

La computation cuántica, la nueva arena

MSc. Ing. Carlos del Porto Blanco

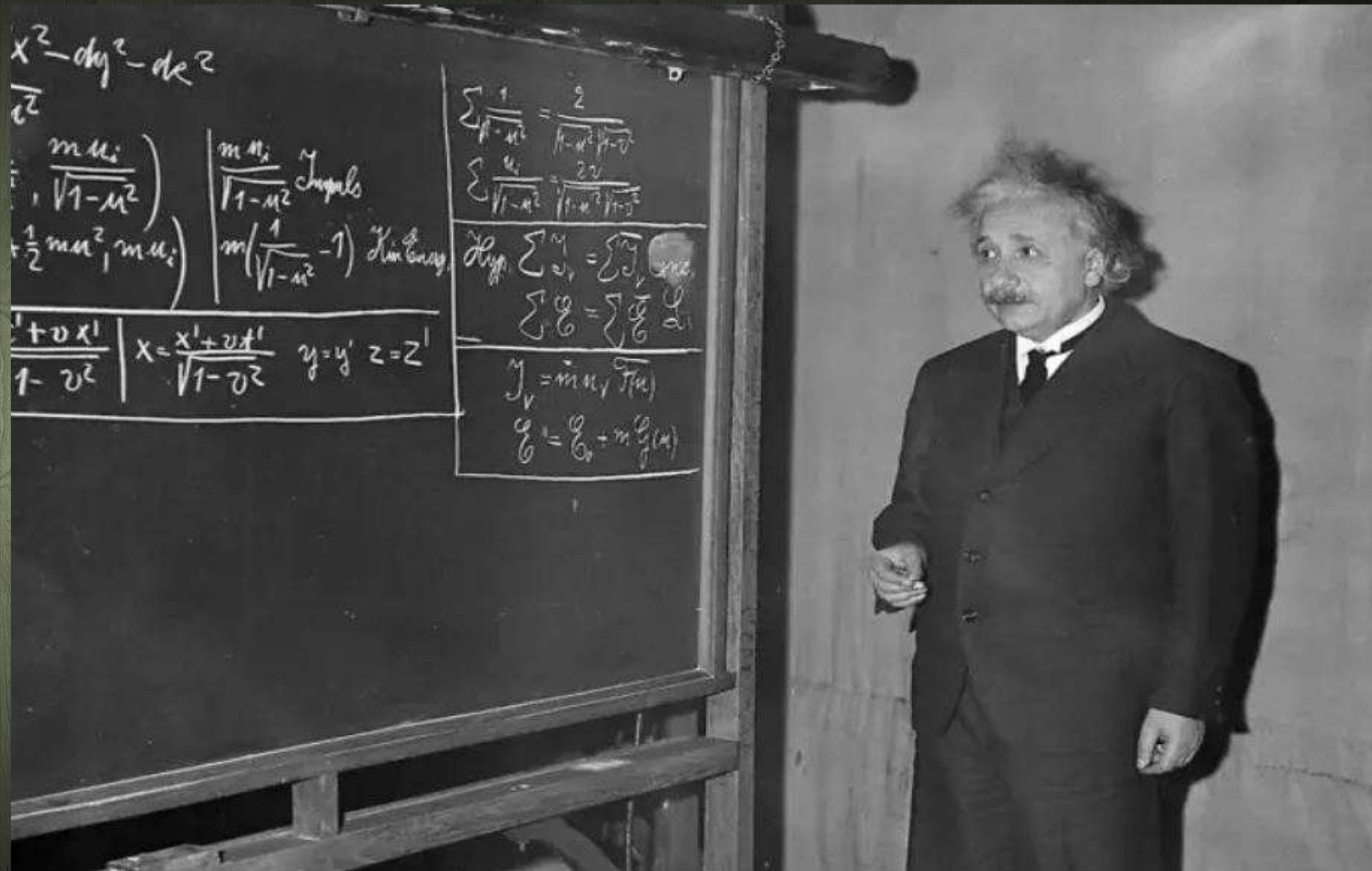
Profesor Auxiliar, ISRI

www.facebook.com/CarlosdelPortoBlanco

Telegram: @CarlosdelPorto

Bluesky: @delportocarlos.bsky.social

Dios no
juega a los
dados con
el Universo



Albert Einstein en polémica con Niels Bohr

Hitos a considerar

Se hace oficial la
World Wide Web,
WWW. **1991.**
Estados Unidos



Aparece la IBM
PC. **1981.**
Estados
Unidos.



Aparece el Iphone.
2007. Estados
Unidos.

Aparece ChtGPT,
Boom de IA
generativa. **2023.**
Estados unidos



Computadora
cuántica

¿De qué hablamos?

La **computación cuántica** es una nueva **forma de cálculo** que utiliza principios de la **física fundamental** para resolver problemas extremadamente complejos muy rápidamente. Si se lanza una **moneda al aire**, se espera obtener **cara o cruz** una vez que ésta cae. Pero mientras la moneda gira en el aire, **no es ni cara ni cruz**; existe la misma probabilidad de que sea ambas. **Esa área gris es la base simplificada de la computación cuántica**



El gato de Schrödinger

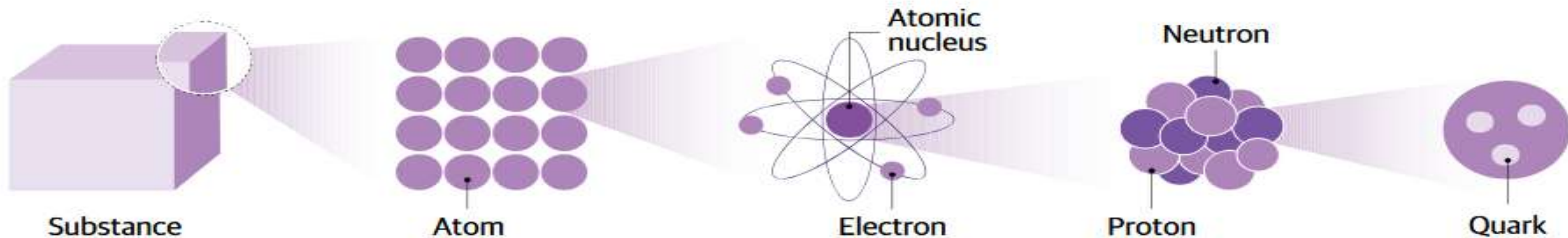


bit

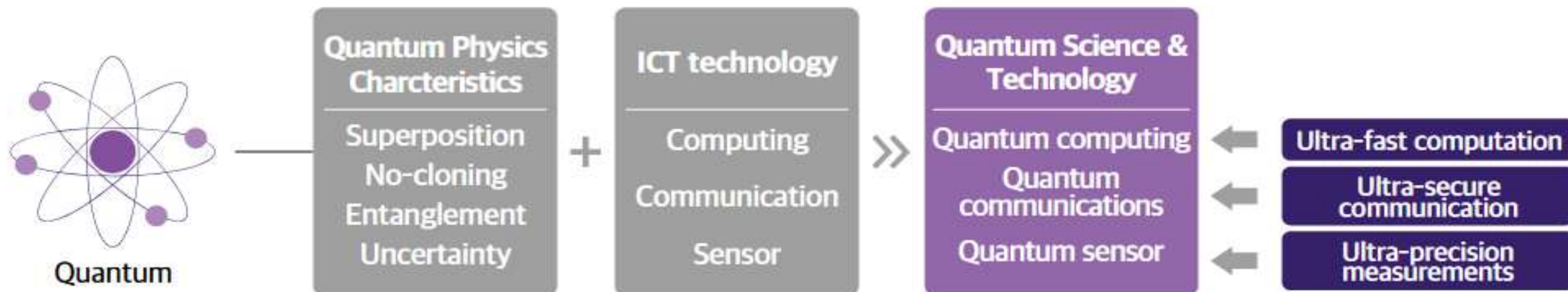


cúbit

Los **bits** pueden estar en **0** o **1**. Los **cúbits** pueden estar en cualquiera de los infinitos estados intermedios entre el **0** y el **1**, como por ejemplo un estado que sea mitad 0 y mitad 1, o tres cuartos de 0 y un cuarto de 1. Ese fenómeno es conocido como **superposición cuántica**



「Tiny physical systems with observable quantum phenomena」



Un ejemplo pedestre de aplicación

Alguien quiere ir de la ciudad A a la B y desea conocer cuál es la mejor ruta entre un millón de opciones disponibles ($N=1\ 000\ 000$).

Habría que digitalizar un **millón de opciones**, lo que implica traducirlas a **lenguaje binario** para la **computadora clásica** y a **cúbits** para la **computadora cuántica**. Mientras la primera necesita ir uno por uno analizando todos los caminos hasta encontrar el deseado, la cuántica utiliza el proceso conocido como paralelismo cuántico que le permite considerar todos los caminos a la vez. Eso implica que la **computadora clásica** necesitaría trabajos del orden de **$N/2$** pasos, es decir, **500 000 intentos**, la cuántica encontraría la ruta óptima en **\sqrt{N}** operaciones sobre el registro, es decir, **mil intentos**.

Una computadora cuántica con 270 cúbits podría tener más estados base en una (cadenas de caracteres diferentes y simultáneas) que el número de átomos en el universo, que se estiman en un valor en el entorno de 2^{80} . Otro ejemplo, se estima que con una computadora cuántica de entre 2000 y 2500 cúbits se podría romper prácticamente toda la criptografía utilizada hoy en día.

La **geopolítica cuántica** es una disciplina emergente que estudia la competición entre los países por **alcanzar la supremacía cuántica**. Es una rama del análisis geopolítico general, más que un campo de estudio desarrollado. La **computación cuántica es una revolución tecnológica que acelerará las comunicaciones**, permitirá avances en campos como la Inteligencia Artificial o la medicina, y **cuestionará los estándares de ciberseguridad actuales**. Su impacto en la economía y en las capacidades de defensa ha dado pie a una carrera entre Estados Unidos, China, India, la Unión Europea, Rusia y otras potencias.

Las computadoras cuánticas **podrían romper los estándares de cifrado** actuales. La infraestructura digital, desde las **comunicaciones militares** hasta la **banca** y el **comercio electrónico**, depende de algoritmos cifrado que estas computadoras podrán descifrar. La perspectiva de que una computadora cuántica, criptográficamente relevante, logre esa capacidad se considera un punto de inflexión para la seguridad nacional de los países

Information unit

1 and 0 probabilistic (superpositioned) qubit

Application



Ultra-fast quantum computers



Ultra-secure reliable quantum Internet



Ultra-precise quantum devices (sensing and measurements)

Quantum Age (2nd Quantum Revolution)

Application



PC



Internet



Digital music



Smartphone

Information unit

0 or 1 deterministic digital bit

Digital Age (1st Quantum Revolution)

Application



TV



Radio



Photograph



Telephone

Information unit

Continuous physical quantities, such as current and voltage

Analog Age

20C First Quantum Revolution

Quantum mechanics' "wave-particle" duality



Laser (induced emission)



Solar cell (photoelectric effect)



Semiconductor (quantum band gap)

21C Second Quantum Revolution



Quantum Computing



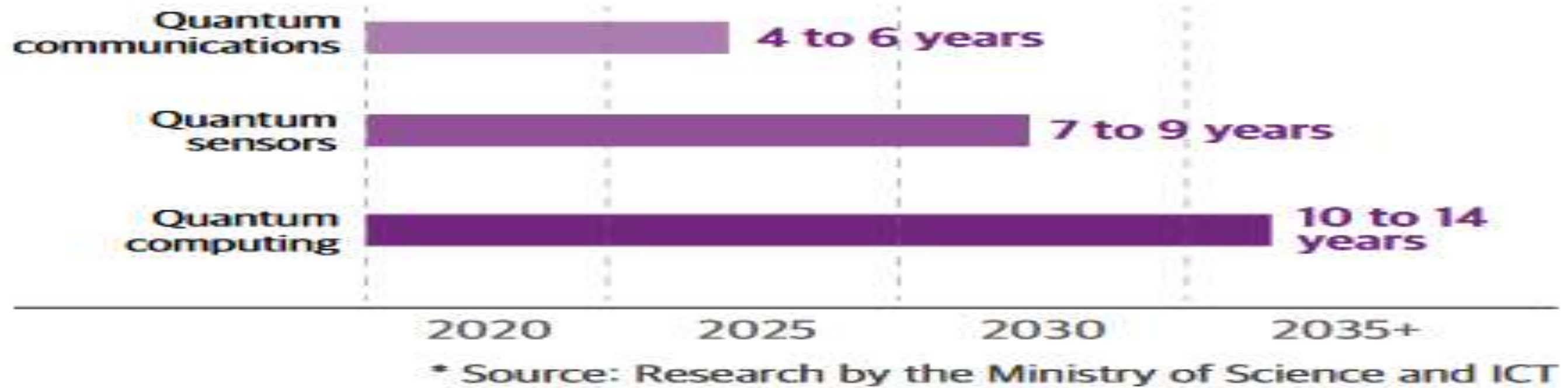
Quantum communication



Quantum sensor

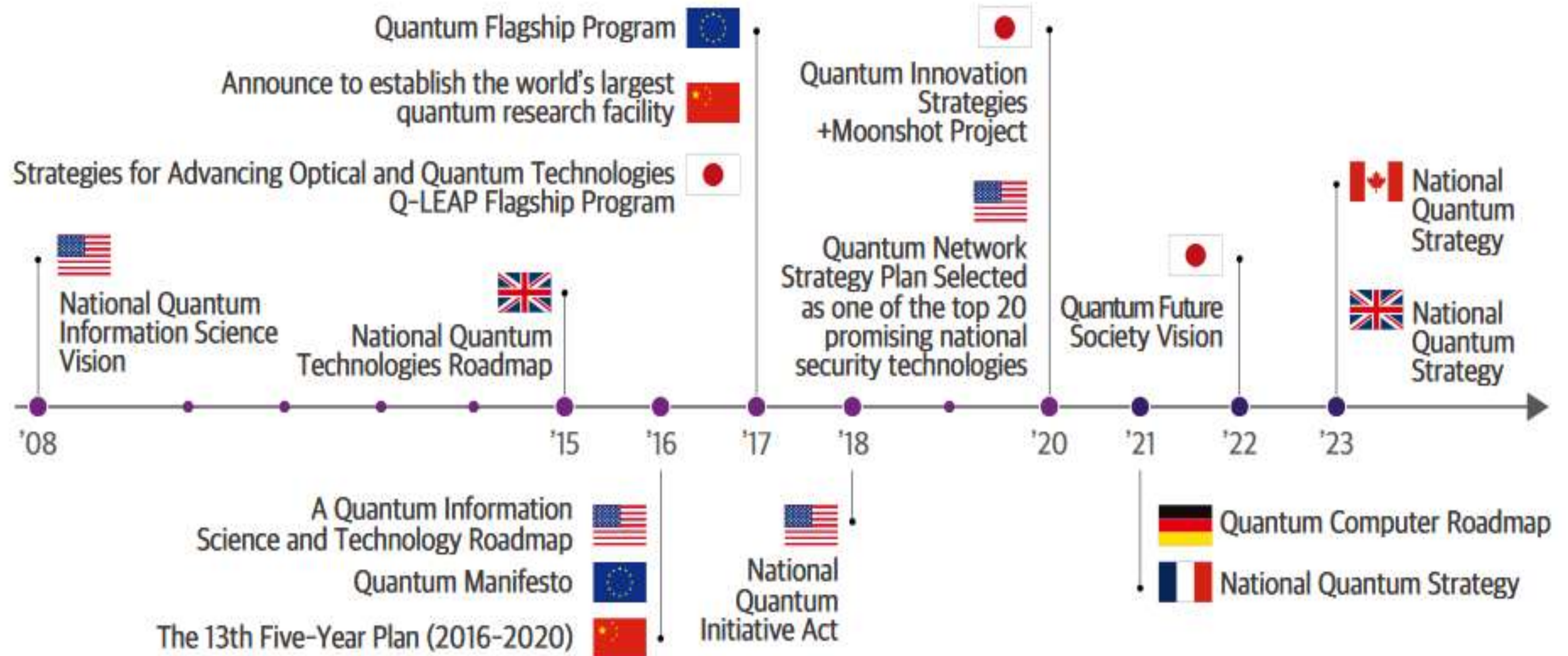


<Projected Quantum Market Size>



<Expected Timeline for the Formation of the Quantum Market>

< Quantum Science and Technology Strategies by Country >





Quantum 1-1

Optimization of Semiconductor Manufacturing and Processing

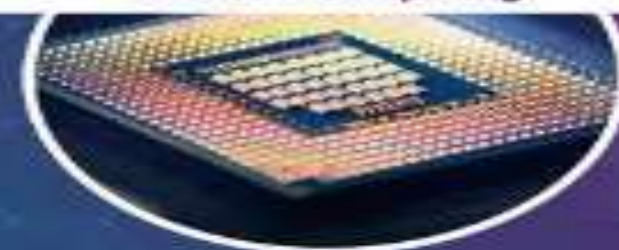
Quantum Sensor-based Wafer Defect Detection



Quantum Communication-based Industrial Confidentiality Protection



Optimized Productivity based on Quantum Computing



Quantum Communication-based Industrial Confidentiality Protection

Quantum Sensor-based Packaging and Ultrafine Defect Detection



Quantum Sensor-based Ultrafine Semiconductor Processing/Diagnosis



Quantum 1-2

Autonomous Driving and Route Optimization for Vehicles

Quantum Compass based GPS-Independent Navigation System

Autonomous Driving based on Quantum LiDAR and Quantum Optical Sensors

Quantum Communication based Synchronization, Positioning, and Navigation Information Transmission and Reception

Generation of Ultra-Precise Positioning, Navigation, and Timing Information based on Quantum Sensors (Atomic Clocks)

Quantum Communication based Satellite PNT Information Reception

Quantum Computer based Route Optimization



Quantum 2-1

Safe Daily Life



Quantum 2-2

Strong Military Force and National Security





Quantum 3-1

Overcoming Incurable Diseases and Developing New Drugs

New Drug Market Authorization

- Ultra-fast, large-scale clinical data analysis using quantum computers
- Medical information protection using quantum communication

Discovery of New Drug Candidates

- Discovery and design of drug candidates using quantum simulation
- Characterization of drug candidate properties using quantum sensors
- Drug discovery and medical information protection through quantum internet-based distributed quantum computing

Preclinical Trials and Animal Testing

- Innovative formulation design using quantum simulation
- Ultra-precise fundamental safety and efficacy validation using quantum sensors

Clinical Trials (phase 1-3)

- High-precision stability check, including body dynamics and side effects, of candidate drugs using quantum sensors
- Exploration of efficacy effects for expected indications using quantum sensor



Quantum 3-2

Precise Diagnosis, Treatment and High-Quality Medical Services

Infant Cardiac Disease Screening using Quantum Sensor Technology

Discovery of Brain Function Mechanisms and Diseases using Quantum Sensor Technology

Human Body Diagnosis through the Development of Digital Biomarkers using Quantum Sensor Technology

Medical Information Protection using Quantum Communication

Microscopic Cancer Detection Using Quantum MRI

Treatment Method Simulation using Quantum Computing

Gracias

MSc. Ing. Carlos del Porto Blanco
Profesor Auxiliar, ISRI

www.facebook.com/CarlosdelPortoBlanco

Telegram: @CarlosdelPorto

Bluesky: @delportocarlos.bsky.social