

Esta iniciativa del Instituto Madrileño de Estudios Avanzados IMDEA Software mejora la privacidad en la red

La Comunidad de Madrid crea un protocolo para compras seguras de productos digitales con criptomonedas

- El sistema *MixBuy* evita que se pueda relacionar la tienda y el cliente a partir de transacciones con estas divisas
- Mejora la confidencialidad de los procesos actuales y es compatible con la mayoría de monedas digitales

14 de diciembre de 2024.- La Comunidad de Madrid ha creado un protocolo criptográfico para garantizar la seguridad y la privacidad de compras de productos digitales con criptomonedas. El Instituto Madrileño de Estudios Avanzados IMDEA Software, ha desarrollado el sistema *MixBuy*, que mejora las soluciones actuales para evitar que se pueda relacionar cliente y tienda a partir de transacciones con monedas digitales.

Hoy en día se pueden comprar muchos productos usando criptomonedas. Sin embargo, en la mayoría de los entornos *blockchain*, que son bases de datos compartidas en red que facilitan este tipo de transacciones, los detalles personales a menudo pueden ser vistos por otras personas, ya que el registro es público.

Para evitar estos inconvenientes, los investigadores Diego Castejón Molina, Dimitris Vailopoulos y Pedro Moreno-Sánchez han introducido a un intermediario -una entidad similar a *Bizum*- entre cliente y tienda. Así, este protocolo impide que alguna de las tres partes involucradas en las transacciones pueda apropiarse el dinero de las otras.

El estudio, denominado *MixBuy: Contingent Payment in the Presence of Coin Mixers*, se presentará en la prestigiosa conferencia internacional Privacy Enhancing Technologies Symposium.