MONERO

GUÍA DEL PROTOCOLO

Monero

Los principios, sin tecnicismos

Qué es, por qué existe y cómo protege tu privacidad.

01

Qué es Monero

Monero es dinero digital que funciona como el efectivo: pagas a otra persona directamente, sin banco de por medio, y nadie más tiene por qué enterarse de quién pagó, a quién ni cuánto. Su unidad se llama XMR y nació en 2014.

SIN INTERMEDIARIOS

No hay empresa, banco ni gobierno que lo controle. Miles de ordenadores de todo el mundo mantienen la red.

PRIVADO POR DEFECTO

La privacidad no se activa con un botón: todas las transacciones la tienen.

CÓDIGO ABIERTO

Cualquiera puede leer el código, revisarlo y proponer mejoras.

02

Cinco ideas previas

Si ya sabes cómo funciona una criptomoneda, salta directamente a la sección 4.

1. **El libro de cuentas compartido.** En un banco, una sola entidad apunta quién tiene cuánto. Aquí el libro es público y lo guardan miles de ordenadores a la vez. Las operaciones se agrupan en bloques encadenados entre sí: la *blockchain* o "cadena de bloques".
2. **Las claves.** Tienes dos números enlazados. La clave pública es como el número de tu buzón: puedes dárselo a cualquiera. La clave privada es la llave que lo abre, y no se comparte nunca.
3. **La firma digital.** Es un sello que solo tú puedes poner con tu clave privada. Demuestra que autorizaste un pago sin revelar la clave.
4. **Los mineros.** Son quienes añaden los bloques nuevos al libro resolviendo un problema que cuesta mucha computación. A cambio cobran monedas nuevas. Hacer trampa costaría más de lo que se gana.

5 **Las salidas.** No tienes un saldo, sino monedas sueltas, como billetes. Para pagar gastas uno o varios billetes enteros y recibes el cambio como un billete nuevo. Un billete gastado no puede gastarse otra vez.

03

El problema: casi todo el dinero digital es público

En Bitcoin y en la mayoría de criptomonedas, el libro es abierto: cualquiera puede ver qué dirección pagó a cuál y cuánto. No aparece tu nombre, pero basta con que una sola vez una dirección se vincule contigo (una compra, un exchange) para poder seguir todo su historial. Es como si tu extracto bancario fuera público con el nombre tapado.

> **Fungibilidad.** Si cada moneda lleva su historial a la vista, una moneda con "mala fama" puede valer menos que otra idéntica. El dinero debería ser intercambiable unidad por unidad. Monero se diseñó para que lo sea.

04

Los tres principios de privacidad

Monero oculta tres cosas a la vez en cada pago, cada una con su propia técnica.

RECEPTOR OCULTO

Direcciones sigilosas

Un buzón nuevo para cada carta.

EMISOR OCULTO

Firmas de anillo

Firmar dentro de una multitud.

CANTIDAD OCULTA

Montos confidenciales

Sobres cerrados que se pueden sumar.

Quién recibe: direcciones sigilosas

Tu dirección de Monero es pública y reutilizable, pero nunca aparece en la cadena. Para cada pago, quien te paga usa tu dirección para fabricar un destino nuevo y de un solo uso que solo tú puedes reconocer como tuyo. Es como si cada carta llegara a un buzón distinto que solo tú sabes abrir: desde fuera, dos pagos a ti no parecen tener relación.

Quién paga: firmas de anillo

Cuando gastas una moneda, tu wallet la mezcla con otras 15 monedas ajenas de la cadena y firma de una forma especial. La firma demuestra que una de las 16 es tuya, pero no cuál. Es como firmar un documento en medio de una multitud que firma a la vez: se sabe que uno de ellos firmó, no quién.

Además, cada moneda gastada deja una etiqueta única que impide gastarla dos veces, sin revelar de cuál se trata.

Cuánto: montos confidenciales

Las cantidades viajan en sobres cerrados. La red no abre ninguno, pero puede sumar los de entrada y los de salida y comprobar que cuadran, es decir, que nadie ha creado dinero de la nada. Una prueba extra garantiza que ningún sobre contiene una cantidad negativa.

> Los tres mecanismos funcionan juntos: nadie sabe quién recibe, quién envía ni cuánto, y aun así cualquiera puede verificar que todo es válido.

05

Un pago, paso a paso

1. Quien te va a pagar usa tu dirección, que es larga y reutilizable.
2. Su wallet crea un destino de un solo uso para ti. Tu dirección no aparece en la cadena.
3. Para gastar sus monedas, el wallet las mezcla con otras 15 y firma. Nadie sabe cuál es la real.
4. Las cantidades van en sobres cerrados que la red comprueba sin abrir.

5. Los mineros incluyen el pago en un bloque, en unos 2 minutos, y miles de nodos lo verifican.
6. Tu wallet reconoce el pago como tuyo con tu clave de vista. Tras unos 20 minutos (10 bloques) ya puedes gastarlo.

06

Qué mantiene segura la red

MINERÍA PARA TODOS

Usa RandomX, un algoritmo pensado para ordenadores normales y poco favorable a las máquinas especializadas.

RECOMPENSA PERMANENTE

Tras la emisión principal, cada bloque sigue pagando 0,6 XMR a los mineros, para que siempre tengan incentivo.

Cada nodo comprueba por su cuenta todas las reglas, así que no hace falta confiar en nadie. Ninguna red es invulnerable: en 2025 un grupo concentró mucha potencia de minería y consiguió reorganizar hasta 18 bloques recientes, el episodio de este tipo más grande de la historia de Monero. Por eso en pagos grandes conviene esperar varias confirmaciones.

REFERENCIA

Glosario rápido

TÉRMINO	EN UNA FRASE
Blockchain	Libro de cuentas público formado por bloques encadenados
Nodo	Ordenador que guarda el libro y comprueba todas las reglas
Minero	Quien añade bloques nuevos y cobra monedas por ello
Wallet	Programa que guarda tus claves y crea tus pagos
Clave pública y privada	Tu buzón, que se comparte, y su llave, que no
Dirección sigilosa	Destino de un solo uso derivado de tu dirección
Firma de anillo	Firma que prueba que uno de varios firmó, sin decir quién
Key image	Etiqueta única de cada moneda gastada que evita el doble gasto
XMR	La unidad de Monero

> **Siguiente paso.** La guía completa, "Monero a fondo", explica cada una de estas piezas con más detalle y sus matemáticas, capítulo a capítulo.

Fuentes: The Block y Cointelegraph (reorganizaciones de 2025).