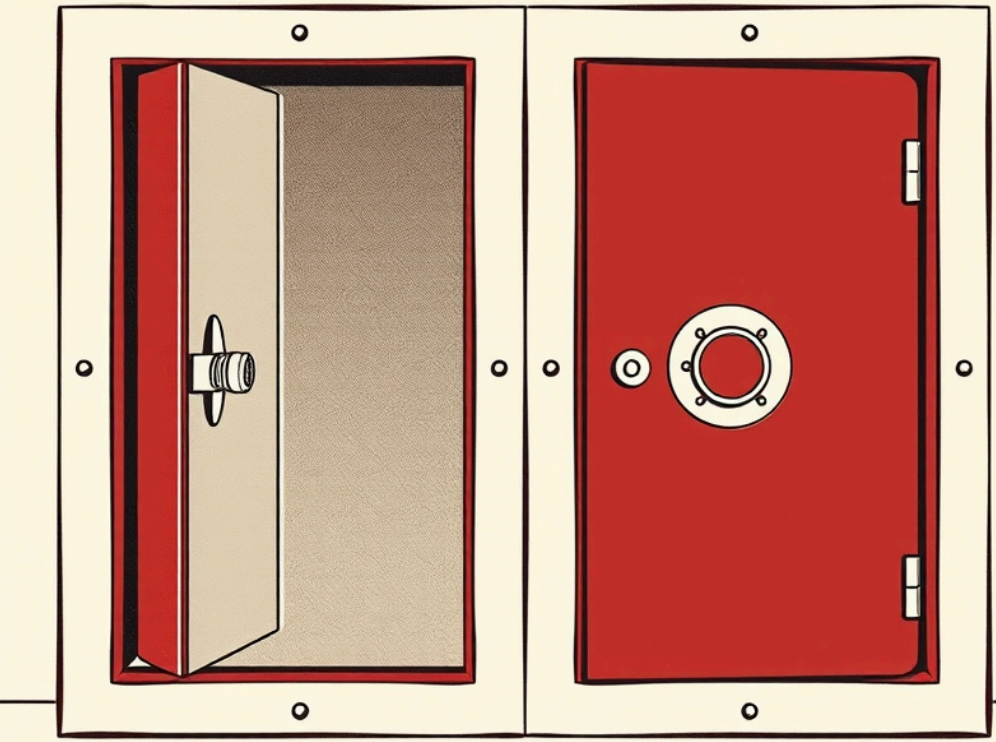
Una guía de campo sobre el dinero que te enseñaron a temer

¿COMPARADO CON QUÉ?



Los peligros reales de las criptomonedas —
y sus gemelos, que ya viven en tu banco.

DMYTRO CHYSTIAKOV

¿COMPARADO CON QUÉ?

Los peligros reales de las criptomonedas —
y sus gemelos, que ya viven en tu banco.

DMYTRO CHYSTIAKOV

Primera edición, 2026

Traducción del original en inglés: Compared to What?

Cada incidente de este libro está documentado en el registro público; al final se incluye una nota sobre las fuentes.

Este libro es informativo. No constituye asesoramiento financiero, de inversión ni legal.

Algunas personas mencionadas en este libro han sido acusadas de delitos pero no condenadas; se presumen inocentes mientras no se pruebe su culpabilidad. Los estados procesales y las cifras corresponden a julio de 2026.

Los nombres de productos y las marcas pertenecen a sus propietarios y se usan solo con fines de identificación; su mención no implica afiliación ni recomendación, incluidas las herramientas de la guía de campo. Las herramientas y direcciones cambian: verifícalas por tu cuenta.

Compuesto en Iowan Old Style.

Introducción: El trato

Hay dos tipos de personas que te van a hablar de cripto, y ninguno de los dos te está hablando a ti.

El primer tipo vende. Ya los conoces—los del Lamborghini alquilado y el atardecer y la palabra *libertad*, los que han descubierto que el activo más fácil de vender es la sensación de haber llegado temprano. Te hablarán de las ganancias. No te dirán qué pasa después, porque lo que pasa después no está en la presentación.

El segundo tipo sabe de lo que habla, y escribe para los suyos. Su trabajo es real y es excelente y es ilegible, porque nunca fue pensado para ti: está dirigido a investigadores, a equipos de cumplimiento, a gente que ya sabe qué es un nonce. Podrías leer cada palabra y aun así no saber si debes tener miedo.

Así que hay un hueco, y en ese hueco es donde en realidad está parado todo el mundo. Millones de personas llegando a una puerta, con los vendedores a un lado y los especialistas al otro, y nadie en el medio que no esté vendiendo ni luciéndose.

Este es el libro que yo quería cuando estaba parado ahí.

Qué es esto

Pasé años construyendo un catálogo de todas las formas documentadas en que la gente ha perdido dinero en esto — cientos de incidentes, desde 2010, cada uno con sus fuentes, verificado y archivado por mecanismo y no por drama. Es gratuito y es público y no es este libro. Es una obra de referencia para profesionales y te va a matar de aburrimiento.

Esto es lo que esa obra de referencia *sabe*, contado como lo que realmente es: un conjunto de historias sobre personas que, en su mayoría, no hicieron nada mal.

No es una advertencia. No es un discurso de venta. No es un curso. **Es lo que me habría gustado que me entregaran entero, en la puerta, antes de tener que improvisarlo todo sobre la marcha.**

El trato

Esto es lo que prometo, y deberías exigirme que lo cumpla todo, porque un libro como este vale exactamente lo que vale su peor frase.

Cada número de este libro es verificable, y los que no lo son se descartan delante de ti. Me verás desechar mi mejor evidencia más de una vez, porque tengo a mano cifras espectaculares que ganarían cualquier discusión y que no puedo respaldar. Si uso un número que un proveedor inventó porque me conviene, no tienes por qué creer ningún otro número del libro, y harías bien.

Cada capítulo tiene un veredicto, y los veredictos no van todos en la misma dirección. Este es el mecanismo que mueve todo el libro, así que aquí va, por adelantado: tomo un peligro de cripto, lo pongo junto a la versión de ese mismo peligro que

ya opera en tu vida financiera ordinaria, y digo sin rodeos cuál es peor. A veces la respuesta es cripto. Es cripto en el capítulo dos, y en el siete, y por mucho en el ocho. Si todos los veredictos cayeran del mismo lado, deberías cerrar el libro, y yo también.

Nada está reconstruido. Cuando no sé algo, lo digo. Hay aquí un robo de $282 millones — mayor que cualquier otra cosa en estas páginas — alrededor del cual me niego a construir un capítulo, porque nadie puede establecer cómo ocurrió, y una historia con las partes interesantes inventadas no es una historia: es una mentira con notas al pie.

Y no voy a decirte qué hacer con tu dinero. Ni una sola vez. No conozco tu situación, no soy tu asesor, y la industria entera de gente que sí *va* a decírtelo es la razón por la que necesitabas este libro.

Qué te llevas

Al final sabrás qué es realmente una billetera y por qué la palabra es una mentira. Qué es una clave privada, y por qué doce palabras pueden ser doscientos cincuenta millones de dólares. Qué es una stablecoin y qué pasa cuando la variante ingeniosa deja de ser ingeniosa. Por qué quieren tu pasaporte, y qué atrapa en realidad el sistema que lo exige. Cómo se construye una memecoin, segundo a segundo, para quitarte dinero legalmente. Qué significa «limpia» y por qué ninguna moneda lo es.

Y conocerás la forma del asunto, que es la parte que no vas a encontrar en ningún otro lado: **que casi nada de esto es nuevo.** La llamada telefónica que se llevó $243 millones es la llamada que tu banco lleva treinta años combatiendo. La billetera de hardware falsificada es un skimmer en una gasolinera. La memecoin es un boiler room — una oficina de vendedores a presión

—, y los boiler rooms son más viejos que el teléfono. Los fraudes no llegaron con cripto. Llegaron con el dinero, y han estado operando, a gran escala, en el lugar donde ya guardas el tuyo, todo este tiempo.

Lo que hizo cripto fue ponerlos por escrito.

Ese es el argumento. Todo lo demás es evidencia — doscientas páginas de ella — y puedes verificar cada línea.

Una cosa, antes del capítulo uno

El miedo que te trajo hasta aquí es correcto.

No voy a quitártelo y no voy a decirte que esto es seguro. Los tres primeros capítulos son lo peor del libro y van al principio a propósito: un hombre que pierde $243 millones por una llamada telefónica, un sistema sin botón de deshacer, y una década de exchanges que resultaron ser un número en la base de datos de alguien.

Léelos primero. Si después cierras el libro, es un desenlace legítimo y el libro ya habrá valido lo que pagaste por él.

Pero si te quedas, la pregunta deja de ser *si esto es peligroso* — lo es — y se convierte en la que nadie hace, que es la única pregunta útil que ha existido jamás sobre todo esto:

¿Comparado con qué?

1
La llamada telefónica

La primera llamada vino de Google.

No de alguien que decía ser Google en el sentido habitual de la frase—la línea con ruido, el número extraño, el enlace que lleva a donde no debe. El número en la pantalla era el de Google. La voz sabía de lo que hablaba. Había un problema con la cuenta, y el hombre llamaba para ayudar a resolverlo.

Para cuando terminó esa llamada, tenían su correo y su almacenamiento en la nube. Es decir: tenían todo lo que él había anotado alguna vez sobre su dinero.

Una hora después llegó la segunda llamada, y esta era de Gemini—un exchange de criptomonedas, uno que él usaba de verdad. El hombre de esta llamada sabía cosas. Sabía qué cuentas

existían. Sabía más o menos qué había en ellas. Sabía detalles que ningún vendedor de esos que llaman en frío podría saber y que ningún estafador tenía por qué saber, y todos eran ciertos, porque una hora antes las mismas personas los habían sacado de la bandeja de entrada de la víctima.

Ese es todo el mecanismo, y vale la pena nombrarlo, porque es la diferencia entre una estafa que cualquiera detectaría y una que no detecta nadie: **cada etapa roba las credenciales que autentican a la siguiente.** La primera llamada es endeble y consigue poco. Ese poco vuelve sólida a la segunda llamada. La segunda llamada lo consigue todo.

En algún momento de la segunda hora, el diecinueve de agosto de 2024, lo guiaron paso a paso para restablecer su autenticación de dos factores y mover sus fondos a una billetera que ellos controlaban. Cuatro mil sesenta y cuatro bitcoin salieron en una sola transacción. Doscientos treinta y ocho millones de dólares, un clic. El total llegó a aproximadamente $243 millones.

Es la mayor cantidad de dinero jamás arrebatada a una sola persona con solo hablarle.

Una billetera no es una billetera

Dos palabras de ese párrafo — *billetera* y *salieron* — están cargando con más peso del que aparentan, y si eres nuevo aquí, las dos te están mintiendo un poco. Arreglémoslas ahora, porque todo este libro descansa sobre ellas.

Una billetera no contiene nada. Nada entra en ella y nada sale. No es un recipiente. Lo que guarda es una *clave* — un número secreto — y lo que esa clave hace es autorizar el movimiento de monedas que están registradas en otra parte. Piénsala menos como un monedero y más como un anillo de sello: el anillo no es la hacienda, es lo que demuestra que una instrucción vino

de ti. Pierde el monedero y pierdes lo que lleva dentro. Pierde el anillo, y otra persona puede ordenar que se venda la hacienda entera.

Y las monedas nunca «salieron» hacia ningún lado. Están en el registro, y el registro es donde se deshace la segunda mentira.

Imagina el libro más aburrido del mundo. Cada página es una lista de transferencias — tanto, desde aquí, hacia allá, en este segundo. Cuando alguien envía dinero, se añade una línea. Eso es todo. Ese es el invento completo. No hay cuentas en el sentido que conoces, ni nombres, ni sucursales, ni horario de cierre. Hay una lista de quién movió qué hacia dónde, y tu saldo no es un número guardado en ninguna parte; es lo que obtienes cuando sumas todas las líneas que alguna vez te mencionaron.

Tres cosas sobre el libro, y la tercera es la razón de que esta historia termine como termina.

Nadie es su dueño. No hay una empresa que lo lleve. Miles de computadoras guardan copias idénticas y acuerdan, constantemente, qué dice la página siguiente. Ese acuerdo — alcanzado por máquinas que no se conocen entre sí y no necesitan hacerlo — es lo que la gente quiere decir cuando dice «blockchain», y es de verdad la parte ingeniosa.

Nada se borra jamás. No puedes arrancar una página. No puedes enmendar una línea. Un error no se corrige; se añade una *línea nueva* que devuelve el dinero, si quien lo tiene acepta devolverlo. Nadie puede meter la mano en el pasado.

Cualquiera puede leerlo. No «cualquiera con autorización». No «cualquiera con una orden judicial». Cualquiera. Ahora mismo, desde tu teléfono, puedes ver cada transferencia del planeta mientras ocurre, incluidas las que acaban de robar algo. El libro se escribe en público, de forma permanente, y siempre ha sido así.

Esta última es la propiedad más extraña de todas las finanzas, y este capítulo está a punto de mostrarte sus dos filos a la vez.

Porque es la razón de que el dinero saliera y no pudiera volver jamás — y es la razón de que sepamos los nombres de los hombres que se lo llevaron.

El hombre que lo perdió

Era un acreedor en la quiebra de Genesis Global Capital, y vivía en Washington, D. C.

El primer dato no es casual — es la razón por la que fue elegido, y le da la vuelta a lo que la mayoría cree sobre cómo pasa esto. No fue descuidado. No era un incauto. No había entrado porque un video se lo dijera. Era una contraparte institucional sofisticada que había prestado a gran escala a una empresa de préstamos, y cuando esa empresa colapsó, su derecho de cobro quedó asentado en un expediente público.

No se toparon con él. Lo buscaron.

Esta es la parte más difícil de asimilar, y el libro volverá a ella: **encontrar una víctima es un problema de investigación, y la investigación es pública.** Los expedientes de la quiebra decían a quién se le debía. La cadena decía qué se tenía y si se había movido. En otro caso documentado de la misma manera, los atacantes armaron su lista corta rastreando el registro en busca de saldos grandes que llevaban años sin moverse — una fortuna dormida es legible desde afuera, y su dueño es un nombre unido a ella en alguna parte.

La transparencia que le permite a un investigador rastrear un robo es la misma transparencia que le permite a un atacante armar una lista de objetivos. Nadie consigue la una sin la otra. Eso no es un defecto del diseño; es el diseño, y en este capítulo llega la factura.

Todos los sistemas funcionaron

Esto es lo que no pasó el diecinueve de agosto.

No se explotó ningún contrato inteligente. No se rompió ninguna criptografía. No se comprometió el firmware de ninguna billetera, no se vulneró ningún exchange, no falló ningún protocolo, no se encontró ningún bug, no se quemó ningún zero-day. Nada en la tecnología salió mal en ningún momento de las dos horas que tomó mover doscientos cincuenta millones de dólares.

Cada componente se comportó exactamente según su especificación. La billetera firmó una transacción correctamente formada, porque una transacción correctamente formada fue lo que le entregaron, y firmarlas es todo su propósito. La red la confirmó, porque era válida. La cadena la escribió de forma permanente y se la mostró a cualquiera en el mundo en cuestión de segundos, que es *para* lo que existe la cadena.

No hay ningún componente de esa pila que haya fallado. Hay un hombre al teléfono, y todo lo que está aguas abajo de él funcionando a la perfección.

Esta es la concesión que el libro tiene que hacer antes de argumentar nada: **aquí hay una capa a la que no se llega con ingeniería, por mucha que se ponga, y es la capa a la que todo lo demás está atornillado.** Puedes custodiar tus propias claves, rechazar a todos los custodios, comprar el hardware, no tocar jamás un sitio que no hayas tecleado tú —y aun así todo el edificio termina en una persona a la que alguien que suena creíble y conoce su saldo puede decirle algo falso.

Los hombres que se lo llevaron

Eran unos muchachos.

Malone Lam tenía veinte años. Nació en Singapur en julio de 2004 y creció en Choa Chu Kang, una zona de vivienda pública en el oeste de la isla. Fue a la escuela secundaria Unity y la abandonó de adolescente para dedicar su tiempo a operar con cripto y a vivir en las comunidades en línea que lo criaron — servidores de Minecraft y Discord.

Con sus compañeros de casa en Texas cofundó, según la acusación federal, algo que llamaron, sin ironía aparente, la **Social Engineering Enterprise** — la «Empresa de Ingeniería Social». Llegó a tener catorce personas repartidas en varios estados. Trabajaban con bases de datos hackeadas, datos de la dark web y correos de phishing, y lo que hacían no era hackear. Era llamar a la gente por teléfono.

Jeandiel Serrano tenía veintiuno, era de Los Ángeles y se hacía llamar «VersaceGod». **Veer Chetal**, que se hacía llamar «Wiz», era aún más joven — un adolescente.

Un veinteañero que dejó la secundaria por Discord le quitó doscientos cuarenta y tres millones de dólares a un acreedor institucional en Washington por teléfono, en unas dos horas, sin romper una sola cosa.

Esa es la frase para la que existe este capítulo, y ninguna parte de ella es una exageración.

Luego lo filmaron

Transmitieron el golpe en vivo para sus amigos.

No como evidencia. Para tener público. Existe una grabación de los hombres que acababan de quitarle $243 millones a un desconocido, viendo caer las notificaciones — las alertas, las confirmaciones, el dinero llegando — y celebrando, y hablando de lo

que venía después. La hicieron para ellos mismos, por la razón por la que la gente que acaba de hacer algo enorme quiere conservar el momento.

Luego se filtró, y se convirtió en lo que los identificó.

Lo que siguió fueron treinta y tres autos de lujo. Relojes. Discotecas. Viajes. No fue un intento de salirse con la suya; fue una ola de gastos a la vista de todos, por gente que no parecía haber pensado más allá de esa semana.

El FBI arrestó a Malone Lam en Miami el dieciocho de septiembre de 2024, un mes después del robo. Un policía fuera de servicio le había avisado de que iban a arrestarlo, y camino del arresto lanzó su teléfono a la bahía de Biscayne.

Veer Chetal se declaró culpable. Entregó en decomiso casi treinta relojes de diseñador, un guardarropa entero y más de $36 millones en ether. Luego, mientras estaba en libertad bajo fianza a la espera de sentencia por el que entonces era el mayor robo cripto a una sola víctima del que haya registro, le revocaron la fianza después de que la fiscalía dijera que había participado en el robo de otros dos millones de dólares.

Pon todo eso junto al resto del capítulo, porque es la única luz que hay aquí. Este es un libro que va a dedicar la mayoría de sus páginas a personas que perdieron dinero y a las que nunca les dijeron qué pasó con él. Esta historia tiene nombres, edades, un video, tres procesos judiciales y un teléfono en el fondo de una bahía.

La razón de que tenga esas cosas es el libro de hace unas páginas.

Esto es lo que «seguir el dinero» significa en realidad, porque no se parece en nada a lo que la frase sugiere y es lo más útil que un recién llegado puede entender.

Cuando los $238 millones se movieron, apareció una línea: *tanto, desde esta dirección, hacia aquella dirección, en este segundo*. Pública. Permanente. Los ladrones hicieron entonces lo que hacen los ladrones—lo dividieron en tres y echaron a correr. Quince exchanges o más. Bitcoin cambiado por litecoin, litecoin por ether, ether por monero, cada vez más rápido, cada salto pensado para romper el rastro.

Cada salto escribió otra línea.

Esa es la trampa, y no tiene fondo. En el mundo que conoces, seguir dinero robado significa pedir. Pedirle a un banco, lo que requiere un motivo; pedirle a un banco de otro país, lo que requiere un tratado; esperar; recibir una negativa; volver a pedir. Cada salto es una puerta, y detrás de cada puerta hay una persona que puede decir que no, y con suficientes puertas se agota cualquiera.

Aquí no hay puertas. El registro no tiene permisos. Un ladrón que mueve dinero por quince exchanges no está cubriendo quince rastros—está escribiendo quince líneas más en un libro que todo el mundo ya puede leer, y no puede dejar de escribir, porque aquí mover *es* escribir. Puede hacer que el camino sea complicado. No puede volverlo privado, y no puede hacer que mañana deje de estar ahí.

Así que alguien lo leyó.

No usa su nombre, y eso es deliberado, así que usaremos el que sí usa: **ZachXBT**. Su avatar es un ornitorrinco de caricatura con gabardina de detective. No es policía. No es regulador, ni agente, ni analista de una firma, ni empleado de nadie. No tiene formación en investigación de ningún tipo—ninguna, ni un curso, ni una placa, ni un día. Él mismo lo ha dicho.

Lo que tiene es una cuenta pendiente.

Llegó en 2017, durante el auge en que cualquiera podía vender un token escribiendo un documento sobre él, e hizo lo que hacían todos: compró los que estaban de moda. Los vio desaparecer. Luego, en 2018, alguien hackeó su billetera y se llevó unos quince mil dólares, que eran, en ese momento, una parte considerable de su dinero.

Y en algún momento de las secuelas de eso — las secuelas concretas que este libro lleva un capítulo describiendo, las que no tienen departamento de fraude ni nadie a quien llamar — hizo algo que casi nadie hace.

Fue y miró.

No su propio robo. El *registro*. Y lo que encontró ahí era lo que a todos les habían dicho y nadie había entendido: todo seguía ahí. Cada salto que el ladrón había dado, todavía a la vista del público, sin borrar, esperando. Nadie lo había retirado porque nadie podía. Nadie lo había escondido porque nadie podía. Simplemente estaba *ahí*, y ahí había estado todo el tiempo, y casi nadie lo estaba leyendo.

Ese es el momento Michael Lewis, si quieres — una persona que nota algo verdadero sobre un sistema antes que la gente a la que le pagan por notarlo. Solo que no era una revelación sobre bonos hipotecarios. Se parecía más a entrar a una biblioteca que a todos les habían dicho que era una bóveda.

Empezó a publicar en 2021. Para cuando los hombres de aquella llamada le quitaron $243 millones a un desconocido en Washington, él era la razón de que ponerles nombre tomara un mes en vez de nunca.

Para 2025, un cofundador de Paradigm situaba la cifra que él había ayudado a recuperar para las víctimas en **más de trescientos cincuenta millones de dólares**.

Un hombre que perdió quince mil y no tenía idea de lo que hacía ha recuperado a arañazos trescientos cincuenta millones para personas que no conoce.

Sin placa. Sin citación judicial. Sin orden. Sin el permiso de nadie. Leyó lo que ya era público, y lo que seguirá siendo público dentro de cien años.

Volverá. El resto de este libro sigue girando, en silencio, en torno a lo que él descubrió.

(Una nota, ya que este libro está a punto de pasar doscientas páginas nombrando gente. Su nombre real consta en registros públicos—salió en un expediente judicial, porque alguien a quien no le gustó ser investigado lo demandó. No va a aparecer aquí. Él pide no ser identificado, el libro no lo necesita, y hay cierta simetría en ello: el hombre que hizo visible el dinero de todos los demás es la única persona de estas páginas cuyo nombre no voy a imprimir.)

Lo que este capítulo no es

Sería fácil, desde aquí, escribir la frase que hace esto soportable. Que debió colgar. Que había una regla, y la pasó por alto.

No la pasó por alto. No hubo ningún momento en el que una persona cuidadosa lo habría detectado, porque para cuando llegó la segunda llamada, esta *tenía evidencia*—evidencia tomada de él una hora antes, y exactamente por eso era precisa. No lo engañó un desconocido que adivinó bien. Lo engañó un desconocido que había leído su correo.

Y cuando terminó, no había nada que hacer. Sin recurso, sin reversión, sin autoridad por encima de la transacción, porque la transacción era válida y estaba correctamente formada e hizo precisamente lo que decía. Vio salir $243 millones de una forma que no tiene botón de deshacer, y la corrección del sistema era la razón por la que no podía deshacerse.

Una parte se recuperó después — incautaciones, decomisos, un guardarropa y una pila de relojes y treinta y tres autos. La mayor parte, no.

Ese es el miedo, y el miedo es correcto. No es superstición y no es un invento de los medios, y este libro no va a quitárselo a nadie. **Aquí, cuando el dinero se va, se va de forma permanente, y la permanencia es una propiedad real con un costo real, y el costo es exactamente lo que parece.**

Quédate con eso un capítulo más antes de que se argumente nada. Se lo ha ganado.

Pero llévate dos cosas, porque el resto está construido sobre ellas.

La primera es que **nada se rompió.** Ni una línea de código, ni una clave, ni una cadena. Lo que falló fue un hombre que le creyó a una voz que conocía su saldo.

La segunda es que sabemos los nombres de quienes lo llamaron, qué edad tenían, qué compraron y dónde cayó el teléfono.