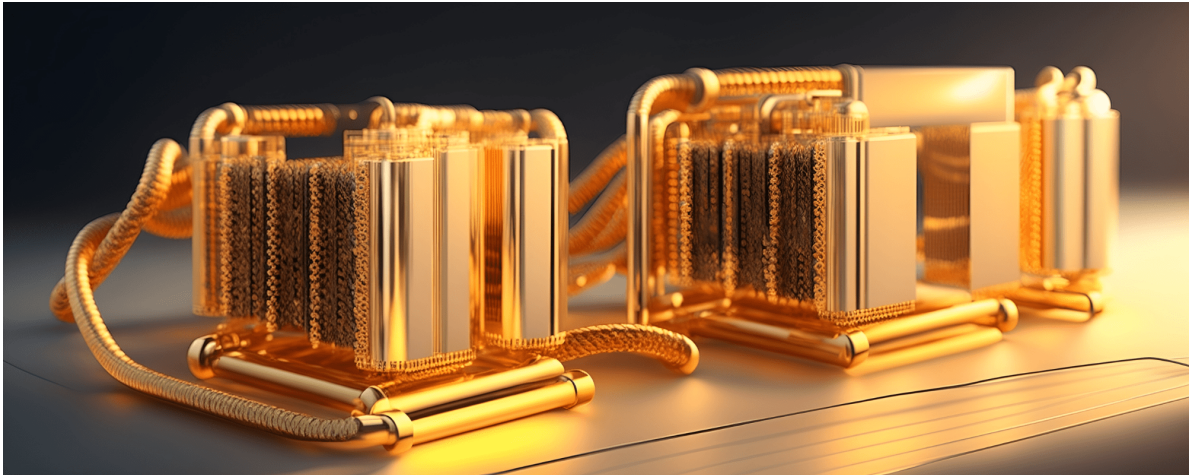


# L'ordinador quàntic: un camí de ciència, tecnologia i sobirania

Alba Cervera Lierta



Llum, espai i ordinadors quàntics. Conceptualització: Luisa Quiroga

“Aquesta és, en el millor dels sentits, la idea més absurda que he sentit mai” [1]. Aquesta va ser l’observació que el Premi Nobel de Física Richard Feynman va amollar a Daniel Hillis quan Hillis li va explicar que volia fundar una empresa per construir un ordinador amb un milió de processadors treballant en paral·lel. La fascinació de Feynman per treballar en les idees més “absurdes” que se li presentaven el va portar a fer una estada al MIT amb l’equip de Hillis l’estiu del 1983 per construir el prototip de la Connection Machine, un dels primers superordinadors. No totes les empreses tenen la sort de tenir un Nobel de Física dissenyant els seus algorismes i processadors. I és que Feynman no va tenir cap problema a aprendre des de zero i especialitzar-se en un camp, el de la computació en paral·lel, on tot estava per fer.

El primer algoritme que es va executar a la Connection Machine va ser el del càlcul de logaritmes, desenvolupat pel mateix Feynman quaranta anys abans durant el projecte Manhattan. Immediatament després, Feynman va utilitzar aquest primer superordinador per fer càlculs de física de partícules de forma molt més eficient que en els ordinadors existents de l’època. I és que l’interès d’aquest físic per les màquines de computar era clar. Desxifrar els mecanismes de la natura és cada cop més i més costós matemàticament, i es requereix una potència de càlcul creixent a mesura que baixem més al detall. De fet, la computació tradicional, anomenada “clàssica”, troba un dels seus topalls en el fet de voler simular la física dels engranatges més petits de la natura: la física quàntica. Aquest fet començava a ser ben conegut per la comunitat científica als anys vuitanta, i sobretot per Feynman, que tot just un parell d’anys abans de la seva “estada d’estiu” va impartir un

seminari magistral sobre els límits de la computació clàssica i la necessitat de la computació quàntica.

## La primera revolució quàntica

Fa més d'un segle naixia la física quàntica. Aquesta teoria física va ser capaç de descriure fenòmens i experiments que la coneguda com a física clàssica no podia explicar. Les conseqüències que es van anar desprenent d'aquesta teoria eren sorprenents i, en molts casos, antiintuïtives, però també ens van permetre entendre fenòmens com ara les reaccions nuclears del nostre Sol o les propietats dels elements químics i les seves reaccions. Aquesta teoria física és la més precisa de totes i, per increïble que ens semblin les seves prediccions, és la que més s'ha testat i validat durant els darrers cent anys.

Tan bon punt els humans descobrim el funcionament de fenòmens naturals, el nostre instint ens impulsa a crear eines que els explotin. La física quàntica no en va ser una excepció. De seguida van començar a aparèixer les primeres aplicacions i dispositius que es van poder dissenyar gràcies a entendre la mecànica quàntica: el làser, les plaques solars, el GPS, la ressonància magnètica, el transistor... Tots van anar sorgint a mitjan segle XX i constitueixen un període que es coneix com a *primera revolució quàntica*. Aquests invents, i molts d'altres, van ser possibles gràcies al fet d'entendre fenòmens quàntics col·lectius.

Durant aquells anys, s'estaven produint altres revolucions tecnològiques en paral·lel. En concret, gràcies a entendre la física dels semiconductors, va sorgir el transistor (1947) i, posteriorment, els seus successors, els microprocessadors. Amb ells, els humans comencem a ser capaços de fer càlculs automatitzats més i més complexos, amb més precisió i sense errors. A poc a poc vam aprendre formes cada vegada més sofisticades de processar informació codificada en les seves unitats mínimes, els bits: els famosos 0 i 1 en què es basa tota la computació clàssica.

Fa més d'un segle naixia la física quàntica, que va ser capaç de descriure fenòmens que la física clàssica no podia explicar. Per increïbles que semblin les seves prediccions, és la teoria que més s'ha testat i validat durant els darrers cent anys

Alguns físics es van començar a preguntar també què passaria si la informació es codifiqués en bits amb propietats quàntiques, anomenats qbits. El camp de la informació quàntica també va sorgir en aquells anys, encara que, en comparació amb la seva germana, la informació clàssica, es va desenvolupar pràcticament per complet en el terreny teòric, en no existir dispositius capaços de contenir i de controlar qbits.

La computació tradicional va anar avançant a un ritme frenètic i els càlculs es van anar intensificant a mesura que els ordinadors eren més i més potents. Els humans també tenim

l'instint de posar tots els nostres invents al límit i, en el cas dels computadors clàssics, un d'aquests límits es troba en la quàntica.

Arribem, doncs, a l'any 1981, quan Feynman va posar fil a l'agulla. En una de les seves ponències, va manifestar la importància de construir ordinadors amb una capacitat de computació que augmentés a la vegada que la mida dels sistemes que volem simular amb ells. Això significa que si, per exemple, volem utilitzar un ordinador per sumar dos nombres, necessitem que els seus recursos (memòria o nombre d'operacions per segon) siguin tan grans com la mida dels nombres que volem sumar. En canvi, si volem multiplicar-los, necessitem que aquest ordinador tingui uns recursos que creixen com el quadrat de la mida dels nombres que volem multiplicar. En el cas de la simulació dels sistemes quàntics, els recursos necessaris creixen exponencialment. Aquest tipus de creixement fa que per a sistemes quàntics petits puguem utilitzar un ordinador estàndard sense problemes, però, a mesura que els sistemes es fan grans, ni tan sols un superordinador té prou recursos per emmagatzemar tanta informació (no cal dir per fer operacions). El motiu és que els ordinadors clàssics codifiquen la informació en bits, i per codificar informació d'un estat quàntic a una cadena de bits en necessitem un nombre exponencial. L'observació de Feynman va consistir a remarcar que, si en lloc de bits clàssics utilitzéssim bits quàntics, no tindríem aquest problema de creixement exponencial de recursos computacionals. En altres paraules, cal utilitzar ordinadors quàntics per simular i estudiar sistemes quàntics.

Significa això que els ordinadors clàssics són inservibles per estudiar la física quàntica? La resposta és que no. Per una banda, aquest creixement exponencial de recursos que intentem evitar es dona en el pitjor dels casos: no tots els fenòmens o sistemes quàntics tenen unes necessitats computacionals tan grans. Per l'altra, podem (i fem) aproximacions en els nostres càlculs que ens permeten obtenir bons resultats. Fa anys que utilitzem superordinadors per estudiar sistemes quàntics com la química, la ciència de materials o la física de partícules, i això ens ha permès avançar en infinitat de camps i d'aplicacions. Tot plegat ens dona més motius per perseguir la invenció d'ordinadors quàntics que ens obrin la porta a entendre millor la física del món microscòpic i, en conseqüència, ens aportin també més aplicacions.

## La computació en l'era de la segona revolució quàntica

A banda de Feynman, altres físics de l'època havien estat treballant en les possibilitats de la computació quàntica. Yuri Manin va arribar a la mateixa conclusió que Feynman pràcticament alhora. Paul Benioff va fer una anàlisi sobre el model matemàtic en què es podia basar la computació quàntica: la màquina de Turing quàntica. Durant els anys vuitanta, molts físics i matemàtics van començar a proposar algoritmes quàntics i a estudiar-ne la complexitat computacional. La computació quàntica va demostrar que certs algoritmes es poden accelerar substancialment amb l'ús de qbits.

El camp va experimentar una gran sacsejada quan el físic Peter Shor va proposar un algorisme capaç de factoritzar nombres de forma eficient amb un ordinador quàntic. Una aplicació matemàtica més si no fos perquè tota la criptografia que utilitzem avui dia es basa

precisament en el fet que factoritzar no sigui gens fàcil. L'algoritme de Shor permet a un ordinador quàntic ideal trencar tota la criptografia actual, i suposa un gran risc per a tota la ciberseguretat. Aquest descobriment va posar la computació quàntica al focus de la indústria i els governs en demostrar que un ordinador quàntic podia ser usat per a molt més que per simular sistemes físics complexos.

Arriba el nou mil·lenni i, amb ell, les primeres portes lògiques quàntiques experimentals. Cirac, Zoller, Mølmer i Sørensen, entre d'altres, desenvolupen la teoria que quasi immediatament s'aplica experimentalment i que permet fer de la computació quàntica una realitat. Amb les portes lògiques, arriben també els qbits. Sorgeixen cada cop més i més propostes sobre com construir xips quàntics. A diferència de la computació tradicional, basada en el silici, hi ha moltes tecnologies possibles per poder fer qbits: ions atrapats, fotons, superconductors... Totes elles se segueixen construint i millorant en paral·lel, ja que tenen característiques molt diferents entre si.

L'algoritme de Shor permet a un ordinador quàntic ideal trencar tota la criptografia actual, i suposa un gran risc per a la ciberseguretat

En definitiva, la tecnologia ja ha avançat prou per fer de la computació quàntica una realitat. I, amb això, les empreses i els governs comencen a invertir seriosament en aquesta segona revolució quàntica, que, a diferència de la primera, ja no es basa en fenòmens quàntics col·lectius: ara som capaços de controlar sistemes quàntics individuals. Aquesta revolució tecnològica abasta les comunicacions, els sensors i, per descomptat, la computació.

## Ciència, tecnologia, sobirania

Ens trobem en un moment històric i privilegiat. Els prototips d'ordinadors quàntics són ja una realitat i cada any ens trobem amb alguna fita tecnològica. Universitats de tot el món tenen grups dissenyant, construint i millorant ordinadors quàntics fets de diverses tecnologies. Les empreses i les *start-ups* que construeixen aquests dispositius comencen a oferir els seus serveis. La inversió pública i privada no para de créixer i cada cop en sorgeixen més aplicacions potencials.

Tot i així, no tot és tan ideal com ens agradaria. Sí, tenim ordinadors quàntics, però encara són petits i imperfectes. Per poder implementar els algorismes quàntics més potents que coneixem, necessitem milions de qbits que siguin pràcticament perfectes, és a dir, que els possibles errors que puguin sorgir durant la computació quàntica es puguin corregir automàticament. Malauradament, la computació quàntica encara no està tan avançada perquè això sigui possible. Els ordinadors quàntics actuals estan formats per un grapat de qbits "sorollosos" (sense correcció d'errors). Ens trobem davant el que es coneix com a

*noisy intermediate-scale quantum computation* (NISQ). Tot i així, seguim endavant i, alhora que la tecnologia millora any rere any, també ho fan els algoritmes i les aplicacions. Moltes persones ens dediquem a buscar com treure el màxim profit dels ordinadors quàntics actuals i a preparar-nos per als ordinadors quàntics del futur.

I és que en aquest punt tenim dos camins: quedar-nos aturats i esperar que la tecnologia millori i en el futur algú ens l'ofereixi, o prendre la iniciativa i ser nosaltres qui desenvolupem aquest ordinador quàntic del futur.

Europa està adoptant el segon camí. Des del 2018 tenim iniciatives com el projecte Quantum Flagship (vaixell insígnia quàntic), amb mil milions d'euros d'inversió en tecnologies quàntiques que es distribueixen en cinc grans pilars: comunicació, sensors, simulació, computació i ciència bàsica. En aquests moments, el programa Quantum Flagship està encetant la segona fase de transferència tecnològica, que intenta construir els prototips d'aplicacions quàntiques estudiades durant la primera fase del projecte. Gràcies a aquest projecte estan sorgint moltes *start-ups* europees especialitzades en la fabricació d'ordinadors quàntics i els seus components. També Europa ha inclòs la computació quàntica en la recent Llei europea de xips (European Chips Act). El missatge és explícit: Europa no vol dependre en un futur de tecnologia estrangera de xips clàssics i quàntics, volem ser-ne els proveïdors, i el suport a la indústria i la ciència europea és clar.

En aquest punt, en què tenim universitats i centres de recerca estudiant i desenvolupant la tecnologia bàsica i en què s'està creant el teixit industrial necessari per explotar aquesta tecnologia i construir els ordinadors quàntics, on queden els usuaris? Al cap i a la fi, algú haurà d'utilitzar aquesta computació per descobrir-ne aplicacions.

La computació quàntica ha arribat a un nivell de desenvolupament suficient perquè surti dels laboratoris i es pugui oferir als usuaris que vulguin explotar-la. Des de fa gairebé deu anys, algunes empreses com IBM, Google, Alibaba i *start-ups* com Rigetti Computing, D-WAVE Systems o IonQ ofereixen accés remot als seus ordinadors quàntics. De fet, proveïdors del núvol com Amazon Web Services aglutinen molts d'aquests ordinadors quàntics i ofereixen un entorn únic d'accés a aquestes màquines. Malgrat que l'accés a alguns dispositius petits pot arribar a ser gratuït, el cert és que els preus per accedir als ordinadors quàntics més avançats estan augmentant de manera significativa, fins al punt que poden ser prohibitius per a la majoria d'usuaris potencials. En una tecnologia com la computació quàntica, que promet ser tan disruptiva, garantir-hi l'accés als investigadors i investigadores i a les petites empreses que volen estudiar-ne possibles aplicacions esdevé fonamental. A aquesta situació cal afegir-hi el vessant polític: qui tindrà els coneixements i la indústria capaços de construir i d'utilitzar la computació quàntica? Estarà únicament en mans privades? Quins països i regions tindran aquestes infraestructures quàntiques?

En aquest punt és on els centres de supercomputació fan un pas endavant i ofereixen la seva experiència pel que fa a mantenir i donar serveis de supercomputació també en la computació quàntica. De la mateixa manera que el projecte Quantum Flagship està finançant el desenvolupament científic i tecnològic de les tecnologies quàntiques (entre elles, la computació), EuroHPC —la branca de la Unió Europea que coordina els projectes

de computació d'altres prestacions— ha començat a finançar projectes d'adquisició, instal·lació i operació d'ordinadors quàntics en entorns de supercomputació. D'una banda, l'objectiu de la iniciativa EuroHPC és garantir un accés públic a ordinadors quàntics, de la mateixa manera que ja fa anys que es garanteix per a superordinadors clàssics. De l'altra, es pretén fomentar el teixit tecnològic europeu adquirint tecnologia desenvolupada a la Unió Europea.

La tecnologia ja ha avançat prou per fer de la computació quàntica una realitat; les empreses i els governs comencen a invertir seriosament en aquesta segona revolució quàntica. Tot i això, els ordinadors quàntics encara són petits i imperfectes

A més, no s'ha d'oblidar la dimensió científica, i és que tots els algorismes quàntics necessiten un component de computació clàssica. Per culminar qualsevol algorisme quàntic, cal preparar i processar gran part del problema utilitzant computació tradicional. La idea principal és que només s'executa part de l'algorisme (la més costosa) en el xip quàntic, mentre que la resta és computació tradicional. A més, el mateix disseny i control dels ordinadors quàntics es pot beneficiar substancialment dels avenços en la computació clàssica. Per tant, els ordinadors quàntics no competiran contra els superordinadors, sinó que en formaran part. Un superordinador no és res més que molts ordinadors connectats i treballant en paral·lel. De la mateixa manera que els superordinadors actuals poden contenir diferents tipus de processadors (CPU, GPU, TPU...), també poden contenir processadors quàntics, que s'utilitzaran únicament per a les aplicacions en què la computació tradicional es pugui quedar curta per la naturalesa del problema que s'ha de resoldre.

## Desplegament d'ordinadors quàntics a Europa i a Espanya

En aquests moments podem trobar diversos prototips d'ordinadors quàntics distribuïts per universitats, centres d'investigació i empreses en territori europeu. La gran majoria estan en un entorn de desenvolupament, és a dir, tenen l'accés restringit als científics i científiques que els construeixen i estudien. De manera natural sorgeixen iniciatives per ampliar aquest accés a altres usuaris per als prototips més avançats. Països com França, Finlàndia, Alemanya, Itàlia, Països Baixos o Espanya han encetat projectes que persegueixen donar accés a ordinadors quàntics. L'EuroHPC també està impulsant la Infraestructura Europea de Computació Quàntica i Simulació (EuroQCS) instal·lant ordinadors quàntics de diferents tecnologies i de fabricació europea en centres de supercomputació.

En concret, a Espanya tenim el projecte Quantum Spain, adreçat a la Xarxa Espanyola de Supercomputació (RES) i coordinat pel Centre Nacional de Supercomputació, el Barcelona Supercomputing Center (BSC). L'objectiu d'aquest projecte és instal·lar un ordinador

quàntic al BSC, l'accés al qual es donarà a través de la Xarxa Espanyola de Supercomputació de forma gratuïta, seguint els mateixos protocols que amb l'accés als superordinadors de la xarxa. L'empresa encarregada de construir aquest ordinador quàntic serà la *start-up* espanyola Qilimanjaro, juntament amb la gran empresa de telecomunicacions GMV. Aquesta unió d'empreses va acompanyada de proveïdors tecnològics europeus, complint així els objectius que ens marca la Unió Europea d'apostar per la sobirania tecnològica. A més de tenir aquest ordinador quàntic, la Xarxa Espanyola de Supercomputació també desenvoluparà emuladors quàntics que permeten simular el comportament d'ordinadors quàntics fins a certa mida en un entorn controlat, per així estudiar els algorismes quàntics sense necessitat d'utilitzar un ordinador real. Quantum Spain també persegueix desenvolupar nous algorismes i aplicacions, i per això la xarxa col·labora amb multitud d'universitats i centres de recerca espanyols experts en aquest camp. Finalment, una peça fonamental en qualsevol desenvolupament tecnològic és la formació de la nova generació d'experts i expertes en aquesta tecnologia. També forma part dels objectius d'aquest projecte impulsar totes les activitats i iniciatives que contribueixin a l'atracció de talent cap a la computació quàntica.

Gràcies al projecte Quantum Spain i a l'experiència demostrada en supercomputació, Europa ha seleccionat Espanya com un dels primers nodes de l'EuroQCS. El BSC tindrà un segon ordinador quàntic finançat per la Unió Europea a través de l'Empresa Comú d'Informàtica d'Alt Rendiment Europea (EuroHPC JU). Els dos ordinadors quàntics s'integraran al superordinador MareNostrum 5, un dels més potents d'Europa. Així, Espanya tindrà una infraestructura de computació pionera i heterogènia, amb processadors amb diferents característiques. Els dos projectes espanyols, Quantum Spain i EuroQCS-Spain, han estat possibles gràcies al finançament de la Secretaria d'Estat de Digitalització i Intel·ligència Artificial amb els fons del Pla de recuperació, transformació i resiliència (PRTR).

## Una mirada al futur

La lluita europea per assolir la sobirania tecnològica es va abandonar durant molts anys en favor dels suposats beneficis de la globalització. Les tensions geopolítiques constants, agreujades per la pandèmia global del coronavirus, han posat de manifest totes les mancances industrials dels països de la UE i han reactivat els esforços per convertir Europa en proveïdor i no només en client.

Malgrat que la sobirania tecnològica ha de ser un objectiu clar en la política europea, cal no oblidar que la ciència i el coneixement no entenen de fronteres, i que les polítiques de recerca han de ser capaces d'assolir un equilibri entre la protecció de la propietat intel·lectual i la col·laboració científica i industrial. Països com els Estats Units, el Canadà o la Xina posseeixen tecnologia més avançada que l'europea. Alhora, Europa és un gran generador de descobriments i de coneixement i, en conseqüència, també és en molts casos una gran exportadora de talent. Els ordinadors quàntics encara són immadurs i el seu veritable potencial encara està per descobrir. Per enfrontar-nos a un repte tecnològic tan gran, cal que tots i totes busquem la millor manera de col·laborar, sense oblidar tampoc tot

el talent que pot quedar amagat en altres països tradicionalment menys enfocats a aquest camp científic.

Tots els algorismes quàntics necessiten un component de computació clàssica. Els ordinadors quàntics no competiran contra els superordinadors, sinó que en formaran part

La computació quàntica no deixa de ser un exemple més dels fruits que es poden obtenir quan un grup obstinat de científics i científiques decideixen fer-se preguntes sobre com funcionen els engranatges de la natura i “què passaria si...?”, sense posar necessàriament el focus en futures aplicacions o invents (que trigarien anys a arribar), només pel plaer i la missió d’expandir les fronteres del coneixement, i decideixen treballar moltes vegades en les idees més absurdes que han sentit mai. Gràcies a ells i elles avui recollim els fruits de la ciència del passat, alhora que plantem les llavors de la ciència i la tecnologia del futur.

## NOTES

1 — La citació original és: “That is positively the dopest idea I ever heard.” Hillis, D. (1989) “Richard Feynman and the Connection Machine”. *Physics Today*, núm. 42(2), p. 78.

## REFERÈNCIES BIBLIOGRÀFIQUES

- Benioff, P. (1980) “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by turing machines”. *Journal of Statistical Physics*, núm. 22(5), p. 563-591.
- Binosi, D. Calarco, T. Colin de Verdière, G. Corni, S. Garcia-Saez, A. Johansson, M. P. Kannan, V. Katz, N. Kerenidis, I. Latorre, J. I. Lippert, Th. Mengoni, R. Michielsen, K. Nominé, J. P. Omar, Y. Öster, P. Ottaviani, D. Schulz, M. Tarruell, L. (2022). “EuroQCS: European Quantum Computing & Simulation Infrastructure”. Quantum Flagship. [Disponible en línia](#).
- Comissió Europea. “European Chips Act” (Llei europea de xips). [Disponible en línia](#).
- EuroHPC - Joint Undertaking (2022). “Selection of six sites to host the first European quantum computers”. Nota de premsa d’octubre del 2022 sobre l’Empresa Comú

d'Informàtica d'Alt Rendiment Europea. [Disponible en línia](#).

- Feynman, R. P. (1982). "Simulating physics with computers". *International Journal of Theoretical Physics*, núm. 21, p. 467-488.
- Manin, Y. (1980). *Computable and Uncomputable*. Moscou: Sovetskoye Radio, p. 128.
- Preskill, J. (2021). "Quantum computing 40 years later". *Feynman Lectures on Computation*. Segona edició, publicat per Taylor & Francis Group, editat per Anthony J. G. Hey.



#### **Alba Cervera Lierta**

Alba Cervera Lierta és investigadora del Barcelona Supercomputing Center - Centre Nacional de Supercomputació (BSC-CNS). És doctora en computació i informació quàntica per la Universitat de Barcelona i té un màster en Física de Partícules. Després del seu doctorat, es va traslladar a la Universitat de Toronto com a investigadora postdoctoral al grup Alán Aspuru-Guizik. Els seus àmbits d'estudi tracten de la computació quàntica i les seves aplicacions a curt termini, així com de les sinergies entre la física quàntica i la intel·ligència artificial. Des de l'octubre del 2021, és coordinadora del projecte Quantum Spain, una iniciativa d'impuls de l'ecosistema de computació quàntica que té per objectiu operar un ordinador quàntic al BSC-CNS.