Computación Cuántica

Marco Marcillo

2024-12-16

Outline

Proceso de fabricación de procesadores/ Parte 1

Es un proceso muy complejo, es el cerebro del computador ya que controla las funciones de este.

1. Se comienza con un buen buguiado de arena, compuesto de silicio dónde se hace un mono cristal de 20*150cm seguido se funde el material con 1370° selcios.
2. Se corta el cristal en los extremos en la superficie exterior, y con una sierra eléctrica se corta de menos de un milímetro de espesor para obtener los woofer hasta llegar a un cilindro perfecto
3. Las obleas se pulen hasta que estén planas, para limpiar hasta las imperfecciones
4. Proceso de dibujado de los transistores (impresión)de sucesivas máscaras, que conforman a cada microprocesador.
5. Cada capaz que se pintan sobre los woofer, preparación para que reciban átomos como aluminio o cobre.

Proceso de fabricación de procesadores/ Parte 2

1. Se produce una longitud de onda mediante máscaras. 380-780 nanómetros.
2. Se cortan los woofer y se controla su calidad e integridad es un proceso automatizado. Y se individualizan los chips.
3. Este proceso se realizan en ambientes limpios. Con sistemas de ventilación ya que cualquier mínima particular puede dañar el proceso.
4. Se dotan de cápsulas protectoras plásticas a las placas. Conectados a los pines metálicos con pines de oro.
5. El proceso de escrito dura 2-3 meses, de cada cristal de silicio se obtiene decenas de miles de procesadores de Dónde la inversión fue arena Y la construcción de la planta

¿Por qué los computadores cuánticos son más poderosos que los computadores clásicos y qué medidas de rendimiento se estima que tienen?

Los computadores cuánticos a diferencia que los computadores clasicos, es que la unidad minima de información son los cubits los cuales,mientras que el ordenador clasico esta compuesto por una serie de bits, esto en si es lo mas importante ya que mientras el ordenador clasico contiene un estado en concreto de tamaño n compuestos con 0 y 1. Por otro lado en el ordenador cuantico este estado en concreto llega a ser una combinación de todas las posibles combinaciones con varios coeficientes de n,1 y 0. Tambien se sabe que los computadores cuánticos son mas potentes en teoria que los computadores clásicos.
El redimiento que estos computadores cuánticos tiene un tamaño de 2^n, lo cual son numerosos procesos/operaciones ya que crece de forma exponencial

¿A qué temperatura trabaja un computador cuántico?

Los computadores cuánticos trabajan en temperaturas muy bajas, más especificamente en [0 Kelvin o -273,15 °C]. Esto para poder reservar la coherencia cuántica, una propiedad fundamental de los qubits.
??

¿Qué compuertas lógicas existen en computación cuántica?/ Parte 1

Por el momento existen muchas puertas logicas y se siguen actualizando. Presentamos algunas de ellas:
-Pauli Es un conjunto de tres compuertas (X, Y, Z) que realizan transformaciones básicas en qubits:
• Pauli-X: Invierte el estado del qubit ($0\rangle 1\rangle 0\rangle 1\rangle$), similar a un NOT clásico.
• Pauli-Y: Rota el estado en el plano xy y agrega una fase compleja.
• Pauli-Z: Cambia la fase del estado $1\rangle 1\rangle$, reflejando el qubit en el eje z.
-Hadamard Genera superposición al convertir un estado base $0\rangle 0\rangle$ o $1\rangle 1\rangle$ en una combinación igual de ambos estados ($0\rangle + 1\rangle 0\rangle + 1\rangle$ o $0\rangle 1\rangle 0\rangle 1\rangle$). Es esencial para los algoritmos cuánticos porque permite explorar múltiples estados simultáneamente.

¿Qué compuertas lógicas existen en computación cuántica? /Parte 2

-CNOT Compuerta de dos qubits: si el qubit de control está en $1\rangle 1\rangle$, invierte (aplica NOT) al qubit objetivo. Se utiliza para generar entrelazamiento entre qubits.
-Toffoli Compuerta de tres qubits: si ambos qubits de control están en $1\rangle 1\rangle$, invierte (aplica NOT) al qubit objetivo. Es universal para la computación reversible, ya que puede simular cualquier circuito clásico.
Encadenando estas compuertas en un algortimo nos lleva a una solución al problema que se planteo.

¿Por qué un computador cuántico podría implicar el fin del block chain?

Un computador cuántico podría amenazar la seguridad del blockchain debido a su capacidad para resolver problemas matemáticos complejos que sustentan los algoritmos criptográficos en los que se basa. La seguridad del blockchain depende principalmente de dos tipos de algoritmos criptográficos:

- Funciones Hash (SHA-256): Utilizadas para la minería y la integridad de los bloques.
- Criptografía Asimétrica (como ECDSA): Protege las claves públicas y privadas que se utilizan para las firmas digitales en las transacciones.
- Puede reducir el tiempo necesario para encontrar colisiones en las funciones hash. Aunque no las rompe por completo, reduce significativamente la seguridad de funciones como SHA-256.