Profesor del Tec CEM colabora en desarrollo de seguridad de blockchain

Salvador Elías Venegas Andraca, profesor investigador en el **departamento de computación** del Tec de Monterrey campus Estado de México, colaboró en el desarrollo de una capa adicional de seguridad al protocolo de blockchain, a efecto de **proteger los protocolos de criptografía de esta tecnología de bloques** contra ataques de computadoras cuánticas**.**

Con la participación del Banco Interamericano de Desarrollo, BID Lab y Cambridge Quantum (CQ), el doctor Venegas Andraca y un equipo de científicos fueron los **primeros** en crear exitosamente este sistema de protección, **basado en tecnología cuántica**, contra vulnerabilidades criptográficas de las cadenas de bloque o **blockchain**.

El doctor Venegas Andraca, **fundador de la Computación Cuántica en México**, comentó que este resultado robustece tanto la estructura actual y futura de blockchain como las aplicaciones que sobre esta tecnología se construyen, por ejemplo la **criptomoneda Bitcoin**.


width="900" loading="lazy">

Amenazas a la ciberseguridad

La tecnología cuántica en la industria de la computación permite mayores avances en la investigación y desarrollo de productos y servicios, pero también mayor facilidad para vulnerar **sistemas de seguridad** que antes eran prácticamente inviolables, como lo es el blockchain.

*“Blockchain es un paradigma tecnológico que va a tener impacto en muchas áreas del quehacer humano en las que hay **intercambio de información** y dicha información necesita ser **almacenada de forma segura.***

*“Cuando haya computadoras cuánticas suficientemente grandes, el empleo del algoritmo de Shor hará que los **protocolos de criptografía** puedan sufrir ataques. En este escenario, la información guardada en blockchain quedaría vulnerable”,* señaló el doctor Venegas Andraca.


width="900" loading="lazy">

Un hito para la industria

LACChain, alianza global liderada por BID Lab para el desarrollo del ecosistema blockchain en América Latina y el Caribe, invitó al doctor Venegas Andraca a desarrollar una propuesta **científico-tecnológica** frente a las amenazas potenciales que la computación cuántica presenta para blockchain.

*“Lo que hicimos fue **construir una capa adicional de tecnología cuántica** para proteger los protocolos de criptografía de blockchain que serían vulnerables ante ataques de computadoras cuánticas que empleasen el algoritmo de Shor”*, explicó.

Una vez desarrollada la propuesta teórica se trabajó en el diseño experimental para validar este nuevo sistema de seguridad, el cual requirió la preparación por parte de un equipo multidisciplinario.

*“Es el **primer resultado conocido** que permite proteger una cadena de blockchain contra ataques de computadoras cuánticas, siendo esta protección el **resultado de la aplicación de tecnología cuántica** como una capa de protección de las blockchain existentes y por existir.*

*“En materia de criptografía, la tecnología cuántica es un toma y daca: por una parte, debilita los protocolos existentes pero, al mismo tiempo, nos da herramientas para **construir nuevos métodos criptográficos**, poderosos y resistentes ”*, destacó.

Este trabajo fue ya presentado a la comunidad científica y empresarial en un artículo científico, mismo que se encuentra en revisión de pares y, desde ya, la industria **puede hacer uso** de este innovador proceso que **marca un hito en el sector informático** para la protección de datos.

width="900" loading="lazy">

Prepararse para el futuro

En el mediano plazo, entre cinco y quince años, se estima que las computadoras cuánticas alcanzarán la **madurez tecnológica**, la competitividad en precios y la penetración de mercado requeridas para **vulnerar sistemas criptográficos avanzados**. El doctor Venegas Andraca comenta que esto conlleva un riesgo:

"Es un problema muy serio, imagínate el horror de saber que, de repente, la aplicación de blockchain que creíamos que era segura resulta no serla y toda la información que está contenida ahí ***queda expuesta****.*

"Pienso en los datos, absolutamente todos los datos que estarían expuestos por ejemplo de las instituciones financieras, eso sería un desastre".

Además de su trabajo académico, el doctor Venegas Andraca también se ha desempeñado como **consultor en computación cuántica** y otras áreas de las tecnologías de la información,

actividades que le permiten reconocer la importancia que las empresas deben tener, desde ahora, en su **preparación contra las amenazas a la ciberseguridad**:

“??El punto es que las organizaciones empresariales y gobiernos tienen que tomar decisiones sobre cómo van a entrenar a su gente o cómo van a incorporar el capital humano para enfrentar los problemas que va a haber en un futuro.

“Ya hay un número nutrido de empresas, por ejemplo en los sectores financiero y farmacéutico, que están contratando especialistas y capacitando matemáticos, científicos e ingenieros en ***tecnología cuántica”****.*

SEGURO QUERRÁS LEER TAMBIÉN: