XXXIV UNIVERSITAT D'ESTIU D'ANDORRA
DEL 4 AL 7 DE SETEMBRE DEL 2017

Sessió del 7 de setembre del 2017

FUTUR QUÀNTIC

José Ignacio Latorre Sentís

Doctor en física i catedràtic de física teòrica a la Universitat de Barcelona,
investigador al Center for Quantum Technologies de Singapur

Doctor en física y catedrático de física teórica en la Universidad de Barcelona,
investigador en el Center for Quantum Technologies de Singapur

Docteur en physique et professeur des universités en physique théorique
à l'Université de Barcelona, chercheur au Center for Quantum Technologies de Singapur

Per citar aquest article / Para citar este artículo / Pour citer cet article :

LATORRE SENTÍS, José Ignacio. « Futur quàntic » [en línia], a: Universitat d'Estiu d'Andorra (34a : 4 - 7 set., 2017 : Andorra la Vella). *Tecnologia i humanitat, llums i ombres = Tecnologia y humanidad, luces y sombras = Technologie et humanité, lumières et ombres*. Andorra: Govern d'Andorra. Ministeri d'Educació i Ensenyament Superior. Universitat d'Estiu d'Andorra, 2018, p. 84-95 (978-99920-0-857-7) <http://www.universitatestiu.ad/UEA2017>

Bona tarda,

És un plaer que m'hàgiu convidat. És realment excepcional el tracte que m'oferiu i una satisfacció poder parlar de mecànica quàntica en aquesta universitat d'estiu.

Els científics com jo, que ens dediquem a la mecànica quàntica, estem molt contents en aquest període de la ciència, perquè vivim una revolució. Els humans estem a prop d'aconseguir controlar la natura en el seu àmbit més elemental, és a dir, en els àtoms i fotons individuals. De sobte, s'ha obert la possibilitat de fer coses que no havíem sospitat mai.

Aquesta xerrada, que no és gens tècnica, tracta d'explicar què és el que estem aconseguint en l'actualitat i quines conseqüències importants tindran aquests progressos en el futur. La xerrada es titula *Futur quàntic*, perquè la ciència condiciona de forma sistemàtica el futur del món i, de fet, tots els grans canvis en la història de la humanitat han estat relacionats amb el progrés científic.

Per començar d'una forma molt planera, vull esmentar certes notícies que apareixen als mitjans de comunicació i de les quals la gent no acaba de ser conscient. Per exemple, una notícia del desembre del 2015 diu: «Google ha comprat un ordinador quàntic»; a més, «aquest ordinador quàntic va cent milions de vegades més ràpid que un ordinador clàssic», com el que tenim tots. Això va disparar totes les alarmes dels empresaris i les institucions responsables de finançar la ciència. Si Google entra en el joc científic, ens hem de posar molt seriosos a l'hora de treballar, perquè ara la lluita ja no és exclusiva entre grups de recerca sinó que, a més, les corporacions que volen assolir i crear coneixement nou s'afegeixen a la competició.

Una altra notícia notable, també de l'any 2015, és que Hillary Clinton, quan encara competia per la presidència dels Estats Units, va dir literalment que «el repte de construir un ordinador quàntic provoca un daltabaix quant a la criptografia i la comunicació segura que fem servir». I afegia: «Els Estats Units necessiten fer un nou Projecte Manhattan per superar el que arribarà amb la computació quàntica.»

Una altra notícia, de l'abril del 2016, diu que la Unió Europea llança l'instrument més potent de recerca que té, anomenat Flagship (nau capdavantera), en tecnologies quàntiques, i se salta tots els protocols burocràtics dels dos projectes anteriors; un relacionat amb el grafè i un altre amb el cervell humà. El

tercer, referent a les tecnologies quàntiques, s'aprova sense anys de discussió sobre què es farà en ciència. S'aproven 1.000 milions d'euros per als propers deu anys dedicats a les tecnologies quàntiques. Un projecte, per cert, presentat a l'abril i, com veieu, aprovat al maig.

I una altra notícia d'aquest estiu: la Xina ha aconseguit un satèl·lit de comunicacions quàntiques que envia llum en forma de fotons, que anomenem *entrellaçats,* en un estat quàntic, a dos llocs del Tibet situats a 1.200 km de distància, i estableix per primera vegada una comunicació secreta basada en mecànica quàntica. La Xina ara mateix ja disposa d'una xarxa de 48 ciutats comunicades de forma quàntica, i avui en dia aquesta comunicació no es pot trencar de cap de les maneres.

És a dir, que les notícies hi són. Hi ha tot un món que avança, i la forma d'explicar-vos-el és resumint el control que han exercit els humans sobre la matèria en tres fases. En la primera fase, del 1900 al 1926, es van establir els criteris que permeten entendre la mecànica quàntica. En la segona, l'any 1926, aquests criteris es van fixar per escrit gràcies a Schrödinger, Bohr, etc.; Einstein també hi va participar. Tots els científics de principis del segle XX, en particular del centre d'Europa, van construir la mecànica quàntica. La tercera fase se situa de l'any 1926 al 2000, quan té lloc l'anomenada primera revolució quàntica. Les persones comencen a utilitzar la mecànica quàntica. Per exemple, el làser. Són fotons en un estat que anomenem de superposició coherent. És un estat genuí de la mecànica quàntica. És bo perquè podem concentrar les posicions d'energia notables en poc espai. Podem crear un bisturí i tallar materials, però també codificar informació, introduir-la en una fibra òptica i d'aquesta manera comunicar-nos amb tota la Terra, o podem corregir la miopia d'un ull.

Gaudim d'un instrument impressionant perquè diposita energia de forma molt precisa en un lloc. Disposem de transistors; els ordinadors fan servir física de l'estat sòlid quàntica. Passa el mateix amb les ressonàncies magnètiques, derivades del fet que les persones som capaces de modificar els estats quàntics dels nuclis dels àtoms dins del cos humà i, quan es desexciten, observar-los i prendre una imatge de l'interior de l'organisme. També comptem amb rellotges atòmics, amb precisions d'una part en un bilió i que posem en òrbita. Donen voltes al planeta, envien un senyal i, en observar la seva interferència, sabem on som a la Terra: construïm un GPS.

Insisteixo, tot és gràcies al fet de tenir un control quàntic de la matèria. Però, encara que sembli aclaparador, és molt groller. A partir de l'any 2000 −sobretot− ja no es tracta de manipular molts fotons o tot el cos humà, sinó que ara ens centrem en cada àtom, en cada fotó, i, per tant, s'obren perspectives noves: la computació quàntica, la criptografia quàntica, la simulació quàntica i els sensors de noves generacions… Tot això configurarà el nostre futur sí o sí, no hi ha opcions.

Ningú no dubta que explicar mecànica quàntica així d'autèntica no és fàcil. Intentaré limitar-me a explicar els elements mínims. Hi ha un fet fonamental que diu que no podem descriure el món com ho feia Newton: amb velocitat, acceleració i ja està. Com podem argumentar que aquesta no és la forma de procedir en el món quàntic? És molt fàcil. Permeteu-me una observació molt filosòfica però fonamental: quan les persones mesurem, afectem l'objecte que mesurem. Com puc saber que un cotxe és al carrer o que veig un ordinador? Hi ha una reacció que produeix un fotó, aquest fotó col·lideix amb l'ordinador, arriba al meu ull, diposita una energia que es dispara pel nervi i va a parar al meu cervell. El que ha passat és que un fotó ha tocat l'element i ha viatjat fins al meu ull. Per tant, hi ha hagut una interacció d'aquest fotó amb l'objecte abans d'arribar al meu ull.

Però si en lloc d'un cotxe fos un electró? El fotó arribaria a l'electró i rebotaria. Què li passaria a l'electró? Se n'aniria. Aleshores què sé? Què he mesurat? Hi havia un electró, però on és? No ho sé perquè la meva forma de mesurar l'ha pertorbat de tal manera que he perdut tota la informació referent a aquest electró. I això és el que anomenem principi d'incertesa: no tenim la capacitat de saber totes les propietats de la matèria perquè en el procés de mesurar l'afectem, la canviem. Com a conseqüència, la informació que n'extraiem senzillament és falsa.

Les persones no podem assolir coneixement sense pertorbar el que estem mesurant. Això és monumental des d'un punt de vista filosòfic i dona lloc a un paradigma diferent de la ciència. Ja no podrem parlar mai més de realitat objectiva perquè no és assolible pels humans. Tan sols podem considerar la informació extreta. Per tant, la mecànica quàntica ja no debat sobre velocitats, posicions i coses d'aquestes; només té en compte quina informació es té. D'això en diem funció d'ona, i codifica la informació del sistema. La manera d'assenyalar estats quàntics és mitjançant dues ratlletes.

I quina situació es pot arribar a donar? Imagineu que teniu una doble escletxa. Envieu una partícula i la detecteu a l'altre costat. Us trobeu a l'altre costat i la veieu arribar a dalt. Direm que la nostra informació del sistema és que aquesta partícula ha fet aquest recorregut i ha arribat a dalt. Però, què passa si ha passat per sota? També és una possibilitat. I què passa si no mirem per on ha passat la partícula? Quin camí ha pres? Què ens diu la mecànica quàntica? L'opció vàlida és la u o la dos?

La mecànica quàntica respon, en aquest cas, de forma molt profunda: la manera de mantenir la informació és la superposició de les dues opcions. Per tant, en mecànica quàntica hem d'arrossegar les superposicions. Això vol dir que hi ha sistemes quàntics la informació dels quals és insuficient, i caldrà decidir que es troba en una superposició d'opcions diferents.

Segurament heu sentit parlar del gat de Schrödinger, que fins i tot ha sortit a *The Big Bang Theory*. La paradoxa del gat de Schrödinger, proposada per aquest científic l'any 1935, es qüestiona les superposicions de la mecànica quàntica. Es va inventar un experiment, descrit per ell mateix de la manera següent: «Ficaré un gat dins d'una capsa on hi ha un àtom radioactiu, i si decau es disparará tot un mecanisme. Al final hi haurà un martell que baixarà, trencarà una ampolla d'àcid cianhídric (perquè fins i tot especifica l'àcid) i el gat morirà. Això només passarà si l'àtom es desintegra. Si no es desintegra, el gat viurà. Però si la capsa està tancada, quin és l'estat del gat?»

Aquí ve la paradoxa. La mecànica quàntica ens diu, de forma molt rigorosa, que la informació del sistema es troba en una superposició quàntica: que el gat sigui viu o que el gat sigui mort. Aquesta paradoxa va impressionar molta gent, i es va començar a generalitzar l'opinió que el gat era viu i mort alhora. No. La mecànica quàntica afirma que la informació sobre el gat és la superposició quàntica dels dos estats, però no que sigui viu i mort al mateix temps. També se sent dir que la mecànica quàntica afirma que pots ser en un lloc i en un altre alhora. No. Hi ha experiments en què potser no saps on ets i, per tant, has d'arrossegar la superposició.

Per il·lustrar que el gat de Schrödinger és un tema apassionant per a molta gent, s'han creat concursos de grafits del gat de Schrödinger. N'hi ha de molt divertits que il·lustren el pobre gat mort i viu i diuen: «Es busca viu i mort»; o hi apareix un metge que diu: «Senyor Schrödinger, tinc bones i males notícies sobre el seu gat.» És simpàtica, aquesta forma de fer-ne humor.

Veiem ja un primer aspecte molt interessant, i és que en el món quàntic cal arrossegar les informacions en superposicions. Podem designar l'estat "gat viu" com a «0» i l'estat "gat mort" com a «1». Així construïm la base de com manipularem la informació en l'àmbit quàntic. Atesa la novetat d'acceptar la superposició quàntica de 0 i 1, veiem que no és un bit clàssic d'informació; l'anomenarem bit quàntic o qbit. Una vegada tenim un qbit, la pregunta és si tot això és mentida o és veritat.

Us presento tres dels centenars de sistemes en què avui en dia els humans han aconseguit fer una superposició quàntica controlable de zeros i uns. En una banda, poso uns fotons que es poden fer amb polaritzacions. Hi afegeixo una trampa de ions que tenen els electrons excitats o no excitats i, a la dreta, una versió impressionant que és un corrent de superconductors que giren cap a la dreta o cap a l'esquerra. Cal acceptar la superposició de girar a la dreta i a l'esquerra. És a dir, la humanitat ja ha fet això. Per què no fer un pas més?

Imagineu-vos que tenim tres qbits. Quantes superposicions quàntiques hi haurà? Tot zeros, zero-zero-u, zero-u-zero…, vuit superposicions possibles. I poden aparèixer en un únic sistema físic. Amb un número «n» tindré un número exponencial de superposicions.

Així, en una trampa de ions amb 1.000 qbits, els estats clàssics que es tracten són 2^{1000}. Això atorga un avantatge exponencial al tractament d'informació, que és el que estem assolint. Així s'il·lustra la seva magnitud.

En resum, en l'actualitat les persones podem controlar la informació en forma de qbits, i en un únic sistema físic podem tractar un número exponencial d'estats, tots al mateix temps, mentre que, amb un ordinador clàssic, només podrien tractar-se d'un en un.

Aquesta és la gran promesa de la computació. Un petit exemple: imagineu que zero-zero-zero és el 0; zero-u-zero en base 2 és el 2; u-u-zero és el 6… Podrem fer una operació anomenada «1» que actuï contra el meu sistema físic. Típicament són irradiacions de làsers, i el resultat s'obté d'haver sumat 1. S'ha aconseguit construir una màquina que suma 1 a tres números alhora amb una única irradiació del làser. O sigui, que un ordinador quàntic té aquesta propietat tan impressionant del paral·lelisme en aprofitar les lleis quàntiques de la natura.

Quan ens preguntem per la importància d'aquest fet, acabem apropant-nos al món de les finances i de la política. Quins problemes rellevants hi ha al món?

N'hi ha un de crític, que és factoritzar. Hi ha problemes "fàcils": multiplicar, sumar… Fàcils vol dir que, per més que el número que es fa servir sigui molt gran, les operacions que es duen a terme no són gaires; és polinòmic. En canvi, hi ha problemes "difícils": si vull factoritzar un número gran (descompondre'l en números primers), necessito moltíssimes operacions.

Factoritzar és difícil. La transcendència d'aquesta dificultat rau en el fet que totes les nostres comunicacions i transaccions (amb entitats bancàries, amb el núvol, en llegir el correu de Gmail…) utilitzen un protocol criptogràfic que les fa secretes. Així, un *hacker* no pot veure, per exemple, les transaccions que fem amb el banc ni robar-ne la clau. Es codifiquen amb criptografia clàssica basada en un problema matemàtic: per crear la clau es multipliquen dos números, el producte dels quals és la clau. S'envia, la rep el client, es codifica la clau i es reenvia.

Si un *hacker* veu passar la clau, la pot agafar, factoritzar i, amb els dos factors obtinguts, podria llegir el missatge que s'ha enviat. Per tant, la computació quàntica posa en perill ni més ni menys que totes les comunicacions secretes de la Terra. Ara potser enteneu per què Hillary Clinton afirma: «El repte de tenir un ordinador quàntic ens força a utilitzar tota la nostra intel·ligència per tirar endavant.»

«La diferència de potència en el món clàssic és exponencial a l'esforç. En el món quàntic és polinòmica a l'esforç.» El primer missatge que vull transmetre és que als nostres laboratoris estem construint les tecnologies que permetran trencar tots els codis que fem servir avui dia.

Als qui treballen en un banc o es dediquen a la política, sentir aquestes afirmacions els pot posar nerviosos. Pot ser que cerquin a Internet les companyies més importants que aposten per fer un ordinador quàntic i busquin els inversors necessaris. Veuran, de sobte, una correlació entre els inversors i el problema que trenca la mecànica quàntica. És a dir, actualment arribem a una situació en què ja no val ser empresari o polític i no conèixer les capacitats de la ciència. Aquesta situació és molt comparable a la del final de la Segona Guerra Mundial, quan la gent no comprenia que els humans començaven a controlar certes propietats de la física nuclear que finalment van permetre construir la bomba atòmica.

Ja existeixen els primers xips. A Barcelona estem posant en marxa el primer grup de tot el sud d'Europa que vol crear un processador quàntic, amb la

modèstia que implica no disposar de diners. Almenys gaudim dels coneixements de les lleis de la física, que és la part més dura. La computació quàntica no només es podrà desprendre de tota la criptografia clàssica, sinó que la potència extraordinària d'un ordinador quàntic ens permetrà fer moltes més coses que no són possibles en l'actualitat.

A tall d'exemple, podrem dissenyar medicaments de forma més subtil; ens permetrà simular les estructures químiques i també els sistemes que són quàntics al mateix temps. És a dir, farem servir un ordinador quàntic per entendre la mecànica quàntica. A més, podrem treballar qüestions d'optimització, i això és imposant: gairebé tots els problemes que ens afecten a la vida es relacionen amb l'optimització. Per exemple, podrem resoldre problemes de trànsit, de temporització, així com problemes d'entrenament de xarxes neuronals, atès que la capa d'intel·ligència artificial següent ja necessita xarxes neuronals de milers de capes i s'han d'entrenar. Segurament ho farem amb ordinadors quàntics.

La mecànica quàntica també proporciona una solució futura a la qüestió del secret en l'àmbit de les comunicacions. Hi ha dues maneres d'intentar resoldre l'actual problemàtica que hi ha en aquest àmbit a escala mundial. Una és fer servir la criptografia postquàntica, que consisteix a substituir els algorismes actuals per uns altres de resistents a un ordinador quàntic. Una altra és utilitzar criptografia quàntica pura, que és una nova forma de generar secret. La criptografia quàntica és molt senzilla d'entendre, i per això torno als fonaments per explicar com podem comunicar-nos de manera secreta.

El problema sempre és el mateix, i l'anomenarem Alice, Bob i Eve. L'Alice vol comunicar-se amb el Bob en secret, però hi ha l'Eve que vol conèixer el secret. L'Alice i el Bob poden ser Leo Messi i Andrés Iniesta, i l'Eve pot ser Cristiano Ronaldo. A la pràctica, perquè s'entengui millor qui és l'Alice i qui és el Bob, l'Alice ets tu, el Bob és el banc i l'Eve és un *hacker*.

Al web Norse es poden veure mapes d'atacs informàtics. És un web de control dels atacs informàtics a la Terra que mostra en directe tots els atacs senzills, és a dir, els que utilitzen protocols fàcils i que miren un port específic del teu ordinador. Això representa milers d'atacs per segon al món. Si la pregunta és si hi ha *hackers* actuant, la resposta és que n'hi ha milers per segon. Per tant, no és una qüestió intranscendent, sinó que ens trobem davant un problema autèntic.

Per fer criptografia quàntica s'aprofita la propietat esmentada al principi, la que deia que si jo mesuro, modifico. Si jo mesuro un electró, el modifico. En comptes de pensar que això és un impediment per fer coses, es pot utilitzar per al nostre profit. Aquesta és la idea bàsica. Per exemple, si envio un spin o un fotó polaritzat en direcció vertical cap a dalt i el mesuro en vertical, la mecànica quàntica diu que el trobaré cap a dalt. Si l'envio en direcció horitzontal i mesuro en vertical cap a dalt, tindré un 50% de probabilitat de trobar-lo cap a dalt o cap a baix. És un fet de la mecànica quàntica, independentment que sigui un spin, un fotó polaritzat o el que sigui. Aleshores creem un protocol.

L'Alice comença a fer polaritzacions de fotons, per exemple, totalment aleatòries. Les envia i el Bob les mesura. Recordem que si era vertical cap a baix i es mesura en la direcció vertical, s'obté cap a dalt; si era horitzontal i es mesura en vertical cap a dalt, de vegades surt cap a dalt i de vegades cap a baix. Imaginem que ha sortit cap a dalt, és a dir, que la tercera línia, si ho mesuro horitzontalment, és a la dreta. Si el Bob fa públic en quines direccions ha mesurat l'Alice però no li diu el resultat, l'Alice és capaç de saber igualment que el Bob el 100% de les vegades ha trobat això; hi ha el 50% de probabilitats per a l'altra opció i el 100% de probabilitats per a l'altra.

Pot fer aquest càlcul, trucar al *New York Times* i dir: «Bob, elimina quan la probabilitat no sigui del 100%.» D'aquesta manera, envien estats quàntics sobre la xarxa i, amb un protocol aleatori d'enviar i de mesurar, l'Alice i el Bob aconsegueixen obtenir el mateix resultat i, per tant, establir una clau aleatòria. Això és la base de la criptografia. No obstant això, si apareix l'Eve, que vol interferir-hi i no sap com, mesurarà les polaritzacions a l'atzar en una direcció o una altra (vertical i horitzontal). Seguint els postulats de la mecànica quàntica, resultarà que un 25% de les vegades la seva acció pertorbarà el sistema de tal manera que l'Alice i el Bob no obtindran el mateix resultat.

Ras i curt: un fa una fibra òptica, hi envia fotons a l'atzar i l'altre els mesura com he explicat. S'estableixen uns qbits de control: si el 100% estan bé, ningú està espiant; si el 25% exacte estan malament, algú està espiant. I això es deu al fet que no hi ha manera de controlar com les persones modifiquem les propietats quàntiques de la matèria. Això està per sobre de tot: si algú mesura allò de què parlen l'Alice i el Bob, ho modifica. I no hi ha cap truc ni es pot fer res per canviar-ho.

En l'actualitat, s'inverteixen molts diners per tractar de no recórrer a tota la parafernàlia de fotons, sinó per provar de substituir l'algorisme que fem servir i deixar de multiplicar números i després factoritzar-los. D'això se'n diu criptografia postquàntica.

Qui inverteix en això? Respondrem que els bancs, però no és així. Actualment l'inversor més gran al món és la Xina, que és qui està creant aquesta criptografia esmentada, i en concret la desenvolupa al Tibet.

Finalment, faré esment del món de la política i els negocis, perquè això és el que afectarà la nostra vida en els deu anys vinents.

Per començar, cal entendre que la lluita rere aquest àmbit de la ciència és, en realitat, global. Tots hi lluitem. He parlat dels Estats Units, que tenen Google, IBM, Microsoft, DARPA (la xarxa militar), el Jet Propulsion Lab (que també és militar), Los Álamos, les universitats… Avui dia, totes aquestes entitats disposen de prototips d'ordinadors quàntics. Per exemple, s'acaba de fer públic que recentment s'ha creat un ordinador de 22 qbits, IBM n'ha instal·lat a la xarxa un de 15, i a Internet es pot consultar el web d'IBM Quantum Experience i veure que, ara per ara, ja es pot fer un ús remot d'un ordinador quàntic.

Pel que fa a la Unió Europea, ja he esmentat que ha llançat el Flagship. A la resta del món hi trobem la Xina, amb el satèl·lit; països com el Canadà, que ha construït un ordinador quàntic que es diu D-Wave i que ja s'ha venut, ja és comercial; Singapur, on jo he treballat, o Israel, amb avenços molt importants en computació quàntica.

La lluita de les tecnologies es basa en aquestes cinc línies: computació, comunicació, sensors, simulació i algorismes. No us he parlat de les tres últimes, però us en donaré dos exemples perquè veieu la magnitud del progrés actual.

Per al control de dos àtoms, de com s'entrellacen, hem aconseguit fer rellotges atòmics que, avui dia, no són precisos en una part en un bilió, sinó en una part en un milió de milions, és a dir, una part en 10^{18}. Això és més precís que un segon a l'edat de l'univers. L'univers té 1.420 milions d'anys i estem parlant de 10^{17} segons. Aquests rellotges de què ja disposem als nostres laboratoris són més precisos que un segon a l'edat de l'univers. Per què necessitem un rellotge precís? Per exemple, per al GPS. Això obre les portes a tenir localitzacions a nivell de micra.

Imagineu-vos localitzar a l'escala d'una micra. Si en aquests moments tinguéssim a les mans un rellotge atòmic, seria possible posicionar un punt dins de l'habitació on ens trobem amb la precisió d'una micra. Seria com un bisturí infinitament més precís que la mà d'un humà fent una operació. És un salt de precisió.

Un altre exemple que m'agrada molt és que avui en dia aconseguim agafar partícules de diamant, que és carbó 12 perfecte, fer-hi un forat a dintre i ficar-hi un únic àtom de nitrogen. El carbó el protegeix. La propietat quàntica del nitrogen, anomenada spin, es controla des de l'exterior, i és molt estable perquè és dintre del carboni. Si a fora hi col·loquem una proteïna, resulta que les propietats de l'spin són sensibles a l'estructura de la proteïna. Per tant, podem començar a saber coses d'una proteïna amb un únic àtom.

Fem un microscopi amb un àtom. Res d'enviar llum de nou: un àtom. No sé com explicar com és d'impressionant el salt entre no controlar centenars de milers o milions d'àtoms alhora sinó un, que és la gran frontera de la precisió. Fa un temps feia xerrades de divulgació científica i al final sempre em feien la mateixa gran pregunta: «I això, quan?» La primera resposta és que ja hi ha coses: tenim la màquina que ja he esmentat, la D-Wave. També hi ha un físic americà pagat per Google que ha dit que a finals d'aquest any aconseguirà el que en diu «supremacia quàntica», una expressió amb què gran part de la meva comunitat no està d'acord. Per primera vegada, un càlcul fet per un ordinador quàntic ja no serà reproduïble pel més potent dels ordinadors clàssics del món, i amb aquest pas farem el salt. Per primera vegada tenim una potència de càlcul superior a la clàssica.

També voldria fer referència a tots els grups científics d'arreu: sempre em sap greu no esmentar la ciència autèntica bàsica que hi ha en totes les institucions.

Però per a mi la gran pregunta no és quan. Per a mi, la pregunta és qui. Es parla sempre d'avenços tecnològics i la pregunta és qui dominarà això; a qui pagaré jo.

Deixeu-me ser més concret. Quan dic *qui* vull dir si serà una nació (per tant, subjecta a les lleis internacionals que fem servir cada dia) o serà una corporació. Serà Google? Qui serà? La recerca que es faci serà oberta o propietària? Ja vam assistir a aquesta lluita amb la seqüenciació del genoma humà. De qui és el genoma humà, d'una corporació o de tots nosaltres? Per tant, aquí es disputa un fet molt important, i és si les institucions públiques han de finançar la recerca

d'aquest estil només pel fet que no quedi en mans de corporacions. I encara hi ha una pregunta més rellevant: hi haurà política darrere de tot això? La bomba atòmica precisament va provocar tota la guerra freda, o sigui que òbviament sí què hi ha política sempre que hi ha un instrument potent, i la computació és un instrument potent: tota la nostra vida es basa en la computació.

També voldria referir-me al món dels negocis. A mi sempre m'agrada dir això: sí o sí. Hi ha noves tecnologies quàntiques disruptives. Cal demanar-se si s'està ben informat i saber si això afecta o no afecta el nostre negoci. Afecta la banca? Sí. Afecta el món de la farmàcia? Sí. Afecta el fet de fer un full d'Excel per controlar els comptes? No. No tot el que és càlcul necessita gran quantitat de càlcul, és a dir que certs negocis sí que es veuran afectats.

L'any 1990 jo era al CERN quan es va inventar el WWW. És una eina de comunicació que s'utilitza actualment i que vam començar a emprar els científics al CERN per enviar-nos dades entre nosaltres. En tornar a Espanya deia a tothom que podria accedir a l'ordinador d'una altra persona. La computació quàntica és brutal. És un canvi de paradigma, com ho ha estat Internet.

El coneixement avançat no només necessita diners, sinó talent. Per tant, cal apostar per les persones que en saben. Això dona un avantatge als països capdavanters i, encara que no ho sembli, tot Europa és capdavantera. I les nacions que no disposen del talent suficient per aconseguir-ho van a la cua, fet que les posa en situació de perill.

Tanmateix, sempre que hi ha un perill hi ha una oportunitat. Així que ja hi ha inversors per tot el món esmerçant recursos en assumptes de computació quàntica. Encara que aquests inversors siguin advocats, per posar un exemple, saben que hi ha un avantatge si s'inverteix en aquesta matèria.

En l'esfera política, els grans països estan totalment bolcats en això. A Espanya agrada la idea de ser un jugador important (a Andorra diria que no us afecta).

Si esteu preparats per a un futur quàntic, segurament ara la superposició "de cap a dalt" ha començat; ja hi tenim un trosset "de cap a dalt".

Moltes gràcies