

GERENCIA

Tecnologías y estrategias para la transformación digital



Cloud Data Management

FRANQUEO CONVENIDO RES. EXTA. N° 519 FECHA: 18 - 8 - 93 AGENCIA: STGO. 1 / Av. Sucre 2235 Ñuñoa Santiago Chile
Código Postal 7770202 - Fono: 224335500 E-mail: prensa@emb.cl



Reporte de Ciberseguridad de Entel Ocean (pág. 18)



Cómo Blockchain puede cambiar los negocios (pág. 32)

TRANSFORMACIÓN DIGITAL ACELERADA

METODOLOGÍA FINLANDESA PROBADA EN CHILE

HELSINKI | SANTIAGO | DUBAI | VIETNAM

SISUA_DIGITAL

Software Robots from Finland

www.sisuadigital.com

Expertos en Automatización de Procesos

Soluciones RPA para:

- Bajar costos operacionales
- Aumentar la calidad de servicio
- Mejorar el rendimiento del equipo

¡Reserve una consulta gratuita en nuestro sitio web!

¿Qué tan seguras son las billeteras digitales?

Como medio de pago, las billeteras digitales utilizan múltiples elementos de seguridad, en la autenticación, transmisión de los datos y confirmación de las transacciones, que incluye técnicas de criptografía, y modelos basados en Blockchain y en Machine Learning, que otorgan un mayor nivel de seguridad en las transacciones.



El uso de las billeteras digitales ha ido al alza. Uno de los principales beneficios que entregan como método de pago se asocia a la mayor seguridad que ofrecen a los consumidores, respecto a los riesgos asociados al fraude o robo de información, explica Rodrigo López, Académico del Departamento de Control de Gestión y Sistemas de Información de la Facultad de Economía y Negocios de la Universidad de Chile.

Al igual que una billetera física, estas almacenan los datos de identificación del usuario. Sin embargo, la principal diferencia radica es que con ellas solo es posible interactuar con su contenido de manera digital, a través de una aplicación de celular o web.

Al ser digitales, utilizan múltiples elementos de seguridad, tanto en la autenticación de datos, como

utilizar más de una de estas categorías, lo cual se conoce como métodos de autenticación de dos factores o pasos". En la transmisión de los datos, se utilizan técnicas de criptografía, las cuales intentan asegurar que ningún tercero pueda leer, manipular o reemplazar los datos de comunicación entre las entidades participantes en la transacción. "Los datos de las tarjetas financieras se almacenan encriptados, haciendo poco probable sustraerlos o falsificarlos", asegura.

Con el fin de detectar transacciones fraudulentas, las entidades financieras están utilizando modelos de Machine Learning, para la confirmación de las transacciones. "Mediante el análisis y evaluación de datos como la fecha, hora y el lugar desde donde se origina la transacción, el monto y el destino del dinero, entre otros datos, las institu-

ciones pueden identificar transacciones que se alejan del patrón de consumo del usuario, marcarlas como fraudulentas y detenerlas antes de su desarrollo", comenta.

Hacia técnicas más robustas

Debido al rápido desarrollo de la tecnología y la exigencia de aumento de seguridad de la información, el académico argumenta que resulta primordial implementar técnicas que sean cada vez más robustas, para el resguardo de las transacciones.

Es por ello que, en los últimos años, han comenzado a utilizarse modelos basados en la tecnología Blockchain para la seguridad de las transacciones, lo que ha permitido alcanzar mayores niveles de robustez, facilitando la creación de nuevos modelos y servicios. Pese a ello, aclara que aún requiere un mayor desarrollo que le permita alcanzar la cantidad de transacciones por minuto del sistema actual.

El académico añade que estos métodos, además, suelen contar con medidas de salvaguarda, las que, ante cualquier actividad inesperada o errada, provocan el bloqueo de la cuenta, mitigando el daño al consumidor y al comercio. **G**



Rodrigo López,
Académico del
Departamento de Control
de Gestión y Sistemas
de Información de la
Facultad de Economía
y Negocios de la
Universidad de Chile.