Los desarrolladores de Solana han diseñado una bóveda resistente a la computación cuántica en la blockchain de Solana para salvaguardar los fondos de los usuarios frente a posibles riesgos derivados de avances en tecnología cuántica.

La herramienta, conocida como *"Solana Winternitz Vault",* utiliza un sistema avanzado de firmas basado en hash que crea nuevas claves cada vez que se realiza una transacción. Así lo explicó Dean Little, investigador en criptografía y científico principal de Zeus Network, en una publicación en GitHub del 3 de enero.

Este método, que genera claves privadas únicas para cada operación, dificulta que las computadoras cuánticas puedan ejecutar ataques dirigidos a claves públicas, las cuales se revelan al momento de firmar una transacción.

La funcionalidad resistente a la computación cuántica no es una mejora de seguridad aplicada a toda la red, sino una característica opcional. Los usuarios deben optar por almacenar sus activos en las bóvedas Winternitz, en lugar de las billeteras estándar de Solana, para obtener protección adicional contra futuras amenazas cuánticas.

Funcionamiento

Primero, la bóveda Winternitz crea un nuevo par de claves Winternitz y calcula la raíz Merkle usando el algoritmo Keccak256 sobre la clave pública.

A continuación, se genera una bóveda «dividida», que consta de una cuenta de transferencia y una de reembolso. El usuario firma un mensaje con una clave Winternitz, especificando la cantidad de "lamports" (la unidad más pequeña de la criptomoneda Solana) que desea transferir.

Cuando la transacción se completa, cualquier saldo restante se transfiere a la cuenta de reembolso, y la bóveda se cierra.

Este desarrollo brinda tranquilidad a los inversores en criptomonedas preocupados por el

riesgo de que computadoras cuánticas puedan comprometer sus activos protegidos por criptografía.

Dean Little, además, hizo una referencia sarcástica al inversor en Bitcoin Fred Krueger al compartir capturas de pantalla de una publicación en X (antes Twitter) del 19 de diciembre, donde Krueger afirmaba que Solana sería la *"primera víctima"* de la computación cuántica.

Por otro lado, la hoja de ruta técnica de Ethereum también incluye soluciones resistentes a la computación cuántica. Sin embargo, uno de sus fundadores, Vitalik Buterin, asegura que no habrá una amenaza significativa por parte de esta tecnología durante, al menos, la próxima década.

> *"Hasta si las computadoras cuánticas 'reales' llegan pronto, podría pasar mucho más tiempo antes de que las personas comunes tengan una en sus laptops o teléfonos. Ese día probablemente estará décadas después de que instituciones poderosas consigan una máquina capaz de romper la criptografía de curvas elípticas",* comentó Buterin en octubre.