

ANÁLISIS EN COMPUTADORAS CUÁNTICAS HACIA LA IMPLEMENTACIÓN EN UNIVERSIDADES DE MÉXICO

Paola Murillo Martínez¹, Mónica del Carmen Olivarría González², Rosa Leticia Ibarra Martínez³, José Nicolás Zaragoza González⁴, Sandra Olivia Quirozco⁵

^{1,2,3,4,5}*Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa (México)*

RESUMEN

Con la creciente evolución de la tecnología se han implementado diferentes tipos de velocidades de procesamiento para que la utilización de las computadoras sea más satisfactoria para los usuarios, y por otro lado las anteriores computadoras clásicas mantienen un ritmo bajo en su utilización por parámetros de expansión, debido a la limitación de memoria de estas mismas. La computación llamada cuántica estudia el fenómeno de la mecánica en tunelización, rendimiento, superposición y la necesidad de resolver problemas que no son realizados por una simple máquina.

Palabras clave: Qubit, criptografía.

INTRODUCCIÓN

La computación cuántica es un nuevo paradigma que explota los principios básicos de la mecánica cuántica, como el enredo y la superposición, lo que potencialmente permite aceleraciones sin precedentes en la resolución de problemas intratables. Las nuevas oportunidades de computación incluyen factorización prima, simulaciones cuánticas para la síntesis de medicamentos y materiales, y optimizaciones complejas. Teóricos tales como Richard Feynmann, del California Institute of Technology, de Pasadena (California); Paul Benioff, de Argonne National Laboratory, en Illinois; David Deutsch, de la Universidad de Oxford, en Inglaterra, y Charles Bennett, del T.J. Watson Research Center de IBM, propusieron por primera vez el concepto de las computadoras cuánticas en las décadas de 1970 y 1980, muchos científicos dudaron que alguna vez ese tipo de computadora pudiera resultar práctica.

Pero en 1994, Peter Shor, de AT and T Research, describió un algoritmo cuántico específicamente diseñado para factorizar números grandes y exponencialmente más rápido que las computadoras convencionales, lo suficientemente rápido como para burlar la seguridad de muchos criptosistemas de clave pública.

El potencial del algoritmo de Shor alentó a muchos científicos a tratar de explotar las capacidades de las computadoras cuánticas. En los últimos años, varios grupos de investigación de todo el mundo han alcanzado progresos significativos en este campo. Mientras estuvo en IBM, Chuang amplió su reputación como uno de los experimentalistas en computación cuántica más importantes del mundo.

Dirigió el grupo que demostró la primera computadora cuántica de 1 qubit en 1998 en la Universidad de California en Berkeley. En IBM Almaden, Chuang y sus colegas fueron los primeros en demostrar los importantes algoritmos cuánticos, el algoritmo de Grover concebido en 1999 para hacer búsquedas en bases de datos con ayuda de una computadora cuántica de 3 qubits, y la búsqueda de pedidos ideada el pasado agosto del año 2000 con una computadora cuántica de 5 qubits.

La factorización con el algoritmo de Shor es el algoritmo más complejo que se haya demostrado hasta ahora usando una computadora cuántica.

Además de su ambicioso programa experimental, la División de Investigación de IBM Research es conocida también por sus muchas contribuciones teóricas en el emergente campo de la información cuántica. Los científicos de IBM fueron pioneros en criptografía cuántica, en comunicaciones cuánticas incluso el concepto de teleporte cuántico y en metodologías eficientes para corregir errores.

David, miembro del cuerpo de investigadores del laboratorio Watson de IBM, ha promulgado los cinco criterios necesarios para construir una computadora cuántica práctica, primero un sistema físico de escala flexible con qubits bien caracterizados, capacidad de inicializar el estado de un qubit, tiempos de descoherencia más largos que el tiempo de operación de la puerta cuántica, un conjunto universal de puertas cuánticas, y la capacidad de medir qubits específicos.

La computación cuántica está basada en las interacciones del mundo atómico, y tiene elementos como el bit cuántico, las compuertas cuánticas, los estados

confusos, la tele transportación cuántica, el paralelismo cuántico, y la criptografía cuántica.

Una arquitectura cuántica, muy aceptada entre los investigadores y orientada a ser compatible con las actuales arquitecturas, cuenta con memoria y una unidad de procesamiento aritmético lógico, y con elementos cuánticos como la tele transportadora de código y el planificador dinámico. Su avance teórico ha sido muy exitoso, aun así, su realización depende de la futura implementación de una computadora cuántica, sin embargo, ya se está desarrollando tecnología comercial basada en esta teoría.

IBM, en los años 2000, dirigido por Isaac Chuang, creó una computadora cuántica de 5-Qbit capaz de ejecutar un algoritmo de búsqueda de orden, que forma parte del Algoritmo de Shor. Este algoritmo se ejecutaba en un simple paso cuando en una computadora tradicional requeriría de numerosas iteraciones. Ese mismo año, científicos de Los Álamos National Laboratory anunciaron el desarrollo de una computadora cuántica de 7-Qbit. Utilizando un resonador magnético nuclear se consiguen aplicar pulsos electromagnéticos y permite emular la codificación en bits de las computadoras tradicionales.

El equipo de investigadores estadounidense dirigido por el profesor Robert Schoelkopf, de la universidad de Yale, que ya en 2007 había desarrollado el Bus cuántico, crea ahora el primer procesador cuántico de estado sólido, mecanismo que se asemeja y funciona de forma similar a un microprocesador convencional, aunque con la capacidad de realizar sólo unas pocas tareas muy simples, como operaciones aritméticas o búsquedas de datos. Para la comunicación en el dispositivo, esta se realiza mediante fotones que se desplazan sobre el bus cuántico, circuito electrónico que almacena y mide fotones de microondas, aumentando el tamaño de un átomo artificialmente.

La primera computadora cuántica comercial es fabricada por la empresa D-Wave Systems fundada en 1999. Una máquina cuántica puede resolver algunos problemas complejos que son insolubles incluso para las computadoras clásicas más poderosas. Al explotar la superposición cuántica y los fenómenos de enredo,

los algoritmos cuánticos pueden lograr desde el polinomio hasta la aceleración exponencial cuando se comparan con sus mejores contrapartes clásicas. Una computadora cuántica formará parte de una computadora heterogénea de varios núcleos en la que un procesador clásico interactuará con varios aceleradores, como FPGA, GPU y también un coprocesador cuántico.

La comunidad científica dedicada a investigar tópicos en el ámbito de la computación cuántica, ha logrado enormes avances teóricos, al demostrar que es posible reducir drásticamente los recursos computacionales requeridos en la ejecución de algoritmos. Algunos de esos algoritmos requieren un inmenso poder de cómputo aún en las computadoras más avanzadas de la actualidad. Algunos algoritmos matemáticos como la búsqueda de los factores de números primos, algoritmos de manejo de información como la búsqueda en bases de datos no ordenadas han sido teóricamente desarrollados con mucho éxito, utilizando los fundamentos de la computación cuántica.

ACERCA DE COMPUTACIÓN CUÁNTICA

En su realización fundamental, una computadora cuántica comprende un procesador cuántico y un controlador electrónico clásico. El procesador cuántico consiste en un conjunto de bits cuánticos qubits que operan a temperaturas extremadamente bajas, típicamente unas pocas decenas, mientras que el controlador electrónico clásico se usa para leer y controlar el procesador cuántico. Aunque el controlador clásico se implementa hoy en día con instrumentos de laboratorio a temperatura ambiente, este enfoque se vuelve cada vez más desafiante y menos rentable a medida que el número de qubits crece hacia los miles y millones, como lo requieren los algoritmos cuánticos prácticos.

La computadora cuántica con la que cuentan Google y NASA es la famosa “D-WAVE 2”. Esta máquina les permite realizar trabajos de investigación y desarrollo de manera rápida, especialmente en los trabajos de inteligencia artificial que vienen desarrollando, sobre todo Google.

Además, Google ya ha comenzado a realizar pruebas para hacer de su navegador Chrome lo suficientemente seguro ante las posibles amenazas que la computación

cuántica traiga consigo, debido a que las propiedades y capacidades de la computación cuántica para el procesamiento de información son tan grandes que los protocolos y sistemas de seguridad que actualmente se emplean en la red se verían seriamente comprometidos si no se realizan modificaciones.

Incluso IBM acaba de poner a disposición su computadora cuántica a cualquier persona mediante Internet. Este ordenador se encuentra en su laboratorio de YorkTown Heights, New York. Será posible utilizarlo desde cualquier computadora y en cualquier parte del mundo mediante un software que se podrá descargar.

Así, IBM pone en marcha una iniciativa por la cual cualquier científico, investigador o programador puede encontrar errores y proponer mejoras, además de tener la oportunidad de trabajar con una máquina súper poderosa que resolvería problemas que para una computadora ordinaria tomaría más tiempo.

Justificación

Una computadora cuántica está basada por medio de qubits, ya que por otro lado las computadoras convencionales contienen bits. Estas pueden ser utilizadas de una buena manera al igual que darles un mal uso, uno de los casos más interesantes en la actualidad es sobre el tema de las criptomonedas, ya que obteniendo una de las maquinas o computadoras cuánticas facilita el robo de dinero electrónico y hace a un lado el manejo de la tecnología Blockchain. Esto sin duda es un tema muy relevante, ya que estas máquinas también están evolucionando al borde de la tecnología debido que muchos usuarios están interesados, debido a que la mayor parte de su audiencia es por lo general universitarios. Está desarrollado por IBM para la implementación para estudiantes u otras necesidades por fuera de universidades, es un tema muy interesante para cualquier persona de cualquier edad, ya sea adolescentes o adultos. Pero por otro lado uno de los problemas a que se enfrentan este tipo de computadoras cuánticas es con no encontrar un hardware adecuado para las diferentes condiciones en que las utilice el usuario y esto hace estar esperando una solución. Se realiza esta investigación para conocer más sobre estas computadoras cuánticas en la utilización y explicación de la importancia que

tienen en la actualidad en el mercado que pueden llegar ser las mejores para los estudiantes universitarios siendo una herramienta fundamental.

2.2 Objetivos Generales y Específicos

2.2.1 Objetivo General

Comprender los modelos que se encuentran hacia la evolución de las computadoras cuánticas con base en los estudiantes y llegar a todas las universidades para forzar el aprendizaje en sus fundamentos informáticos.

2.2.2 Objetivo Especifico

Analizar por qué las computadoras cuánticas han desarrollado este tipo de interés en grandes empresas de manera oportuna desde su creación en 2007, por primera vez una computadora capaz de ejecutar el temple cuántico, por otro lado, explicar la parte fundamental de la utilización y conocimiento en estudiantes, ya que es una forma completamente distinta de utilizar una computadora convencional y cambiar la mentalidad para crear posibilidades hacia universidades que procesan su interés.

METODOLOGÍA

Debido al gran debate que presentan en la actualidad, las computadoras cuánticas son realmente seguras o hechas para el uso de universitarios, es importante dar a conocer su importancia para el uso práctico al ser una herramienta fundamental para el estudiante universitario contribuir de alguna manera para adoptar esta iniciativa.

Las nuevas tecnologías actualmente están evolucionando conforme hay cambios, pero anteriormente nunca se pensó que las computadoras cuánticas fueran para un uso personal o algún método para algo más grande, sólo era posible el hecho de existir, hasta que llegó el momento de realizar esta tecnología como la llamamos computadoras cuánticas. En nuestros días estas tecnologías funcionan completamente diferente a las computadoras convencionales tal como las conocemos en la actualidad, una de las ventajas de estas mismas es que procesan

millones de veces más rápido que una computadora normal, como codificar información de manera inmediata, una de las empresas que lanzó al mercado la computadora cuántica fue DWave Systems.

Pero no obstante también cuentan con desventajas al utilizarlas y una muy común es su gran elevación de precio, esto conlleva a que pocos de los usuarios puedan obtener este tipo de posibilidad. Por algún aproximado de 10 millones de dólares, ya que contiene un gran potencial de mejoras y su procesamiento, los estudios de la computadora cuántica es considerado la informática cuántica del futuro.

Por otro lado, es importante saber la importancia de estas computadoras y la relación que tienen para las universidades, por esta razón se realizarán métodos de investigación para entender su significado y el uso que se les puede hacer llegar a los estudiantes, ya que se considera una herramienta fundamental para nuevas generaciones y este contribuye con resultados eficientes en estudiantes debido a que será más fácil de operar y dejará atrás máquinas del pasado, y así llegar por medio de técnicas de páginas web, revistas, conferencias del razonamiento de la utilización en universidades.

Para promover esta investigación se utilizarán distintas formas para hacer llegar información necesaria de las computadoras cuánticas, implementar soluciones que se pueden al utilizar estas computadoras y podrían hacer la necesidad de tiempo a futuro tanto para los estudiantes cursando la universidad como también en el campo laboral dentro de la institución. Se realizarán investigaciones más profundas del tema para mantener una actualización de la información relacionada con respecto a las computadoras cuánticas y sus procedimientos que contienen, habrá personas que desconozcan sobre el tema y es cuando entra el método explicativo de hacer entender que es una nueva herramienta de implementación para los estudiantes que cursan la universidad, con la finalidad de contar con más posibilidades y conocimiento de estas computadoras.

La computadora cuántica contiene grandes características y perspectivas para los estudiantes que contribuyen para una mejor educación y aprendizaje en el área de la informática, ya que son los principales en la utilización de esta tecnología tan

avanzada, pero contiene grandes resultados, es por eso que se hará énfasis en la utilización de estas mismas computadoras.

RESULTADOS

Los resultados del estudio de esta investigación se analizarán de las dependencias de universidades si hay interés de implementarlas, por otro lado, se realizarán encuestas sobre el conocimiento de las computadoras cuánticas en la Facultad de Informática Mazatlán de la Universidad Autónoma de Sinaloa, ya que en esta misma facultad se desarrollan campos hacia el rendimiento y capacidad de almacenamiento y esto es una propuesta de gran interés para dicha facultad, así como también la recolección de datos, si los estudiantes la utilizaran como método empleado hacia las tecnologías de la innovación y una vez recolectada la información se analizará para posteriormente relacionarla con otras propuestas de diferentes universidades y con ello lograr el objetivo de que México contribuya a que los estudiantes cuenten con mejores herramientas en el campo informático.

CONCLUSIÓN

Con este documento se tuvo como objetivo comprobar las grandes características con las que cuentan las computadoras cuánticas, si son seguras para los usuarios o solamente es un método más para hacer trabajos relacionados en computadora, anteriormente nunca se determinarían estas tecnologías y mucho menos llamarían la atención de los usuarios por utilizar este método, la mayoría de los usuarios las utilizan generalmente como uso cotidiano, las que conocemos hoy en día, es decir, las computadoras convencionales. Por otra parte, llegar a un éxito por parte del gobierno de México para que tenga la posibilidad de ofrecer nuevas posibilidades de estudio en el área de la informática en universidades de México sería un gran cambio en el país al reconocer nuevas tecnologías.

REFERENCIAS

- [1] B. Patra, R. Incandela, J. Dijk, "Cryo-CMOS Circuits and Systems for Quantum Computing Applications", *Cryogenics, Quantum computing process control*, Volumen 53, no. Issue: 1, pp. 309-321, 2017.
- [2] C.G Almuderver, N. Khammassi, L. Hutn "Towards a scalable quantum computer", *International Conference on Design & Technology of Integrated System in Nanoscale*, en Taormina, Italy 2018.
- [3] Coincrispi. Cómo las computadoras cuánticas pueden poner en riesgo el futuro del Bitcoin, Consultado 11 de diciembre 2018. Obtenido de:
<https://www.coincrispy.com/2017/11/22/computadoras- cuanticas-futuro-bitcoin/>
- [4] Boletín UNAM-DGCS-413. Computadoras cuánticas, futuro de la informática como complemento más poderoso y potente, consultado 11 de diciembre 2018. Obtenido de:
http://www.dgcs.unam.mx/boletin/bdboletin/2018_413.html.
- [5] IBM. Los estudiantes españoles están conociendo la computación cuántica de primera mano, Consultado 12 diciembre 2017. Obtenido de:
<https://www.ibm.com/blogs/think/eses/2017/12/12/estudiantes-y-computacion-cuantica/>.
- [6] Computación cuántica, ventajas, desventajas, límites y futuro, Consultado 1 mayo 2016. Obtenido de :
<http://generacionnuevadecomputacioncuantica.com/2016/05/computacioncuantica-ventajas-desventajas.html>.
- [7] Fundamentos de la computación cuántica, Consultado 12 diciembre 2018. Obtenido de: <http://www1.eafit.edu.co/asr/courses/computacion-cuantica-CB120/index.html>.
- [8] Computación cuántica: que es, de donde viene y que se ha conseguido, Consultado 13 de diciembre 2018. Obtenido de:
<https://www.xataka.com/ordenadores/computacion-cuantica-quees-de-donde-viene-y-que-ha-conseguido>.

- [9] Computación cuántica, Consultado 12 diciembre 2018. Obtenido de:
<https://decode.la/blog/quees-la-computacion-cuantica/>.
- [10] Las promesas de la computación cuántica y un nuevo récord mundial en simulación, Consultado 10 diciembre 2018. Obtenido de:
<https://www.infobae.com/america/tecno/2018/07/29/las-promesas-de-la-computacion-cuanticay-un-nuevo-record-mundial-en-simulacion/>.
- [11] IBM colabora con instituciones académicas para acelerar la computación cuántica, Consultado 10 de diciembre de 2018. Obtenido de:
<https://www.interempresas.net/TIC/Articulos/206540-IBMcolabora-con-instituciones-academicas-para-acelerar-la-computacion-cuantica.html>.