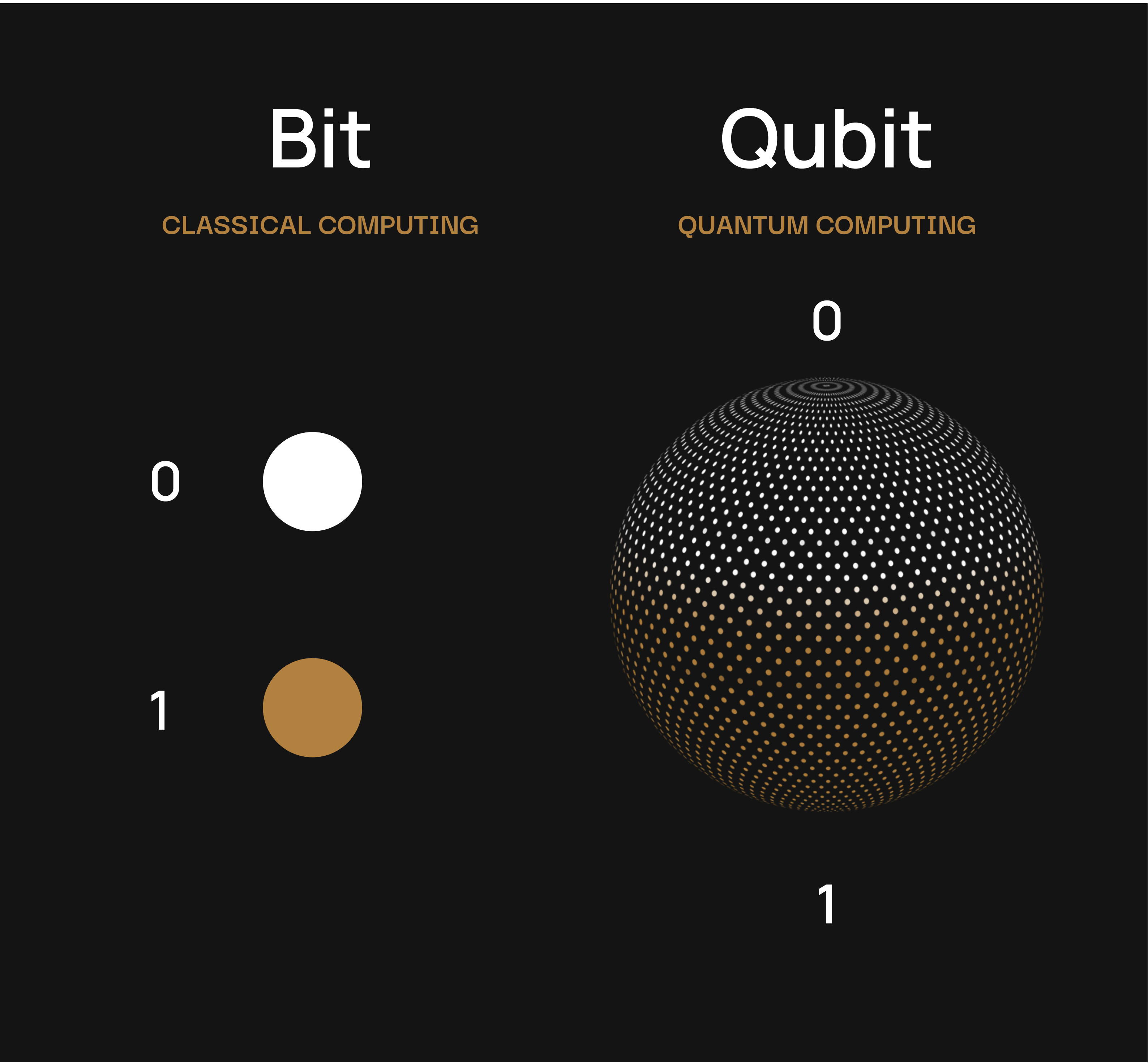


**D** THE STATES CANNOT BE DESCRIBED INDEPENDENTLY, REGARDLESS OF DISTANCE BETWEEN THEM

# What is a ‘qubit’?

## Just like a classical compute ‘bit’ a qubit is short for "quantum bit". It is the foundational unit of information in quantum computing.

Their ability to be in a superposition means that quantum algorithms can use a group of qubits in a superposition to shortcut through calculations, giving them their innate capacity to work faster. However, it is important to note that the connectivity of the qubits play a pivotal role in determining their time-to-solution.



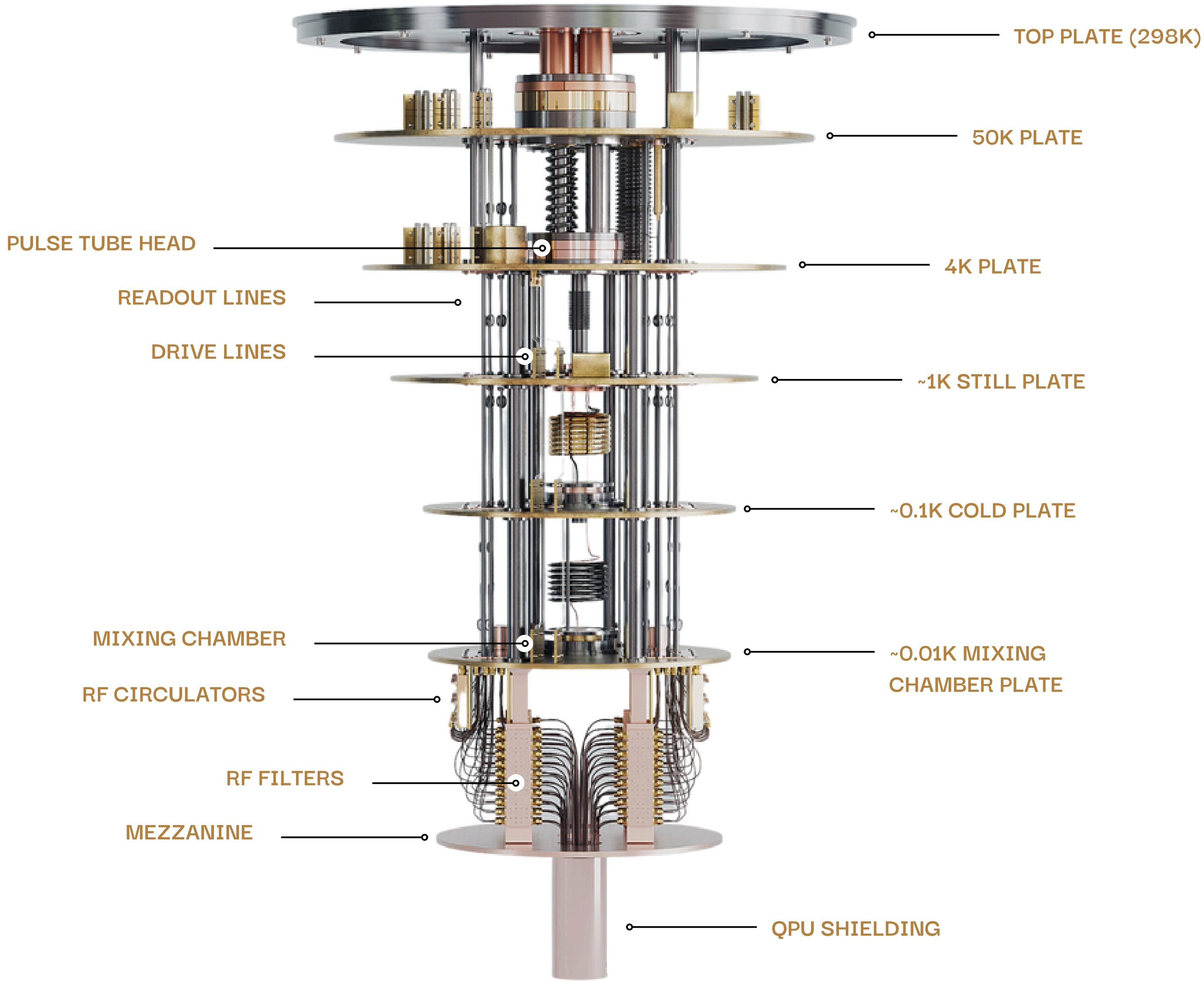
Not all qubits are created equally, and depending on the particles used determines their special properties and key traits such as their ideal operating environment.
**The most 'common' qubits are:**

| | |
|---|---|
| **SUPERCONDUCTING** | Superconducting qubits are implemented using superconducting circuits. These circuits include Josephson Junctions, which are at the core of superconducting qubits. |
| **NEUTRAL ATOMS** | This approach uses laser cooling and trapping techniques for neutral atoms and manipulates their quantum states using optical or microwave pulses. |
| **TRAPPED IONS** | This method uses atoms or molecules with a net electrical charge known as "ions" that are trapped and manipulated using electric and magnetic fields to store and process quantum information. |
| **SILICON SPINS** | Silicon qubits made up of pairs of quantum dots and can be manufactured with existing CMOS techniques. These 'coupled' quantum dots could be used as qubits. |
| **PHOTONIC** | These types of quantum computers use photons (particles of light) to carry and process quantum information. Photonic qubits are potentially an alternative to trapped ions and neutral atoms that require cryogenic or laser cooling. |

## OQC uses superconducting qubits

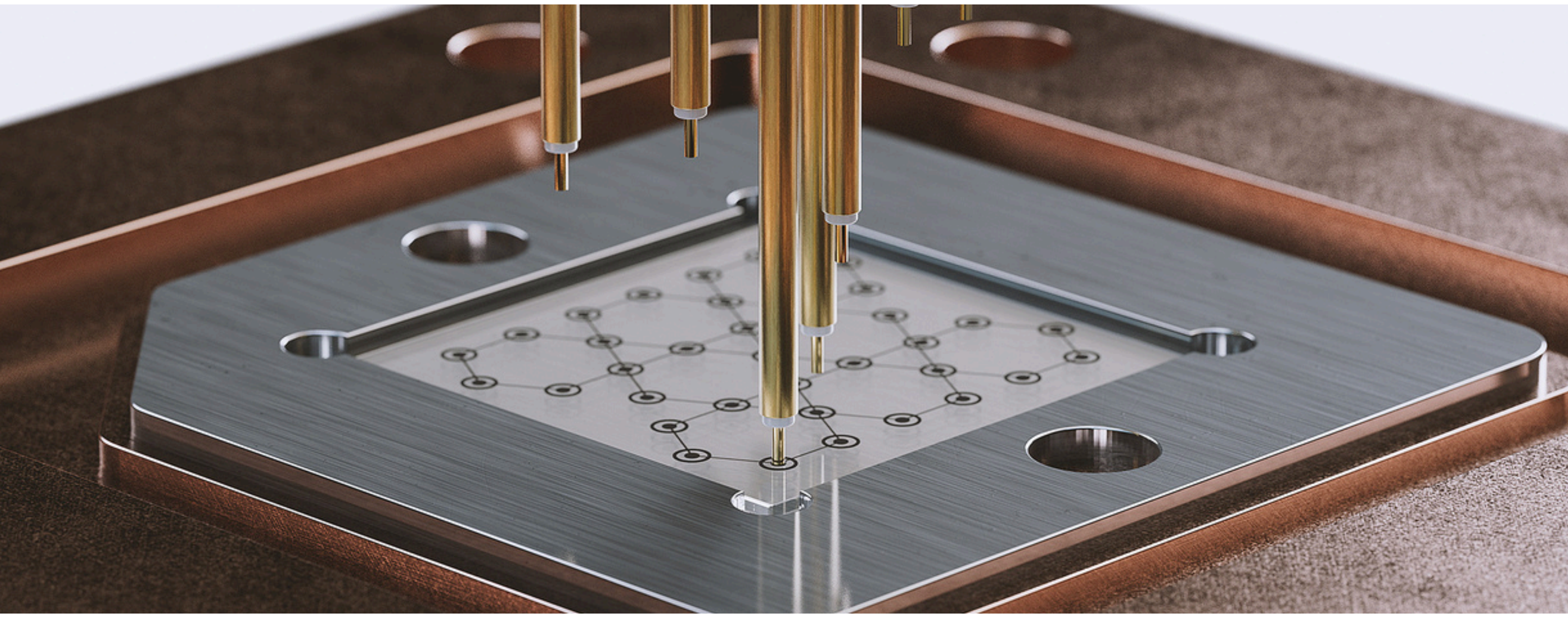
The most commonly used, they have historically been seen to have relatively short coherence times, making them susceptible to noise and decoherence. However, significant progress has been made in extending coherence times through engineering and error detection techniques, such as OQC's hardware efficient method for reducing the most significant source of error in our quantum computers.

These qubits are then used to create quantum chips: an integral part of the quantum system.



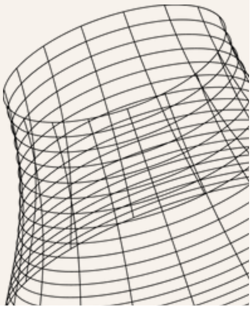
# Quantum chip vs computation chips

A quantum computing chip is the processor for quantum computers which critically contain qubits, that provide the ability to process data, algorithms and equations exponentially faster than classical computers: the key advantage of quantum vs classical compute.

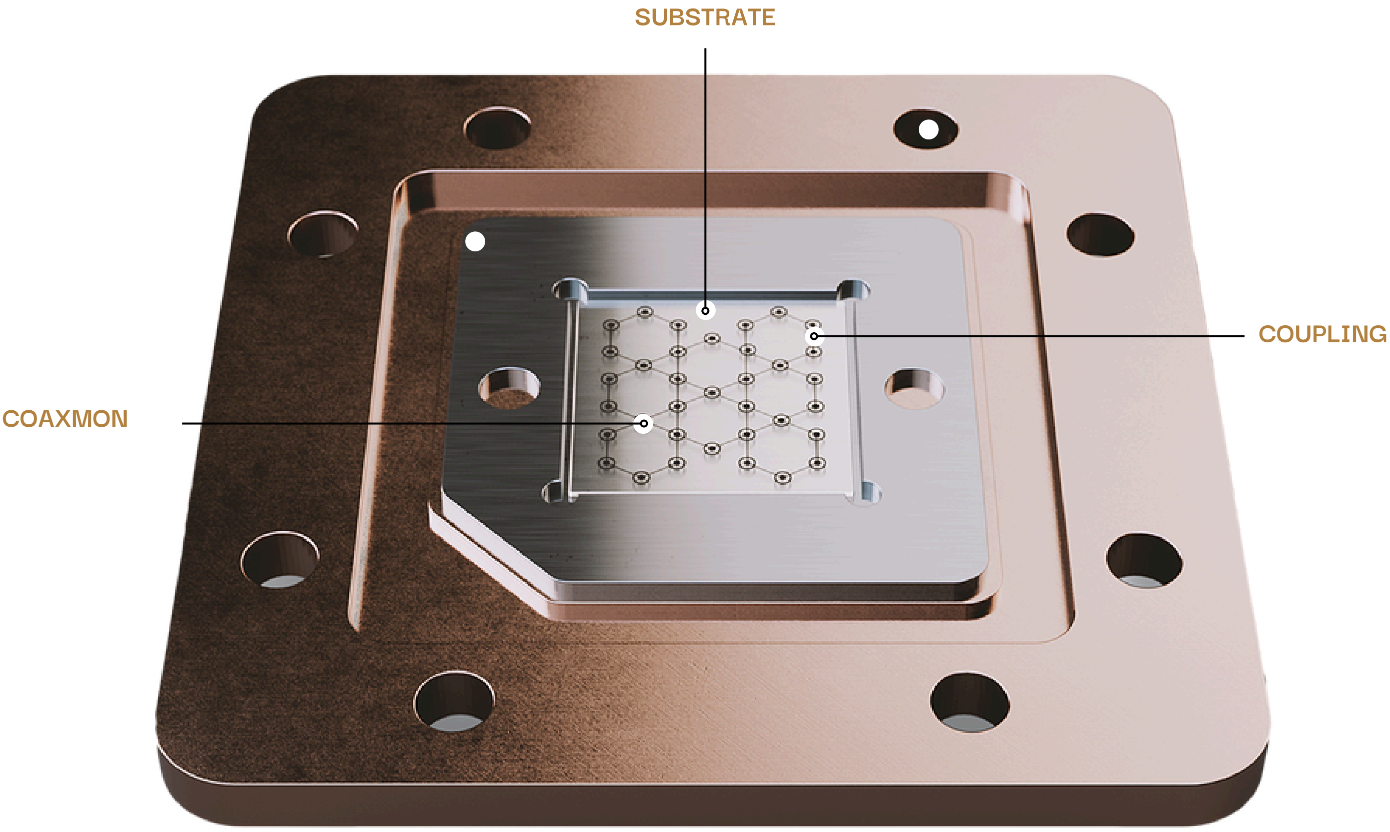


Despite their enormous power that is derived from the interaction of different qubits, quantum states are very fragile and can only exist at incredibly low temperatures. Maintaining their quantum states from initialisation through to readout is very delicate: operating at low temperatures reduces the thermal noise and helps maintain stability, whilst also being required for the superconductivity of the QPU.

IN 2000, PHYSICIST DAVID DIVINCENZO PUBLISHED “DIVINCENZO’S CRITERIA”. THIS OUTLINED THE FIVE ELEMENTS VITAL TO CREATING A QUANTUM COMPUTER AND HAS SINCE SERVED AS A SIGNIFICANT TEMPLATE FOR THE PRODUCTION OF QUANTUM COMPUTING DEVICES.



Classical chips have demonstrated an energy-intensive nature, which means trillions of transistors are required to manifest in ‘useful’ computation. Adding additional transistors does not have a simple relationship to improve performance: the resource towards classical computing year-on-year amounts to 100s of billions, highlighting just how complex the engineering is. In a traditional supercomputer, doubling the number of bits will double its processing power.



Comparatively, the energy difference between an idling and running quantum computer is negligible, this gives us a huge potential energy advantage. This advantage holds as a quantum computer scales. This, in combination with quantum algorithms that are exponentially faster, give us a technology that scales favourably in not just computational power but also energy efficiency.

Traditional 2D superconducting circuits require increasingly intricate engineering to route control wiring across the chip to the qubit. This degrades the quality of the qubits, and increases engineering errors. The OQC Coaxmon has a three-dimensionally integrated architecture that brings key componentry off-chip for vastly increased simplicity, flexibility, engineerability and, crucially, scalability.

Similarly, the interaction of multiple qubits also inherently impacts the speed of processing and requires precise maintenance to ensure the stability of many qubits for an extended time period. Qubit states are often manipulated by quantum gates, another fundamental component of quantum computing.

# Quantum gates

Often referred to as quantum logic gates or quantum operators, quantum gates manipulate the quantum states of qubits, performing specific operations to allow for the execution of quantum algorithms and computations.

This works with the same precedent as classical logic gates in classical computing circuits, however quantum gates are unitary operators. This means that they are reversible and preserve the length of the quantum state, which is critical in ensuring the probabilistic interpretation of quantum computation remains true.

There are various types of quantum gates, which include:

| | |
|---|---|
| **SINGLE-QUBIT GATES** | Which operate on individual qubits |
| **TWO-QUBIT GATES** | These operate on pairs of qubits, used to entangle qubits and perform more complex quantum operations |
| **MULTI-QUBIT GATES** | These are gates that operate on more than two qubits which allows for the construction of complex circuits for quantum algorithms |

By utilising this hardware, engineers and developers can look to develop quantum algorithms to solve large, complex problems.

# Quantum software

Combining quantum software and hardware together has the potential to not only revolutionise computation, but dramatically speed-up computation over conventional algorithms and hardware. While the hardware is the lock, software is the key to opening all of the exciting possibilities of quantum computing in our everyday lives.

Quantum algorithms can be hard to develop and programme, and the most promising applications hard to identify, however extensive research and experimenting of quantum algorithms is already underway by organisations and academics around the globe. Some have already started on this journey with OQC, such as the Department for Transport and Network Rail, who are utilising OQC and Q-Ctrl to address train schedule optimisation for both large-scale rail networks and detailed station routing, bringing a new generation of quantum solutions to pressing government problems.

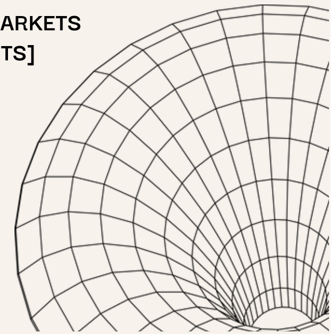
**Software required for quantum computing ranges across the full stack including:**

- Applications from simulation of material to machine learning and cyber security
- Benchmarking, testing, and verification of quantum technologies
- Quantum programming languages, compilers, and interfaces
- Emulation of quantum hardware for algorithm design and testing

One of the most commonly known aspects of quantum software is Shor's algorithm. Named after the mathematician, Peter Shor, the quantum factoring algorithm was designed to efficiently factorise large composites of numbers, which made many concerned of its ability to decrypt security measures such as RSA, a widely used public key cryptosystem. However, the inability to run Shor's algorithm means that these systems are currently safe and many boards such as NIST are working on post-quantum standards that will ensure even once the algorithm is able to be run on a quantum computer, the data will be protected in additional ways to render the algorithm unusable.

THE QUANTUM COMPUTING MARKET AS A WHOLE WAS VALUED AT $472M IN 2021 AND IS EXPECTED TO REACH $1.7BN BY 2026.

[SOURCE: MARKETS AND MARKETS]



# A brighter future, enabled by quantum

**Despite remarkable developments across the industry, there is still a long but exciting journey ahead for quantum computing.**

Quantum computing is poised to reshape our world by addressing the complex challenges we face today. As a world-leading quantum computing company, we deliver enterprise-ready quantum solutions to our customers' fingertips and enable them to make breakthrough discoveries.

OQC's solutions will enable you to confidently build your quantum capabilities and prepare for challenges of tomorrow: whether it's through the cloud, in colocation data centres, via open source quantum services, or integrated into your applications through QCaaS. We work with partners around the world to tackle the world's most pressing challenges through quantum computing solutions.

Our team are dedicated to ensuring OQC quantum computers are accessible, secure, reliable, reproducible and resilient. To find out more about what we do or how we could support your business, check out the links below.

oqc.tech

twitter

linkedin