

Criptografía y Blockchain


Módulo 4

Computación cuántica

Introducción

La **computación cuántica** es una tecnología que emerge rápidamente y aprovecha las **leyes de la mecánica cuántica para resolver problemas demasiado complejos** para las computadoras clásicas.

Hoy en día, empresas como IBM ponen a disposición de los desarrolladores *hardware* cuántico real, con procesadores cuánticos superconductores cada vez más potentes.



Las **supercomputadoras** son computadoras clásicas muy grandes, a menudo con **miles de núcleos clásicos de CPU y GPU** capaces de ejecutar cálculos muy grandes e inteligencia artificial avanzada.

Los **problemas complejos** son problemas con muchas variables que interactúan de maneras complicadas. Modelar el comportamiento de átomos individuales en una molécula, identificar patrones sutiles de fraude en transacciones financieras o la nueva física en un supercolisionador son problemas complejos.

Computación clásica vs. cuántica

Supongamos que algunos científicos quieren saber cómo se comportará una molécula, entonces la sintetizan y experimentan con ella en el mundo real. Si quieren saber cómo un ligero ajuste afectaría su comportamiento, generalmente necesitan sintetizar la nueva versión y ejecutar su experimento nuevamente. Este es un proceso costoso y lento.

Una **supercomputadora clásica** podría intentar simular el comportamiento molecular con fuerza bruta, aprovechando sus muchos procesadores para explorar todas las formas posibles en que cada parte de la molécula podría comportarse.

A medida que avanza más allá de las moléculas más simples y directas disponibles, la supercomputadora se detiene. Ninguna computadora tiene la memoria de trabajo para manejar todas las posibles permutaciones del comportamiento molecular utilizando métodos conocidos.

Los **algoritmos cuánticos** adoptan un nuevo enfoque para este tipo de problemas complejos: crear espacios computacionales multidimensionales. Esto resulta ser una forma mucho más eficiente de resolver problemas complejos.

Fundamentos

Qubits

Los **qubits** (*quantum bits*) son los **equivalentes cuánticos de los bits digitales clásicos**. La implementación física de estos qubits deben ser algunas propiedades de objetos físicos a nivel subatómico, por ejemplo, una unión Josephson.

A diferencia de los bits clásicos, cuyos estados posibles son 0 y 1, los qubits se encuentran en un **estado de superposición**, es decir, como combinación de 0 y 1. Para modificar el estado de los qubits, debemos utilizar principios de la mecánica cuántica.

Al finalizar las operaciones computacionales, podremos medir el estado de los qubits proyectándolos sobre bits digitales clásicos. Los qubits son **probabilísticos**, y pierden su valor al ser medidos.

Un problema inherente de los qubits es su **decoherencia**: con el tiempo, pierden su información debido a la interacción con su entorno. Otros problemas importantes son la **escalabilidad** y la **corrección cuántica de errores**.

Máquina de Turing cuántica

Una **máquina de Turing cuántica** o **computadora cuántica universal** es una máquina abstracta utilizada para modelar teóricamente el funcionamiento de una computadora cuántica.

La **supremacía cuántica** es la capacidad potencial que una computadora cuántica posee (y una computadora clásica no) para resolver determinados problemas.



NISQ (*Noisy Intermediate Scale Quantum*)

En la actualidad, nos encontramos en la era de las tecnologías cuánticas de escala intermedia ruidosa. El término NISQ se refiere al estado actual de la tecnología de fabricación de procesadores cuánticos, que les impiden alcanzar la supremacía cuántica. La escala intermedia se refiere a la cantidad de qubits, **ruidosa** significa que el “ruido” ambiental afecta su coherencia.

Una computadora cuántica completa y altamente escalable no se ha realizado. Sin embargo, se están construyendo computadoras cuánticas más pequeñas, principalmente para demostrar en forma limitada algunas de las capacidades de la computación cuántica.

Criterios de DiVincenzo

En 2000, David DiVincenzo creó una lista de **criterios para la tecnología de computadoras cuánticas** y sus modelos de comunicación:

- Una computadora cuántica debe consistir de **bits cuánticos bien identificados**, y debe ser un sistema físico escalable.
- Una computadora cuántica debe **configurar el estado inicial de los bits cuánticos**. Esto es similar al botón de *Reset* de una computadora de escritorio.
- Una computadora cuántica debe poseer tiempos de **decoherencia prolongados**.
- Una computadora cuántica debe basarse en un conjunto de **puertas cuánticas universales**.
- Una computadora cuántica debe tener una **característica medible** relacionada al estado de los bits cuánticos.
- Una computadora cuántica debe tener la capacidad de **intercambiar los bits** cuánticos dinámicos y estáticos.
- Una computadora cuántica debe tener la capacidad **transmitir bits** cuánticos a grandes distancias.

Computadoras cuánticas comerciales

Las computadoras cuánticas comerciales disponibles pertenecen a Rigetti, Google, IBM y Microsoft.

Rigetti

Las computadoras de Rigetti poseen los siguientes componentes: Quil, PyQuil, QUILC, QVM (*Quantum Virtual Machine*).

Google

Google Quantum Computing Playground tiene soporte de scripting, IDE basado en navegador, registros cuánticos de 22 bits, programas y compilación, lógica, modelado de compuertas cuánticas, soporte de funciones matemáticas y modos de visualización.

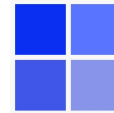


IBM

IBM Quantum Experience consiste en los módulos de composición de circuitos cuánticos, visualizador de circuitos cuánticos, soporte para compuertas cuánticas, registros cuánticos y Notebooks Qiskit basadas en Jupyter.

Microsoft

Microsoft Quantum Development Kit soporta Microsoft Q# y QDK. Posee un simulador y IA open source para que los desarrolladores creen programas usando circuitos cuánticos, compuertas y simuladores.



Computadoras cuánticas de IBM

Un **procesador cuántico** de IBM es de tamaño similar al que se encuentra en una computadora portátil.

Un **sistema de *hardware* cuántico** es de tamaño similar a un automóvil, compuesto principalmente por sistemas de enfriamiento para mantener el procesador superconductor a su temperatura operativa, una centésima de grado por encima del cero absoluto, para evitar la decoherencia.

A estas temperaturas, ciertos materiales exhiben un importante efecto mecánico cuántico: los electrones se mueven a través de ellos sin resistencia. Esto los convierte en superconductores.

Cuando los electrones pasan a través de los superconductores, coinciden, formando **pares de Cooper**. Estos pares pueden llevar una carga a través de barreras, o aislantes, a través de un proceso conocido como **túnel cuántico**. Dos superconductores colocados a cada lado de un aislante forman una **unión Josephson**.

Las computadoras cuánticas usan uniones *Josephson* como qubits superconductores. Al disparar fotones a estos qubits, se puede controlar su comportamiento y hacer que sostengan, cambien y lean unidades individuales de información cuántica.

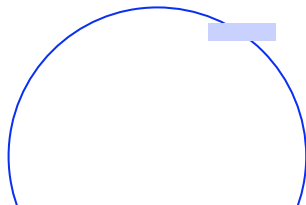
El **entrelazamiento cuántico** es un efecto que correlaciona el comportamiento de dos objetos cuánticos separados. Los físicos han descubierto que cuando dos qubits están entrelazados, los cambios en un qubit afectan directamente al otro.

En un entorno de **qubits entrelazados** colocados en un estado de superposición, hay **ondas de probabilidades**. Estas son las probabilidades de los resultados de una medición del sistema. Estas ondas pueden interferir entre sí.

Un **cálculo** en una computadora cuántica funciona preparando una superposición de todos los estados computacionales posibles.

Un **circuito cuántico**, preparado por el usuario, **utiliza la interferencia** en forma selectiva sobre los componentes de la superposición de acuerdo con un algoritmo.

Muchos resultados posibles se cancelan a través de la interferencia, mientras que otros se amplifican. **Los resultados amplificados son las soluciones al cálculo.**



IBM Quantum System One

IBM Q System One es la primera computadora cuántica para uso comercial, de negocios e investigación, y ha sido creada por la empresa IBM.

Se presentó en público el martes 8 de enero de **2019**.



Cálculo general

Un cálculo general en una computadora cuántica consiste en una **superposición de todos los estados de cálculo posibles**. Esto se utiliza como una entrada a un circuito cuántico que interfiere selectivamente los componentes de la superposición de acuerdo con un algoritmo prescrito. Lo que queda después de cancelar las amplitudes y fases relativas del estado de entrada es la solución al cálculo realizado por el circuito cuántico.



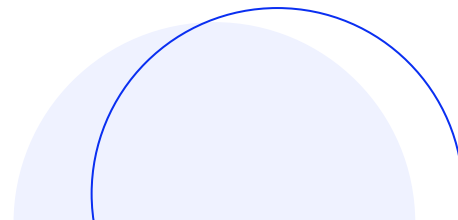
Qiskit

Qiskit es un **SDK** (*Kit de Desarrollo de Software*) de IBM para realizar **cálculos cuánticos que utilizan los principios de entrelazamiento e interferencia mediante circuitos cuánticos**.

Los circuitos cuánticos están formados por compuertas cuánticas, instrucciones y lógica de control clásica. Los circuitos cuánticos permiten expresar algoritmos y aplicaciones complejas de una manera abstracta que se puede ejecutar en una computadora cuántica.

Qiskit es un motor de construcción, optimización y ejecución de circuitos cuánticos.

Las capas adicionales de algoritmos y aplicaciones aprovechan los circuitos cuánticos, a menudo junto a recursos informáticos clásicos, para resolver problemas de optimización, química cuántica, física, aprendizaje automático y finanzas.



Un **flujo de trabajo típico** de un algoritmo cuántico consiste en:

1

El **problema** que queremos resolver.

2

Un **algoritmo clásico** que genera una descripción de un circuito cuántico.

3

El **circuito cuántico** que necesita ejecutarse en hardware cuántico.

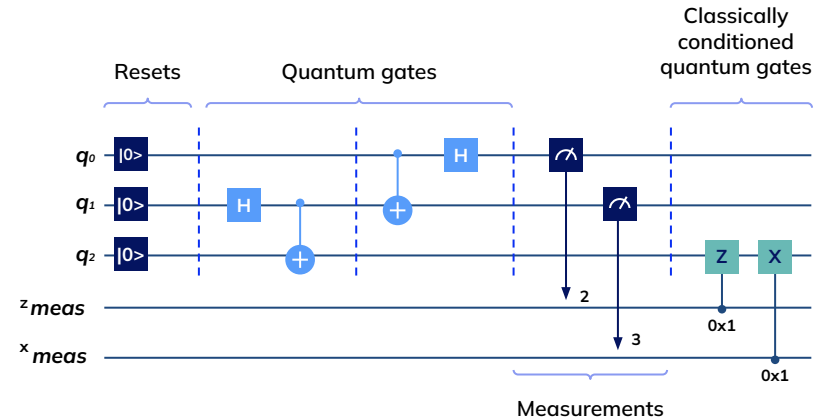
4

La **salida** (clásica) que es la solución.

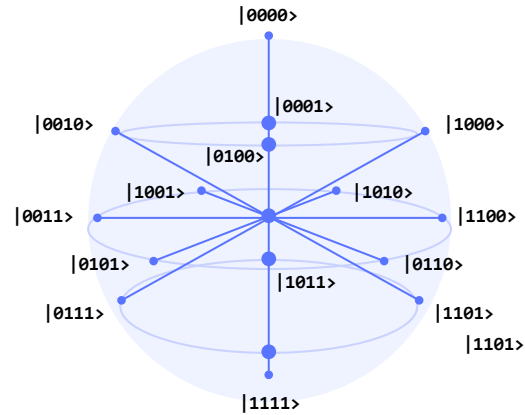
Circuito cuántico

Un circuito cuántico es una **rutina computacional que consiste en operaciones cuánticas coherentes sobre datos cuánticos**, como los que se mantienen en qubits, y computación clásica concurrente en tiempo real. Cada línea horizontal, o cable en un circuito representa un qubit, siendo el extremo izquierdo del cable los datos cuánticos iniciales, y el derecho los datos cuánticos finales generados por el cálculo del circuito cuántico. Las operaciones en qubits se pueden colocar en estos cables y están representadas por cajas.

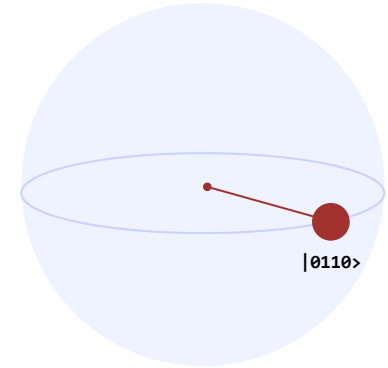
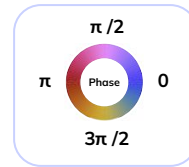
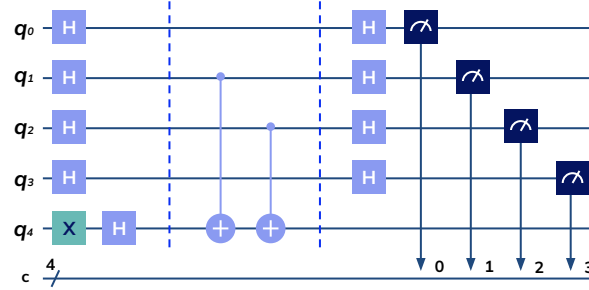
Ejemplo de un circuito de teletransportación de un estado cuántico:



Circuito cuántico



Superposición de todas
las posibilidades



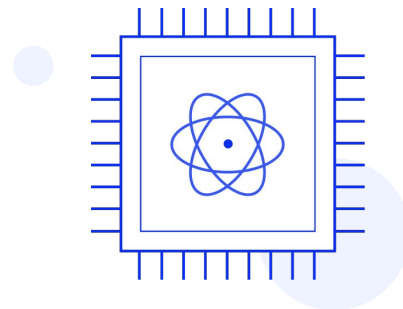
Solución

Qiskit Runtime

Qiskit Runtime es un **servicio de computación cuántica** basado en la nube desarrollado por **IBM**.

Ofrece **primitivas computacionales** para realizar tareas fundamentales de computación cuántica que utilizan técnicas integradas de supresión y mitigación de errores.

Las primitivas se pueden ejecutar dentro de las sesiones, de modo que las colecciones de circuitos pueden ejecutarse conjuntamente en una computadora cuántica sin ser interrumpidas por los trabajos de otros usuarios.



Cuando se utiliza Qiskit, un **flujo de trabajo de usuario** consiste de cuatro pasos de **alto nivel**:

1. Construir

Diseñar un circuito cuántico que represente el problema que está considerando.

1. Compilar

Compilar circuitos para un servicio cuántico específico, por ejemplo, un sistema cuántico o un simulador clásico.

3. Ejecutar:

Ejecutar los circuitos compilados en los servicios cuánticos especificados. Estos servicios pueden estar basados en la nube o ser locales.

3. Analizar

Calcular estadísticas de resumen y visualizar los resultados de los experimentos.

**¡Sigamos
trabajando!**