Evidencia 4 – Crónica de la conferencia de Enrique Fernández Borja

Apellidos: Pino Jiménez

Nombre: Pablo

Grupo: Grupo 1|Grupo 2

Comité: Comunicación

Horas totales: 20 minutos

Evidencias:

1. Trabajé durante 20 minutos en la redacción de la crónica acerca de la conferencia de Enrique Fernández Borja.

CONFERENCIA ENRIQUE FERNÁNDEZ BORJA

Esta conferencia ha sido impartida por el doctor Enrique Fernández Borja, licenciado y doctorado en Física Teórica. En esta conferencia se ha dado una visión general de la física cuántica aplicada a la informática.

Para empezar, se han dado los cuatro principios de la física cuántica que son: la discretización de la energía; la superposición, según la cual 2 estados excluyentes según la física clásica no tienen por qué serlo en la física cuántica, como por ejemplo la existencia de una partícula con 2 posiciones y energías distintas de forma simultánea; el colapso, según el cuál el hecho de realizaar mediciones sobre la partícula altera el estado de la misma; y el entrelazamiento cuántico, según es cual las propiedades de los estados de 2 o más partículas están correlacionados.

Clásicamente, los estados posibles de un bit hann sido 0 y 1. En el caso del la física cuántica, el qúbit, se define por la superposición de

los estados 0 y 1, y por ello, el cúbit se puede expresar como la combinación linear de 0 y 1 ($A|0> + B|1>$, siempre y cuando $A^2 + B^2 = 1$). El qúbit es 0 o 1 dependiendo del electrón de la última capa.

Una ventaja de los computadores cuánticos respecto a los clásicos, es que mientras los clásicos tienen n bits por cada unidad de información, los cuánticos tienen 2^n bits por unidad de información, en éste caso sus átomos.

Los computadores cuánticos son más veloces que los computadores clásicos, pero para comprender la importancia de esto se deben de analizar los tipo de problemas existentes según su complejidad:

Los problemas de tipo P son aquellos que se pueden resolver en un tiempo aceptable.

Los problemas de tipo NP son aquellos que se pueden comprobar rápidamente, independientemente de que puedan resolverse en un tiempo aceptable.

Los problemas de tipo NP completos son aquellos que tienen una complejidad demasiado alta como para poder ser resueltos en un tiempo aceptable. Estos problemas en concreto presentan la característica de que si se halla la forma de resolver uno de ellos en un tiempo aceptable (tiempo polinomial), se demuestra que todos los problemas de la clase NP son en realidad problemas de la clase P.

Los problemas de tipo BQP son problemas de tipo NP, que se pueden resolver en tiempo polinomial mediante el uso de ordenadores cuánticos.

Por último, la criptografía cuántica es más segura que la actual debido a que no se pueden copiar los datos, puesto a que para copiarlos hay que leerlos y al leerlos se produce el fenómeno cuántico de colisión, por lo que el mensaje se rompe y queda inservible. Aun así, se pueden obtener las claves de cifrado y el mensaje si hay fallos en la transmisión, o recepción. A esto último se le llama hacking cuántico.