FSR GPS Podcast Series
Episode 10 – Impact of quantum computing in financial services

Michael Vrisakis	Hi everyone. I'm Michael Vrisakis, a Partner in the Herbert Smith Freehills Financial Services Team. Welcome to our podcast series called the FSR GPS. This series focuses on topical and emerging issues in financial services regulation which we think are the most strategic and important issues for our clients. Feel free to suggest topics you would like us to cover in the future but for now, we hope you enjoy today's episode.
Peter Jones	Hi everyone, I'm Peter Jones, a Partner here at Herbert Smith Freehills in our technology, media and telecommunications team. I have around about 20 odd years in advising financial services clients in relation to technology projects and I'm also a co-chair in our firm's global bank sector group, and every much looking forward to spending some time with you today.
Susannah Wilkinson	Hi, I'm Susannah Wilkinson, I'm the regional head of HSF's emerging technology group for the APAC region. So we are just focusing on advising clients on the adoption of key emerging technologies.
Anjelica Balis	Hi, I'm Anjelica Balis. I'm a senior associate within the financial services regulatory team at HSF, with a focus on the banking and financial services sectors, fintech and payments, non-bank lending and anti-money laundering.
Nayan Bhathela	Hi, I'm Nayan Bhathela and I'm a solicitor also in the technology, media and telecommunications team at HSF with a specialisation in privacy and data and general commercial issues in the tech sector. In this episode of the FSR GPS podcast series, we'll be looking at a slightly different topic, which is the impact of quantum computing on the financial services sector. We're going to explore what quantum computers are, some of their potential use cases in the financial services sector, and some of the security and legal risks that they pose. So what is a quantum computer?
Susannah Wilkinson	Nayan, let me jump in there. So quantum computing technically is a multidisciplinary field comprising aspects of computer science, physics, and maths that uses quantum mechanics to solve highly complex problems that

would be outside the reach of classical computers. So a powerful quantum computer could solve problems in hours that would take classical computers or even supercomputers years to solve. So how does it do this? Well, a classical computer expresses information in binary states. Think of a series of switches being either on or off, these are represented by bits - units of information as individual electrical impulses we know as zero's and one's.

In contrast, quantum computers use qubits that can express multiple states simultaneously. Thanks to the phenomenon of superposition, quantum bits or qubits can store a zero or a one but can also contain a zero and a one at the same time, so it's essentially a form of multidimensional storage.

Now it gets a little bit confusing but if we oversimplify it. If you think of classical computing as a string of coins lying either heads or tails. The more coins you add the more possible combinations of heads and tails - but there can only ever be one combination at a time. Now if you imagine the same number of coins balancing delicately on their edges. Each coin can either be heads or tails or a probability of being either, heads or tails.

So an analogy that is often used in quantum computing – pause there and allow a recut. The analogy often used is solving a path through a maze. Classical computers must sequentially crunch through one path after another up to the maximum possible paths to find the way through. But a quantum computer thanks to this super position can work out all possible paths or can test all possible paths at once and return the correct path.

So in effect the powerful potential of quantum computers is this ability to carry out multiple calculations at the same time.

Nayan Bhathela — How could quantum computers be used in the financial services sector?

Anjelica Balis — Quantum computing potentially has huge application in financial services, and a number of large financial services institutions worldwide have already started to invest their quantum computing capabilities, including the Commonwealth Bank of Australia and JP Morgan.

So one example of use cases of quantum in the financial services sector is through portfolio and trading optimisation – a powerful enough quantum computer could be used to run more complex algorithms and provide more useful optimisation results that take into account more variables than say classical computers could. So these optimisation can be useful for lending,

---

but improving the ability for banks to estimating the probability of default before they make lending decisions.

Another example is in pricing financial assets – so sufficiently powerful quantum computers could simulate a larger number of possible outcomes necessary for allocating pricing with greater speed and accuracy.

Quantum computing can also increase the power of AI systems used by financial services institutions in their operations, so for example in relation to say call centres or other customer engagement services.

Nayan Bhathela — That sounds really interesting, thanks Anjelica. So where are we up to at the moment with the development of quantum computers?

Susannah Wilkinson — Nayan, a number of companies around the world have already started building working quantum computers, including the big players like IBM and Microsoft and so on, as well as start-ups like D-wave, quantum Brilliance and others.

But it's important to note that current models of quantum computers still face numerous challenges and they're not really powerful or stable enough yet for wide scale commercial use. At this stage, they are useful for solving some specific types of problems, but they will increasingly become more useful for real world problems as they become more powerful and as the error rates start to drop. They're also just physically really large machines and they're really expensive to buy and operate.

So unsurprisingly we're seeing quantum as a service emerge, which is effectively cloud-based quantum computing services. This offers an exciting opportunity for developers and researchers and businesses. It gives them a platform to develop and test quantum algorithms on real quantum computers or simulators via the cloud. And I think this is an interesting area because these services will offer great access to quantum computing capabilities as the technology continues to advance but remains too expensive for sort of wide-scale own and operate.

Nayan Bhathela — Thanks Susannah. So you've mentioned that current quantum computers aren't powerful enough for widespread use. When do you think we'll get to that point?

Susannah Wilkinson

The million dollar question Nayan. Look there are as I said several challenges still facing quantum. Effectively the power of a quantum computer lies primarily in the number of qubits that can be arranged into that quantum computer's processor. So as we add more qubits into the processor we're able to perform more and more complex and more useful algorithms at a much greater speed, but the problems is that qubits are really sensitive to interference. When qubits are interfered with they collapse and leave their quantum state, quantum decoherence as that term is called. So back to the coin analogy I referred to earlier. Imagine all the coins balancing delicately and then something bumps the table and all the coins fall over.

So the more qubits on a processor the harder it is to maintain their fragile quantum states and there's a great quote that I really like by Carl O'Connell from Cosmos Magazine and he says, "A qubit is the ultimate diva, while a Hollywood starlet might demand a gigantic dressing room and a bath full of rose petals, a qubit demands perfect isolation and a thermostat set at 100th of a degree above absolute zero". So we're talking about minus 273 degrees celsius. The slightest vibration from a nearby atom can cause a qubit to throw a quantum tantrum and lose its super position. So you get the idea that they're really, really sensitive and often they're in huge fridges, so big machines.

So despite all of that there's been a lot of progress towards the development of more powerful quantum computers, IBM for example recently announced Condor which is a general purpose quantum computer and it's got 1,121 qubits and they're planning on the release of a 4,000 qubit machine in 2025 so there's a bit of a timeline. But to put that into context back in October 2019 Google claimed to have reached quantum supremacy. So this was a big thing that a lot of people were waiting for which was when a quantum computer could purportedly solve a problem beyond the capabilities of a classical machine and at that point they only had an array of 54 qubits. So now we're talking about looking at 4,000 qubit machines so that's a big jump. So back then they performed a series of operations in 200 seconds that Google claimed at the time would take a supercomputer about 10,000 years to complete. Now IBM disagreed a little bit and said that there was a better comparison in terms of the estimate of time that it might have taken two and a half days using techniques that maximise computing speed in a classical supercomputer. But all of that aside, where are we heading? So Google is aiming to build a useful quantum computer by 2029 and IBM's roadmap that you can see on their website shows sort of progress milestones out to about 2033. Other companies are claiming that or aiming

	to develop their version earlier. Academics and industry are still, you know, their making strides towards building the use case for quantum computers but it really isn't yet clear when we'll get to a point where they will be both ready and ready for wide scale commercial adoption and also affordable.
Nayan Bhathela	Thanks Susannah. So on the more slightly concerning side one of the hot topics in the realm of quantum computing is that quantum computers will have the ability to break modern forms of encryption. What exactly is the risk here and how will it impact our current systems?
Peter Jones	Yeah thanks Nayan and I'm not sure why, as a tech partner who's used to proselytising new technology, I'm out here potentially looking at the negative, but nevertheless in spite of some of the challenges that Susannah went through in terms of where we currently are with quantum computing, it's certainly the case that a sufficiently powerful quantum computer would be able to break many of the widely used public peak cryptography systems commonly used today which obviously could include those that are used to secure communications over the internet and of course secure communications over the internet are crucial to our modern financial system so this vulnerability could be severe if it was to eventuate. It is also the case that it could impact the operation of some blockchains, cryptocurrency and crypto wallets which make use of some of the potentially vulnerable systems and communication networks. As I mentioned at the outset though, the biggest caveat here is that this risk will only eventuate with quantum computers that are significantly more powerful than the ones that we have today.
Nayan Bhathela	Thanks Peter. So we heard earlier that we could have useful quantum computers within the decade does that mean that we'll also be able to break public key systems in that time as well?
Peter Jones	I think it's important here to distinguish between a useful quantum computer on the one hand and then on the other one which is actually powerful enough to break public key systems. Estimates for how many qubits would be required to break public key systems in a reasonable time do certainly vary but some researchers have estimated you would need around 20 million. Clearly based on some of the commentary that Susannah ran through before, we're a long way away from that. So at this stage it isn't

	clear when we will actually get to the point at which we are at risk or indeed if we ever will, but it's fair to say some estimates are also suggesting as early sometime in the 2030's. And of course despite all of this though, quantum computers with far fewer qubits than 20 million have already been shown to be very useful, again focusing here very much on the negative side of things in terms of the risk to some of the public key encryption systems that are used at the moment.
Nayan Bhathela	So it does sound like this is a risk that won't eventuate for a while then if it does at all. Is this something that we need to be worried about now?
Peter Jones	Yeah it's a good question Nayan. I guess there is a risk always that data which is currently encrypted using known systems at the moment that may in the future become vulnerable, that data could, of course, can be stolen now and hoarded and then decrypted later using sufficiently powerful quantum computers which is called a 'steal now decrypt later' attack. It's not new, it's been around for years in the espionage community where various spy agencies for different entities would effectively ex-filtrate certain encrypted information and then over many years attempted to decrypt and then eventually would find something useful. But like in those sort of scenarios as well a lot of the data that would be the subject of the "steal now decrypt later" attack won't actually be valuable to a potential hacker in 10-15 years' time however there still could be as part of the data that's ex-filtrated now certain very sensitive information that could still have some value. So for example things like sensitive information that might be collected about customers as a result of due diligence before granting loans or issuing insurance that might turn up issues in terms of addiction problems or serious health issues which at a later point in time could be somewhat challenging and sensitive and clearly potentially embarrassing.
Nayan Bhathela	So what can we do about this risk? Can it be minimised at all?
Peter Jones	Well the National Institute of Science and Technology in the United States or perhaps better known to many in the community as (NIST) has been working on new encryption standards that are intended to be 'quantum-safe' and they have been doing this, working on this project since 2016. NIST is planning to finalise that process and publish these post-quantum cryptographic standards that can be used for commercial products by this

year. Although we're still waiting for standards to be finalised and this hasn't stopped the likes of Apple and Signal developing their own post-quantum cryptographic protocols in the meantime to secure their own messaging functions. Another way we could secure communications is through a technology known as quantum key distribution which relies on the properties of qubits to establish secure connections. A key advantage of post-quantum cryptography though is that it can be operated on our current internet infrastructure, whereas quantum key distribution relies on a whole new set of infrastructure. So for that reason, organisations like the Australian Signals Directorate currently prefer post-quantum cryptography over quantum key distribution technologies as a means of securing communications in a post-quantum world, but the ASD has signalled that it will keep monitoring the developments of quantum key distribution technologies as you would obviously expect. But even then, moving over to post-quantum encryption systems is still likely to take considerable time and resources particularly for large financial services entities given the complexity and multiplicity of their information systems.

Nayan Bhathela

Thanks Peter. So it seems quite clear then that despite the enormous opportunities which quantum computing presents, it does pose some operational and security risks as well. What are some of the legal issues arising from quantum computing?

Susannah Wilkinson

Thanks Nayan it's important to note at this stage that this is really a nascent area and it's going to continue to evolve but there are a couple of key legal points that we probably want to highlight. So companies are generally obliged under the Australian Privacy Act to take reasonable steps to protect personal information that they hold from unauthorised access or disclosure. So it's reasonable in the future our regulators might see the adoption of post quantum cryptography as necessary to comply with that requirement although it's not clear when as we've discussed earlier.

Another interesting legal issue is whether or not the stealing of encrypted information that Peter spoke about before can be used at some point later down the track being decrypted using quantum computers and whether that could be a data breach which has to be notified under the Privacy Act. A similar question arises in relation to cyber security incidents under the Security of Critical Infrastructure legislation and information security

---

incidents under CPS234, which would apply to a number of financial service operators.

Now these aren't bright line tests, and it will always depend on the type of data in question and the perception of risk. So as we often find ourselves in the context of emerging technology in the absence of clear regulation, guidance from regulators on these issues will really play a big role in getting a clear understanding of what the obligations are and what the expectations are for companies.

Angelica Balis

Thanks Susannah. More specifically for APRA-regulated entities, there are also key security and operational requirements under various prudential standards that would be affected by quantum computing so APRA prudential standards CPS234 sets out some base line obligations for APRA regulated entities in relation to information security. It requires regulated entities to maintain security capabilities which are commensurate with the size and extent of threats to their information assets and to enable continued sound operation of that entity. It also requires adequate security controls to be put in place to protect information assets. CPS220 provides additional requirements in relation to the management of risks by APRA-regulated institutions, which includes setting up risk management frameworks to handle risks, which include operational, insurance and investment risks. The recently finalised CPS230 also includes specific obligations relating to the effective management of operational risks, which includes legal risks, technology risks and data risks. That includes the development of internal controls and business continuity plans to manage those operational risks.

Recently, APRA has identified technology risks as a strategic priority, with the regulator warning the industry to "tread carefully, conduct due diligence, put appropriate monitoring in place, test the board's risk appetite and ensure there is also adequate board oversight."

Entities which are not regulated by APRA but hold an Australian Financial Services licence are required to, among other requirements, establish and maintain adequate risk management systems and to do all things necessary to ensure the financial services provided by the licensee are provided "efficiently, honestly and fairly". In the 2022 case of *ASIC v RI Advice Group*, the Federal Court held that these obligations extended to the effective management of cybersecurity risks and cyber resilience. It was the first time an Australian court held that an AFS licensee had failed to have

---

adequate risk management systems in place in order to manage its cybersecurity risks.

So as quantum computing continues to develop, it's likely that any controls or policies that financial services entities have in place will need to take into account the threats of quantum computing to remain compliant with the prudential standards and financial services laws generally.

Nayan Bhathela

Thanks Anjelica. So it's pretty clear that there is a broad range of regulatory obligations that could be impacted by quantum computing. How are other jurisdictions regulating this issue?

Peter Jones

Probably the jurisdiction that is at the moment the most advanced is the United States which has been making some important moves in this space in terms of the regulatory environment. In 2022, the *Quantum Computing Cybersecurity Preparedness Act*, pretty lengthy term if ever there was one, was passed by Congress with bipartisan support. This Act requires US federal agencies to annually take inventory of their IT systems that are or may be vulnerable to quantum computing and to develop plans to upgrade their systems to post-quantum cryptography once it has been standardised by NIST.

At this stage, the US hasn't set any timeline on by when that migration needs to occur. They also haven't imposed any migration requirements on private companies yet – but it's likely that federal agencies affected by the quantum law would pass-on these migration requirements to any service providers in their supply chain. So in effect at the very least I'd expect there to be indirect regulation through those third party suppliers. At the moment there aren't any other jurisdictions which have imposed similar obligations like those in the US, but it's certainly conceivable that governments and legislatures around the world might follow the lead that the US has taken as the risk becomes more tangible and to also remain frankly in alignment with the United States either with respect to similar legislation or with potentially softer requirements like guidelines, codes and similar.

Nayan Bhathela

So what are some of the steps that companies can be taking now to assess the risk of quantum computing to them?

Susannah Wilkinson	So Nayan, we've heard that regulators around the world have, you know some regulators have issued helpful guidelines on what companies can be doing now while post-quantum encryption standards are still being finalised. One of the first steps for companies in Australia for example is to take inventory of sensitive datasets and encryption systems that are being used to determine which ones would be vulnerable to quantum computing. This would include identifying third party suppliers that provide systems or services which involve the handling of sensitive information or systems, so fairly broad - but this would help understand the scope of potential vulnerabilities and to figure out what will be needed to focus on any potential migration in the future. So while there is a general sense that the widespread quantum computing sort of adoption is still a fair way off as we've seen with other sort of waves of emerging tech from a risk management perspective that's only going to hold true until it suddenly doesn't so having an idea of what the potential vulnerabilities are within an organisation over the next couple of years will set businesses up for success I think.
Peter Jones	I think that's a really important point Susannah which is the good old fashioned everything is fine until it isn't fine.
Susannah Wilkinson	Exactly.
Peter Jones	And I think just if we look then what does that mean for organisations and the financial services sector. Well I think you can kind of take a little bit of a queue from some of the prudential standards which Anjelica has already mentioned and certainly the approach that regulators in this country and others are probably taking which clearly seems to indicate that organisations should be taking steps to prioritise those systems which are going to be first for migration and then of course prioritisation should be based on, in large parts, some of the vulnerabilities associated with those systems and the types of data that those systems are effectively protecting. Based on those efforts, organisations would then be working on a plan to migrate once your post-quantum encryption standards are available. That plan ideally would be holistic, and include testing of new standards, renegotiating third party supply agreements as required, and decommissioning old vulnerable systems. All of which sounds incredibly

easy to say but of course is incredibly difficult in practice for anyone who has gone through any form of minor regulatory uplift process would also attend and indeed this would not necessarily be a minor uplift process.

So all of this will be a very resource intensive process particularly for large institutions like trading retail banks and similar, so it is something that financial services companies need to start thinking about if not today then certainly in the very short term.

Nayan Bhathela — Thanks very much Peter, Susannah and Anjelica. That's all we have time for today, thanks for joining us.

You have been listening to a podcast brought to you by Herbert Smith Freehills. For more episodes, please go to our channel on iTunes, Spotify or SoundCloud and visit our website herbertsmithfreehills.com for more insights relevant to your business.
