The Real Business Case for Quantum Computing

Disregard the alarmist headlines: Quantum computers won't end privacy online. In fact, their most revolutionary impact may be felt offline.

Internet security could soon have a new enemy: quantum computers. Such computers will be able to **break** existing encryption algorithms, removing protection for data exchanged over the Internet. Those who build quantum computers will make a lot of **money**.

These statements make appealing headlines. However, we must exercise caution when thinking about real-world implications of quantum computing. In reality, a general-purpose quantum computer doesn't exist yet. The day it does, it will be fast, but pretty bad at solving cryptographic puzzles. Some companies – like European IT services corporation Atos – are already selling quantum software, without ever having built a quantum computer. And the true business case for using this technology should interest smart-city visionaries more than those who are concerned with Internet privacy.

Quantum is not for code breaking

Contemporary semiconductors process information using bits, that is, units that can take either a state of 0 or the state of 1. Quantum computing relies on qubits (aka quantum bits). A qubit can simultaneously take a state of 1 and 0. Hence, two qubits can represent four states, four qubits 16 states and so forth. In addition, qubits are "entangled" because they can interact with one another to arrive at a **solution**.

While the current semiconductors enable exact calculations (2+2=4), quantum computing is based on probabilities. In addition, most current qubit technologies require an extremely low temperature to operate. Higher temperatures decrease qubits' stability, ultimately increasing computational noise. When you compute 2+2, the quantum computer will return several results, with 4 ideally having the highest probability. Yet, given the noise, when someone computes 2+2 hundreds of times, it might be that in some of the iterations, 4 isn't the result with the highest probability. While companies invest a lot of money to reduce the noise in quantum calculations, it is likely to be there for a long time.

These difficulties could well make quantum processors unsuitable for common encryption problems. Computers rely on precise calculations when encrypting or decrypting files. A recipient would not be able to decrypt an encrypted message using a quantum processor. Such a processor would only be able to approximately apply encryption keys. Consequently, it might be **unable** to break encryption behind current Internet protocols.

Develop quantum software before hardware

As you can imagine, there is no single standard for building a quantum computer. It is as if we were in the **pre-ENIAC** days when no one knew how to build a transistor, not to mention a CPU. Companies like IBM or Microsoft are investing a lot of money to build quantum hardware. This is an expensive and highly uncertain task.

Atos, under the leadership of its CEO Thierry Breton, has chosen a different path. It has developed the Atos Quantum Learning Machine (Atos QLM) which allows programmers to write software without waiting for a general-purpose quantum computer to be built. The QLM can do that because it simulates the laws of physics that govern quantum computing. A similar technique is used to simulate behaviours of physical projects that don't yet exist, such as airplanes. For example, a programmer can state that she wants to simulate interactions with a 16-qubit quantum computer, and the platform will behave accordingly. As of July 2018, the QLM was capable of **simulating up to 41 qubits**.

As more and more companies use this platform, they are likely to converge on a common approach to program quantum computers and may also agree on what quantum hardware should look like. It would be like giving ENIAC's creators in 1940s a platform for writing programs on an Intel processor in 1970s. This, in turn, would allow engineers to create a better ENIAC in anticipation of Intel's architecture. Hence, software will drive the hardware with Atos leading the way into the future. According to the Atos executives I interviewed, their QLM sells really well in the United States. This makes them proud to be part of a European company that can compete on an equal (or better) footing with much larger American players. It also puts Atos at the core of the emerging ecosystem around quantum computing, as other participants develop technologies that would be compatible with QLM.

Quantum in smart cities

Despite its challenges, quantum computing is best suited for cases that involve massive data processing, but don't require 100 percent precision in computations. Future smart cities represent a context in which such problems abound. Imagine London or Paris full of driverless cars. The artificial intelligence algorithms, sitting under the hood of every smart car, would solve the local problems. They would navigate the streets by constantly scanning the car's environment to determine the best tactic, for instance, should the car stop or accelerate at the nearby intersection. Yet, such local decisions might not be optimal on a larger scale. Thus, the city might want to have a quantum computer to optimise the city-wide traffic flows. The system could give different suggestions to different cars to shorten their travel time. Even if a given forecast – e.g. the next five cars should detour via Street A to unclog Street B – is only 98 percent accurate, it would still be good enough on average. Everyone would have a better chance to arrive in time for dinner. Other possible uses of quantum computing include the optimisation of electrical grids: This is another problem that requires massive computational power, but can tolerate small errors.

Looking ahead

Working with quantum computers is a little like being in Alice's Wonderland. These computers will be powerful, yet imprecise; a general-purpose machine is not built, yet we can write software for it. They will not be privacy's enemies, but the friends of complex problems.

Andrew Shipilov *is a Professor of Strategy and Akzo Nobel Fellow at INSEAD. He is a programme director for* ***Blue Ocean Strategy****, an Executive Education programme. He is also a co-author of* ***Network Advantage: How to Unlock Value from Your Alliances and Partnerships****.*

Follow INSEAD Knowledge on ***Twitter*** *and* ***Facebook****.*

Find article at
https://knowledge.insead.edu/blog/insead-blog/the-real-business-case-for-quantum-computing-10836