🡪Introduction:

It all starts with the so-called Moore's Law, the American engineer who co-founded Intel, said in 1965 that the number of processors in an integrated circuit would double every year. Then he reviewed this postulate and affirmed that it would double every two years, which actually happened over the following decades because the circuits became smaller and more powerful.

There is talk that, since 2012, this reality has been slowing down and to recover the pace it will be necessary to appeal to circuits built with other materials than silicon or its alloys. Intel and institutions such as MIT and the University of Texas work on this together with the biggest companies.

🡪What is a Quantum Computer?

In recent years, some large technology companies such as IBM, Microsoft, Intel or Google are working in relative silence on something that sounds very good: Quantum Computing.

The main problem with this, at least for us, is that it is difficult to know what exactly it is and what it can be useful for.

There are some questions that can be easily solved. For example, Quantum Computing is not going to be useful at the moment so that you have more FPS on your graphics card. Nor will it be as easy as changing your computer’s CPU by a “Quantum CPU” to make it hyper-fast. Quantum Computing is fundamentally different from the computation to which we are accustomed.

After this brief introduction, let’s define what a Quantum Computer is. Theoretically it is a computer that uses Q-bits to perform operations instead of the traditional bits of classical computers, which allows you to solve problems much faster, which would take an ordinary computer too long or even, it could be unable to solve.

The Quantum Computer that Google and NASA have is the famous D-WAVE 2. They acquired it in 2013 and both entities have collaborated in its development. This computer allows them to carry out research and development work much more quickly, especially in the artificial intelligence jobs they have been developing, especially Google.

🡪What is Q-bit?

To understand why we are interested, let's take a short break and think about how a classic computer works. The basic unit of information is the bit, which can have two possible states (1 or 0) and with which we can perform several logical operations (AND, NOT, OR). By joining n bits we can represent numbers and operate on those numbers, but with limitations: we can only represent up to 2 ^ n different states, and if we want to change x bits we have to perform at least x operations on them: there is no way to change them magically without touching them.

Well, superposition and entanglement allow us to reduce these limitations: with the superposition we can store many more than just 2 ^ n states with n quantum bits (qubits), and the interlacing keeps certain relationships between qubits fixed so that operations in one qubit they forcefully affect the rest.

🡪Quantum Computer vs Classical Computer

In the quantum world (physical phenomena at microscopic scales) a particle can have two or more value of an observable quantify, for example: let’s see this particle as if it were an Apple. This apple can be in two or more places at the same time, it can have none, two or more bites at the same time, it can be Green, blue, red, yellow or black at the same time etc. This phenomenon is called quantum superposition.

We can summarize in these four differences:

* In digital computing, a bit can only take two values: 0 or 1. In contrast, in Quantum Computing, the laws of quantum mechanics intervene, and the particle can be in coherent superposition: it can be 0, 1 and it can be 0 and 1 at a time (two orthogonal states of a subatomic particle). This allows several operations to be carried out at the same time, according to the number of Q-bits.
* With conventional bits, if we had a three-bit register, there were eight possible values and the register could only take one of those values. On the other hand, if we have a vector of three Q-bits, the partible can take eight different values at the same time thanks to the quantum superposition.
* A Quantum Computer of 30 Q-bits would be equivalent to a conventional processor of 10 teraflops (millions of floating point operations per second), when computers currently work in the order of gigaflops (billions of operations).
* In classical computing the binary system is used and in Quantum Computing the unary system is used.

🡪Problems of Quatum Computer

The de-coherence times for the candidate systems, in particular the transverse relaxation time (in the terminology used in nuclear magnetic resonance and magnetic resonance imaging) are typically between nanoseconds and seconds, at low temperatures. The error rates are typically proportional to the ratio between operating time versus decoherence time, so that any operation must be completed in a much shorter time than the decoherence time.

If the error rate is low enough, it is possible to effectively use quantum error correction, which would allow calculations times longer than the decoherence time and, in principle, arbitrarily long.

A limit error rate of 10^4 is often cited, below which it is assumed that the efficient application of quantum error correction would be possible.

Another major problem is scalability, especially considering the considerable increase in Qbits needed for any calculation that involves error correction. For none of the currently proposed systems is a design trivial capable of handling a high enough number of Qbits to solve computationally interesting problems nowadays.

🡪Practical Quantum Computer Applications

Big Data: The exponential computing power of quantum computing is of interest to the massive data processing.

Chemistry: It will accelerate the investigation of new medicines, materials and physical components at the molecular level.

Machine learning: Quantum computers will accelerate the automatic learning process for artificial intelligence.

Cryptography: Cryptography uses principles of quantum mechanics to guarantee absolute confidentiality of the information transmitted.

🡪Conclusion

In conclusion, Quantum Computers are based on the use of Qbits instead of bits, and gives rise to new “logical gates” that make possible new algorithms.

They have a calculation capacity much higher than the current computers thanks to the massive (exponential) parallelism due to the superposition of states in the Qbit.

One aspect to note is that in the field of cryptography they propose a new approach: absolute security control at the communication level and their capacity to perform factorization operations (decomposition into prime numbers), which represents a threat to the encrypted communications they use many institutions in their security systems, and that are based in turn on the difficulty of making codes.

Finally, to say that Quantum Computing is a field in which there is still much to discover.