**Quantum computing: what impacts on our daily lives?**

Since the 2000s, researchers around the world have been trying to develop the quantum computer which is based on important aspects of quantum mechanics such as superposition and entanglement. A classical computer program is a binary system (i.e. bits that can take the value of 0 or 1), whereas qubits (quantum and bits) would be the component of the quantum computer programs. Qubits can have multiple values simultaneously (for 2 qubits, it is a superposition of 00, 01, 10, 11). Instead of performing one calculation at a time, the quantum computer processes all the hypotheses at the same time. This speed is what makes quantum computing a very promising field in many different areas (not only in science but also in business…). When a classical computer would have taken ten million years to find the solution, a quantum computer will perform the calculation in just a few hours.

While it seems unrealistic to develop quantum computers as a personal tool in the foreseeable future for financial reasons, because of their fragility (to manipulate qubits, the temperature must be -273 ° C), but also because they would be useless when performing our daily tasks, many other applications are possible. This quantum technology could, for example, allow the optimization of logistics, weather forecasting (to build better climate models by studying more parameters) and plot the evolution of financial market. All of which would require calculations unachievable with conventional technologies. According to Bernard Ourghanglian, quantum computing is likely going to improve the AI applications as we know them today. Indeed, the results obtained by a team of physicists in California using quantum technologies regarding satellite image recognition are promising and better than with conventional technologies. In the longer term, the quantum computer could revolutionize our modes of communication by establishing the quantum internet.

However, our current data encryption technique, which is based on the "RSA" technique named after its three founders (R. Rivest, A. Shamir, L. Adleman) and has been effective for more than 40 years, could be inefficient against quantum computing. Indeed the mode of encryption, as we know it today, is asymmetric meaning that the public encryption key consists of the product of two huge prime numbers and is different from the private decryption key which consists of these two numbers, unknown to the rest of the world (if you want to know more of this subject, I strongly recommend the video on quantum computing by veritasium or the course on cryptocurrency by Brilliant). Public keys as well as encrypted messages could be intercepted. Using the public key, the quantum computer would perform the necessary computation to find the two prime numbers, the data could be decrypted easily therefor accessible by huge corporation like google or Microsoft who have invested in such promising technology. Today, some nations or independent organizations store encrypted data (such as passwords, search results, or other secret government information) in order to decrypt it in a decade or so during a procedure called "Store Now Decrypt Later". This is why NIST in the United States is working on the development of a post-quantum cryptography norm that could be integrated into the HTTPS protocol.

The main powers have already invested in this quantum race such as China with "its colossal investments", the GAFA which invest in "research centers that cost them tens of millions per year" as well as the European Union, not to mention the many renowned physicists renoun for their discovery in this field such as the French Alain Aspect, the American John F. Clauser and the Austrian Anton Zeilinger awarded the Nobel Prize in Physics for their discoveries on quantum entanglement.

However, this quantum race, which will revolutionize the internet of tomorrow, is far from over. Today, most quantum computers contain between twenty and a thousand qubits at most which are not necessarily all operational. Once the superposition of all possible results has been obtained, it must be possible to extract only the desired information; which for the moment is only feasible in some very specific cases, using for example the Fourier algorithm. Lately Microsoft announced a “ground-breaking discovery”, on the storage of qubits which would be step in the right direction towards the “quantum super-computer” (you can read this article for more information : “Microsoft achieves first milestone towards a quantum supercomputer”)