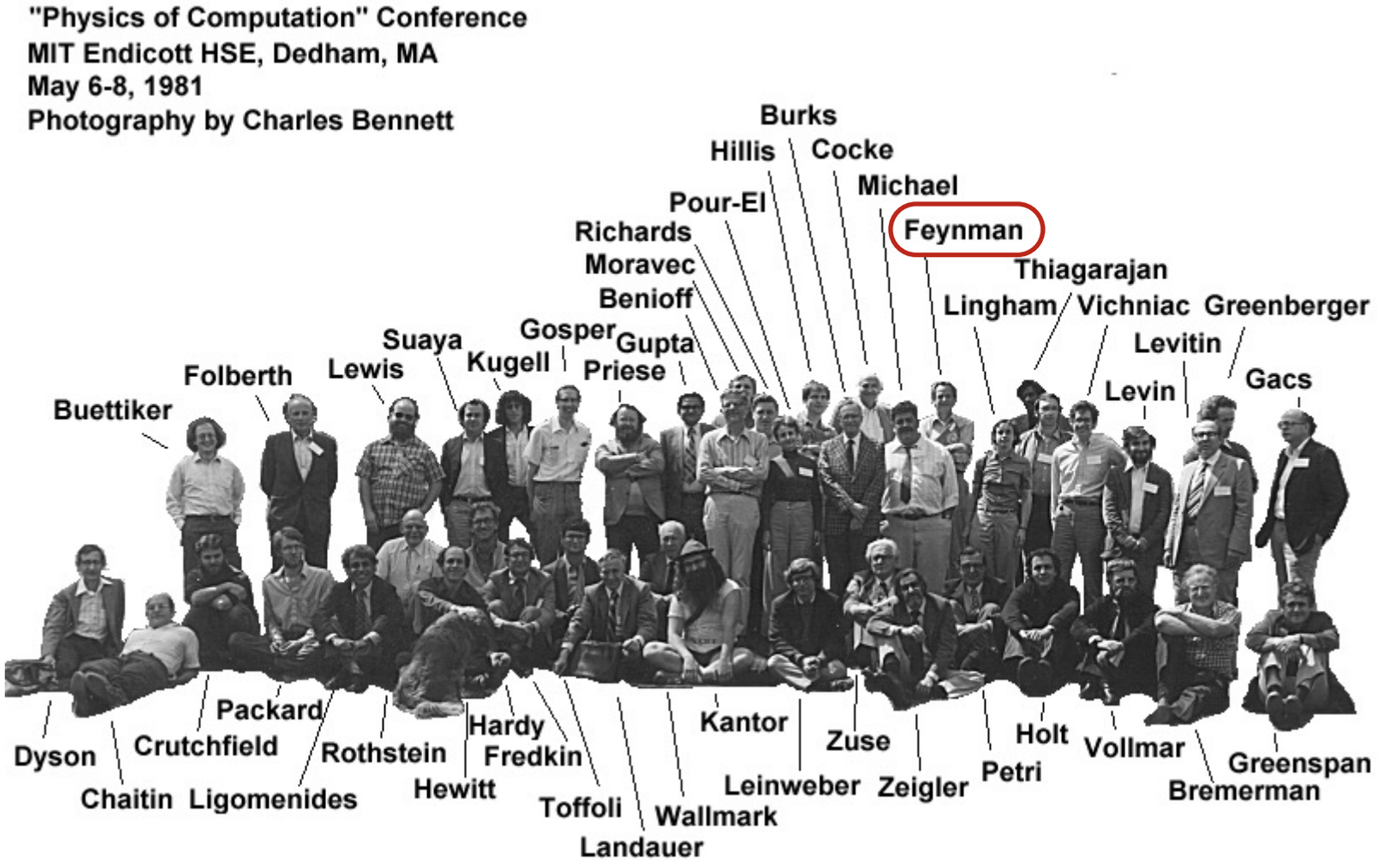
Bizkaia lantik

Introducción a la Computación Cuántica

Valentin Garcia

Física computacional



I think I can safely say that nobody understands quantum mechanics.

[Richard P. Feynman (1965)]

Bizkaia lantik

Agenda

- Mecánica cuántica
- Conceptos básicos
- Computación cuántica
- Algunos usos

Bizkaia lantik

Mecánica cuántica

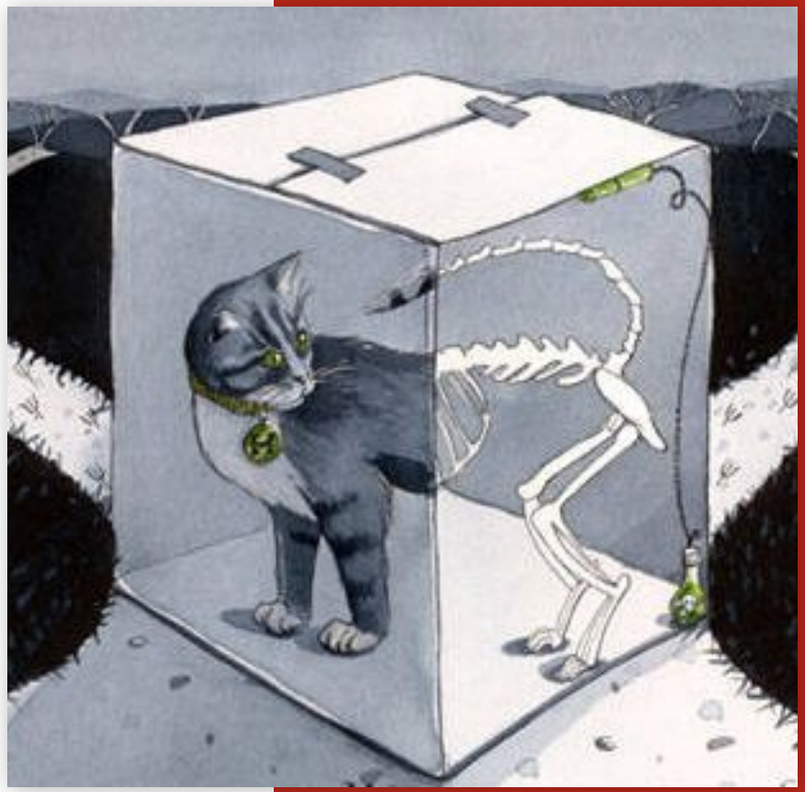
El término de mecánica cuántica se acuñó a principios del siglo XX para describir los fenómenos que se producen debido a la existencia e interacción de ondas y partículas subatómicas.

Gracias a estos primeros estudios se produjo la primera revolución cuántica, que condujo al desarrollo de inventos como el reloj atómico, los semiconductores o el láser.

Superposición cuántica

La superposición cuántica ocurre en la naturaleza cuando una partícula elemental posee simultáneamente dos o más estados, como pasa por ejemplo con los fotones, que pueden permanecer en dos lugares diferentes al mismo tiempo, algo inimaginable en el mundo físico ordinario.

Esta propiedad se ha observado también en otras partículas, como los electrones o neutrones, en los átomos o incluso en pequeñas moléculas, según ha ido descubriendo la ciencia.



Entrelazamiento cuántico

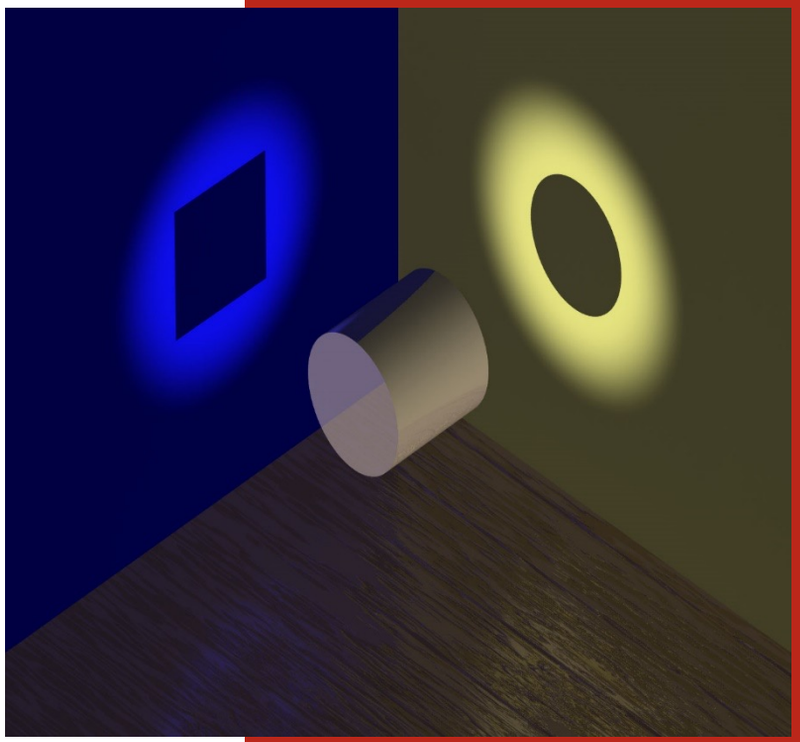
Ocurre cuando dos partículas están conectadas de tal manera que lo que sucede con una inmediatamente afecta a la otra, sin importar cuan grande sea la distancia entre ellas.

Esto tiene como consecuencia que cuando se perturba una de esas dos partículas, la otra sabe instantáneamente (más rápido que la velocidad de la luz) la información que ha sido perturbada de la primera.

Dualidad onda - partícula

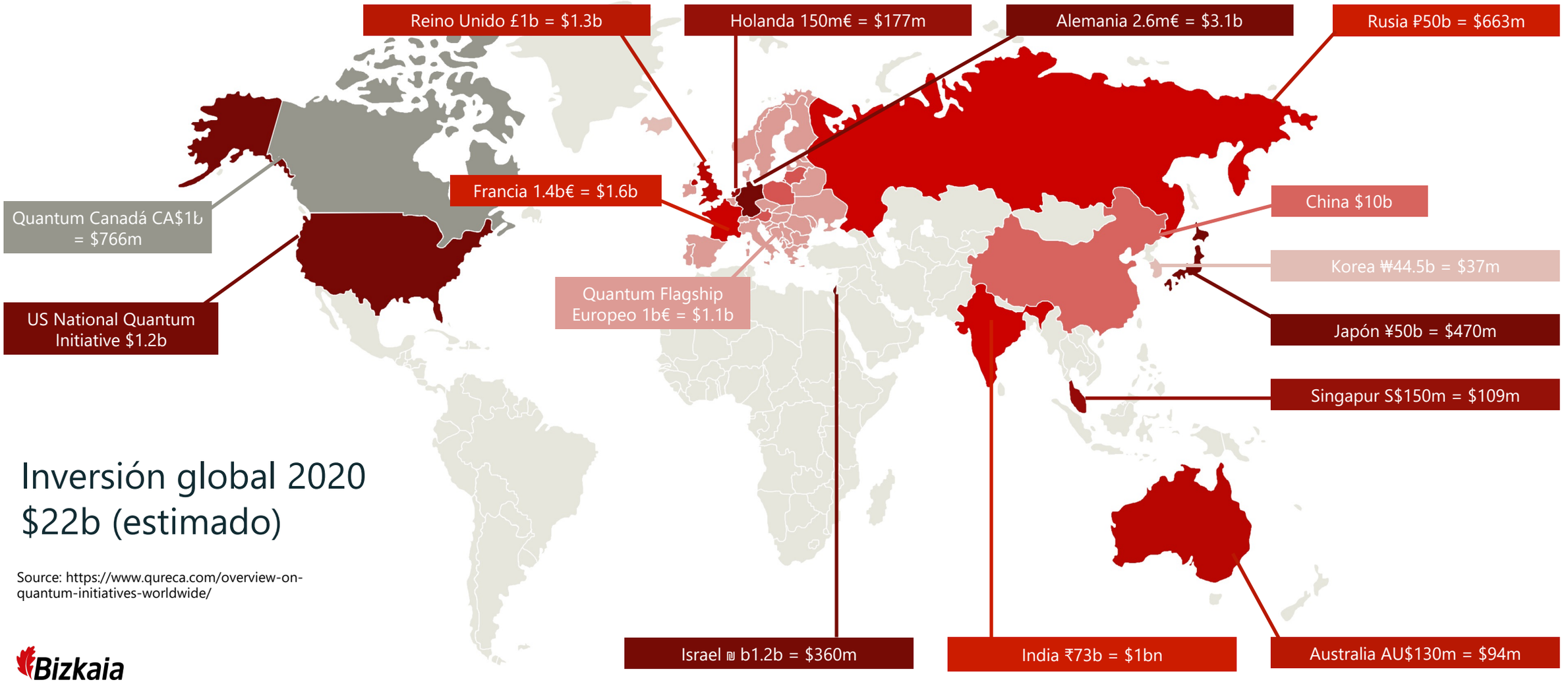
Concepto de la mecánica cuántica según el cual no hay diferencias fundamentales entre partículas y ondas: las partículas pueden comportarse como ondas y viceversa.

Propone la existencia de ondas de materia, es decir que toda materia tenía una onda asociada a ella.



Inversiones en tecnologías cuánticas

Top 15 regiones del Sector Público



Inversión global 2020
$22b (estimado)

Source: https://www.qureca.com/overview-on-quantum-initiatives-worldwide/

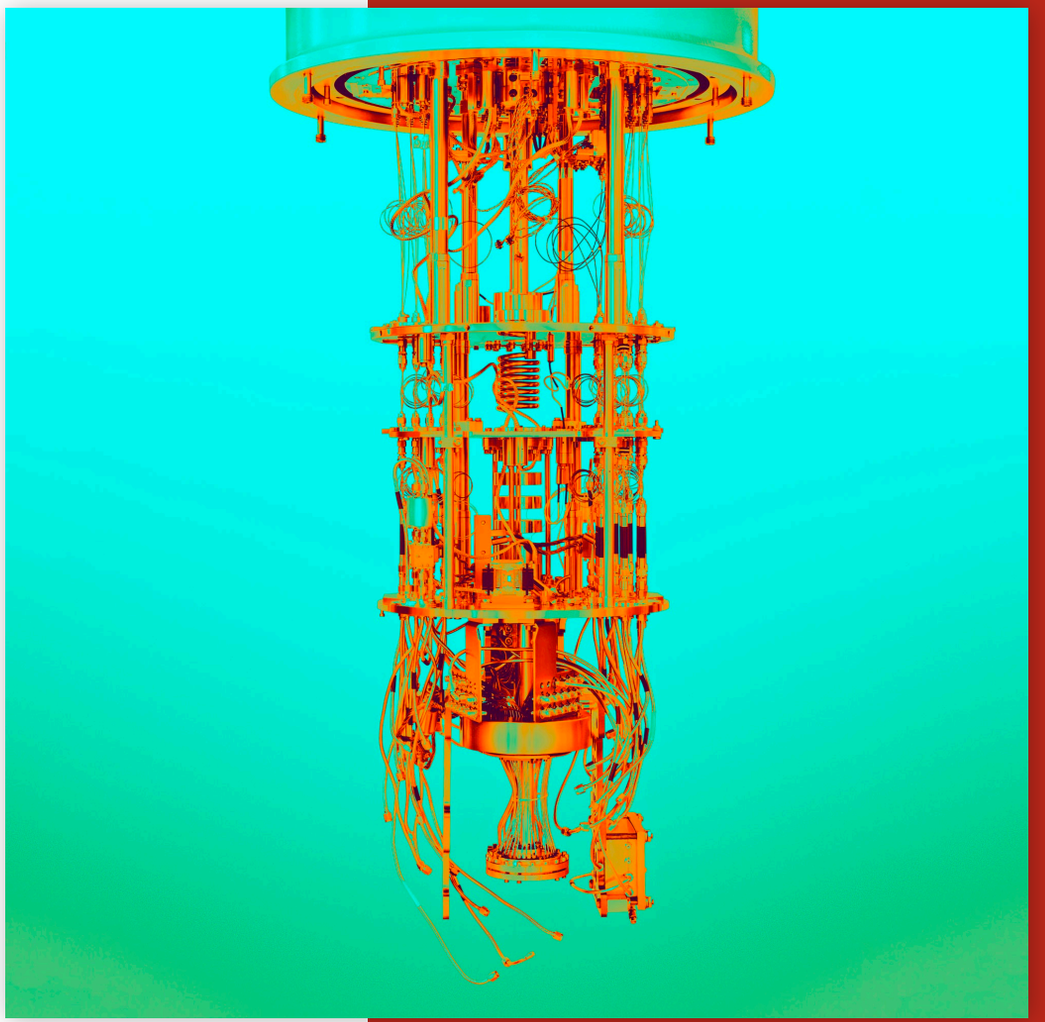
Bizkaia lantik

Computación Cuántica

Quantum Computing

La computación cuántica o informática cuántica es un paradigma de computación distinto al de la informática clásica o computación clásica.

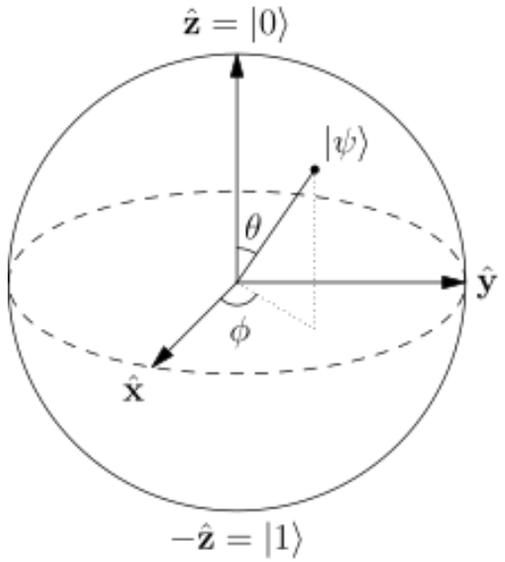
Se basa en el uso de cúbits, una especial combinación de unos y ceros. Los bits de la computación clásica pueden estar en 1 o en 0, pero solo un estado a la vez; en tanto el cúbit puede tener los dos estados simultáneos también. Esto da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.



Cúbit (Qbit – Qubit)

En la informática cuántica, un cúbit o bit cuántico es la unidad básica de la información cuántica, la versión cuántica del bit binario clásico realizado físicamente con un dispositivo de dos estados.

En un sistema clásico, un bit tendría que estar en uno u otro estado 0 o 1. Sin embargo, la mecánica cuántica permite que el cúbit esté en una superposición coherente de ambos estados simultáneamente.



Qbit state

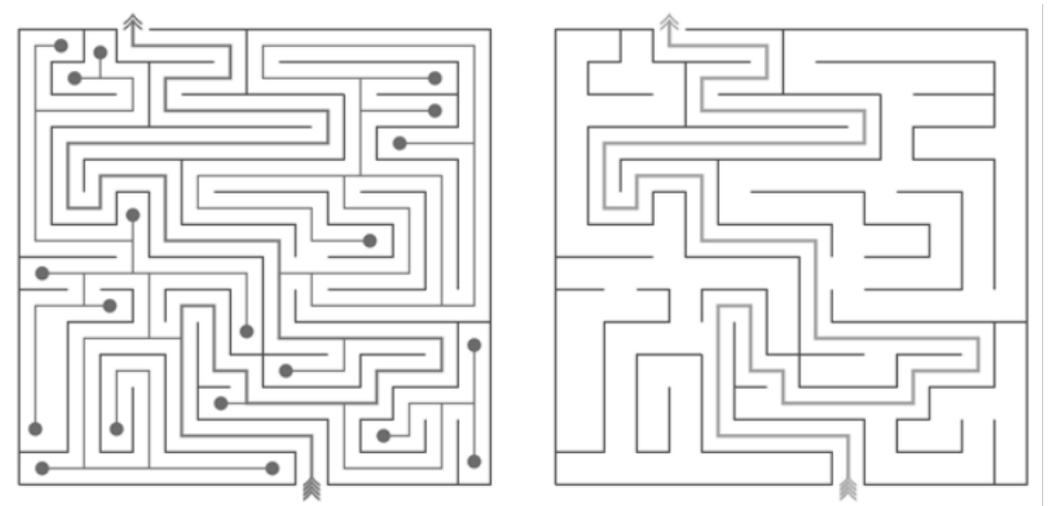
$$\psi = \alpha|0\rangle + \beta|1\rangle$$

Probablity of the spin existing as $|1\rangle$

Probablity of the spin existing as $|0\rangle$

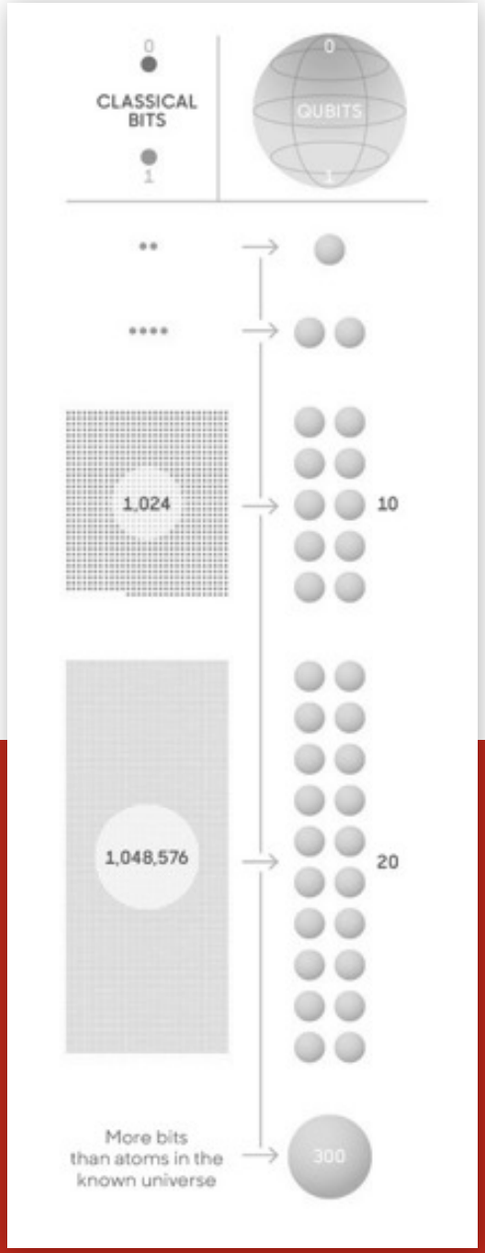
Es necesario un cambio de paradigma: transición de bit a cúbit

Estos ordenadores no se comportan como los clásicos, pero sabemos teóricamente que son más rápidos para cierto tipo de problemas...

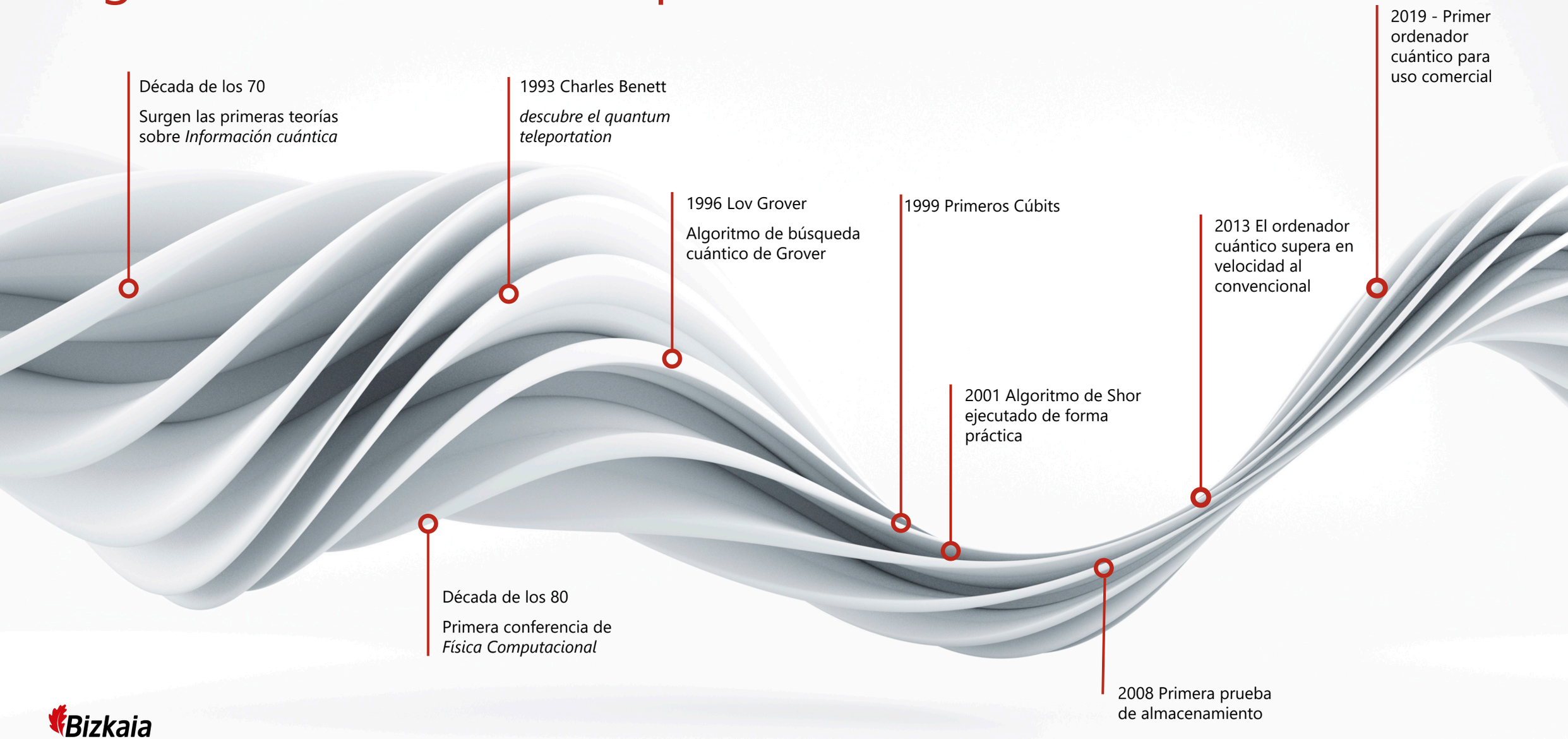


Un ordenador clásico tiene que mirar cada camino a través del laberinto

Un ordenador cuántico mira el laberinto de manera completa y obtiene el camino más corto



Algunos hitos de la computación cuántica



Bizkaia lantik

Adopción de las tecnologías

1 Mainframe

2 Client-server and pcs

3 Web 1.0 eCommerce

4 Web 2.0, cloud, mobile

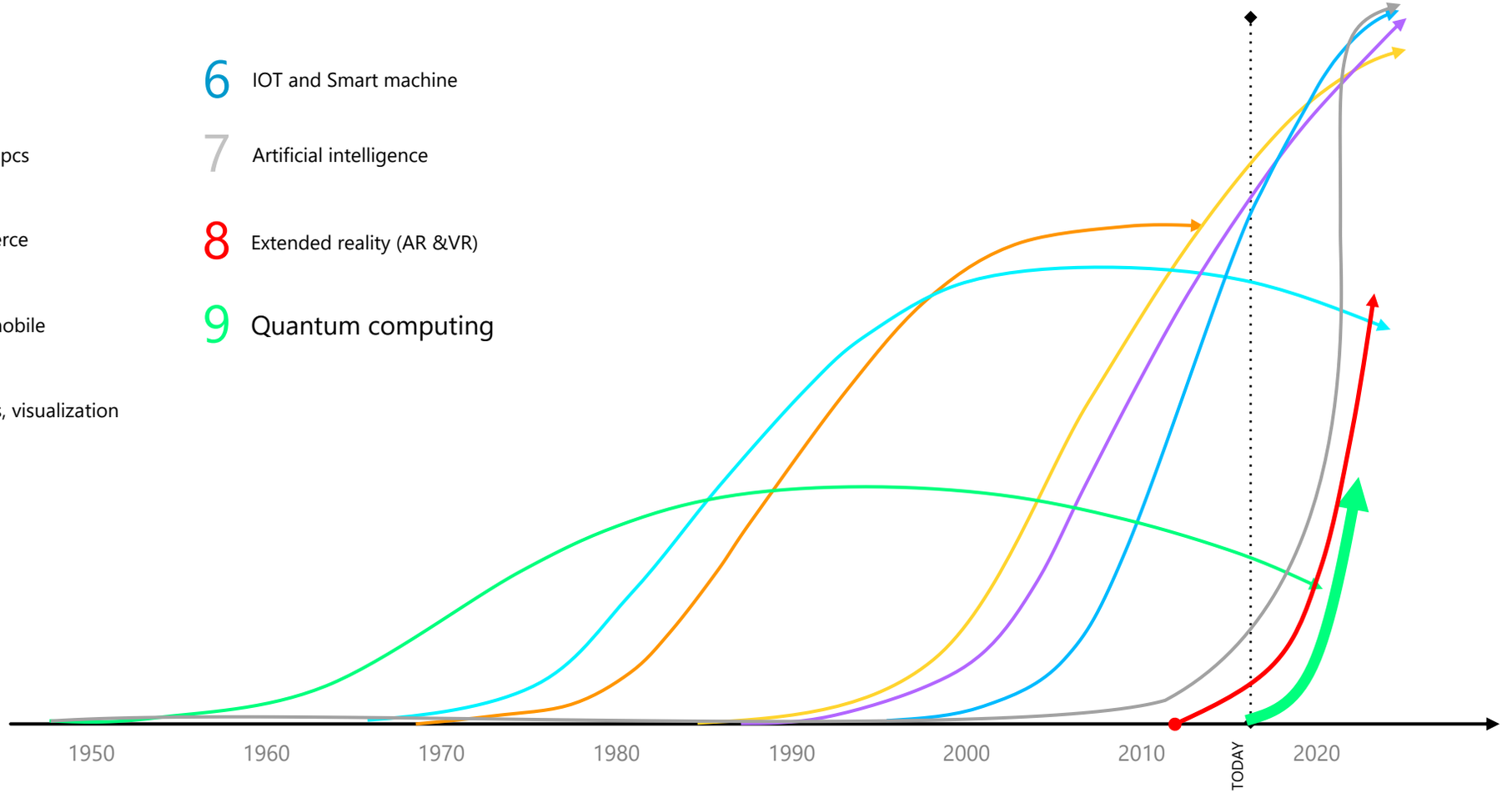
5 Big data, analytics, visualization

6 IOT and Smart machine

7 Artificial intelligence

8 Extended reality (AR &VR)

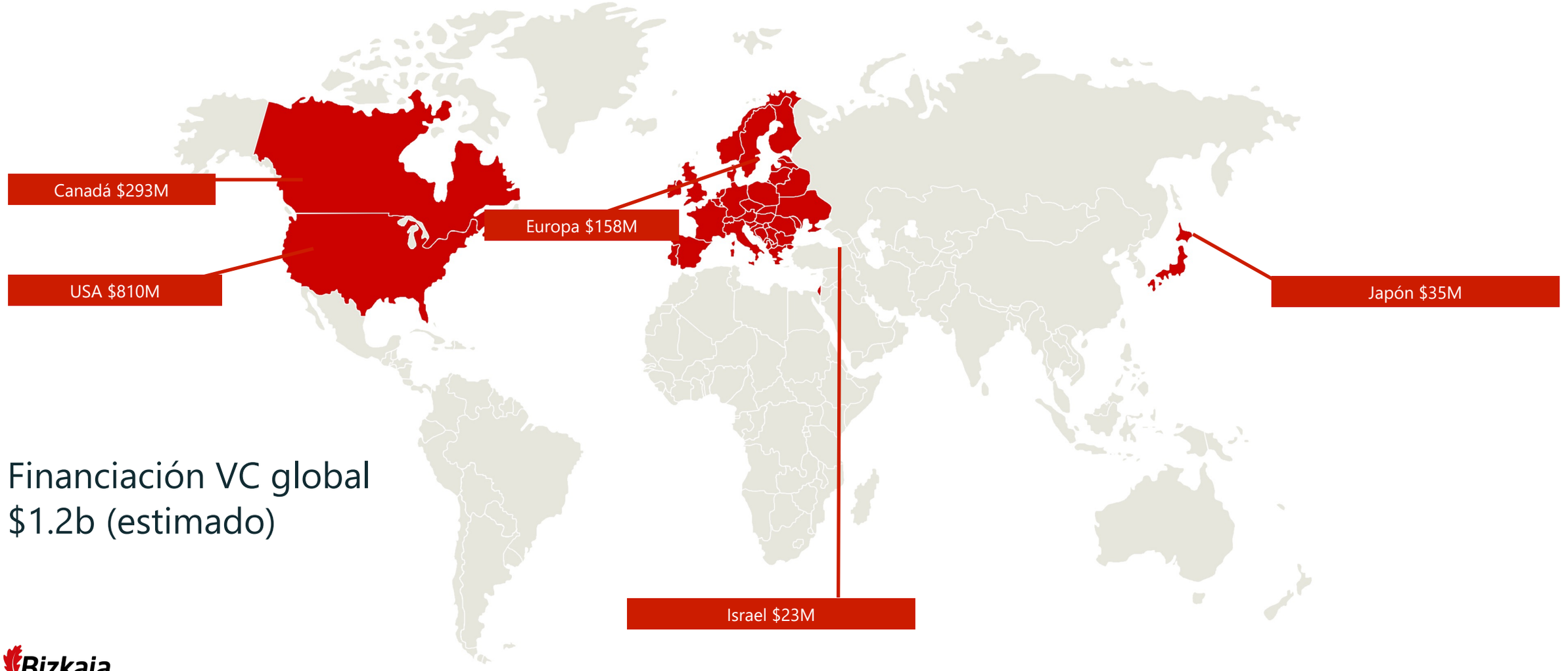
9 Quantum computing



Bizkaia lantik

Inversiones en computación cuántica

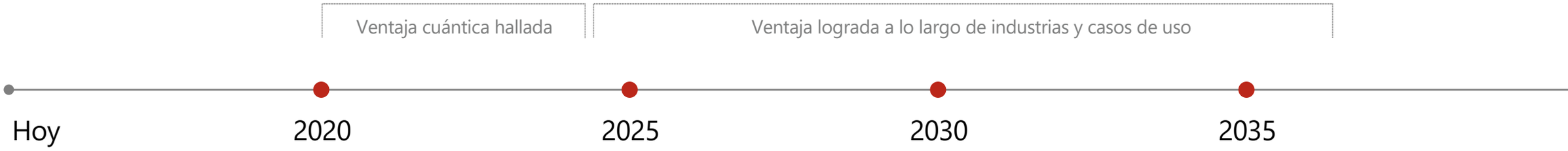
Top 5 regiones



Financiación VC global
$1.2b (estimado)

Bizkaia lantik

Supremacía cuántica



Educar clientes y construir software para la futura ventaja cuántica

Efecto complementario de computación cuántica + clásica

Las primeras aplicaciones reales llegan en el sector farmacéutico simulando nuevos materiales

Técnicas de optimización cuántica viables para trading financiero

Las empresas de supply chain redefinen sus procesos y estrategias globales gracias a los algoritmos de optimización cuánticos

Quantum machine learning sobrepasa las aproximaciones clásicas

Los ordenadores cuánticos rompen la seguridad y son capaces de desencriptar cualquier dato que no esté usando cifrado resistente a tecnologías cuánticas

Algunos usos

Aplicaciones de la computación cuántica

Problemas que QC tiene el potencial a resolver, congregado alrededor de tres áreas principales:

Algoritmos de Machine Learning

(e.g. factorización, sistemas de ecuaciones – criptografía…)

Optimización combinatoria

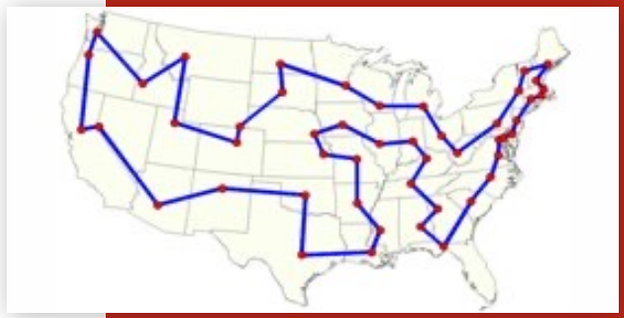
(e.g. problema del viajero, optimización de procesos de negocio, análisis de riesgo…)

Muestreo y simulación

(e.g. química, ciencia de materiales…)

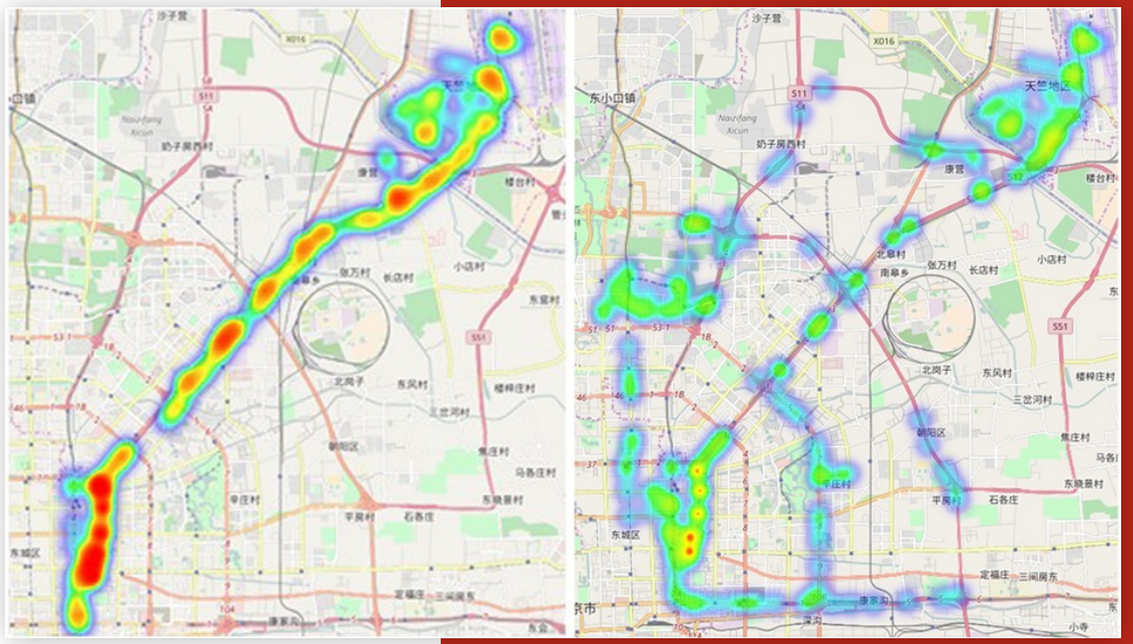
CRYPTOGRAPHY
Mientras que la Computación cuántica resolverá muchos de los problemas de negocio, hay una amenaza asociada con la tecnología. Los ordenadores cuánticos ofrecen un fuerte encriptado, protegiendo el negocio y sus consumidores, aunque también convertirán al encriptado convencional más vulnerable a ataques.

Optimización de rutas



Mediante el uso de la detección de caminos y/o circuitos hamiltonianos y los puntos por los que tiene que pasar una flota de por ejemplo, camiones podemos trazar su ruta optima.

Al igual que se puede trazar la ruta optima se puede realizar la distribución del tráfico de la flota para realizar en el menor tiempo posible el reparto.



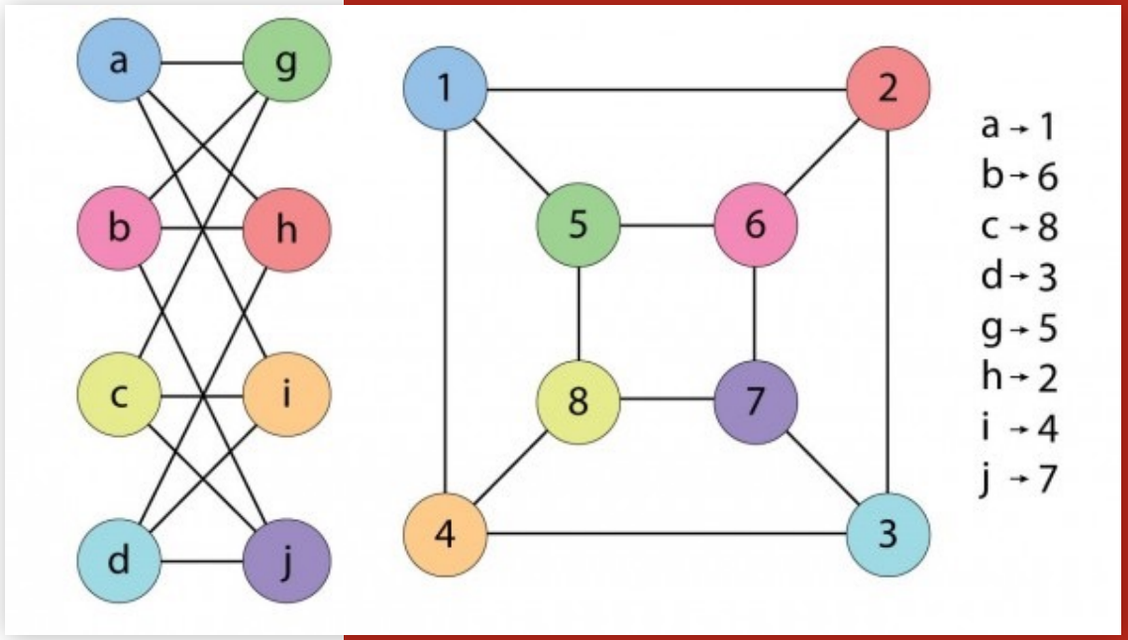
Optimización de procesos de manufactura

Al igual que ocurre con las rutas entre dos puntos, las cadenas de montaje también se pueden considerar como puntos de un grafo cada acción sobre la cual se tiene que realizar este proceso. Por ejemplo, cuando montamos un coche, podemos ensamblar la puerta a la carrocería o podemos encajar los decorados de la puerta y luego ensamblarla, dependiendo del tiempo que lleve realizar cada una de las tareas podemos decidir cuándo realizar cada una. Al final, la traducción del problema es, cada punto donde se realiza una acción es un punto del grafo y se elige el camino a realizar en función de las dependencias.

Secuenciación y comparación de moléculas

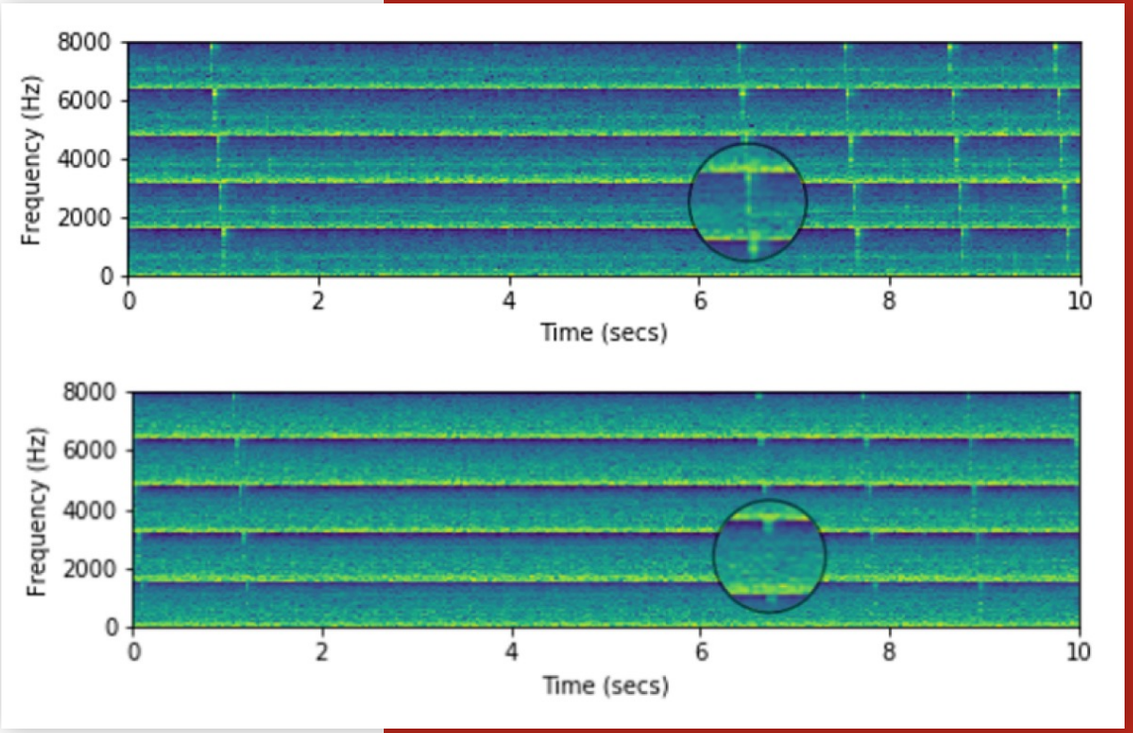
Al igual que ocurre con las cadenas de montaje, las moléculas se comportan como grafos y para evaluar si dos moléculas son iguales se aplica la teoría de isomorfía de grafos, que también se puede realizar mediante teoría de grafos comparando los circuitos de los mismos.

Resultado: Ahorro significativo en los costes de producción (Fertilizante)



Detección de anomalías

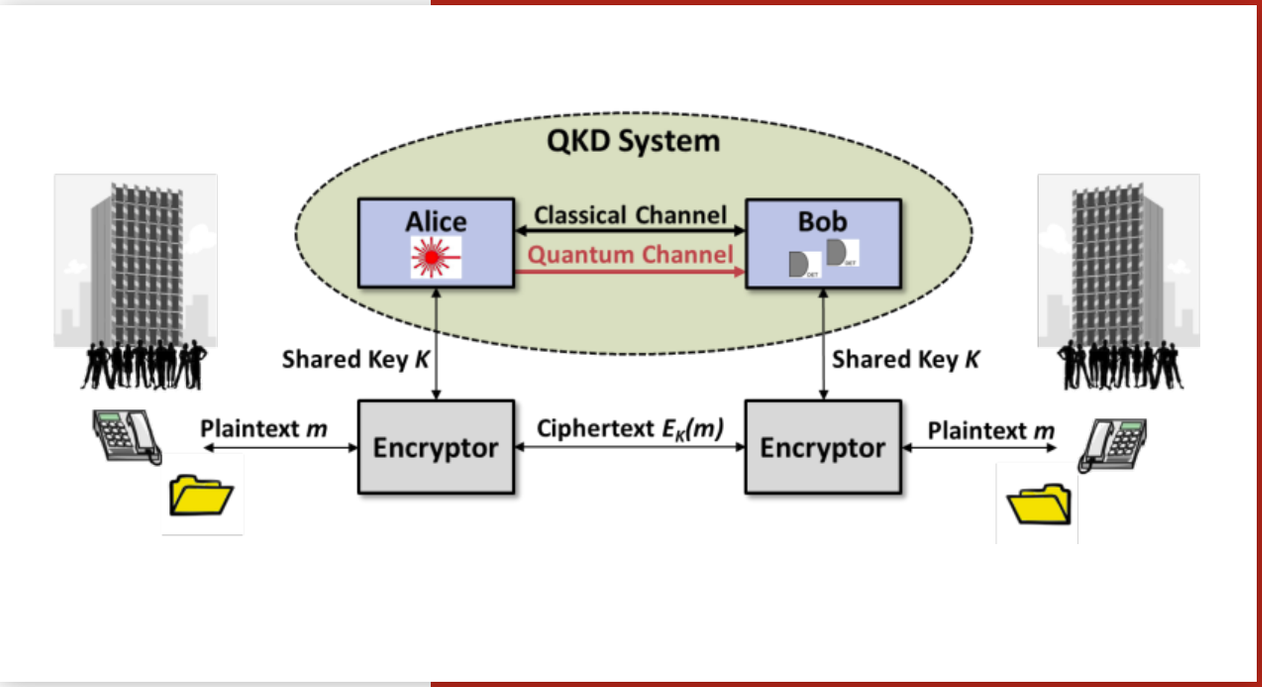
A través de la computación cuántica se puede realizar detección de anomalías como se muestra en el siguiente paper aplicando QC + ML. Este paper ilustra que con un gran dataset de información se puede reducir la complejidad de la detección en O(Log(N)).

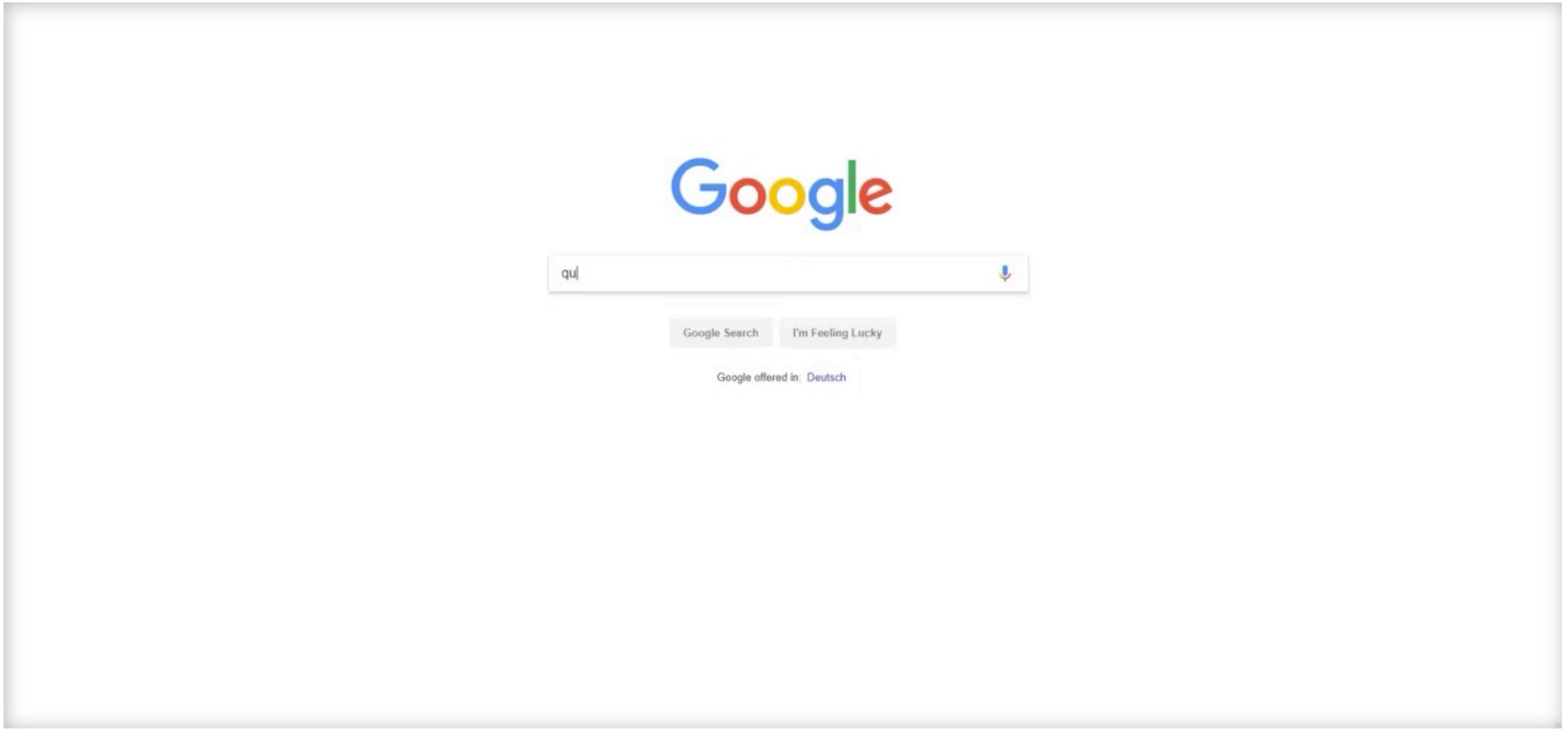


Bizkaia lantik

Cifrado de mensajería

Como hemos visto en el punto anterior de algoritmos existe el algoritmo QKD, que permite el intercambio de claves muy largas que pueden ser utilizadas para proporcionar la confidencialidad de los mensajes mediante el cifrado de una sola clave. Debido a su alto costo, esto significa que su principal área de aplicación es la de las aplicaciones de muy alta seguridad.




Google
qu
Google Search
I'm Feeling Lucky
Google offered in: Deutsch

Bizkaia lantik

Eskerrik asko!

valentin.garcia@bizkaia.eus