Criptomonedas y activos digitales

Cómo funcionan, cómo guardarlas y cómo operar de forma segura.

¿Qué son las criptomonedas?

Son activos digitales descentralizados que usan criptografía para proteger las transacciones y controlar la creación de nuevas unidades.

Descentralización	No dependen de un banco ni de un gobierno central. Funcionan sobre una red distribuida de personas usuarias y equipos que validan las operaciones.
Privacidad relativa	Las transacciones usan direcciones digitales en lugar de nombres reales. Pero quedan registradas y, en algunos casos, pueden vincularse con una persona.
Irreversibilidad	Una vez confirmada, una transacción en general no se puede revertir. Revisá bien los datos antes de enviar fondos.

Claves y direcciones: el acceso a tus fondos

Para operar se usan dos elementos, parecidos a los de una cuenta bancaria:

- **Dirección de billetera:** es como el número de cuenta. Es pública y podés compartirla para recibir fondos.
- **Clave privada:** es la credencial que permite acceder y mover los fondos. **Nunca la compartas:** quien la tenga controla tu dinero.

Billeteras virtuales (wallets)

Las billeteras permiten gestionar las claves necesarias para operar:

Billeteras calientes (hot wallets)	Están conectadas a Internet: apps, programas o servicios web. Son prácticas para el uso diario, pero la conexión permanente aumenta los riesgos.
Billeteras frías (cold wallets)	Dispositivos o medios que guardan las claves privadas sin conexión. Son una de las opciones más seguras para guardar activos a largo plazo.

Blockchain: la tecnología detrás

El **blockchain** o cadena de bloques es un registro digital compartido por todos los participantes de la red, donde las transacciones se guardan en orden cronológico. Los bloques se enlazan con mecanismos criptográficos, lo que dificulta alterarlos y aporta transparencia.

Consejos de ciberseguridad

- **Activá el segundo factor de autenticación (MFA)** en plataformas de intercambio y billeteras. Si podés, usá apps autenticadoras o llaves físicas de seguridad.

- **Protegé tu frase de recuperación:** guardá las palabras semilla en un lugar físico seguro. Nunca las compartas ni las ingreses en sitios, correos o mensajes que te las pidan.
- **Verificá sitios y apps:** antes de iniciar sesión, confirmá que la dirección web sea la oficial y descargá apps solo de fuentes oficiales.
- **Mantené tus dispositivos actualizados** con las últimas actualizaciones de seguridad.
- **Desconfiá de las ganancias garantizadas:** las falsas oportunidades de inversión son uno de los engaños más usados.
- **Invertí con responsabilidad:** por su volatilidad, usá solo dinero que estés en condiciones de arriesgar.