Quantum Computing 101

Duncan Blaikie	Welcome everyone to this first in a series of podcasts where we're going to be delving into the world of quantum computing. For this podcast we've asked David Subel and Emily Bradley to do a little bit of research into what is meant by the term quantum computing and report back on what they've found out. David is an associate in one of our corporate teams and Emily is a professional support lawyer in our Financial Regulation group. Both are members of Slaughter and May's quantum technologies hub.
David Subel	Hi I'm David.
Emily Bradley	Hi I'm Emily.
David Subel	And today we're going to take you through some of the basics of quantum computing.
Emily Bradley	All the basics as far as we can understand them armed only with humanity degrees.
David Subel	So Emily, let's start with the obvious question. What is a quantum computer?
Emily Bradley	Well, as I understand it quantum computers are computers which make use of quantum mechanics so dipping into my physics A level from yester-year, the branch of physics which deals the behaviour of very small objects like electrons and when an objects are very small it transpires that they behave in ways that would deem to be quite unintuitive and it is these properties that are harnessed by quantum computers and two words that crop up a lot when you hear about quantum computers are super-position and entanglement.
David Subel	I've heard of super-position.
Emily Bradley	Well I'm definitely going to leave it to you to explain then.
David Subel	Well, super-position refers to the ability of individual units to exist in several possible states at the same time. Have you perhaps heard of Schrodinger's cat.
Emily Bradley	Yes, isn't that the thought experiment where the cat is simultaneously alive and dead there as long as the box is closed.
David Subel	Yes that's right. So we could say that the cat is in super-position of two states it is simultaneously alive and dead. So a quantum computer makes use of the exact same idea through quantum bits or qubits
Emily Bradley	Ok. So is that similar to how the computers we use at the moment use bits as units of information
David Subel	Yes, exactly. So we refer to those computers as classical computers and they make use of bits which can only exist in one or two states on or off, one or zero. By contrast the qubit can be on, off or on and off in a variety of combined states at a single point in time.
Emily Bradley	Goodness. That makes my head swim a bit
David Subel	You certainly aren't you alone. It can be helpful to try thinking of a qubit as an imaginary sphere. Whereas the classical bit can be in two states at either of the two poles on the sphere a qubit can be at any point on the sphere.
Emily Bradley	Yeah. I think I find that a bit easier than the cat.

David Subel	Well it follows that if one cubit can be a super-position of two states zero or one, then two cubits can in a super-position of four states, three cubits can be in super-position of eight states and so on. This means that each time we add a qubit to a quantum computer its power grows exponentially. This does not happen if you add a bit to a classical computer as a bit can only be in one state at a time. All of that said, I'm not so sure about the second property that quantum computers can make use of, entanglement.
Emily Bradley	Yeah. I've actually heard a bit about that because I remember hearing that Albert Einstein once dismissed it as, "spooky action at a distance", was his quote and that struck me as quite a funny way to put it. And as I recall in quantum mechanics entanglement describes the phenomenon where particles interact with each other and share physical states for an instant and that occurs no matter how great the distance that separates them. So it means that the states of entangled particles cannot be described independently of each other which I think is quite romantic.
David Subel	Indeed. So how does that apply to quantum computers?
Emily Bradley	I think it means that state of a series of qubits can become linked even if those qubits are physically separated.
David Subel	Ok, so if you have a qubit A and you measure it that will tell you something about qubit B if the two are entangled?
Emily Bradley	Yes, exactly. And following on from that changing the state of that qubit A will have an impact on qubit B if the two are entangled.
David Subel	Ok. So I think I now have some understanding of how quantum computers are different to classical computers. That does help explain some of what I've read about how quantum computers will be able to help us where classical computers can't at the moment.
Emily Bradley	Interesting, what have you read?
David Subel	Well, what I gather is that it's anticipated that quantum computers will make use of super-position and entanglement to process information, identify causal relationships and tackle particular calculations with greater efficiency and at far greater speeds than a classical computer not least because they should be able to solve multiple problems or calculations in parallel.
Emily Bradley	Interesting. And that reminds me of something actually that I saw, and it was talking about how quantum computers will speed up the rate at which certain machine learning tasks are performed and as a result enable us to better analyse and model complex data sets that underpin systems like biological systems, chemical, human, financial and that will help us model complex processes like for example the spread of a virus like corona virus or even something seemingly as simple but actually very complicated as modelling the chemical formula of ammonia.
David Subel	Yes, exactly and incidentally I've also seen a lot about the fact that once powerful enough to run an algorithm called Shor's algorithm quantum computers will be able to crack certain

	cryptographic codes in tiny fractions of the time scales needed by classical computers and this matters because it will render the commonly used encryption standard RSA, vulnerable.
Emily Bradley	All of this, to put it lightly, sounds like quite a lot might change and I've heard that some of the quantum computers that have been built have already achieved what's called a quantum advantage which means they can perform particular tasks faster than a classical computer.
David Subel	Yes, that's true. Although we should be bear in mind that quantum computers are not yet ready to solve real world problems and are still prone to high rates of error. That said, some commentators believe quantum computers will be in mass use by governments and by companies by the early 2030s so not as far off as you might expect.
Emily Bradley	No, a very near horizon. Well I've certainly learn a lot and I'm really looking forward to getting some experts in. So with that said, do tune into the rest of our podcast series where we will be talking to cyber security specialists Dr Ali Kaafarani and Robert Hannigan, and catching up with our clients about what they are getting up to in this space.
	For more information on this topic or to hear our other podcasts please visit www.slaughterandmay.com. You can also subscribe to the Slaughter and May podcast on iTunes or GooglePlay.