tendencias criptograficas

SEGURIDAD CUÁNTICA

En 2019, Google afirmó haber alcanzado la supremacía cuántica con su computadora cuántica Sycamore, un dispositivo con 54 qubits, de los cuales 53 estaban operativos. Sycamore resolvió en solo 200 segundos un problema matemático diseñado para demostrar la ventaja cuántica, consistente en muestrear las salidas de un circuito cuántico aleatorio. Según los cálculos de Google, esta misma tarea le habría tomado a Summit, la supercomputadora más rápida del mundo en ese momento, unos 10,000 años.

El término "supremacía cuántica" se refiere al momento en que una computadora cuántica supera significativamente a las computadoras clásicas en una tarea específica. Sin embargo, este avance fue objeto de debate: IBM, uno de los líderes en computación cuántica, cuestionó la afirmación de Google, argumentando que con un enfoque optimizado, Summit podría haber realizado la tarea en 2.5 días, no en miles de años.

A pesar de las disputas, el experimento de Sycamore marcó un hito histórico, ya que mostró cómo los sistemas cuánticos pueden realizar ciertos cálculos exponencialmente más rápidos que las máquinas clásicas. Aunque el problema resuelto no tiene aplicaciones prácticas inmediatas, este logro acercó a la computación cuántica al desarrollo de algoritmos útiles para áreas como la química, la inteligencia artificial y la criptografía, y planteó nuevos retos en seguridad, dado que muchos sistemas criptográficos actuales podrían ser vulnerables frente a algoritmos cuánticos avanzados.

Este evento también reforzó la carrera global por liderar la computación cuántica, con empresas como IBM, Google y Microsoft, junto con naciones como China, invirtiendo significativamente en este campo emergente.