El reto de diseñar un metaverso libre de estafas

El desarrollo de este nuevo ecosistema virtual plantea desafíos en materia de protección de la privacidad de los usuarios y de control de sus activos digitales

ÁNGEL G. PERIANES

Pasados apenas unos meses desde el anuncio de su nacimiento, el metaverso se ha convertido ya en el gran protagonista del panorama tecnológico. Pese a que esta red de entornos virtuales no ha hecho más que dar sus primeros pasos, en ese camino aún incierto han surgido ya inquietudes relacionadas con su privacidad y seguridad.

La amplia colección de datos confidenciales que promete albergar este universo en el que se vive, se compra y se vende a través de avatares, sin un método concreto para identificar a los cibercriminales, presenta un gran atractivo para la piratería. La tecnología del *blockchain* es la base de su posible descentralización, ya que elimina intermediarios al realizar una gestión segura de la autentificación o la validación de los procesos. Eso descarta ataques por fuerza bruta, pero, según los expertos, no excluye de la necesidad de poner coto a las tácticas de ingeniería social que pueden desarrollarse.

Así lo asegura Yaiza Rubio, *chief Metaverse officer* de Telefónica: "La exposición en la *Web 3.0* sobre la que se basa el metaverso es más grande que nunca y los cibercriminales tendrán más intención de comprometer a los usuarios con técnicas ya conocidas como el *phising*". Esta estrategia de engaño a través de archivos infectados o enlaces a páginas fraudulentas en el *mail* es ya el principal riesgo en las primeras experiencias con plataformas virtuales para acceder a perfiles ajenos o robar activos digitales.

Sin embargo, la experta apunta que existe otro riesgo igual de importante que atañe a la propiedad intelectual en el mercado de los NFT, llamados a ser el pilar de interacción y transacción de los usuarios en el metaverso. OpenSea, el mercado más popular de estos activos, de momento solo puede verificar las obras *a posteriori*, y eso hace que muchas de las que se han creado con esta herramienta sean falsas o plagiadas, como ha reconocido la plataforma.

Un ejemplo: este año, la firma de lujo Hermès demandó a un creador de NFT por vender copias del diseño de su bolso Birkin. "Ahora mismo, cualquiera puede comercializar algo con una simple foto sin propiedad intelectual, y por eso hay que crear plataformas que la protejan. No se puede delegar todo en el usuario", sostiene Rubio.

DINERO DIGITAL. El mundo de las criptomonedas apunta a ser otro factor clave para la seguridad del metaverso. Según un reciente estudio encargado por Agora, proveedor de API, el 70 % de los desarrolladores considera que el intercambio de estas monedas a través de *blockchain* será clave para dar forma al metaverso.

Durante los últimos años, este mercado se ha disparado y, con él, el interés de los ciberdelincuentes. A ese respecto, Chester Wisniewski, investigador principal de amenazas de Sophos, explica que "la percepción de que las criptomonedas son más seguras debido a la encriptación y a las matemáticas que implican es falsa". De hecho, añade, "su carácter anónimo facilita su robo, y además, la naturaleza irreversible del *blockchain* hace casi imposible arreglar las cosas cuando una transacción es ilegítima".

En opinión de este experto, los millones de dólares robados durante los últimos años (casi 6.800 en 2021, según un análisis de Crypto Head) demuestran que "se trata de un mercado problemático". De hecho, opina que "la forma más segura de guardar criptomonedas es en un monedero *offline*".

Para Eusebio Nieva, director técnico de Check Point Software para España y Portugal, "el riesgo siempre va a ser la gestión de contraseñas". Así, se han multiplicado los timos relacionados incluso con criptomonedas falsas que crean los estafadores para, una vez disparar su valor, huir con las ganancias. Y otro tipo de ciberataques como el *ransomware* (secuestro de billeteras) o minería de criptomonedas introduciendo *software* fraudulento en servidores de usuarios para acceder al dinero de forma masiva.

Por eso, de cara a su uso en el metaverso, Miguel Ángel Fañanás, director de VU Security en Europa, ve necesario dar al usuario "herramientas y entidades para legitimar y verificar las transacciones sin acciones sospechosas". En este sentido, Wisniewski recuerda que la complejidad de criptomonedas como Ethereum, que utilizan "contratos inteligentes [programas que se ejecutan solo cuando ocurre un evento concreto]", no ha impedido "que se produzcan fraudes".

En la misma línea, Rubio opina que "alguien que controle código y tenga malas intenciones puede llegar a ejecutar ciertas operaciones". Y por eso cree que habrá un auge de auditores que certifiquen contratos en el metaverso.

A juicio de Marina Pareja, consultora de Asuntos Públicos de Atrevia, al ritmo que la experiencia del mundo físico se traslade a este entorno virtual irán surgiendo riesgos ya identificados, como el ciberacoso o el ciberespionaje, con "la posibilidad de acceder a una reunión de trabajo virtual con el robo de una identidad digital". Incluso los propios dispositivos "serán una superficie más de ataque" como recopiladores de datos, añade, a medida que su desarrollo madure y el metaverso gane atractivo.