Quantum communication, how does it work? Let's talk about the future with Angelo Bassi

di **Redazione Trieste All News** - 4 Ottobre 2020

How does a quantum computer work?

More or less everyone knows of the existence of **quantum theory:** it explains how it is possible, in the universe (and therefore also in the everyday reality and in our home: the old cathode ray tube television was an example of this) that quantities of energy are not continuously exchanged but through bundles, defined by specific and precise values. **Max Planck,** a German physicist who at the end of the nineteenth century was the father of these studies, was advised, when he was still a boy, not to study physics, because **almost everything had already been discovered;** it was not really so, and it was then understood that light is made of a little bit of electromagnetism and a little bit of particles, and that the quantum of electromagnetic radiation was the photon, an indivisible particle able to **bombard the nucleus of an atom and disintegrate it.**

The first half of the twentieth century, the period in which physics made, thanks to the studies of Planck and his contemporaries, enormous leaps forward, is now a hundred years away from us; studies and progress have never stopped, they have reached and surpassed new goals, and one of the thresholds that are about to be crossed, behind which lies a new world, is precisely that of calculation through quantum computers, and on this threshold **Trieste is facing,** ready to contribute to the step forward that will **transform our way of life again. Quantum computers** perform calculation procedures based on the probability of a certain object to be in one state or another before the measurement that will determine that state intervenes: it is the paradox of the cat, at the same time alive and dead, or rather neither alive nor dead (one of the most famous paradoxes through which quantum physics is explained and which highlights its limits), applied however to **data processing:** the quantum computer, or quantum calculator, calculates not only based on the on or off state of one of its internal switches (the famous 'zero' and 'one': bits) but on the probability that one of these states occurs, correlating them mathematically to those of other objects and making it possible to give a precise definition, for these switches, also to a state of 'on' or 'off' that we don't yet know: a bit like being able to precisely define the position of a spinning coin thrown in the air before it reaches us: **these 'superpositions' are called qubits instead of bits.** The whole thing becomes a complex calculation: a linear combination (that's what it's called) that talks about **'states**

of freedom' and can be represented with a sphere; and to leave all this to mathematical enthusiasts, and to get back to our little reference system, we can say that working with qubits you can make calculations much faster. We discuss this with Professor **Angelo Bassi,** an international reference scientist in this very field, who received the **New York Times**' praise in June this year, among others.

Professor, how do you build a quantum computer? By working with light, as in optical fibre?

"Those who design and build a **quantum computer** try to create a version of the classic computer that, however, passes a quantum current through its elements. Using light is one of the possible ways to make the elements communicate with each other, but not the best. A classical computer is made by **building and miniaturising a series of switches connected by 'cables'**, of smaller and smaller dimensions, up to the molecules: an electric current passes between these switches: and this is classical physics. In the quantum computer, on the other hand, we have components that are cooled to a very low temperature; the material of which they are composed begins to behave in a quantum way. And it that moment, essentially flows are created that are **not classical electric currents**: they do not exist only as a situation of 'pass current-not pass current' but that are at the same time a 'flow that passes and does not pass'.

Do real quantum computers already exist?

"News of a few days ago, which made a lot of fuss, is the publication by IBM describing the planned route, the roadmap, for its quantum computers. Until a few years ago the goal was to have a quantum computer with 10 or 12 qubits; they are just the basis, not even a real computer. **Today we are fighting to reach 100 or 200 qubits of processing capacity.** IBM expects a computer with **1000 qubits by 2023**; a number that seemed unreachable. Today IBM promises this, and it is not a company that has just entered the market. **From 1000 qubits, we will then reach a million**".

What is quantum computing?

"In some ways, the answer is trivial: it is a calculation based on the laws of quantum physics instead of classical physics. One can think of what **Richard Feynman**, one of his fathers, said in the 1980s: when we talk about computation, we think of the circuit model and the bits, zero and one, and the logical gates that change the value of bits. Feynman ultimately said that all this is beautiful, but that the computer is then a physical object made according to the laws of classical physics; if instead we design a computer that works according to the **laws of quantum physics,** we will have a new calculation tool. Quantum computation replaces classical bits with quantum bits, which are not worth only zero or one but can represent the superposition of different values: they can be in more than one state at the same time. It may seem only a **mathematical oddity** but in reality it is **something that can be achieved physically".**

How many states can a quantum computer qubit have?

"**Infinite**. And this results into a computer's ability to do macro-operations, to 'handle' larger amounts of data in the same unit of time?
"Essentially it means being **able to solve a problem faster.**

For example?

"Let's think of an **algorithm** to search a data in a **randomly organized** database, in which I have to identify one element among all the others. If I have to search for a single element among a number of elements — 'n' elements, then — typically I should do 'n' operations: unless I am lucky and try through a **probabilistic calculation**, I have to keep searching among all the data until I find exactly what I am looking for. In the quantum case, I can look for this element with the root of **'n' operations**; somehow, by

encoding the database in a quantum register and using the superposition of states that the qubit allows — and here I should explain the whole theory — I get to the solution of the problem faster and find the data I wanted".

So, I'm on Google, I do an Internet browser search on a huge amount of data that has been collected without any criteria, and I have an answer in a much faster time than today.

"Exactly. Or, I can use another, even more famous, textbook example: the **factorization of polynomials**. Typically, in computer security, numbers that are the product of a prime number play an important role, **like 15 which is 5 times 3.** Factoring a number, for example 15, is a classically difficult problem, even for a computer: the effort required increases exponentially with the size of the number, the bigger the number, the more difficult the factoring is. It is not possible to find, and one is assuming that there is no classical algorithm that can efficiently factor numbers, especially high numbers, even if there is no mathematical proof of this. And all cryptography, or at least much of **classical cryptography,** is based on this very principle".

It would take too long to break the protection key.

"**Exactly. It would take too long to factorise**; if you can't factorise, you can't break the encryption system, you can't crack the key. In 1994, Peter Shor demonstrated that the same algorithm, revised in quantum key, becomes easy: **it grows polynominally** and no longer exponentially".

What does this involve?

"It puts all current security encryption systems at risk. And in fact the secret services, like the **US NSA,** are very concerned. And governments are taking quantum computing very seriously: it is assumed that **China** has invested more than the equivalent of one billion euros. The **European Union plans to create a quantum cryptographic network** on the European continent itself".

Potentially, there would be no more computer security.

"For a short time. Just as the quantum computer is able to break one of today's security keys with potential ease, it can create much more secure ones. **And we get to the other side of quantum computing**: the quantum computer is one of the applications, then we get to quantum communication".

What is it?

"It is another important technology, which gives us back what the quantum computer takes away. With quantum communication you can **create protection keys** that are intrinsically safe: according to the laws of quantum physics, these keys cannot be cracked — and not in the sense that they cannot be breached, but in the sense that if someone tries to break a key you will notice what is happening. **And so, countermeasures can be taken immediately".**

And that would lead to computer security.

"On the distribution of **protection keys,** yes. That would lead to **complete security."**

And by adding a system based on the blockchain, for example a financial transaction system or an electronic voting system, with quantum communication we would have total protection?

“Clearly, computer security is a complex area of research that includes many elements. One example: I can have secure protection keys and a perfect system to generate them, but suffer from an imperfect authentication process — **i.e., for a payment,** for example, I believe I am talking to you, and so I am giving you my protection key, but in reality ‘you’ are not ‘you’, but someone else who has**somehow stolen your identity**. And if this happens, the protection key I give you is also stolen. So, I don’t just need **quantum technology and the blockchain** to achieve absolute protection, but certainly quantum technology and quantum communication guarantee a **much higher level of security** than today”.

And if a nation becomes the owner of quantum communication technology not owned by other nations, it may be able to threaten all classic systems, the ‘old computers’.

“There is much awareness of the **importance of making rapid progress.** We are talking about fibre-optic and satellite quantum communication and encryption networks. And just like **Europe**, so is the **United States”.**

A paradigm shift.

“**A paradigm shift, and a change of technology.** The classic computer was one, compared to previous calculation techniques and until the 1950s; and then, with the computer, the whole world changed. Then the Internet in the nineties. The quantum computer promises to change it again, and to cause a **similar revolution**“.

What are you doing in Trieste?

“Trieste has already had a renowned quantum physics school for decades, which includes **researchers from the University of Trieste** like myself, **Sissa** and **ICTP**. I think we can say that in Trieste there is one of the largest concentrations of **quantum physicists in Italy**“.

A ‘think tank’ on the Adriatic.

“I think so, I believe that it is difficult to find a concentration of brains engaged in physics, like here, in other parts of Italy. And Trieste has been able to show over the years that it is able to create synergies and succeed in carrying out great collaborative projects: I am thinking of **Elettra Sincrotrone,** of **ICGEB**. It is thanks to the strong collaboration between scientific institutions, politics, economics and the city itself. In the field of calculation and quantum technology, what has already happened in the past is currently being repeated, and I hope it will be completed”.
Is there already something specific, or are we talking about the future? “One of the first elements already visible is the support of the **Friuli Venezia Giulia Region,** which has approved and financed the **Quantum FVG** quantum communication project: it will start in 2021, will be implemented in **Trieste** and then extended to the whole region. This project will create the conditions to be able to distribute quantum keys”.

What does it take to do this?

“A communication channel. A satellite, for example, or optical fibre. And the instrumentation that allows the creation of the quantum keys themselves. Trieste already has an excellent optical fibre infrastructure, called Lightnet: a consortium led by the **University of Trieste** which is unique in Italy. It is a network parallel to others that serves institutions to communicate with each other and do research. We will experiment with quantum communication and cryptography on this optical fibre network: as was done at ESOF 2020, with the demonstration carried out together with Premier Conte. We used a section of **Lightnet’s fibre optic network** to create a secure channel between the University of Trieste and the Porto

Vecchio: with **Alessandro Zavatta**'s group at the **CNR**, which supported the quantum part, on this channel the rector **Roberto Di Lenarda** and premier **Giuseppe Conte** spoke on video call. However, it will be difficult to make quantum communication on optical fibre used only for this purpose: it would mean duplicating the existing optical fibre infrastructure. One of the next frontiers is therefore to use optical fibre already in use for other purposes: on the same fibre we will therefore make classic communication and quantum communication at the same time. In order to do this it is necessary to access optical fibres with special properties, and here again **Trieste** already has them at its disposal".

And the actual calculation, the supercomputers?

"At ICTP there are scientists who have experience in quantum computing; this is what I teach in my master's degree course at the University of Trieste, in collaboration with **IBM** and **Intel**. So we are already trying to go beyond research, to work with companies both in Italy and internationally; and it is also for this reason that the Minister for Economic Development, **Stefano Patuanelli,** is in favour of opening a quantum technology institute right here in Trieste, an idea supported by **Premier Conte** himself. Now we are working in this direction".

Do students show enthusiasm about it?

"I see it every day. And in addition to the students, who immediately approached the courses with great interest, there are young people who already have specific training and skills in the field and who are unfortunately working abroad because the conditions for doing so are not yet in place in Italy and there is no offer. These **young people** could start extremely solid and competitive lines of research in **Trieste**. It is essential to create the conditions to attract them and offer them work, to create an environment in which they can carry out their scientific projects. Above all because I believe that Italy is already in a good position to do so: but we need to do even better, well is not enough. We certainly need to invest more".

Shall we give the government a little poke?

"No. I'm used to being self-critical before criticising the government. So far, governments have undoubtedly invested little in research, but what the scientific community lacks is ambition and strategic vision. And the ability to work together to realise this vision. **Giving money,** if there is no clear project, is useless. If the projects are clear, if you collaborate, you create the conditions to attract investment; if the scientist has no ideas, politics does not give money. In **Trieste** there has been a concrete strategic vision and political will to achieve it, and this must also happen at a national level".

Will the quantum computer help in finding a cure for Covid-19?

"It's unlikely to make it in time, when it's really ready the **Covid** will already be behind us. In general, however, the answer is yes, quantum computers will be able to help medicine on two fronts: first, in **biochemistry**, in the study and testing of new **drugs and materials through the simulation of their properties**; a molecule is ultimately a quantum system, and the quantum computer is the natural tool to study them. And for a doctor, and this is the second front, being able to analyse new data and arrive at personalised medicine, designed for the specific patient. And even a person is a **complex system**: being able to have fast algorithms will allow to optimize even the medical answers".

And what about artificial intelligence? Will it benefit from the quantum computer's ability to quickly process huge amounts of information?

“For **artificial intelligence** to have at least a semblance of real intelligence, speed plays a fundamental role. **Manipulating information** is a problem, even if the quantity is large, but if there is time to solve it, the difficulty is to manipulate that same amount of data in a sufficiently short time to be able to react and respond adequately to the need that arises, **and that is what our brain does”.**

Will a quantum computer think? I only ask you for an opinion, of course.

“If you can achieve this, and if the quantum computer can give fast answers to **very complicated situations**, I think it can behave like a real intelligence. Not necessarily the same as human intelligence, **but very similar”.**

Thank you, Professor.

And if, but only for the time being, **classical computer technology is still able to handle any task assigned to a quantum computer** (and not everyone – even among experts in the field – believes that the effort and the game to develop new technologies are worth the effort), companies like **IBM** and **Google** are making systems capable of aggregating and processing more and more qubits accurately, they firmly believe it and are convinced that that step beyond the threshold of a new world is very close. **Why not believe it in Trieste too? And the right time is now.**