Computadoras cuantias

Luis Enrique Perez Señalin

<2024-06-19 mié>

Outline

Pregunta 1

¿Por qué los computadores cuánticos son más poderosos que los computadores clásicos y qué medidas de rendimiento se estima que tienen? Es gracias a su capacidad para aprovechar los principios de la mecánica cuántica, como la superposición y el entrelazamiento. En un computador clásico, la unidad básica de información es el bit, que puede ser 0 o 1. En un computador cuántico, la unidad básica es el qubit, que puede estar en una superposición de 0 y 1 al mismo tiempo. Esto permite que un computador cuántico realice muchas más operaciones en paralelo comparado con un computador clásico.

Pregunta 1 - 2

Las medidas de rendimiento de los computadores cuánticos se evalúan a través de varias métricas:
Número de qubits: Indica la cantidad de qubits que tiene el sistema.
Tiempo de coherencia: El tiempo durante el cual los qubits mantienen su estado cuántico. Fidelidad de las puertas cuánticas: Mide la precisión con la que se pueden realizar operaciones cuánticas. Quantum Volume (Volumen Cuántico): Una métrica compuesta que considera tanto el número de qubits como la fidelidad de las operaciones y la conectividad entre los qubits.

Pregunta 2

¿A qué temperatura trabaja un computador cuántico?
A temperaturas bajas, cercanas al cero absoluto (0 Kelvin, que es -273.15 grados Celsius). Esto se hace para reducir el ruido térmico y otros tipos de interferencia que pueden desestabilizar los estados cuánticos de los qubits. En la práctica, los sistemas de computación cuántica como los de IBM y Google suelen operar a temperaturas alrededor de 10-15 milikelvin, usando refrigeradores de dilución.

Pregunta 3

¿Qué compuertas lógicas existen en computación cuántica?
Las compuertas lógicas manipulan qubits y son análogas a las compuertas lógicas en computación clásica, pero más variadas y complejas debido a las propiedades cuánticas. Algunas de las compuertas cuánticas más comunes son:
Puerta Hadamard (H): Crea una superposición de estados. Puerta Pauli-X (X): Equivalente a la compuerta NOT clásica, invierte el estado de un qubit.

Pregunta 3 - 2

Puerta Pauli-Y (Y) y Pauli-Z (Z): Operaciones de rotación sobre los ejes Y y Z de la esfera de Bloch.
Puerta de Control-NOT (CNOT): Realiza una operación NOT en el segundo qubit solo si el primer qubit es 1.
Puerta Toffoli (CCNOT): Es una puerta de tres qubits que actúa como una AND controlada.
Puerta de fase (S y T): Aplican rotaciones específicas alrededor del eje Z de la esfera de Bloch.

Pregunta 4

¿Por qué un computador cuántico podría implicar el fin del blockchain?
Debedido a su capacidad para resolver problemas matemáticos complejos mucho más rápido que los computadores clásicos.
La seguridad del blockchain se basa en algoritmos criptográficos como RSA y ECC, que son seguros porque los computadores clásicos no pueden factorizar números grandes o resolver el problema del logaritmo discreto en un tiempo razonable. Sin embargo, un computador cuántico suficientemente poderoso, utilizando algoritmos como el algoritmo de Shor, podría romper estos esquemas criptográficos al factorizar grandes números en un tiempo factible, comprometiendo así la seguridad de las transacciones en blockchain y otras aplicaciones que dependen de la criptografía asimétrica.