MISIÓN 1 · LA FERIA DEL BARRIO

Fundamentos del Dinero Digital y Redes Persona a Persona (P2P)

Guía teórico-práctica de respaldo para consolidar lo que acabás de experimentar en el simulador: por qué existen las redes descentralizadas, cómo viaja el valor sin intermediarios, qué es realmente un bloque público y cómo protegerte desde el primer día.

NIVEL	SIMULADOR ASOCIADO	DESBLOQUEO HOTMART
Inicial · Cero previos	**La Feria del Barrio**	**Quiz Módulo 01 → 02**

Qué vas a dominar al terminar este manual

- Entender el concepto de **punto único de fallo** y por qué una red P2P sigue operando aunque caiga un banco o procesador de pagos.
- Distinguir con claridad **dirección pública** (lo que compartís para cobrar) de **clave privada** (lo que jamás compartís).
- Leer la anatomía real de una transacción en un **registro público (blockchain)** sin necesidad de saber programar.
- Aplicar el protocolo de verificación **Regla 4-4-Test** para evitar el error más costoso de todo principiante: enviar fondos a una dirección equivocada.

SECCIÓN 01 · EL PROBLEMA RAÍZ

¿Por qué existe el dinero persona a persona?

Cuando pagás en efectivo en una feria, el intercambio es directo: vos le entregás un billete físico a Don Mateo y la operación termina en ese instante. Nadie tiene que aprobarla, ningún servidor puede caerse y ninguna empresa cobra comisión por autorizarla.

El problema aparece cuando pasamos al **dinero digital**. Un archivo digital se puede copiar infinitas veces (lo que en informática se llama el *problema del doble gasto*: si un billete digital fuera solo una foto, podrías enviársela a diez personas a la vez). Durante décadas, la única solución que conoció el mundo fue poner a un **intermediario centralizado** —un banco, una red de tarjetas o una billetera corporativa— que lleva el cuaderno maestro de quién tiene cuánto.

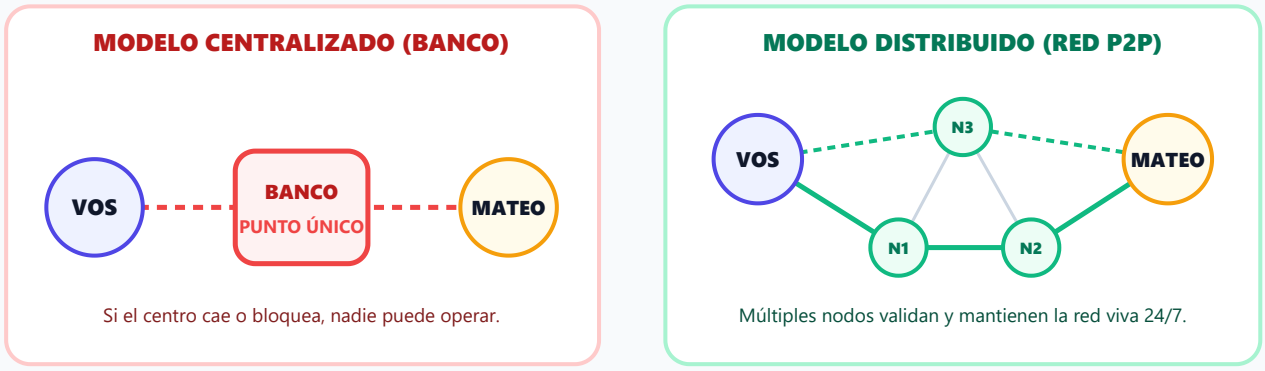


Figura 1.1 — Diferencia estructural entre depender de un único servidor central y operar sobre nodos distribuidos P2P.

Qué es un «Punto Único de Fallo» (Single Point of Failure)

En ingeniería de sistemas, un punto único de fallo es cualquier componente cuya caída paraliza a toda la red. En el simulador de *La Feria del Barrio* lo comprobaste en cinco segundos: vos tenías `50.00 mUSD`, Don Mateo tenía el producto, pero al caer el servidor bancario la operación rebotó.

Limitaciones del modelo tradicional

Depende de horarios bancarios, mantenimientos, límites arbitrarios de monto, costos altos para envíos internacionales y riesgo de congelamiento o fallas técnicas en un solo proveedor.

Qué aporta una red P2P

Funciona 24/7 los 365 días del año en cualquier país. Ninguna empresa única puede apagar la red completa porque miles de computadoras independientes (**nodos**) comparten el mismo registro.

💡 Idea clave para recordar

Una criptomoneda no es «plata mágica de internet»: es un **sistema de contabilidad compartido entre miles de computadoras** que permite mover valor digital directo de persona a persona, igual que el efectivo físico, pero a distancia y verificable matemáticamente.

SECCIÓN 02 · MECÁNICA INTERNA

Cómo funciona tu billetera sin un banco detrás

Uno de los mayores malentendidos de quien empieza es creer que «las monedas están guardadas adentro del celular». En realidad, **tus fondos siempre viven en el registro público de la red**. Tu billetera (*wallet*) es un llavero criptográfico que demuestra que vos sos el único dueño autorizado a mover esos fondos.

📬 Dirección Pública (tu «CBU / Alias»)

Es una cadena de letras y números como `0x7F4A...9B2E`. Podés mostrarla en un QR en una feria, imprimirla o mandarla por WhatsApp para que te paguen. **Compartirla es 100% seguro**: con ella solo pueden enviarte dinero o consultar el historial público.

🔑 Clave Privada / Frase Semilla (tu «Firma Maestra»)

Es el secreto matemático (normalmente representado como 12 o 24 palabras) que firma tus envíos. **Quien tiene esas palabras controla el dinero.** Jamás se escribe en formularios web ni se le pasa a ningún «soporte técnico».

Anatomía de un envío P2P en 4 pasos (lo que hiciste en el Paso 3)

1. **Construís la orden:** indicás destinatario (`0x7F4A...9B2E`), monto (`10.00 mUSD`) y comisión de red.
2. **Verificás la dirección:** comparás visualmente los primeros 4 y últimos 4 caracteres contra la tarjeta de Don Mateo para evitar errores o direcciones falsas (`...9B2F`).
3. **Firmás criptográficamente:** tu billetera usa tu clave privada internamente (sin revelarla nunca) para generar una firma digital imposible de falsificar.
4. **Propagación y registro:** los nodos de la red comprueban que tenías saldo suficiente y que la firma es válida, y escriben la operación en el siguiente **bloque público**.

⚠️ ¿Por qué una dirección equivocada no tiene «botón de deshacer»?

Porque no existe un gerente de banco con poder para editar el pasado del libro contable. Esa misma **inmutabilidad** que impide que alguien te robe o borre un pago ya recibido hace que **verificar el destino antes de firmar sea una responsabilidad indelegable**.

SECCIÓN 03 · TRANSPARENCIA VERIFICABLE

Qué fue exactamente el «Bloque #1042» que viste en pantalla

Cuando completaste el pago a Don Mateo, apareció un recibo con el título **BLOQUE #1042**. Esa palabra —*bloque*— es la pieza central de una **blockchain** (cadena de bloques): un libro contable público donde las páginas (bloques) se van sellando una detrás de otra con un código matemático único llamado **hash**.

```
BLOQUE: #1042 (Número secuencial en la cadena)
HASH PREVIO: 0x41aa9f...0c71 (Enlace matemático al Bloque #1041)
TX HASH: 0x9c4e...81a2 (Comprobante único e irrepetible de tu pago)
REMITENTE: Tu dirección pública (saldo: 50.00 → 40.00 mUSD)
DESTINATARIO: Don Mateo · 0x7F4A...9B2E (+10.00 mUSD)
ESTADO: ✓ CONFIRMADO POR CONSENSO DE NODOS
```

¿Por qué nadie puede hacer trampa ni falsificar un recibo?

Cada bloque incluye la huella digital (*hash previo*) del bloque anterior. Si alguien intentara alterar retroactivamente tu pago en el Bloque #1042 para cambiar `10 mUSD` por `1000 mUSD`, cambiaría la huella de ese bloque y rompería la cadena en todos los bloques siguientes. El resto de los nodos de la red detecta la inconsistencia al instante y rechaza la versión falsa.

✓ Cómo se usa esto en la vida real (Exploradores de Bloques)

En redes reales como Bitcoin o Ethereum, cualquier persona puede pegar el **TX Hash** en un explorador público (como *mempool.space* o *etherscan.io*) y comprobar en segundos si el pago realmente salió, a qué dirección fue y cuántas confirmaciones tiene — sin capturas de pantalla falsificables.

Seudonimato vs. Anonimato

Un error muy común es creer que las criptomonedas son «invisibles». En la mayoría de las blockchains públicas, **todas las transacciones son visibles para cualquiera**: no aparece tu nombre y apellido impreso en el bloque, pero sí tu dirección pública y cada movimiento que hizo. Por eso hablamos de redes **seudónimas**, no secretas.

SECCIÓN 04 · CRITERIO PRÁCTICO

Mito vs. Realidad: lo que diferencia a un alumno formado

Mito frecuente	Realidad técnica verificada
«Las transferencias P2P son siempre gratis»	Toda red pública cobra una comisión de red (*gas* o *fee*) para recompensar a los validadores y evitar spam. Veremos cómo optimizarla en el Módulo 2.
«Si me equivoco de dirección, llamo a soporte y lo cancelan»	No existe mesa de ayuda central con poder de reversión. Una vez confirmada la transacción en el bloque, es definitiva.
«Mis criptos están guardadas adentro del celular»	Tus fondos viven en la blockchain; el celular solo guarda las llaves. Si perdés el teléfono pero conservás tu frase semilla offline, recuperás el 100%.
«En blockchain nadie puede ver qué pagué»	El registro es público y auditable. Cualquiera con el TX Hash o la dirección puede verificar fecha, monto y destino.
«Si alguien me ofrece recibir mis pagos en su cuenta es más cómodo»	Reintroducís un intermediario sin garantías legales ni técnicas: perdés el control directo (custodia) de tu dinero.

🛡️ **Protocolo Obligatorio antes de enviar dinero real: la «Regla 4-4-Test»**

Usá estos 4 hábitos en cada operación real para blindarte contra el 95% de los errores operativos:

1. **Verificá los primeros 4 y últimos 4 caracteres** de la dirección pegada (para detectar malware o direcciones parecidas como `...9B2F` vs `...9B2E`).
2. **Confirmá que la red coincida** entre origen y destino (lo practicaremos en profundidad en el Módulo 2).
3. **Envío de prueba (Test):** si vas a mover un monto importante a una dirección nueva, enviá primero un monto mínimo de prueba y confirmá su llegada antes de mandar el resto.
4. **Nunca firmes apurado** ni bajo presión de un desconocido por chat o llamada.

SECCIÓN 05 · REFERENCIA RÁPIDA

Glosario de Bolsillo (12 conceptos que ya entendés)

Red P2P (Peer-to-Peer)
Red donde los participantes interactúan directamente sin servidor central obligatorio.

Punto Único de Fallo
Componente central cuya caída frena todo el sistema (ej. un único banco).

Nodo
Computadora independiente que valida transacciones y guarda copia del registro.

Blockchain
Cadena de bloques enlazados criptográficamente que forma el libro contable público.

Dirección Pública
Identificador alfanumérico (o QR) que compartís para recibir fondos.

Clave Privada
Secreto matemático que firma y autoriza salidas de dinero. Nunca se comparte.

Frase Semilla (Seed)
Respaldo de 12 o 24 palabras que reconstruye todas tus claves si perdés el dispositivo.

TX Hash
Huella única que funciona como recibo verificable de una transacción específica.

Irreversibilidad
Propiedad por la cual un pago confirmado no puede deshacerse unilateralmente.

Consenso
Reglas compartidas por los nodos para ponerse de acuerdo sobre qué pagos son válidos.

Seudonimato
Operaciones públicas asociadas a direcciones criptográficas, no a tu DNI directo.

Doble Gasto
Intento de gastar el mismo dinero digital dos veces; la blockchain lo impide por diseño.

Autoevaluación rápida (antes de pasar al Módulo 2)

Respondé mentalmente antes de revisar la clave: **1)** Si un comercio te manda su dirección por WhatsApp, ¿qué revisás antes de tocar «Enviar»? **2)** Si perdés el celular pero tenés tu frase semilla guardada en papel, ¿perdiste tus fondos? **3)** ¿Por qué el recibo on-chain (TX Hash) vale más que una captura de pantalla?

Respuestas guía: (1) Primeros 4 y últimos 4 caracteres + envío de prueba si el monto es alto. (2) No, los fondos viven en la red y los recuperás con la semilla. (3) Porque cualquiera puede auditar el TX Hash en el registro público y no se puede editar con Photoshop.

🔓 **Desbloqueo automático en Hotmart Club**

Ingresá este código en el Quiz del Módulo 1 dentro de Hotmart Club para habilitar el **Módulo 2: La Fila del Peaje (Redes, Billeteras y Gas)**.

`FERIA-P2P-2026`