ISSUE 139

BOARD PERSPECTIVES: Risk Oversight

QUANTUM COMPUTING: WHY THE BOARD SHOULD CARE

Quantum computing offers companies a powerful value proposition for solving complex problems in ways not attainable today. Those unprepared to harness quantum's capabilities risk being left in the dust by competitors who are.

There is a growing interest across the world in the feasibility of quantum computing and when it will finally become a reality in business. And that's for good reason. Quantum would enable problem-solving capabilities to address simulations and complicated optimisation questions involving a formidable number of variables and potential outcomes at amazing speeds not attainable with conventional computers. For example, it could:

- Revolutionize all areas of logistics in moving products, create complex engineering designs, and improve artificial intelligence (AI) applications in consumer products and manufacturing.
- Predict materials behaviour in different conditions to support development of cost-effective material compositions with improved or desired properties to meet performance specifications in chemicals and manufacturing.
- Improve sensor development, optimise network designs and energy distribution, and maximise oil well output in energy and utilities.
- Rebalance documented portfolio gains, optimise trading trajectory, elevate credit risk analysis, and integrate AI for near-real-time fraud detection in financial services.
- Optimise search data for better AI diagnostic aids (from faint marks in MRIs to overall symptom comparisons), model and simulate molecular interactions to accelerate drug discovery, and analyse genetics to facilitate the development of

protiviti®
Face the Future with Confidence

personalised treatments in healthcare and life sciences.

- Enable better, faster search capabilities, boost AI and machine learning capabilities, optimise training data, create new algorithms, optimise advertising and marketing analysis, and verify and validate software in technology, media and telecommunications.

In summary, quantum-inspired algorithms could bring innovative solutions and approaches to product development, reduce time to market, optimise customer delivery, and speed up data transfers. There isn't an industry that wouldn't be significantly affected once one or two competitors harness quantum's disruptive computing power. The remaining players in the sector will be left scrambling to catch up.

Importantly, general purpose quantum computers could significantly weaken, even kill, current cryptography systems used to hide and secure data so that only certain people can view it. In other words, a quantum computer of sufficient power will instantly render today's security systems obsolete and break the encryption of sensitive data protected by today's strongest security. When this performance threshold is met, an organisation's data, intellectual property (trade secrets, proprietary systems, formulas, patents, customer information and data) will be at risk. Any information shared on public channels now or in the future will be vulnerable.

Clearly, this would have huge implications for industries such as financial services and healthcare that have significant regulatory requirements for data privacy and security. Quantum's business, legal and ethical impacts can compromise the security of financial and banking transactions, the confidentiality of medical data and healthcare records, safe storage of personal data in the cloud, and access restrictions to confidential corporate networks. And the impact wouldn't be limited to the private sector, as government and military communications would also be compromised.

While this may sound like science fiction, both the opportunities and threats posed by quantum are real. Companies need to start laying the foundation for quantum so that they don't get left behind. The good news is that practical quantum advantage in specific applications will come years before the threat to cryptography. If quantum applications were to begin in, say, three years, there would be a rush for the talent and resources needed to harness its power. The early movers across the globe may end up with the top players.

So, for boards, there are three relevant questions.

What is quantum computing?

Quantum computers are machines that use the properties of quantum physics to store data and perform computations. The capabilities they provide will one day significantly outperform even the most powerful supercomputers for solving especially complex problems. This future inflection point, or "quantum supremacy," could come as soon as 2023, taking current road maps by IBM or IonQ into account. What kind of supremacy? Google's Sycamore computer completed a complex computation in 200 seconds that the company believed the most powerful supercomputers would take about 10,000 years to complete.[1] While other researchers have challenged this result and the practicality of the calculation itself, this demonstration offers a context for understanding just how powerful quantum can be.

Conventional computers store data using bits, which have a value of either zero or one, whereas quantum computing uses "qubits" (short for quantum bits), which can represent both zero and one simultaneously. Think of it this way: a coin is binary, heads or tails — the "value" is either one or the other. But when a coin is flipped, it's both heads and tails, as well as all combinations of the two. This fundamental

[1] "Google's Quantum Computer Just Aced an 'Impossible' Test," by Tim Childers, *Live Science*, October 24, 2019: www.livescience.com/google-hits-quantum-supremacy.html.

ability of a quantum system to exist in more than one state at any time is called superposition. Instead of coins, quantum abilities use atoms to fuel this new way of computing.

Some believe that Moore's Law — the ability to double the number of transistors in a dense integrated circuit about every two years — has hit the wall of physical limitations. So, while conventional computers will have a role to play in the foreseeable future, there are complex problems they'll never be able to solve. Algorithms written to take advantage of qubits can perform certain types of computations much more quickly and with much less energy than conventional computers. Herein lies the promise of quantum.

When does quantum computing become real in our industry?

No one knows for sure how to answer this question. True, there is hype that some characterise as overreach. But as time passes, the forecast for practical use cases compresses. Certain things are clear: Technology companies are investing heavily in quantum capabilities, and when quantum is commercially feasible, it will be a game-changer for how business is done. Companies in various industries are already experimenting with the technology to address logistics and investing in startups focused on the hardware, software, algorithms, security and analytics that will make quantum computing a reality.[2]

Therefore, as companies assess the "when" question and keep a watchful eye on market developments, they should also prepare for this brave new computing world. Numerous cloud environments already exist that allow companies to access quantum simulators and real quantum computers. Microsoft Azure Quantum, Amazon Braket and IBM Quantum Experience are a few examples, each one featuring rich development interfaces and tools.

Many companies think that when a competitor builds a better mousetrap, they can replicate it in a relatively short period. But that won't be possible with quantum since computing applications will be proprietary. It takes time and talent to prepare for a quantum world. The market experienced something like this four years ago with machine learning applications. However, quantum will pose an even steeper learning curve, requiring substantial emphasis on acquiring and skilling the talent needed to leverage this game-changing capability.

What do we do now?

There are several steps companies should take today:

- **Select a quantum champion.** Obtain executive sponsorship. Designate someone responsible for following industry progress on quantum capabilities and for leading preparations for the eventual quantum world, possibly within the CIO organisation.
- **Conduct a quantum-readiness assessment.** Ask questions such as: How much do we know about quantum computing? How will it likely be applied in our industry? What do we need to remain relevant and competitive as this advanced computing environment evolves? For example, take talent. Quantum requires significant training on new engineering and programming techniques to envision the problems to be solved and the coding required to address those problems using quantum algorithms and resources. There will be a shortage of skills required to take advantage of quantum computing for companies that wait too long to begin developing and acquiring them.
- **Identify quantum computing use cases and assess their value to your organisation.** The quantum champion should work with all business units to determine important business and technology issues the company is unable to address today but

[2] "Investors Tell Us Why They're Pouring Millions Into Quantum Computing," by Biz Carson, *Protocol*, May 4, 2020: www.protocol.com/manuals/quantum-computing/vc-investments-bullish-quantum-computing-coronavirus.

may be able to address using quantum. The various data analysis, simulation and optimisation issues should be ranked according to priority.

- **Uncover potential risks to encryption and other aspects of company security.** The threats quantum presents to conventional cryptography are formidable. When quantum computing becomes mature, it will also quickly make many of today's encryption methods obsolete and easy to crack. On the defensive security side, companies will find themselves in a new arms race to stay ahead of quantum decryption capabilities. In fact, the initial focus of quantum in business may very well be to safeguard data. That's why it's time to start thinking about cryptographic agility and assessing necessary changes. The National Institute of Standards and Technology (NIST) is currently evaluating new algorithms to replace those at risk.
- **Chart a quantum course and multiyear road map.** Based on the identified priority use cases and encryption and security exposure, lay out a road map for developing quantum capabilities.
- **Start your journey and reassess the road map every six to 12 months.** Update the road map based on new quantum-computing discoveries and developments, the emergence of new use cases, and relevant changes in the industry and business environment.

In summary, positioning a company for the quantum revolution is all about being watchful, prepared and flexible. Boards should advise their companies to start planning sooner rather than later to avoid resource challenges that could leave them missing out on the benefits and necessary protections of quantum. Understanding the opportunity and issues and preparing to seize and solve them when the inevitable inflection point arrives could yield dramatic business advantage — and disruption.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the opportunities and risks inherent in the company's operations:

- Do we understand what quantum computing is? Do we have a point of view as to how quantum will likely disrupt our industry? Are we aware of competitors focusing on how they will harness quantum? Should we sit and watch or get into the game?
- If we don't prepare for the advantages of quantum and our competitors do, will we be at a competitive disadvantage once it is deployed in the industry? Conversely, how might we leverage quantum computing to gain a competitive advantage in the future?
- Are there critical processes and technologies we have today that rely on encryption that quantum will make obsolete? Are there business challenges we're unable to solve today that quantum computing will be well-suited to solve in the future? If we don't know, should we find out?
- Are we positioned to tap into the available pool of quantum computing talent soon? Over the next three to five years?
- Is there effective governance over where and how we invest in quantum computing? For example, in leveraging quantum, what criteria do we use when choosing between financial optimisation and, say, the simulation of chemical reactions through trial and error for purposes of developing lifesaving medicine?

How Protiviti Can Help

Our quantum computing services help clients prepare today to manage risks and identify opportunities to take advantage of this powerful capability. While practical applications of quantum computing are still a few years away, now is the time to prepare to ensure your business is positioned to harness the power of quantum computing rather than become a casualty of the revolution. We help organisations in all industries identify real use cases, determine the value, assess their risk and take action to become quantum-ready.

Audit Committee Self-Assessment Questions

In these dynamic times, it is best practise for boards and their standing committees and individual directors to self-assess their performance periodically and formulate actionable plans to improve board performance based on the results of that process. To that end, audit committees should consider the illustrative questions we have made available at ***www.protiviti.com/US-en/insights/bulletin-assessment-questions-audit-committees****. These comprehensive questions consider the committee's composition, charter, agenda and focus, and may be customised to fit the committee's assessment objectives in light of current challenges the company is facing.*

protiviti®