

A Brief Introduction to Quantum Computing

🕒 READ TIME: 2 MINS

👥 AUDIENCE: BUSINESS & TECHNOLOGY

Quantum computers have appeared in science fiction novels and films for years but what actually is it and why are so many tech giants talking about it now? Modern computing technology has come far from the first computer and now quantum computers are no longer science fiction. What does the mean for modern technology and more importantly security?

WHAT ARE QUANTUM COMPUTERS?

Quantum computers are faster and more efficient than current computing approaches. In classical computers, bits can only exist in 1 of 2 states, a 1 or a 0. Quantum mechanics allows for a third state, a superposition of 0 and 1, where the bit is both 0 and 1 at the same time meaning these quantum bits (qubits) can exist in multiple different combinations at once. If a computer consisted of 4 bits, for example, the computer can only exist in 1 of 16 states at a time while a quantum computer could exist in all 16 at the same time. This fact indicates just how much faster a quantum computer could carry out processes.

Large technology companies are building

quantum computers prototypes, IBM, Microsoft, Intel, to name a few. Although prototypes exist, quantum computers will not be public for a time however, due to the security concerns that arise from the existence of near instant computing. Passwords would be compromised. Brute force hacking is a common technique of testing all possible outcomes until a match is found, with classical computers this is very time consuming but with a quantum computer that can test every outcome at the same time this would be near instantaneous.

The majority of research around quantum computers is about building quantum security and secure communication. Once

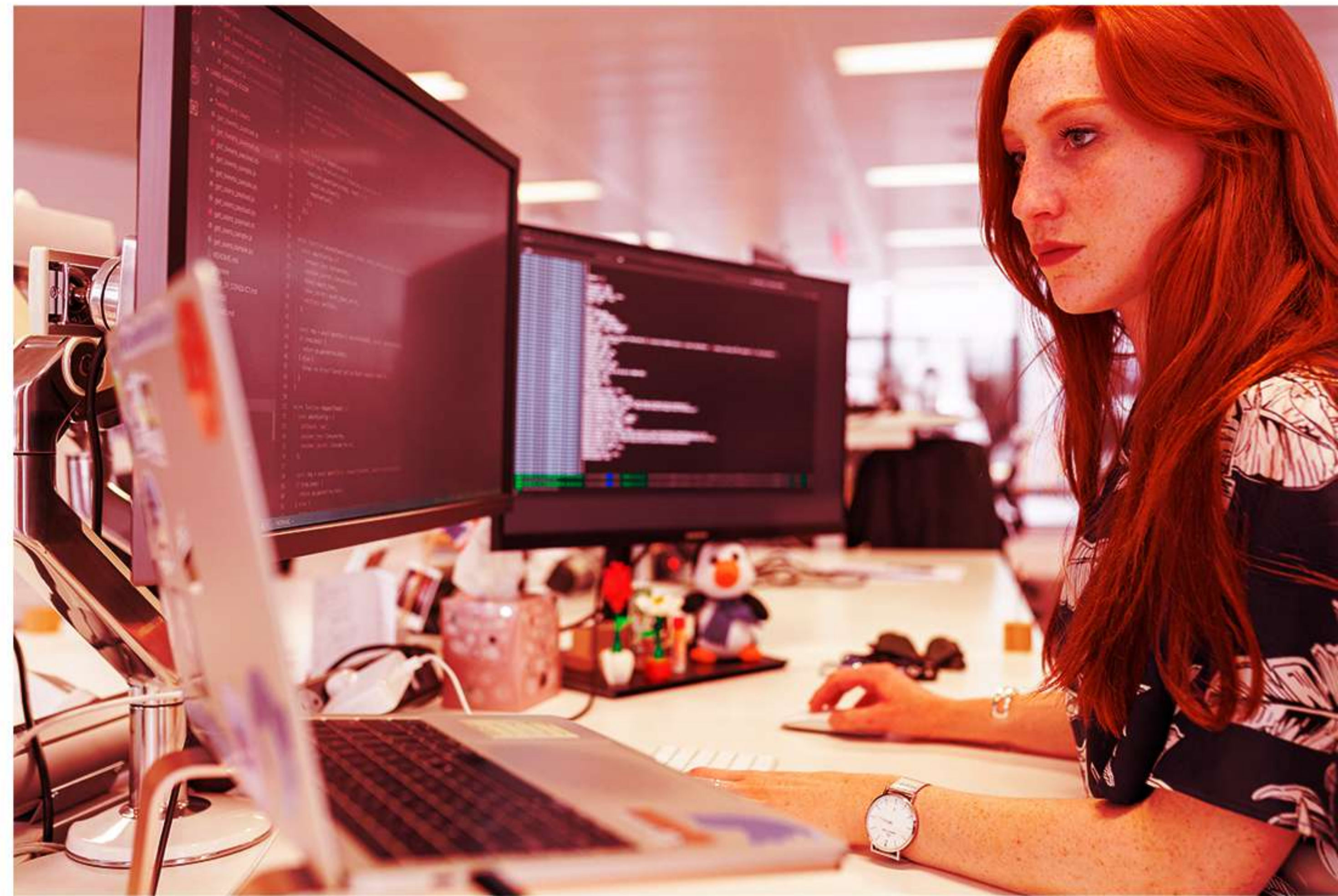
DOES YOUR BUSINESS NEED QUANTUM?

security is assured then the computers will make their way to commercial market. At present there are 2 major theoretical security protocols attempting to provide secure communication which allow for tampering detection and secure transmission of information.

When quantum computing is fully realised there will be many exciting new approaches to communication technology. Quantum teleportation, the instantaneous transmission of information across space; Superdense coding, the ability to encode 2 bits of information into a single qubit; Quantum search algorithms, allowing for vast sets of data to be searched rapidly.

When it's fully realised, Quantum Computing will be a security game changer.

While the future of quantum computing is an exciting field, commercial use of quantum computers is a long way off. As such, most companies will not need to worry about going quantum just yet.



ABOUT US

The Lancashire Cyber Foundry runs a programme designed to support businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business strategy support available too. This includes workshops dedicated to the evaluation of the driving forces which will shape the world of today and beyond. Consider how your business is affected by external changes, now consider how much time your business spends evaluating them and planning for them.

To find out more and how your business can access support or register on one of upcoming workshops contact us: cyberfoundry@lancaster.ac.uk

ABOUT THE AUTHOR

Alexander Lee

Alexander Lee is an analyst developer on the Lancashire Cyber Foundry. Having recently graduated from Lancaster University with a master's in Physics, Alexander has always enjoyed software development building multiple physics based simulations. During his degree he studied Quantum Mechanics and Quantum Information Processing sparking an interest in the future of quantum computing.

