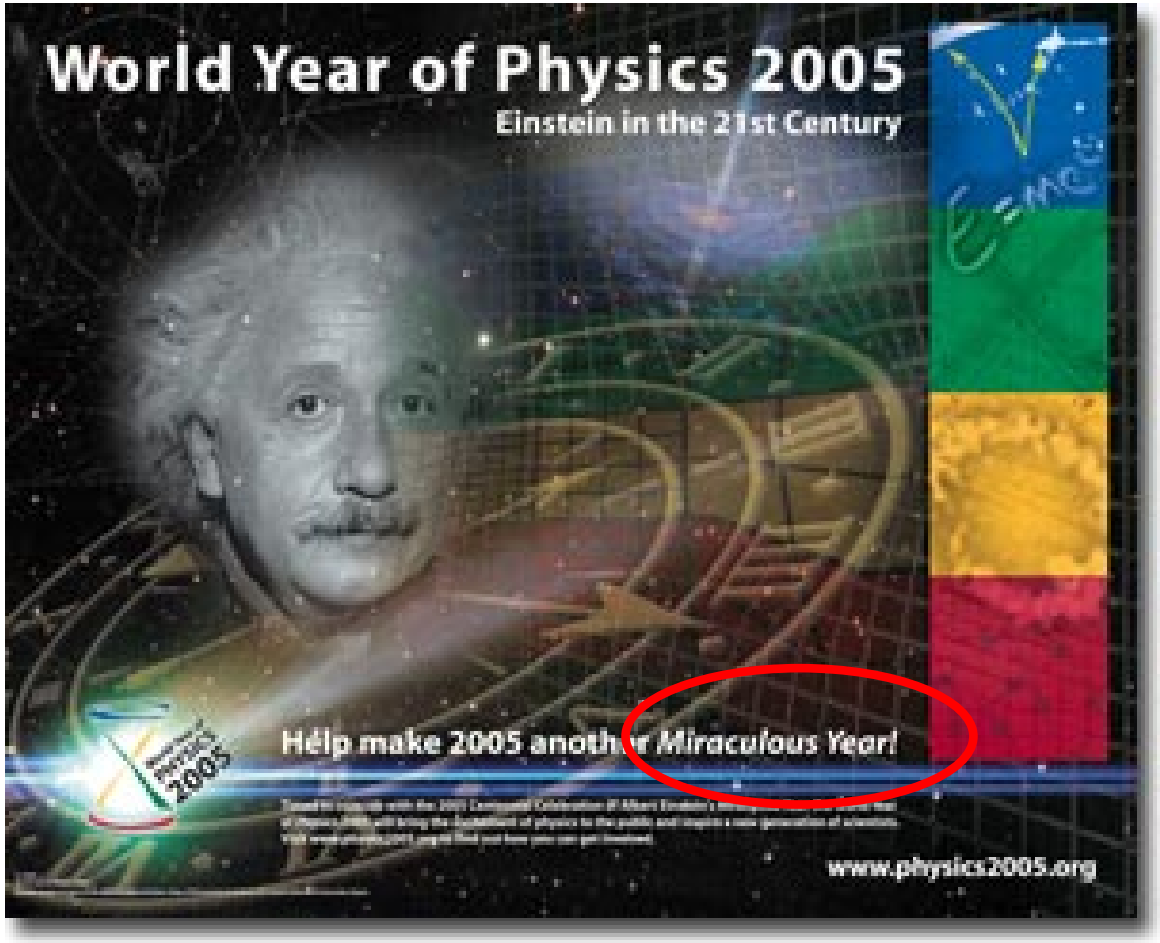
COMPUTACIÓ i CRIPTOGRAFIA QUÀNTICA

Rossend Rey

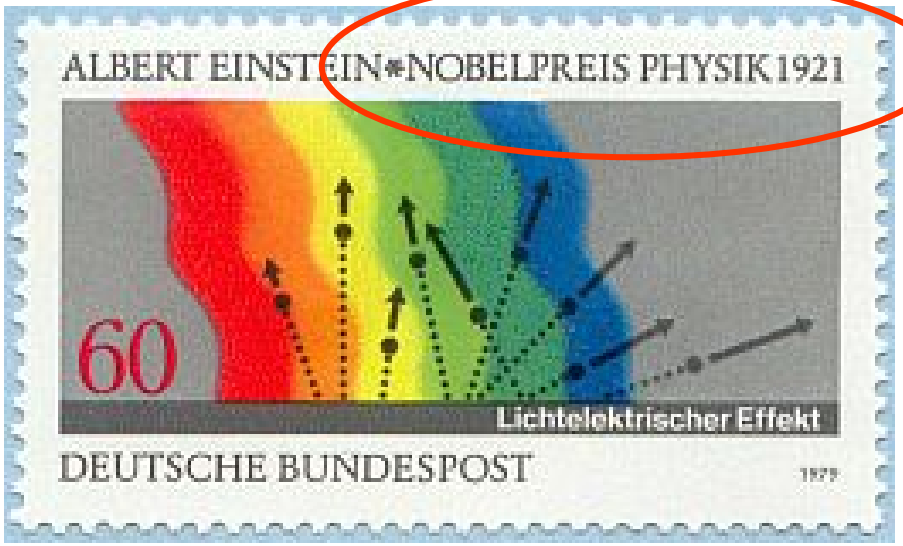
Departament de Física

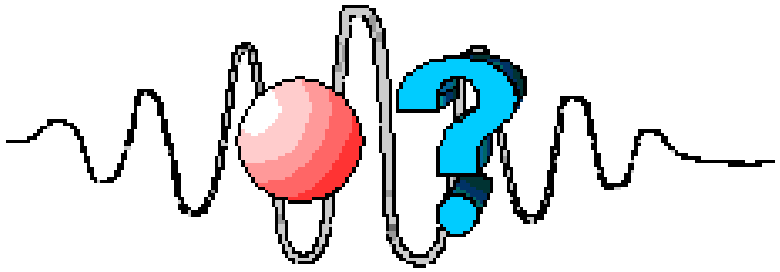
rosendo.rey@upc.edu B5-205

Un lloc on començar:
2005 Any Mundial de la Física



Un origen de la Física Quàntica: EFECTE FOLTOELÈCTRIC





La radiació està constituïda per “QUANTUMS” d’energia

FOTÓ

primera partícula predita teòricament

Com va ser rebuda aquesta teoria?

"…que en algunes ocasions les seves especulacions hagin errat el tret com, per exemple, la seva hipòtesi dels quantums de llum, no s'hauria d'utilitzar en contra seva…"

Recomanació per entrar a L'Acadèmia de Prússia, 1913

però…

"A l'Albert Einstein pels seus seveis a la Física Teòrica i especialment per la seva descoberta de la llei de l'efecte fotoelèctric"

Premi Nobel, 1922

Quin era el problema?

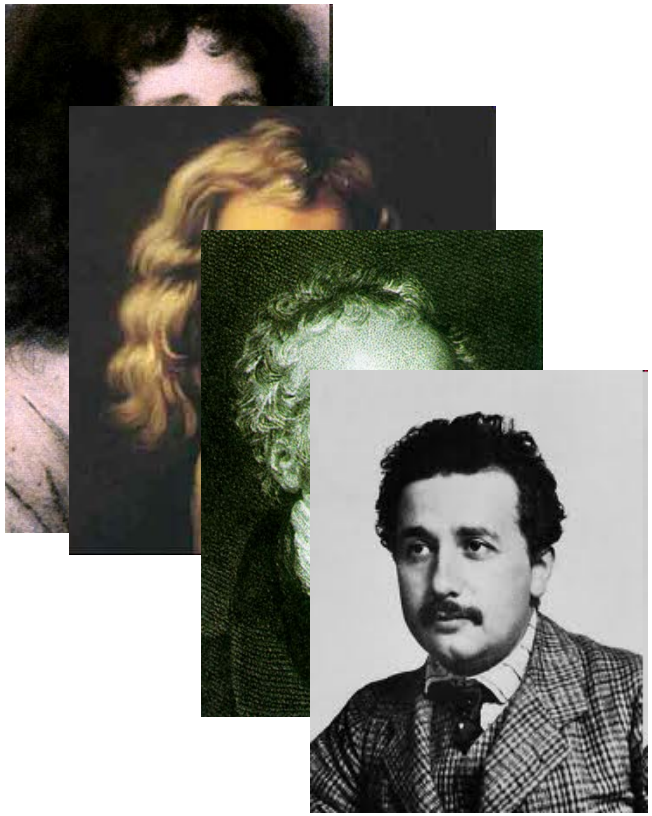
"…semblava violar tot el que sabíem sobre la interferència de la llum"

R.A. Millikan, 1948

Premi Nobel, 1923 (en part per intentar demostrar experimentalment que la teoria d'Einstein era incorrecta)

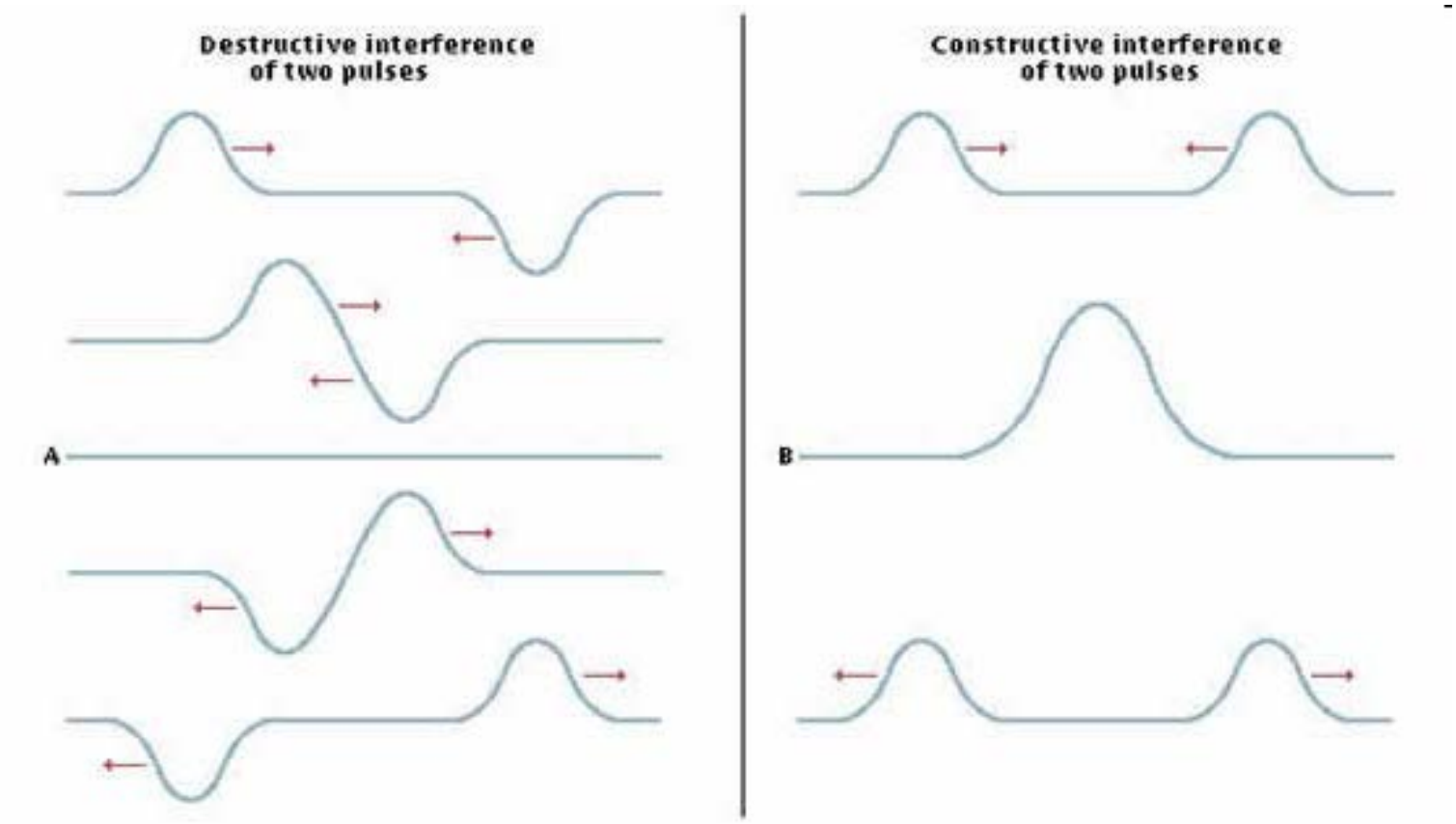
El culebrot de la llum: Huyguens vs. Newton vs. Young vs. Einstein vs. ?

- El 1680 en Huyguens va proposar que la llum és una ona.
- Al mateix temps Newton deia que està constituïda per petites partícules.
- Cap al 1803 en Young va demostrar que dóna lloc a **interferències**, tal i com és típic de les ones.
- El 1905 l'Einstein diu que d'acord, però que en alguns experiments es comporta com una partícula.

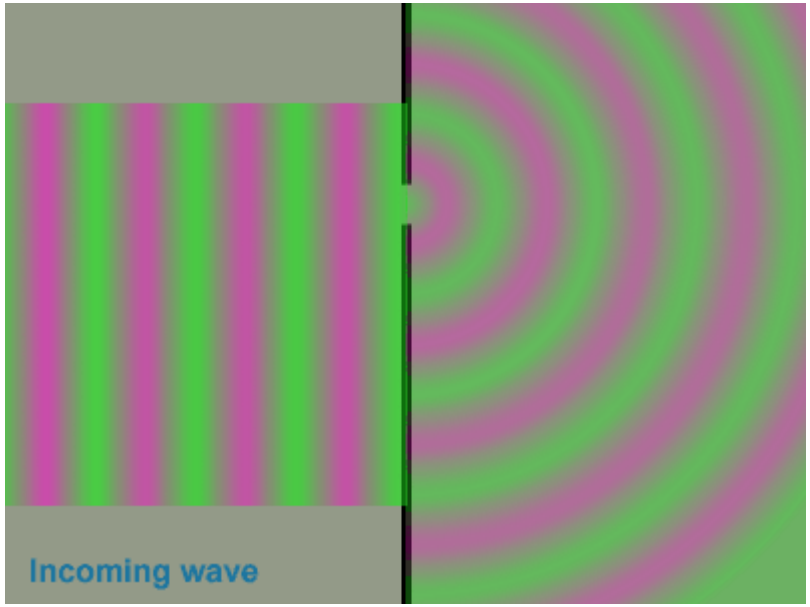


Furguem en aquest misteri…és el nucli de la Quàntica

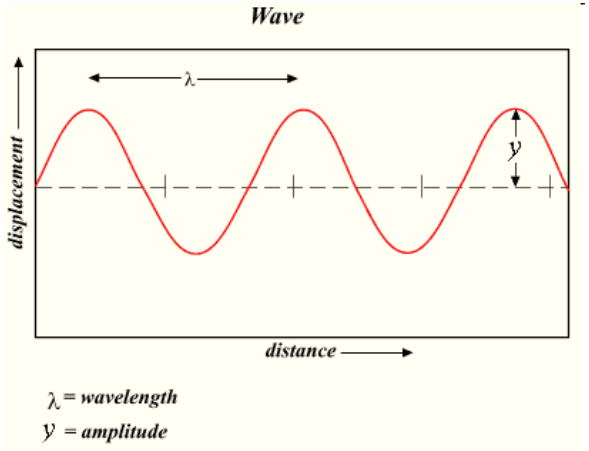
Interferències, el tret característic: ones en una corda



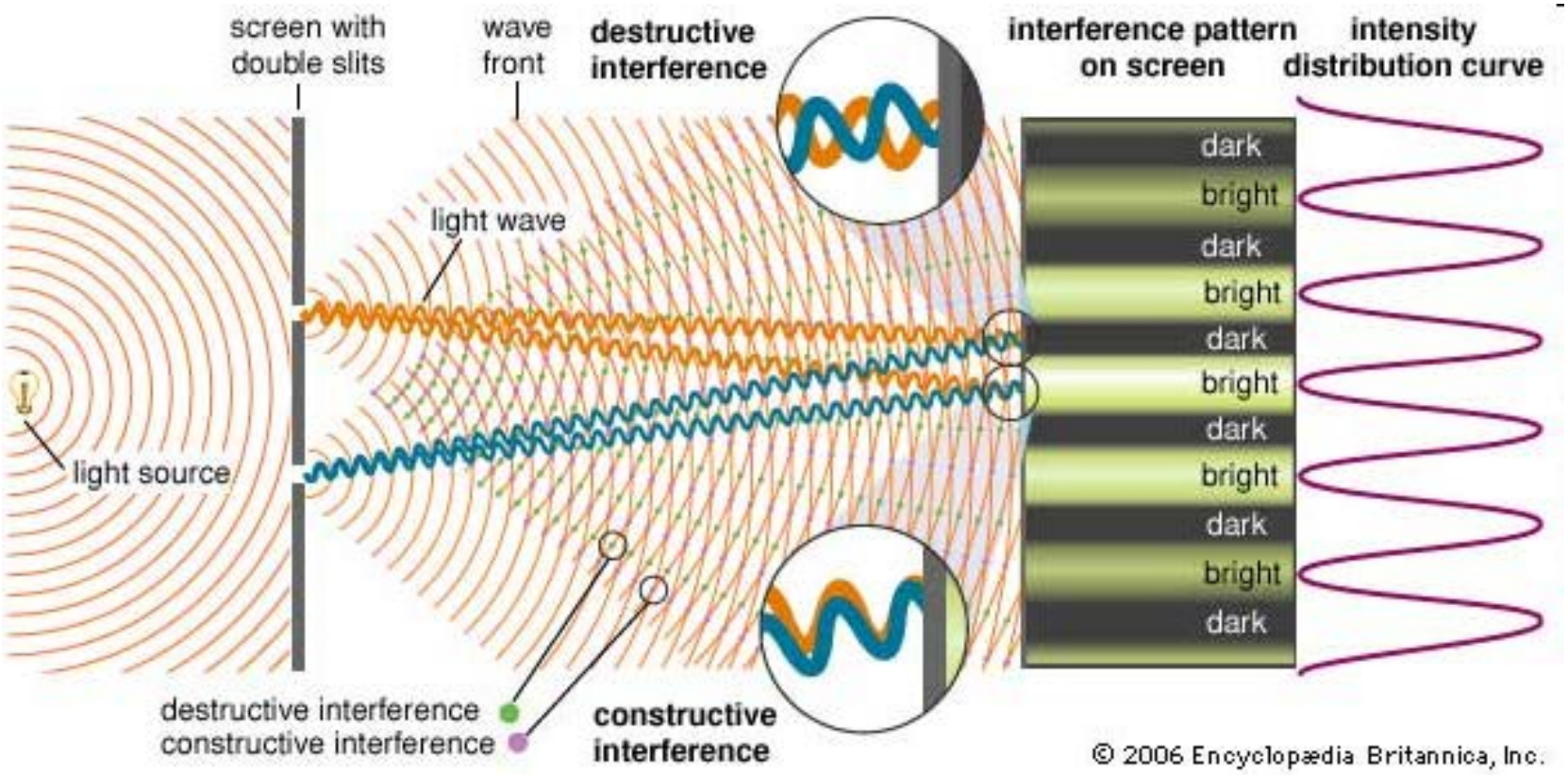
A més, no sempre van en línia recta!



Si la longitud d'ona és comparable a les dimensions del forat

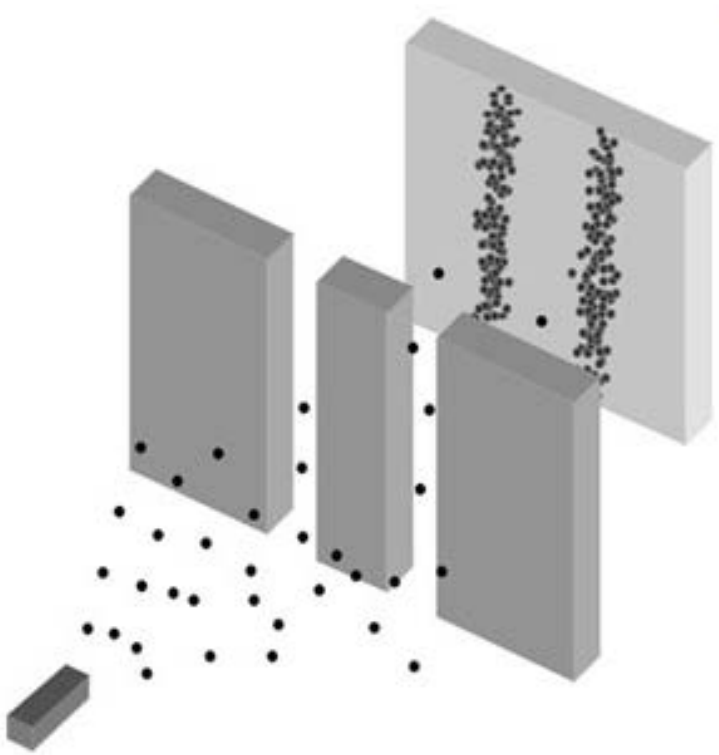


Experiment de Young



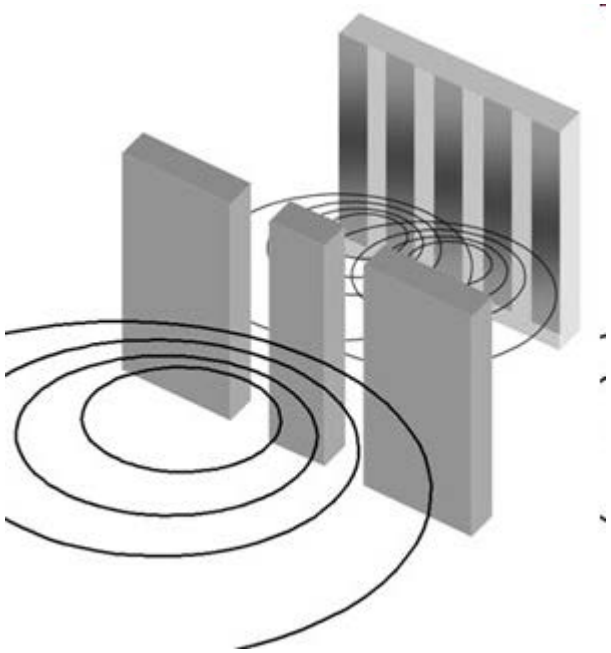
Escollit com el 5e experiment més bonic de la història de la Física

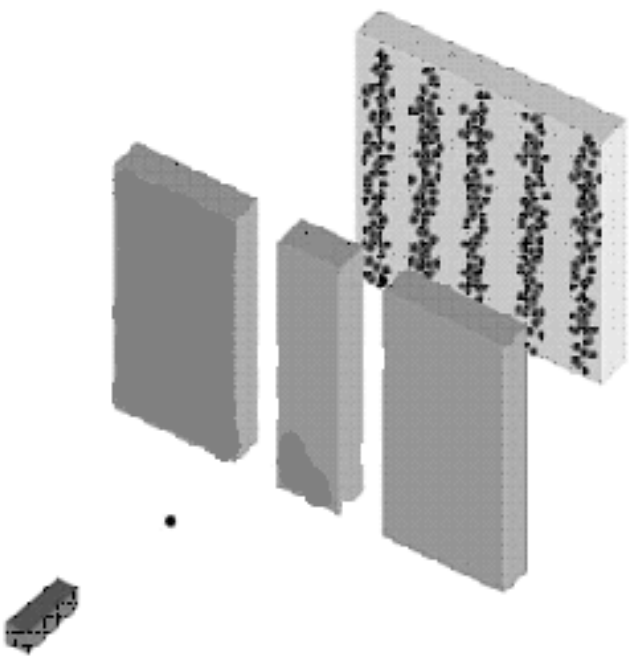
On és el problema amb els fotons de l'Einstein? Si són partícules …



Només haurien de sortir dues franges!
Per suposat cap franja central!

Doble personalitat: la sorpresa de la "dualitat ona-partícula"





Si és una ona: ok amb les franges …

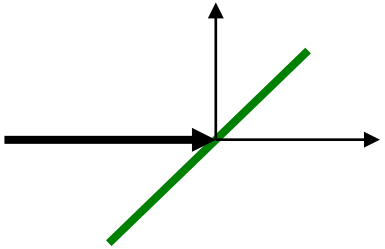
… però quan mirem sempre veiem que passa per una excletxa!...

Si és una partícula…ok amb la detecció…

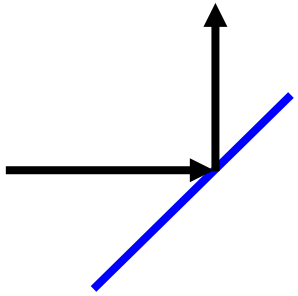
… però les franges són típiques de quelcom que passa per les dues excletxes!

Per si no ens estranya: un altre experiment d'Interferometria

FOTONS

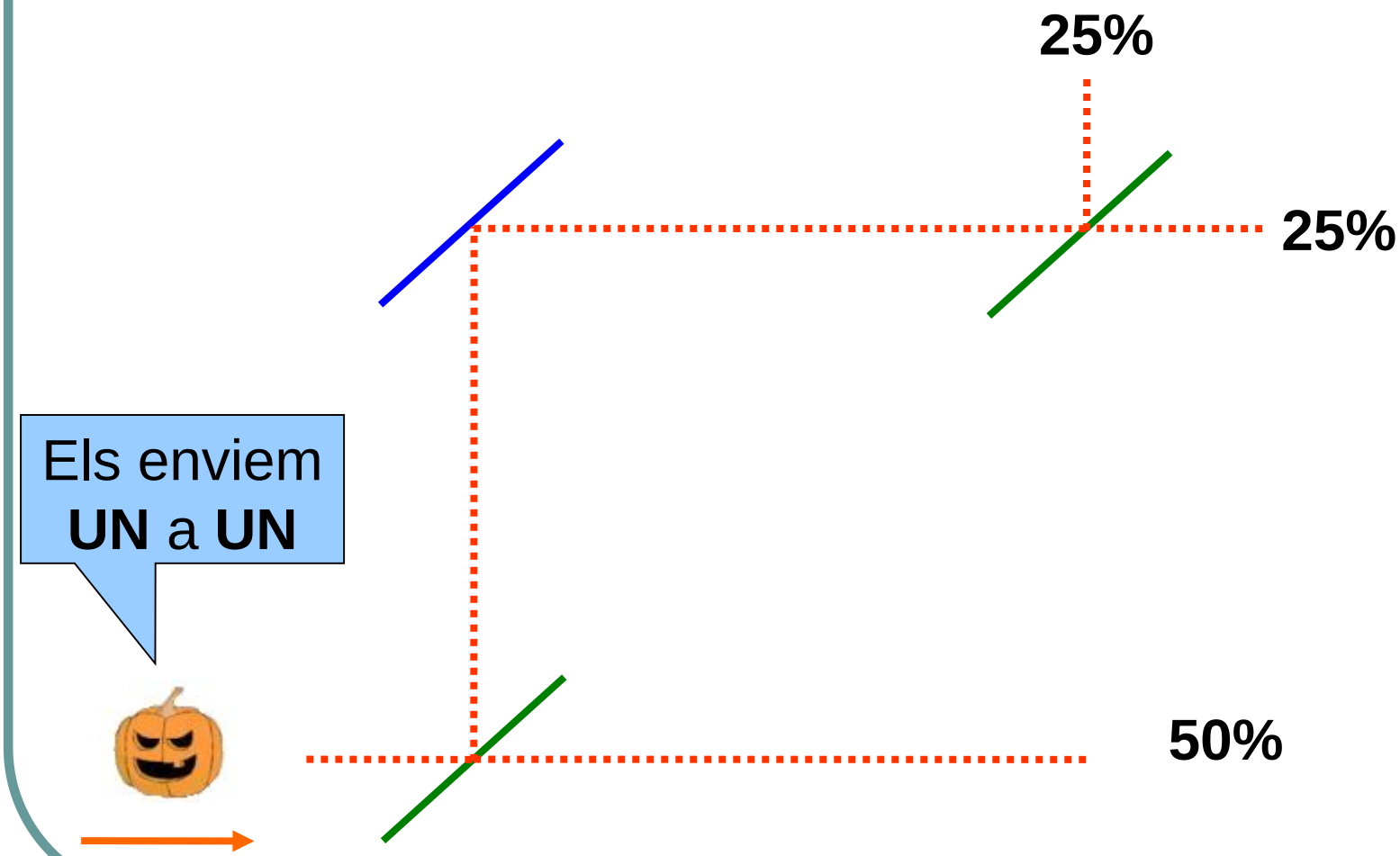


VIDRES SEMITRANSPARENTS

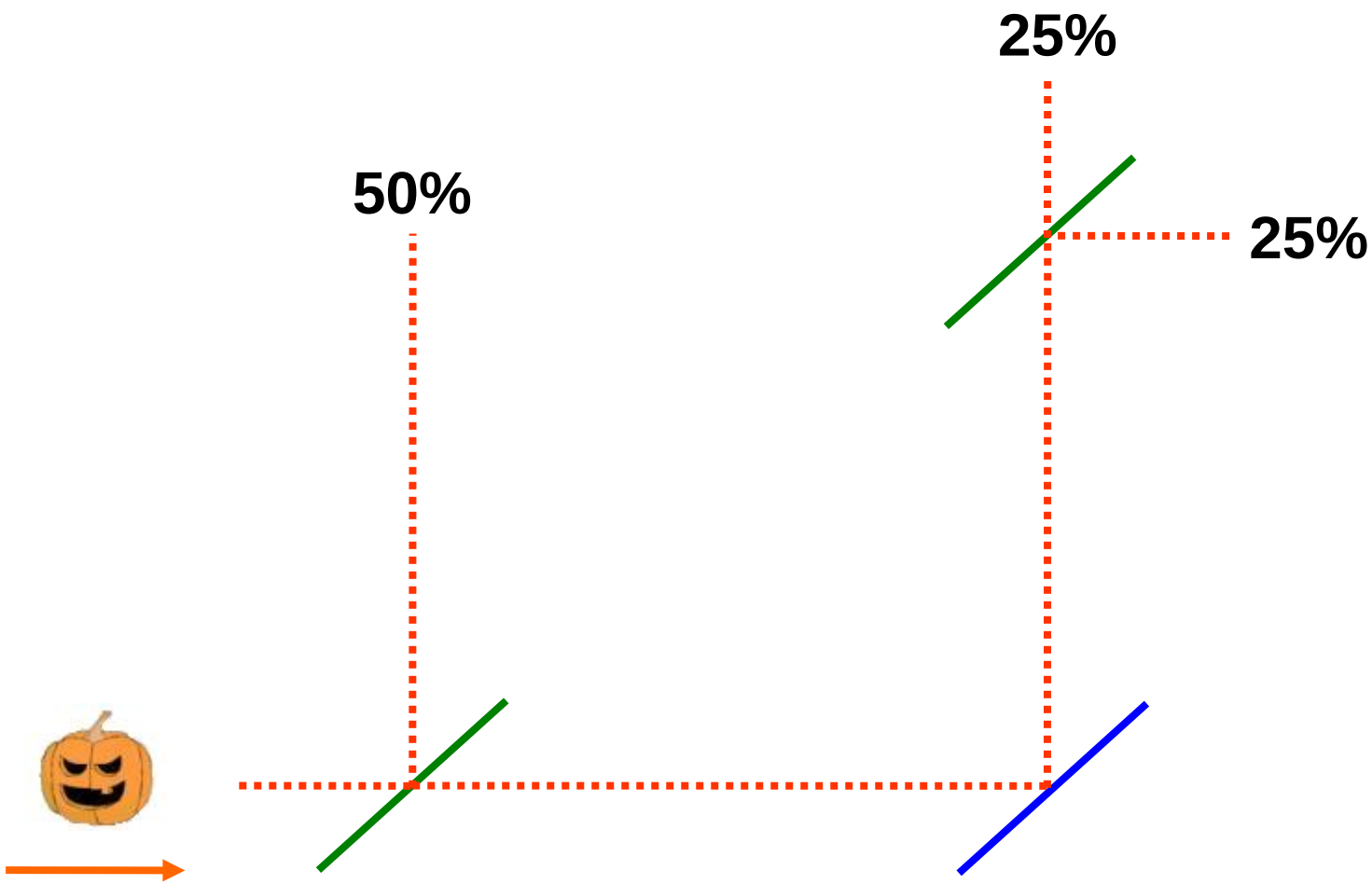


MIRALLS

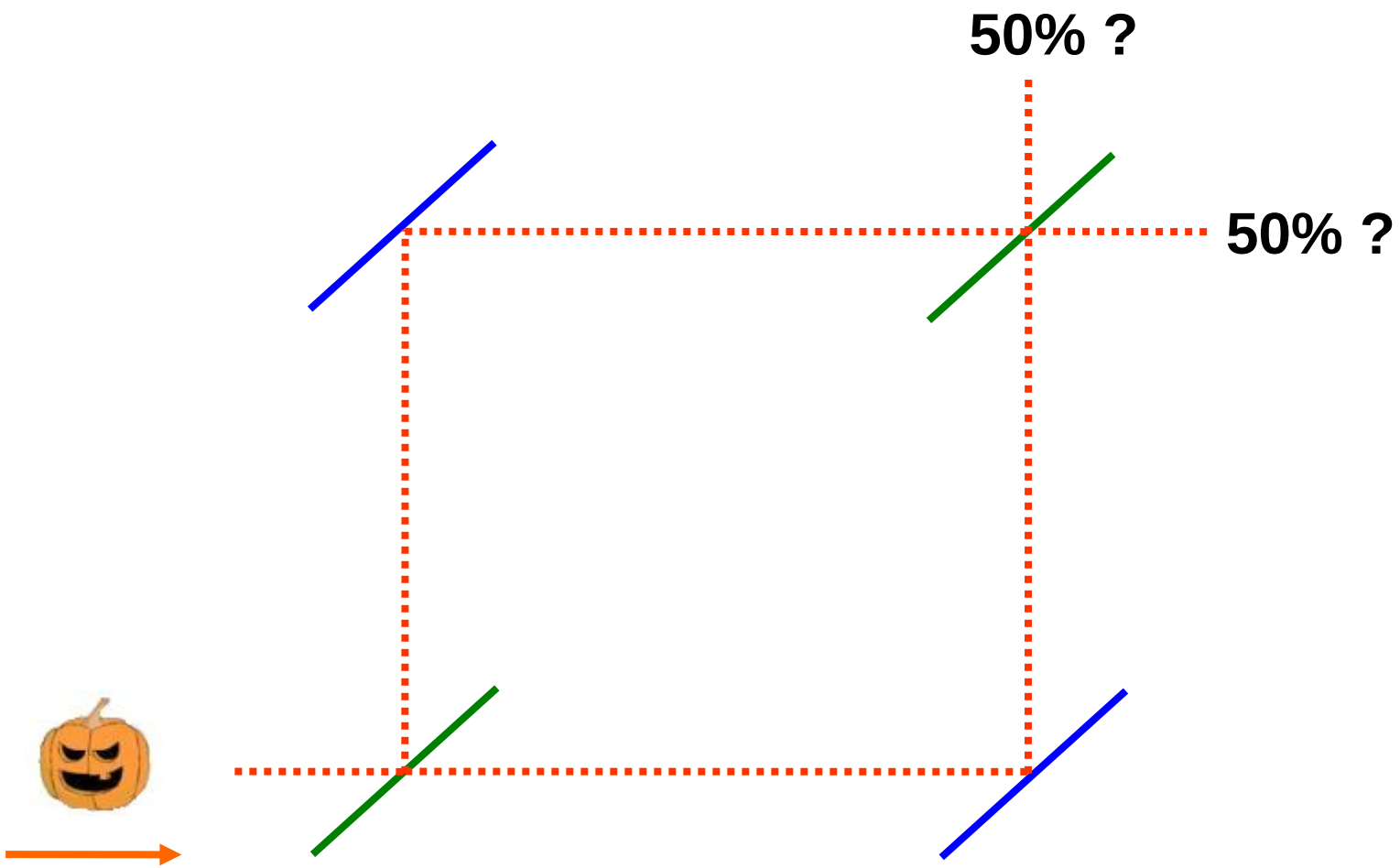
Semblen molt avorrits …



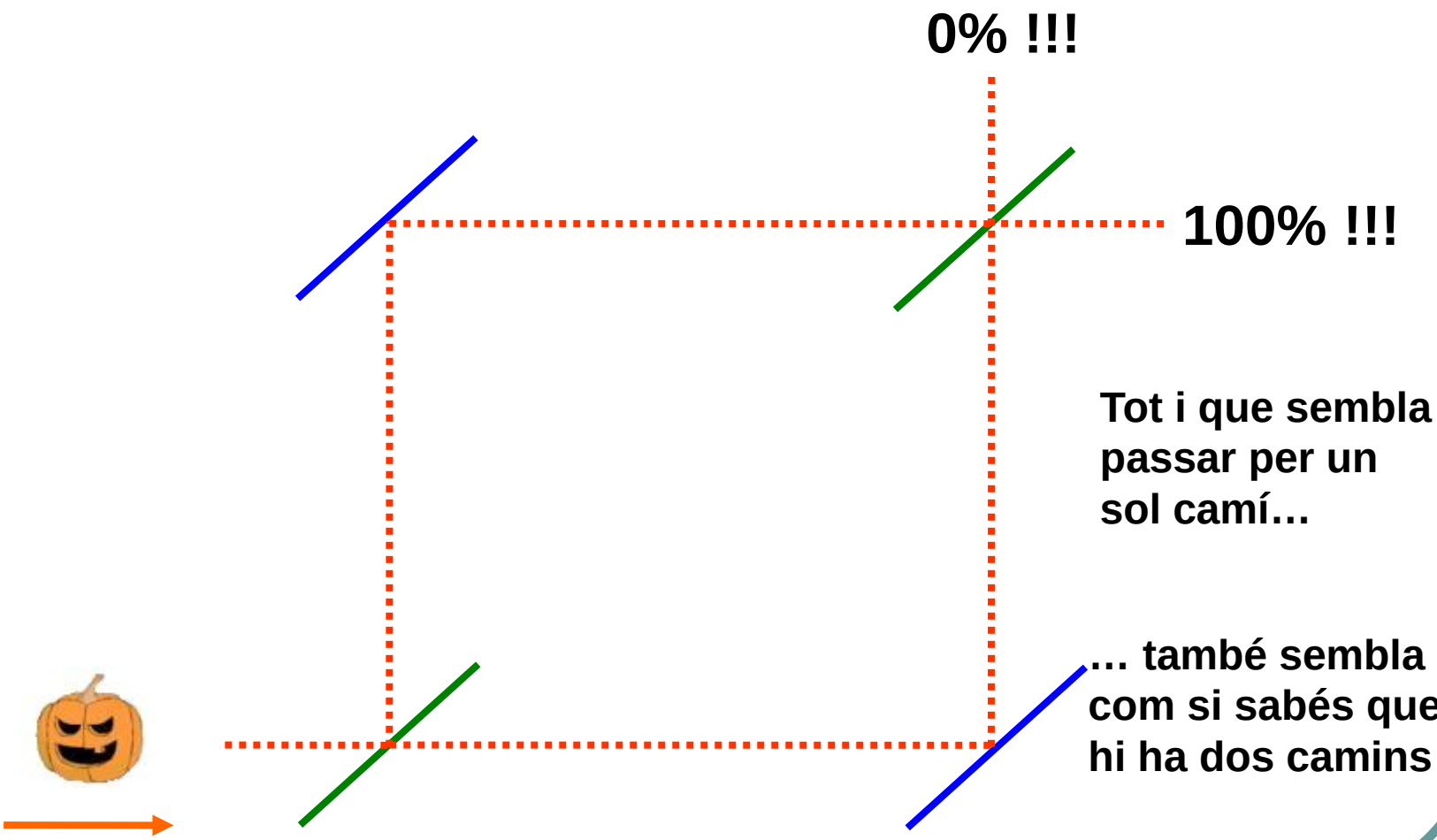
Res de nou …



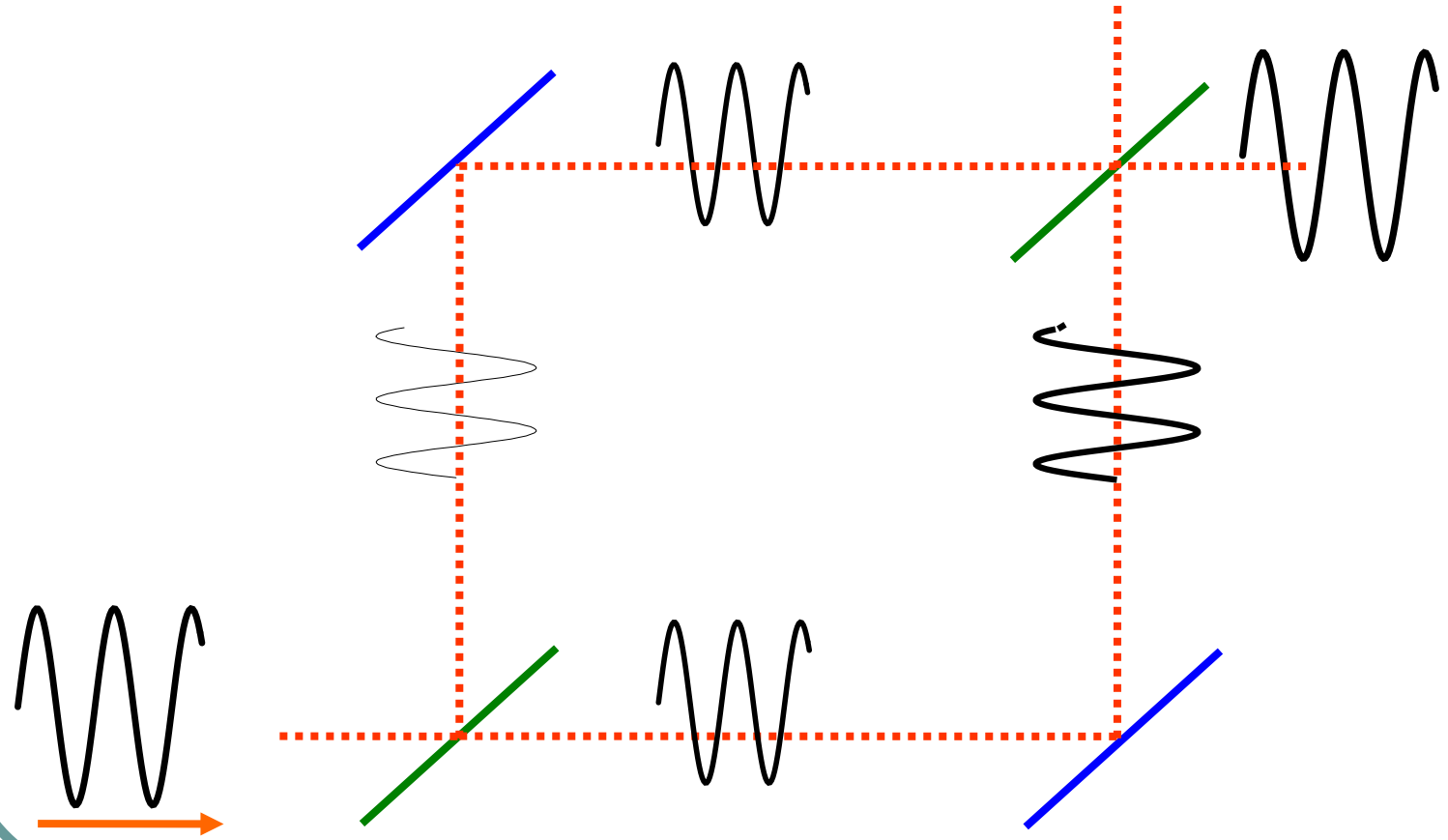
Interferòmetre Mach-Zehnder



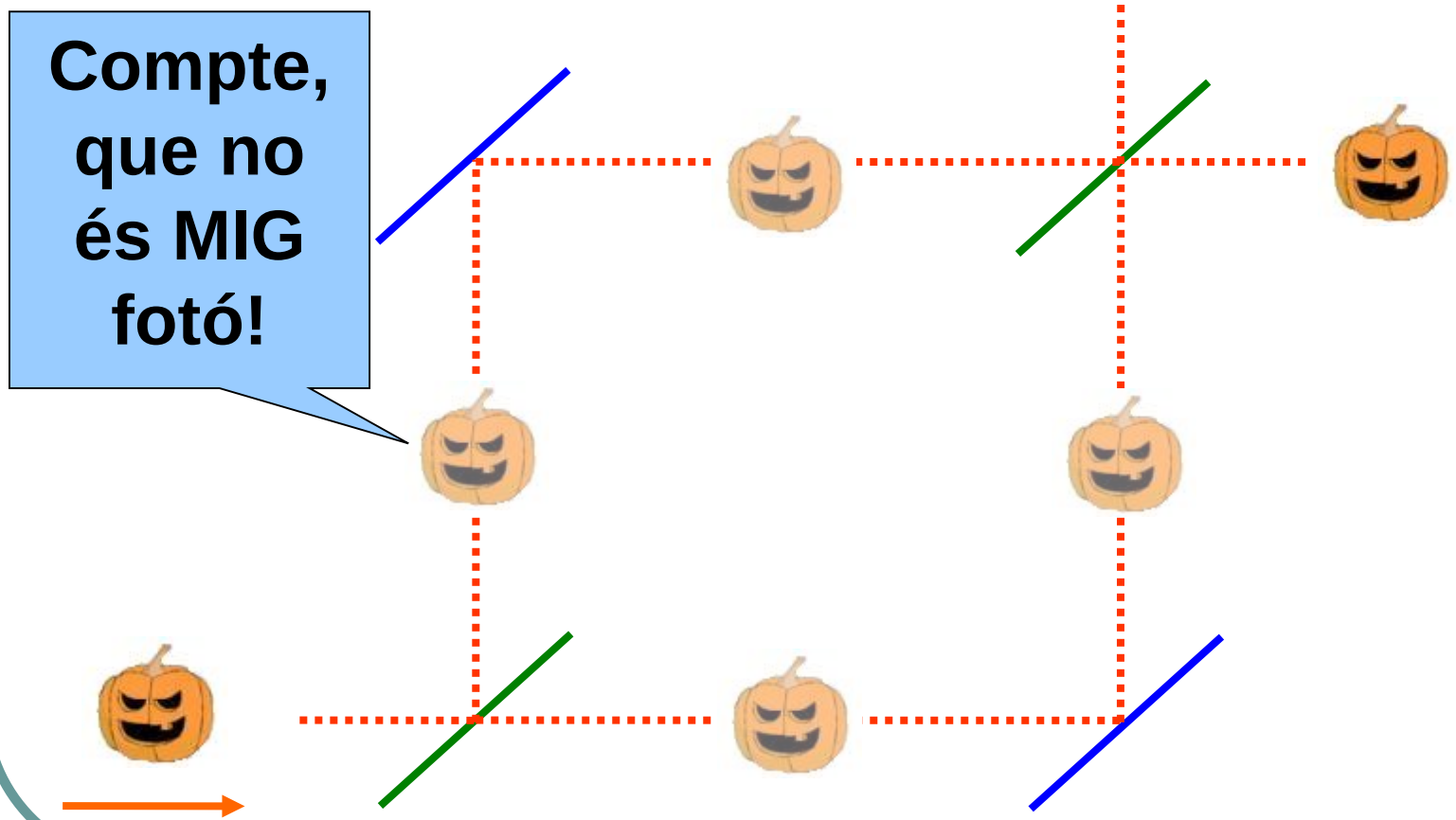
Sorpresa!


0% !!!
100% !!!
Tot i que sembla passar per un sol camí…
… també sembla com si sabés que hi ha dos camins

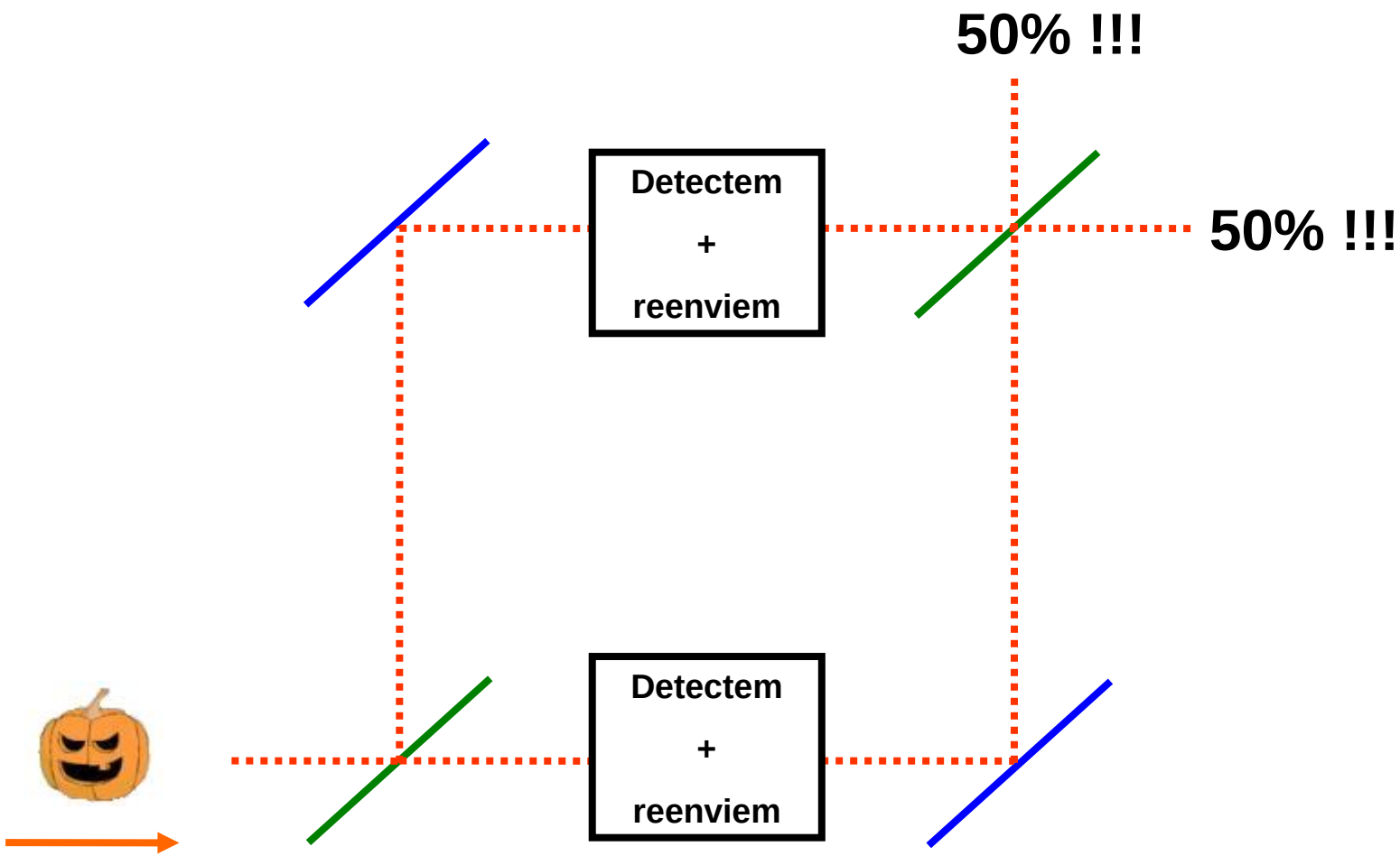
Tot “funciona” si pensem en ones



Costa MOLT d'imaginar…



I si els espiem?



“Doble personalitat”

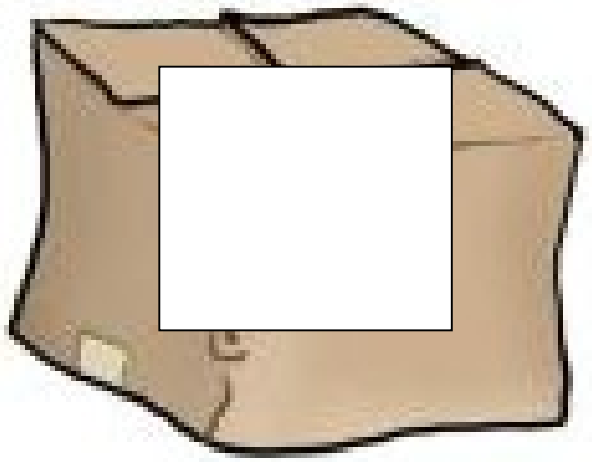
- Quan mirem on és, es comporta com una PARTíCULA !
- Quan no estem mirant, es comporta com una ONA !

El passat és fet de partícules…

el futur d’ones!

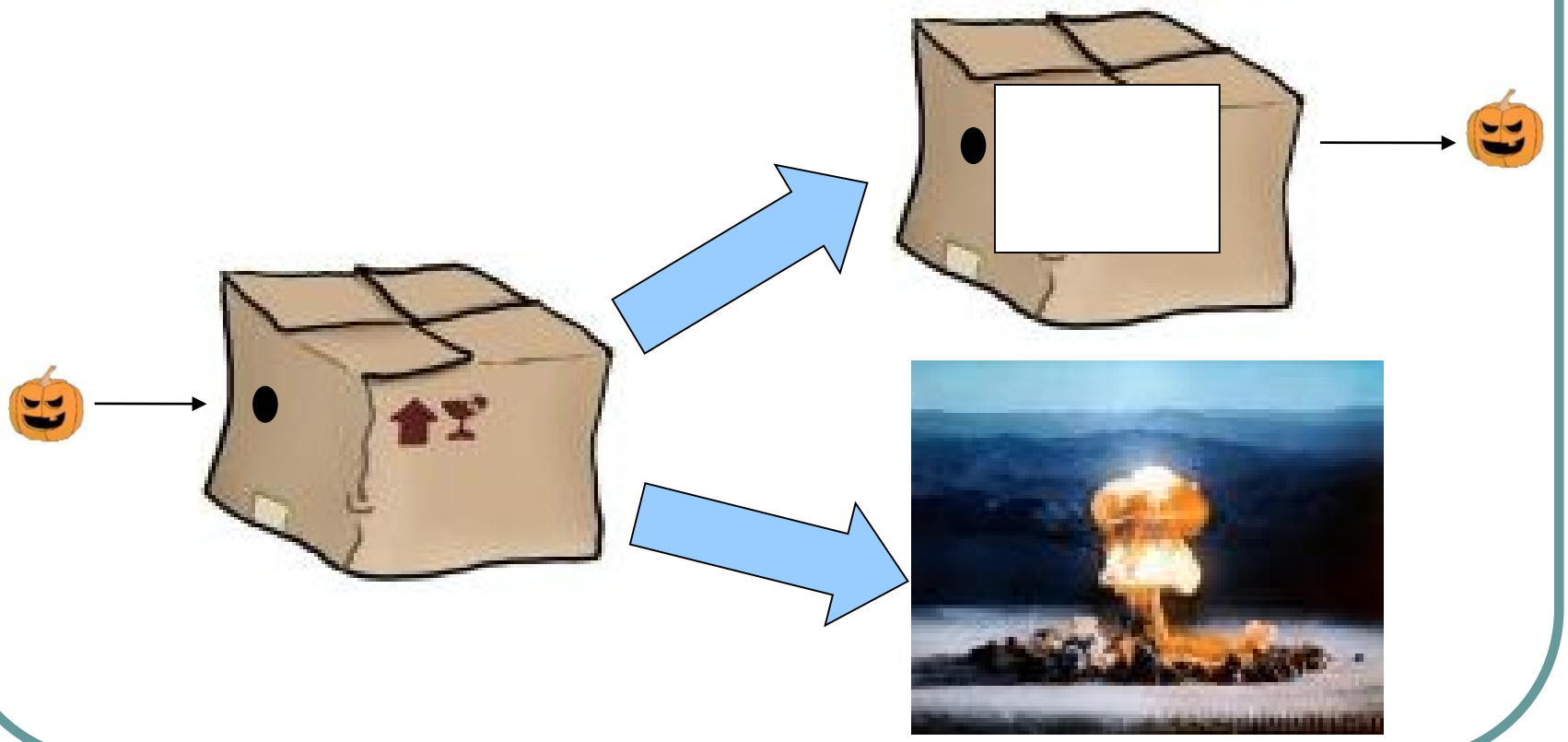
Per si encara no us sembla prou estrany: veure-hi sense mirar

Una caixa pot contenir una bomba …

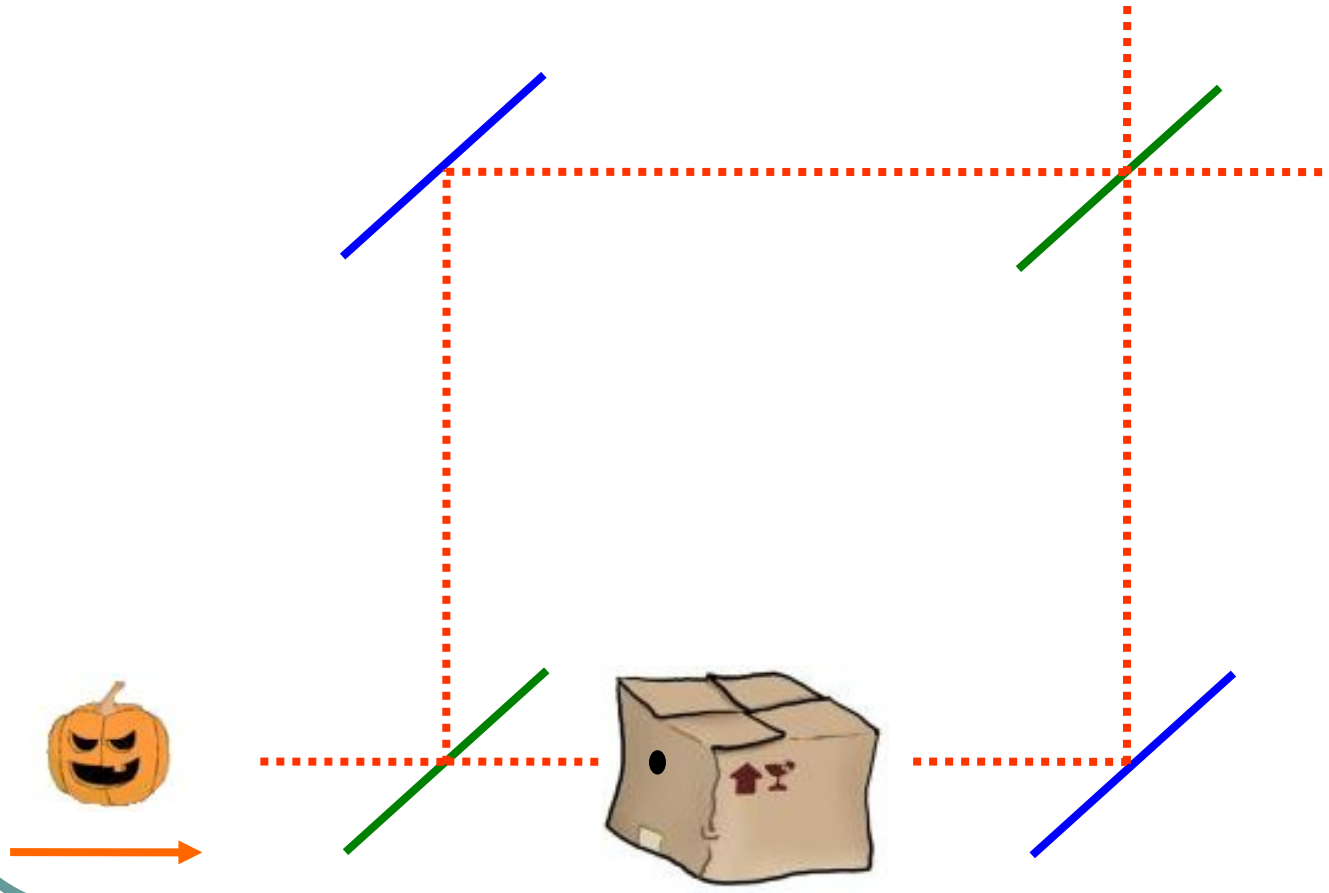


…ultrasensible

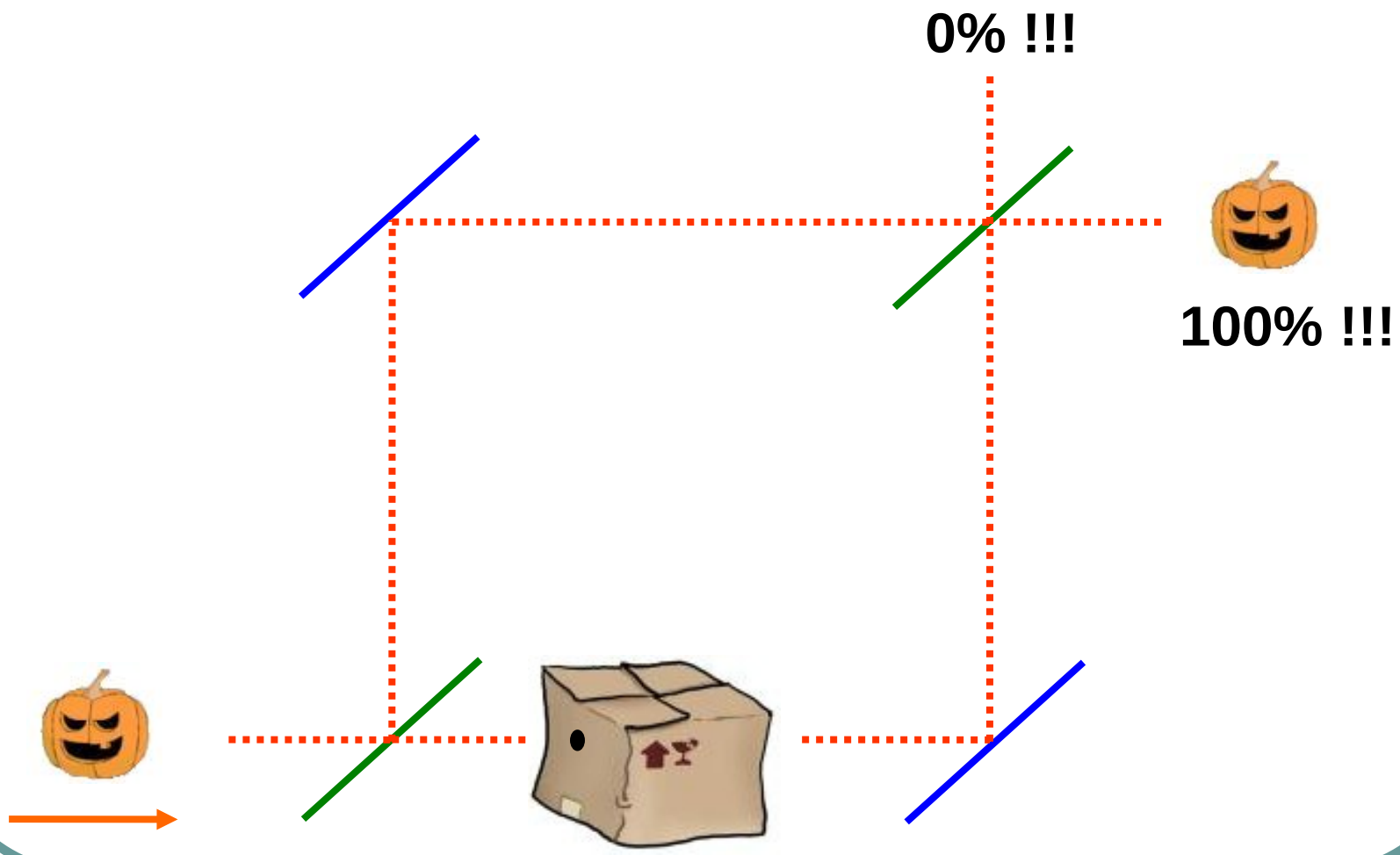
Un sol fotó pot fer-la explotar



Posem la caixa en un Mach-Zender

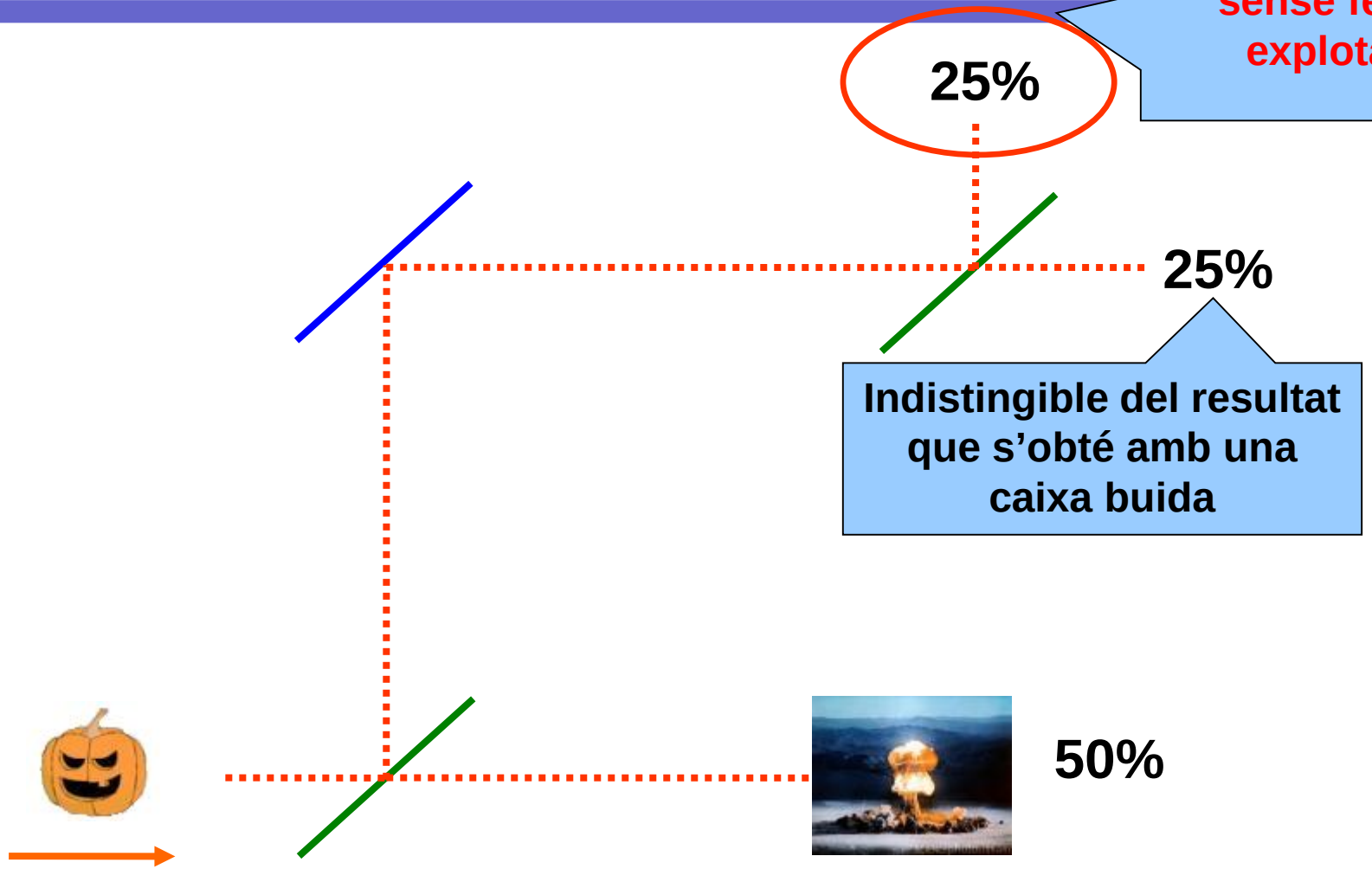


Si la caixa és buida...



Si sempre hi ha bomba...

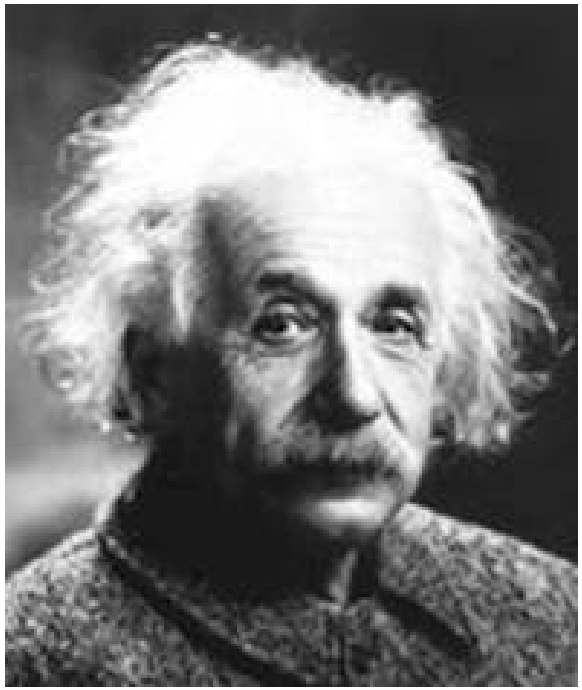
Aquests fotons ens diuen que hi ha una bomba sense fer-la explotar!



Màgia!

- Podem detectar ¼ de les bombes sense fer-les explotar i, per tant, sense que cap fotó hagi entrat per “comprovar” si hi ha una bomba o no
- Es pot refinar fins que la probabilitat pugi des de ¼ fins a un nombre tant proper a 1 com es vulgui

Realment tot és molt estrany



"Aquests cinquanta anys de cavilacions no m'han portat més prop de respondre la pregunta: què és el quantum de llum?"

A. Einstein, 1951

I no és l´únic…

R. Feynman, Premi Nobel, 1965

*"…**crec que puc dir amb tota tranquilitat que ningú enten la Física Quàntica**…*

…no vagin preguntant-se ¿però com pot ser?, perquè s'endinsaran en un carreró del que ningú ha pogut sortir-ne encara…"

Compte, és considerat el fundador! Ja hem passat del 40è anniversari

En un article del **1981** va suggerir la **possibilitat d'ordinadors quàntics més potents que els "clàssics**":

"…la descripció quàntica completa d'un sistema gran … no es pot simular amb un ordinador normal … però pot ser simulada amb elements d'un ordinador quàntic…"

Fer de la necessitat virtut

- Feynman (1982): per què no utilitzar un sistema quàntic que puguem controlar per simular-ne un altre?

- David Deutsch (1985): és possible que un ordinador quàntic resolgui problemes computacionals que no tenen solució eficient en un ordinador clàssic?

Començament modest però sorprenent: Algorisme de Deutsch

- Donada una moneda, podem determinar amb **una sola tirada** si és bona o està falsificada?

Bona: cara i creu
Falsa: dues cares o dues creus

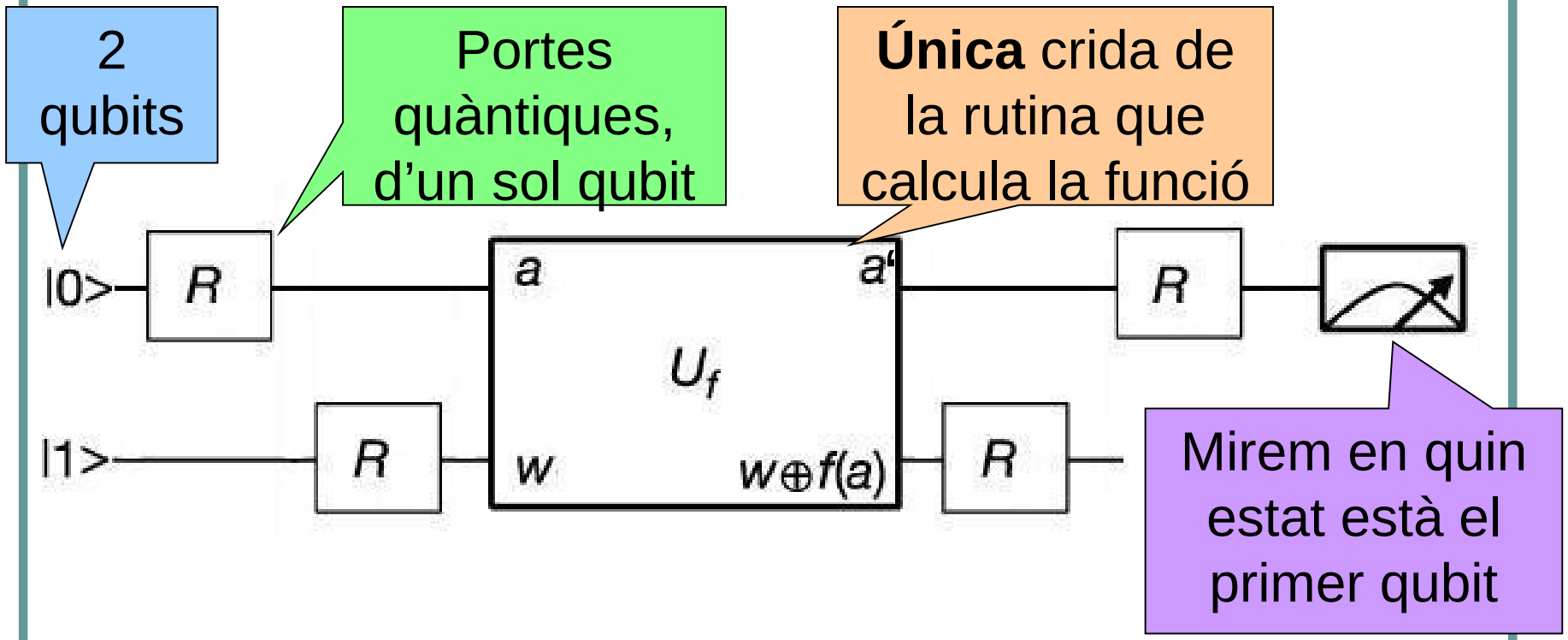
En llenguatge més matemàtic

- Donada una funció binària, podem saber amb **una sola consulta** si és constant?

f(0) = 0	f(1) = 0
f(0) = 1	f(1) = 1
f(0) = 0	f(1) = 1
f(0) = 1	f(1) = 0

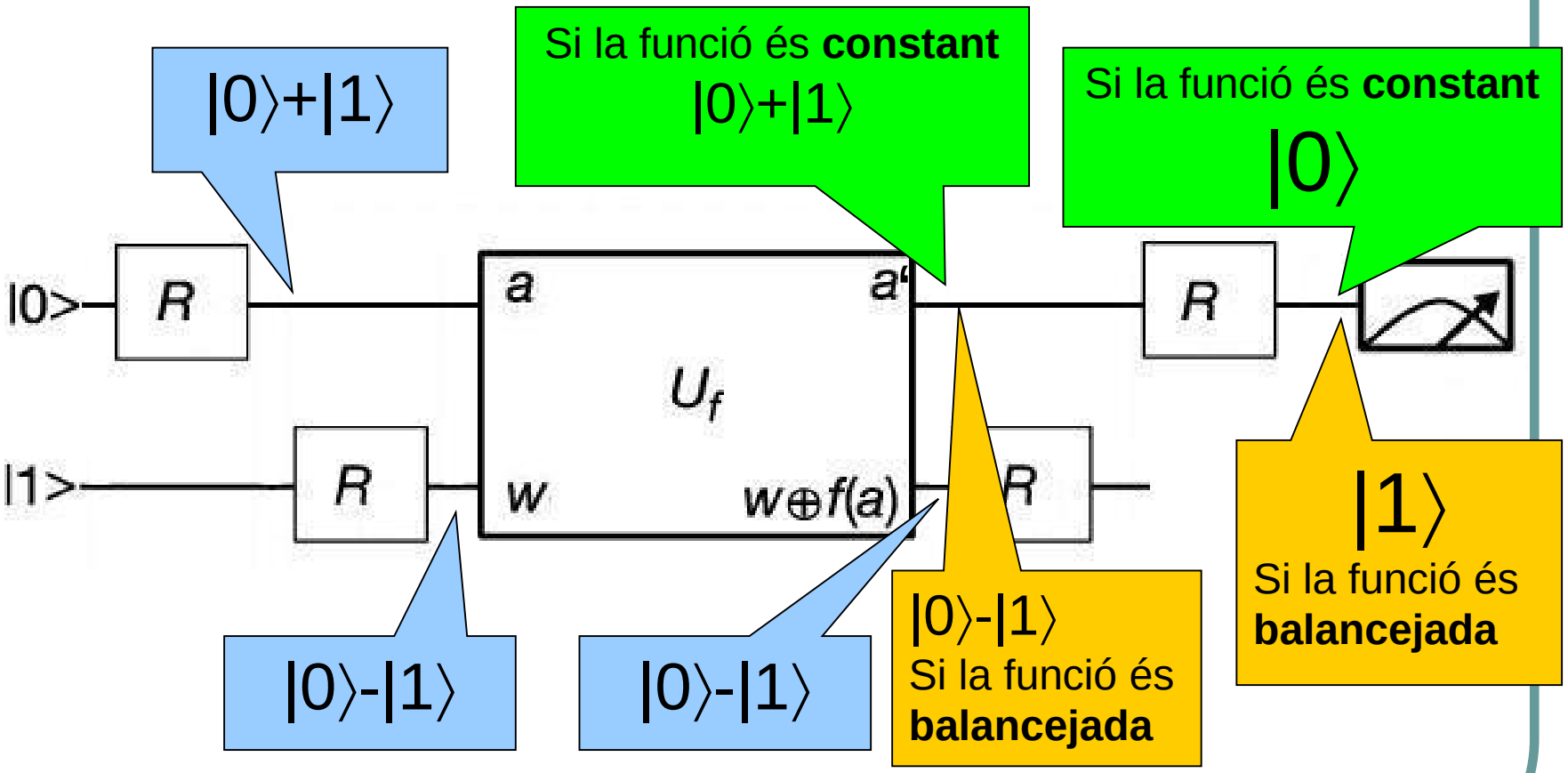
La lògica habitual ens diu que primer haurem de cridar la rutina pel valor 0, després pel valor 1, i comparar el resultat $\Rightarrow$ **2** crides

Aquest “ordinador quàntic” ho fa amb una sola crida!

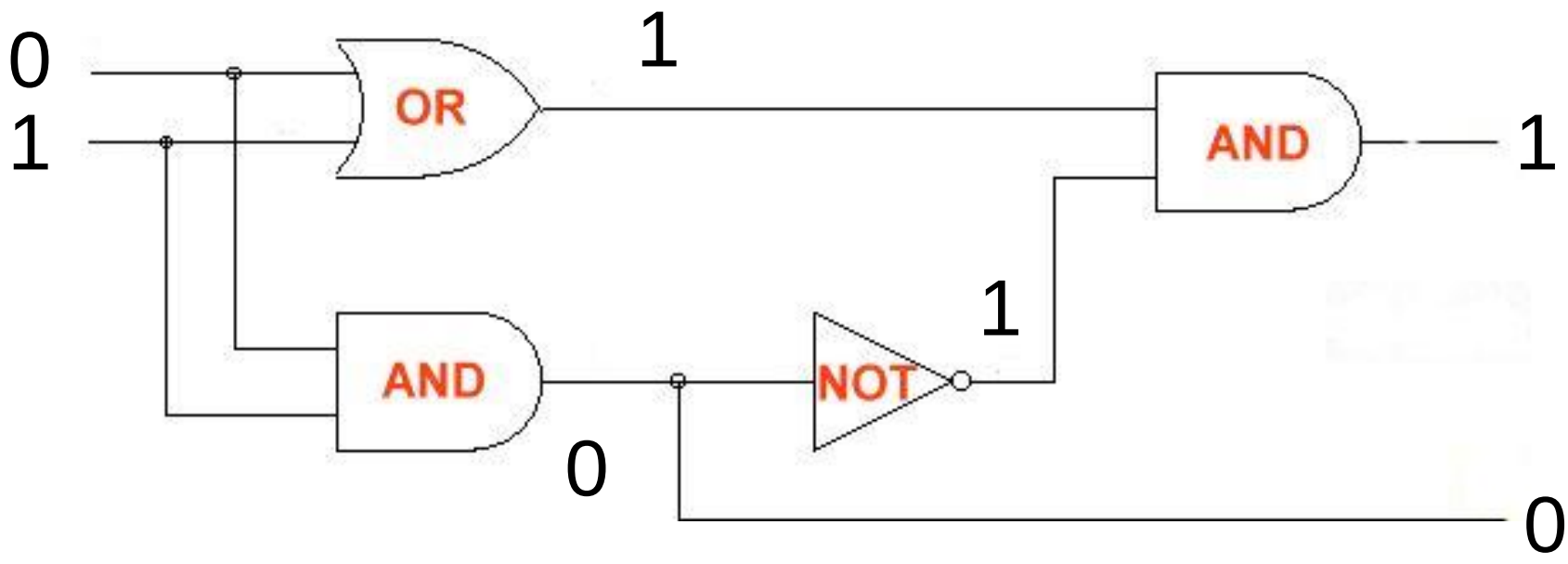


- ✓Implementat físicament l’any 1998 per primer cop
- ✓ Des de llavors s’ha aconseguit utilitzant diferents “tecnologies” (spins, ions atrapats, …)

El dimoni s'amaga en els detalls

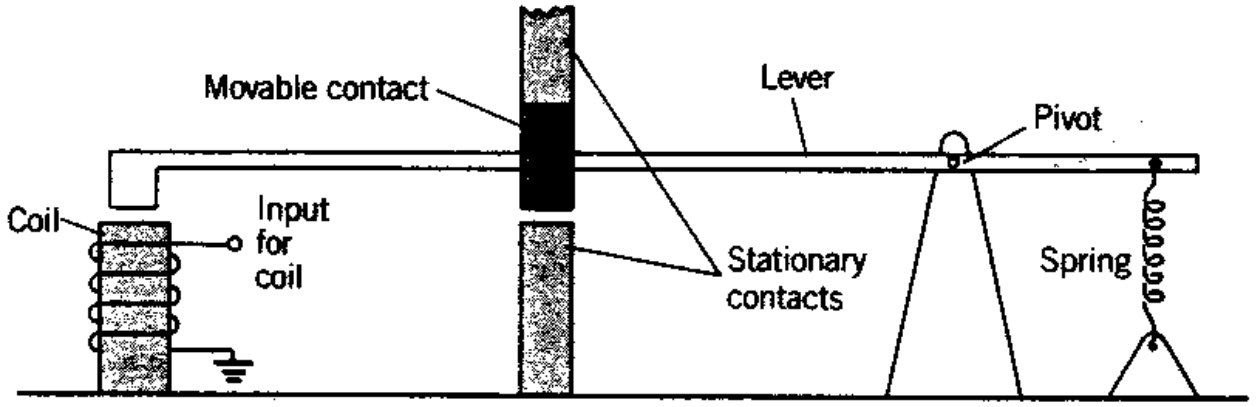


Comparem amb un circuit “clàssic”



Fins ara la Física només millorava l'eficiència d'aquest esquema

- En els ordinadors actuals sols ha canviat la implementació física de les portes
- Els 'relés' podíen fer exactament el mateix que els chips



Aquest canvi és profund

“ La Teoria de la Computació tradicionalment s’ha estudiat…com un tema de Matemàtiques...

…això és un error. Els ordinadors són objectes físics i les computacions processos físics…

…el que els ordinadors poden o no poden fer està sols determinat per les lleis de la Física, i no per les de les Matemàtiques”.

D. Deutsch

Tornem al fil històric de la computació quàntica

- 1981 proposta d'en Feynmann
- 1985 Deutch formalitza el concepte d'ordinador quàntic+algorisme
- 1993 Vazirani-Bernstein proposen un problema amb avantatge superpolinòmic
- 1994 Simon proposa un problema amb avantatge exponencial
- 1994 Shor proposa un algorisme per factoritzar, amb avantatge gairebé exponencial

1994: any miraculós de la CQ?

- En Peter Shor va descobrir:

✓ Un algorisme quàntic per trencar RSA fàcilment

✓ Una manera de corregir errors en els qubits.

PREMI NEVANLINNA 1998

~ Premi Nobel de la Informàtica

Q-day: el dia en que els ordinadors quàntics “trencaran internet”:

NEWS FEATURE | 08 February 2022

The race to save the Internet from quantum hackers

“Let’s say that a quantum computer is deployed in 2024,” says Rescorla. “Everything you’ve done on the Internet before 2024 will be open for discussion.”

Ara mateix s’estan decidint els criptosistemes **post-quantum** que substitueixin els actuals

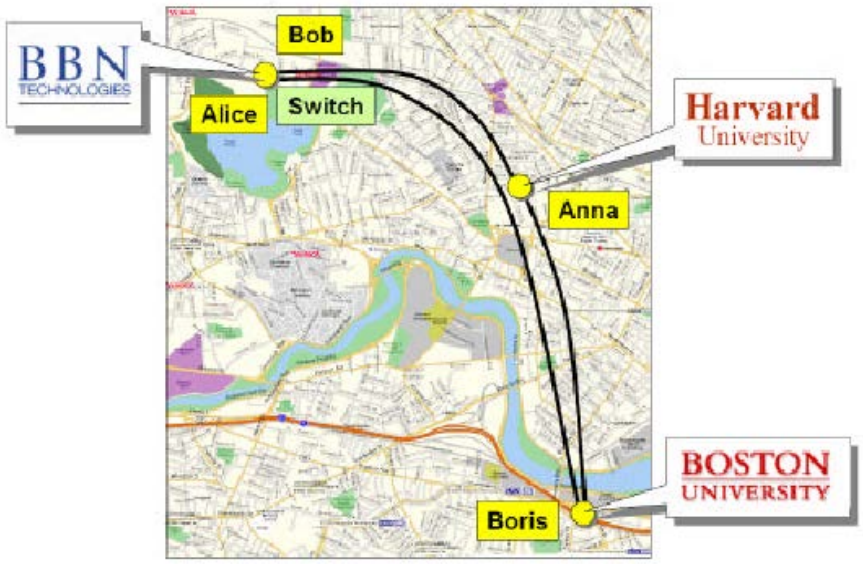
Wikipedia: NIST Post-Quantum Cryptography Standardization

La bena abans de la ferida

- La Física Quàntica proporciona la base per Criptografia totalment segura.

- Títol de l'article amb la primera implementació (Bennet et al., 1989): *"The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!*"

Ja fa temps de la primera xarxa!



- DARPA Quantum Network
- Operacional al Juny del 2004
- Link per aire al Juny del 2005

BBN Technologies va ser la companyia que va montar el precursor de l'actual INTERNET a l'any 1969 (ARPANET)

On som ara en Criptografia?

Basat en *“Quantum Computing 40 Years Later”, John Preskill (2021)*

- S’estan desenvolupant nous codis de criptografía clàssica (post-quantum criptography), basats en problemes que es consideren més difícils que la factorització
- Junt amb comunicacions quàntiques
- Probablement els dos desenvolupaments conviuran

On som ara en Computació?

- La idea del Feynmann de simular altres sistemes quàntics sembla ser la que té més present (aplicació a la Química Quàntica)
- NO s'espera que puguin trobar solucions exactes a problemes d'optimització que són NP de forma eficient

Respecte a l'algorísmia

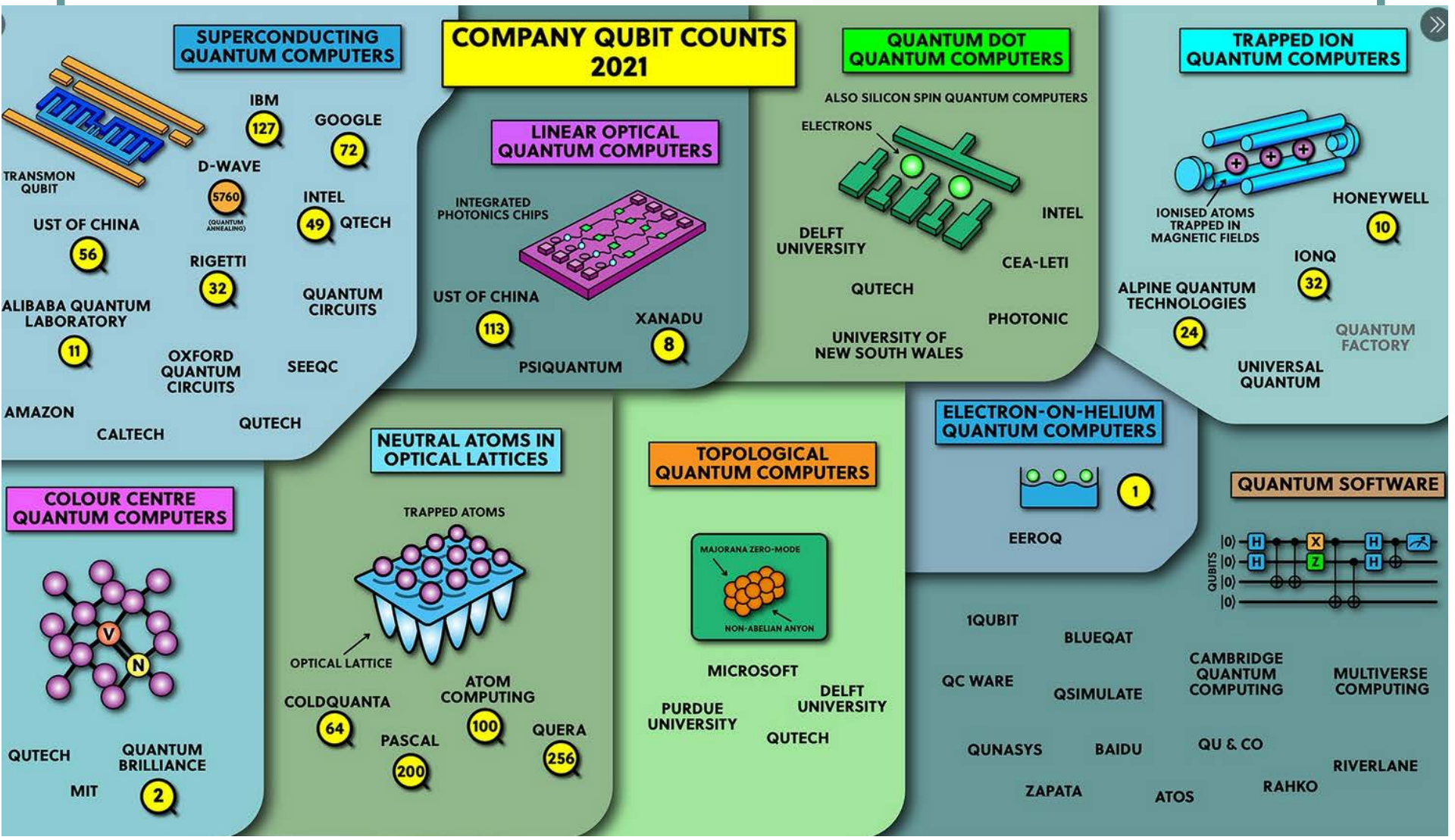
- Hi ha l'algorisme de Grover per buscar bases de dades però l'acceleració és quadràtica (i això suposant el mateix rellotge!)
- En el cas de la simulació de sistemes físics: clàssicament creix exponencialment amb N i en canvi linialment en un ordinador quàntic

Respecte al hardware

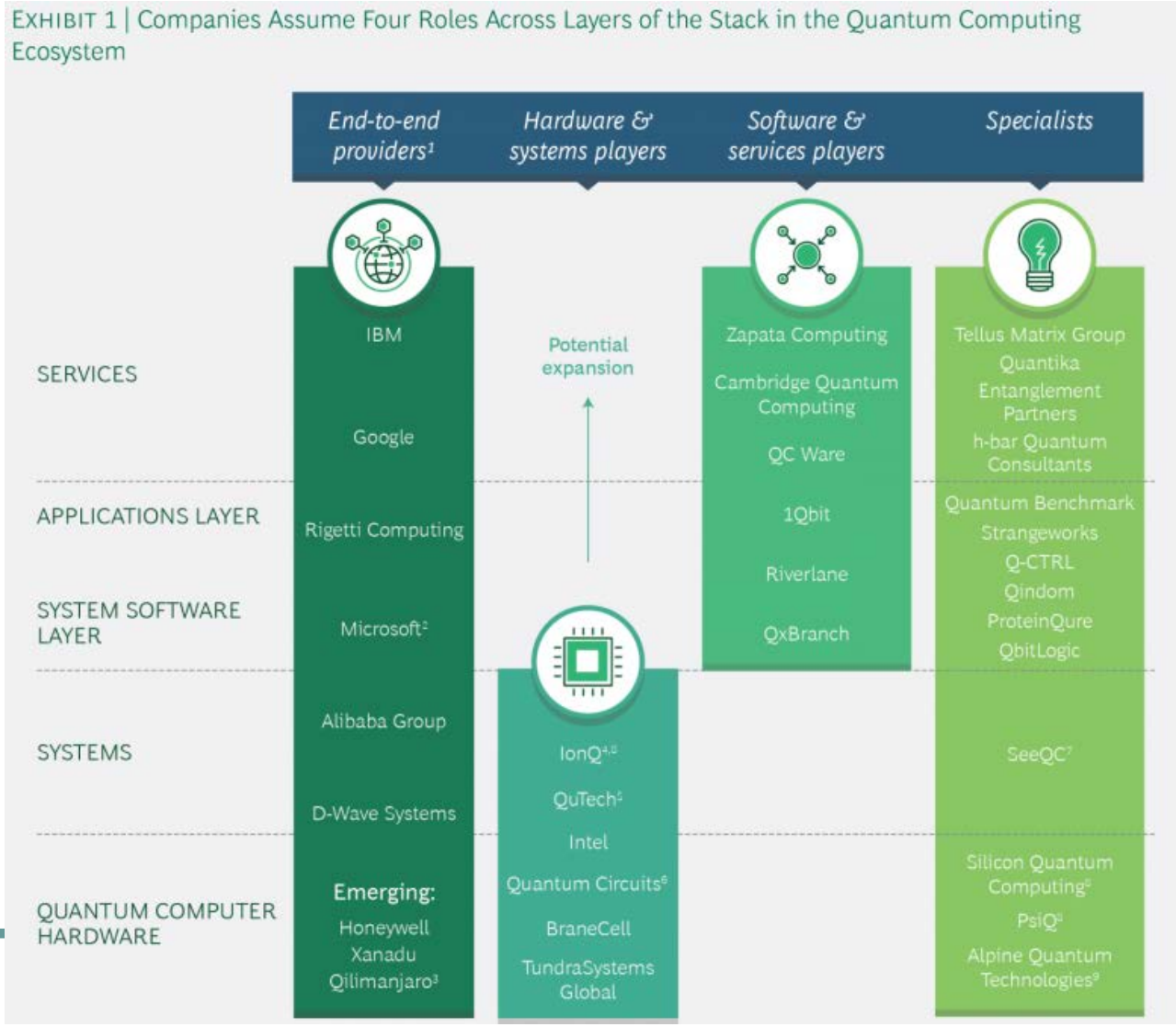
- Visió positiva: ja **existeixen els ordinadors quàntics**
- Hi ha moltes línies de recerca basades en diferents sistemes físics (com pels clàssics):
  - trampes d'ions
  - xarxes òptiques
  - circuits superconductors
  - circuits òptics

Això és el que hi ha ara mateix

(Dominic Walliman, també a youtube)



Els actors famosos volen fer tots els papers de l'auca



Un de casa nostra!

QILIMANJARO
QUANTUM · TECH

ABOUT CAREERS CONTAC

We develop quantum computers to accelerate widespread availability of quantum advantage for real-world optimization and Machine Learning problems.

We offer quantum algorithm expertise for customers to leverage the growing set of quantum computing platforms as well as of specialized quantum simulator platforms.

This customer experience translates into key guidance for Qilimanjaro's development of its high-quality superconducting qubit quantum computers, both gate-based and analog-based, with a special focus on its new generation of coherent analog quantum processors and a powerful and easy-to-use cloud access toolset.

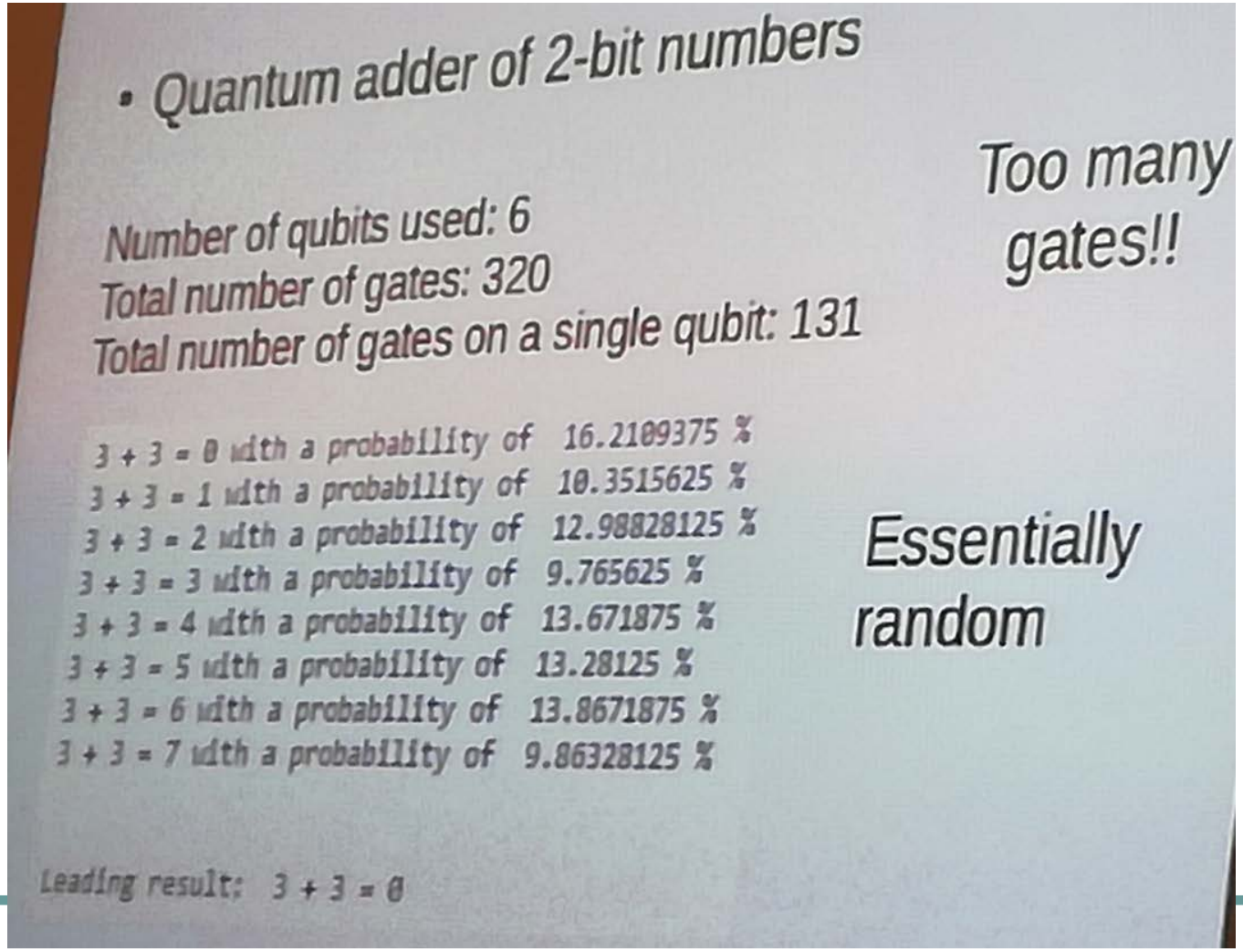
Qilimanjaro then works with customers to develop targeted quantum algorithmic solutions to their hard-computational problems, leading to the development of Qilimanjaro's software framework for algorithm and hardware co-design.

We build on the quantum expertise of our scientific founders with over fifty years of accumulated quantum experience and we leverage both the resources of IFAE's state-of-the-art lab infrastructure, BSC's leading high performance computing back-end as well as BSC and UB teams' advanced algorithmic expertise.

Tot i que ja em vist que

- De moment però segueixen sense ser gaire útils
- El problema és que estem pels vols de 100 qubits i això no permet correcció d'errors sobre els qubits
- Tampoc les portes tenen la fidelitat suficient

Un exemple (visió pessimista)



Som a l'era NISQ (Preskill): Noisy Intermediate-Scale Quantum

- **Intermediate scale**: aquests "dispositius" amb de l'ordre de 100 quibits **NO** poden ser simulats amb força bruta mitjançant els ordinadors clàssics més potents!
- **Noisy**: no tenen correcció d'errors i per tant el soroll limita molt la seva capacitat de càcul
- **Pels físics són molt interessants**: permeten estudiar, de forma controlada, sistemes sistemes quàntics que interactúen.
- **Pel món en general**: segurament només són un pas cap a l'objectiu final, no hi ha cap argument que justifiqui que poden fer res útil ara per ara.

Coses “realistes” que s’estan intentant ara mateix (entre moltes altres coses)

Hybrid quantum/classical, que bàsicament significa mirar d’introduir una acceleració “quàntica”:

- Aprofitar els ordinadors convencionals i utilitzar la part quàntica per alguna tasca molt concreta

- Utilitzar els ordinadors clàssics per optimitzar les connexions quàntiques per obtenir-ne el millor rendiment, a partir de l’anàlisi dels seus outputs per diferents casos

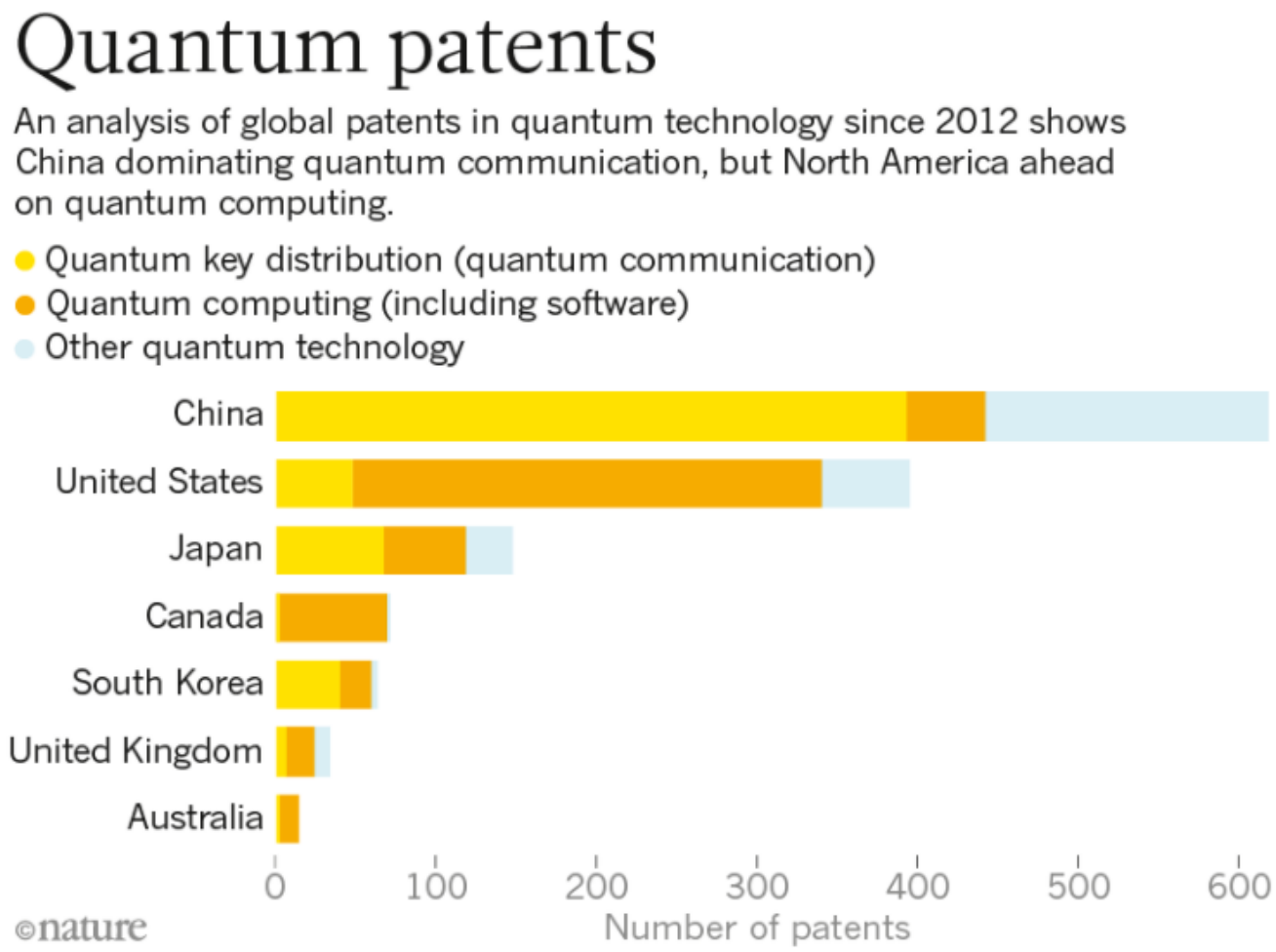
El futur?

- Requerirà FTQC (fault tolerant quantum computing, és a dir portes millors) i QEC (quantum error correction, qubits més estables)

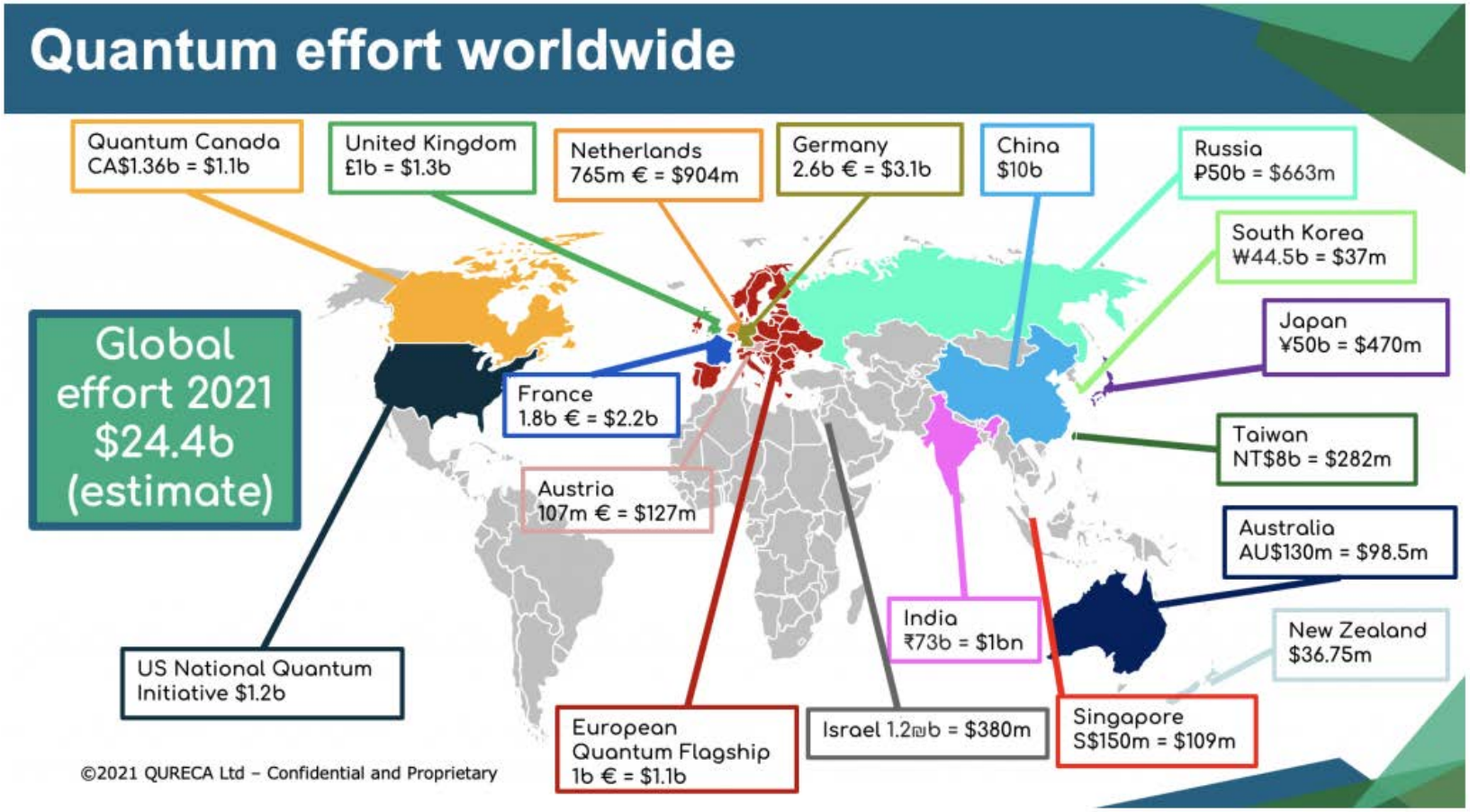
- Implica un overhead gran en nombre de qubits i de portes

- L'ordre de magnitud "segur" seria de 1,000,000 de qubits

Però és clar que això no espanta



I en termes d'inversió



O simplement no poden córrer el risc de quedar-ne fora…si funciona

De la wikipedia directament...

La juguesca de Pascal

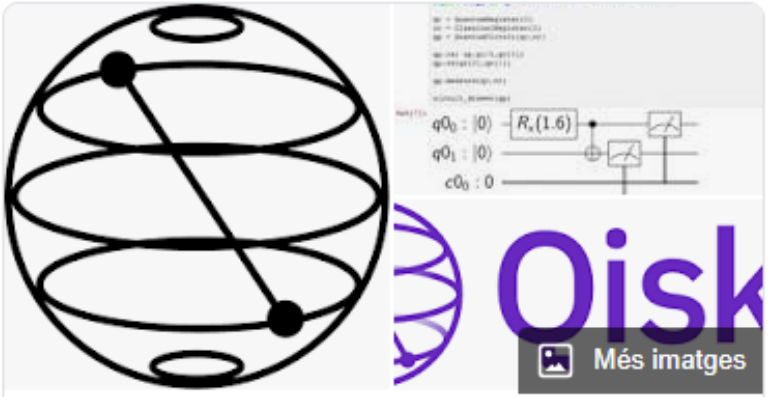
Pascal argumenta que una persona racional hauria de viure com si Déu existís... Si Déu no existeix, aquesta persona només tindrà una pèrdua finita (alguns plaers, riquesa, etc.), mentre que opta a tenir un guany infinit (representat per l'eternitat en el Paradís) i evita tenir una pèrdua infinita (l'eternitat a l‘Infern)

CONCLUSIONS?

- Les “paradoxes” de la Mecànica Quàntica permeten fer càlculs i transmissió d’informació de formes que fins ara no s’havien imaginat.

- Ja existeixen ordinadors quàntics però no són encara útils, potser vosaltres podreu contribuir-hi …

No calen professors…?



Qiskit

Programari

Qiskit és una eina creada per IBM per al desenvolupament de Programari quàntic. Usa el llenguatge de programació de Python tot i que n'hi ha versions per Swift i Javascript també disponible. Qiskit està basat en la llibreria d'OpenQASM per a la representació de circuits quàntics. Viquipèdia

Llenguatge de programació: Python

Nosaltres, poc a poc i bona lletra

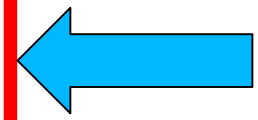
Building the quantum workforce

02/01/22 | By Amanda Solliday

Making strides in quantum information science and its applications will require cooperation among experts from a variety of backgrounds, she says.

A growing field

Through courses in computer science, physics, engineering and math, students gain expertise that's in demand as the quantum field expands. For students wanting to explore quantum technology, physicist Aaron Chou has this advice: Spend some time understanding quantum mechanics. It's not as intimidating as you think.



Programa: un llarg camí

- **PRIMERA PART: FONAMENTACIÓ**
  - Ones/partícules macro
  - Ones/partícules micro
  - Equació Schrodinger
  - Maquinària de la Mecànica Quàntica

- **SEGONA PART: APLICACIÓ A LA CCQ**
  - Qubits
  - Criptografia Quàntica
  - Portes quàntiques
  - Algorismes quàntics