LA GRAN REVOLUCIÓN MONETARIA

BITCOIN

Historia, fundamentos, funcionamiento técnico, seguridad y futuro

Autor: David Maceiras - Julio de 2026

Índice

PARTE VII · PREGUNTAS FRECUENTES

PARTE VIII · REFERENCIA

PARTE I

FUNDAMENTOS PREVIOS

Capítulo 1. El dinero: qué es y cómo ha evolucionado

Antes de poder entender Bitcoin de verdad, hay que entender el dinero. No el dinero como la tarjeta que llevamos en la cartera o el número que aparece en la aplicación del banco, sino el dinero como herramienta: qué problema resuelve, por qué lo inventamos y por qué ha ido cambiando de forma a lo largo de la historia. Bitcoin no se entiende como una pieza de tecnología aislada; se entiende como el último capítulo, de momento, de una historia que empezó hace miles de años.

¿Qué es realmente el dinero?

El dinero es, ante todo, una solución a un problema práctico: cómo intercambiar valor entre personas que no confían plenamente la una en la otra y que no siempre quieren lo mismo en el mismo momento. Para que algo funcione como dinero, la tradición económica le exige cumplir tres funciones al mismo tiempo.

- Medio de intercambio: sirve para comprar y vender sin necesidad de que las dos partes quieran exactamente lo que la otra ofrece. Es, en el fondo, un traductor universal de valor: el panadero no necesita encontrar a un zapatero que quiera pan, porque ambos aceptan la misma moneda como puente entre lo que cada uno tiene y lo que cada uno necesita.
- Depósito de valor: permite guardar el fruto de tu trabajo hoy para poder usarlo en el futuro, sin que se deteriore o desaparezca. Es como una nevera para el esfuerzo: en lugar de guardar pescado (que se pudre en días) o ladrillos (que pesan demasiado para acumular), guardas algo que conserva su utilidad durante años o décadas.
- Unidad de cuenta: da una referencia común para medir el precio de las cosas, de modo que se puedan comparar peras con sillas o con horas de trabajo. Funciona como el metro o el kilogramo, pero para el valor: sin una unidad común, cada comparación de precios exigiría convertir mentalmente entre decenas de bienes distintos.

Cualquier objeto que cumpla razonablemente bien estas tres funciones puede actuar como dinero, y a lo largo de la historia la humanidad ha usado cosas muy distintas para este propósito: conchas, sal, ganado, piedras talladas, plumas, tabaco y, sobre todo, metales.

El problema del trueque

Antes de que existiera el dinero tal y como lo conocemos, el intercambio se hacía mediante trueque: yo te doy grano, tú me das una cabra. El trueque funciona en comunidades pequeñas, pero se rompe rápidamente a medida que la sociedad crece, por un problema que los economistas llaman la "doble coincidencia de necesidades". Para que un intercambio ocurra, no basta con que yo quiera lo que tú tienes; también hace falta que tú quieras exactamente lo que yo tengo, en el momento adecuado y en la cantidad adecuada. Si yo soy pescador y quiero zapatos, tengo que encontrar a un zapatero que, precisamente ese día, quiera pescado. Si no lo hay, no hay intercambio.

Además, el trueque tiene otros problemas: muchos bienes no se pueden dividir con facilidad (no puedes pagar media cabra), no todos los bienes se conservan bien con el tiempo (el pescado se pudre) y no existe una forma sencilla de comparar el valor de cosas muy distintas entre sí. El dinero nace, precisamente, para resolver estos problemas.

El dinero mercancía

La primera solución que encontraron las civilizaciones antiguas fue elegir un bien concreto, aceptado por todos dentro de una comunidad, para que hiciera de intermediario en los intercambios. A este tipo de dinero se le llama dinero mercancía, porque el propio objeto que circula como dinero tiene, además, un valor de uso por sí mismo.

Se han usado como dinero mercancía la sal en buena parte del mundo antiguo (de ahí viene la palabra "salario"), el ganado en muchas culturas pastoriles, las conchas de cauri en África y Asia, el cacao entre los pueblos mesoamericanos, y muchos otros bienes locales. Con el tiempo, casi todas las civilizaciones convergieron en el mismo tipo de bien para este propósito: los metales preciosos, especialmente el oro y la plata.

Por qué el oro ganó la partida

El oro no fue elegido al azar. Tiene un conjunto de propiedades que lo hacen extraordinariamente bueno como dinero, y entender estas propiedades es clave, porque más adelante veremos que Bitcoin fue diseñado deliberadamente para imitarlas en el mundo digital.

- Escasez: no se puede fabricar oro de la nada; hay que extraerlo, y su cantidad total en el planeta es limitada. Es la diferencia entre una obra de arte original, que vale porque solo existe una, y una fotocopia, que cualquiera puede producir en cantidad ilimitada: el oro se acerca más a lo primero que cualquier otro material abundante en la naturaleza.
- Durabilidad: el oro no se oxida ni se degrada con el tiempo; una moneda de oro de hace dos mil años sigue siendo oro hoy. Comparado con el trigo, que se pudre en meses, o con el hierro, que se oxida en años, el oro es prácticamente eterno a escala humana.
- Divisibilidad: se puede fundir y dividir en piezas más pequeñas sin perder valor proporcional. Un lingote se puede convertir en cien monedas de igual peso, cada una con la centésima parte exacta del valor original, algo que no se puede hacer con una vaca o una casa.
- Fungibilidad: un gramo de oro puro vale lo mismo que cualquier otro gramo de oro puro, sin importar su origen o su forma. Es como el agua embotellada de una misma marca:

da igual qué botella concreta te den, todas son intercambiables entre sí sin que a nadie le importe cuál en particular recibe.

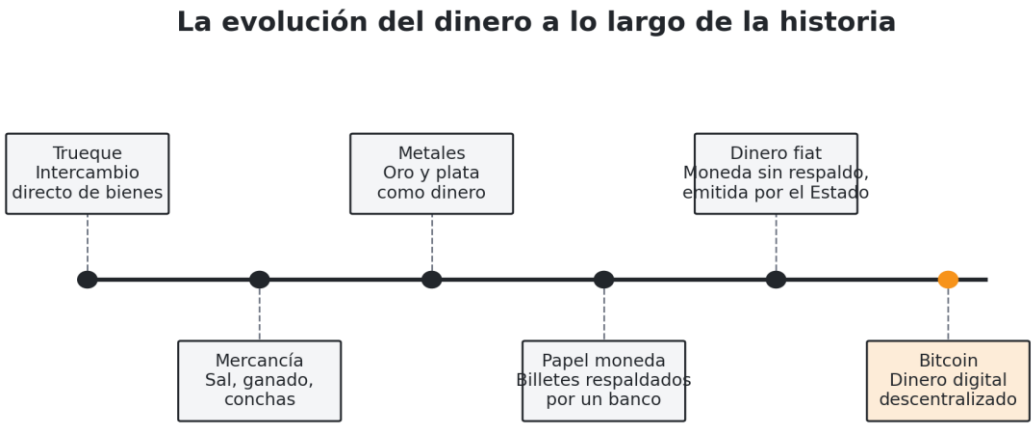
- Portabilidad: comparado con el ganado o la sal, es fácil de transportar porque concentra mucho valor en poco peso. Un puñado de monedas de oro puede representar el valor de varias vacas, sin necesidad de arrear un rebaño para pagar una deuda.
- Verificabilidad: existen formas relativamente sencillas de comprobar su pureza y autenticidad, por ejemplo mediante su densidad, su color o pruebas químicas sencillas, lo que dificulta (aunque no elimina del todo) la falsificación.

Estas seis propiedades —escasez, durabilidad, divisibilidad, fungibilidad, portabilidad y verificabilidad— se conocen en economía como las propiedades del "buen dinero" (sound money). Cuanto mejor cumple un bien estas propiedades, mejor funciona como dinero a largo plazo.

De las monedas al papel

Transportar y pesar oro en cada transacción era incómodo y arriesgado, así que las sociedades avanzaron hacia formas más prácticas. Primero aparecieron las monedas acuñadas por autoridades que garantizaban su peso y pureza, lo que redujo la necesidad de pesar y verificar el metal en cada intercambio. Más adelante, orfebres y bancos empezaron a emitir recibos de papel que representaban una cantidad de oro depositada en sus cámaras acorazadas. Esos recibos —los primeros billetes— eran mucho más fáciles de transportar que el metal físico, y con el tiempo la gente empezó a intercambiar directamente los recibos en lugar de ir a buscar el oro que representaban.

Este fue un paso importante: por primera vez, el dinero que circulaba en la calle no era en sí mismo el bien escaso y valioso, sino una promesa —un derecho a canjear ese papel por oro real en cualquier banco emisor—. A este sistema se le llama patrón oro, y funcionó, con distintas variantes, durante gran parte de los siglos XIX y XX.



La evolución del dinero a lo largo de la historia: del trueque al dinero digital.

La ruptura del patrón oro

El patrón oro imponía una disciplina importante a los gobiernos: no podían imprimir más billetes de los que podían respaldar con el oro que tenían guardado. Esto limitaba su

capacidad de gastar más de lo que ingresaban. Durante el siglo XX, sobre todo en los periodos de guerra y de crisis económica, muchos gobiernos encontraron este límite demasiado incómodo.

Estados Unidos suspendió parcialmente la convertibilidad interna del dólar en oro en 1933, y en 1971 el presidente Richard Nixon anunció el cierre definitivo de la "ventanilla del oro": desde ese momento, el dólar —y con él, indirectamente, buena parte de las monedas del mundo, que estaban ancladas al dólar— dejó de estar respaldado por ningún bien físico. Nació así lo que hoy llamamos dinero fiat, del latín "que así sea": dinero que tiene valor porque una autoridad lo declara de curso legal y porque la sociedad confía en que otros lo aceptarán, pero que ya no representa ningún derecho sobre un bien escaso.

El dinero fiat: ventajas y problemas

El dinero fiat moderno tiene ventajas evidentes: es cómodo, es aceptado universalmente dentro de cada país, y da a los bancos centrales herramientas para intentar suavizar las crisis económicas, bajando tipos de interés o inyectando liquidez en momentos difíciles. Gracias a él, los gobiernos han podido financiar guerras, rescates bancarios y programas sociales sin depender de las reservas físicas de un metal.

Pero también tiene un problema estructural: al no estar limitado por ningún recurso físico escaso, su cantidad depende enteramente de la voluntad de quien lo emite. Un banco central puede, en principio, crear tanto dinero nuevo como decida, y la historia está llena de ejemplos de gobiernos que, ante la tentación de financiar su gasto imprimiendo dinero en lugar de subir impuestos o pedir préstamos, terminaron generando inflaciones muy altas o incluso hiperinflaciones que destruyeron los ahorros de su población: la Alemania de Weimar en los años veinte, Hungría tras la Segunda Guerra Mundial, Zimbabue en la década de 2000 o Venezuela en la de 2010 son ejemplos citados con frecuencia.

Incluso en economías consideradas estables, la erosión del poder adquisitivo del dinero fiat es constante: un euro o un dólar de hace treinta años compraba muchas más cosas que uno de hoy. Esta pérdida gradual de valor, la inflación, es en cierto modo un impuesto invisible que afecta especialmente a quienes guardan su dinero en efectivo o en cuentas de bajo rendimiento, en lugar de invertirlo.

> *La pregunta que llevó a la creación de Bitcoin no fue "¿cómo hacemos el dinero más cómodo?", sino "¿es posible crear un dinero tan escaso y fiable como el oro, pero que funcione con la velocidad y la comodidad de internet?".*

Lo que Bitcoin intenta recuperar

Con esta perspectiva histórica en la cabeza, Bitcoin empieza a cobrar sentido antes incluso de explicar una sola línea de su funcionamiento técnico. Sus creadores y primeros defensores lo describieron, desde el principio, como un intento de devolver al dinero las propiedades del oro —escasez verificable, resistencia a la manipulación, independencia de cualquier autoridad central— pero llevándolas al terreno digital, donde el dinero pueda moverse a la velocidad de un correo electrónico, a cualquier parte del mundo, sin pedir permiso a ningún intermediario.

En los próximos capítulos veremos por qué esto no era tan sencillo como parece —por qué copiar un archivo digital es trivial, pero copiar dinero digital sin que pierda su escasez es un

problema que desafió a la informática durante décadas— y cómo un conjunto de ideas de criptografía, combinadas de una manera nueva, terminaron resolviéndolo.

Capítulo 2. El problema del dinero digital y los intentos anteriores a Bitcoin

Cuando internet empezó a popularizarse en los años noventa, resultó evidente casi de inmediato que hacía falta una forma de dinero pensada para ese nuevo entorno. Enviar un correo electrónico era instantáneo y gratuito; enviar dinero a otra persona seguía dependiendo de bancos, comisiones y días de espera. Durante casi veinte años, algunos de los mejores criptógrafos e informáticos del mundo intentaron resolver este problema, y sus fracasos e ideas parciales son, en realidad, los cimientos sobre los que se construyó Bitcoin.

El problema del doble gasto

Cualquier archivo digital —una foto, un documento, una canción— se puede copiar de forma perfecta e infinita sin ningún coste. Esta propiedad, maravillosa para compartir información, es catastrófica si se intenta usar para representar dinero. Si el dinero fuera simplemente un archivo digital, cualquiera podría copiarlo y gastarlo dos veces, tres veces o las que quisiera: enviárselo a un vendedor por una compra y, acto seguido, enviar esa misma copia a otro vendedor para otra compra distinta. A este problema se le conoce como el "doble gasto" (double spending), y durante décadas fue considerado el obstáculo central para crear dinero verdaderamente digital.

La solución tradicional al doble gasto es tener un tercero de confianza —normalmente un banco— que lleve un registro central de quién tiene cuánto dinero, y que reste el importe de la cuenta del emisor cada vez que se hace un pago, impidiendo que ese mismo dinero se use dos veces. Esto funciona, pero exige confiar en esa entidad central: que no manipule el registro, que no sea hackeada, que no censure pagos que no le gusten y que no quiebre llevándose los ahorros de la gente. La pregunta que se hicieron los primeros criptógrafos fue: ¿es posible resolver el doble gasto sin depender de ningún tercero de confianza?

DigiCash: la primera gran promesa (1989)

El criptógrafo David Chaum fue pionero en este campo. En 1989 fundó DigiCash, una empresa que desarrolló un sistema de dinero digital llamado ecash, basado en una técnica criptográfica inventada por el propio Chaum llamada "firma ciega" (blind signature). Esta técnica permitía que un banco emitiera dinero digital verificable sin poder ver los detalles de cada transacción concreta, lo que ofrecía a los usuarios un nivel de privacidad notable, similar al del dinero en efectivo.

DigiCash llegó a firmar acuerdos con bancos importantes y generó gran expectación en la prensa tecnológica de la época. Sin embargo, el sistema seguía dependiendo de un servidor central operado por la propia empresa para validar cada transacción y evitar el doble gasto. Ese punto central lo hacía frágil: bastaba con que DigiCash quebrara —como ocurrió en 1998, tras no conseguir la adopción masiva que esperaba— para que todo el sistema dejara de funcionar. Además, dependía de que los bancos quisieran integrarlo, y la mayoría prefirió no hacerlo.

B-money y Bit Gold: las ideas que faltaban

A finales de los noventa, dos propuestas teóricas, nunca implementadas completamente en su momento, se acercaron mucho más a lo que después sería Bitcoin.

En 1998, el criptógrafo Wei Dai publicó la descripción de "b-money", un sistema en el que los propios participantes de la red, y no un banco central, mantendrían un registro compartido de cuánto dinero tenía cada uno. Dai proponía que crear nuevo dinero exigiera resolver problemas computacionales costosos —una idea que anticipaba lo que Bitcoin llamaría más tarde "prueba de trabajo"— y que las disputas se resolvieran mediante depósitos y contratos entre los propios usuarios.

Casi al mismo tiempo, el científico informático Nick Szabo diseñó "bit gold", un sistema en el que los participantes resolverían problemas criptográficos difíciles (lo que él llamó "cadenas de prueba de trabajo") y el resultado de cada problema resuelto se encadenaría criptográficamente con el siguiente, creando un registro cada vez más difícil de alterar. Szabo, de hecho, había reflexionado extensamente sobre por qué el oro funcionó como dinero durante milenios, y bit gold era su intento explícito de replicar esas propiedades —sobre todo la escasez verificable y el coste real de producción— en formato digital.

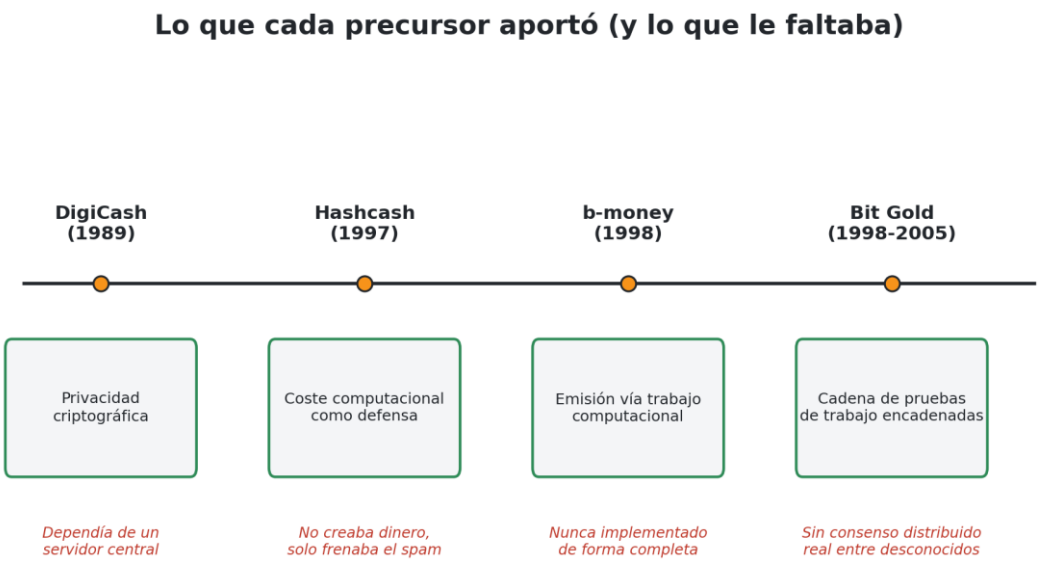
Tanto b-money como bit gold compartían una limitación crucial: ninguno de los dos resolvía de forma completa y práctica cómo lograr que una red de ordenadores repartidos por el mundo, sin conocerse ni confiar entre sí, se pusiera de acuerdo sobre un único registro válido, sin que nadie pudiera hacer trampas. A este problema, más general, los informáticos lo llaman el "problema de los generales bizantinos" o, de forma más técnica, el problema de alcanzar consenso distribuido en presencia de participantes que pueden actuar de mala fe.

La analogía que da nombre a este problema, propuesta en 1982 por los investigadores Leslie Lamport, Robert Shostak y Marshall Pease, imagina varios generales del ejército bizantino rodeando una ciudad enemiga, cada uno al mando de una división situada en un punto distinto. Para ganar, todos los generales deben atacar exactamente al mismo tiempo, o todos deben retirarse a la vez: un ataque parcial sería una derrota segura. El problema es que solo pueden comunicarse mediante mensajeros que tardan en llegar y que podrían perderse, y que, además, uno o varios generales podrían ser traidores que envían mensajes contradictorios a propósito, diciéndole a unos "atacad" y a otros "retirad" para sembrar el caos. La pregunta que plantea el problema es si existe algún procedimiento que permita a los generales leales ponerse de acuerdo de forma fiable, a pesar de los mensajeros lentos y de los traidores que intentan confundirlos. Trasladado a Bitcoin, cada "general" es un nodo de la red, cada "mensajero" es la comunicación por internet (que también puede retrasarse o fallar), y los "traidores" son participantes que intentan hacer trampas -por ejemplo, gastando el mismo dinero dos veces-. La prueba de trabajo que describiremos en el capítulo 11 es, precisamente, el mecanismo que Bitcoin usa para que miles de "generales" desconocidos entre sí logren, por fin, ponerse de acuerdo.

Hashcash: el coste como defensa

Otra pieza clave llegó en 1997 de la mano del criptógrafo británico Adam Back, con un sistema llamado Hashcash. La idea original de Hashcash no era crear dinero, sino combatir el correo basura (spam): obligaba a que cada correo electrónico llevara adjunta la solución a un pequeño problema matemático costoso de calcular, pero fácil de verificar. Para una persona que envía pocos correos, este coste computacional es insignificante; para alguien que intenta enviar millones de mensajes de spam, el coste acumulado se vuelve prohibitivo.

El mecanismo de Hashcash —exigir una prueba de esfuerzo computacional real, verificable en un instante por cualquiera— es, en esencia, el mismo principio que después se conocería como "prueba de trabajo" (proof of work), y se convertiría en el corazón del mecanismo de minería de Bitcoin, como veremos en detalle más adelante en este libro.



Cada precursor de Bitcoin resolvió una parte del problema, pero ninguno logró resolverlas todas a la vez.

Por qué ninguno llegó a cuajar

Mirando en retrospectiva, cada uno de estos proyectos aportó una pieza del rompecabezas: DigiCash resolvió la privacidad y la validación criptográfica de las monedas; b-money y bit gold plantearon la idea de crear dinero mediante trabajo computacional verificable, sin banco central; Hashcash demostró que se podía usar el coste computacional como una defensa práctica y funcional contra el abuso. Pero a ninguno de ellos se le ocurrió, o no consiguió implementar con éxito, la pieza que faltaba: un mecanismo por el cual miles de ordenadores desconocidos entre sí, repartidos por todo el planeta, pudieran ponerse de acuerdo sobre un único historial de transacciones válido, de forma automática, sin necesidad de que nadie confiara en nadie y sin que existiera ningún punto central que pudiera fallar, ser hackeado o ser cerrado por un gobierno.

Esta combinación —red descentralizada, prueba de trabajo como mecanismo de creación y de defensa, y un método para que la red completa se pusiera de acuerdo sobre qué transacciones son válidas— es precisamente lo que resolvió el documento que analizaremos en el capítulo 5: el whitepaper de Bitcoin, publicado en 2008 bajo el seudónimo de Satoshi Nakamoto. Antes de llegar allí, en el próximo capítulo repasaremos las herramientas de criptografía básica que hacen posible todo esto, para que ningún concepto técnico posterior resulte oscuro.

Una pieza más: la lista de correo cypherpunk como caldo de cultivo

Ninguno de estos proyectos surgió de forma aislada: DigiCash, b-money, bit gold y Hashcash compartían un mismo ecosistema intelectual, la lista de correo electrónico "cypherpunks", activa desde 1992, en la que un grupo internacional de criptógrafos, programadores y

activistas de la privacidad discutía abiertamente, año tras año, cómo usar la criptografía para proteger la libertad individual frente al poder de gobiernos y corporaciones, un tema que retomaremos con más detalle en el capítulo 4. Esta lista de correo no era un grupo académico formal ni una empresa, sino una comunidad informal y descentralizada por naturaleza -de forma casi profética respecto a lo que después construiría Bitcoin-, en la que las ideas se probaban, se criticaban sin miramientos y, en la mayoría de los casos, se abandonaban tras detectarse algún defecto insalvable. Es precisamente en esa lista de correo donde Satoshi Nakamoto anunció, en octubre de 2008, el whitepaper de Bitcoin, y donde b-money de Wei Dai había circulado una década antes: no fue casualidad que Nakamoto citara explícitamente el trabajo de Dai y de Szabo en su propio documento técnico, como veremos en el capítulo 5, sino el reconocimiento directo de una conversación colectiva que llevaba cerca de veinte años en marcha antes de que Bitcoin lograra, por fin, cerrar el círculo que ninguno de sus precursores había conseguido cerrar por completo.

Fuentes y estudios citados en este capítulo

- Chaum, D. (1983). "Blind Signatures for Untraceable Payments". Advances in Cryptology, Proceedings of Crypto '82. El artículo que introdujo la técnica de firma ciega usada por DigiCash.
- Dai, W. (1998). "b-money". Propuesta original distribuida en la lista de correo cypherpunks, citada explícitamente en el whitepaper de Nakamoto.
- Szabo, N. (2005). "Bit Gold". Ensayo publicado en su blog personal, ampliamente considerado un precursor conceptual directo de Bitcoin.
- Back, A. (2002). "Hashcash - A Denial of Service Counter-Measure". Documento técnico que formaliza el sistema propuesto originalmente por Back en 1997.
- Lamport, L., Shostak, R., Pease, M. (1982). "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems, 4(3). El artículo académico que formalizó el problema de consenso distribuido que da nombre a la analogía de este capítulo.

Capítulo 3. Criptografía básica para entender Bitcoin

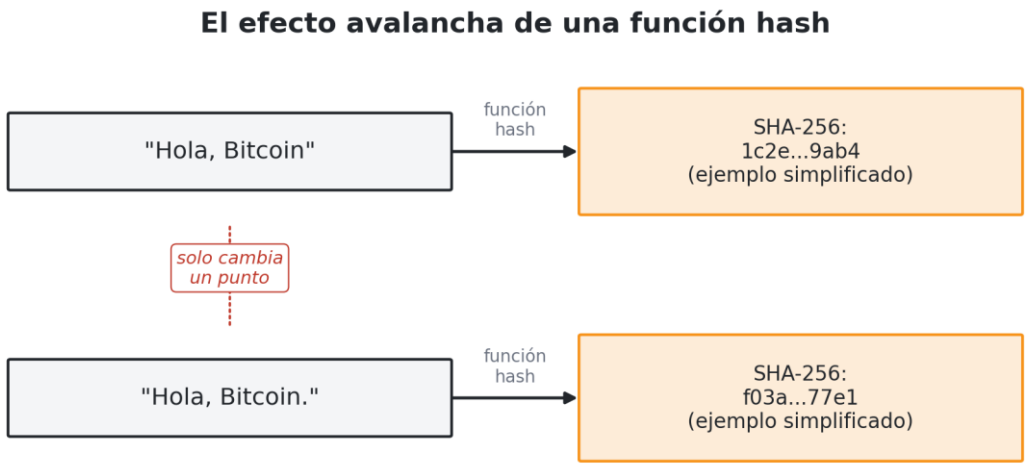
La palabra "criptografía" asusta a muchas personas que se acercan por primera vez a Bitcoin, pero las ideas que hacen falta para entenderlo son, en realidad, bastante intuitivas si se explican con calma. Este capítulo cubre solo dos herramientas —las funciones hash y la criptografía de clave pública— porque son las dos piezas matemáticas sobre las que se construye absolutamente todo lo demás en este libro. No hace falta ningún conocimiento matemático previo: basta con entender qué hacen estas herramientas y qué propiedades garantizan.

Las funciones hash: huellas digitales de la información

Una función hash es, en esencia, una máquina que recibe cualquier cantidad de información —una palabra, una foto, un libro entero— y devuelve siempre una salida de longitud fija, algo así como "una huella digital" de esa información. Bitcoin usa principalmente una función hash llamada SHA-256, que siempre produce una salida de 256 bits, representada habitualmente como una cadena de 64 caracteres (letras y números).

Estas funciones tienen tres propiedades que las hacen extraordinariamente útiles.

- Determinismo: la misma entrada produce siempre exactamente la misma salida. Si dos personas calculan el hash del mismo archivo, obtienen el mismo resultado, sin importar en qué ordenador, país o momento lo hagan, lo que permite usar el hash como una especie de matrícula única y verificable para cualquier dato.
- Efecto avalancha: un cambio mínimo en la entrada —incluso una sola letra o un solo punto— produce una salida completamente distinta e impredecible. No hay ninguna relación visible entre entradas parecidas y sus hashes, de modo que ver dos hashes no permite adivinar si las entradas que los generaron eran parecidas o completamente distintas.
- Unidireccionalidad: es extremadamente fácil calcular el hash de una entrada, pero es, a efectos prácticos, imposible hacer el camino inverso: a partir de un hash, no hay forma de reconstruir la entrada original salvo probando entradas una por una (lo que con SHA-256 llevaría más tiempo que la edad del universo). Una analogía habitual es la de una picadora de carne: es trivial convertir un filete en carne picada, pero no existe ningún procedimiento para devolver la carne picada a su forma original de filete; una función hash hace, matemáticamente, algo parecido con la información.



El efecto avalancha: una entrada casi idéntica produce salidas totalmente distintas.

Para qué sirven las funciones hash en Bitcoin

Estas propiedades, que pueden parecer una curiosidad matemática, resuelven varios problemas prácticos muy concretos que veremos en detalle en capítulos posteriores.

- Permiten comprobar que un archivo o un bloque de datos no ha sido alterado: basta con volver a calcular su hash y compararlo con el original. Si coincide, el contenido es idéntico; si no coincide, algo ha cambiado, del mismo modo que un precinto de seguridad roto en un paquete te avisa, sin que tengas que revisar todo el contenido, de que alguien lo ha abierto por el camino.
- Permiten encadenar bloques de información de forma que alterar un bloque antiguo obligue a recalcular también todos los bloques posteriores, algo que —como veremos— resulta extremadamente costoso en la red de Bitcoin. Es como una torre de fichas de dominó numeradas en las que cada ficha lleva grabado el número de la anterior: cambiar una ficha del medio obliga a regrabar y sustituir también todas las que vienen después para que la numeración vuelva a encajar.
- Sirven de base para el mecanismo de minería, donde los mineros deben encontrar, mediante prueba y error, una entrada cuyo hash cumpla una condición concreta (por ejemplo, empezar por una cierta cantidad de ceros). No existe ningún atajo para acertar a la primera: hay que probar millones de combinaciones, de forma parecida a marcar números al azar en una máquina tragaperras hasta que sale la combinación ganadora.
- Permiten resumir grandes cantidades de transacciones en un único valor mediante una estructura llamada árbol de Merkle, que estudiaremos en el capítulo 7, de forma parecida a como un único código de barras en la caja de un supermercado puede representar, de manera verificable, el contenido completo de esa caja sin tener que abrirla y listar cada producto por separado.

Criptografía de clave pública: firmar sin revelar el secreto

La segunda herramienta es la criptografía de clave pública (o criptografía asimétrica), desarrollada de forma pública en los años setenta por investigadores como Whitfield Diffie,

Martin Hellman y, poco después, Ronald Rivest, Adi Shamir y Leonard Adleman. Su idea central resulta, la primera vez que se escucha, casi mágica: es posible generar un par de números matemáticamente relacionados —una clave privada y una clave pública— de tal manera que:

- Cualquier cosa firmada con la clave privada se puede verificar públicamente usando la clave pública correspondiente, sin que nadie necesite conocer la clave privada. Esto permite demostrar autoría sin exponer el secreto, algo imposible con una firma manuscrita tradicional, que cualquiera podría intentar imitar con más o menos éxito.
- A partir de la clave pública es, a efectos prácticos, imposible deducir la clave privada, aunque ambas estén matemáticamente relacionadas. La relación funciona en una sola dirección, como mezclar pintura: es fácil combinar dos colores para obtener un tercero, pero, mirando el color resultante, no hay forma de saber con certeza qué dos colores exactos se mezclaron para producirlo.
- Cualquiera puede comprobar que una firma es válida, pero solo quien conoce la clave privada puede generar esa firma, de la misma manera que cualquiera puede comprobar si un sello encaja perfectamente en un documento, aunque solo el dueño del sello original pueda producir esa marca exacta.

Bitcoin utiliza una variante concreta de esta tecnología llamada criptografía de curva elíptica (en concreto, la curva secp256k1), que ofrece el mismo tipo de garantías que otros esquemas de clave pública más conocidos, pero con claves más cortas y cálculos más eficientes. No hace falta entender la matemática de las curvas elípticas para seguir este libro: basta con quedarse con la idea de que existe una clave privada secreta, una clave pública derivada de ella que se puede compartir sin ningún riesgo, y un mecanismo de firma que demuestra que alguien conoce esa clave privada sin tener que revelarla nunca.

La analogía del candado y las dos llaves

Una forma útil de visualizar esto es imaginar un candado especial que se puede cerrar con una llave y abrir con otra llave distinta. Tú fabricas miles de copias de la "llave de abrir" (tu clave pública) y las repartes libremente a todo el mundo: en tu web, en tu tarjeta de visita, donde quieras. Guardas la "llave de cerrar" (tu clave privada) en un lugar absolutamente seguro y no se la enseñas a nadie.

Cuando quieres demostrar que un mensaje viene realmente de ti, lo "cierras" con tu llave secreta. Cualquiera que tenga una copia de tu llave pública puede comprobar que ese cierre encaja perfectamente y, por tanto, que solo pudo hacerlo alguien que tuviera la llave secreta correspondiente —es decir, tú—. Nadie necesita ver tu llave secreta para confiar en la firma; solo necesita la llave pública, que es información que puedes compartir sin ningún temor.

Esta es exactamente la lógica que usa Bitcoin para demostrar la propiedad del dinero: cuando gastas tus bitcoins, firmas la transacción con tu clave privada, y cualquier nodo de la red puede verificar, usando tu clave pública, que la firma es auténtica y que, por tanto, tienes derecho a gastar ese dinero, sin que tu clave privada tenga que salir nunca de tu dispositivo.

Firma digital ≠ cifrado

Conviene aclarar una confusión muy habitual: firmar digitalmente algo no significa ocultarlo. Las transacciones de Bitcoin son completamente públicas y visibles para cualquiera; lo que

aporta la firma digital no es privacidad, sino autenticidad e integridad: la certeza matemática de que una transacción concreta solo pudo haber sido autorizada por quien controla la clave privada correspondiente, y que nadie ha podido modificarla después de ser firmada, porque cualquier alteración, por mínima que sea, invalidaría la firma.

> *Con estas dos herramientas en la mochila —funciones hash y firmas de clave pública— ya tenemos todo lo necesario para entender, sin ninguna caja negra, cómo funciona Bitcoin por dentro. El resto es, sorprendentemente, una combinación ingeniosa de estas mismas ideas.*

Fuentes y estudios citados en este capítulo

- Diffie, W., Hellman, M. (1976). "New Directions in Cryptography". IEEE Transactions on Information Theory, 22(6). El artículo fundacional de la criptografía de clave pública.
- Rivest, R., Shamir, A., Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, 21(2). El artículo que presentó el algoritmo RSA.
- National Institute of Standards and Technology (NIST). FIPS PUB 180-4, "Secure Hash Standard (SHS)". Estándar oficial que define, entre otras, la familia de funciones hash SHA-256 usada por Bitcoin.
- Certicom Research (2010). "SEC 2: Recommended Elliptic Curve Domain Parameters". Documento que especifica la curva secp256k1 utilizada por Bitcoin.

En el próximo capítulo dejaremos la teoría y entraremos en la historia concreta: el contexto de crisis financiera global en el que apareció Bitcoin, y quién —o quiénes— estaban detrás del seudónimo que lo hizo posible.

PARTE II

ORIGEN Y FUNDAMENTOS DE BITCOIN

Capítulo 4. La crisis de 2008 y el terreno abonado para Bitcoin

Bitcoin no nació en el vacío. Apareció en octubre de 2008, en pleno epicentro de la peor crisis financiera global desde la Gran Depresión, y esa coincidencia no fue casual: fue, según todos los indicios, la motivación directa de su creación. Para entender por qué Bitcoin despertó tanto interés entre quienes desconfiaban del sistema financiero tradicional, hace falta repasar, aunque sea brevemente, qué ocurrió aquel año.

La burbuja inmobiliaria y las hipotecas subprime

Durante los años previos a 2008, especialmente en Estados Unidos, los bancos concedieron un volumen enorme de hipotecas a personas con escasa capacidad real de pago, las llamadas hipotecas "subprime". Estas hipotecas se agrupaban después en paquetes financieros complejos —titulizaciones y derivados con nombres como CDO (obligaciones de deuda garantizada)— que se vendían a inversores de todo el mundo con calificaciones de riesgo, otorgadas por las agencias de calificación, que resultaron ser muy optimistas.

Mientras los precios de la vivienda subían, el sistema parecía funcionar: quien no podía pagar su hipoteca simplemente vendía la casa, que valía más que cuando la compró, y saldaba la deuda. El problema apareció cuando los precios de la vivienda dejaron de subir y empezaron a caer: de repente, millones de propietarios debían más de lo que valía su casa, los impagos se dispararon y el valor de todos esos paquetes financieros complejos se desplomó, arrastrando a los bancos e inversores que los tenían en sus balances.

La caída de Lehman Brothers

El símbolo más recordado de la crisis es la quiebra del banco de inversión Lehman Brothers, el 15 de septiembre de 2008, hasta entonces uno de los mayores bancos de Estados Unidos. Su colapso desató el pánico en los mercados financieros de todo el mundo: los bancos dejaron de fiarse unos de otros y de prestarse dinero entre sí, el crédito se congeló, las bolsas se hundieron y varias instituciones financieras de primer nivel estuvieron al borde del colapso en cuestión de días.

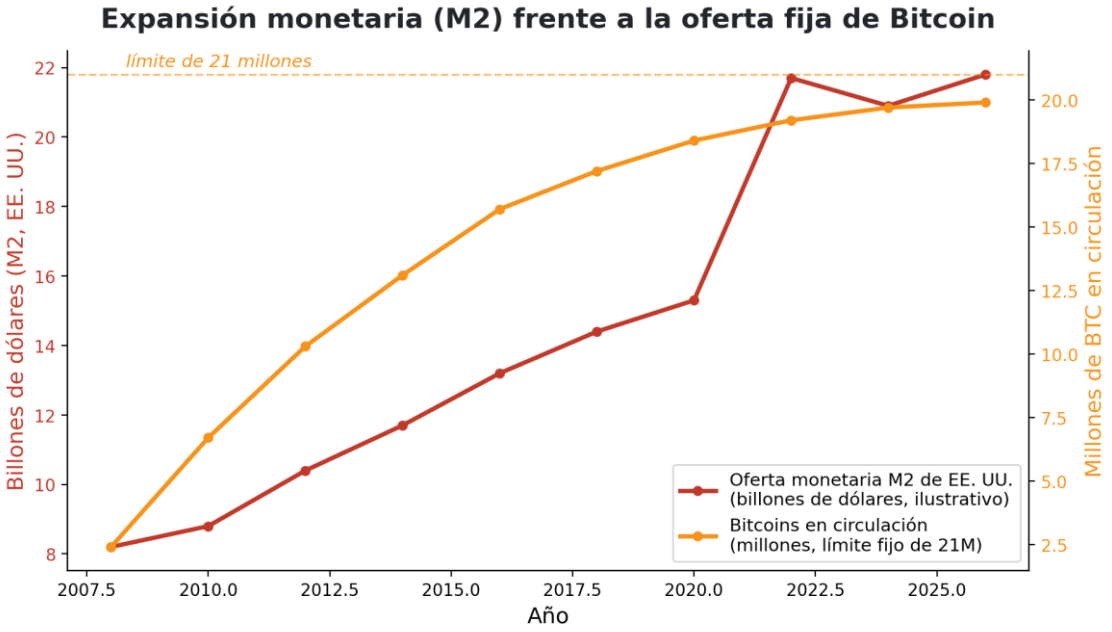
Los rescates bancarios ("bailouts")

Ante el riesgo de un colapso sistémico que arrastrara a toda la economía mundial, los gobiernos —empezando por el de Estados Unidos, con el Programa de Alivio de Activos en Problemas (TARP), dotado con setecientos mil millones de dólares— decidieron rescatar a numerosos bancos y aseguradoras con dinero público. El razonamiento oficial era que estas instituciones eran "demasiado grandes para caer" (too big to fail): su quiebra habría provocado un daño tan enorme al conjunto de la economía que el coste de rescatarlas, por elevado que fuera, resultaba menor.

Lo que generó una indignación duradera en amplios sectores de la población fue la asimetría de este rescate: los mismos bancos y ejecutivos cuyas decisiones de riesgo habían provocado la crisis fueron rescatados con dinero de todos los contribuyentes, mientras millones de familias corrientes perdían sus casas, sus ahorros y sus empleos sin recibir ninguna ayuda comparable. Muchos ejecutivos de los bancos rescatados, además, siguieron cobrando bonificaciones millonarias poco después del rescate, lo que profundizó la sensación de injusticia.

La respuesta de los bancos centrales

Para intentar reactivar la economía, los bancos centrales de todo el mundo —la Reserva Federal estadounidense a la cabeza— bajaron los tipos de interés hasta casi cero y pusieron en marcha programas masivos de compra de activos conocidos como "flexibilización cuantitativa" (quantitative easing), que en la práctica supusieron crear enormes cantidades de dinero nuevo para inyectarlo en el sistema financiero. Estas políticas evitaron, según la mayoría de los análisis, un colapso económico todavía peor, pero también alimentaron la desconfianza de quienes veían en ellas una forma más de "imprimir dinero" para tapar los problemas del sistema, con el riesgo de devaluar el ahorro de la gente corriente a largo plazo.



Cifras de M2 ilustrativas, con fines comparativos; no representan una serie oficial exacta.

La expansión de la masa monetaria frente a la oferta fija de Bitcoin, el contraste que motivó a sus primeros defensores.

Un caldo de cultivo ideológico

Esta combinación de factores —bancos rescatados con dinero público tras haber tomado riesgos excesivos, ejecutivos que apenas rindieron cuentas, bancos centrales creando dinero a gran escala y millones de familias perdiendo su patrimonio— generó una profunda desconfianza hacia las instituciones financieras tradicionales y hacia la capacidad (o la voluntad) de los gobiernos de gestionar el dinero de forma responsable. En ese ambiente de indignación y búsqueda de alternativas, un pequeño grupo de programadores, criptógrafos y economistas libertarios —muchos de ellos vinculados a un colectivo de correo electrónico llamado "cypherpunks", que desde los años noventa defendía el uso de la criptografía como herramienta de libertad individual frente al poder de gobiernos y corporaciones— llevaba años buscando la manera de crear un dinero que no dependiera de ninguna institución central.

El mensaje escondido en el primer bloque

El 3 de enero de 2009, cuando se creó el primer bloque de la cadena de Bitcoin —conocido como el "bloque génesis"—, su creador incluyó dentro de los datos del bloque un texto que no tenía ninguna función técnica, pero que funcionaba como una declaración de intenciones inequívoca. El texto, extraído literalmente de la portada del periódico británico The Times de ese mismo día, decía:

> *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" ("El Canciller al borde de un segundo rescate para los bancos").*

Este mensaje cumplía dos funciones: demostraba de forma verificable que el bloque no se había creado antes de esa fecha (porque incluía una noticia real de ese día concreto) y, al mismo tiempo, dejaba constancia explícita de la motivación detrás del proyecto: Bitcoin nacía como una alternativa al sistema en el que los bancos centrales y los gobiernos podían rescatar bancos, devaluar el ahorro de la gente e imprimir dinero según su propio criterio, sin que los ciudadanos tuvieran ninguna forma de protegerse ni de participar en esa decisión.

Con este contexto ya claro, en el próximo capítulo veremos quién publicó, apenas unos meses antes de ese primer bloque, el documento técnico que hizo posible todo esto: el whitepaper de Bitcoin, firmado por un autor —o autores— que se ocultaron tras el nombre Satoshi Nakamoto y cuya identidad real sigue siendo, hoy en día, un misterio sin resolver.

Fuentes y estudios citados en este capítulo

- Financial Crisis Inquiry Commission (2011). "The Financial Crisis Inquiry Report". Informe oficial encargado por el Congreso de Estados Unidos para investigar las causas de la crisis financiera de 2008.
- Reinhart, C., Rogoff, K. (2009). "This Time Is Different: Eight Centuries of Financial Folly". Princeton University Press. Estudio de referencia sobre la historia de las crisis financieras y bancarias.
- Reserva Federal de Estados Unidos, actas e informes públicos sobre los programas de flexibilización cuantitativa (quantitative easing) iniciados a partir de 2008.

Capítulo 5. Satoshi Nakamoto y el whitepaper de Bitcoin

El 31 de octubre de 2008, en plena tormenta financiera mundial, alguien que firmaba como Satoshi Nakamoto envió un correo electrónico a una lista de distribución de criptografía llamada "The Cryptography Mailing List", frecuentada por buena parte de los especialistas más avanzados del mundo en esta materia. El mensaje incluía un enlace a un documento de nueve páginas titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin: un sistema de dinero electrónico peer-to-peer). Ese documento, hoy conocido simplemente como "el whitepaper", es el acta de nacimiento de Bitcoin.

Quién era Satoshi Nakamoto

La identidad real de Satoshi Nakamoto sigue siendo, más de quince años después, uno de los grandes misterios de la tecnología moderna. Se sabe que se comunicaba en un inglés impecable, con expresiones tanto británicas como americanas mezcladas, lo que ha dado pie a especulaciones de todo tipo. Participó activamente en foros y en el desarrollo del software durante poco más de dos años, escribiendo con otros primeros colaboradores como Hal Finney -un reconocido criptógrafo que fue la primera persona, aparte del propio Nakamoto, en ejecutar el software de Bitcoin y en recibir una transacción-, hasta que, a finales de 2010, empezó a reducir su actividad, y en abril de 2011 escribió su último mensaje conocido, en el que decía que había "pasado a otras cosas" y dejaba el proyecto en manos de la comunidad de desarrolladores que ya se había formado a su alrededor.

Numerosos periodistas, investigadores y libros han intentado identificar a la persona (o al grupo de personas) detrás del seudónimo, señalando a diversos candidatos a lo largo de los años -entre ellos Hal Finney, Nick Szabo (cuyas ideas sobre "bit gold" se mencionaron en el capítulo 2) o el empresario Craig Wright, que llegó a reclamar públicamente ser Satoshi Nakamoto, una afirmación que no ha logrado sostener con pruebas criptográficas convincentes y que fue rechazada en varios procesos judiciales-. A día de hoy, ninguna de estas hipótesis cuenta con pruebas concluyentes generalmente aceptadas, y la identidad de Nakamoto sigue sin confirmarse.

Se estima, a partir del análisis de las primeras direcciones de la red, que Satoshi Nakamoto podría poseer alrededor de un millón de bitcoins, minados durante los primeros meses del proyecto, que nunca se han movido. Al valor que ha alcanzado Bitcoin en los últimos años, esto convertiría a su creador, si estuviera vivo y conservara esas monedas, en una de las personas más ricas del planeta -y, sin embargo, esas monedas permanecen inmóviles desde 2010, un dato que muchos interpretan como una muestra adicional de que la motivación original del proyecto no era el enriquecimiento personal de su autor.

Por qué el anonimato fue una decisión deliberada

El anonimato de Nakamoto no parece un accidente, sino una elección consciente y coherente con la propia filosofía del proyecto. Un sistema que aspira a no depender de ninguna autoridad central pierde parte de su credibilidad si depende de la reputación, la biografía o incluso la mera existencia legal de una persona concreta. Al desaparecer, Nakamoto evitó que Bitcoin se convirtiera en "el proyecto de una persona", susceptible de presión legal, de ataques personales o de decisiones unilaterales, y forzó a que el protocolo sobreviviera -o

no- exclusivamente por el valor de sus propias ideas y por el consenso de la comunidad que las adoptó.

Qué decía exactamente el whitepaper

El documento de nueve páginas es sorprendentemente claro y directo, incluso para lectores sin formación técnica avanzada. En su primera frase, resume todo el proyecto: propone "una versión puramente peer-to-peer del dinero electrónico" que permitiría "que los pagos en línea se enviaran directamente de una parte a otra sin pasar por una institución financiera". El resto del documento explica, sección por sección, cómo lograrlo.

- Explica el problema del doble gasto y por qué las soluciones anteriores dependían de un tercero de confianza. Nakamoto parte de un diagnóstico claro: todo sistema de dinero digital previo, desde DigiCash hasta las tarjetas de crédito, resolvía el doble gasto poniendo a un intermediario en el centro de cada transacción, exactamente el punto único de fallo que Bitcoin se proponía eliminar.
- Propone resolverlo mediante una red distribuida de nodos que registran las transacciones en un historial público (lo que después se llamaría blockchain). En lugar de un único libro de cuentas guardado bajo llave por un banco, miles de copias idénticas del mismo libro, en manos de participantes que no se conocen entre sí, se vigilan mutuamente.
- Introduce la idea de encadenar bloques de transacciones mediante hashes, de forma que alterar el historial pasado resulte extremadamente costoso, aplicando exactamente el mismo principio de la "torre de fichas de dominó numeradas" que vimos en el capítulo 3, pero a escala de todo el historial financiero de la red.
- Propone usar la prueba de trabajo (inspirada, como vimos, en Hashcash) tanto para decidir quién añade el siguiente bloque como para proteger la red frente a manipulaciones, convirtiendo el derecho a escribir en el libro de cuentas en algo que hay que ganarse con un coste real, no en algo que se pueda falsificar gratis.
- Describe un mecanismo de incentivos económicos -la recompensa por bloque y las comisiones- para que a los participantes les resulte más rentable comportarse honestamente que intentar hacer trampas, apostando por el interés propio racional, y no por la buena voluntad, como verdadero motor de la seguridad del sistema.
- Calcula, con fórmulas de probabilidad, la seguridad del sistema frente a un atacante que intentara reescribir el historial, concluyendo que la probabilidad de éxito cae exponencialmente cuantas más confirmaciones (bloques) pasan, de forma similar a como la probabilidad de acertar diez veces seguidas tirando una moneda al aire se vuelve, en la práctica, casi nula cuantas más tiradas hacen falta.

Lo notable del whitepaper no es tanto que cada una de sus ideas fuera absolutamente nueva -como vimos en el capítulo 2, varias piezas ya existían por separado-, sino la forma en que Nakamoto las combinó en un único sistema coherente, resolviendo por fin el problema del consenso distribuido sin autoridad central que había frenado a todos los intentos anteriores.

Del papel al código: enero de 2009

Nakamoto no se limitó a publicar una idea teórica. El 9 de enero de 2009, apenas semanas después de crear el primer bloque, publicó también la primera versión funcional del software

de Bitcoin, permitiendo que cualquiera pudiera descargarlo, ejecutarlo y empezar a participar en la red como nodo o como minero. El 12 de enero de 2009 se registró la primera transacción de la historia entre dos personas: Satoshi Nakamoto envió diez bitcoins a Hal Finney.

> *El whitepaper de Bitcoin es, todavía hoy, de lectura obligada para cualquiera que quiera entender el proyecto en profundidad: apenas nueve páginas que cambiaron la forma en que millones de personas piensan sobre el dinero.*

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". El documento original, todavía disponible públicamente y de lectura recomendada en su idioma original o traducido.
- Registro público de la lista de correo "The Cryptography Mailing List" (metzdowd.com), donde Nakamoto anunció por primera vez el proyecto el 31 de octubre de 2008.
- Historial público de la blockchain de Bitcoin, consultable por cualquiera mediante un nodo propio o un explorador de bloques, como fuente primaria para verificar la fecha del bloque génesis y la primera transacción entre Nakamoto y Hal Finney.

En el próximo capítulo veremos cómo fueron esos primeros años de vida de Bitcoin: desde una curiosidad de nicho intercambiada entre un puñado de entusiastas de la criptografía hasta los primeros usos reales, incluida la compra más famosa -y, en retrospectiva, más cara- de la historia: dos pizzas por diez mil bitcoins.

Capítulo 6. Los primeros años: del bloque génesis al reconocimiento mundial

Entre 2009 y 2013, Bitcoin pasó de ser un experimento casi desconocido, intercambiado entre un puñado de entusiastas de la criptografía, a convertirse en un fenómeno mundial que empezaba a atraer la atención de medios de comunicación, reguladores, inversores y, también, de delincuentes que vieron en él nuevas oportunidades. Este capítulo recorre esos años fundacionales.

El bloque génesis (3 de enero de 2009)

Como vimos en el capítulo 4, el primer bloque de la historia de Bitcoin -el "bloque génesis" o "bloque 0"- fue minado por Satoshi Nakamoto el 3 de enero de 2009. A diferencia de todos los bloques posteriores, este bloque tiene una peculiaridad técnica: su recompensa de cincuenta bitcoins quedó, por el propio diseño del software original, inutilizable, sin que se pueda gastar dentro de las reglas normales del protocolo. Esto ha llevado a algunos a interpretarlo como un gesto simbólico: los primeros bitcoins de la historia no podían, ni siquiera en teoría, usarse jamás.

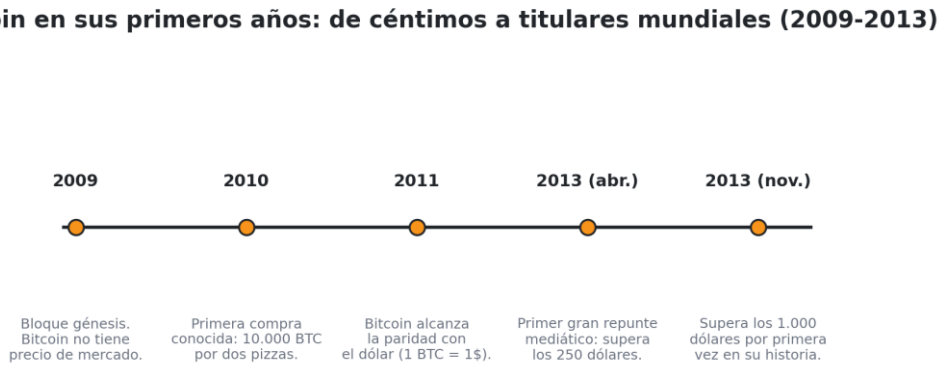
Los primeros usuarios y el valor cero

Durante todo 2009, Bitcoin no tenía ningún valor de mercado reconocido: minarlo era tan sencillo que cualquier ordenador doméstico podía generar bloques, y quienes lo hacían eran, principalmente, programadores curiosos que participaban por el interés técnico del proyecto, sin ninguna expectativa económica real. La primera cotización conocida de bitcoin frente al dólar, en octubre de 2009, fue de aproximadamente 1.309 BTC por un dólar -es decir, un valor prácticamente insignificante-, calculada por un usuario a partir del coste eléctrico de minarlo.

El día de la pizza (22 de mayo de 2010)

El episodio más célebre de estos primeros años ocurrió el 22 de mayo de 2010, cuando un programador de Florida llamado Laszlo Hanyecz publicó en un foro una oferta: pagaría diez mil bitcoins a quien le consiguiera dos pizzas. Otro usuario aceptó el trato y le hizo llegar las pizzas a cambio de esa cantidad de bitcoins. En aquel momento, diez mil bitcoins valían alrededor de cuarenta y un dólares -el precio aproximado de dos pizzas grandes-. Esta transacción es ampliamente considerada la primera compra documentada de un bien físico con bitcoin, y hoy se celebra cada año como el "Bitcoin Pizza Day".

Con las valoraciones que Bitcoin alcanzaría en años posteriores, esos diez mil bitcoins llegaron a valer en algunos momentos varios cientos de millones de dólares, lo que convirtió esta anécdota en el ejemplo favorito de la comunidad para ilustrar, con una mezcla de humor y advertencia, el coste de oportunidad de gastar bitcoin de forma prematura -y, al mismo tiempo, en un recordatorio de que, para que Bitcoin funcionara como moneda de intercambio real, alguien tenía que estar dispuesto a usarla para comprar cosas concretas.



Cronología ilustrativa de hitos de precio ampliamente documentados; los valores exactos varían ligeramente según el exchange histórico consultado.

De un valor prácticamente nulo en 2009 a superar los 1.000 dólares en 2013: los primeros hitos de precio de Bitcoin.

Los primeros exchanges y el nacimiento de un mercado

A medida que más gente se interesaba por Bitcoin, empezaron a surgir plataformas donde comprarlo y venderlo por moneda tradicional. La más influyente de esta primera etapa fue Mt. Gox, fundada originalmente en 2010 como una plataforma de intercambio de cartas de un juego de rol (su nombre proviene de "Magic: The Gathering Online Exchange") y reconvertida ese mismo año en un exchange de bitcoin. Durante varios años, Mt. Gox llegó a gestionar la mayoría del volumen mundial de operaciones con bitcoin, antes de protagonizar, en 2014, uno de los mayores escándalos de la historia de las criptomonedas, que analizaremos en el capítulo dedicado a los ataques contra usuarios y plataformas.

Silk Road y la sombra del uso ilícito

En 2011 apareció Silk Road, un mercado en la red oscura (dark web) donde se compraban y vendían, sobre todo, sustancias ilegales, utilizando bitcoin como método de pago por el pseudonimato que ofrecía frente a las transacciones bancarias tradicionales. Silk Road funcionó hasta octubre de 2013, cuando el FBI lo cerró y detuvo a su fundador, Ross Ulbricht.

Este episodio marcó de forma duradera la percepción pública de Bitcoin, asociándolo en la mente de muchas personas -y de muchos reguladores- con actividades ilícitas. Conviene matizar esta percepción con datos: numerosos estudios posteriores de empresas de análisis de blockchain, como Chainalysis, han mostrado que la proporción de transacciones de bitcoin vinculadas a actividad delictiva es, en la actualidad, una fracción muy pequeña del volumen total -inferior, de hecho, a la que numerosos organismos internacionales atribuyen al dinero en efectivo tradicional-, en parte precisamente porque, al contrario de lo que mucha gente cree, la blockchain de Bitcoin es un libro público y permanente, lo que ha permitido a las autoridades rastrear y perseguir con éxito numerosos delitos años después de haberse cometido. Analizaremos este debate con más detalle en el capítulo 26.

De la curiosidad de nicho al reconocimiento mundial

A lo largo de 2013, Bitcoin experimentó su primera gran subida de precio mediática, superando la barrera simbólica de los mil dólares por primera vez en noviembre de ese año,

coincidiendo con un aumento notable del interés en China y con las primeras audiencias en el Senado de Estados Unidos sobre cómo regular esta nueva tecnología. Empresas como WordPress y Overstock.com empezaron a aceptar bitcoin como forma de pago, y aparecieron los primeros cajeros automáticos de bitcoin.

Este periodo, entre 2009 y 2013, sentó las bases de casi todo lo que vendría después: la comunidad técnica que seguiría desarrollando el protocolo, los primeros mercados y su enorme volatilidad, la tensión permanente entre el uso legítimo y el uso ilícito, y el interés creciente -a partes iguales entusiasta y receloso- de gobiernos, medios de comunicación e inversores institucionales de todo el mundo.

Con esta base histórica ya establecida, la Parte III de este libro deja atrás la narrativa y entra en el terreno técnico: cómo funciona Bitcoin por dentro, bloque a bloque, transacción a transacción, desde la estructura de la blockchain hasta el proceso exacto por el cual se crean nuevos bitcoins.

Fuentes y estudios citados en este capítulo

- Popper, N. (2015). "Digital Gold: The Untold Story of Bitcoin". Harper. Uno de los relatos periodísticos más documentados sobre los primeros años de Bitcoin, incluida la historia de Mt. Gox y Silk Road.
- Chainalysis. "Crypto Crime Report" (informes anuales). Análisis cuantitativos sobre la proporción de actividad ilícita en el volumen total de transacciones de criptomonedas.
- Departamento de Justicia de Estados Unidos, documentación judicial del caso United States v. Ross William Ulbricht (2013-2015).

PARTE III

CÓMO FUNCIONA BITCOIN POR DENTRO

Capítulo 7. La blockchain: estructura y funcionamiento

Llegados a este punto, con el dinero, la criptografía y la historia ya explicados, podemos entrar en el corazón técnico de Bitcoin: la blockchain, o cadena de bloques. Este capítulo explica qué es exactamente, cómo se construye y por qué su diseño concreto la hace tan difícil de manipular.

Qué es, en el fondo, la blockchain

La blockchain de Bitcoin es, ni más ni menos, un libro de contabilidad público y compartido: un registro que anota, de forma ordenada y cronológica, todas las transacciones que se han realizado desde el bloque génesis hasta hoy. Lo que la hace especial no es la idea de llevar un registro de transacciones -eso lo hacen también los bancos-, sino el hecho de que ese registro no lo controla ninguna entidad central, sino que se replica de forma idéntica en miles de ordenadores (nodos) repartidos por todo el mundo, y que está diseñado matemáticamente para que resulte extraordinariamente difícil alterar su historial una vez escrito.

El nombre "cadena de bloques" describe literalmente su estructura: las transacciones no se registran una a una de forma suelta, sino que se agrupan en paquetes llamados bloques, y estos bloques se enlazan entre sí, uno detrás de otro, formando una cadena continua desde el primer bloque (el génesis) hasta el más reciente.

Qué contiene un bloque

Cada bloque de Bitcoin se compone de dos partes principales: una cabecera (header), que contiene los metadatos del bloque, y un cuerpo, que contiene la lista completa de transacciones incluidas en ese bloque. Es útil pensar en la cabecera como la etiqueta de envío pegada a un paquete: no contiene el paquete entero, pero sí toda la información necesaria para identificarlo, verificarlo y situarlo en su lugar exacto dentro de la cadena. La cabecera es, en realidad, la parte más importante desde el punto de vista de la seguridad, y contiene, entre otros datos:

- El hash del bloque anterior: el resultado de aplicar la función hash SHA-256 (dos veces, en realidad) a la cabecera del bloque previo. Es, literalmente, el eslabón físico de la

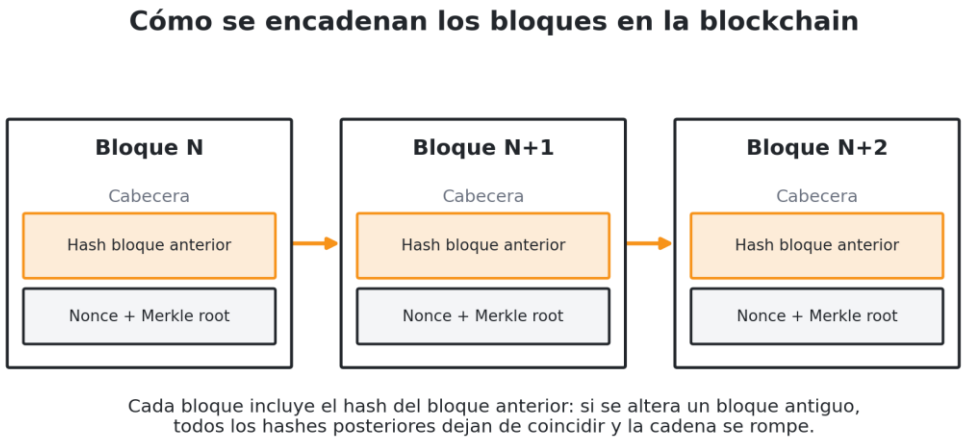
cadena: sin este dato, los bloques serían paquetes de transacciones sueltos, sin ningún orden verificable entre ellos.

- La raíz de Merkle: un único hash que resume de forma verificable todas las transacciones incluidas en ese bloque (lo explicamos en detalle en el próximo capítulo). Gracias a ella, no hace falta guardar ni transmitir todas las transacciones para comprobar si una en concreto pertenece al bloque: basta con un pequeño fragmento de información adicional.
- La marca de tiempo (timestamp): el momento aproximado en que se creó el bloque, que sirve tanto de referencia histórica como de dato de entrada para el ajuste automático de dificultad que veremos en el capítulo 11.
- La dificultad objetivo: un valor que indica cuán difícil debe ser, en ese momento, encontrar un hash válido para el bloque (lo veremos en el capítulo de minería). Es equivalente a subir o bajar el listón de un examen: cuanto más exigente es el listón, menos "aprobados" (hashes válidos) se encuentran por segundo en toda la red.
- El nonce: un número que los mineros van cambiando, probando una y otra vez, hasta encontrar un hash de bloque que cumpla la condición de dificultad exigida. Es, en la práctica, el número de billete de lotería que los mineros generan y comprueban miles de millones de veces por segundo, con la esperanza de que alguno resulte premiado.

El eslabón que lo hace todo seguro: el hash del bloque anterior

La pieza clave de todo el diseño es que cada bloque incluye, dentro de su propia cabecera, el hash del bloque inmediatamente anterior. Esto crea una dependencia encadenada: el hash del bloque 100 depende de todo el contenido del bloque 100, que a su vez incluye el hash del bloque 99, que depende de todo el contenido del bloque 99, que incluye el hash del bloque 98, y así sucesivamente hasta el bloque génesis.

La consecuencia de este diseño es enorme: si alguien intentara alterar, por ejemplo, una sola transacción del bloque 100 mucho después de que se haya creado, el hash de ese bloque cambiaría por completo (recordemos el efecto avalancha del capítulo 3). Pero como el bloque 101 contiene el hash original del bloque 100, ese cambio invalidaría también el bloque 101, lo que a su vez invalidaría el bloque 102, y así hasta el bloque más reciente. El atacante tendría que volver a calcular, desde el bloque alterado hasta el final de la cadena, un trabajo computacional (como veremos, la prueba de trabajo) que crece exponencialmente cuantos más bloques se hayan añadido después. Alterar transacciones antiguas se vuelve, a efectos prácticos, más difícil cuanto más tiempo ha pasado.



Cómo se encadenan los bloques: cada uno incluye el hash del anterior.

Confirmaciones: la seguridad que aumenta con el tiempo

Esta propiedad da lugar a un concepto central en Bitcoin: las confirmaciones. Cuando una transacción se incluye en un bloque, se dice que tiene una confirmación. Cuando se mina el siguiente bloque encima de ese, la transacción pasa a tener dos confirmaciones, y así sucesivamente. Cuantas más confirmaciones tiene una transacción, más costoso -y por tanto, más improbable- resulta que alguien pueda revertirla, porque haría falta rehacer todo el trabajo computacional de todos los bloques posteriores, además de superar el ritmo al que la red honesta sigue añadiendo bloques nuevos.

Por convención práctica, muchos servicios consideran una transacción razonablemente segura a partir de seis confirmaciones (aproximadamente una hora, dado que Bitcoin produce un bloque nuevo cada diez minutos de media), aunque para importes pequeños suele bastar con una sola confirmación, y para importes muy grandes algunos servicios exigen más.

Bitcoin como base de datos distribuida

Una forma útil de pensar en la blockchain es imaginarla no como "una única base de datos en algún servidor", sino como miles de copias idénticas de la misma base de datos, cada una guardada por un nodo distinto, en distintos países, operados por personas y organizaciones que no se conocen entre sí. Cuando se añade un bloque nuevo válido, todos los nodos lo verifican de forma independiente -comprobando que las firmas son correctas, que no hay doble gasto, que se cumplen todas las reglas del protocolo- y, si todo es correcto, lo añaden a su propia copia del registro.

Esto es lo que hace a Bitcoin resistente a la censura y a los puntos únicos de fallo: no existe un servidor central que se pueda apagar, hackear o intervenir judicialmente para detener la red. Mientras exista al menos un puñado de nodos ejecutando el software en algún lugar del mundo, la red y su historial siguen existiendo.

Inmutabilidad: relativa, no absoluta

Conviene matizar una idea que a veces se repite de forma imprecisa: la blockchain de Bitcoin no es "matemáticamente imposible" de alterar, sino "económicamente y computacionalmente

impracticable" de alterar, en la medida en que su seguridad depende de que la mayoría del poder de cómputo de la red (el llamado hashrate) sea honesta. En el capítulo 16 explicaremos en detalle qué ocurriría si un atacante consiguiera controlar una mayoría de ese poder de cómputo -el llamado "ataque del 51%"- y por qué, en la práctica, resulta extraordinariamente costoso llevarlo a cabo contra una red tan grande como la de Bitcoin hoy en día.

Con la estructura general de la blockchain ya clara, en el próximo capítulo bajaremos un nivel más de detalle para entender exactamente qué es una transacción de Bitcoin, cómo se construye y por qué utiliza un modelo distinto al de una simple cuenta bancaria: el modelo UTXO.

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", secciones 3 a 5, donde se describe originalmente la estructura de bloques encadenados mediante hashes.
- Merkle, R. (1980). "Protocols for Public Key Cryptosystems". Proceedings of the IEEE Symposium on Security and Privacy. Trabajo pionero sobre árboles de hash, que da nombre a la raíz de Merkle explicada en el capítulo siguiente.
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., Felten, E. (2015). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". IEEE Symposium on Security and Privacy. Panorámica académica de referencia sobre la seguridad de Bitcoin.

Capítulo 8. Transacciones y el modelo UTXO

Cuando la mayoría de la gente piensa en "tener bitcoins", imagina algo parecido a una cuenta bancaria: un saldo, un número, que sube y baja con cada movimiento. Pero Bitcoin no funciona así por dentro. Utiliza un modelo distinto, más parecido a un monedero lleno de billetes de distinto valor, llamado modelo UTXO (Unspent Transaction Output, o "salida de transacción no gastada"). Entender este modelo es clave para comprender de verdad cómo se mueve el dinero en la red.

Qué es un UTXO

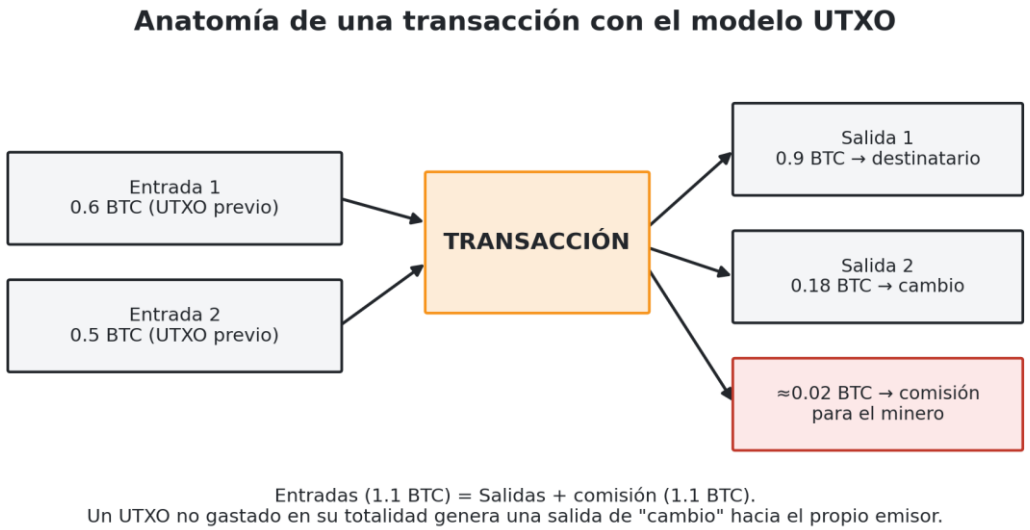
Un UTXO es, literalmente, un fragmento de bitcoin que fue creado como salida de una transacción anterior y que todavía no ha sido gastado. Cuando alguien te envía bitcoin, lo que realmente ocurre es que se crea un nuevo UTXO asociado a tu dirección, con una cantidad concreta. Tu "saldo" en Bitcoin no es un número guardado en algún sitio, sino la suma de todos los UTXO dispersos por la blockchain que están asociados a las direcciones que tú controlas.

La analogía más citada es la del monedero con billetes y monedas físicas: si tienes un billete de veinte euros y otro de diez, tu "saldo" de treinta euros no existe como tal en ningún sitio; existe como la suma de dos objetos físicos concretos que posees. Si quieres pagar veinticinco euros, tendrás que entregar ambos billetes y recibir cinco euros de cambio -no puedes "partir" un billete de veinte en dos-. Los UTXO funcionan de forma muy parecida.

Anatomía de una transacción

Toda transacción de Bitcoin tiene la misma estructura básica: consume uno o varios UTXO existentes como entradas (inputs) y crea uno o varios UTXO nuevos como salidas (outputs). La suma total de las entradas debe ser igual o mayor que la suma total de las salidas; la diferencia, si la hay, se destina como comisión (fee) para el minero que incluya la transacción en un bloque.

- Entradas (inputs): referencias a UTXO previos que el emisor posee y que decide gastar en esta transacción, junto con la firma digital que demuestra que tiene derecho a gastarlos. Cada entrada señala, con total precisión, a qué transacción anterior exacta pertenece ese fragmento de bitcoin, de forma parecida a como un cheque hace referencia a una cuenta y un número concretos.
- Salidas (outputs): las cantidades nuevas que se crean, cada una asociada a una dirección de destino concreta (que puede ser la del receptor del pago, o la del propio emisor, si sobra dinero). Cada salida es, en sí misma, un nuevo UTXO recién nacido, listo para ser gastado en el futuro como entrada de otra transacción distinta.
- Comisión (fee): la diferencia entre el total de entradas y el total de salidas, que se paga implícitamente al minero, sin que exista ningún campo explícito de "comisión" en la transacción: el minero simplemente se queda con lo que sobra entre lo que entra y lo que sale.



Anatomía de una transacción: entradas, salidas y comisión bajo el modelo UTXO.

El "cambio": por qué casi toda transacción tiene dos salidas

Siguiendo con la analogía de los billetes: si tienes un único UTXO de 0,6 BTC y quieres pagar 0,35 BTC a alguien, no puedes "cortar" ese UTXO en dos partes directamente. En su lugar, tu monedero construye una transacción que gasta ese UTXO completo como entrada, y crea dos salidas nuevas: una de 0,35 BTC hacia el destinatario, y otra -el "cambio"- de vuelta hacia una dirección que tú controlas, por el resto (menos la comisión). Este mecanismo de cambio es una de las razones por las que, si observas la blockchain, verás que la inmensa mayoría de las transacciones tienen dos salidas, no una.

Este detalle también tiene implicaciones de privacidad, ya que a veces resulta posible para un observador externo distinguir cuál de las dos salidas es el pago real y cuál es el cambio, algo que las técnicas modernas de construcción de wallets intentan mitigar generando direcciones de cambio que no se distinguen visualmente de una dirección de pago normal.

Combinar varios UTXO en una sola transacción

Del mismo modo que puedes pagar con varios billetes a la vez si uno solo no te alcanza, una transacción de Bitcoin puede usar varios UTXO como entradas simultáneamente. Si quieres pagar 1,2 BTC y tienes tres UTXO de 0,5, 0,4 y 0,5 BTC, tu monedero puede combinar, por ejemplo, los tres para sumar 1,4 BTC, pagar 1,2 BTC al destinatario y devolverte 0,2 BTC (menos la comisión) como cambio.

Por qué Bitcoin eligió este modelo en lugar de un sistema de cuentas

Otros sistemas -incluida la red Ethereum, entre otras- utilizan un modelo de cuentas, mucho más parecido al de un banco tradicional: cada dirección tiene un saldo, y las transacciones simplemente restan de una cuenta y suman a otra. El modelo UTXO de Bitcoin tiene, frente a ese enfoque, varias ventajas técnicas relevantes:

- Verificación en paralelo: como cada UTXO es independiente, los nodos pueden verificar muchas transacciones a la vez sin tener que procesarlas estrictamente en un orden

secuencial, lo que facilita la validación y ciertas optimizaciones técnicas, de forma parecida a como varios cajeros de un supermercado pueden cobrar a distintos clientes al mismo tiempo, en lugar de tener que atenderlos uno detrás de otro por una única caja.

- Menor riesgo de "doble gasto accidental": es matemáticamente sencillo comprobar que un UTXO concreto no se ha gastado ya en otra transacción, simplemente consultando si sigue figurando como no gastado en el conjunto (set) de UTXO vigente, algo tan directo como comprobar si un billete concreto, con su número de serie, sigue en tu cartera o ya lo entregaste.
- Mejor privacidad potencial: al no existir un "saldo total" visible de forma directa en ninguna dirección concreta (solo la suma de sus UTXO), y al poder generar una dirección nueva para cada pago recibido, resulta algo más difícil vincular todas las transacciones de una misma persona entre sí, aunque este beneficio depende en gran medida de cómo se use el software.

La contrapartida es que el modelo UTXO resulta algo menos intuitivo al principio, y que las wallets tienen que hacer, de forma transparente para el usuario, un trabajo de selección y combinación de UTXO ("coin selection") cada vez que se construye una transacción, para elegir de forma eficiente qué UTXO usar como entradas.

El campo scriptPubKey: quién puede gastar cada UTXO

Cada salida de una transacción no solo especifica una cantidad, sino también las condiciones exactas que hay que cumplir para poder gastarla en el futuro, expresadas en un pequeño lenguaje de programación propio de Bitcoin llamado Script. En el caso más habitual, la condición es sencilla: "solo puede gastar este UTXO quien pueda proporcionar una firma válida correspondiente a esta clave pública concreta". Pero Script permite también condiciones más sofisticadas -por ejemplo, que hagan falta varias firmas distintas para autorizar un gasto (lo que se llama "multifirma" o multisig), o que el UTXO no se pueda gastar antes de una fecha determinada-, que dan lugar a usos avanzados que iremos mencionando a lo largo del libro.

Con el modelo UTXO ya claro, en el próximo capítulo bajaremos otro nivel más: cómo se generan las claves privadas y públicas que permiten controlar esos UTXO, y cómo, a partir de ellas, se construye la dirección de Bitcoin que compartes cuando alguien quiere enviarte dinero.

Fuentes y estudios citados en este capítulo

- Bitcoin Core Developer Documentation, "Transactions" y "The UTXO Set", documentación técnica de referencia mantenida por los desarrolladores del software Bitcoin Core.
- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sección 9, donde se describe el formato original de las transacciones.

Capítulo 9. Claves privadas, claves públicas y direcciones

Todo lo que hemos explicado hasta ahora sobre transacciones y UTXO depende de un mecanismo concreto para demostrar la propiedad: las claves criptográficas que presentamos de forma general en el capítulo 3. Este capítulo explica, paso a paso, cómo se genera una clave privada de Bitcoin, cómo se deriva de ella la clave pública y, finalmente, la dirección que compartes con otras personas.

La clave privada: un número (muy) aleatorio

En su forma más pura, una clave privada de Bitcoin es, simplemente, un número aleatorio de 256 bits -es decir, un número elegido al azar entre aproximadamente 1,15 por 10 elevado a 77 posibilidades, una cifra tan inmensa que resulta más grande que el número estimado de átomos en toda la Vía Láctea. Esta magnitud no es un capricho: es lo que hace que resulte, a efectos prácticos, imposible que alguien adivine o encuentre por fuerza bruta la clave privada de otra persona, incluso empleando toda la capacidad de cómputo disponible en el planeta durante miles de millones de años.

La seguridad de todo el sistema depende, en última instancia, de que ese número se genere de verdad al azar, con una fuente de aleatoriedad de calidad criptográfica. Un generador de números aleatorios defectuoso o predecible es, históricamente, una de las causas reales -aunque poco frecuentes- detrás de robos de fondos en Bitcoin, y es la razón por la que se recomienda usar siempre software de wallet reputado y bien auditado en lugar de herramientas caseras o poco conocidas.

De la clave privada a la clave pública

A partir de la clave privada, mediante las operaciones de la criptografía de curva elíptica que mencionamos en el capítulo 3 (concretamente sobre la curva secp256k1), se calcula de forma determinista una clave pública. Este cálculo es un ejemplo perfecto de "función de un solo sentido": resulta extremadamente rápido calcular la clave pública a partir de la clave privada, pero no existe ningún método conocido -ni se espera que exista, salvo con ordenadores cuánticos suficientemente potentes, como veremos en el capítulo 20- para hacer el camino inverso.

De la clave pública a la dirección

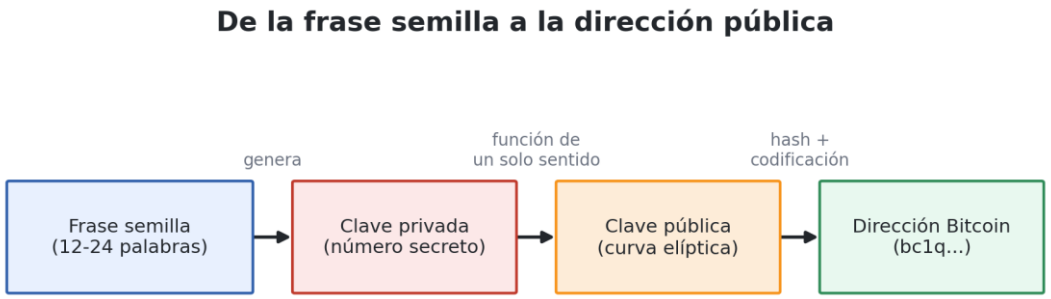
La dirección de Bitcoin que compartes para recibir pagos no es, técnicamente, la clave pública en sí, sino el resultado de aplicarle una serie de funciones hash adicionales (una combinación de SHA-256 y otra función llamada RIPEMD-160) y, después, codificar el resultado en un formato de texto legible y con protección frente a errores de transcripción.

A lo largo de la historia de Bitcoin han existido varios formatos de dirección, cada uno introducido para mejorar algún aspecto del sistema:

- Direcciones "Legacy" (empiezan por 1): el formato original, presente desde 2009, hoy en desuso progresivo pero todavía válido y aceptado por toda la red.

- Direcciones P2SH (empiezan por 3): introducidas para soportar transacciones con condiciones más complejas, como la multifirma, permitiendo "esconder" dentro de la propia dirección un conjunto de reglas de gasto más sofisticadas de lo que permitía el formato original.
- Direcciones SegWit nativas o Bech32 (empiezan por bc1q): introducidas en 2017 junto con la mejora SegWit (capítulo 21), más eficientes en cuanto a espacio -lo que se traduce en comisiones algo más bajas para quien las usa- y con mejor detección de errores de escritura.
- Direcciones Taproot o Bech32m (empiezan por bc1p): el formato más reciente, introducido en 2021, que habilita funcionalidades avanzadas de privacidad y de contratos inteligentes con menor coste, de forma que transacciones complejas pueden llegar a parecer, de puertas afuera, indistinguibles de un pago simple.

Todos estos formatos incluyen una comprobación de checksum: un pequeño fragmento adicional derivado matemáticamente del resto de la dirección, que permite detectar casi cualquier error tipográfico al escribir o copiar una dirección manualmente, de forma muy parecida a como el último dígito de un IBAN o de un ISBN de un libro permite detectar automáticamente si alguien ha transcrito mal un número. Si escribes mal un solo carácter, el software detectará que el checksum no cuadra y rechazará la dirección, en lugar de enviar el dinero a un destino equivocado (aunque, como norma general de seguridad, siempre es preferible copiar y pegar o escanear un código QR en lugar de teclear direcciones a mano).



De la frase semilla a la dirección pública: un proceso irreversible en un solo sentido.

La frase semilla (seed phrase): una copia de seguridad legible por humanos

Gestionar decenas de claves privadas distintas -una por cada dirección usada- sería muy poco práctico para un usuario normal. Por eso, prácticamente todas las wallets modernas usan un estándar llamado BIP-39 (Bitcoin Improvement Proposal 39), que permite generar, a partir de una única fuente de aleatoriedad inicial, una secuencia de doce o veinticuatro palabras comunes -la "frase semilla" o seed phrase- de la que se pueden derivar matemáticamente, de forma determinista, un número prácticamente ilimitado de pares de claves privadas y públicas.

Esto tiene una consecuencia práctica enorme: basta con anotar esas doce o veinticuatro palabras, en el orden exacto en que se generaron, para poder reconstruir absolutamente todas las claves y, por tanto, recuperar el acceso a todos los fondos asociados, incluso si el

dispositivo original donde se creó la wallet se pierde, se rompe o es robado. Por esta misma razón, esa frase semilla es, en la práctica, el objeto más sensible de toda la seguridad de un usuario de Bitcoin, y dedicaremos el capítulo 25 entero a cómo protegerla correctamente.

Una dirección nueva para cada pago

Una buena práctica recomendada de forma casi universal en la comunidad de Bitcoin es generar una dirección nueva para cada pago que se recibe, en lugar de reutilizar siempre la misma. Las wallets modernas hacen esto de forma automática y transparente para el usuario. La razón es de privacidad: si siempre usas la misma dirección, cualquiera que consulte la blockchain (que, recordemos, es completamente pública) puede ver de un vistazo el historial completo de todos los pagos que has recibido en esa dirección a lo largo del tiempo. Usar direcciones distintas dificulta, aunque no elimina por completo, esta capacidad de seguimiento.

> *Clave privada, clave pública y dirección forman una cadena de un solo sentido: puedes ir siempre hacia adelante (de la privada a la dirección), pero nunca hacia atrás. Esa asimetría matemática es, literalmente, lo único que separa "tener bitcoins" de "no tenerlos".*

Fuentes y estudios citados en este capítulo

- Palatinus, M., Rusnak, P., Voisine, A., Bowe, S. (2013). "BIP-39: Mnemonic code for generating deterministic keys". Bitcoin Improvement Proposal que estandariza la frase semilla.
- Wuille, P. (2012). "BIP-32: Hierarchical Deterministic Wallets". Bitcoin Improvement Proposal que define la derivación jerárquica de claves.
- Certicom Research (2010). "SEC 2: Recommended Elliptic Curve Domain Parameters", especificación de la curva secp256k1.

En el próximo capítulo veremos cómo estas claves se gestionan en la práctica, a través de los distintos tipos de monederos (wallets) que existen, y qué diferencias de seguridad y comodidad hay entre ellos.

Capítulo 10. Wallets: qué son y qué tipos existen

La palabra "wallet" (monedero) genera una de las confusiones más habituales entre quienes se acercan por primera vez a Bitcoin, porque sugiere -de forma engañosa- que se trata de un contenedor donde se "guardan" los bitcoins, de forma parecida a como una cartera guarda billetes físicos. En realidad, como vimos en el capítulo anterior, los bitcoins (los UTXO) siempre están en la blockchain, no en ningún dispositivo. Una wallet no guarda bitcoins: guarda claves privadas, y con ellas, la capacidad de gastar los UTXO asociados a esas claves.

Qué hace realmente una wallet

Una wallet de Bitcoin es, en esencia, un programa (software) que cumple varias funciones:

- Genera y almacena de forma segura tu frase semilla y las claves privadas derivadas de ella, normalmente cifradas en el propio dispositivo, o aisladas por completo del mundo exterior en el caso de un monedero hardware.
- Consulta la blockchain (directamente o a través de un servidor de terceros) para calcular tu saldo, sumando todos los UTXO asociados a tus direcciones, un poco como una aplicación bancaria que recorre todos tus movimientos para mostrarte un único número final.
- Construye y firma nuevas transacciones cuando quieres enviar bitcoin, usando tus claves privadas, encargándose de toda la complejidad técnica -selección de UTXO, cálculo de comisión, formato correcto- que tú, como usuario, no necesitas ver.
- Genera direcciones nuevas y códigos QR para que puedas recibir pagos, siguiendo la buena práctica de no reutilizar siempre la misma dirección que explicamos en el capítulo anterior.

Entender esto -que la wallet gestiona claves, no monedas- es la base para entender por qué existen tantos tipos distintos de wallets, cada uno con un enfoque diferente sobre dónde y cómo se guardan esas claves privadas.

La gran distinción: custodia propia frente a custodia de terceros

La primera y más importante clasificación de wallets no tiene que ver con la tecnología, sino con quién controla la clave privada.

- Wallets de autocustodia (self-custody, "non-custodial"): la clave privada se genera y se guarda exclusivamente en el dispositivo o soporte del propio usuario. Nadie más tiene acceso a ella. Ejemplos: la mayoría de las apps de wallet que se instalan en el móvil o el ordenador, y todos los monederos hardware. Es el equivalente a guardar tu propio dinero en una caja fuerte de tu casa: nadie puede impedirte usarlo, pero tampoco hay nadie a quien llamar si pierdes la combinación.
- Wallets custodiadas (custodial): un tercero -típicamente un exchange como Coinbase, Binance o Kraken- guarda las claves privadas en tu nombre, y tú simplemente tienes una cuenta con un saldo, de forma muy parecida a una cuenta bancaria tradicional. Es cómodo, pero implica confiar en que esa empresa gestione bien la seguridad y no restrinja tu acceso a los fondos, exactamente igual que depositar tu dinero en un banco:

ganas comodidad y recuperación en caso de olvido, a cambio de depender de la solvencia y la buena fe de un tercero.

Esta distinción da lugar a una de las máximas más repetidas en la comunidad de Bitcoin: "not your keys, not your coins" ("si no son tus claves, no son tus monedas"). Quien mantiene bitcoin en un exchange no tiene, en sentido estricto, bitcoin bajo su control directo, sino un derecho contractual frente a esa empresa para reclamarlo -un derecho que, como veremos en el capítulo 18, no siempre se ha podido honrar cuando esas empresas han quebrado o han sido hackeadas.

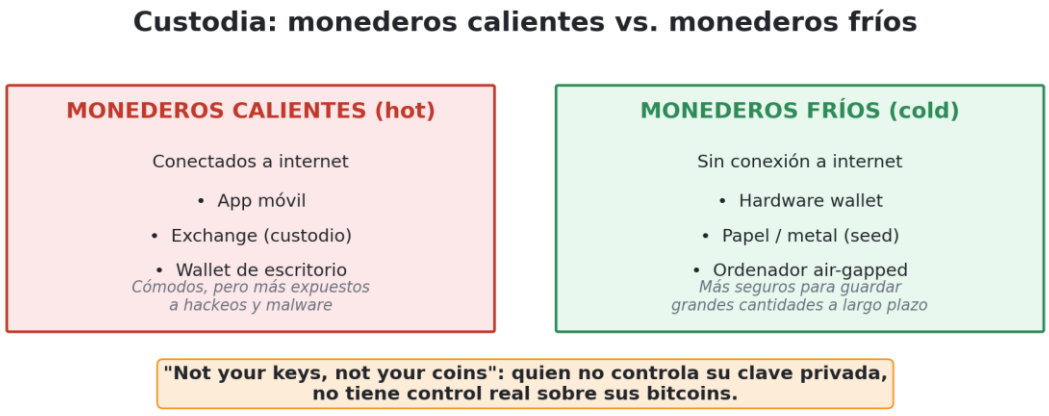
Monederos calientes (hot wallets)

Se llaman "calientes" los monederos cuyas claves privadas están, en algún momento, en un dispositivo conectado a internet. Incluyen las apps móviles de wallet, las extensiones de navegador, los programas de escritorio y las cuentas en exchanges. Son cómodos para el uso frecuente -pagos del día a día, pequeñas cantidades- pero, precisamente por estar conectados a internet, son más vulnerables a malware, virus, phishing y ataques remotos.

Monederos fríos (cold wallets o cold storage)

Se llaman "fríos" los monederos cuyas claves privadas nunca han estado, ni están, conectadas a internet. Incluyen los monederos hardware (dispositivos físicos dedicados, como Ledger o Trezor, diseñados específicamente para generar y guardar claves privadas de forma aislada), los monederos de papel (donde la clave o la frase semilla se escribe o imprime físicamente) y las placas de metal grabadas, pensadas para resistir incendios e inundaciones.

Un monedero hardware funciona firmando las transacciones dentro del propio dispositivo, sin que la clave privada salga jamás de él: el ordenador o móvil conectado solo envía los datos de la transacción sin firmar, el dispositivo hardware la firma internamente y devuelve la transacción ya firmada, lista para transmitirse a la red, sin que la clave privada haya estado expuesta en ningún momento a un dispositivo conectado a internet.



Monederos calientes frente a monederos fríos: comodidad frente a seguridad.

Wallets con múltiples firmas (multisig)

Además de la distinción caliente/fría, existe otra dimensión relevante: cuántas claves hacen falta para autorizar un gasto. Una wallet "multisig" (multifirma) exige varias firmas independientes, de varias claves privadas distintas, para poder gastar los fondos -por ejemplo, una configuración "2 de 3" en la que hacen falta al menos dos de tres claves posibles-. Esto se usa mucho en empresas, para evitar que una sola persona pueda mover fondos sin supervisión, y también entre particulares avanzados, para eliminar cualquier punto único de fallo: si pierdes una de las tres claves, o si alguien te roba una, los fondos siguen a salvo mientras las otras dos permanezcan seguras.

Wallets deterministas jerárquicas (HD wallets)

Prácticamente todas las wallets modernas siguen el estándar BIP-32/BIP-44, que permite derivar de una única frase semilla una estructura jerárquica casi infinita de claves distintas, organizadas en "cuentas" y "ramas". Esto es lo que permite que una sola copia de seguridad (la frase semilla) proteja todas las direcciones que uses, presentes y futuras, sin necesidad de hacer una copia de seguridad nueva cada vez que generas una dirección.

Cómo elegir: no existe una única respuesta correcta

La elección del tipo de wallet depende del uso que se le vaya a dar al dinero. Una analogía útil, habitual entre usuarios experimentados, es pensar en los distintos tipos de wallet como se piensa en el dinero físico: llevas encima en la cartera (hot wallet) solo el efectivo que necesitas para el día a día, y guardas los ahorros importantes en una caja fuerte (cold wallet) a la que no accedes constantemente. Dedicaremos el capítulo 25 a explicar, con recomendaciones prácticas, cómo aplicar este principio de forma concreta.

Con las wallets ya explicadas, en el próximo capítulo entramos en uno de los procesos más característicos -y más incomprendidos- de Bitcoin: la minería y la prueba de trabajo, el mecanismo que crea nuevos bitcoins y que, al mismo tiempo, protege toda la red frente a manipulaciones.

Fuentes y estudios citados en este capítulo

- Gutierrez, C. et al. (2014). "BIP-44: Multi-Account Hierarchy for Deterministic Wallets". Bitcoin Improvement Proposal que estandariza la organización de cuentas y direcciones dentro de una wallet.
- Ledger y Trezor, documentación técnica pública sobre el diseño de seguridad de los monederos hardware (elementos seguros, firma aislada de transacciones).

Capítulo 11. Minería y la Prueba de Trabajo (Proof of Work)

La minería de Bitcoin es, probablemente, el aspecto más citado y menos comprendido de todo el sistema. La imagen popular de "mineros resolviendo complicadas ecuaciones matemáticas" no es del todo precisa: lo que hacen, en realidad, es un proceso de fuerza bruta guiado, basado en las funciones hash que ya conocemos del capítulo 3. Este capítulo explica el proceso completo, por qué es necesario y qué problema resuelve exactamente.

El problema que resuelve la minería

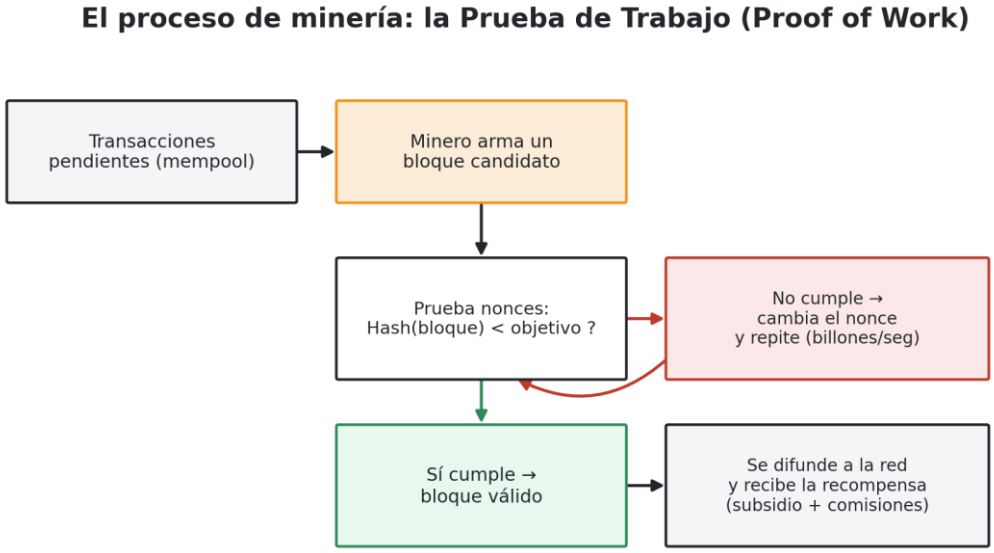
Bitcoin necesita que, cada cierto tiempo, alguien decida qué transacciones pendientes se incluyen en el siguiente bloque y en qué orden, y que el resto de la red se ponga de acuerdo en aceptar esa decisión. El problema es que no hay ninguna autoridad central que pueda tomar esa decisión de forma legítima, así que Bitcoin necesita un mecanismo para que ese derecho -el derecho a proponer el siguiente bloque- se reparta de una forma que sea, al mismo tiempo, difícil de manipular y verificable por cualquiera. La solución de Nakamoto fue convertir ese derecho en algo que hay que "ganarse" mediante un coste real: trabajo computacional.

Cómo funciona, paso a paso

Un minero que quiere proponer el siguiente bloque sigue, en esencia, este proceso:

- Recopila un conjunto de transacciones pendientes de la mempool (el conjunto de transacciones válidas que todavía no se han incluido en ningún bloque), priorizando normalmente las que pagan una comisión más alta por byte de datos, de forma parecida a como un repartidor con varios paquetes por entregar prioriza primero los que tienen un porte más caro.
- Construye un bloque candidato con esas transacciones, calcula la raíz de Merkle correspondiente (capítulo 7) y arma la cabecera del bloque con el hash del bloque anterior, la marca de tiempo y la dificultad vigente: prepara, en definitiva, el "billete de lotería" completo antes de empezar a rellenarlo.
- Elige un número llamado nonce (que empieza normalmente en cero) y calcula el hash SHA-256 (dos veces, en realidad, un proceso llamado doble SHA-256) de toda la cabecera del bloque.
- Comprueba si ese hash resultante es menor que un valor objetivo determinado por la dificultad actual de la red -en la práctica, esto se traduce en exigir que el hash empiece por una cierta cantidad de ceros-. Es como si el premio solo se otorgara a los boletos cuyo número termine en una larga secuencia de ceros: cuantos más ceros se exigen, menos boletos ganan, y más boletos hace falta comprar (calcular) para encontrar uno premiado.
- Si el hash no cumple la condición (lo habitual, la inmensa mayoría de las veces), cambia el nonce por otro valor distinto y repite el cálculo. Esto se repite miles de millones -en realidad, billones- de veces por segundo en el hardware moderno, sin que ningún intento "acerque" al minero a la solución: cada prueba es tan independiente e impredecible como la anterior, por el efecto avalancha que vimos en el capítulo 3.

- En cuanto un minero, en cualquier parte del mundo, encuentra por fin un nonce cuyo hash cumple la condición, difunde inmediatamente el bloque completo a toda la red, donde cualquier nodo puede comprobar la solución en un instante, como quien verifica en segundos un boleto de lotería premiado sin tener que repetir el sorteo.



El proceso de minería: probar nonces hasta encontrar un hash válido.

Por qué es difícil encontrarlo pero fácil de comprobar

Esta es la propiedad central que hace que todo el sistema funcione: no existe ningún atajo matemático conocido para encontrar un nonce válido más rápido que probando muchísimas combinaciones al azar (debido al efecto avalancha de las funciones hash, que vimos en el capítulo 3, no hay ninguna relación predecible entre el nonce y el hash resultante). Pero, una vez que un minero encuentra la solución, cualquier otro nodo de la red puede comprobar en una fracción de segundo, con un único cálculo, que ese hash concreto efectivamente cumple la condición de dificultad exigida. Esta asimetría -difícil de encontrar, trivial de verificar- es la que da su nombre a la "prueba de trabajo": el hash válido es, en sí mismo, la prueba de que se ha realizado una cantidad enorme de trabajo computacional real.

El ajuste de dificultad

Bitcoin está diseñado para producir, en promedio, un bloque nuevo cada diez minutos, sin importar cuánta potencia de cómputo total (hashrate) tenga la red en cada momento. Para lograr esto, el protocolo reajusta automáticamente la dificultad del objetivo cada 2.016 bloques -aproximadamente cada dos semanas-, comparando el tiempo que realmente ha tardado la red en minar esos bloques con el tiempo teórico esperado (dos semanas). Si la red ha ido más rápido de lo esperado (porque se ha sumado más potencia de cómputo), la dificultad sube; si ha ido más lenta (porque, por ejemplo, muchos mineros se han desconectado), la dificultad baja. Este mecanismo de autorregulación es una de las piezas de ingeniería más elegantes del diseño original de Nakamoto, y ha mantenido el ritmo de bloques notablemente estable durante más de quince años, a pesar de que la potencia de cómputo total de la red ha crecido varios billones de veces desde 2009.

El hardware de minería: de la CPU al ASIC

En los primeros años, cualquier ordenador doméstico podía minar bitcoin usando su procesador (CPU). Muy pronto, la comunidad descubrió que las tarjetas gráficas (GPU), diseñadas para procesar gráficos en paralelo, eran mucho más eficientes para este tipo concreto de cálculo repetitivo, lo que desplazó a la minería por CPU hacia la irrelevancia. Más adelante aparecieron dispositivos programables llamados FPGA, y finalmente, desde 2013, chips diseñados específicamente y exclusivamente para calcular hashes SHA-256 lo más rápido y con el menor consumo eléctrico posible, llamados ASIC (Application-Specific Integrated Circuit). Hoy en día, la minería competitiva a gran escala se realiza casi exclusivamente con hardware ASIC especializado, operado en instalaciones industriales, un tema que retomaremos con detalle en el capítulo 23.

La recompensa del minero: subsidio más comisiones

El minero que encuentra el hash válido y consigue que su bloque sea aceptado por la red recibe una recompensa económica, compuesta por dos elementos: el subsidio por bloque (block subsidy), una cantidad de bitcoins recién creados que el propio protocolo asigna automáticamente (y que se reduce a la mitad periódicamente, como veremos en el capítulo 13), y la suma de todas las comisiones que pagaron las transacciones incluidas en ese bloque. Esta recompensa se paga a través de una transacción especial, llamada "coinbase", que es la primera transacción de todo bloque y que, a diferencia del resto, no consume ningún UTXO previo: es, literalmente, el punto donde nacen los bitcoins nuevos.

Minería en solitario frente a pools de minería

Dada la enorme potencia de cómputo total de la red actual, la probabilidad de que un minero individual encuentre un bloque en solitario es extremadamente baja, lo que generaría ingresos muy irregulares (podrían pasar años sin encontrar ningún bloque). Para suavizar esta variabilidad, la mayoría de los mineros se agrupan en "pools de minería": conjuntos de participantes que combinan su potencia de cómputo, y que reparten la recompensa de cada bloque encontrado, de forma proporcional al esfuerzo computacional aportado por cada uno, entre todos los miembros del pool, en lugar de que se la lleve entero quien encontró el bloque exacto por casualidad.

Con la minería ya explicada, en el próximo capítulo veremos cómo todos estos elementos -bloques, hashes, prueba de trabajo- se combinan para resolver el problema del consenso distribuido: cómo consigue una red de miles de nodos desconocidos entre sí ponerse de acuerdo sobre una única versión válida de la historia.

Fuentes y estudios citados en este capítulo

- Back, A. (2002). "Hashcash - A Denial of Service Counter-Measure". Documento técnico que formaliza el mecanismo de prueba de trabajo adoptado después por Bitcoin.
- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", secciones 4 y 11, sobre el mecanismo de prueba de trabajo y su ajuste de dificultad.
- Cambridge Centre for Alternative Finance. "Cambridge Bitcoin Electricity Consumption Index" (CBECI). Fuente de referencia para las estimaciones de hashrate y consumo energético de la red que se citan en el capítulo 23.

Capítulo 12. Los nodos y el consenso descentralizado

Se habla mucho de los mineros de Bitcoin, pero son, en realidad, los nodos -no los mineros- quienes tienen la última palabra sobre qué es y qué no es una transacción o un bloque válido. Este capítulo explica qué es un nodo, en qué se diferencia de un minero y cómo, entre todos, logran ponerse de acuerdo sin que nadie esté al mando.

Qué es un nodo

Un nodo de Bitcoin es, sencillamente, un ordenador que ejecuta el software de Bitcoin (el más habitual es Bitcoin Core, la implementación de referencia derivada directamente del código original de Satoshi Nakamoto) y que mantiene una copia completa -o, en algunas variantes, parcial- de la blockchain. Un "nodo completo" (full node) descarga y valida, de forma completamente independiente, cada bloque y cada transacción de toda la historia de Bitcoin desde el bloque génesis, comprobando que cumplen absolutamente todas las reglas del protocolo: que las firmas son válidas, que no hay doble gasto, que no se ha creado más dinero del permitido, que se respeta el límite de tamaño de bloque, y muchas más comprobaciones.

Cualquier persona puede, en principio, descargar el software gratuito de Bitcoin Core y ejecutar su propio nodo completo, con un ordenador relativamente modesto (el requisito principal es espacio de almacenamiento, ya que la blockchain completa ocupa varios cientos de gigabytes) y una conexión a internet razonable. En la actualidad existen varios decenas de miles de nodos completos públicamente visibles repartidos por todo el mundo, además de un número desconocido de nodos privados que no anuncian su presencia en la red.

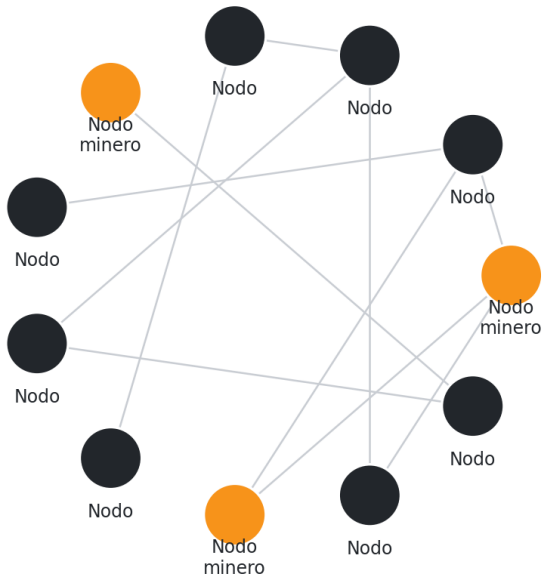
Nodos frente a mineros: un malentendido habitual

Existe una confusión muy extendida que conviene aclarar: los mineros no deciden las reglas de Bitcoin, ni pueden imponerlas al resto de la red. Un minero puede intentar incluir en un bloque una transacción que rompa las reglas del protocolo -por ejemplo, que intente crear bitcoins de la nada, o que reutilice un UTXO ya gastado-, pero si lo hace, cualquier nodo completo de la red rechazará automáticamente ese bloque en cuanto lo reciba, por no cumplir las reglas de validación, sin importar cuánta potencia de cómputo tenga ese minero. El bloque simplemente sería ignorado por el resto de la red, y el minero habría desperdiciado todo el trabajo computacional invertido en encontrarlo, sin recibir ninguna recompensa.

Este detalle es fundamental para entender el equilibrio de poder en Bitcoin: los mineros aportan la seguridad física de la red (mediante el coste de la prueba de trabajo) y proponen el orden de las transacciones, pero son los nodos -operados, potencialmente, por cualquier persona en el mundo, incluidos usuarios individuales sin ninguna potencia de minería- quienes tienen la autoridad final para aceptar o rechazar lo que los mineros proponen, verificando de forma independiente que cumple las reglas. Una analogía útil es la de un partido de fútbol: los mineros son como los jugadores, que proponen la jugada y hacen el esfuerzo físico sobre el campo, pero son los árbitros -los nodos, repartidos por todo el estadio y de acuerdo entre sí sobre el reglamento- quienes deciden si esa jugada es válida o si hay que anularla, sin que la fuerza o la velocidad de un jugador le dé ningún poder para cambiar las reglas del juego. A este equilibrio se le suele describir como el verdadero núcleo de la descentralización de Bitcoin: ni siquiera una mayoría abrumadora de mineros podría, por

ejemplo, aumentar el límite de 21 millones de bitcoins, porque los nodos simplemente rechazarían cualquier bloque que lo intentara.

La red descentralizada de nodos de Bitcoin



Cada nodo guarda una copia completa del libro de contabilidad y valida de forma independiente cada bloque y cada transacción.

La red descentralizada de nodos: cada uno valida de forma independiente.

Cómo se propaga la información por la red

Bitcoin utiliza una arquitectura de red "peer-to-peer" (entre iguales): cada nodo se conecta directamente con un número limitado de otros nodos (normalmente entre ocho y ciento veinticinco conexiones), sin que exista ningún servidor central que coordine las comunicaciones. Cuando un nodo recibe una transacción nueva o un bloque nuevo, y tras comprobar que es válido según sus propias reglas, lo retransmite inmediatamente a todos sus nodos conectados, que a su vez lo retransmiten a los suyos, y así sucesivamente, de forma que la información se propaga por toda la red en cuestión de segundos, mediante un mecanismo conocido como "gossip" (rumor).

¿Y si dos mineros encuentran un bloque casi al mismo tiempo?

Dado que la red está distribuida geográficamente y las comunicaciones tardan un tiempo -pequeño, pero no nulo- en propagarse, puede ocurrir que dos mineros distintos, en lugares diferentes del mundo, encuentren un bloque válido casi simultáneamente, cada uno basándose en el mismo bloque anterior. Esto crea, temporalmente, dos versiones distintas de "cuál es el último bloque", una situación llamada bifurcación temporal o "fork" (en su sentido más técnico y benigno, sin relación necesaria con los forks del capítulo 21).

La regla que resuelve esta situación, definida en el propio whitepaper, es sencilla: cada nodo considera válida, en caso de empate, la cadena que representa mayor cantidad total de trabajo computacional acumulado -en la práctica, casi siempre la cadena más larga-. Cuando se mina el siguiente bloque sobre una de las dos ramas, esa rama se vuelve más larga que la otra, y todos los nodos convergen automáticamente hacia ella, descartando ("huérfanando") el bloque de la rama más corta. Las transacciones del bloque huérfano que no llegaron a incluirse en la cadena ganadora vuelven a la mempool, a la espera de ser incluidas en un bloque futuro.

Por qué las confirmaciones importan tanto

Esta posibilidad de bifurcaciones temporales explica por qué, como vimos en el capítulo 7, se recomienda esperar varias confirmaciones antes de considerar una transacción definitivamente segura, especialmente para importes elevados: cuantos más bloques se han añadido después de una transacción, más improbable resulta que esa parte de la cadena termine siendo descartada en favor de una rama alternativa.

La descentralización como propiedad, no como eslogan

Es habitual escuchar que Bitcoin es "descentralizado", pero conviene entender exactamente en qué sentido lo es: no existe una empresa, fundación o gobierno que controle el protocolo, ni ningún servidor cuya caída detendría la red, ni ninguna autoridad capaz de censurar transacciones concretas sin el consentimiento (voluntario o forzado) de una parte sustancial de los participantes. Esto no significa que Bitcoin sea inmune a toda forma de concentración de poder -en los capítulos 16 y 23 analizaremos, con honestidad, dónde existen hoy ciertos grados de concentración, por ejemplo en la minería o en el desarrollo del software-, pero sí que su diseño elimina, de raíz, cualquier punto único cuya intervención pudiera detener o alterar unilateralmente el sistema completo.

En el próximo capítulo dejaremos el terreno del consenso y la seguridad para entrar en la dimensión económica de Bitcoin: cómo se crea y se reparte exactamente el suministro de nuevos bitcoins, y por qué su límite de 21 millones es, quizá, su característica más citada -y también una de las más malentendidas.

Fuentes y estudios citados en este capítulo

- Lamport, L., Shostak, R., Pease, M. (1982). "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems, 4(3).
- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sección 5, "Network", sobre la propagación de bloques y la regla de la cadena más larga.
- Bitnodes (bitnodes.io), proyecto independiente de rastreo del número y la distribución geográfica de nodos completos públicamente visibles en la red de Bitcoin.

Capítulo 13. La oferta monetaria: emisión, halving y los 21 millones

Pocas cifras son tan repetidas en torno a Bitcoin como el límite de 21 millones de unidades. Este capítulo explica de dónde sale exactamente esa cifra, cómo se van creando los bitcoins con el tiempo, qué es el "halving" y qué implicaciones económicas tiene un sistema monetario con una oferta fija y conocida de antemano.

Cómo se crean los bitcoins nuevos

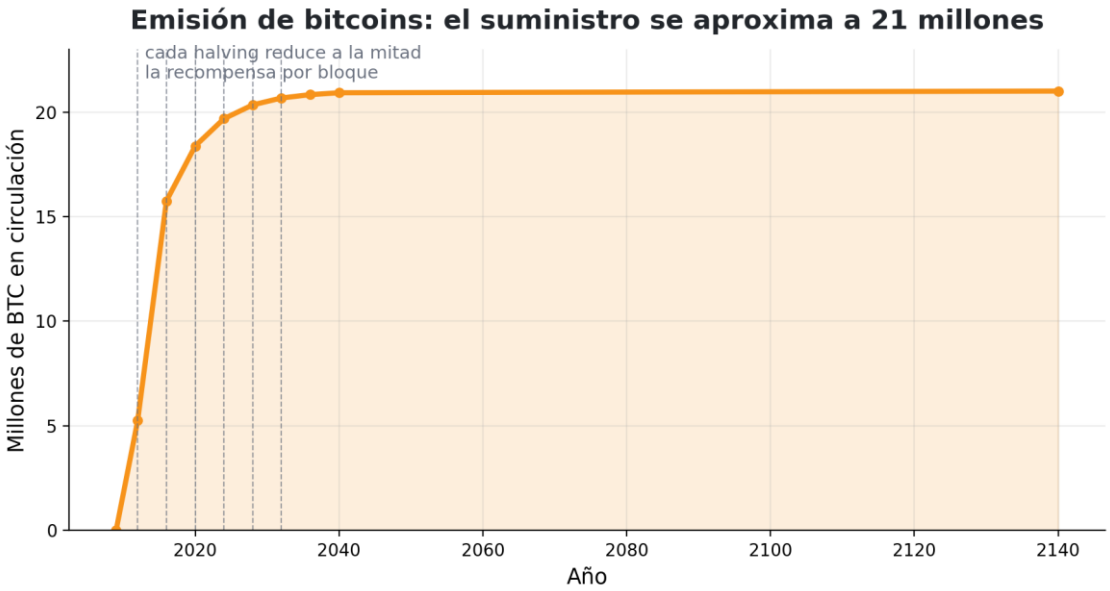
Como vimos en el capítulo 11, los bitcoins nuevos se crean exclusivamente a través de la transacción coinbase que encabeza cada bloque minado: es la única vía posible para que existan bitcoins nuevos en circulación. No existe ningún otro mecanismo -ni banco central, ni comité, ni votación- que pueda crear bitcoins adicionales al margen de esta regla, que está fijada en el propio código del protocolo y que solo podría cambiarse si una fracción abrumadora de la comunidad (nodos, mineros, usuarios, empresas) aceptara voluntariamente adoptar un cambio de software que la modificara, algo que, dada la resistencia casi religiosa de la comunidad a alterar esta regla concreta, se considera extraordinariamente improbable.

El halving: la recompensa se reduce a la mitad

Cuando Bitcoin se puso en marcha en 2009, la recompensa por cada bloque minado era de cincuenta bitcoins. El protocolo especifica que, cada 210.000 bloques -aproximadamente cada cuatro años, dado el ritmo medio de un bloque cada diez minutos-, esa recompensa se reduce exactamente a la mitad. A este evento se le llama "halving" (o, en español, a veces "reducción a la mitad").

- Noviembre de 2012: la recompensa bajó de 50 a 25 BTC por bloque.
- Julio de 2016: bajó de 25 a 12,5 BTC por bloque.
- Mayo de 2020: bajó de 12,5 a 6,25 BTC por bloque.
- Abril de 2024: bajó de 6,25 a 3,125 BTC por bloque.

Este proceso continuará, reduciéndose a la mitad cada aproximadamente cuatro años, hasta que la recompensa por bloque sea tan diminuta que, alrededor del año 2140, se considerará -por el redondeo inherente a trabajar con la unidad mínima indivisible de Bitcoin- que ya no quedan más bitcoins nuevos por emitir, alcanzándose así, de forma asintótica, el límite total de 21 millones de unidades.



La emisión de bitcoins se aproxima gradualmente a 21 millones a través de sucesivos halvings.

Por qué el límite es (aproximadamente) 21 millones

La cifra de 21 millones no es arbitraria en el sentido de tener algún significado místico, sino que es, simplemente, el resultado matemático de sumar una serie geométrica decreciente: 210.000 bloques a 50 BTC, más 210.000 bloques a 25 BTC, más 210.000 a 12,5 BTC, y así sucesivamente, hasta el infinito. Esa suma converge matemáticamente a un valor ligeramente inferior a 21 millones. Este diseño convierte a Bitcoin en el primer activo de la historia -digital o físico- cuya oferta máxima total es conocida de antemano, con precisión matemática, y no puede alterarse sin el consentimiento generalizado de toda la red.

El satoshi: la unidad más pequeña

Bitcoin es divisible hasta ocho decimales. La unidad más pequeña posible se llama "satoshi" (o "sat"), en honor a su creador, y equivale a 0,00000001 BTC; es decir, un bitcoin completo se compone de cien millones de satoshis. Esta divisibilidad extrema resuelve, de raíz, una preocupación habitual entre quienes descubren que el precio de un bitcoin entero puede ser muy elevado: no hace falta comprar un bitcoin completo para participar en la red, del mismo modo que no hace falta comprar un lingote de oro entero para poseer algo de oro. Es perfectamente posible, y de hecho habitual, comprar, poseer y transferir cantidades muy pequeñas, del orden de unos pocos miles o incluso unos pocos cientos de satoshis.

Qué ocurrirá cuando se agote la emisión

Alrededor del año 2140, cuando ya no se emitan nuevos bitcoins, los mineros dejarán de recibir el subsidio por bloque y su único incentivo económico para seguir asegurando la red serán las comisiones pagadas por los usuarios en cada transacción (el segundo componente de la recompensa del minero, que mencionamos en el capítulo 11). Uno de los debates económicos más interesantes -y todavía abiertos- dentro de la comunidad técnica de Bitcoin es si el mercado de comisiones, por sí solo, será suficiente para mantener un nivel de seguridad comparable al actual dentro de más de un siglo, una discusión en la que influyen

factores como el previsible crecimiento del volumen de transacciones, el desarrollo de soluciones de segunda capa (capítulo 22) y la propia evolución del valor de Bitcoin.

Escasez absoluta frente a escasez relativa: la comparación con el oro

Recordando el capítulo 1, el oro es escaso, pero no de forma absoluta: si mañana se descubriera una técnica más barata para extraer oro del fondo del océano, o se empezara a minar oro de asteroides a gran escala -una posibilidad que algunas empresas han explorado seriamente-, la oferta mundial de oro podría aumentar de forma significativa e impredecible. Bitcoin, en cambio, tiene una escasez absoluta y verificable por cualquiera que ejecute un nodo: su límite de 21 millones (menos, en realidad, ya que se estima que una parte de los bitcoins existentes se ha perdido para siempre, por pérdida de claves privadas, como veremos en el capítulo 19) no puede alterarse por ningún descubrimiento tecnológico ni por ninguna decisión política, salvo el consenso extremadamente improbable de prácticamente toda la red.

Esta propiedad es la base del argumento, defendido por muchos partidarios de Bitcoin, de que constituye un activo especialmente adecuado como depósito de valor a largo plazo, en contraste con las monedas fiat, cuya oferta puede aumentar según la decisión de un banco central. Conviene señalar, sin embargo, que este argumento no es aceptado de forma unánime entre economistas, y que la volatilidad histórica de Bitcoin (que analizaremos en el capítulo 26) complica, al menos por ahora, su comparación directa con activos refugio tradicionales como el oro.

En el próximo capítulo cerraremos esta parte técnica del libro con el análisis de las comisiones: cómo se determinan, por qué varían tanto de un momento a otro, y qué ocurre cuando la red se satura de transacciones pendientes.

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sección 6, "Incentive", sobre el diseño de la recompensa por bloque y su reducción progresiva.
- Hayes, A. (2019). "Bitcoin price and its marginal cost of production: support for a fundamental value". Applied Economics Letters. Estudio académico sobre la relación entre el coste de minería y el valor de mercado de Bitcoin.
- Registro público de la blockchain de Bitcoin, fuente primaria verificable por cualquiera para confirmar las fechas exactas de cada halving.

Capítulo 14. Comisiones y el mercado de las fees

Cualquiera que haya usado Bitcoin en un momento de mucha actividad en la red se habrá encontrado con una realidad incómoda: las comisiones no son fijas, y a veces resultan sorprendentemente altas. Este capítulo explica por qué funcionan así, cómo se determinan y qué relación tienen con el tamaño limitado de los bloques.

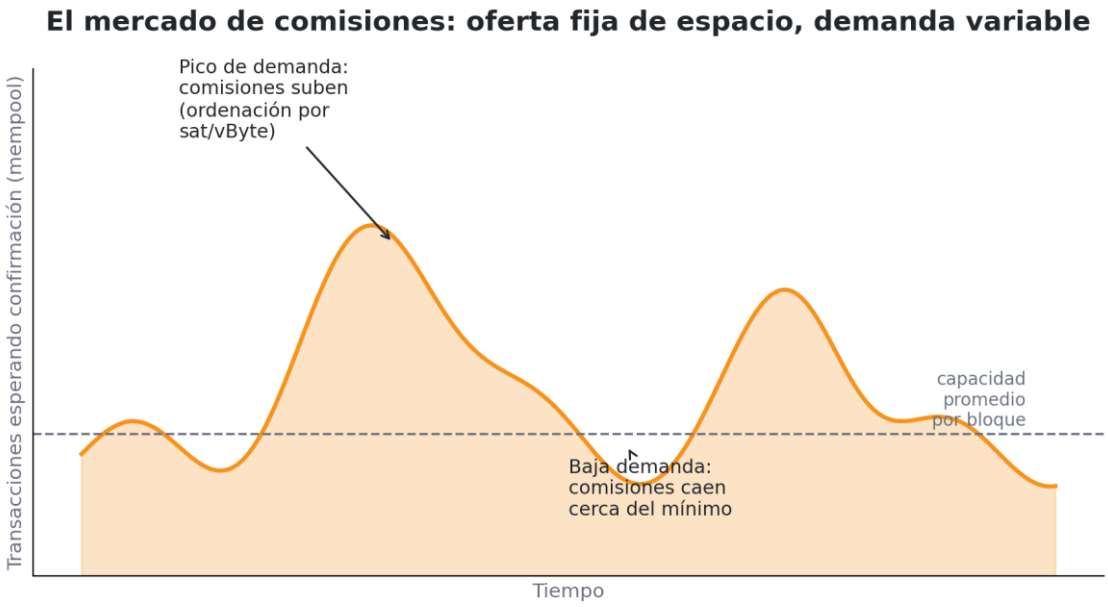
Por qué existe un límite de tamaño de bloque

Cada bloque de Bitcoin tiene un límite de tamaño (medido, desde la mejora SegWit de 2017 que veremos en el capítulo 21, en una unidad llamada "peso" o weight, aunque a efectos prácticos suele hablarse de un límite equivalente a alrededor de entre uno y cuatro megabytes, según cómo se compongan las transacciones incluidas). Este límite no es un descuido, sino una decisión de diseño deliberada: bloques más grandes contendrían más transacciones y podrían, en teoría, reducir las comisiones al haber más espacio disponible, pero también tardarían más en propagarse por toda la red mundial y ocuparían más espacio de almacenamiento en cada nodo completo, lo que dificultaría que usuarios con ordenadores y conexiones modestas pudieran seguir ejecutando un nodo propio -un requisito que, como vimos en el capítulo 12, es clave para mantener la descentralización real de la red. Este equilibrio, entre capacidad de transacción y accesibilidad para ejecutar nodos, fue precisamente el centro del debate que analizaremos en el capítulo 21.

Cómo se forma el precio de una comisión: subasta de espacio

Dado que el espacio en cada bloque es limitado, y la demanda de transacciones varía constantemente, Bitcoin funciona, en la práctica, como una subasta continua por el espacio disponible en el siguiente bloque, de forma muy parecida a un peaje de carretera con tarifa dinámica: cuando hay poco tráfico, cruzar cuesta casi nada, pero en hora punta el precio sube porque muchos coches compiten por el mismo carril disponible. Cada usuario que quiere enviar una transacción decide qué comisión está dispuesto a pagar, expresada normalmente en satoshis por unidad de peso de la transacción (una transacción más compleja, con más entradas o salidas, ocupa más espacio y, por tanto, suele requerir una comisión total mayor para la misma prioridad).

Los mineros, que buscan maximizar sus ingresos, tienden a priorizar las transacciones pendientes en la mempool que ofrecen la comisión más alta por unidad de espacio, dejando fuera del siguiente bloque -temporalmente- las que ofrecen menos. Cuando hay pocas transacciones esperando, casi cualquier comisión, por pequeña que sea, basta para entrar en el siguiente bloque; cuando hay mucha congestión, solo las transacciones que ofrecen comisiones más generosas consiguen una confirmación rápida, mientras el resto espera, a veces durante horas o incluso días, hasta que se libera espacio.



Representación conceptual del mempool y la subasta de espacio por bloque; no refleja datos reales de ningún periodo concreto.

El mercado de comisiones funciona como una subasta continua: la demanda varía, la oferta de espacio por bloque no.

Qué provoca los picos de comisiones

Históricamente, los mayores picos de comisiones en Bitcoin han coincidido con periodos de fuerte interés especulativo y aumento súbito del número de usuarios -como ocurrió a finales de 2017 y, de nuevo, en ciertos momentos de 2021 y 2023-, así como con la aparición de nuevos usos que generan un volumen inesperado de transacciones, como los llamados "Ordinals" e "inscripciones" (una forma de incrustar datos adicionales, como imágenes, dentro de transacciones de Bitcoin, popularizada desde 2023), que en determinados momentos han llegado a competir de forma intensa por el espacio limitado de los bloques con las transacciones puramente monetarias.

Cómo estiman las wallets la comisión adecuada

La mayoría de las wallets modernas incluyen un estimador automático de comisiones, que analiza el estado actual de la mempool y sugiere una comisión razonable según la urgencia deseada por el usuario (por ejemplo, "próximo bloque", "en menos de una hora" o "sin prisa, en las próximas veinticuatro horas"). Estos estimadores no son perfectos -la congestión de la red puede cambiar de forma repentina entre el momento de construir la transacción y el momento de transmitirla-, pero suelen dar una aproximación razonable en circunstancias normales.

Herramientas para gestionar comisiones mal calculadas

Cuando una transacción se envía con una comisión demasiado baja para las condiciones actuales de la red, puede quedar "atascada" en la mempool durante mucho tiempo sin ser confirmada. El protocolo de Bitcoin ofrece dos mecanismos principales para resolver esta situación:

- Replace-By-Fee (RBF): permite reemplazar una transacción no confirmada por una versión nueva, idéntica salvo por una comisión más alta, siempre que la transacción original se haya marcado explícitamente como reemplazable al crearla. Es como volver a hacer la misma oferta en una subasta, pero por un importe mayor, retirando la puja anterior antes de que nadie la haya aceptado todavía.
- Child-Pays-For-Parent (CPFP): permite crear una nueva transacción que gaste como entrada una salida de la transacción atascada, pagando una comisión lo bastante alta como para que, sumada a la de la transacción original, resulte rentable para un minero incluir ambas juntas en el mismo bloque. Funciona como pagar tú la propina que le faltaba a un compañero de mesa para que el camarero atienda el pedido conjunto de los dos cuanto antes.

Comisiones y segunda capa: por qué existe Lightning Network

Este mercado de comisiones, con su volatilidad inherente, es una de las razones fundamentales que impulsaron el desarrollo de soluciones de "segunda capa" como Lightning Network, que estudiaremos en detalle en el capítulo 22: sistemas que permiten realizar muchísimos pagos pequeños fuera de la cadena principal (off-chain), liquidando después, con una única transacción en la cadena principal, el resultado neto de multitud de pagos individuales. Esto permite que Bitcoin escale su capacidad de procesar pagos sin necesidad de aumentar indefinidamente el tamaño de los bloques, preservando el equilibrio entre capacidad y descentralización que mencionamos al principio de este capítulo.

> *Las comisiones de Bitcoin no son un defecto del sistema, sino la consecuencia directa y deliberada de un espacio de bloque limitado a propósito, para preservar la posibilidad de que cualquiera, en cualquier parte del mundo, pueda seguir ejecutando su propio nodo completo y participando en igualdad de condiciones en la validación de la red.*

Con esto concluye la Parte III de este libro, dedicada al funcionamiento técnico de Bitcoin. En la Parte IV entraremos en el terreno de la seguridad: qué ataques son teóricamente posibles contra Bitcoin, cuáles ya se han producido en la práctica -normalmente no contra el protocolo en sí, sino contra usuarios y plataformas- y cómo protegerse de ellos.

Fuentes y estudios citados en este capítulo

- Easley, D., O'Hara, M., Basu, S. (2019). "From Mining to Markets: The Evolution of Bitcoin Transaction Fees". Journal of Financial Economics, 134(1). Estudio académico de referencia sobre la formación de precios en el mercado de comisiones de Bitcoin.
- Wuille, P., Lombrozo, E., Lau, J. (2015-2017). "BIP-141: Segregated Witness (Consensus layer)". Bitcoin Improvement Proposal que introdujo SegWit y su efecto sobre el cálculo del tamaño de bloque.
- Mempool.space y otros exploradores públicos de la mempool, usados habitualmente para observar en tiempo real el estado del mercado de comisiones descrito en este capítulo.

PARTE IV

SEGURIDAD Y ATAQUES

Capítulo 15. El modelo de seguridad de Bitcoin

Antes de repasar ataques concretos, conviene entender el marco general en el que se piensa la seguridad de Bitcoin, porque es distinto del marco con el que solemos pensar en la seguridad de un banco o de un sistema informático tradicional. Este capítulo sienta las bases conceptuales que usaremos durante el resto de la Parte IV.

Seguridad basada en incentivos económicos, no solo en criptografía

Buena parte de la seguridad informática tradicional se basa en impedir físicamente que alguien haga algo: cifrados que no se pueden romper, permisos que bloquean accesos no autorizados. Bitcoin añade a esto una capa adicional, y en cierto modo más sofisticada: un diseño de incentivos económicos que hace que comportarse honestamente sea, para la inmensa mayoría de los participantes, más rentable que intentar hacer trampas.

Un minero podría, en teoría, intentar incluir transacciones fraudulentas en un bloque. Pero como vimos en el capítulo 12, cualquier nodo de la red rechazaría ese bloque de inmediato, y el minero perdería todo el coste eléctrico y de hardware invertido en encontrarlo, sin recibir ninguna recompensa a cambio. El propio diseño hace que el fraude evidente sea, casi siempre, una estrategia perdedora desde el punto de vista puramente económico, sin necesidad de que nadie tenga que "impedirlo" activamente.

Distintos niveles de seguridad, distintos ataques

Los cuatro niveles de seguridad de Bitcoin: cuanto más se aleja el nivel de la criptografía pura, más incidentes reales se han producido en la práctica.

Es útil distinguir, desde el principio, entre varios niveles distintos de seguridad, porque los ataques que analizaremos en los próximos capítulos operan en niveles muy diferentes, y confundirlos es una fuente habitual de malentendidos en los debates públicos sobre Bitcoin.

- Seguridad del protocolo: la robustez de las reglas de consenso y de la criptografía subyacente (funciones hash, firmas digitales). Hasta la fecha, no se ha encontrado ninguna vulnerabilidad práctica que rompa estos fundamentos; es, en cierto modo, la caja fuerte más probada del sistema, el cimiento sobre el que se apoya todo lo demás.
- Seguridad de la red: la resistencia de la red de nodos y mineros frente a intentos de manipular el historial de transacciones o censurar transacciones concretas (capítulos 16 y 17). Aquí es donde entran en juego el tamaño y la diversidad geográfica de la red, más que la criptografía en sí.
- Seguridad de los usuarios y las plataformas: la protección de las claves privadas individuales y de las empresas (exchanges, custodios) que gestionan bitcoin en nombre de terceros (capítulo 18). Este nivel depende, sobre todo, de buenas prácticas humanas y organizativas, no de las matemáticas del protocolo.
- Seguridad frente a errores humanos: pérdidas de fondos que no son ataques de nadie, sino consecuencia de descuidos, olvidos o malas prácticas (capítulo 19). Es, paradójicamente, el nivel más "tonto" de los cuatro y, a la vez, el que más dinero real se ha llevado por delante a lo largo de la historia de Bitcoin.

La inmensa mayoría de los bitcoins perdidos o robados a lo largo de la historia lo han sido en los dos últimos niveles -usuarios y plataformas, o errores humanos-, no por ninguna

vulnerabilidad del protocolo en sí. Este dato, respaldado por prácticamente todos los análisis serios del historial de incidentes de Bitcoin, contradice una percepción popular bastante extendida, que tiende a atribuir estos incidentes a "un fallo de Bitcoin" cuando, en la mayoría de los casos, el protocolo funcionó exactamente como estaba diseñado.

Por qué conviene separar estos niveles al valorar un riesgo

Confundir estos cuatro niveles es, probablemente, la fuente más habitual de malentendidos en cualquier discusión pública sobre la seguridad de Bitcoin, dentro y fuera de la comunidad. Cuando un exchange sufre un hackeo (nivel de usuarios y plataformas) y un titular de prensa lo resume como "hackean Bitcoin", se está atribuyendo al protocolo -el nivel más probado y menos vulnerado de los cuatro- un fallo que en realidad ocurrió varios pisos por encima, en una empresa concreta con sus propias prácticas de seguridad, buenas o malas. Lo mismo ocurre a la inversa: alguien que pierde el acceso a su wallet por no haber guardado correctamente la frase semilla (nivel de errores humanos) puede sentir la tentación de concluir que "Bitcoin no es seguro", cuando el protocolo, en ese caso concreto, hizo exactamente lo que estaba diseñado para hacer: proteger esos fondos de cualquiera que no tuviera la clave correcta, incluido su propio dueño despistado. Separar estos niveles con claridad no es un simple ejercicio académico: permite dirigir el esfuerzo de protección personal hacia donde realmente importa -sobre todo los dos niveles superiores, usuarios y errores humanos, que concentran la inmensa mayoría de las pérdidas reales-, en lugar de preocuparse, por ejemplo, de un hipotético fallo criptográfico del protocolo que, a día de hoy, no tiene ningún precedente documentado en más de quince años de funcionamiento ininterrumpido.

El "modelo de amenaza": pensar como un atacante, con honestidad

Los profesionales de la seguridad informática utilizan un concepto llamado "modelo de amenaza" (threat model): antes de diseñar o evaluar una defensa, hay que definir con precisión de qué se está protegiendo exactamente, y frente a qué tipo de adversario. Aplicado a Bitcoin, esto significa distinguir con claridad preguntas como: ¿puede alguien falsificar una firma digital sin conocer la clave privada? (No, con la tecnología actual). ¿Puede alguien reescribir transacciones de hace diez años? (Es teóricamente posible, pero extraordinariamente costoso, como veremos en el capítulo 16). ¿Puede alguien robarte tus bitcoins si consigue acceso físico a tu móvil desbloqueado con la wallet abierta? (Sí, casi con toda seguridad).

Adoptar esta mentalidad -evaluar cada riesgo de forma específica, en lugar de tratar "la seguridad de Bitcoin" como una pregunta de sí o no- es la actitud correcta con la que abordar el resto de esta parte del libro, y también la actitud más útil para protegerte de verdad en la práctica, como retomaremos en el capítulo 25.

Bitcoin lleva más de quince años sin ser hackeado en su núcleo

Un dato relevante para poner en contexto los capítulos siguientes: desde su lanzamiento en enero de 2009, el protocolo central de Bitcoin -las reglas de consenso, la criptografía subyacente- no ha sufrido ningún compromiso exitoso que haya permitido crear bitcoins de la nada, falsificar firmas o gastar bitcoins ajenos sin la clave privada correspondiente. Ha habido, eso sí, algunos incidentes puntuales en el propio software de referencia en sus primerísimos años (el más citado es un error de 2010 que permitió crear una cantidad enorme

de bitcoins de forma fraudulenta durante unas pocas horas, corregido mediante un cambio de software coordinado con la comunidad antes de que causara ningún daño real), y numerosas vulnerabilidades detectadas y corregidas de forma responsable a lo largo de los años por investigadores de seguridad. Pero el diseño fundamental del sistema —la combinación de prueba de trabajo, criptografía de clave pública y reglas de consenso verificadas por nodos independientes— ha demostrado, a lo largo de más de una década y media de funcionamiento ininterrumpido, procesando cientos de miles de millones de dólares en valor, una robustez que pocos sistemas informáticos pueden reivindicar.

En los próximos capítulos analizaremos, uno por uno, los principales vectores de ataque contra Bitcoin: empezando por el más citado de todos, el ataque del 51%, y siguiendo con ataques a la red, ataques a usuarios y plataformas, errores humanos y, finalmente, la pregunta sobre el futuro que más se repite en los últimos años: ¿podría la computación cuántica romper Bitcoin?

Fuentes y estudios citados en este capítulo

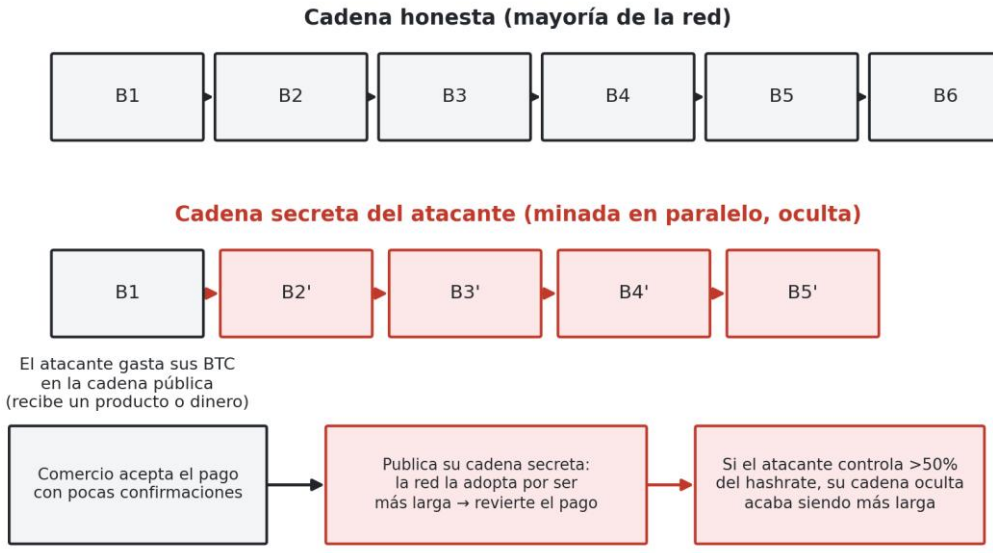
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., Felten, E. (2015). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". IEEE Symposium on Security and Privacy. Panorámica académica de referencia sobre los distintos niveles de seguridad de Bitcoin usada como base conceptual de este capítulo.
- Bitcoin Core, registro de historial de versiones (changelog) y de vulnerabilidades divulgadas de forma responsable a lo largo de los años, incluida la corrección del error de desbordamiento de valor ("value overflow incident") detectado y solucionado en agosto de 2010.

Capítulo 16. El ataque del 51% y el doble gasto

Si has leído o escuchado algo sobre los riesgos de seguridad de Bitcoin, es casi seguro que te has topado con el término "ataque del 51%". Es, con diferencia, el ataque más mencionado -y también uno de los más malentendidos- contra la red. Este capítulo explica exactamente en qué consiste, qué podría lograr un atacante con éxito, qué NO podría lograr, y por qué resulta tan costoso llevarlo a cabo contra Bitcoin en la actualidad.

En qué consiste exactamente

Recordemos, del capítulo 12, que cuando dos versiones distintas de la cadena compiten entre sí, la red adopta la que representa mayor cantidad de trabajo computacional acumulado. Un ataque del 51% consiste en que un atacante -o una coalición de atacantes- consiga controlar más de la mitad de todo el poder de cómputo (hashrate) dedicado a minar Bitcoin en un momento dado. Con esa mayoría, el atacante podría, en teoría, minar en secreto una cadena alternativa más rápido que el resto de la red honesta minando la cadena pública, y en algún momento publicarla, forzando a la red a adoptarla por ser más larga (por representar más trabajo acumulado).



Cómo funcionaría, en teoría, un ataque del 51% con doble gasto.

El escenario típico: doble gasto contra un comercio

El uso práctico más citado de este ataque es el doble gasto: el atacante realiza un pago legítimo, en apariencia, a un comercio o a un exchange -por ejemplo, para comprar un producto caro o para retirar fondos de una plataforma-, y esa transacción se incluye en la cadena pública. El comercio, tras ver una o varias confirmaciones, entrega el producto o el servicio. Mientras tanto, en paralelo y en secreto, el atacante ha estado minando una cadena alternativa que no incluye esa transacción de pago, sino que reserva esos mismos fondos para gastarlos de nuevo. Si el atacante consigue que su cadena secreta supere en longitud a la cadena pública y la publica, la red la adoptará como la válida, y la transacción de pago original desaparecerá del historial -como si nunca hubiera ocurrido-, mientras el atacante

conserva sus bitcoins y, además, se ha quedado con el producto o servicio que recibió del comercio engañado.

Qué NO puede hacer un atacante con el 51%

Es fundamental entender los límites de este ataque, porque a menudo se exagera su alcance en discusiones informales. Incluso con una mayoría absoluta del hashrate, un atacante NO podría:

- Crear bitcoins de la nada, más allá de las reglas de emisión del protocolo (recordemos, del capítulo 12, que los nodos rechazarían cualquier bloque que lo intentara). Ni siquiera controlando toda la potencia de cómputo del planeta podría un atacante convencer a los árbitros -los nodos- de aceptar una jugada que rompe el reglamento.
- Robar bitcoins de direcciones ajenas sin conocer sus claves privadas: no puede falsificar firmas digitales, porque el hashrate no tiene ninguna influencia sobre la criptografía de curva elíptica del capítulo 3, que sigue siendo tan segura frente a un atacante con el 90% del hashrate como frente a uno con el 1%.
- Alterar transacciones muy antiguas, ya confirmadas hace mucho tiempo, sin rehacer literalmente todo el trabajo computacional acumulado desde entonces, lo que resulta, en la práctica, imposible más allá de unos pocos bloques recientes: es como intentar reescribir la primera página de un diario encuadernado hace años sin que se note que todas las páginas posteriores tuvieron que rehacerse también.
- Cambiar las reglas del protocolo, como el límite de 21 millones o el tamaño de bloque, sin el consentimiento del resto de la red (los nodos, no los mineros, deciden qué reglas aceptar, como vimos en el capítulo 12).

En resumen: el ataque del 51% permite, como mucho, revertir transacciones muy recientes propias del propio atacante (para hacer doble gasto) o censurar temporalmente transacciones ajenas, pero no permite robar fondos de terceros ni alterar las reglas fundamentales del sistema.

Por qué es tan caro llevarlo a cabo contra Bitcoin

Ejecutar este ataque contra la red de Bitcoin en su estado actual exigiría adquirir u operar una cantidad de hardware ASIC especializado (capítulo 11 y 23) y un consumo eléctrico comparables a los que hoy despliega, de forma legítima y repartida por todo el planeta, toda la industria minera de Bitcoin junta -una inversión de miles de millones de dólares en hardware, además de un coste energético operativo constante, sostenido mientras dure el ataque-. A esto hay que sumar un problema económico adicional: si el ataque tiene éxito y se hace público, es previsible que la confianza en Bitcoin -y, por tanto, su precio de mercado- caiga de forma drástica, lo que reduciría enormemente el valor tanto de los bitcoins que el atacante pretendiera obtener mediante doble gasto como del propio hardware de minería especializado que compró para el ataque, que perdería buena parte de su utilidad económica una vez cumplido su propósito.

Esta combinación de coste técnico extraordinario y de incentivo económico perverso (el propio éxito del ataque devalúa lo que se pretendía robar) es la razón principal por la que, hasta la fecha, nunca se ha producido un ataque del 51% exitoso contra la red principal de Bitcoin.

Ataques del 51% en la práctica: sí han ocurrido, pero en otras redes

Este ataque no es puramente teórico: se ha ejecutado con éxito varias veces contra criptomonedas más pequeñas, con un hashrate total mucho menor y, por tanto, mucho más barato de igualar o superar. Bitcoin Gold, Ethereum Classic y Vertcoin, entre otras, han sufrido ataques del 51% documentados y con pérdidas económicas reales para exchanges y usuarios, precisamente porque su seguridad total -determinada por el coste de reunir la mayoría del hashrate- es varios órdenes de magnitud inferior a la de Bitcoin.

Un matiz importante: el ataque no exige el 51% exacto

Conviene aclarar un matiz técnico: el nombre "ataque del 51%" es, en cierto modo, una simplificación popular. Investigaciones académicas posteriores al whitepaper original -en particular sobre una estrategia llamada "selfish mining" o minería egoísta, que analizaremos en el próximo capítulo- han demostrado que, bajo determinadas condiciones, un atacante podría obtener ciertas ventajas desproporcionadas con algo menos del 50% del hashrate total, aunque estas variantes son más complejas de ejecutar con éxito y sus ventajas prácticas resultan, en cualquier caso, mucho más limitadas que las de un control mayoritario total.

En el próximo capítulo seguiremos en el terreno de los ataques a la propia red, analizando otras estrategias -Sybil, eclipse y minería egoísta- que no requieren una mayoría del hashrate, sino que explotan otras características de cómo se comunican los nodos entre sí.

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sección 11, "Calculations", con el análisis probabilístico original de un ataque de reescritura de la cadena.
- Rosenfeld, M. (2014). "Analysis of Hashrate-Based Double Spending". Estudio independiente que amplía el modelo matemático del whitepaper para distintos escenarios de doble gasto.
- Eyal, I., Sirer, E. G. (2014). "Majority is not Enough: Bitcoin Mining is Vulnerable". Financial Cryptography and Data Security, LNCS 8437. Referencia académica del matiz sobre el umbral real necesario para ciertas ventajas desproporcionadas, ampliada en el próximo capítulo.
- Casos documentados de ataques del 51% contra Bitcoin Gold (2018) y Ethereum Classic (2019), recogidos en informes públicos de los propios exchanges afectados y de firmas de seguridad blockchain.

Capítulo 17. Ataques a la red: Sybil, eclipse y minería egoísta

Además del ataque del 51% que vimos en el capítulo anterior, existen otras familias de ataques dirigidos contra la propia infraestructura de red de Bitcoin -no contra sus fundamentos criptográficos, sino contra la forma en que los nodos se comunican entre sí-. Este capítulo repasa las tres más estudiadas: los ataques Sybil, los ataques eclipse y la minería egoísta.

El ataque Sybil: multiplicar identidades falsas

El nombre de este ataque proviene de un caso psiquiátrico real, popularizado por un libro y una película de los años setenta sobre una mujer diagnosticada con un trastorno de identidad disociativo con múltiples personalidades. En el contexto de las redes distribuidas, un "ataque Sybil" consiste en que un único atacante crea una gran cantidad de identidades falsas (en este caso, nodos falsos) para intentar obtener una influencia desproporcionada sobre la red, haciéndose pasar por muchos participantes independientes cuando en realidad todos están controlados por la misma persona.

En Bitcoin, crear nodos falsos es trivial y barato -cualquiera puede poner en marcha cientos de nodos con relativamente poco esfuerzo-, pero esto, por sí solo, no le da al atacante ningún poder real sobre las reglas de consenso: como vimos en el capítulo 12, cada nodo valida las reglas de forma completamente independiente, basándose en criptografía verificable, no en un recuento de votos entre nodos. Tener muchos nodos falsos no permite, por ejemplo, aprobar bloques inválidos ni cambiar el límite de 21 millones. El riesgo real de un ataque Sybil en Bitcoin no está en la validación del consenso, sino en la capa de comunicación de la red, y es precisamente lo que hace posible el siguiente ataque.

El ataque eclipse: aislar a una víctima

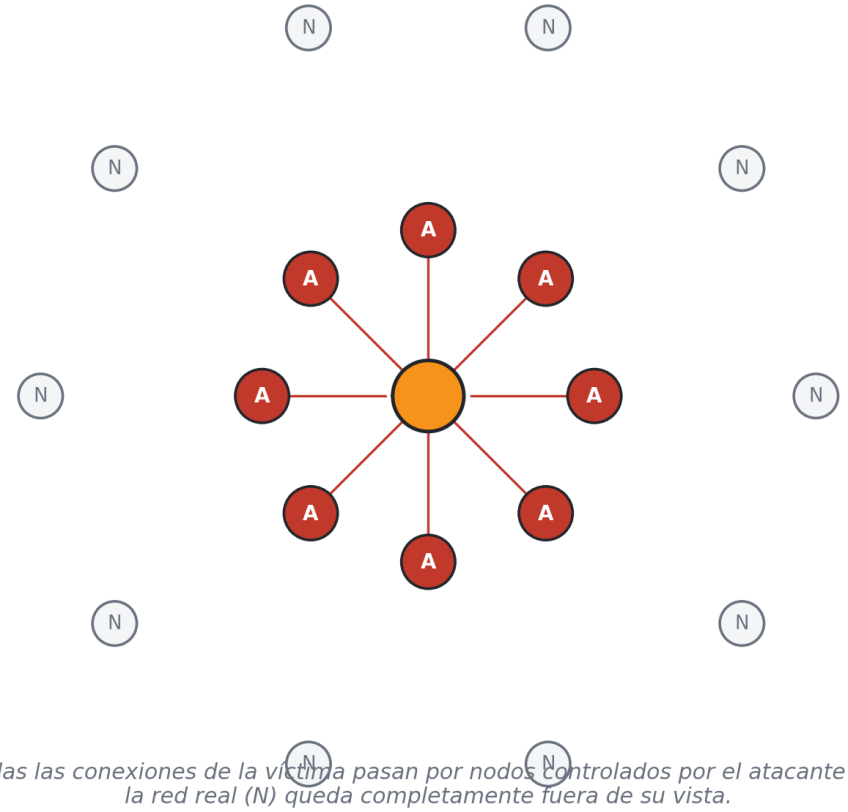
Un ataque eclipse es una forma más dirigida y potencialmente más dañina de aprovechar un gran número de nodos falsos: en lugar de intentar influir sobre toda la red, el atacante concentra sus esfuerzos en rodear las conexiones de un único nodo víctima, consiguiendo que todas -o casi todas- las conexiones de ese nodo con el resto de la red pasen, sin que la víctima lo sepa, a través de nodos controlados por el atacante.

Una vez "eclipsado" de esta forma, el nodo víctima queda aislado de la visión real de la red: el atacante puede mostrarle una versión manipulada de la blockchain o de las transacciones pendientes, ocultarle transacciones legítimas, hacerle creer que ha recibido un pago que en realidad no se ha confirmado en la cadena real, o incluso facilitar un ataque de doble gasto dirigido específicamente contra esa víctima concreta (por ejemplo, un exchange o un comercio que confía en la información de un único nodo vulnerable). Es el equivalente digital de rodear a alguien de amigos falsos que solo le cuentan las noticias que el atacante quiere que crea: la víctima sigue pensando que está informada, pero en realidad vive dentro de una burbuja construida a su medida, sin ningún contacto real con lo que ocurre fuera de ella.

Existen defensas conocidas y ampliamente implementadas contra este tipo de ataque -como diversificar las conexiones salientes de un nodo, limitar cuántas conexiones puede establecer una misma dirección IP o un mismo rango de red, y usar fuentes de conexión inicial (los llamados "seed nodes") variadas y fiables-, incorporadas de forma progresiva al software de

Bitcoin Core a raíz de investigaciones académicas que demostraron la viabilidad teórica de este ataque en configuraciones vulnerables.

El ataque eclipse: aislar a una víctima de la red real



Todas las conexiones de la víctima pasan por nodos controlados por el atacante (A); la red real (N) queda completamente fuera de su vista.

En un ataque eclipse, todas las conexiones de la víctima quedan controladas por el atacante, que la aísla por completo de la red real.

La minería egoísta (selfish mining)

La minería egoísta es una estrategia distinta, descrita formalmente en un influyente artículo académico de 2013 (de los investigadores Ittay Eyal y Emin Gün Sirer), que demostró que, bajo ciertas condiciones, un minero (o un pool de minería) podría obtener una parte de la recompensa total de minería desproporcionadamente mayor a su cuota real de hashrate, sin necesidad de alcanzar una mayoría absoluta del 51%.

La estrategia consiste, de forma simplificada, en que el minero egoísta, cuando encuentra un bloque válido, no lo anuncia inmediatamente a la red, sino que lo mantiene en secreto y sigue minando en privado sobre él, intentando adelantarse a la red pública con una ventaja de uno o más bloques. Si el resto de la red encuentra un bloque público antes de que el minero egoísta decida revelar el suyo, este responde publicando inmediatamente su propia cadena secreta (si es al menos igual de larga), lo que provoca que el trabajo de los mineros honestos que encontraron el bloque público quede descartado, mientras el minero egoísta se queda con la recompensa. Repetida sistemáticamente, esta estrategia puede generar, según el análisis matemático de sus autores, una ventaja de ingresos superior a la proporción real de hashrate del atacante, a costa de los mineros honestos.

Este resultado generó un debate técnico considerable dentro de la comunidad, en parte porque cuestionaba la suposición, hasta entonces bastante extendida, de que la estrategia óptima para cualquier minero era, siempre y en cualquier circunstancia, publicar cada bloque encontrado de inmediato. En la práctica, ejecutar minería egoísta con éxito exige que el atacante controle una proporción sustancial del hashrate total (generalmente estimada en torno a un tercio o más para que resulte claramente rentable) y una infraestructura de propagación de bloques muy eficiente, lo que limita considerablemente el número de actores capaces de intentarlo de forma creíble contra la red actual de Bitcoin, y no hay evidencia consolidada de que se haya practicado de forma sostenida y exitosa contra la red principal.

La defensa común a todos estos ataques: descentralización real

Los tres ataques de este capítulo comparten una misma vulnerabilidad de fondo: todos se vuelven más fáciles cuanto más concentrado está el poder de la red -ya sea el número de nodos independientes, la diversidad de las conexiones entre ellos, o la distribución del hashrate entre distintos mineros y pools-. Esta es la razón por la que la comunidad técnica de Bitcoin insiste tanto en la importancia de que un número elevado y diverso de personas, en países y proveedores de internet distintos, ejecute sus propios nodos completos, y en que el hashrate de minería no se concentre en exceso en pocos pools o pocas regiones geográficas -un tema al que volveremos, con datos actuales, en el capítulo 23.

En el próximo capítulo cambiamos de nivel: dejamos los ataques teóricos contra el protocolo y la red para entrar en el terreno donde, en la práctica, se ha producido la inmensa mayoría de las pérdidas reales de bitcoin a lo largo de la historia: los ataques dirigidos contra usuarios individuales y contra las plataformas que gestionan sus fondos.

Fuentes y estudios citados en este capítulo

- Douceur, J. (2002). "The Sybil Attack". Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS). El artículo que definió y dio nombre a este tipo de ataque en redes distribuidas.
- Heilman, E., Kendler, A., Zohar, A., Goldberg, S. (2015). "Eclipse Attacks on Bitcoin's Peer-to-Peer Network". USENIX Security Symposium. Estudio que demostró de forma práctica la viabilidad del ataque eclipse contra Bitcoin Core y motivó las defensas incorporadas después al software.
- Eyal, I., Sirer, E. G. (2014). "Majority is not Enough: Bitcoin Mining is Vulnerable". Financial Cryptography and Data Security, LNCS 8437. El artículo original que describe formalmente la estrategia de minería egoísta.

Capítulo 18. Ataques a usuarios y plataformas: phishing, malware y exchanges hackeados

Si el protocolo de Bitcoin nunca ha sido comprometido con éxito en más de quince años, ¿de dónde salen entonces los titulares habituales sobre "millones de dólares en bitcoin robados"? La respuesta, casi sin excepción, es la misma: esos robos no atacan el protocolo, sino a las personas y a las plataformas que gestionan las claves privadas. Este capítulo repasa los vectores de ataque más comunes contra usuarios y contra exchanges, con algunos de los casos más relevantes de la historia de Bitcoin.

Phishing: el engaño más antiguo, adaptado a Bitcoin

El phishing consiste en engañar a la víctima para que revele voluntariamente información sensible -en este caso, una clave privada o una frase semilla-, o para que autorice una transacción fraudulenta sin darse cuenta. En el mundo de Bitcoin, las variantes más habituales incluyen correos electrónicos o mensajes que suplantan la identidad de un exchange conocido pidiendo "verificar" la cuenta mediante un enlace falso, webs que imitan con gran fidelidad visual a wallets o exchanges legítimos, extensiones de navegador maliciosas que sustituyen silenciosamente la dirección de destino copiada al portapapeles por una dirección del atacante (los llamados "clipboard hijackers"), y perfiles falsos en redes sociales que ofrecen soporte técnico o regalos de bitcoin a cambio de un pequeño pago inicial o de la frase semilla "para verificar la wallet" -una petición que ningún servicio legítimo hace jamás, porque ninguna empresa necesita tu frase semilla para ayudarte-.

Malware: software diseñado para robar claves

Existen familias enteras de software malicioso diseñadas específicamente para robar bitcoin: registradores de teclado (keyloggers) que capturan todo lo que escribes, incluidas contraseñas y frases semilla si se llegan a teclear; malware que analiza el portapapeles en busca de direcciones de Bitcoin y las sustituye por una del atacante justo antes de que se pegue en el campo de envío de la wallet; troyanos disfrazados de software legítimo de minería, wallets falsas o incluso versiones modificadas de wallets reales, distribuidas fuera de los canales oficiales, que exfiltran las claves privadas en cuanto se generan. La defensa más eficaz frente a todas estas variantes es utilizar siempre software descargado de fuentes oficiales y verificadas, mantener el sistema operativo actualizado y, para cantidades significativas, utilizar un monedero hardware, donde la clave privada nunca queda expuesta a un ordenador potencialmente infectado (como explicamos en el capítulo 10).

El caso Mt. Gox (2014): el colapso que marcó una era

Ya mencionamos Mt. Gox en el capítulo 6 como el exchange dominante de los primeros años de Bitcoin. En febrero de 2014, la plataforma anunció que había perdido aproximadamente 850.000 bitcoins -de sus propios usuarios y de la propia empresa-, ya fuera por robo continuado a lo largo de varios años mediante vulnerabilidades técnicas explotadas por atacantes externos, por una gestión interna deficiente, o por una combinación de ambos factores, según las distintas investigaciones y procesos judiciales que siguieron al colapso. En su momento, esa cantidad representaba en torno al siete por ciento de todos los bitcoins en circulación, y su pérdida provocó el cierre y la posterior quiebra de la que hasta entonces

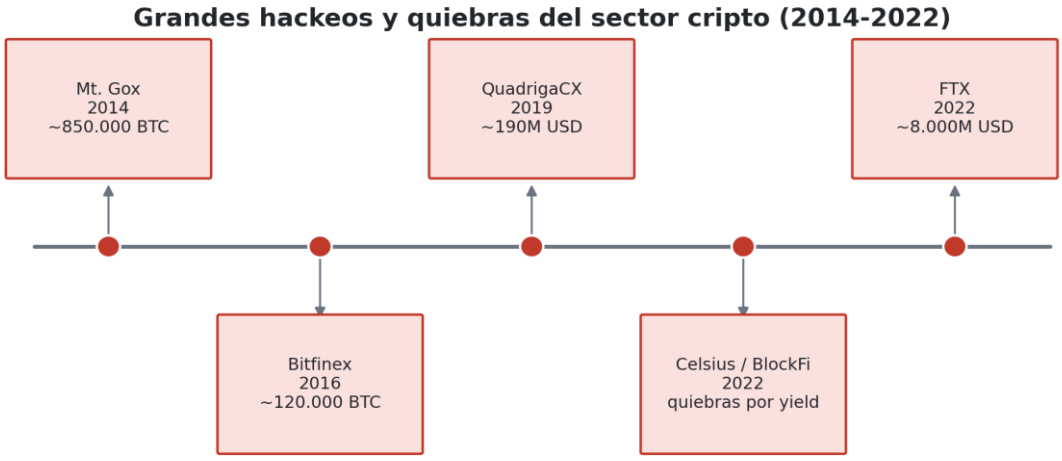
era la mayor plataforma de intercambio del mundo, además de un desplome notable del precio de mercado. El proceso legal derivado de Mt. Gox se ha prolongado durante más de una década, con la devolución parcial de fondos a los antiguos usuarios afectados iniciándose recién en los años recientes.

Otros grandes incidentes en exchanges

La historia de Bitcoin y las criptomonedas está salpicada de incidentes similares, aunque no siempre por los mismos motivos:

- Bitfinex (2016): sufrió un hackeo que resultó en el robo de aproximadamente 120.000 bitcoins, uno de los mayores robos directos de la historia; una parte sustancial de esos fondos fue recuperada por las autoridades estadounidenses varios años después, tras rastrear su movimiento en la blockchain pública, un recordatorio de que el pseudonimato de Bitcoin no es sinónimo de impunidad a largo plazo.
- Coincheck (2018): un exchange japonés sufrió el robo de una cantidad enorme de otra criptomoneda (NEM, no bitcoin directamente), por un valor de cientos de millones de dólares, tras almacenar los fondos en un monedero caliente sin protecciones adecuadas, en lugar de repartir el grueso de los activos en monederos fríos como recomienda la buena práctica del sector.
- FTX (2022): aunque este caso se centró más en una gestión fraudulenta y en el uso indebido de fondos de clientes que en un hackeo técnico externo, su colapso reforzó de manera contundente, entre millones de nuevos usuarios, la lección repetida durante años por la comunidad de Bitcoin: mantener fondos en un exchange implica un riesgo de contraparte real, no solo un riesgo técnico, tan real como el riesgo de que quiebre cualquier otra empresa a la que le confíes tu dinero.

Estos casos, y muchos otros de menor escala, comparten un patrón común: en casi ningún caso el problema fue una vulnerabilidad del protocolo de Bitcoin en sí, sino fallos de seguridad interna, malas prácticas de custodia, o directamente conductas fraudulentas por parte de la propia plataforma o de sus empleados.



Algunos de los mayores hackeos y quiebras de plataformas en la historia de Bitcoin y las criptomonedas.

Ingeniería social: el eslabón más débil sigue siendo humano

Muchos de los robos más sofisticados no dependen de romper ninguna barrera técnica, sino de manipular psicológicamente a la víctima: llamadas telefónicas haciéndose pasar por soporte técnico de un exchange, falsas urgencias ("tu cuenta ha sido comprometida, actúa ya"), intercambio fraudulento de tarjeta SIM (SIM swapping) para interceptar los códigos de verificación en dos pasos enviados por SMS y así tomar el control de cuentas de exchanges, o el llamado "ataque de la llave inglesa de cinco dólares" (una expresión popularizada por una viñeta que ironiza sobre cómo, frente a toda la sofisticación criptográfica de Bitcoin, a veces el método más "eficaz" para un atacante es simplemente la coacción física directa contra el propietario de las claves).

> *Ningún nivel de seguridad criptográfica protege frente a un usuario que, engañado o coaccionado, entrega voluntariamente su clave privada o autoriza él mismo una transacción fraudulenta. La seguridad de Bitcoin termina, literalmente, donde empieza el criterio humano de quien controla las claves.*

En el próximo capítulo seguimos en el terreno de las pérdidas de fondos, pero cambiando de protagonista: no atacantes externos, sino los propios usuarios, y los errores -sorprendentemente comunes- que han hecho desaparecer para siempre una parte sustancial de todos los bitcoins que existen.

Fuentes y estudios citados en este capítulo

- Chainalysis. "Crypto Crime Report" (informes anuales). Estadísticas sobre robos, hackeos de exchanges y su evolución a lo largo de los años.
- Informes de investigación y procesos judiciales públicos relacionados con el colapso de Mt. Gox (2014), tramitados ante los tribunales de Japón y Estados Unidos.
- Departamento de Justicia de Estados Unidos (2022). Documentación judicial sobre la incautación de fondos vinculados al hackeo de Bitfinex de 2016.
- Elliptic e informes públicos de la propia Coincheck sobre el incidente de 2018.

Capítulo 19. Errores humanos y la pérdida irreversible de claves

Ningún atacante, ningún hackeo, ningún fallo del protocolo: se estima que una parte muy significativa de todos los bitcoins que existen -distintos análisis de la cadena de bloques sitúan la cifra entre el quince y el veinte por ciento del suministro total minado hasta hoy- están perdidos para siempre, simplemente porque sus propietarios perdieron el acceso a las claves privadas correspondientes. Este capítulo explica por qué esto ocurre, con qué frecuencia, y qué lo hace tan distinto de perder dinero tradicional.

Por qué una pérdida de clave es irreversible por diseño

En el sistema bancario tradicional, si olvidas tu contraseña o pierdes tu tarjeta, existe siempre un procedimiento de recuperación: el banco verifica tu identidad por otros medios y te devuelve el acceso a tu cuenta. Bitcoin, precisamente por estar diseñado para no depender de ninguna autoridad central capaz de intervenir sobre las cuentas de nadie (recordemos el capítulo 12, sobre la ausencia de puntos únicos de control), no tiene ningún mecanismo equivalente. Si pierdes tu clave privada -y no tienes ninguna copia de seguridad de tu frase semilla-, los fondos asociados a esa clave permanecen, visibles en la blockchain pública para siempre, pero son matemáticamente inaccesibles para cualquiera, incluido tú mismo. Nadie -ni Satoshi Nakamoto, ni ningún desarrollador, ni ningún gobierno- tiene la capacidad técnica de "restaurar" el acceso a esos fondos.

El caso más citado: James Howells y el disco duro en el vertedero

Uno de los ejemplos más repetidos de esta clase de pérdida es el del ingeniero informático galés James Howells, que en 2013 tiró por error un disco duro que contenía la única copia de la clave privada de una wallet con 8.000 bitcoins minados en los primeros años del proyecto, cuando su valor era insignificante. El disco duro terminó, junto con el resto de la basura doméstica de esa semana, en un vertedero municipal de Newport, Gales. Howells ha pasado los años siguientes intentando, sin éxito, obtener permiso de las autoridades locales para excavar en el vertedero y recuperar el disco -una empresa cada vez más improbable, dado el paso del tiempo y las condiciones del propio vertedero-, mientras el valor de esos bitcoins, si se recuperaran, alcanzaría hoy varios cientos de millones de dólares.

Stefan Thomas y las diez oportunidades perdidas

Otro caso muy citado en la prensa es el del programador Stefan Thomas, que posee un pequeño dispositivo de almacenamiento cifrado (un IronKey) con 7.002 bitcoins, protegido por una contraseña que olvidó. El dispositivo permite únicamente diez intentos de contraseña antes de cifrar permanentemente su contenido de forma irreversible; Thomas ya ha agotado ocho de esos diez intentos sin éxito, y ha declarado públicamente que ha dejado de intentarlo por el riesgo de perder el acceso para siempre en los dos intentos restantes.

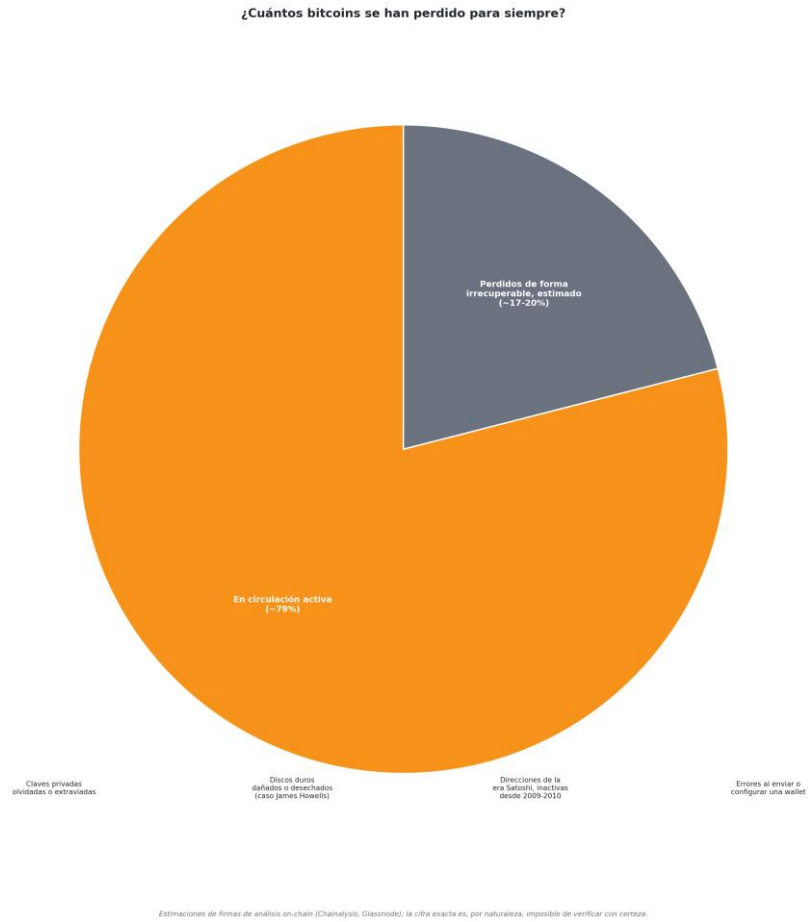
Formas habituales de perder acceso a los fondos

Más allá de estos casos extremos y muy mediáticos, existen patrones de pérdida mucho más comunes y menos espectaculares, que conviene conocer precisamente para evitarlos:

- No hacer ninguna copia de seguridad de la frase semilla al configurar una wallet por primera vez, confiando en que "ya la haré luego", un "luego" que con demasiada frecuencia nunca llega, hasta que un fallo del dispositivo lo hace irremediable.
- Guardar la frase semilla en un único soporte que se deteriora, se moja, se quema o simplemente se pierde con el tiempo (un papel manuscrito guardado sin ninguna protección adicional), sin ninguna copia adicional que sirva de respaldo si ese único soporte falla.
- Guardar la frase semilla únicamente en formato digital -una foto en el móvil, un documento de texto, una nota en la nube- sin cifrar, lo que además la expone a robo, como vimos en el capítulo anterior: es, a la vez, frágil ante la pérdida del dispositivo y vulnerable frente a cualquiera que consiga acceder a él remotamente.
- Olvidar la contraseña adicional (passphrase o "palabra 25", un mecanismo opcional de BIP-39 que añade una capa extra de protección a la frase semilla estándar) usada para proteger la wallet, sin la cual la frase semilla original ya no reconstruye las claves correctas: es como cambiar la cerradura de una caja fuerte y olvidar después la combinación nueva, dejando la llave original inútil.
- Enviar fondos a una dirección de una red distinta a la esperada, o a un formato de dirección incompatible con el software de destino, un error que en algunos casos resulta irreversible, de forma parecida a enviar una carta con un código postal inexistente: en el mejor de los casos se pierde por el camino, y en el peor, llega a un destino que nadie puede reclamar.
- El fallecimiento del propietario sin haber dejado ninguna instrucción, documento o plan de sucesión que permita a sus herederos acceder a los fondos, un problema creciente a medida que la primera generación de usuarios de Bitcoin envejece, y para el que, a diferencia de una cuenta bancaria heredable mediante un simple certificado de defunción, no existe ningún trámite legal capaz de "desbloquear" una clave privada perdida.

Bitcoins perdidos, no destruidos: el efecto sobre la escasez

Desde el punto de vista económico, los bitcoins perdidos no desaparecen del registro de la blockchain -siguen existiendo, técnicamente, como UTXO no gastados-, pero quedan permanentemente fuera de circulación, sin que nadie pueda moverlos jamás. Este fenómeno tiene un efecto colateral interesante: reduce, de facto, el suministro circulante real por debajo de los 21 millones teóricos que vimos en el capítulo 13, lo que algunos analistas interpretan como un factor adicional -aunque no planificado por el diseño original- de escasez para el resto de bitcoins que sí siguen bajo control activo de sus propietarios.



Estimación aproximada de la proporción de bitcoins perdidos de forma irrecuperable frente a los que siguen en circulación activa.

La lección práctica de este capítulo

Estos casos, lejos de ser simples anécdotas curiosas, ilustran una realidad central de Bitcoin que retomaremos con recomendaciones concretas en el capítulo 25: la autocustodia otorga un control total sobre el propio dinero, sin depender de ningún tercero, pero traslada también, de forma completa e irrevocable, la responsabilidad de protegerlo correctamente. No existe ningún departamento de atención al cliente al que llamar si se pierde una frase semilla.

En el próximo y último capítulo de esta parte dedicada a la seguridad, dejaremos los riesgos actuales para mirar hacia un riesgo futuro, todavía especulativo pero ampliamente debatido dentro de la comunidad técnica: ¿podrían los ordenadores cuánticos, si algún día alcanzan la potencia suficiente, romper la criptografía en la que se basa Bitcoin?

Fuentes y estudios citados en este capítulo

- Chainalysis. Informes y estimaciones periódicas sobre el volumen de bitcoin inactivo o presuntamente perdido, calculadas a partir del análisis de direcciones sin movimiento durante largos periodos.
- Cobertura periodística contemporánea de los casos de James Howells y Stefan Thomas, incluidas entrevistas directas publicadas por medios como The New York Times, BBC y Wired.

- Registro público de la blockchain de Bitcoin, fuente primaria que permite verificar de forma independiente la existencia y el estado (no gastado) de los UTXO asociados a estos casos.

Capítulo 20. Bitcoin frente a la computación cuántica

Ningún riesgo de seguridad genera tanta especulación -y tanta desinformación- como la amenaza, todavía hipotética, de la computación cuántica. Este capítulo explica, con el máximo rigor posible dado el estado actual de la tecnología, en qué consiste exactamente el riesgo, qué partes de Bitcoin estarían afectadas y qué se está haciendo al respecto.

Qué es un ordenador cuántico, en pocas palabras

Un ordenador clásico -el que usas para leer este libro- procesa información en bits, que solo pueden valer 0 o 1. Un ordenador cuántico utiliza en su lugar "qubits", que aprovechan fenómenos de la mecánica cuántica (como la superposición) para representar y procesar información de una forma fundamentalmente distinta, lo que permite, para determinados tipos muy concretos de problemas matemáticos, alcanzar soluciones exponencialmente más rápido que cualquier ordenador clásico, por potente que sea. Una analogía imperfecta pero útil: si buscar una salida en un laberinto de forma clásica es probar un pasillo, volver atrás si es un callejón sin salida y probar el siguiente, un ordenador cuántico se comporta, para ciertos problemas concretos, como si pudiera explorar muchos pasillos a la vez en lugar de uno por uno, encontrando antes las combinaciones que sí funcionan. Esto no convierte a los ordenadores cuánticos en máquinas "más rápidas en general" -de hecho, para la inmensa mayoría de las tareas cotidianas resultan peores que un ordenador convencional-, sino en herramientas especializadas, extraordinariamente potentes solo para ciertos problemas matemáticos concretos.

El algoritmo de Shor y la criptografía de clave pública

En 1994, el matemático Peter Shor demostró teóricamente que un ordenador cuántico suficientemente potente podría resolver, en un tiempo razonable, ciertos problemas matemáticos que hoy son la base de la seguridad de buena parte de la criptografía mundial -incluida la factorización de números muy grandes (base de RSA) y el problema del logaritmo discreto en curvas elípticas (base de la criptografía que usa Bitcoin, como vimos en el capítulo 3)-. Un ordenador cuántico con suficientes qubits estables y ejecutando el algoritmo de Shor podría, en teoría, calcular la clave privada correspondiente a una clave pública conocida, rompiendo la asimetría de un solo sentido que, como explicamos en el capítulo 9, es la base de toda la seguridad de las claves de Bitcoin.

¿Estamos cerca de esa capacidad? La respuesta corta: no, todavía no

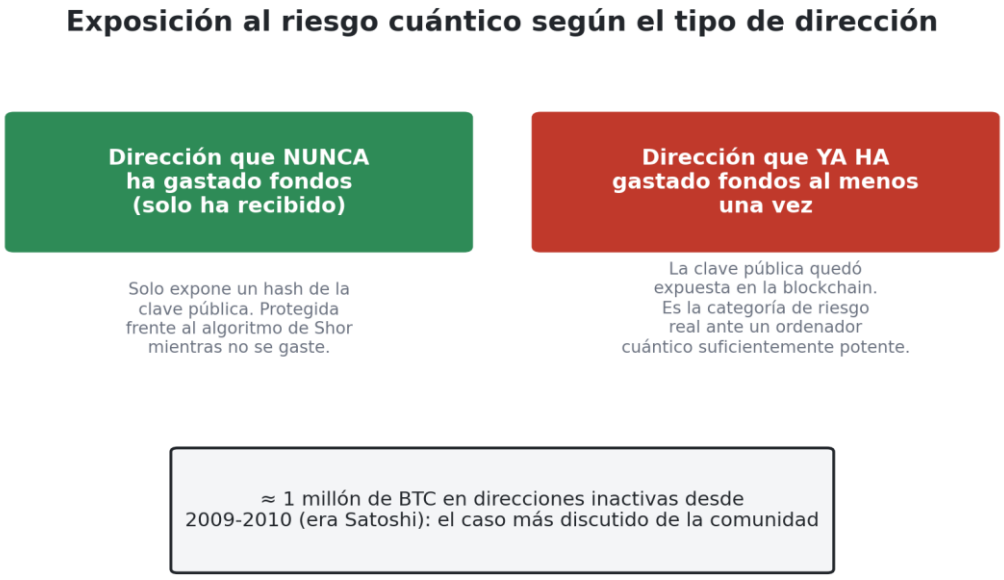
Los ordenadores cuánticos más avanzados construidos hasta la fecha, por empresas como Google, IBM o IonQ, cuentan con un número de qubits todavía muy alejado -según la inmensa mayoría de los expertos en computación cuántica y criptografía- del necesario para ejecutar el algoritmo de Shor contra una clave de curva elíptica de 256 bits como las de Bitcoin, un cálculo que las estimaciones más citadas sitúan en un rango que va desde varios millones hasta miles de millones de "qubits lógicos" estables y con corrección de errores -una tecnología que hoy dista mucho de estar disponible, y cuyo desarrollo, según la mayoría de las proyecciones serias del sector, podría tardar todavía muchos años, si es que llega a materializarse en absoluto en la forma necesaria-. Conviene distinguir, además, entre "qubits físicos" (los que anuncian los titulares de prensa) y "qubits lógicos" estables, ya que hacen

falta muchísimos qubits físicos, trabajando conjuntamente con técnicas de corrección de errores, para producir un solo qubit lógico fiable.

Qué partes de Bitcoin estarían realmente en riesgo

Es importante matizar que el riesgo cuántico no afectaría por igual a todos los fondos existentes. Las funciones hash (como SHA-256, usada en la minería y en la derivación de direcciones) son, según el consenso académico actual, mucho más resistentes a los algoritmos cuánticos conocidos que la criptografía de clave pública: el algoritmo cuántico relevante para funciones hash (el algoritmo de Grover) solo ofrece una mejora cuadrática, no exponencial, lo que se puede compensar de forma relativamente sencilla aumentando el tamaño de la clave.

El riesgo real se concentraría en las claves públicas que ya han sido expuestas públicamente en la blockchain -lo que ocurre, en el diseño actual de Bitcoin, en el momento en que se gasta un UTXO por primera vez, ya que la transacción debe incluir la clave pública correspondiente para que la red pueda verificar la firma-. Los fondos guardados en direcciones que nunca han sido usadas para gastar (solo para recibir) exponen únicamamente un hash de la clave pública, no la clave pública en sí, lo que ofrece una capa adicional de protección frente a este escenario concreto.



No todas las direcciones de Bitcoin están igual de expuestas a un eventual ataque cuántico: depende de si su clave pública ya ha quedado visible en la blockchain.

Lo que la comunidad técnica está preparando de antemano

La comunidad de desarrolladores de Bitcoin lleva años debatiendo y diseñando, de forma preventiva, esquemas de firma "post-cuánticos" -algoritmos criptográficos diseñados específicamente para resistir ataques de ordenadores cuánticos, incluso hipotéticos-, que podrían adoptarse mediante una actualización coordinada del protocolo (una "soft fork" o "hard fork", conceptos que explicaremos en el capítulo 21) si en algún momento la amenaza cuántica empezara a parecer suficientemente cercana en el tiempo como para justificarlo. El

propio Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha estado estandarizando, de forma independiente a Bitcoin, algoritmos de criptografía post-cuántica desde 2016, lo que da a la comunidad de Bitcoin un conjunto ya evaluado y probado de alternativas de las que partir cuando llegue el momento de actuar.

Un riesgo que se sigue de cerca, no que ocurra mañana

La postura más extendida entre criptógrafos y desarrolladores de Bitcoin no es negar el riesgo cuántico -sería intelectualmente deshonesto hacerlo, dado el ritmo real de avance de esta tecnología en los últimos años-, sino señalar que se trata de un riesgo con un horizonte temporal probablemente lejano (la mayoría de las estimaciones serias hablan de más de una década, posiblemente varias, antes de que exista una amenaza práctica real), y que la propia naturaleza descentralizada y de código abierto de Bitcoin permite a la comunidad prepararse, debatir soluciones y coordinar una actualización del protocolo con la debida antelación, en lugar de reaccionar de forma improvisada ante una amenaza repentina.

> *El riesgo cuántico es real como posibilidad a largo plazo, pero no es, con la tecnología disponible hoy, una amenaza práctica contra Bitcoin. Es, más bien, un ejemplo de cómo la comunidad técnica del proyecto vigila y se prepara para amenazas futuras años -o décadas- antes de que se materialicen.*

Con esto concluye la Parte IV de este libro, dedicada a la seguridad y a los ataques contra Bitcoin. En la Parte V dejaremos los riesgos para explorar la evolución del ecosistema: las mejoras técnicas que ha ido incorporando el protocolo, las soluciones de segunda capa como Lightning Network, la industria minera y el debate energético, y la creciente adopción institucional y estatal de Bitcoin en todo el mundo.

Fuentes y estudios citados en este capítulo

- Shor, P. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing, 26(5) (versión ampliada de la comunicación original de 1994 en el IEEE Symposium on Foundations of Computer Science).
- Grover, L. (1996). "A Fast Quantum Mechanical Algorithm for Database Search". Proceedings of the 28th Annual ACM Symposium on Theory of Computing. Artículo de referencia sobre el algoritmo cuántico relevante para funciones hash mencionado en este capítulo.
- National Institute of Standards and Technology (NIST). "Post-Quantum Cryptography Standardization Project", iniciado en 2016, con los primeros estándares publicados en 2024.

PARTE V

EVOLUCIÓN Y ECOSISTEMA

Capítulo 21. Forks, SegWit y la guerra del tamaño de bloque

En el capítulo 14 mencionamos que el límite de tamaño de bloque genera un mercado de comisiones, y que aumentar ese límite era una de las opciones consideradas para reducir la congestión. Lo que no contamos entonces es que esta cuestión, aparentemente técnica, provocó uno de los debates más intensos y duraderos de la historia de Bitcoin, y terminó dividiendo a la comunidad. Este capítulo cuenta esa historia.

Qué es un "fork" en el contexto del software de Bitcoin

Como cualquier proyecto de software de código abierto, Bitcoin evoluciona mediante propuestas de mejora (llamadas BIP, Bitcoin Improvement Proposals) que la comunidad de desarrolladores discute, prueba y, si alcanzan suficiente consenso, incorpora al software. Cuando un cambio de este tipo modifica las reglas del protocolo, puede producirse lo que se llama un "fork" (bifurcación), del cual existen dos tipos con implicaciones muy distintas:

- Soft fork: un cambio de reglas que resulta más restrictivo que el anterior -es decir, algo que antes era válido deja de serlo-, pero que los nodos que no han actualizado su software siguen considerando válido, porque las nuevas reglas son un subconjunto de las antiguas. Es, por diseño, compatible hacia atrás, de forma parecida a como una comunidad de vecinos que decide prohibir aparcar en doble fila sigue reconociendo como válidos todos los aparcamientos anteriores que ya cumplían esa norma más estricta.
- Hard fork: un cambio de reglas que resulta menos restrictivo, o simplemente incompatible con las reglas anteriores -algo que antes era inválido pasa a ser válido, o viceversa de forma incompatible-. Los nodos que no actualizan su software rechazan los bloques producidos bajo las nuevas reglas, y viceversa, lo que puede dividir la red en dos cadenas independientes si una parte de la comunidad no adopta el cambio, de forma parecida a como dos facciones de un mismo club, incapaces de ponerse de acuerdo sobre las reglas del juego, terminan formando dos ligas separadas que ya no juegan entre sí.

El origen del debate: cómo escalar Bitcoin

Alrededor de 2015, el uso de Bitcoin había crecido lo suficiente como para que los bloques, con su límite original de aproximadamente un megabyte, empezaran a llenarse con regularidad, generando comisiones más altas y tiempos de confirmación más largos en los momentos de mayor demanda. La comunidad se dividió, en términos generales, en dos visiones sobre cómo resolver este problema.

- Un sector, que terminaría asociándose con el nombre "Bitcoin Cash", defendía aumentar directamente el límite de tamaño de bloque -a varios megabytes, o incluso más-, argumentando que esto permitiría procesar muchas más transacciones por bloque y mantener las comisiones bajas, aunque a costa de bloques más pesados de propagar y almacenar.
- Otro sector, que terminaría prevaleciendo en lo que hoy seguimos llamando simplemente "Bitcoin", defendía mantener el tamaño de bloque cercano al original, priorizando que ejecutar un nodo completo (capítulo 12) siguiera siendo accesible para el mayor número posible de personas en todo el mundo, y buscar la escalabilidad mediante mejoras de eficiencia dentro de ese límite y mediante soluciones de segunda capa por encima de la cadena principal (capítulo 22).

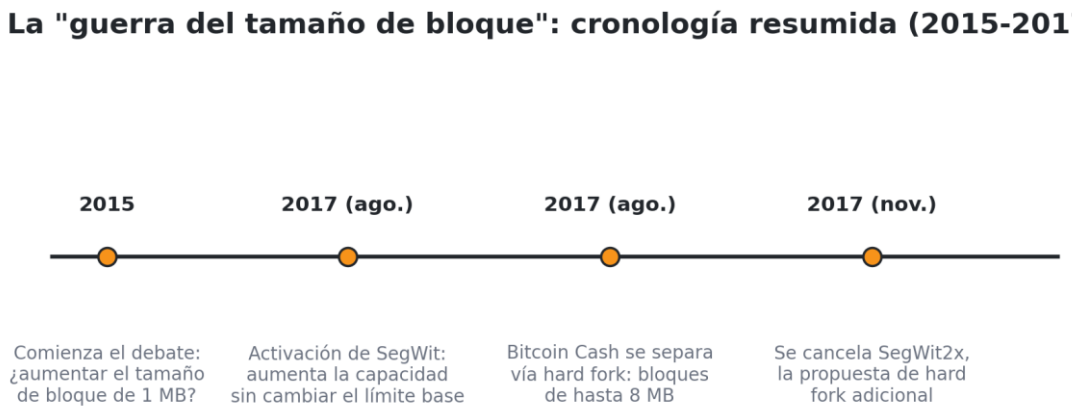
SegWit: la solución técnica que ganó el debate (2017)

La propuesta que terminó imponiéndose se llamó Segregated Witness, o SegWit, activada en agosto de 2017 mediante un soft fork. Su nombre describe su mecanismo principal: separa ("segrega") los datos de la firma digital ("witness", testigo) del resto de los datos de la transacción, contabilizándolos de forma distinta a efectos del límite de tamaño de bloque. Esto tuvo varios efectos beneficiosos simultáneos: aumentó de forma efectiva la capacidad de transacciones por bloque sin aumentar formalmente el límite original de una manera que exigiera un hard fork, corrigió un problema técnico previo (llamado "maleabilidad de transacciones") que dificultaba construir de forma fiable protocolos de segunda capa como Lightning Network, y sentó las bases técnicas para mejoras posteriores como las direcciones Bech32 mencionadas en el capítulo 9.

El nacimiento de Bitcoin Cash (agosto de 2017)

Al no lograrse un consenso suficiente para adoptar directamente un aumento del tamaño de bloque en la cadena principal, el sector que defendía esa postura ejecutó un hard fork propio el 1 de agosto de 2017, creando una cadena y una criptomoneda independientes: Bitcoin Cash (BCH), con un límite de bloque bastante mayor desde su lanzamiento. Cualquiera que poseyera bitcoin en el momento exacto de la bifurcación recibió automáticamente una cantidad equivalente de Bitcoin Cash, ya que ambas cadenas compartían el mismo historial hasta ese momento.

Bitcoin Cash sufrió, a su vez, su propia división interna en 2018, dando lugar a Bitcoin SV (Satoshi's Vision), impulsada por Craig Wright -el mismo empresario mencionado en el capítulo 5 por reclamar sin pruebas suficientes ser Satoshi Nakamoto-, en otro desacuerdo sobre el rumbo técnico del proyecto. Hoy en día, tanto Bitcoin Cash como Bitcoin SV mantienen una capitalización de mercado y un nivel de adopción muy inferiores a los de Bitcoin, aunque continúan operando de forma independiente.



Cronología resumida de la "guerra del tamaño de bloque": de SegWit al nacimiento de Bitcoin Cash.

Taproot (2021): la siguiente gran mejora

Tras SegWit, la mejora más significativa incorporada al protocolo llegó en noviembre de 2021, también mediante un soft fork, con el nombre de Taproot. Esta actualización introdujo, entre otras cosas, un nuevo esquema de firmas (llamado Schnorr, que permite combinar de forma más eficiente y con mayor privacidad transacciones que requieren múltiples firmas) y mejoras que abaratan y hacen más privados los contratos inteligentes complejos construidos sobre Bitcoin, sentando las bases técnicas de las que, más adelante, se beneficiarían desarrollos como los Ordinals mencionados en el capítulo 14.

Por qué esta historia importa más allá de la anécdota técnica

El episodio de la guerra del tamaño de bloque es, más allá de sus detalles técnicos, una lección muy reveladora sobre la gobernanza de Bitcoin: no existe ningún comité, empresa ni fundación con autoridad formal para imponer un cambio de protocolo. Cualquier actualización necesita, en la práctica, el respaldo suficiente de desarrolladores, mineros, empresas del sector y, sobre todo, de los propios usuarios que ejecutan nodos (recordemos, del capítulo 12, que son los nodos quienes tienen la última palabra). Cuando ese respaldo suficiente no se logra sobre un cambio concreto, el resultado -como ocurrió en 2017- puede ser directamente la creación de una cadena separada, en lugar de la imposición forzada de una decisión sobre toda la comunidad.

En el próximo capítulo profundizaremos en la solución de escalabilidad que finalmente ganó peso dentro de la propia cadena de Bitcoin: Lightning Network, la red de segunda capa que permite realizar pagos casi instantáneos y con comisiones mínimas.

Fuentes y estudios citados en este capítulo

- Wuille, P., Lombrozo, E., Lau, J. (2015-2017). "BIP-141: Segregated Witness (Consensus layer)". Bitcoin Improvement Proposal que define SegWit.

- Wuille, P., Nick, J., Ruffing, T. (2020). "BIP-340: Schnorr Signatures for secp256k1"; y "BIP-341: Taproot: SegWit version 1 spending rules". Bitcoin Improvement Proposals que definen Taproot y las firmas Schnorr.
- Repositorio público de Bitcoin Improvement Proposals (github.com/bitcoin/bips), fuente primaria de todas las propuestas mencionadas en este capítulo.
- Registro histórico de la bifurcación de Bitcoin Cash (agosto de 2017), verificable de forma independiente en las blockchains públicas de ambos proyectos.

Capítulo 22. Lightning Network: pagos instantáneos de segunda capa

Como vimos en los capítulos 14 y 21, la cadena principal de Bitcoin tiene una capacidad limitada de transacciones por bloque, una decisión de diseño deliberada para preservar la descentralización. Esto plantea, sin embargo, un reto real: ¿cómo puede Bitcoin servir para pagos cotidianos -un café, una propina, una compra online- si cada transacción en la cadena principal compite por un espacio limitado y puede tardar minutos en confirmarse? La respuesta más desarrollada hasta la fecha es Lightning Network.

La idea central: mover la mayoría de los pagos fuera de la cadena

Lightning Network, propuesta en un documento técnico de 2015 por Joseph Poon y Thaddeus Dryja y desarrollada activamente desde entonces por varios equipos independientes, es un protocolo de "segunda capa" (Layer 2): un sistema construido encima de Bitcoin que permite realizar un número prácticamente ilimitado de pagos entre dos partes sin registrar cada uno de ellos individualmente en la blockchain principal, sino únicamente el resultado neto final, cuando las partes deciden liquidarlo.

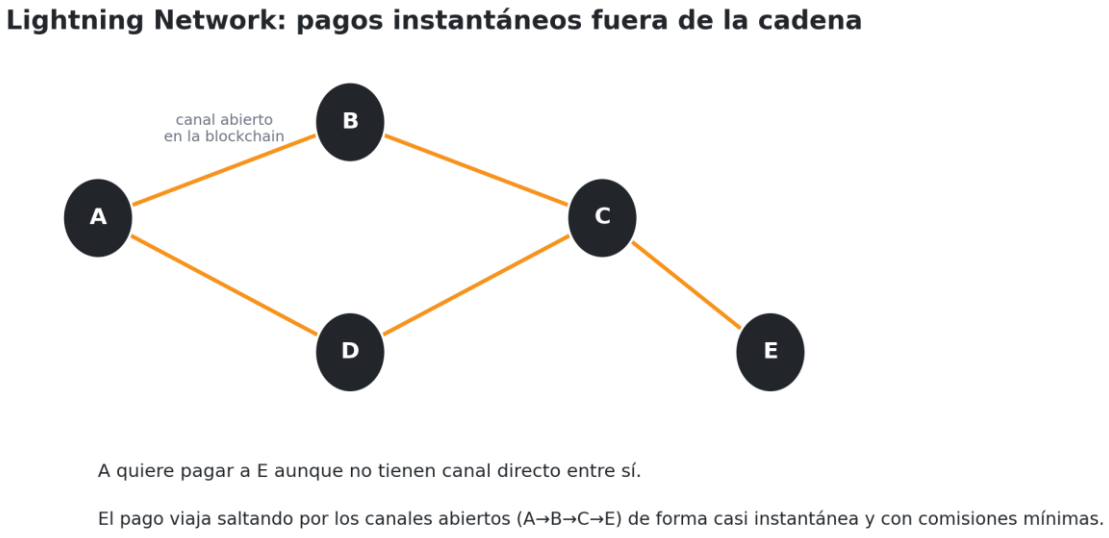
Cómo funciona un canal de pago

La unidad básica de Lightning es el "canal de pago": dos participantes bloquean conjuntamente una cantidad de bitcoin en una dirección especial mediante una única transacción en la cadena principal (esto se llama "abrir un canal"). Es muy parecido a abrir una cuenta a modo de "fiado" en un bar de confianza: en lugar de pagar en efectivo cada consumición por separado, el bar apunta cada ronda en una cuenta compartida, y solo al final de la noche se salda la cuenta con un único pago; el canal Lightning funciona igual, pero la "cuenta" se cierra formalmente en la blockchain solo cuando ambas partes lo deciden. A partir de ese momento, ambas partes pueden intercambiarse, de forma instantánea y sin ningún coste ni registro en la blockchain, tantos pagos parciales como quieran entre ellas, simplemente actualizando de mutuo acuerdo, mediante firmas criptográficas intercambiadas directamente entre ambos, cómo se reparte el saldo total del canal. Cuando cualquiera de las dos partes decide terminar la relación, se realiza una segunda -y última- transacción en la cadena principal ("cerrar el canal"), que liquida en la blockchain únicamente el balance final acordado, sin importar cuántos pagos individuales se hayan realizado mientras el canal estuvo abierto.

La red: pagar a quien no tienes un canal directo

La potencia real de Lightning no está en los canales individuales, sino en que forman, entre todos los usuarios que participan, una red interconectada. Si tú tienes un canal abierto con una persona, y esa persona tiene, a su vez, un canal abierto con un comercio al que quieres pagar, puedes enviar el pago "saltando" a través de esa cadena de canales intermedios, sin necesidad de abrir un canal directo con el comercio. Cada nodo intermedio de la ruta cobra una comisión mínima por facilitar el salto, y gracias a un mecanismo criptográfico llamado Hash Time-Locked Contracts (HTLC), el pago se completa de forma atómica: o llega correctamente a su destino final a través de toda la ruta, o no se mueve ningún fondo en

ningún tramo del camino, sin posibilidad de que un nodo intermedio se quede con el dinero sin completar la ruta.



Lightning Network: los pagos saltan de canal en canal hasta llegar a su destino.

Ventajas frente a la cadena principal

- Velocidad: los pagos se confirman en milisegundos, no en minutos, porque no hace falta esperar a que ningún minero incluya nada en un bloque: basta con el intercambio directo de firmas entre las partes del canal.
- Coste: las comisiones son, típicamente, una fracción minúscula de las comisiones on-chain, lo que hace viables pagos muy pequeños (micropagos) que resultarían antieconómicos directamente en la cadena principal, como pagar unos pocos céntimos por leer un artículo o por escuchar una canción.
- Escalabilidad: en teoría, la capacidad total de la red no está limitada por el tamaño de bloque, sino por la cantidad de canales y de liquidez disponible en la red, lo que permite un volumen de transacciones muy superior al que la cadena principal podría soportar por sí sola.
- Privacidad: los pagos intermedios de la red no quedan registrados de forma permanente y pública en la blockchain, a diferencia de las transacciones on-chain, ya que solo la apertura y el cierre del canal quedan grabados de forma permanente.

Limitaciones y retos actuales

Lightning no sustituye a la cadena principal, sino que la complementa, y tiene sus propias limitaciones. Requiere que los usuarios gestionen liquidez -cada canal tiene una capacidad máxima, determinada por el bitcoin bloqueado al abrirlo, así que enviar o recibir pagos más grandes que esa capacidad exige abrir canales más grandes o encontrar rutas alternativas-. Además, mantener un nodo Lightning propio con buena conectividad exige cierto conocimiento técnico, lo que ha impulsado la aparición de proveedores de servicios de custodia (wallets Lightning "custodiales") que simplifican la experiencia a cambio de renunciar, parcialmente, a la autocustodia total que analizamos en el capítulo 10. También existe el reto técnico de que un usuario debe permanecer, en cierta medida, atento al estado

de sus canales para evitar ciertos escenarios de fraude por parte de una contraparte de mala fe, aunque el desarrollo de "watchtowers" (servicios de vigilancia automatizada de canales) y de wallets cada vez más sofisticadas ha reducido notablemente esta carga para el usuario medio.

Adopción real de Lightning Network

A pesar de estos retos, Lightning ha experimentado un crecimiento sostenido desde su lanzamiento en la red principal en 2018, con miles de nodos públicos y una capacidad total de la red que ha crecido de forma constante. Casos de adopción notables incluyen su uso extendido en El Salvador tras la adopción de Bitcoin como moneda de curso legal (que veremos en el capítulo 24), su integración en aplicaciones populares de pagos y redes sociales, y su papel creciente en remesas internacionales, donde permite enviar dinero de un país a otro con comisiones y tiempos de liquidación muy inferiores a los de los sistemas tradicionales de transferencia internacional.

Los datos más recientes, de mediados de 2026, permiten cuantificar ese crecimiento con algo más de precisión: la red pública cuenta con unos 41.000 canales repartidos entre aproximadamente 17.400 nodos visibles, con una capacidad pública agregada de entre 4.900 y 5.600 bitcoins según la fuente consultada, aunque los analistas del sector coinciden en que esa cifra infravalora de forma sustancial la capacidad real total, porque no incluye los canales privados y no anunciados que usan de forma creciente las billeteras móviles, los proveedores de servicios de liquidez y los grandes exchanges: la capacidad total estimada, sumando capacidad pública y privada, podría superar los 12.000 bitcoins. El volumen de pagos mensuales cursados a través de la red, por su parte, ronda ya los 1.100 millones de dólares. Un patrón interesante de esta fase de madurez de la red es que el número de nodos públicos ha descendido desde el máximo histórico de unos 20.700 alcanzado en 2022 hasta los 17.400 actuales, no porque la red se use menos, sino porque la actividad se ha ido concentrando en un número menor de nodos gestionados de forma más profesional y mejor capitalizados -un patrón de consolidación no muy distinto, salvando las diferencias, del que describimos a propósito de los pools de minería en el capítulo 39-, mientras que los operadores más pequeños y aficionados han tendido a cerrar sus nodos o a trasladar sus fondos a wallets que gestionan la complejidad de los canales por ellos.

Volumen de pagos mensuales: en torno a 1.100 millones de dólares. Fuentes: 1ML, Bitcoin Visuals, Spark Research.

La red Lightning en cifras: nodos, canales y capacidad pública a mediados de 2026.

> *Lightning Network es, en esencia, la respuesta de Bitcoin a la pregunta "¿cómo puede un sistema con bloques limitados a propósito procesar millones de pagos pequeños?": no forzando a la cadena principal a crecer sin límite, sino construyendo una capa adicional, más rápida y más barata, que se apoya en la seguridad de la cadena principal solo cuando hace falta, para abrir y cerrar cada canal.*

En el próximo capítulo cambiamos de tema por completo, para abordar uno de los debates públicos más recurrentes en torno a Bitcoin: su consumo energético y el impacto medioambiental de la minería industrial.

Fuentes y estudios citados en este capítulo

- Poon, J., Dryja, T. (2016). "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". Documento técnico original que propuso Lightning Network.
- 1ML.com y Amboss.space, exploradores públicos independientes de la red Lightning, usados habitualmente para monitorizar su capacidad total y su número de nodos y canales.
- Informes del Banco Central de Reserva de El Salvador y del Fondo Monetario Internacional sobre el impacto de Bitcoin y Lightning Network en las remesas internacionales del país, ampliados en el capítulo 24.
- Spark Research, "State of the Lightning Network in 2026"; Bitcoin Visuals, estadísticas de capacidad y nodos de la red Lightning, mediados de 2026.

Capítulo 23. Minería industrial, energía y el debate medioambiental

Pocos aspectos de Bitcoin generan un debate público tan polarizado como su consumo energético. Este capítulo intenta presentar los datos y los argumentos de ambos lados con el mayor rigor posible, sin minimizar el consumo real ni exagerar sus implicaciones.

Cuánta energía consume realmente la red

Estimar el consumo energético exacto de Bitcoin es complejo, porque no existe un registro centralizado de qué hardware está minando ni dónde, pero distintos observatorios académicos e independientes -como el Cambridge Bitcoin Electricity Consumption Index, de la Universidad de Cambridge- llevan años elaborando estimaciones basadas en el hashrate total de la red y en la eficiencia energética conocida del hardware de minería disponible en el mercado. Estas estimaciones han situado el consumo anual de la red, en los últimos años, en un rango comparable al de países de tamaño mediano, del orden de entre cien y ciento cincuenta teravatios-hora al año, una cifra que ha crecido de forma notable a medida que el precio de Bitcoin ha atraído más inversión en infraestructura de minería.

Por qué Bitcoin consume tanta energía por diseño

Este consumo no es un efecto secundario indeseado, sino una consecuencia directa -y, según sus defensores, deliberada y necesaria- del propio mecanismo de prueba de trabajo explicado en el capítulo 11: la seguridad de la red depende, precisamente, de que atacarla resulte extraordinariamente costoso en términos de hardware y energía real, no solo teóricos. Un sistema que pudiera asegurarse "gratis" sería, por la misma razón, trivial de atacar. Bajo esta perspectiva, el gasto energético de Bitcoin no es un desperdicio, sino el coste tangible de un bien concreto: una red monetaria global, resistente a la censura y sin necesidad de confiar en ningún intermediario.

El argumento crítico: la huella de carbono

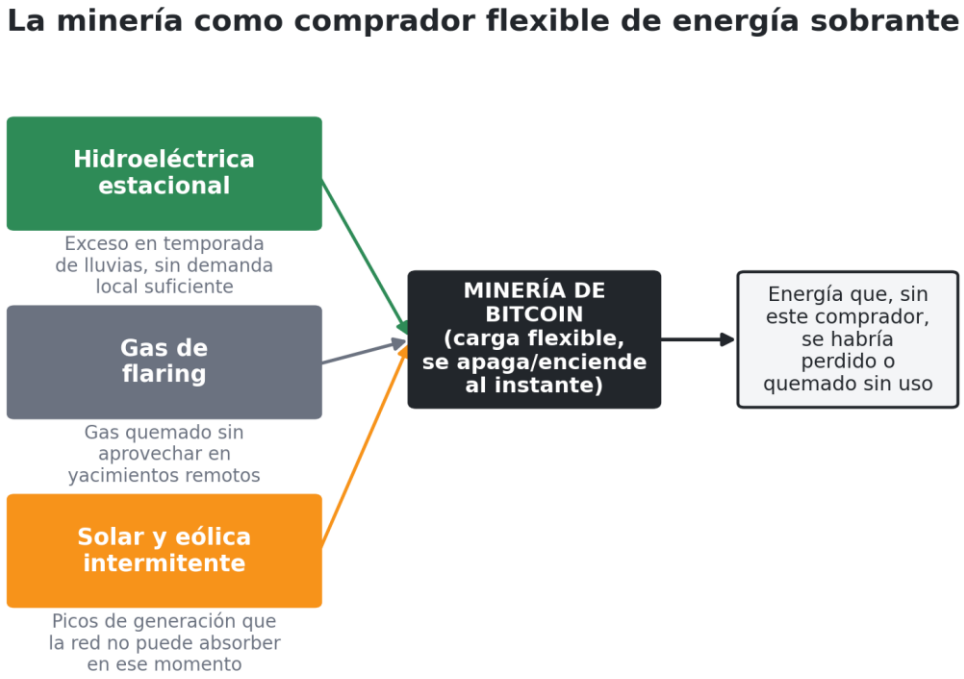
Los críticos del consumo energético de Bitcoin señalan que, más allá de la cantidad total de energía consumida, importa de dónde proviene esa energía. Si una proporción significativa de la minería se alimenta de fuentes de energía fósil -carbón, gas-, su huella de carbono resulta considerable, comparable a la de industrias tradicionales enteras, en un momento en que la comunidad internacional busca reducir las emisiones globales de gases de efecto invernadero para mitigar el cambio climático. Estudios académicos con distintas metodologías han llegado a estimaciones variadas sobre el porcentaje exacto de energía renovable utilizada en la minería de Bitcoin, sin que exista todavía un consenso unánime al respecto, en parte por la dificultad de rastrear con precisión el origen exacto de la electricidad consumida por operaciones de minería repartidas por todo el planeta y, en ocasiones, poco transparentes sobre sus fuentes energéticas.

El argumento a favor: el mix energético y la energía "varada"

Los defensores de Bitcoin señalan varios factores que, en su opinión, matizan sustancialmente el argumento crítico. En primer lugar, destacan que la minería de Bitcoin

tiene una característica poco común entre las industrias intensivas en energía: puede instalarse en prácticamente cualquier lugar del mundo con acceso a electricidad e internet, sin necesidad de estar cerca de mercados de consumo o de rutas de transporte, lo que la convierte en un comprador atractivo de energía que, de otro modo, se desperdiciaría -la llamada "energía varada" (stranded energy), un concepto parecido al de la fruta que un agricultor no puede vender a tiempo porque el mercado más cercano está demasiado lejos: en lugar de dejarla pudrirse sin ningún aprovechamiento, un comprador dispuesto a instalarse justo al lado del huerto puede darle una salida económica que, de otro modo, no existiría-. Ejemplos citados con frecuencia incluyen el gas natural que, en ciertos yacimientos petrolíferos remotos, se quema directamente en la atmósfera (flaring) por falta de infraestructura para transportarlo a donde se necesita -y que algunas operaciones mineras han empezado a capturar para generar electricidad en el propio lugar, reduciendo las emisiones netas frente a la quema directa sin aprovechamiento-, o el excedente de energía hidroeléctrica en regiones con temporadas de lluvias que superan la demanda local, como ciertas provincias de China o de otros países con abundante capacidad hidroeléctrica estacional.

En segundo lugar, señalan que, a diferencia de la mayoría de las industrias, la minería de Bitcoin puede apagarse y encenderse casi instantáneamente sin dañar el equipo ni el proceso, lo que la convierte en un consumidor flexible capaz de actuar como "válvula de escape" para redes eléctricas con exceso puntual de energía renovable intermitente (solar y eólica), consumiendo el excedente en los momentos de máxima generación y reduciendo o deteniendo su actividad cuando la red necesita esa capacidad para otros usos, un servicio de estabilización de red por el que algunas operaciones mineras han empezado a recibir compensación económica directa de operadores eléctricos.



Los críticos señalan que esta lectura no debe minimizar el uso simultáneo de energía fósil convencional por buena parte de la industria minera — ambos fenómenos conviven según la región y la operación (ver capítulo 44).

La minería como comprador flexible de energía que, de otro modo, se perdería o se quemaría sin uso.

Comparaciones controvertidas

Es habitual, en ambos lados del debate, recurrir a comparaciones -el consumo de Bitcoin frente al de países enteros, frente al del sistema bancario tradicional, frente al de la industria del oro, frente a otros usos de electricidad como el aire acondicionado o los centros de datos de streaming de vídeo-. Estas comparaciones pueden ser informativas, pero conviene tratarlas con cautela: dependen mucho de la metodología usada, y comparar sistemas tan distintos en su función (un sistema monetario global frente a, por ejemplo, el consumo doméstico de un país) no siempre ofrece una imagen completa por sí sola, sin analizar también qué servicio concreto se obtiene a cambio de ese consumo.

La concentración geográfica e industrial de la minería

Más allá del debate energético, existe una preocupación relacionada con la descentralización: la minería se ha ido concentrando, con el tiempo, en operaciones industriales a gran escala, capaces de negociar tarifas eléctricas favorables y de invertir en el hardware ASIC más eficiente (capítulo 11), en detrimento de la minería doméstica o a pequeña escala, que hoy resulta económicamente inviable en la inmensa mayoría de los casos frente a estos grandes operadores. China concentró, durante años, una proporción muy significativa del hashrate mundial, hasta que en 2021 prohibió por completo la minería de criptomonedas en su territorio, provocando una reubicación masiva y repentina de la industria hacia Estados Unidos, Kazajistán y otros países, en un episodio que, paradójicamente, demostró la resiliencia y la capacidad de adaptación geográfica de la red: a pesar de perder de la noche a la mañana una fracción enorme de su hashrate total, Bitcoin siguió funcionando sin interrupción, ajustando automáticamente su dificultad (capítulo 11) hasta recuperar su ritmo normal de producción de bloques en cuestión de semanas.

En el próximo capítulo cerramos esta parte del libro con la dimensión más visible de los últimos años: cómo gobiernos, reguladores, empresas cotizadas y fondos de inversión de todo el mundo han ido incorporando Bitcoin a sus estrategias, desde su adopción como moneda de curso legal en El Salvador hasta la llegada de los fondos cotizados (ETF) de Bitcoin al mercado financiero tradicional.

Fuentes y estudios citados en este capítulo

- Cambridge Centre for Alternative Finance, Universidad de Cambridge. "Cambridge Bitcoin Electricity Consumption Index" (CBECI), fuente independiente de referencia para las estimaciones de consumo energético citadas en este capítulo.
- de Vries, A. (2018). "Bitcoin's Growing Energy Problem". Joule, 2(5), Cell Press. Uno de los estudios académicos más citados en la vertiente crítica del debate energético.
- Bendiksen, C., Gibbons, S. (CoinShares Research). "The Bitcoin Mining Network" (informes periódicos). Estudios independientes sobre el mix energético y la distribución geográfica de la minería, representativos de la vertiente más favorable del debate.
- Cambridge Centre for Alternative Finance (2022). "3rd Global Cryptoasset Benchmarking Study", con datos sobre la reubicación de la minería tras la prohibición china de 2021.

Capítulo 24. Regulación, adopción institucional y estatal

Durante su primera década de existencia, Bitcoin fue, en gran medida, ignorado o tratado con recelo por gobiernos, bancos centrales y grandes inversores institucionales. Desde alrededor de 2020, esa relación ha cambiado de forma notable. Este capítulo repasa los hitos más importantes de esa transición hacia la adopción convencional (mainstream).

El Salvador: el primer país con Bitcoin como moneda de curso legal

El 7 de septiembre de 2021, El Salvador se convirtió en el primer país del mundo en adoptar Bitcoin como moneda de curso legal, junto al dólar estadounidense (que el país ya usaba como moneda oficial desde 2001). La medida, impulsada por el presidente Nayib Bukele, obligaba en su formulación original a que los comercios aceptaran bitcoin como forma de pago cuando se les ofreciera, e incluyó el lanzamiento de una wallet estatal (Chivo) y un bono de bienvenida en bitcoin para los ciudadanos que se registraran.

La medida generó reacciones muy divididas: organismos como el Fondo Monetario Internacional expresaron reiteradamente su preocupación por los riesgos para la estabilidad financiera y fiscal del país, mientras que sus defensores señalaron beneficios como el abaratamiento de las remesas internacionales -una fuente de ingresos muy relevante para la economía salvadoreña, dado el elevado número de emigrantes que envían dinero a sus familias- gracias en parte al uso de Lightning Network (capítulo 22), y un notable impulso a la visibilidad internacional y al turismo relacionado con Bitcoin en el país. La adopción real por parte de la población salvadoreña en su día a día ha sido, según distintas encuestas y estudios independientes, más limitada de lo que el gobierno proyectó inicialmente, y en enero de 2025, como parte de un acuerdo de financiación con el FMI, el país modificó la ley para hacer voluntaria -en lugar de obligatoria- la aceptación de bitcoin por parte de los comercios, aunque el gobierno salvadoreño ha continuado, en paralelo, con su propia estrategia de acumulación de bitcoin en las reservas del Estado.

Bitcoin City: la ciudad libre de impuestos financiada con "bonos volcán"

En noviembre de 2021, el gobierno salvadoreño anunció un proyecto todavía más ambicioso que la propia adopción de Bitcoin como moneda de curso legal: la construcción de "Bitcoin City", una ciudad planificada desde cero junto al volcán de Conchagua, en el departamento oriental de La Unión, diseñada para funcionar como una zona económica especial sin impuesto sobre la renta, sin impuesto sobre la propiedad, sin impuesto sobre las plusvalías y sin impuesto municipal, con la única excepción del IVA, la mitad del cual se destinaría a financiar la deuda municipal de la ciudad y la otra mitad a servicios públicos. Según el plan original, la ciudad se alimentaría de energía geotérmica extraída del propio volcán -una fuente renovable, abundante y muy barata en la región- para dar servicio tanto a la vida cotidiana de sus residentes como a instalaciones industriales de minería de Bitcoin (capítulo 35), en un intento explícito de conectar la narrativa energética del proyecto con la narrativa financiera.

La financiación del proyecto se diseñó en torno a los llamados "bonos volcán" (Volcano Bonds), un instrumento de deuda soberana respaldado parcialmente por bitcoin con el que el gobierno pretendía recaudar 1.000 millones de dólares: la mitad destinada a comprar bitcoin adicional para las reservas del Estado y la otra mitad a financiar directamente la

infraestructura de Bitcoin City. Tras varios años de retrasos regulatorios y ajustes en su diseño legal, la emisión de estos bonos se formalizó finalmente a finales de 2024, y sus fondos han empezado a destinarse, según las fuentes oficiales del gobierno, a acelerar el desarrollo de la infraestructura geotérmica de la zona de Conchagua.

La distancia entre el anuncio original y la realidad sobre el terreno, sin embargo, ha sido objeto de un escrutinio periodístico considerable, y conviene presentarla con el mismo rigor evenhanded que aplicamos al resto de iniciativas estatales relacionadas con Bitcoin en este libro: mientras que comunicados oficiales de principios de 2026 hablan de avances en la infraestructura geotérmica y en la delimitación de la zona económica especial, investigaciones periodísticas independientes realizadas sobre el terreno -incluida una visita a la localidad de Conchagua a comienzos de 2025- no encontraron indicios visibles de construcción real, y el propio ayuntamiento de la zona confirmó en ese momento que las obras aún no habían comenzado. En la práctica, Bitcoin City sigue siendo, varios años después de su anuncio, un proyecto en una fase muy temprana de desarrollo de infraestructura básica -carreteras, conexión eléctrica, internet de alta velocidad- más que la metrópolis futurista que mostraban las representaciones arquitectónicas originales, un patrón de desfase entre el anuncio político y la ejecución material que quien siga el proyecto de cerca debería tener en cuenta antes de sacar conclusiones definitivas en cualquier dirección.

Otros países y su relación con Bitcoin

La postura de los distintos gobiernos del mundo frente a Bitcoin varía enormemente, desde la adopción entusiasta hasta la prohibición total. China ha prohibido tanto la minería como el comercio de criptomonedas en su territorio desde 2021, aunque la aplicación real de esta prohibición al comercio en la práctica ha sido objeto de debate. Estados Unidos, la Unión Europea (a través del reglamento MiCA, Markets in Crypto-Assets, en vigor desde 2024) y la mayoría de las economías desarrolladas han optado por marcos regulatorios que permiten la posesión y el comercio de Bitcoin, sometiéndolo a obligaciones fiscales, de prevención de blanqueo de capitales y de protección al consumidor, sin llegar a prohibirlo ni a adoptarlo como moneda oficial. Otros países, como la República Centroafricana, han hecho intentos puntuales de adopción similares al de El Salvador, con resultados y continuidad muy diversos. El capítulo 34 recoge, con una tabla comparativa más extensa, cómo regulan Bitcoin una docena de países representativos de los distintos enfoques.

La llegada de los ETF de Bitcoin al contado (enero de 2024)

Uno de los hitos regulatorios más significativos de la historia reciente de Bitcoin ocurrió el 10 de enero de 2024, cuando la Comisión de Bolsa y Valores de Estados Unidos (SEC) aprobó, tras años de solicitudes rechazadas, la cotización de varios fondos cotizados en bolsa (ETF) de Bitcoin al contado (spot), gestionados por algunas de las mayores gestoras de activos del mundo, entre ellas BlackRock, Fidelity y Ark Invest. Un ETF (fondo cotizado en bolsa) es, en esencia, un producto financiero que se compra y se vende como si fuera una acción cualquiera, pero cuyo valor sigue el precio de otra cosa -en este caso, bitcoin- sin que el inversor tenga que poseer directamente ese activo subyacente: es parecido a comprar un recibo que representa oro guardado en una cámara acorazada ajena, en lugar de comprar el lingote físico y tener que guardarlo tú mismo. Estos productos permiten a inversores institucionales y particulares obtener una exposición al precio de Bitcoin a través de sus

cuentas de inversión tradicionales -brókers, planes de pensiones, fondos de inversión-, sin necesidad de comprar, custodiar o gestionar directamente bitcoin ni sus claves privadas.

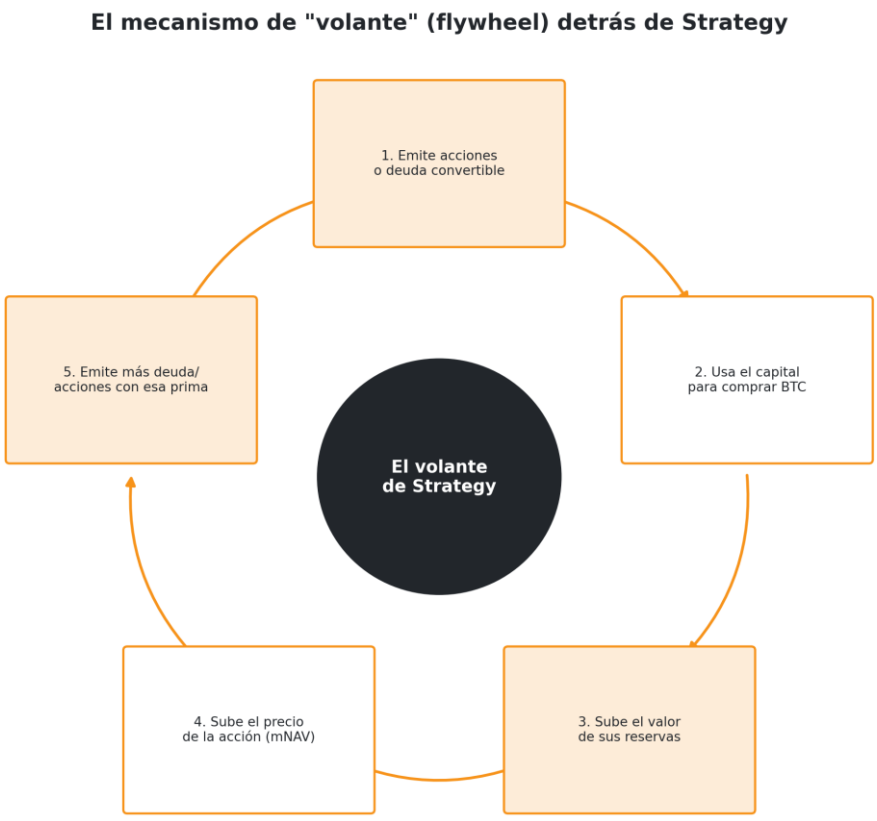
La aprobación de estos ETF eliminó una barrera de entrada importante para el capital institucional -muchos fondos de pensiones, aseguradoras y gestoras patrimoniales tienen restricciones internas o regulatorias que les impiden comprar activos "no tradicionales" directamente, pero sí pueden invertir en un ETF regulado-, y se tradujo en una entrada de capital muy sustancial hacia estos productos durante sus primeros meses de cotización, consolidando a Bitcoin como una clase de activo reconocida dentro de las carteras de inversión convencionales, un estatus que durante buena parte de la década anterior le había sido esquivo.

Empresas que incorporan Bitcoin a su tesorería

Otro fenómeno relevante de los últimos años ha sido la adopción de Bitcoin como reserva de valor por parte de empresas cotizadas. El caso más destacado, con enorme diferencia, es el de Strategy (anteriormente conocida como MicroStrategy), una empresa que originalmente se dedicaba al software de inteligencia empresarial y que, desde agosto de 2020, bajo el impulso de su fundador y actual presidente ejecutivo, Michael Saylor, reorientó buena parte de su actividad corporativa a acumular bitcoin como activo principal de tesorería. Otras empresas, incluida Tesla en determinados periodos, han incorporado bitcoin a sus balances con distintos grados de compromiso y continuidad, pero ninguna se acerca a la escala ni a la estrategia de Strategy, que merece una explicación aparte.

El caso Michael Saylor y Strategy

Michael Saylor había fundado MicroStrategy en 1989 como una empresa de software de análisis de datos, con una trayectoria bursátil discreta durante más de dos décadas. En agosto de 2020, la empresa anunció que destinaría una parte de su efectivo corporativo a comprar bitcoin como reserva de valor principal, alegando la erosión del poder adquisitivo del dólar por las políticas monetarias expansivas que mencionamos en el capítulo 4. Lo que empezó como una decisión de tesorería se convirtió, con los años, en el núcleo del negocio: la empresa ha financiado compras adicionales de bitcoin emitiendo de forma repetida deuda convertible, acciones preferentes y acciones ordinarias nuevas, en una estrategia que sus propios responsables han descrito como un "volante de inercia" (flywheel): cuando el mercado valora las acciones de la empresa por encima del valor neto de sus bitcoins en cartera (una relación que el mercado sigue de cerca bajo el nombre de mNAV, o valor liquidativo de mercado), emitir nueva deuda o nuevas acciones para comprar más bitcoin resulta, en teoría, rentable para los accionistas existentes, porque cada operación aumenta la cantidad de bitcoin respaldando cada acción. A julio de 2026, Strategy mantenía en su balance 843.775 bitcoins, adquiridos a un precio medio aproximado de 66.385 dólares por unidad, por un coste total acumulado superior a los 33.000 millones de dólares, lo que la convierte en la mayor tenedora corporativa de bitcoin del mundo, muy por delante de cualquier otra empresa cotizada. En febrero de 2025, la compañía formalizó este giro cambiando su nombre a, simplemente, Strategy.



Los cinco pasos del "volante" de Strategy, explicados en el texto.

Los instrumentos financieros que sostienen la estrategia

Para financiar estas compras sin depender únicamente de la emisión de acciones ordinarias -que diluye a los accionistas existentes-, Strategy ha desarrollado, desde 2025, toda una familia de instrumentos financieros específicos, cada uno con un nombre corto y un perfil de riesgo distinto: STRK, STRF, STRD, STRC y STRE son acciones preferentes que pagan a sus compradores un dividendo fijo, típicamente de entre el 8% y el 10% anual, distribuido con carácter trimestral, y que se ordenan entre sí según su prioridad de cobro en caso de dificultades financieras -STRF y STRE como las más senior, STRC en un nivel intermedio, y STRD como la más subordinada, aunque todas ellas por delante de las acciones ordinarias de la empresa (las MSTR) en caso de liquidación-. Entre estos instrumentos, STRC es, con diferencia, el mayor: acumula unos 10.500 millones de dólares de los aproximadamente 15.500 millones de dólares en acciones preferentes emitidas en total. A esto se suma la deuda convertible propiamente dicha -bonos que pueden transformarse en acciones bajo determinadas condiciones-, de la que Strategy ha llegado a recomprar parte de forma anticipada: en mayo de 2026, la empresa completó la recompra de 1.500 millones de dólares de sus notas convertibles senior al 0% con vencimiento en 2029, empleando para ello sus propias reservas de caja, una gestión activa de su deuda que contrasta con la imagen, a veces simplificada, de una empresa que se limita a acumular bitcoin sin más.

Por qué Michael Saylor importa tanto para la narrativa de adopción

Más allá de las cifras, Saylor se ha convertido en uno de los divulgadores más visibles e influyentes de Bitcoin entre el público institucional: aparece con enorme frecuencia en medios financieros, organiza conferencias propias dedicadas a promover la adopción corporativa de Bitcoin, y defiende públicamente la tesis de que Bitcoin es "la propiedad digital definitiva", una reserva de valor superior al resto de activos precisamente por las propiedades de escasez absoluta que explicamos en el capítulo 13. Su influencia real es difícil de exagerar: buena parte del interés que otras empresas y algunos fondos institucionales mostraron por Bitcoin a partir de 2020 y 2021 se atribuye, al menos en parte, al ejemplo -y a la insistente labor de evangelización pública- de Saylor y Strategy. De hecho, el modelo que Saylor popularizó ha dado lugar a todo un ecosistema de imitadores, lo que algunos analistas del sector han empezado a llamar "Treasury 2.0": empresas que adoptan una versión de la misma estrategia, con distintos grados de agresividad. A mediados de 2026, entre los mayores tenedores corporativos de bitcoin del mundo, muy por detrás de Strategy pero ya con cifras significativas, se encuentran Twenty One Capital (43.514 BTC), la japonesa Metaplanet (43.000 BTC, y que ha llegado a fijarse el objetivo declarado de alcanzar 100.000 BTC), MARA Holdings (36.303 BTC, una empresa que combina minería propia con acumulación directa) y Tesla, con una posición mucho más modesta y estable de aproximadamente 11.509 BTC. Strategy, por sí sola, concentra en torno al 60% de todo el bitcoin en manos de las principales empresas cotizadas del mundo.

Los riesgos y las críticas a la estrategia de Strategy

La propia mecánica que ha impulsado el crecimiento de Strategy es también su mayor vulnerabilidad, y varios analistas de mercado la han descrito abiertamente como "una receta para el desastre" si las condiciones cambian. Todo el modelo depende de que el mercado siga dispuesto a pagar una prima por las acciones de Strategy por encima del valor neto de sus bitcoins (mNAV superior a 1): si esa prima se reduce o desaparece -algo que ha llegado a ocurrir en 2026, coincidiendo con el auge de los ETF de bitcoin al contado del propio capítulo, que ofrecen una exposición mucho más simple y sin las capas adicionales de deuda corporativa y acciones preferentes que arrastra Strategy-, la empresa pierde su principal palanca para seguir comprando más bitcoin sin diluir en exceso a sus accionistas actuales. A esto se suma el riesgo, más clásico, del apalancamiento: parte de las compras se han financiado con deuda convertible y con acciones preferentes que exigen el pago de dividendos regulares de entre el 8% y el 10% anual -de hecho, en julio de 2026 la propia Strategy vendió una parte de sus bitcoins, por primera vez desde una operación puntual de 2022 por motivos fiscales, precisamente para poder financiar esos dividendos-, lo que introduce una dependencia de los mercados de capitales y un riesgo, todavía hipotético pero señalado repetidamente por analistas críticos, de verse forzada a vender bitcoin en un mal momento de mercado si el acceso a nueva financiación se estrechara justo cuando el precio de Bitcoin estuviera cayendo con fuerza. Cuanto más se expande esta arquitectura de instrumentos financieros superpuestos -deuda senior, acciones preferentes con distintos niveles de prioridad, acciones ordinarias-, más se aleja la experiencia de un inversor en MSTR de la experiencia, mucho más simple, de poseer bitcoin directamente o a través de un ETF al contado, un matiz que conviene tener muy presente antes de asumir que "comprar acciones de Strategy" equivale a "comprar bitcoin".

El historial legal de Saylor: una nota de contexto necesaria

Por rigor informativo, conviene mencionar dos episodios legales del propio Saylor, anteriores y independientes de su estrategia de bitcoin, que sus críticos citan con frecuencia al valorar su credibilidad. En el año 2000, la SEC llevó y resolvió un caso de fraude contable civil contra MicroStrategy y tres de sus directivos, entre ellos Saylor, por sobrestimar los ingresos y beneficios de la empresa durante los años del auge de las puntocom; sin admitir ni negar las acusaciones, Saylor aceptó devolver unos 8,28 millones de dólares y pagar una sanción civil de 350.000 dólares. Más recientemente, en junio de 2024, Saylor y Strategy acordaron pagar 40 millones de dólares para cerrar una demanda de la Fiscalía General del Distrito de Columbia, que alegaba que Saylor había fingido residir en jurisdicciones con impuestos más bajos (Florida y Virginia) mientras vivía realmente en Washington D.C., evadiendo así más de 25 millones de dólares en impuestos sobre la renta locales entre 2005 y 2021; fue la mayor recuperación fiscal de la historia del distrito. Ninguno de los dos episodios está relacionado directamente con la estrategia de acumulación de bitcoin de la empresa, pero ambos forman parte, de forma legítima, del historial público que cualquiera debería considerar al evaluar la credibilidad de una de las voces más influyentes -y más interesadas económicamente- en la narrativa de adopción institucional de Bitcoin.

Bancos centrales y reservas estatales de Bitcoin

Además de El Salvador, otros gobiernos han empezado a explorar o a mantener reservas de bitcoin, ya sea por adquisición directa o por la incautación de fondos vinculados a actividades delictivas (como ocurrió, por ejemplo, con parte de los fondos recuperados del hackeo de Bitfinex mencionado en el capítulo 18). En Estados Unidos, en marzo de 2025, la administración establecida en ese momento anunció la creación de una "reserva estratégica de Bitcoin" formada, en gran parte, a partir de bitcoin ya incautado por agencias federales en distintos procesos judiciales, un paso que generó un intenso debate sobre su alcance real y sus implicaciones futuras, dado lo reciente de la medida en el momento de escribir este libro.

Un ecosistema cada vez más entrelazado con las finanzas tradicionales

Tomados en conjunto, estos desarrollos -adopción estatal, ETF regulados, tesorerías corporativas, marcos legales cada vez más definidos en la mayoría de las grandes economías- describen una trayectoria clara: Bitcoin ha pasado, en poco más de una década, de ser un experimento marginal de un pequeño grupo de entusiastas de la criptografía a convertirse en un activo reconocido, debatido y, cada vez más, integrado dentro del sistema financiero global que, según vimos en el capítulo 4, en gran medida pretendía ofrecer una alternativa.

Con esto concluye la Parte V de este libro. En la Parte VI, la última, dejaremos atrás la descripción técnica e histórica para abordar las cuestiones prácticas y reflexivas: cómo proteger correctamente tus propios bitcoins, un repaso honesto a las críticas y debates que siguen abiertos en torno a Bitcoin, y una mirada, necesariamente especulativa, hacia su futuro.

Fuentes y estudios citados en este capítulo

- Fondo Monetario Internacional (2021-2024). Informes del Artículo IV y documentos de "Selected Issues" sobre El Salvador, con el análisis oficial del FMI sobre los riesgos de la adopción de Bitcoin como moneda de curso legal.

- Comisión de Bolsa y Valores de Estados Unidos (SEC). Orden de aprobación de la cotización de ETF de Bitcoin al contado, 10 de enero de 2024.
- Unión Europea. Reglamento (UE) 2023/1114, "Markets in Crypto-Assets" (MiCA), en vigor desde 2024.
- Informes públicos trimestrales y comunicados 8-K de Strategy ante la SEC sobre sus adquisiciones de bitcoin, la estructura de sus acciones preferentes (STRK, STRF, STRD, STRC, STRE) y la recompra de notas convertibles de mayo de 2026.
- Datos agregados de tenencias corporativas de bitcoin verificados por observatorios independientes como bitcointreasuries.net y SatsIntel, incluida la comparación con Twenty One Capital, Metaplanet, MARA Holdings y Tesla.
- Comisión de Bolsa y Valores de Estados Unidos (SEC) (2000). Comunicado de resolución del caso de fraude contable contra MicroStrategy y sus directivos.
- Fiscalía General del Distrito de Columbia (2024). Comunicado sobre el acuerdo de 40 millones de dólares en el caso de fraude fiscal contra Michael Saylor y MicroStrategy.
- Global Finance Magazine, "El Salvador: 'Volcano Bonds' Ready Eruption" (2025); Blockworks, "El Salvador Plans 'Bitcoin City' Funded by Bitcoin Bonds and Powered by a Volcano" (2021-2026), sobre el diseño y la financiación de Bitcoin City.
- Reportajes de seguimiento sobre el terreno en Conchagua (2025-2026), incluida cobertura de AInvest ("Bitcoin City: El Salvador's Volcano Bond Dream Stalls") y KuCoin ("The World's First Bitcoin Nation: Where Does El Salvador Stand in 2026?"), sobre el desfase entre los anuncios oficiales y el avance real de la construcción.

PARTE VI

REFLEXIÓN FINAL

Capítulo 25. Custodia y buenas prácticas de seguridad personal

Después de recorrer la historia, el funcionamiento técnico y los riesgos de Bitcoin, este capítulo reúne, de forma práctica y accionable, las recomendaciones de seguridad más importantes para cualquier persona que posea o quiera empezar a poseer bitcoin. No sustituye el asesoramiento profesional para grandes patrimonios, pero cubre los principios que aplican prácticamente a cualquier usuario.

Principio 1: entiende qué estás protegiendo

Como vimos en los capítulos 9 y 10, lo único que realmente importa proteger es la frase semilla (o las claves privadas derivadas de ella): quien tenga acceso a esa frase tiene control total e irrevocable sobre los fondos asociados, sin necesidad de ninguna contraseña adicional, verificación de identidad ni intervención de terceros. Protegerla no es una tarea puntual al configurar la wallet, sino una responsabilidad continua mientras conserves esos fondos.

Principio 2: separa el uso diario del ahorro a largo plazo

Igual que en el mundo físico no llevamos todos nuestros ahorros en la cartera del día a día, la práctica más recomendada por la comunidad es distinguir claramente entre:

- Una wallet caliente (capítulo 10), con una cantidad pequeña, para gastos cotidianos, pagos rápidos o pruebas, tratándola mentalmente como el dinero suelto que llevarías en el bolsillo, no como tus ahorros de toda la vida.
- Una wallet fría, preferiblemente un monedero hardware, para el grueso de tus ahorros, que no necesitas mover con frecuencia, exactamente igual que guardarías las joyas de familia en una caja fuerte y no encima de la mesa del salón.

Para cantidades significativas, muchos usuarios avanzados añaden una tercera capa: una configuración multifirma (capítulo 10), que elimina cualquier punto único de fallo -la pérdida o el robo de una sola clave, o de un solo dispositivo, no compromete los fondos.

Principio 3: verifica tu copia de seguridad antes de confiar en ella

Un error extraordinariamente común -y silencioso hasta que es demasiado tarde- es anotar la frase semilla de forma apresurada o con errores de transcripción, y no descubrirlo hasta el momento de necesitar restaurarla, cuando ya puede ser demasiado tarde. La práctica recomendada es, tras anotar la frase semilla, hacer una restauración de prueba en un dispositivo distinto (o en el mismo, tras borrar la wallet) para confirmar que la frase anotada reconstruye exactamente las mismas direcciones, antes de depositar fondos significativos.

Principio 4: protege la frase semilla frente a distintos tipos de riesgo

Guardar la frase semilla de forma segura implica protegerla frente a varias amenazas distintas y, en ocasiones, contrapuestas, por lo que conviene pensar en cada una por separado:

- Robo o acceso no autorizado: no guardes la frase semilla en ningún dispositivo conectado a internet (fotos, notas, correos, gestores de contraseñas en la nube sin cifrado adicional adecuado); considera dividir el conocimiento de la frase completa entre distintas ubicaciones si el riesgo lo justifica.
- Daño físico: el papel se quema, se moja y se degrada con el tiempo; las placas de metal grabado, diseñadas específicamente para resistir incendios, inundaciones y corrosión, ofrecen una protección muy superior para copias de seguridad a largo plazo.
- Pérdida por olvido o desconocimiento de terceros: guarda al menos una copia en una ubicación distinta a tu domicilio habitual (una caja de seguridad, la casa de un familiar de confianza), y considera dejar instrucciones claras -sin revelar la frase semilla en sí- para que tus herederos puedan localizarla y acceder a ella en caso de fallecimiento o incapacidad, un aspecto de planificación patrimonial cada vez más relevante, como mencionamos en el capítulo 19.

Principio 5: desconfía por defecto

La mayoría de los robos de bitcoin, como vimos en el capítulo 18, no explotan ninguna vulnerabilidad técnica sofisticada, sino que dependen de que la víctima baje la guardia. Algunas reglas simples reducen drásticamente el riesgo: ningún servicio legítimo te pedirá jamás tu frase semilla, ni por teléfono, ni por correo, ni por chat de soporte; verifica siempre, carácter a carácter o mediante código QR, la dirección de destino antes de confirmar un envío, especialmente si la copiaste y pegaste (recordemos el riesgo de los "clipboard hijackers" del capítulo 18); descarga el software de wallet exclusivamente desde las webs oficiales de cada proyecto, verificando el enlace con cuidado; y sospecha de cualquier oportunidad de inversión, regalo o "duplicación" de bitcoin que suene demasiado buena para ser verdad, porque casi con toda seguridad lo es.

Principio 6: la comodidad y la seguridad son un equilibrio, no un extremo

No existe una configuración de seguridad "perfecta" válida para todo el mundo: alguien con pequeñas cantidades destinadas al uso cotidiano puede razonablemente priorizar la comodidad de una wallet móvil sencilla, mientras que alguien con un patrimonio significativo en bitcoin puede justificar la complejidad adicional de una configuración multifirma distribuida geográficamente. Lo importante es tomar esta decisión de forma consciente y proporcional al

valor que se está protegiendo, en lugar de replicar sin pensar la configuración de otra persona con circunstancias distintas.

Principio 7: revisa y practica tu configuración periódicamente

Una configuración de seguridad que era adecuada hace cinco años puede haber quedado obsoleta sin que te des cuenta: el dispositivo hardware que usas puede haber dejado de recibir actualizaciones de seguridad del fabricante, la ubicación física donde guardas una copia de la frase semilla puede haber cambiado de circunstancias (una mudanza, la venta de una propiedad, el fallecimiento de un familiar de confianza que conocía su ubicación), o simplemente puede haber aparecido una alternativa notablemente más robusta -como la migración de una wallet de firma única a una configuración multifirma- que en su momento no resultaba necesaria por el volumen de fondos protegidos. La comunidad de seguridad recomienda revisar la configuración completa de custodia al menos una vez al año, como quien revisa el estado de un extintor doméstico: no porque se espere que falle, sino precisamente porque, si falla, el momento en que se descubre no debe ser el momento en que se necesita. Esta revisión debería incluir, como mínimo, comprobar que los dispositivos hardware siguen siendo compatibles con el software de wallet, que las copias de la frase semilla siguen siendo legibles y accesibles físicamente, y que las instrucciones de sucesión mencionadas en el principio anterior siguen reflejando la situación familiar y patrimonial actual del propietario, no la de varios años atrás.

Igual de importante que la revisión periódica es el simulacro de recuperación completo: no basta con haber verificado la frase semilla una vez, al configurar la wallet por primera vez, como recomendamos en el principio 3; para cantidades significativas, conviene repetir ese ejercicio de tanto en tanto, restaurando la wallet completa desde cero en un dispositivo distinto (o, si se trata de una configuración multifirma, verificando que efectivamente pueden reunirse las firmas necesarias entre las personas o dispositivos designados), precisamente para detectar con tiempo cualquier problema práctico -una llave que ha cambiado de ubicación sin que nadie lo actualizara, un colaborador de custodia compartida que ya no está disponible o localizable- antes de que ese problema se descubra en la peor circunstancia posible: un momento de urgencia real, en el que ya no hay margen para corregirlo.

> *La autocustodia de Bitcoin traslada al individuo un nivel de responsabilidad sobre su propio dinero que no tiene equivalente en el sistema financiero tradicional. Es, a la vez, su mayor promesa de libertad y su mayor exigencia práctica.*

En el próximo capítulo dejaremos las recomendaciones prácticas para abordar, con la mayor honestidad posible, las críticas más serias y los debates que siguen abiertos en torno a Bitcoin: su volatilidad, su relación con la actividad ilícita y las dudas sobre la concentración de poder dentro de su propio ecosistema.

Capítulo 26. Críticas y debates abiertos

Un libro honesto sobre Bitcoin no puede limitarse a explicar cómo funciona y por qué sus defensores lo valoran: también debe presentar, con el mismo rigor, las críticas más serias que se le hacen, muchas de ellas formuladas por economistas, tecnólogos y reguladores con argumentos sólidos. Este capítulo repasa las más relevantes, sin pretender zanjarlas de forma definitiva.

La volatilidad del precio

Bitcoin ha mostrado, a lo largo de toda su historia, oscilaciones de precio extremas en periodos cortos de tiempo, con caídas superiores al setenta u ochenta por ciento desde sus máximos en más de una ocasión (2013-2015, 2017-2018, 2021-2022), seguidas de recuperaciones igualmente pronunciadas. Esta volatilidad plantea un problema práctico real para su función como "unidad de cuenta" y "depósito de valor estable" en el sentido tradicional que vimos en el capítulo 1: resulta difícil fijar precios en una moneda cuyo poder adquisitivo puede variar de forma tan drástica en cuestión de semanas, y resulta arriesgado depender de ella para gastos a corto plazo.

Los defensores de Bitcoin suelen responder a esta crítica señalando que se trata de un activo todavía joven y en proceso de maduración, cuya volatilidad ha tendido a reducirse -aunque de forma irregular y no garantizada- a medida que su capitalización de mercado y su liquidez han crecido con los años, y que su propuesta de valor fundamental no es la de servir como moneda estable de uso diario a corto plazo, sino la de un activo de reserva de valor a largo plazo, en cuyo horizonte temporal más amplio su tendencia histórica de precio ha sido, hasta la fecha, marcadamente alcista, aunque el rendimiento pasado, como en cualquier activo, no garantiza en absoluto el comportamiento futuro.

¿Es Bitcoin un esquema Ponzi o una estafa piramidal?

Es, probablemente, la acusación más repetida contra Bitcoin en debates informales, y merece una respuesta precisa, porque "Ponzi" y "pirámide" son términos técnicos con una definición jurídica y económica concreta, no simples insultos intercambiables.

Qué es, exactamente, un esquema Ponzi

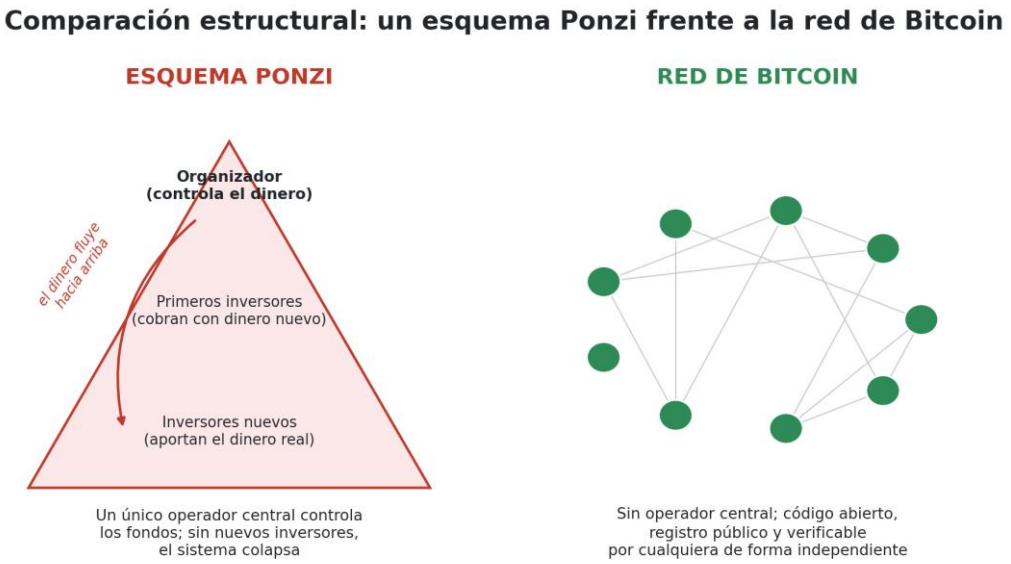
El término proviene de Charles Ponzi, un estafador que en 1920, en Boston, prometió a sus inversores una rentabilidad del 50% en cuarenta y cinco días, supuestamente obtenida arbitrando cupones de respuesta postal internacional; en realidad, jamás llevó a cabo esa actividad a la escala necesaria, y se limitó a pagar a los primeros inversores con el dinero que aportaban los siguientes, hasta que el esquema colapsó al cabo de unos meses. Un esquema Ponzi moderno reproduce esa misma estructura: un operador central capta dinero prometiendo una rentabilidad fija y poco realista, no genera ningún beneficio real a través de ninguna actividad productiva, paga los primeros rendimientos con el capital de los inversores más recientes, y colapsa de forma matemáticamente inevitable en cuanto las nuevas aportaciones dejan de superar a los reembolsos prometidos. La clave, a efectos legales, es que el operador conoce desde el principio que el modelo es insostenible y oculta deliberadamente esa realidad a sus inversores.

Qué es, exactamente, un esquema piramidal

Un esquema piramidal comparte con el Ponzi la naturaleza fraudulenta, pero se diferencia en su mecánica: exige que cada participante reclute activamente a otros nuevos participantes para poder obtener beneficios, normalmente a cambio de una cuota de entrada, de modo que la estructura solo se sostiene mientras el número de personas reclutadas crezca de forma exponencial, generación tras generación. Esa exigencia de crecimiento exponencial es, precisamente, lo que hace que un esquema piramidal resulte matemáticamente imposible de sostener más allá de un número limitado de niveles: incluso en el escenario más optimista, la base de población disponible para reclutar se agota en pocas rondas.

Por qué Bitcoin no encaja, estructuralmente, en ninguna de las dos definiciones

Comparando punto por punto: no existe ningún operador central que capte dinero de los usuarios de Bitcoin, porque no hay ninguna empresa ni persona que "venda" Bitcoin en su nombre ni que reciba las aportaciones de quienes lo compran, a diferencia de Ponzi, que gestionaba personalmente cada aportación. Ninguna fuente oficial de Bitcoin promete una rentabilidad concreta -de hecho, ni siquiera existe una "fuente oficial": la red es un protocolo abierto sin ningún departamento de relaciones con inversores-, y su volatilidad se advierte y se documenta abiertamente, todo lo contrario al ocultamiento deliberado que caracteriza a un fraude Ponzi. Nadie necesita reclutar a otras personas para poder comprar, poseer o vender bitcoin: puedes adquirir bitcoin sin que nadie te haya "patrocinado", sin pagar ninguna cuota de entrada a un reclutador y sin obtener ningún beneficio por convencer a un tercero de que compre, a diferencia de un esquema piramidal, donde la propia posibilidad de obtener beneficio depende explícitamente de la incorporación de nuevos reclutas por parte de cada participante. Y no existe ninguna entidad capaz de "quedarse" con el dinero de los últimos compradores, porque cada operación de compraventa ocurre entre dos partes que acuerdan libremente un precio de mercado, de la misma manera en que ocurre al comprar o vender oro, acciones o una vivienda. El propio suministro de Bitcoin es, además, completamente auditable por cualquiera en tiempo real (capítulo 7) -cualquier persona puede verificar, en cualquier momento, exactamente cuántos bitcoins existen y en qué direcciones, sin tener que confiar en la palabra de nadie-, algo que ningún esquema Ponzi permite jamás, precisamente porque su ocultamiento es la condición necesaria para que el fraude funcione.



Un esquema Ponzi depende de un operador central; la red de Bitcoin, no.

La crítica legítima que se esconde detrás de la etiqueta equivocada

Dicho esto, conviene ser justos con la preocupación real que suele esconderse detrás de esta acusación, aunque esté mal etiquetada. Es la llamada "teoría del más tonto" (greater fool theory), que sostiene que el precio de Bitcoin depende, en última instancia, de que siempre haya alguien dispuesto a pagar más por él en el futuro, ya que -a diferencia de una acción, que genera dividendos, o de un inmueble, que genera alquiler- Bitcoin no produce ningún flujo de caja propio que permita calcular un "valor intrínseco" con los métodos tradicionales de valoración financiera. Es la posición que defienden, de forma pública y reiterada durante años, inversores tan reputados como Warren Buffett, que llegó a calificar a Bitcoin como "veneno para ratas al cuadrado" y afirmó que, si le regalaran todo el bitcoin del mundo por veinticinco dólares, no lo aceptaría porque "no sabría qué hacer con él", o su histórico socio Charlie Munger, que lo describió como "un contrato de apuesta" -ni una moneda, ni una materia prima, ni un valor financiero, en su opinión- y llegó a pedir públicamente su prohibición siguiendo el ejemplo de China. Es una crítica económica legítima y todavía abierta, que Bitcoin comparte en parte con el oro (que tampoco genera ningún flujo de caja) y, en menor medida, con cualquier activo cuyo valor dependa mayoritariamente de la oferta y la demanda futuras más que de una renta que produzca por sí mismo. Conviene distinguir con claridad, sin embargo, esta crítica válida sobre la dificultad de valorar Bitcoin -sostenida por figuras serias del mundo de la inversión, no por desconocimiento- de la acusación, estructuralmente incorrecta, de que se trate de un fraude piramidal.

Fraudes reales que sí encajan en la definición, y que no son Bitcoin

Existen, eso sí, auténticos esquemas Ponzi y piramidales que se han disfrazado de proyectos de criptomonedas para aprovechar la popularidad de Bitcoin y la falta de familiaridad de muchos inversores con el sector, y distinguirlos con nombres y cifras concretas ayuda a entender la diferencia real. BitConnect prometía a sus usuarios rendimientos diarios garantizados de hasta un 1% a través de un supuesto "bot de trading" que, en realidad, nunca existió; entre 2016 y su colapso en enero de 2018 captó unos 2.400 millones de dólares de

al menos 4.500 personas en casi un centenar de países, pagando los rendimientos prometidos con el capital de los inversores más recientes, el mecanismo Ponzi clásico. Su fundador, Satish Kumbhani, fue acusado formalmente en Estados Unidos en 2022 y se enfrenta a una pena máxima de setenta años de prisión, aunque continúa en paradero desconocido; su principal promotor en Norteamérica, Glenn Arcaro, se declaró culpable y fue condenado a 38 meses de cárcel. OneCoin, por su parte, ni siquiera contaba con una blockchain real que respaldara la criptomoneda que decía vender -una diferencia estructural fundamental con Bitcoin, cuya blockchain, como hemos visto a lo largo de todo este libro, es pública y verificable por cualquiera-, y captó a través de una estructura piramidal de reclutamiento un total estimado de unos 4.000 millones de dólares en todo el mundo; su fundadora, Ruja Ignatova, apodada "la Reina de las Criptomonedas", huyó en 2017 y figura desde entonces en la lista de los fugitivos más buscados del FBI, mientras que su socio Karl Sebastian Greenwood fue condenado a veinte años de prisión en Estados Unidos. Confundir estos casos concretos de fraude -con operadores identificables, promesas de rentabilidad garantizada y, en el caso de OneCoin, ni siquiera una blockchain real- con el propio Bitcoin es, paradójicamente, uno de los malentendidos que más ha dañado la reputación pública de una tecnología que, en este aspecto muy concreto, funciona de una manera fundamentalmente distinta a la de los fraudes que se le atribuyen.

Por qué Bitcoin genera tanta oposición

Más allá de la etiqueta de Ponzi, vale la pena preguntarse por qué Bitcoin concentra un nivel de crítica y de rechazo que pocos activos financieros reciben, porque las razones no son todas del mismo tipo, y conviene distinguirlas con el mismo cuidado.

Una amenaza institucional real

Bitcoin compite, aunque sea todavía a pequeña escala, con el monopolio que los bancos centrales ejercen sobre la emisión de dinero (capítulo 4) y con los ingresos por señoreaje que ese monopolio genera para los Estados, y también con el negocio de comisiones de buena parte del sector bancario y de pagos tradicional, que factura por intermediar transferencias y pagos que Bitcoin permite hacer sin intermediarios (capítulo 12). El episodio de la llamada "Operation Choke Point 2.0" que analizamos en el capítulo 28 -la presión regulatoria informal ejercida entre 2021 y 2025 sobre bancos estadounidenses para que restringieran el acceso de empresas de criptoactivos a servicios financieros básicos- es un ejemplo documentado de cómo esa fricción institucional puede traducirse en acciones concretas, más allá del debate puramente teórico. Es razonable esperar cierta resistencia, más o menos abierta, de instituciones cuyo modelo de negocio o cuyas competencias regulatorias se ven, al menos parcialmente, cuestionadas.

Crítica económica y técnica formulada por voces serias

Como hemos visto a lo largo de este capítulo y del anterior, existen objeciones serias y bien argumentadas sobre la volatilidad, la dificultad de valoración, el coste energético y la escalabilidad de Bitcoin, formuladas por economistas y tecnólogos sin ningún interés particular en desacreditarlo, sino desde el rigor de sus respectivas disciplinas. Las críticas de inversores como Buffett y Munger que citamos más arriba, o de numerosos economistas académicos que cuestionan la viabilidad de un sistema monetario con oferta fija e inelástica (capítulo 26, apartado sobre la sustitución del dinero fiat), entran en esta categoría: no buscan

desacreditar a Bitcoin por motivos espurios, sino que aplican, con honestidad intelectual, los mismos criterios de valoración y de análisis macroeconómico que aplicarían a cualquier otro activo o propuesta monetaria.

Algunas de estas voces merecen citarse por su nombre, precisamente porque su prestigio profesional obliga a tomar en serio sus argumentos en lugar de descartarlos como ruido. El premio Nobel de Economía Paul Krugman ha comparado en varias ocasiones, desde su columna en The New York Times, la revalorización de Bitcoin con episodios históricos de burbujas especulativas como la manía de los tulipanes del siglo XVII, argumentando que un activo sin flujos de caja, sin respaldo de ningún bien o servicio productivo y cuyo valor depende enteramente de que otro comprador esté dispuesto a pagar más por él en el futuro, no cumple los requisitos económicos clásicos de un buen dinero ni de una inversión racional a largo plazo. El economista Nouriel Roubini, conocido por haber anticipado la crisis financiera de 2008 -lo que le valió el apodo de "Dr. Doom"-, ha sido uno de los críticos más constantes y explícitos del sector, calificando repetidamente a Bitcoin como "la madre de todas las burbujas" y argumentando que su volatilidad extrema lo inhabilita, por definición, para cumplir la función de reserva de valor estable que sus defensores le atribuyen. El también premio Nobel Joseph Stiglitz ha llegado a proponer que las criptomonedas deberían prohibirse directamente, por considerar que su principal utilidad práctica demostrada hasta la fecha ha sido facilitar la evasión fiscal y el blanqueo de capitales, más que ofrecer ningún beneficio social neto que compense esos costes.

Quienes defienden Bitcoin responden a estas críticas concretas señalando que la comparación con la manía de los tulipanes ignora que Bitcoin lleva más de quince años revalorizándose de forma sostenida a través de múltiples ciclos completos de auge y caída -algo que ninguna burbuja histórica documentada ha logrado-, que la propia naturaleza incipiente de cualquier activo monetario nuevo implica, casi por definición, una volatilidad inicial que tiende a reducirse con la maduración del mercado (un patrón que, como vimos en el capítulo 32, se observa de forma empírica en los datos de volatilidad de Bitcoin de la última década), y que la evasión fiscal y el blanqueo de capitales, si bien son usos reales y documentados, representan hoy una fracción decreciente y minoritaria del volumen total de transacciones, como recogen los propios informes anuales de Chainalysis citados en el capítulo 6. Ninguna de estas respuestas cierra el debate de forma definitiva -Krugman, Roubini y Stiglitz mantienen, a día de 2026, posiciones sustancialmente similares a las que formularon hace años-, pero sí ilustran que se trata de un desacuerdo genuino entre marcos analíticos distintos, no de una discusión resuelta por la evidencia disponible en un solo sentido.

Una reputación heredada de sus primeros años

Como vimos en los capítulos 6 y 18, la asociación temprana de Bitcoin con mercados como Silk Road y con numerosos fraudes y hackeos ha dejado una huella reputacional que persiste en la percepción pública mucho después de que los datos -la propia trazabilidad de la blockchain, la proporción decreciente de uso ilícito- hayan matizado sustancialmente esa imagen inicial. Esta clase de reputación heredada es notoriamente lenta de revertir: numerosos estudios de percepción pública muestran que la asociación inicial de una tecnología nueva con un uso problemático tiende a persistir en la opinión general durante mucho más tiempo del que tarda esa tecnología en diversificar sus usos reales.

Incentivos mediáticos hacia el sensacionalismo

Las caídas bruscas de precio, los hackeos y los fraudes generan titulares mucho más fácilmente que la explicación pausada de cómo funciona el protocolo o de sus casos de uso legítimos, lo que produce una cobertura mediática estructuralmente sesgada hacia el sensacionalismo, sin que eso implique necesariamente mala fe por parte de cada medio en particular: es, simplemente, el mismo sesgo que favorece la cobertura de accidentes de avión sobre la de los miles de vuelos diarios que aterrizan sin incidentes.

Un desacuerdo ideológico genuino

Como exploramos en el capítulo 27, una parte de la oposición a Bitcoin no es económica ni técnica, sino política: proviene de quienes consideran que cierto grado de control colectivo y democrático sobre la política monetaria es preferible a un dinero apolítico que ningún gobierno puede ajustar en una crisis. Esta postura tiene representantes visibles en la esfera política de distintos países -legisladores que han impulsado activamente una regulación más restrictiva sobre criptoactivos alegando riesgos de protección al consumidor, de blanqueo de capitales o de estabilidad financiera-, y es, dentro del debate público, una posición tan legítima como la contraria, aunque parta de premisas normativas distintas sobre el papel que debe jugar el Estado en la gestión del dinero.

Tratar toda esta oposición como un bloque monolítico -"atacan a Bitcoin porque les conviene" o, en sentido inverso, "toda crítica a Bitcoin es ignorancia"- simplifica en exceso un fenómeno en el que se mezclan, de forma real, intereses institucionales legítimos en juego, crítica técnica y económica seria formulada por voces reputadas, inercia reputacional, sesgos mediáticos estructurales y un desacuerdo político de fondo que no tiene una respuesta correcta única.

El uso en actividades ilícitas

Ya abordamos este debate en el capítulo 6 a propósito de Silk Road, y conviene retomarlo aquí con más matices. Es innegable que Bitcoin se ha usado, y se sigue usando, para actividades ilegales -mercados de la red oscura, ransomware, evasión de sanciones internacionales, entre otras-. Al mismo tiempo, la naturaleza pública y permanente de la blockchain (capítulo 7) ha convertido a Bitcoin, paradójicamente, en una de las herramientas más rastreables jamás utilizadas por delincuentes, muy distinta en ese sentido al efectivo físico verdaderamente anónimo. Empresas especializadas en análisis de blockchain colaboran habitualmente con las fuerzas de seguridad de numerosos países para rastrear fondos ilícitos, y varios de los casos citados en este libro -desde Silk Road hasta el hackeo de Bitfinex- terminaron con detenciones o recuperaciones de fondos gracias, precisamente, a ese rastro público e inmutable. Los datos disponibles de organizaciones como Chainalysis sitúan de forma consistente la proporción de actividad ilícita sobre el volumen total de transacciones de Bitcoin en cifras muy reducidas, comparables o inferiores a las estimadas para el sistema financiero tradicional, aunque el debate sobre la metodología exacta de estas estimaciones sigue abierto entre distintos analistas e instituciones.

La concentración de la minería y el desarrollo del software

Ya mencionamos en los capítulos 17 y 23 que, a pesar del ideal de descentralización total, la minería se concentra en la práctica en un número relativamente reducido de grandes operaciones industriales y de pools de minería, y que ciertos países han llegado a concentrar, en determinados momentos, una fracción muy significativa del hashrate mundial. Un patrón similar, aunque de naturaleza distinta, se observa en el desarrollo del software: aunque cualquiera puede, en teoría, proponer cambios al protocolo, en la práctica un número relativamente reducido de desarrolladores experimentados, con gran reputación técnica acumulada en el proyecto, ejerce una influencia considerable sobre qué propuestas de mejora avanzan y cuáles no. Los defensores de Bitcoin argumentan que esta influencia es, en cualquier caso, muy distinta de un control formal -como demostró el propio episodio de la guerra del tamaño de bloque del capítulo 21, donde los desarrolladores no lograron imponer una postura sin el respaldo del resto de la comunidad-, pero se trata de un matiz real frente a la narrativa más simplificada de "descentralización total" que a veces se presenta de forma poco crítica.

El coste energético frente a su utilidad real

Ya analizamos este debate en profundidad en el capítulo 23, pero conviene recordar aquí su núcleo: para los críticos, el consumo energético de Bitcoin representa un coste social y medioambiental difícil de justificar frente a otras formas más eficientes de mover valor digitalmente; para sus defensores, ese consumo es precisamente la fuente de la seguridad y la resistencia a la censura que hacen valioso al sistema, y no un desperdicio comparable a otros usos de energía sin ningún propósito equivalente.

¿Bitcoin sustituirá al dinero fiat?

Existe un desacuerdo considerable, incluso dentro de la propia comunidad de Bitcoin, sobre cuál será su papel final dentro del sistema financiero global: desde quienes defienden un escenario "hiperbitcoinizado", en el que Bitcoin sustituiría por completo a las monedas fiat como referencia mundial de valor, hasta quienes lo ven más bien como un activo de reserva complementario -una suerte de "oro digital" dentro de carteras de inversión diversificadas- que coexistirá indefinidamente junto con las monedas tradicionales, sin llegar nunca a reemplazarlas en el uso cotidiano. La mayoría de los economistas convencionales, incluidos muchos que reconocen méritos técnicos genuinos en el diseño de Bitcoin, se muestran escépticos ante el escenario de sustitución total, señalando la dificultad práctica de que un sistema con oferta fija e inelástica gestione adecuadamente los ciclos económicos de una economía moderna del modo en que, con sus propias imperfecciones, intentan hacerlo los bancos centrales actuales.

> *Ninguna de estas críticas invalida, por sí sola, el valor técnico o económico de Bitcoin, pero tampoco deberían descartarse solo porque provengan de fuera de su comunidad de partidarios más convencidos. Entender Bitcoin de verdad exige sostener, a la vez, el entusiasmo por lo que resuelve y el escepticismo razonable ante lo que todavía no ha demostrado.*

El próximo capítulo retoma, desde un ángulo más filosófico, una de las promesas centrales que ha acompañado a Bitcoin desde su nacimiento y que ya hemos rozado varias veces a lo largo de este libro: su potencial como herramienta frente a la vigilancia financiera y frente al poder que los Estados ejercen sobre el dinero de los ciudadanos.

Fuentes y estudios citados en este capítulo

- Yermack, D. (2013). "Is Bitcoin a Real Currency? An Economic Appraisal". National Bureau of Economic Research, Working Paper No. 19747. Uno de los análisis académicos más citados sobre las limitaciones de Bitcoin como moneda en el sentido económico tradicional.
- Chainalysis. "Crypto Crime Report" (informes anuales), fuente principal de las estimaciones sobre actividad ilícita citadas en este capítulo y en el capítulo 6.
- de Vries, A. (2018). "Bitcoin's Growing Energy Problem". Joule, 2(5). Referencia de la vertiente crítica del debate energético, ampliada en el capítulo 23.
- Bank for International Settlements (BIS), informes anuales sobre criptoactivos y su papel dentro del sistema financiero internacional, representativos de la perspectiva escéptica de los bancos centrales.
- Departamento de Justicia de Estados Unidos (2022). Acusación formal contra Satish Kumbhani, fundador de BitConnect, y documentación judicial de la condena de Glenn Arcaro por el esquema Ponzi de BitConnect (2.400 millones de dólares).
- Departamento de Justicia de Estados Unidos, documentación judicial del caso OneCoin, incluida la condena de Karl Sebastian Greenwood y la situación de fugitiva de Ruja Ignatova, incluida en la lista de más buscados del FBI.
- Declaraciones públicas de Warren Buffett (2018, CNBC) y Charlie Munger (2021-2023, diversas apariciones públicas de Berkshire Hathaway) sobre Bitcoin, citadas como representativas de la crítica de inversores tradicionales basada en la ausencia de flujo de caja del activo.

Capítulo 27. Vigilancia financiera, poder estatal y la promesa de libertad individual

En el capítulo 4 mencionamos de pasada a los "cypherpunks", el colectivo de programadores y criptógrafos libertarios de los años noventa que defendía la criptografía como herramienta de libertad individual frente al poder de gobiernos y corporaciones, y de cuyas ideas nació buena parte del terreno intelectual sobre el que se construyó Bitcoin. Este capítulo retoma esa idea y la desarrolla: por qué una parte muy significativa de la comunidad de Bitcoin entiende el proyecto no solo como una tecnología o una inversión, sino como una respuesta política a una tendencia que perciben como real y creciente, el control cada vez más estrecho del Estado sobre el dinero de los ciudadanos, y qué objeciones serias se le hacen a esa visión.

El dinero como interruptor: una idea incómoda

Damos por hecho que el dinero que tenemos en el banco es "nuestro" de la misma forma en que lo es el efectivo que llevamos en la cartera. En la práctica, no es exactamente así: un depósito bancario es, jurídicamente, un derecho de crédito frente a un banco, gestionado a través de una infraestructura -el sistema de pagos- sobre la que ni tú ni el banco tenéis el control último. Esa infraestructura puede, en circunstancias excepcionales pero documentadas, actuar como un interruptor: alguien con la autoridad suficiente puede, sin necesidad de tocar un solo billete físico, impedir que uses tu propio dinero. No es una hipótesis abstracta; ha ocurrido, de forma verificable, en varias democracias consolidadas en los últimos años, no solo en regímenes autoritarios.

Casos reales: cuando el sistema financiero se convierte en un interruptor

- Canadá, 2022: durante las protestas del "Freedom Convoy" contra las restricciones sanitarias por la pandemia, el gobierno federal invocó la Ley de Emergencias y, sin necesidad de una orden judicial previa, congeló alrededor de doscientas seis cuentas bancarias vinculadas a manifestantes y a quienes habían donado dinero a la protesta, por un valor conjunto de unos 7,8 millones de dólares canadienses. En enero de 2024, un tribunal federal falló que la invocación de la ley no estaba justificada por ninguna emergencia nacional real y que la congelación de cuentas sin ningún criterio objetivo previo vulneró los derechos constitucionales a la libertad de expresión y de reunión pacífica, y a la protección frente a registros e incautaciones injustificadas; el Tribunal Federal de Apelación confirmó ese fallo en 2025, y el gobierno ha pedido a la Corte Suprema de Canadá que revise el caso.
- Nigeria, 2020: durante las protestas #EndSARS contra la brutalidad policial, el Banco Central de Nigeria ordenó a la banca privada congelar las cuentas de varias decenas de organizadores y organizaciones que financiaban las protestas, alegando sospechas de blanqueo de capitales y financiación del terrorismo, sin ningún proceso judicial previo. Human Rights Watch documentó que las cuentas permanecieron bloqueadas durante meses, dejando a los afectados sin acceso a su propio dinero para gastos básicos; un tribunal federal nigeriano terminó ordenando su desbloqueo en febrero de 2021.
- Controles de capital y confiscación por inflación: en países como Argentina o Venezuela, gobiernos sucesivos han impuesto, en distintos momentos, restricciones severas a la

compra de divisas extranjeras o a la retirada de depósitos bancarios (los llamados "corralitos"), mientras que episodios de hiperinflación han licuado, de facto, los ahorros denominados en la moneda local de millones de personas sin necesidad de ninguna confiscación formal.

Estos episodios no demuestran que todo control financiero estatal sea ilegítimo -en los tres casos existían, al menos en la intención declarada de las autoridades, objetivos de orden público o de lucha contra el delito-, pero sí demuestran que la capacidad técnica de congelar o restringir el acceso al dinero de un ciudadano, sin mediar necesariamente un proceso judicial previo, es real, se ha usado contra manifestantes pacíficos y disidentes políticos en más de una democracia, y no es exclusiva de regímenes autoritarios lejanos.

El auge de las monedas digitales de banco central (CBDC)

Como mencionamos en el capítulo 24, numerosos bancos centrales del mundo están desarrollando sus propias monedas digitales (CBDC, central bank digital currency). El Banco Central Europeo, por ejemplo, seleccionó en julio de 2026 a treinta y seis proveedores de servicios de pago para el programa piloto del euro digital, con vistas a una posible emisión hacia 2029 si el proceso legislativo europeo avanza según lo previsto. A diferencia de un depósito en un banco comercial actual, una CBDC podría implicar, según cómo se diseñe finalmente, que el propio banco central tenga visibilidad directa sobre cada transacción individual, e incluso la capacidad técnica de programar el dinero -por ejemplo, con fechas de caducidad, restricciones sobre en qué se puede gastar, o límites de acumulación-, algo que ningún billete físico ha permitido nunca. El propio Banco Central Europeo insiste en que el diseño del euro digital incorporará "los máximos niveles de privacidad" y salvaguardas específicas para que ni el BCE ni el Eurosistema puedan identificar a los usuarios a partir de los datos de pago, y el reglamento correspondiente sigue, de hecho, encallado en el Parlamento Europeo precisamente porque varios grupos políticos exigen garantías de privacidad más estrictas antes de aprobarlo. Organizaciones de defensa de las libertades civiles han señalado, sin embargo, que la arquitectura técnica final -y no solo la promesa política del momento del diseño- es la que determinará si esas garantías de privacidad resultan, en la práctica, irreversibles frente a un cambio futuro de gobierno, de circunstancias o de prioridades políticas.

La visión cypherpunk: la privacidad como condición de una sociedad abierta

En 1993, el ingeniero Eric Hughes publicó lo que se conoce como el "Manifiesto Cypherpunk", que sintetizaba la filosofía de este movimiento en una frase muy citada desde entonces: "la privacidad es necesaria para una sociedad abierta en la era electrónica". La idea central no era el secretismo por el secretismo, sino que las personas necesitan poder elegir qué información revelan sobre sí mismas -igual que, en el mundo físico, no todo el mundo puede ver lo que hay dentro de tu casa o escuchar tus conversaciones privadas- para que exista, de verdad, una esfera de autonomía individual frente al poder, ya sea del Estado o de grandes corporaciones. Para este movimiento, del que ya hablamos a propósito de DigiCash y de b-money en el capítulo 2, la criptografía no era una curiosidad técnica, sino literalmente una forma de defensa: código en lugar de leyes, matemáticas en lugar de promesas políticas, precisamente porque las leyes y las promesas políticas pueden cambiar de un gobierno al

siguiente, mientras que ciertas propiedades matemáticas, una vez bien diseñadas, no dependen de la buena voluntad de nadie.

Bitcoin como efectivo digital resistente a la censura

Bitcoin hereda directamente esa filosofía y le añade algo que ningún proyecto cypherpunk anterior había conseguido: funcionar, de forma efectiva y a escala global, sin depender de ningún servidor ni institución central que alguien pudiera presionar, intervenir o cerrar. Como vimos en el capítulo 12, ningún banco central, ningún gobierno y ninguna empresa puede, por sí solo, congelar una wallet de autocustodia, impedir que una transacción válida se incluya en la blockchain, ni imponer una fecha de caducidad sobre unos bitcoins que ya posees: la validación depende de miles de nodos independientes repartidos por todo el planeta, no de una base de datos central que una orden administrativa pueda modificar. Para quienes defienden esta visión, esa propiedad -la resistencia a la censura, verificable técnicamente y no solo prometida políticamente- es la que convierte a Bitcoin en algo cualitativamente distinto de cualquier forma de dinero digital emitida por un Estado, por muchas garantías de privacidad que ese Estado incorpore en el diseño inicial.

El argumento de "libertad es Bitcoin"

A partir de estos elementos, una parte sustancial de la comunidad de Bitcoin defiende una tesis más amplia: que un dinero cuya emisión nadie controla, cuya posesión nadie puede confiscar sin acceso físico a las claves privadas, y cuyo uso nadie puede bloquear unilateralmente, no es simplemente una alternativa de inversión, sino una herramienta de emancipación política frente a Estados cuya capacidad de vigilancia y de control financiero, argumentan, no ha dejado de crecer en las últimas décadas -a través de la expansión de las normas de identificación obligatoria (KYC), del seguimiento fiscal automatizado, de los propios proyectos de CBDC, y de episodios como los de Canadá o Nigeria citados antes-. Bajo esta lectura, comprar y custodiar tus propios bitcoins no es solo una decisión financiera, sino un acto con una dimensión política: la de retirar una parte de tu patrimonio del alcance directo de cualquier autoridad que, en un momento de crisis, decida usar el sistema financiero como instrumento de presión.

Herramientas prácticas para quien quiere ejercer esa privacidad

Más allá del debate filosófico, existe un conjunto de herramientas técnicas concretas, desarrolladas y mantenidas por la propia comunidad de código abierto, para quien decide llevar a la práctica la privacidad financiera que este capítulo defiende como legítima. La más conocida es el CoinJoin, una técnica que permite a varios usuarios combinar sus transacciones en una única transacción conjunta, de modo que un observador externo de la blockchain pública no pueda determinar con certeza qué entrada corresponde a qué salida, rompiendo buena parte del rastro de trazabilidad que, como recordamos en el capítulo 18, hace de la blockchain un libro de contabilidad público y permanente. Wallets como Wasabi o Samourai (esta última descontinuada tras la detención de sus fundadores en 2024, un episodio que analizamos con más detalle en el capítulo 26 a propósito del debate sobre software de privacidad y responsabilidad penal) implementaron esta técnica de forma accesible para usuarios sin conocimientos técnicos avanzados. Es importante subrayar, con el mismo rigor que el resto de este capítulo, que estas herramientas no ofrecen anonimato absoluto ni resultan sencillas de dominar correctamente: errores de uso -por ejemplo, mezclar

fondos y luego enviarlos de vuelta a una dirección ya vinculada a una identidad conocida, como un exchange regulado que exige verificación KYC- pueden anular buena parte de la protección obtenida, y firmas de análisis de blockchain como Chainalysis han desarrollado técnicas de "desmezclado" cada vez más sofisticadas para varias implementaciones de CoinJoin.

Una segunda capa de protección, complementaria y no sustitutiva de la anterior, consiste en proteger la propia conexión de red al transmitir una transacción, usando la red Tor (The Onion Router) para evitar que tu proveedor de internet o un observador de la red pueda vincular tu dirección IP real con la transacción que estás transmitiendo, un vínculo que, de otro modo, podría revelar tu ubicación aproximada o tu identidad incluso si la propia transacción en la blockchain no contiene ningún dato personal directo. La mayoría de los nodos completos de Bitcoin Core, mencionados en el capítulo 12, incluyen soporte nativo para transmitir y recibir tráfico a través de Tor sin configuración adicional compleja. Un tercer conjunto de prácticas, más básico pero igualmente eficaz, consiste simplemente en evitar la reutilización de direcciones -generar una dirección nueva para cada pago recibido, algo que la mayoría de las wallets modernas hacen ya de forma automática por defecto- para dificultar que un observador externo pueda agrupar todas tus transacciones bajo una misma identidad on-chain con solo mirar el historial público.

Conviene señalar, para que esta sección no se lea como una recomendación indiscriminada, que el uso de estas herramientas no es delictivo en sí mismo en la inmensa mayoría de las jurisdicciones -de la misma manera que usar un sobre cerrado para enviar una carta, en lugar de una postal abierta, no convierte a nadie en sospechoso-, pero que, como cualquier tecnología de doble uso, también ha sido empleada por actores maliciosos para dificultar el rastreo de fondos ilícitos, lo que explica buena parte del escrutinio regulatorio creciente que estas herramientas concretas -y no Bitcoin en general- han recibido en los últimos años, incluido el caso judicial de Samourai Wallet ya mencionado.

Las objeciones a esta visión

Esta lectura, con todo, no es unánime, y conviene exponer con el mismo rigor las razones por las que muchos economistas, reguladores y también una parte de los propios usuarios de Bitcoin la matizan o la rechazan.

- La blockchain es pública y, como vimos en los capítulos 18 y 26, extraordinariamente rastreable: quien no toma precauciones adicionales de privacidad dista mucho de operar de forma anónima, lo que debilita, en la práctica cotidiana, buena parte del argumento de "escapar de la vigilancia" para quien no invierte un esfuerzo técnico considerable en protegerla.
- No toda vigilancia financiera es ilegítima: los mismos mecanismos de identificación y control que esta visión critica -KYC, prevención del blanqueo de capitales, reporte de operaciones sospechosas- son también los que, como vimos en el capítulo 18, permitieron rastrear y recuperar parte de los fondos robados en el hackeo de Bitfinex, y los que protegen a consumidores corrientes de buena parte del fraude financiero cotidiano.
- Presentar cualquier CBDC como un proyecto necesariamente orwelliano es una generalización discutible: el diseño final del euro digital, por ejemplo, sigue siendo objeto de negociación política precisamente sobre estas garantías, y organismos como el

Banco Central Europeo insisten en que la privacidad del usuario es un objetivo de diseño explícito, no una ocurrencia tardía; que ese compromiso se mantenga en la práctica, con los años y los cambios de gobierno, es una pregunta legítima, pero distinta de asumir de antemano que fracasará.

- Renunciar a las herramientas de política monetaria y de supervisión financiera tiene costes reales que la mayoría de los economistas convencionales, como vimos en el capítulo 26, consideran significativos: la capacidad de un banco central de actuar en una crisis económica, o la capacidad de un Estado de perseguir la financiación del terrorismo y el crimen organizado a gran escala, son bienes públicos que buena parte de la sociedad valora, no simples instrumentos de opresión.
- La propia premisa de que "más control financiero estatal" equivale, de forma lineal, a "menos libertad individual" es en sí misma una posición política, compartida por una tradición de pensamiento liberal-libertario con una larga historia intelectual, pero no un hecho neutral ni universalmente aceptado; otras tradiciones políticas defienden que cierto grado de supervisión colectiva del sistema financiero es, precisamente, lo que permite sostener servicios públicos, perseguir el fraude a gran escala y responder a emergencias económicas colectivas.

Una herramienta, no una ideología por sí sola

Lo que sí parece razonablemente establecido, más allá de dónde se sitúe cada lector en este debate, es que Bitcoin ofrece, por primera vez en la historia, una propiedad técnica verificable -la imposibilidad de que un tercero congele o confisque unilateralmente unos fondos en autocustodia- que antes solo existía, de forma imperfecta, en el efectivo físico, y que los episodios de Canadá y Nigeria descritos en este capítulo muestran que esa propiedad no es un temor hipotético sin base real. Si esa propiedad debe valorarse principalmente como una salvaguarda legítima frente a abusos de poder documentados, o si conlleva también costes sociales serios en términos de financiación del crimen, evasión fiscal o pérdida de herramientas colectivas de gestión económica, es, en última instancia, un juicio de valores sobre el que personas razonables e informadas siguen, hoy, en desacuerdo.

> *Satoshi Nakamoto no escribió un manifiesto político junto al whitepaper de Bitcoin, pero eligió, para el primer bloque de toda la cadena, una frase sobre un rescate bancario. Quizá la lectura más honesta de ese gesto no sea que Bitcoin resuelve el problema del poder, sino que lo pone, de forma verificable y permanente, sobre la mesa.*

Por qué esta defensa de la libertad y la privacidad importa, hoy más que nunca

Quienes defienden la visión expuesta en este capítulo no la presentan como un ejercicio académico abstracto, sino como una urgencia práctica: sostienen que la tendencia hacia una mayor visibilidad estatal sobre las finanzas individuales no solo no se ha detenido desde los episodios de Canadá y Nigeria, sino que se ha acelerado y ampliado también dentro de las democracias más consolidadas, incluida la Unión Europea. En enero de 2026 comenzó a desplegar su estructura de supervisión la nueva Autoridad Europea contra el Blanqueo de Capitales (AMLA), con sede en Fráncfort, que a partir de 2028 supervisará de forma directa a entidades financieras de gran tamaño; el mismo paquete normativo que la crea, el Reglamento (UE) 2024/1624, introduce a partir de julio de 2027 un límite máximo de 10.000 euros para cualquier pago en efectivo dentro de la Unión, con los Estados miembros

habilitados para fijar límites todavía más bajos, y prohíbe la apertura de cuentas y monederos de criptoactivos anónimos. Para quienes defienden la lectura cypherpunk de este capítulo, esta acumulación de medidas -sumada al proyecto del euro digital ya descrito- no es una serie de episodios aislados, sino la traducción concreta, medida legislativa a legislativa, de la misma tendencia de fondo: cada vez es técnicamente más difícil para un ciudadano corriente mover, guardar o simplemente poseer una cantidad significativa de su propio dinero sin que quede registrada, vinculada a su identidad y accesible para una autoridad, algo que hace apenas una generación era la norma, no la excepción, incluso dentro de las democracias más abiertas.

Es habitual, en el debate público, que esta preocupación se exprese con una retórica muy cargada, comparando la trayectoria regulatoria de la Unión Europea u otras democracias con la de regímenes históricamente totalitarios; conviene señalar, con el mismo rigor que el resto de este capítulo, que esa comparación concreta no resiste el contraste histórico -la Unión Europea es una unión voluntaria de estados democráticos, con elecciones libres, tribunales independientes ante los que estas mismas normas pueden impugnarse (como muestra el propio litigio en curso sobre el euro digital) y una prensa libre que informa activamente sobre estas medidas, condiciones que ningún régimen totalitario del siglo veinte permitió jamás a sus ciudadanos-, y que invocarla sin matices tiende a debilitar, más que a reforzar, un argumento que puede sostenerse perfectamente sobre hechos verificables sin necesidad de exagerarlo. Dicho esto, la preocupación de fondo no depende de esa comparación para ser legítima: el ritmo y el alcance con el que se está reduciendo el margen de anonimato financiero cotidiano, documentado con las cifras y las normas citadas en este mismo capítulo, es un hecho verificable, y decidir cuánto de esa reducción es un precio razonable a cambio de más seguridad colectiva, y cuánto empieza a erosionar una esfera de autonomía individual que vale la pena proteger activamente, es precisamente la pregunta que este capítulo ha intentado plantear con toda la seriedad que merece, sin pretender cerrarla por el lector.

Con esta reflexión filosófica ya planteada, cerramos la parte más discursiva del libro con una mirada, inevitablemente especulativa, hacia el futuro de Bitcoin.

Fuentes y estudios citados en este capítulo

- Hughes, E. (1993). "A Cypherpunk's Manifesto", el texto fundacional de la filosofía cypherpunk citado en este capítulo.
- Federal Court of Canada (2024) y Federal Court of Appeal (2025), sentencias sobre la invocación de la Ley de Emergencias durante las protestas del "Freedom Convoy" de 2022 y la congelación de cuentas bancarias asociada.
- Human Rights Watch (2020, 2021). "Nigeria: Punitive Financial Moves Against Protesters" y cobertura posterior sobre el desbloqueo de las cuentas de los organizadores de #EndSARS.
- Banco Central Europeo. "Progresos en el euro digital" y documentación pública sobre el diseño de privacidad del proyecto, incluida la selección de proveedores del programa piloto anunciada en julio de 2026.
- Cato Institute, análisis independientes sobre el uso de la Ley de Emergencias canadiense y sus implicaciones para las libertades civiles, representativos de la perspectiva crítica con el control financiero estatal.

- Reglamento (UE) 2024/1624 y Reglamento (UE) 2024/1620, sobre el límite de pagos en efectivo de 10.000 euros desde julio de 2027, la prohibición de cuentas de criptoactivos anónimas y la creación de la Autoridad Europea contra el Blanqueo de Capitales (AMLA), con sede en Fráncfort desde enero de 2026.

Capítulo 28. El futuro de Bitcoin

Cualquier ejercicio de predicción sobre el futuro de una tecnología tan discutida como Bitcoin debe abordarse con humildad: nadie, ni siquiera los expertos más informados, puede afirmar con certeza qué papel tendrá dentro de diez, veinte o cien años. Pero sí es posible, con el material que hemos ido acumulando a lo largo del libro, identificar con precisión los retos concretos que la propia comunidad técnica, económica y regulatoria discute hoy abiertamente. Este capítulo, el más extenso de esta parte final, desarrolla en detalle cada uno de esos retos: qué problema plantean exactamente, qué datos existen hoy sobre ellos y qué soluciones, si las hay, se están explorando.

La consolidación como punto de partida

Antes de entrar en los retos, conviene recordar el contexto: la tendencia más consolidada de los últimos años es la de Bitcoin como activo de reserva dentro de carteras diversificadas, impulsada por los ETF del capítulo 24, la adopción corporativa y el interés creciente de inversores institucionales. Bitcoin ha dejado de ser, para una parte importante del mundo financiero, un experimento marginal. Pero esa consolidación no resuelve, por sí sola, ninguno de los retos técnicos, económicos y políticos que exponemos a continuación; en todo caso, los hace más relevantes, porque cuanto más valor y más gente dependen de que Bitcoin siga funcionando como hasta ahora, más costoso resultaría no tener una respuesta razonable para cada uno de ellos.

Reto 1: el presupuesto de seguridad cuando se agote la emisión

Como explicamos en el capítulo 13, la recompensa por bloque se reduce a la mitad cada aproximadamente cuatro años, y hacia el año 2140 dejará de emitirse cualquier bitcoin nuevo. A partir de ese momento, la seguridad de toda la red -el coste que hace que un ataque del 51% resulte prohibitivo, como vimos en el capítulo 16- dependerá exclusivamente de las comisiones que paguen los usuarios. El problema es puramente de aritmética: en 2026, las comisiones representan, según distintos análisis del sector minero, entre un 12% y un 15% de los ingresos totales de los mineros, frente a menos de un 7% antes del halving de 2024; un umbral que buena parte de la industria considera necesario para que la red pudiera, en teoría, sostenerse solo con comisiones -de forma parecida a como un negocio necesita que sus ingresos recurrentes superen un cierto umbral antes de poder prescindir de una inversión inicial que lo sostenía- es que las comisiones representen de forma consistente más del 20% de los ingresos, una cifra a la que la red se está acercando pero que todavía no alcanza de forma estable. Nadie sabe con certeza si, dentro de cien años, el volumen de transacciones en la cadena principal -incluyendo las liquidaciones periódicas de las capas adicionales como Lightning Network- generará comisiones suficientes para mantener un nivel de seguridad comparable al actual. Una propuesta técnica que resolvería el problema de raíz, la llamada "emisión de cola" (tail emission, un pequeño subsidio permanente y perpetuo en lugar de reducirlo a cero), ha sido debatida repetidamente en la comunidad y rechazada de forma prácticamente unánime, porque rompería la promesa fundacional de los 21 millones que analizamos en el capítulo 13 y que buena parte de la comunidad considera intocable. El reto, por tanto, sigue abierto: confiar en que el crecimiento del volumen de uso baste para sostener la seguridad, sin la palanca de emisión que ha funcionado hasta ahora.

Reto 2: la migración poscuántica y el problema de las monedas que nadie puede mover

Ya explicamos en el capítulo 20 por qué la computación cuántica no es, hoy, una amenaza práctica. El reto de futuro no es tanto si llegará esa capacidad, sino qué ocurre incluso después de que la comunidad diseñe y adopte con éxito un esquema de firma resistente a ordenadores cuánticos. Adoptar el nuevo esquema criptográfico exige un cambio de protocolo (probablemente conflictivo, como vimos con la guerra del tamaño de bloque del capítulo 21) y, después, que cada usuario mueva activamente sus fondos a un nuevo formato de dirección compatible. Ahí aparece un problema que ninguna solución puramente técnica puede resolver: existen aproximadamente un millón de bitcoins, muchos de ellos asociados a las direcciones más antiguas de la red y a las que se atribuye a Satoshi Nakamoto, que llevan sin moverse desde 2009 o 2010. Si sus propietarios han perdido las claves, han fallecido sin dejar herencia digital (capítulo 19), o simplemente no vuelven a conectarse jamás, esos fondos no pueden migrarse a un formato seguro por mucho que la comunidad avise con años de antelación, porque migrarlos exige una acción activa de alguien que quizá ya no exista o no pueda actuar. Esto deja abierto un debate incómodo y sin consenso: ¿debería la comunidad, llegado el caso de una amenaza cuántica real y verificable, congelar o invalidar unilateralmente esas monedas dormidas y vulnerables para proteger al resto de la red, aunque eso suponga tocar, por primera vez en la historia de Bitcoin, saldos que nadie ha autorizado a mover? Cualquier respuesta -hacerlo o no hacerlo- entra en tensión directa con alguno de los principios fundacionales del proyecto.

Reto 3: el crecimiento indefinido de la cadena y el coste de validar toda la historia

Cada bloque que se mina se suma, para siempre, al historial que cualquier nodo completo debe descargar y validar desde el bloque génesis si quiere participar plenamente en la red, como explicamos en el capítulo 12. En febrero de 2026, la blockchain completa de Bitcoin ocupaba aproximadamente 718 gigabytes, y crece a un ritmo de entre 50 y 60 gigabytes cada año, sin ningún límite natural que detenga ese crecimiento mientras la red siga funcionando. Existen mecanismos como el modo "podado" (pruning), que permiten a un nodo reducir el espacio que ocupa en disco hasta apenas 7 gigabytes conservando toda la capacidad de validar de forma independiente cada nueva transacción, pero un nodo podado no puede ayudar a otros nodos nuevos a descargar el historial completo ni servir bloques antiguos al resto de la red, una función que solo pueden cumplir los nodos con el archivo completo. El reto de fondo es de accesibilidad a largo plazo: si dentro de veinte o treinta años la sincronización completa de un nodo desde cero exige varios terabytes y semanas de descarga, el número de personas dispuestas y capaces de ejecutar un nodo con el historial íntegro podría reducirse con el tiempo, concentrando esa función en manos de un número menor de operadores -exactamente el tipo de concentración que, como vimos en el capítulo 12, es la que sostiene la resistencia de Bitcoin frente a la censura y la manipulación-. Propuestas técnicas como "assumeutxo", que permiten a un nodo nuevo empezar a operar con seguridad razonable sin descargar y reprocesar absolutamente todo el historial desde el primer bloque, mitigan el problema pero no lo eliminan.

Reto 4: la concentración geopolítica de la minería y de la fabricación de hardware

Más allá de la concentración de pools de minería que ya analizamos en los capítulos 17 y 23, existe un reto de fondo menos discutido: la fabricación de los chips ASIC especializados (capítulo 11) que hacen posible la minería competitiva está concentrada en un número muy reducido de empresas, con una cadena de suministro fuertemente dependiente de fabricantes y ensambladores radicados en muy pocos países. Esta concentración plantea, al menos en teoría, un riesgo de punto único de fallo distinto al de la red misma: si la inmensa mayoría del hardware de minería del mundo proviene de un puñado de fabricantes, cualquier vulnerabilidad, restricción de exportación o -en el escenario más extremo planteado por algunos investigadores de seguridad- una puerta trasera deliberada introducida en el propio hardware, podría tener un efecto desproporcionado sobre la seguridad o la disponibilidad de la red minera mundial. A esto se suma un fenómeno más reciente: a medida que gobiernos empiezan a acumular bitcoin como reserva estratégica -como el propio Estados Unidos, según vimos en el capítulo 24-, crece también el incentivo de algunos Estados para invertir directamente en capacidad de minería nacional, no solo por motivos económicos sino por consideraciones de seguridad nacional, lo que podría introducir, con el tiempo, una dimensión geopolítica más explícita en la distribución del hashrate mundial de la que ha existido hasta ahora.

Reto 5: la fragmentación regulatoria global y el riesgo de la "desbancarización"

Ya vimos, en el capítulo 24, que la regulación de Bitcoin varía enormemente de un país a otro. El reto de futuro no es solo esa fragmentación evidente -prohibición total en algunos países, adopción entusiasta en otros-, sino un riesgo más sutil y menos visible: la presión administrativa informal sobre los bancos para que eviten servir a empresas del sector cripto, incluso cuando esas empresas operan de forma completamente legal. En Estados Unidos, una investigación del Comité de Servicios Financieros de la Cámara de Representantes, publicada en noviembre de 2025, documentó cómo distintos reguladores federales presionaron, entre 2021 y comienzos de 2025, a entidades bancarias para que restringieran el acceso de empresas de criptoactivos a servicios financieros básicos mediante normas ambiguas y un uso extensivo de conceptos discrecionales como el "riesgo reputacional", un fenómeno conocido informalmente como "Operation Choke Point 2.0", que dejó sin acceso bancario a al menos treinta entidades o particulares del sector. En agosto de 2025, la nueva administración estadounidense firmó una orden ejecutiva para poner fin a esta práctica, y a lo largo de 2026 distintos reguladores bancarios han ido retirando formalmente el "riesgo reputacional" como criterio de supervisión. Este episodio ilustra un reto que puede repetirse, con matices, en cualquier país: un gobierno no necesita prohibir Bitcoin de forma explícita para dificultar seriamente su uso, si consigue -de manera formal o informal- que el sistema bancario tradicional se retire de dar servicio a quienes operan con él.

Reto 6: los riesgos propios de escalar mediante capas adicionales

Lightning Network, que explicamos en detalle en el capítulo 22, resuelve buena parte del problema de la capacidad de la cadena principal, pero introduce sus propios retos de futuro. La topología real de la red tiende a concentrar una parte significativa de la liquidez en un número relativamente reducido de nodos muy bien conectados ("hubs"), lo que podría reproducir, a otra escala, el mismo tipo de concentración que la propia arquitectura descentralizada de la cadena principal está diseñada para evitar: si la mayoría de los pagos

dependen de rutas que pasan por un puñado de grandes operadores, esos operadores adquieren una capacidad de observación -y, en el peor de los casos, de censura selectiva- que no tendrían en un sistema verdaderamente distribuido. A esto se suma el resurgimiento parcial del riesgo de custodia: muchas wallets Lightning pensadas para el usuario medio delegan la gestión de los canales en un proveedor externo, reintroduciendo por la puerta de atrás parte de la dependencia de terceros que la autocustodia (capítulo 10) pretende eliminar. Investigadores de seguridad han documentado además una categoría de ataque llamada "channel jamming" (bloqueo de canales), en la que un atacante satura deliberadamente, a bajo coste, la capacidad de rutas de pago ajenas, degradando la utilidad de la red para el resto de usuarios sin necesidad de robar ningún fondo directamente. Ninguno de estos problemas es, a día de hoy, una amenaza existencial para Lightning Network, pero todos siguen siendo objeto de investigación activa y de propuestas de mitigación todavía en desarrollo.

Reto 7: la sostenibilidad del propio desarrollo del protocolo

Como mencionamos en el capítulo 26, un número relativamente reducido de desarrolladores con gran reputación técnica ejerce una influencia considerable sobre la evolución del software de Bitcoin. Un reto de futuro menos discutido públicamente es el de la sostenibilidad económica de ese trabajo: buena parte de los desarrolladores principales de Bitcoin Core reciben financiación, de forma directa o a través de becas, de un número igualmente reducido de empresas y fundaciones del sector -entre ellas plataformas de intercambio, fabricantes de hardware y organizaciones sin ánimo de lucro dedicadas específicamente a sufragar este trabajo-. Esta dependencia de un grupo pequeño de financiadores no equivale a un control directo sobre las decisiones técnicas -el propio historial del proyecto muestra que los desarrolladores han tomado, repetidamente, decisiones contrarias a los intereses inmediatos de empresas del sector-, pero sí introduce una pregunta legítima sobre la resiliencia a largo plazo de un modelo de gobernanza que depende, en última instancia, de que un número reducido de personas cualificadas sigan queriendo -y pudiendo permitirse- dedicar su carrera a mantener un proyecto de código abierto sin ánimo de lucro directo.

Reto 8: la presión regulatoria creciente sobre el consumo energético

Ya analizamos en profundidad el debate energético de Bitcoin en el capítulo 23. De cara al futuro, el reto no es tanto el consumo en sí -que la propia industria ha defendido con los argumentos que ya expusimos-, sino la posibilidad de que gobiernos concretos introduzcan, en el marco de políticas más amplias de transición energética y reducción de emisiones, restricciones o impuestos específicos dirigidos a la minería de criptoactivos, con independencia de su mix energético real. Algunas jurisdicciones ya han explorado medidas de este tipo en los últimos años, y no existe, por ahora, ningún consenso internacional sobre cómo debería tratarse fiscal o regulatoriamente una industria cuyo consumo energético es, a la vez, deliberado por diseño (capítulo 11) y objeto de un intenso escrutinio público.

Tres escenarios, no mutuamente excluyentes, del futuro de Bitcoin

Los tres escenarios comparten un elemento común: ninguno depende de que Bitcoin sustituya por completo al dinero fiduciario a corto o medio plazo.

Síntesis ilustrativa basada en los argumentos expuestos en este capítulo; no constituye una predicción ni una recomendación de inversión.

Tres escenarios plausibles y no mutuamente excluyentes para el papel futuro de Bitcoin.

Un experimento en marcha, no un proyecto terminado

Ninguno de estos ocho retos tiene, hoy, una solución cerrada y unánimemente aceptada, y es poco probable que la tengan pronto: son, en su mayoría, tensiones estructurales entre principios que Bitcoin intenta sostener simultáneamente -descentralización, seguridad, accesibilidad, resistencia a la censura, oferta fija- y que no siempre resultan fáciles de conciliar a medida que la red crece y el tiempo avanza. Quizá la conclusión más honesta con la que cerrar este capítulo es que Bitcoin sigue siendo, más de quince años después de su creación, un experimento en marcha: un sistema cuyo diseño fundamental se ha mantenido notablemente estable y probado a gran escala, pero cuyos retos de futuro no son hipótesis lejanas, sino problemas ya identificados, medibles y, en varios casos, ya en curso, sobre los que la propia comunidad técnica, económica y política que rodea a Bitcoin sigue, hoy mismo, deliberando sin una respuesta definitiva.

Antes de cerrar el libro con un glosario de referencia, el próximo capítulo baja de la teoría a la práctica más inmediata: una guía paso a paso, pensada para quien parte de cero, sobre cómo comprar tus primeros bitcoins, guardarlos con seguridad y entender tus obligaciones fiscales.

Fuentes y estudios citados en este capítulo

- Análisis de mercado de la industria minera (2026), incluidos informes de Bitcoin Magazine Pro y de firmas especializadas en economía de la minería, sobre la evolución de la proporción de comisiones frente al subsidio por bloque en los ingresos totales de los mineros.
- Comité de Servicios Financieros de la Cámara de Representantes de Estados Unidos (2025). "Operation Chokepoint 2.0: Biden's Debanking of Digital Assets", informe de la mayoría republicana sobre la presión regulatoria informal contra empresas de criptoactivos entre 2021 y 2025.

- Orden ejecutiva de la presidencia de Estados Unidos (agosto de 2025) sobre el fin de la "desbancarización" injustificada de sectores lícitos, incluido el de los criptoactivos.
- Datos públicos sobre el tamaño y el crecimiento anual de la blockchain de Bitcoin, recogidos por observatorios independientes como blockchainsize.org y Statista.
- Bitcoin Optech y Bitcoin Core, documentación técnica sobre "assumeutxo" y los modos de nodo podado (pruning) como mitigaciones al crecimiento del historial de la cadena.
- Investigaciones académicas sobre ataques de "channel jamming" en redes de pago de segunda capa tipo Lightning Network, y propuestas de mitigación como los mecanismos de reputación y garantía económica por ruta.

Capítulo 29. Cómo empezar a operar e invertir en Bitcoin: guía paso a paso

Después de dedicar todo este libro a entender qué es Bitcoin, cómo funciona por dentro y qué riesgos y debates lo rodean, este capítulo baja del todo a la práctica: los pasos concretos para comprar tus primeros bitcoins, guardarlos con seguridad y entender tus obligaciones fiscales, pensado para alguien que parte de cero. Antes de empezar, una advertencia necesaria: este capítulo ofrece información general para orientarte, no asesoramiento financiero, legal ni fiscal personalizado. Bitcoin es un activo volátil (capítulo 26), y las normas fiscales y regulatorias cambian con el tiempo y varían según el país; antes de invertir cantidades significativas o de presentar cualquier declaración, conviene contrastar la información con un asesor financiero o fiscal cualificado y con las fuentes oficiales vigentes en el momento en que leas esto.

Antes de comprar: define tu punto de partida

El primer paso no es abrir ninguna cuenta, sino responder con honestidad a un par de preguntas. La primera es cuánto dinero estás dispuesto a destinar a esto sin que un desplome del cincuenta o el setenta por ciento -algo que, como vimos en el capítulo 26, ha ocurrido varias veces en la historia de Bitcoin- te cause un problema económico real. Una regla informal, repetida hasta la saciedad en la comunidad, es no invertir nunca dinero que vayas a necesitar a corto plazo ni dinero cuya pérdida total pondría en riesgo tu estabilidad financiera. La segunda pregunta es tu horizonte temporal: comprar pensando en usarlo dentro de unos meses es una apuesta muy distinta, en términos de riesgo, a comprar con la intención de mantenerlo durante varios años, precisamente porque la volatilidad de Bitcoin tiende a suavizarse -aunque nunca a desaparecer del todo- cuanto más amplio es el periodo que se analiza.

Los riesgos que asumes al invertir en Bitcoin

Antes de comparar a Bitcoin con otros activos o de dar un solo paso práctico, conviene reunir en un mismo lugar, y con el detalle suficiente, todos los riesgos concretos que hemos ido mencionando a lo largo del libro, porque quien invierte necesita verlos juntos, no dispersos en capítulos distintos, para valorar de verdad si está dispuesto a asumirlos.

Mapa de los ocho riesgos descritos en este libro

Los ocho riesgos que se desarrollan a continuación, de un vistazo.

Riesgo de mercado y volatilidad

El precio de Bitcoin puede caer con mucha más fuerza y mucha más rapidez que la de la mayoría de los activos tradicionales, como hemos visto en el capítulo 26: caídas del cincuenta, del setenta o incluso de más del ochenta por ciento desde máximos se han repetido varias veces en su historia, y no existe ningún mecanismo, ni gubernamental ni de mercado, que amortigüe esas caídas, a diferencia de los "circuit breakers" (interrupciones automáticas de la negociación) que existen en las principales bolsas de valores para frenar el pánico en momentos de desplome extremo. La propia coyuntura de 2026, con una caída acumulada en torno al 28% mientras el oro apenas retrocedía un 3,9% (capítulo 29, comparativa de activos), es un recordatorio reciente de que esta volatilidad no es un fenómeno del pasado, exclusivo de los primeros años de Bitcoin, sino una característica que sigue presente incluso con una capitalización de mercado ya de más de un billón de dólares.

Riesgo regulatorio

Como muestra el propio caso de la salida de Binance de la Unión Europea que veremos más abajo, o la prohibición completa de la minería y el comercio en China (capítulo 24), las normas que rigen el acceso, la fiscalidad o incluso la legalidad de Bitcoin pueden cambiar, a veces de forma repentina, en cualquier país. Este riesgo no se limita a prohibiciones explícitas: como analizamos en el capítulo 28 a propósito de la "Operation Choke Point 2.0" en Estados Unidos, un gobierno puede dificultar seriamente el acceso a Bitcoin mediante presión administrativa informal sobre el sistema bancario, sin necesidad de declarar ninguna

prohibición formal, lo que hace que este riesgo sea, en ocasiones, más difícil de anticipar que una simple ley publicada en un boletín oficial.

Riesgo de custodia y de plataforma

Dejar tus fondos en un exchange te expone a que la empresa sea hackeada, gestione mal la seguridad o quiebre, como ocurrió con Mt. Gox y FTX (capítulo 18), episodios que combinados supusieron la pérdida o el bloqueo temporal de varios miles de millones de dólares en fondos de clientes. Gestionar tú mismo tus claves privadas elimina ese riesgo concreto de contraparte, pero lo sustituye por un riesgo de naturaleza distinta: el de perder tú mismo el acceso por error humano, olvido o negligencia (capítulo 19), un tipo de pérdida que, a diferencia de un fraude bancario tradicional, no tiene ningún departamento de atención al cliente ni ningún seguro de depósitos al que recurrir después.

Riesgo tecnológico y de protocolo

Aunque el núcleo de Bitcoin no ha sido comprometido con éxito en más de quince años (capítulo 15), no puede descartarse por completo el descubrimiento futuro de alguna vulnerabilidad grave en el propio protocolo o en el software que lo implementa, ni resolverse todavía con certeza el reto a largo plazo de la computación cuántica (capítulos 20 y 28). Es un riesgo de probabilidad baja pero de impacto potencialmente muy alto, de la misma naturaleza que otros riesgos tecnológicos de cola larga (low-probability, high-impact) que resulta difícil de cuantificar con precisión, precisamente porque no existe ningún precedente histórico directo sobre el que apoyar una estimación fiable.

Riesgo de liquidez en momentos de estrés

Aunque Bitcoin cotiza permanentemente, en episodios de pánico generalizado del mercado la profundidad real de compradores dispuestos a pagar un precio razonable puede reducirse de forma notable, ampliando las caídas más de lo que ocurriría en un mercado más líquido: es la misma dinámica que, en cualquier mercado financiero, hace que las órdenes de venta grandes ejecutadas en momentos de pánico obtengan, de media, precios peores que las mismas órdenes ejecutadas en condiciones normales, un efecto que se agrava cuando, además, varias plataformas experimentan problemas técnicos de sobrecarga -algo que ha ocurrido en el pasado en exchanges concretos durante picos extremos de volatilidad- justo quiy más se necesita poder operar con normalidad.

Riesgo fiscal y administrativo

Como veremos más abajo, declarar mal tus ganancias, olvidar el Modelo 721 si corresponde, o no entender que un simple canje entre criptomonedas ya genera una obligación fiscal, puede acarrear sanciones administrativas que nada tienen que ver con el rendimiento de tu inversión: es perfectamente posible ganar dinero con Bitcoin y, aun así, terminar con un problema económico neto por una gestión fiscal descuidada, algo que muchos principiantes no anticipan hasta que ya es demasiado tarde para corregirlo sin coste.

Riesgo de productos apalancados o indirectos

Instrumentos que ofrecen una exposición amplificada a Bitcoin -ya sea mediante apalancamiento directo en un exchange, ya sea a través de vehículos corporativos que se financian con deuda y acciones preferentes para comprar bitcoin, como analizamos en detalle en el capítulo 24 a propósito de Strategy y Michael Saylor- añaden una capa de riesgo adicional, distinta y superior a la de poseer bitcoin directamente, porque combinan la volatilidad del activo subyacente con el riesgo financiero de quien emite el producto. Comprar acciones de una empresa que posee bitcoin apalancado con deuda no es lo mismo que comprar bitcoin: como vimos en el capítulo 24, ese tipo de vehículos puede perder valor más rápido que el propio bitcoin en una caída de mercado, precisamente por el apalancamiento que en las subidas amplifica las ganancias.

Riesgo psicológico y de comportamiento

El miedo a perderse una subida (FOMO) y el pánico ante una caída son, en la práctica, responsables de una parte muy significativa de las pérdidas reales de los inversores particulares, con independencia de cómo se comporte objetivamente el mercado a largo plazo: numerosos estudios sobre el comportamiento de los inversores particulares en activos volátiles muestran, de forma consistente, que el rendimiento medio obtenido por los propios inversores suele ser inferior al rendimiento del activo en sí, precisamente porque tienden a comprar después de las subidas más pronunciadas -cuando el entusiasmo es mayor- y a vender después de las caídas más pronunciadas -cuando el miedo es mayor-, exactamente al revés de la estrategia racional.

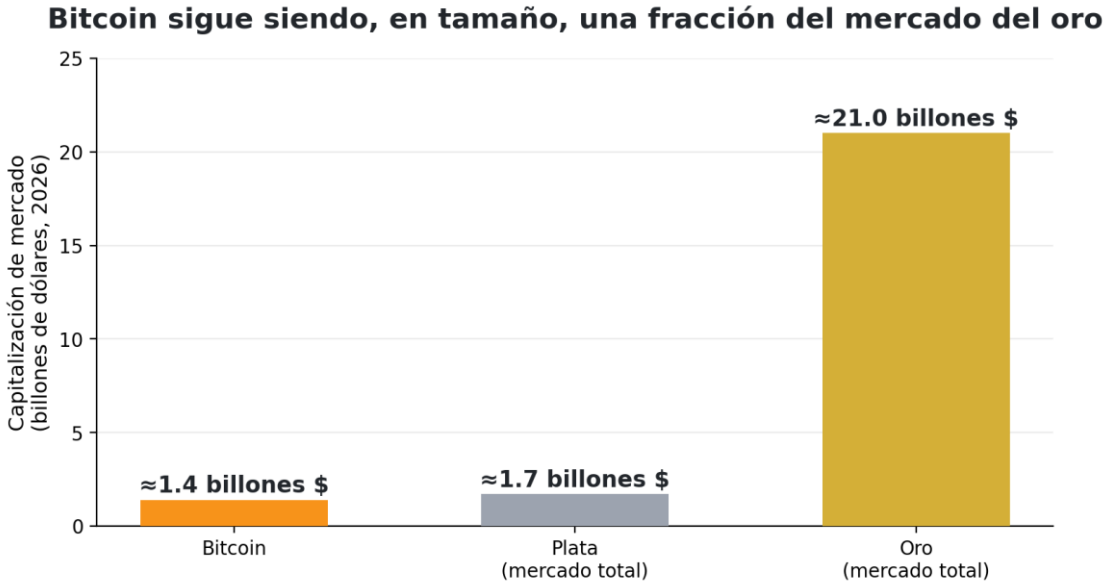
Ninguno de estos riesgos, por separado, es exclusivo de Bitcoin -la volatilidad también existe en la plata, el riesgo regulatorio también afecta a otros activos financieros, el riesgo de custodia también existe con el oro físico-, pero la combinación simultánea de todos ellos, y su intensidad particular en el caso de Bitcoin, es lo que exige el nivel de prudencia con el que se plantea este capítulo.

Bitcoin frente al oro, la plata y el forex: una comparación honesta

Antes de decidir cuánto destinar a Bitcoin, muchas personas se preguntan cómo se compara con otros activos tradicionalmente usados para proteger o hacer crecer el patrimonio: el oro, la plata y el mercado de divisas (forex). No son sustitutos perfectos entre sí -cada uno cumple una función distinta en una cartera-, pero conviene entender sus diferencias objetivas antes de decidir. Los datos de esta sección corresponden a la situación de mercado en 2026 y cambian constantemente; se ofrecen como referencia comparativa, no como previsión de rentabilidad futura.

Activo	Naturaleza	Tamaño aproximado del mercado (2026)	Volatilidad	Horario y liquidez
Bitcoin	Activo digital con oferta fija de 21 millones de unidades (capítulo 13)	En torno a 1,3-1,5 billones de dólares en capitalización	Alta: aproximadamente entre 5 y 6 veces más volátil que el oro, con oscilaciones intradía en torno al 5%	Mercado abierto 24 horas al día, 7 días a la semana, en todo el mundo

Activo	Naturaleza	Tamaño aproximado del mercado (2026)	Volatilidad	Horario y liquidez
Oro	Materia prima física, metal precioso con miles de años de uso como reserva de valor	En torno a 20-22 billones de dólares en capitalización, el activo no financiero más valioso del mundo	Baja-moderada: oscilaciones intradía en torno al 1,6% de media	Mercados con horario de negociación, aunque con centros abiertos de forma casi continua en distintas zonas horarias
Plata	Materia prima física, con una demanda dividida entre inversión y uso industrial (electrónica, paneles solares)	Muy inferior a la del oro; un mercado mucho más pequeño y, por ello, más sensible a entradas o salidas de capital	Alta para tratarse de un metal precioso, en parte por su menor tamaño de mercado y por su exposición a los ciclos de la demanda industrial	Mercados con horario de negociación, ligado a las mismas plazas que el oro
Forex (mercado de divisas)	Mercado de intercambio entre monedas fiat; no es una "reserva de valor" en el mismo sentido que los anteriores, sino el mecanismo mediante el que se determina el valor relativo entre monedas	Con diferencia, el mercado financiero más grande del mundo: un volumen negociado de unos 9,6 billones de dólares cada día, según datos del Banco de Pagos Internacionales	Variable según el par de divisas, generalmente inferior a la de Bitcoin salvo en episodios de crisis cambiaria	Mercado abierto prácticamente 24 horas al día, 5 días a la semana



El mercado de divisas (forex) no se incluye por ser un flujo diario (≈9,6 billones de $/día), no un valor total acumulado como los anteriores.

Capitalización de mercado de Bitcoin frente al oro y la plata (2026).

Bitcoin frente al oro: la comparación más citada

La etiqueta "oro digital", que ya mencionamos en el capítulo 13, resume la comparación más habitual: ambos activos comparten una oferta limitada y verificable, ninguno depende de la decisión de un banco central, y ambos se han usado históricamente como cobertura frente a la pérdida de valor de las monedas fiat. Pero la diferencia de escala es enorme: con una capitalización en torno a 1,3-1,5 billones de dólares frente a los 20-22 billones del oro, Bitcoin representa hoy apenas entre un 6% y un 7% del valor total del mercado del oro, y tendría que multiplicar su precio varias veces solo para igualarlo. La propia coyuntura de 2026 ilustra bien que "oro digital" es una etiqueta sobre sus propiedades a largo plazo, no una garantía de que se comporte igual que el oro a corto plazo: en lo que va de año, Bitcoin acumula una caída en torno al 28%, mientras que el oro apenas ha retrocedido un 3,9%, un recordatorio de que, pese a las similitudes conceptuales, siguen siendo activos con una dinámica de precio muy distinta, y de que el oro ha mantenido, hasta la fecha, una estabilidad muy superior en los momentos de mayor incertidumbre.

Bitcoin frente a la plata

La plata comparte con el oro su naturaleza física y su papel histórico como reserva de valor, pero su mercado es mucho más pequeño, lo que la hace más volátil que el oro -aunque, en general, todavía menos volátil que Bitcoin-. A esa volatilidad se suma un factor que el oro apenas tiene: una parte sustancial de la demanda de plata proviene de usos industriales (paneles solares, electrónica, vehículos eléctricos), lo que significa que su precio depende, en parte, de ciclos económicos e industriales que nada tienen que ver con su papel como refugio de valor, una dimensión que ni el oro ni Bitcoin comparten de la misma manera.

Bitcoin frente al forex

El forex merece una precisión distinta a los dos anteriores: comprar dólares, yenes o francos suizos no es, en sentido estricto, una "inversión" comparable a comprar oro o Bitcoin con la expectativa de que se revalorice con el tiempo, sino una operación sobre el valor relativo entre dos monedas fiat, cada una de ellas sujeta a la política monetaria de su banco central respectivo (capítulo 4). Es, con diferencia, el mercado más líquido del planeta -mueve en un solo día casi siete veces la capitalización total de Bitcoin-, y se usa sobre todo para cubrir riesgos de tipo de cambio en el comercio internacional o para especular con esas fluctuaciones a corto plazo, no como depósito de valor a largo plazo. Comparar el forex con Bitcoin es, en cierto modo, comparar dos categorías distintas: una apuesta sobre el valor relativo de monedas gestionadas activamente por bancos centrales, frente a un activo cuya oferta nadie puede alterar.

El argumento a favor de Bitcoin frente a estas alternativas

Quienes defienden destinar una parte de su patrimonio a Bitcoin en lugar de -o además de- oro, plata o forex suelen señalar su portabilidad (puedes trasladar cualquier cantidad, de cualquier valor, a cualquier parte del mundo en minutos, sin pasar por una aduana ni pagar un transporte físico asegurado, algo imposible con lingotes de oro o plata), su divisibilidad exacta hasta el satoshi (capítulo 13, frente a la dificultad práctica de dividir físicamente un lingote), la posibilidad de autocustodia sin depender de una cámara acorazada ni de un banco (capítulo 10), su mercado abierto permanentemente, y un historial de rentabilidad a largo

plazo -aunque errático y con caídas muy pronunciadas por el camino- superior al del oro, la plata o cualquier divisa importante en la década transcurrida desde su creación.

El argumento a favor del oro, la plata o el forex

Quienes prefieren mantenerse en los activos tradicionales, o combinarlos con Bitcoin en lugar de sustituirlos, señalan con razón que el oro cuenta con miles de años de aceptación universal como reserva de valor, frente a los poco más de quince de Bitcoin; que su volatilidad muchísimo menor lo hace más adecuado para quien no puede permitirse caídas del 50% o el 70% en su patrimonio; que no depende de ninguna infraestructura tecnológica, clave privada ni conexión a internet que pueda perderse o fallar (capítulo 19); y que 2026, con el oro resistiendo con una caída mínima mientras Bitcoin se dejaba más de una cuarta parte de su valor, es precisamente el tipo de año que ilustra por qué muchos gestores de patrimonio siguen considerando al oro, no a Bitcoin, el refugio más fiable en momentos de incertidumbre. El forex, por su parte, sigue siendo la herramienta más adecuada -no un competidor real de Bitcoin o el oro- para quien necesita cubrirse frente al riesgo de tipo de cambio en operaciones comerciales o viajes internacionales.

No son sustitutos, sino herramientas distintas

La conclusión más honesta de esta comparación es que Bitcoin, el oro, la plata y el forex no compiten exactamente por el mismo papel dentro de una cartera: el forex es, ante todo, una herramienta de cobertura y de especulación a corto plazo sobre el valor relativo de las monedas; el oro es el activo con el historial más largo y la volatilidad más baja como reserva de valor; la plata añade una dimensión industrial que ninguno de los otros tres tiene; y Bitcoin ofrece propiedades tecnológicas -portabilidad, divisibilidad, autocustodia, un mercado permanentemente abierto- que ninguno de los activos tradicionales puede igualar, a cambio de una volatilidad y una historia mucho más cortas. Muchos inversores, en lugar de elegir uno solo, combinan varios de estos activos precisamente por sus diferencias, no a pesar de ellas. Cuál es la combinación adecuada para ti depende de tu tolerancia al riesgo, tu horizonte temporal y tu situación personal, y es, de nuevo, una decisión que conviene tomar con información, y no solo con este libro como única fuente.

Paso 1: elige una plataforma regulada para comprar

La forma más habitual de conseguir tus primeros bitcoins es a través de un exchange (una plataforma de compraventa) o, cada vez más, a través del propio banco. Desde el 1 de julio de 2026, el Reglamento europeo MiCA (Markets in Crypto-Assets), que ya mencionamos en el capítulo 24, se aplica de forma plena en España, y la Comisión Nacional del Mercado de Valores (CNMV) supervisa a todos los proveedores de servicios de criptoactivos que operan en el país, que ahora necesitan una autorización expresa para poder ofrecer sus servicios legalmente. Es como el paso de un mercadillo sin ningún control de calidad a un mercado con inspectores permanentes: no elimina todos los riesgos de invertir, pero sí garantiza que la plataforma cumple unos requisitos mínimos de solvencia, transparencia y protección al usuario. Operar con una entidad sin autorización MiCA no es necesariamente una estafa, pero sí implica renunciar a buena parte de las protecciones que este nuevo marco regulatorio está precisamente diseñado para ofrecerte.

Comparativa de plataformas (situación en julio de 2026)

La tabla siguiente resume la situación, a fecha de escribir este libro, de algunas de las plataformas más conocidas entre el público español. Se trata de una fotografía de un momento muy concreto -las licencias, las comisiones y hasta la disponibilidad de una plataforma en un país pueden cambiar en cuestión de semanas, como demuestra el propio caso de Binance-, así que antes de decidirte por una conviene comprobar su situación actualizada directamente en el listado oficial de entidades autorizadas que publica la CNMV.

Plataforma	Tipo	Autorización MiCA en España (jul. 2026)	Comisión aproximada	Notas
Binance	Exchange global	No dispone de ella; cesó el servicio a clientes de la UE el 1 de julio de 2026 tras retirar su solicitud en Grecia	No aplica	Los usuarios existentes solo pueden retirar los fondos que ya tenían depositados; no admite nuevos registros, compras ni canjes
Coinbase	Exchange global	Sí, mediante pasaporte europeo emitido en Luxemburgo	Aproximadamente 0,5%-1,5% por operación	Interfaz sencilla, orientada a usuarios que empiezan
Kraken	Exchange global	Sí, mediante pasaporte europeo emitido en Irlanda	Aproximadamente 0,16%-0,26% por operación	Comisiones más ajustadas, pensado para usuarios algo más habituados
Crypto.com	Exchange global	Sí, licencia de entidad financiera limitada de la autoridad de Malta (MFSA) desde 2025-2026	Variable según volumen y método de pago	Muy centrado en su tarjeta de débito cripto y en programas de recompensas
Bit2Me	Plataforma española	Sí; primera cripto-fintech española autorizada por la CNMV bajo MiCA, y también primera con licencia adicional del Banco de España para pagos con stablecoins reguladas	Variable según el servicio	Atención al cliente en español y soporte de transferencias SEPA nacionales
Bancos tradicionales (Openbank, CaixaBank, Renta 4, BBVA, entre otros)	Banco con servicio de criptoactivos	Sí, autorizados por la CNMV	Habitualmente algo más altas que en un exchange especializado	Cómodo si ya eres cliente, con todo integrado en la misma app del banco; oferta de criptoactivos disponibles normalmente más limitada

Conviene leer esta tabla con perspectiva histórica, no solo como una lista de recomendaciones: el caso de Binance -durante años el mayor exchange del mundo por volumen, y hasta hace apenas unas semanas la opción más usada por cientos de miles de españoles- ilustra de forma muy concreta uno de los riesgos que mencionamos en el capítulo 18 sobre exchanges: la disponibilidad y las condiciones de una plataforma pueden cambiar de la noche a la mañana por motivos regulatorios, no solo por un hackeo o una quiebra, y quien mantenía fondos allí ha tenido que moverlos con urgencia. Es otro argumento más a favor del principio del capítulo 10 que retomamos más abajo: cuanto antes retires tus bitcoins a una wallet propia, menos dependes de que una plataforma concreta siga operando en tu país.

Paso 2: verifica tu identidad (KYC)

Al registrarte en cualquier plataforma regulada, tendrás que pasar por un proceso llamado KYC ("know your customer", conoce a tu cliente): subir una foto de tu documento de identidad, a veces una selfie de verificación, y en ocasiones justificar el origen de los fondos que vas a usar. Es exactamente el mismo tipo de trámite que ya haces al abrir una cuenta bancaria, y responde a las mismas obligaciones legales de prevención del blanqueo de capitales que analizamos, desde otro ángulo, en el capítulo 26. Puede resultar tedioso, pero es una señal de que la plataforma cumple con la regulación, no un obstáculo arbitrario.

Paso 3: deposita fondos

La mayoría de las plataformas permiten ingresar dinero mediante transferencia bancaria (habitualmente la opción con menores comisiones, aunque más lenta) o mediante tarjeta de débito o crédito (más rápida, pero normalmente con una comisión adicional notable). Conviene evitar, como norma general, financiar una compra de bitcoin con una tarjeta de crédito o cualquier otra forma de deuda: es un consejo tan válido para Bitcoin como para cualquier otro activo volátil, porque combina el riesgo de la inversión con el coste añadido de los intereses de la deuda si el valor cae antes de que puedas devolverla.

Paso 4: haz tu primera compra

Con fondos ya en la plataforma, comprar bitcoin es, técnicamente, sencillo: seleccionas el importe y confirmas la operación. Las plataformas suelen ofrecer dos tipos principales de orden: la orden de mercado, que compra de inmediato al mejor precio disponible en ese momento (rápida, pero sin control exacto sobre el precio final), y la orden límite, que solo se ejecuta si el precio alcanza el valor que tú especifiques (más control, pero sin garantía de que llegue a ejecutarse). Muchos usuarios que empiezan, precisamente para evitar la presión de intentar "acertar el momento perfecto" -algo que ni los profesionales consiguen de forma consistente-, optan por una estrategia llamada compra periódica o dollar-cost averaging: invertir una cantidad fija y modesta a intervalos regulares (por ejemplo, cada mes), en lugar de una única cantidad grande de una sola vez. Esto no garantiza mejores resultados que comprar todo de golpe -depende, en última instancia, de cómo evolucione el precio, algo que nadie puede predecir con certeza-, pero sí reduce el riesgo de invertir todo tu capital justo antes de una caída pronunciada, repartiendo ese riesgo a lo largo del tiempo, del mismo modo que repartir la siembra de un campo a lo largo de varias semanas reduce el riesgo de perderlo todo si una sola tormenta arrasa el cultivo plantado en un único día.

Paso 5: retira tus bitcoins a tu propia wallet

Este es, probablemente, el paso más importante -y el que más se salta la gente que empieza-. Como explicamos en el capítulo 10, mientras tus bitcoins permanecen en la cuenta del exchange, no los controlas realmente: dependes de que esa empresa gestione bien la seguridad y de que no restrinja tu acceso, tal como vimos con los casos de Mt. Gox o FTX en el capítulo 18, y como acabamos de ver con la propia salida de Binance de la Unión Europea. La recomendación casi universal de la comunidad, especialmente para cantidades que superen lo que necesitas mover con frecuencia, es retirar tus fondos a una wallet propia -al menos una wallet de software de confianza para empezar, y un monedero hardware si la cantidad lo justifica-, siguiendo exactamente el proceso que describimos en el capítulo 10: instalar la wallet, generar y anotar correctamente tu frase semilla, y solo entonces enviar los fondos desde el exchange a la dirección que tu propia wallet te proporcione, verificando la dirección con cuidado antes de confirmar el envío.

Paso 6: protege tu copia de seguridad desde el primer día

No dejes este paso para "más adelante": como vimos en el capítulo 19, buena parte de los bitcoins perdidos en la historia lo fueron por falta de una copia de seguridad correcta, no por ningún ataque. Sigue los principios que detallamos en el capítulo 25 -copia física, verificada, protegida frente a robo y frente a daño físico- desde el momento en que generas tu primera wallet, no cuando ya tengas una cantidad que te preocupe perder.

Fiscalidad en España: lo que debes saber, en líneas generales

En España, las ganancias obtenidas al vender bitcoin, al cambiarlo por otra criptomoneda o al usarlo para pagar tributan en el IRPF como ganancias patrimoniales, dentro de la base imponible del ahorro, con tipos que en 2026 van, según el tramo de la ganancia, aproximadamente entre el 19% y el 28%, sin ningún mínimo exento: cualquier beneficio, por pequeño que sea, debe declararse. Un matiz que sorprende a muchos principiantes es que cambiar bitcoin directamente por otra criptomoneda (por ejemplo, por ether) es, a efectos fiscales, un hecho imponible igual que venderlo por euros, aunque nunca hayas pasado por dinero fiat en el proceso; el cálculo de la ganancia o pérdida se realiza, con carácter general, mediante el método FIFO ("first in, first out"), que da por vendidos primero los bitcoins que compraste primero, por orden cronológico. Si mantienes criptoactivos por un valor superior a 50.000 euros en plataformas situadas en el extranjero, existe además una obligación informativa específica, el Modelo 721, que debe presentarse entre el 1 de enero y el 31 de marzo del año siguiente. Dado que estas normas -tipos impositivos, umbrales, plazos- pueden cambiar de un ejercicio fiscal a otro, conviene confirmar siempre los detalles vigentes directamente en la Sede Electrónica de la Agencia Tributaria o con un asesor fiscal antes de presentar cualquier declaración.

Errores más comunes de quien empieza

- Comprar impulsado por el miedo a quedarse fuera (FOMO, "fear of missing out"), normalmente durante una subida rápida de precio, sin haber definido antes cuánto estás dispuesto a arriesgar ni durante cuánto tiempo piensas mantener la inversión.

- Usar apalancamiento (invertir con dinero prestado por la propia plataforma, multiplicando tanto las ganancias como las pérdidas potenciales) sin entender completamente el riesgo de perder mucho más de lo invertido inicialmente; es una práctica que incluso muchos inversores experimentados evitan por su enorme volatilidad.
- Dejar indefinidamente todos los fondos en el exchange, ignorando el principio de autocustodia del capítulo 10, por pura comodidad o por no querer enfrentarse a la curva de aprendizaje de una wallet propia.
- No verificar con cuidado una dirección de destino antes de confirmar un envío, especialmente al copiarla y pegarla, un riesgo que ya explicamos en el capítulo 18 a propósito del malware que sustituye direcciones en el portapapeles.
- Caer en promesas de rentabilidad garantizada, de "duplicación" de bitcoin o de inversiones con retornos extraordinarios y sin riesgo: como vimos en el capítulo 18, ninguna oportunidad legítima funciona así, y este tipo de ofertas sigue siendo, año tras año, una de las formas más habituales de estafa alrededor de Bitcoin.

> *Empezar en Bitcoin no exige ser un experto en criptografía ni en economía monetaria - aunque, si has llegado hasta aquí, ya sabes bastante más que la mayoría-. Exige, sobre todo, ir despacio: informarte antes de invertir, invertir solo lo que puedas permitirte perder, y tomarte tan en serio la custodia de tus claves como te tomarías la de las llaves de tu propia casa.*

Antes de cerrar el libro, la última parte reúne cincuenta preguntas frecuentes, organizadas por bloques temáticos, que resumen en formato rápido de consulta las dudas más habituales de quien se acerca a Bitcoin por primera vez, y un glosario final con las definiciones más importantes de todos los términos técnicos que hemos ido introduciendo a lo largo de estas páginas.

Fuentes y estudios citados en este capítulo

- Comisión Nacional del Mercado de Valores (CNMV). "Nueva regulación de criptoactivos - Reglamento MiCA", listado y criterios sobre entidades autorizadas a operar en España tras la aplicación plena del reglamento desde julio de 2026.
- Reglamento (UE) 2023/1114, "Markets in Crypto-Assets" (MiCA), citado también en el capítulo 24.
- Agencia Tributaria. "Modelo 721: Declaración informativa sobre monedas virtuales situadas en el extranjero", sede electrónica oficial, con los requisitos, umbrales y plazos de presentación vigentes.
- Agencia Tributaria, información general sobre la tributación de las ganancias y pérdidas patrimoniales derivadas de operaciones con criptomonedas en el IRPF.
- Cobertura periodística de junio y julio de 2026 sobre la retirada de Binance del Espacio Económico Europeo tras no obtener la autorización MiCA, y sobre el listado de entidades ya autorizadas por la CNMV, incluidas Coinbase, Kraken, Crypto.com y Bit2Me.
- Banco de Pagos Internacionales (BIS). Encuesta trienal sobre el volumen diario negociado en los mercados mundiales de divisas.

- Datos de capitalización de mercado del oro y Bitcoin, y de rentabilidad comparada en 2026, recogidos por observatorios de mercado como MacroMicro y análisis sectoriales del mercado del oro y la plata.
- Estudios sobre el comportamiento financiero de los inversores particulares (behavioral finance) y la brecha habitual entre la rentabilidad de un activo y la rentabilidad media realmente obtenida por sus inversores, citados como referencia del riesgo psicológico descrito en este capítulo.

PARTE VII

PREGUNTAS FRECUENTES

Capítulo 30. Concepto básico de Bitcoin

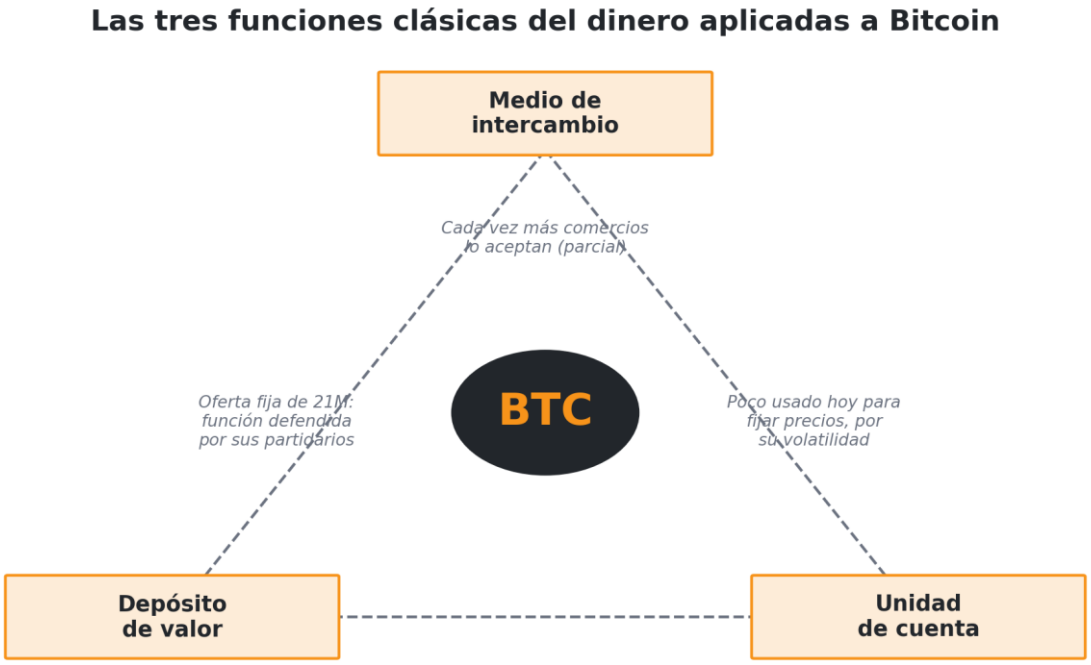
Después de treinta capítulos explicando la historia, el funcionamiento técnico, la seguridad y los debates que rodean a Bitcoin, esta nueva parte del libro cambia de formato: en lugar de capítulos narrativos, encontrarás cincuenta preguntas, agrupadas en nueve bloques temáticos, que son exactamente las que suele hacerse alguien que oye hablar de Bitcoin por primera vez -o que lleva tiempo usándolo pero nunca ha tenido la ocasión de resolver sus dudas más básicas-. Cada respuesta remite, cuando corresponde, al capítulo del libro donde se trata esa cuestión con más profundidad, de modo que esta parte funciona también como un mapa de consulta rápida sobre todo lo anterior. Empezamos por las preguntas más fundamentales: qué es Bitcoin, en realidad.

¿Qué es exactamente Bitcoin, es dinero real o solo "números en una pantalla"?

Bitcoin es, en su definición más precisa, un sistema de dinero digital descentralizado: un protocolo informático que permite transferir valor entre dos personas cualquiera del mundo sin necesidad de un banco, un gobierno o cualquier otro intermediario que autorice la operación. Cada unidad de Bitcoin no es un archivo que se copia y se envía, como ocurriría con una fotografía por correo electrónico, sino una entrada verificada en un libro de contabilidad público y compartido por miles de ordenadores en todo el mundo, la cadena de bloques o blockchain, que detallamos en el capítulo 7. Esa es la diferencia esencial con "números en una pantalla" en el sentido despectivo con el que a veces se usa la expresión: los números que ves en tu aplicación de Bitcoin no son una cifra arbitraria que una empresa privada pueda cambiar a su antojo, como sí podría hacer, en teoría, el operador de un videojuego con la moneda interna de ese juego. Representan una participación real y verificable en un sistema cuya oferta total está matemáticamente limitada a 21 millones de unidades (capítulo 13) y cuyas reglas de funcionamiento están fijadas por un protocolo que miles de participantes independientes verifican de forma constante, no por la decisión de una sola entidad.

Que sea "dinero real" depende, en el fondo, de qué entendamos por dinero. Como explicamos en el capítulo 1, cualquier forma de dinero -desde las conchas o el ganado en sociedades

antiguas hasta el papel moneda actual- cumple su función en la medida en que un número suficiente de personas confía en ella y la acepta a cambio de bienes y servicios. El euro que llevas en la cartera tampoco tiene, por sí mismo, ningún valor intrínseco: es papel impreso cuyo valor depende enteramente de que el resto de la sociedad, y en última instancia el Estado que lo respalda, acepte usarlo como medio de pago. Bitcoin cumple, en mayor o menor medida según el contexto, las tres funciones clásicas que la economía exige a cualquier forma de dinero: sirve como medio de intercambio (puedes usarlo para pagar, aunque de forma todavía limitada), como depósito de valor (aunque de forma volátil, como veremos en el bloque de precio e inversión) y, de manera más discutida, como unidad de cuenta. Que hoy se use sobre todo como inversión y menos como medio de pago cotidiano no lo convierte en "menos real": simplemente refleja en qué fase de adopción se encuentra un tipo de dinero todavía muy joven.



Las tres funciones clásicas del dinero: en cuáles encaja Bitcoin hoy, y en cuáles solo parcialmente.

¿Quién creó Bitcoin y por qué lo hizo?

Bitcoin fue creado por una persona -o un grupo de personas- que se presentó bajo el seudónimo Satoshi Nakamoto, cuya identidad real nunca se ha confirmado con certeza, como explicamos con detalle en el capítulo 5. Nakamoto publicó el 31 de octubre de 2008 el documento técnico ("whitepaper") que describía el funcionamiento de Bitcoin, y el 3 de enero de 2009 puso en marcha la red minando el primer bloque de la cadena. Participó activamente en el desarrollo del software y en los foros de discusión durante poco más de dos años, y a mediados de 2010 fue delegando progresivamente el control del proyecto en otros programadores de la comunidad, hasta desaparecer por completo de la vista pública a comienzos de 2011, sin volver a comunicarse desde entonces bajo esa identidad.

En cuanto al porqué, el propio contexto histórico ofrece la respuesta más sólida, desarrollada en el capítulo 4: Bitcoin nació en octubre de 2008, en pleno epicentro de la crisis financiera global, cuando los bancos centrales rescataban con dinero público a entidades financieras que habían asumido riesgos excesivos, mientras millones de familias corrientes perdían sus casas y sus ahorros. Nakamoto dejó constancia explícita de esa motivación al incluir, en los datos del primer bloque de la cadena, el titular de un periódico británico de ese mismo día sobre un segundo rescate bancario. El objetivo declarado era crear una forma de dinero cuya oferta no pudiera alterarse por decisión de ningún gobierno o banco central, y cuyo funcionamiento no dependiera de la confianza en ninguna institución concreta, sino de las matemáticas y de un protocolo verificable por cualquiera. Que su creador permanezca en el anonimato, lejos de restar credibilidad al proyecto, es coherente con esa misma filosofía: Bitcoin no depende de la reputación ni de la autoridad de una persona concreta para funcionar, sino del código que esa persona dejó publicado y que la red sigue ejecutando, sin cambios en sus reglas fundamentales, más de diecisiete años después.

¿Bitcoin es una moneda, una inversión o una especie de acción digital?

La respuesta honesta es que Bitcoin no encaja del todo en ninguna de esas tres categorías tradicionales, y esa dificultad de clasificación es, en sí misma, uno de los motivos por los que genera tanto debate regulatorio, como veremos en el bloque de legalidad. No es exactamente una moneda en el sentido clásico, porque aunque sirve para pagar en los comercios que lo aceptan, su volatilidad (bloque siguiente) lo hace poco práctico todavía como unidad de cuenta estable del día a día: pocas personas fijan el precio de un alquiler o un salario en bitcoin, precisamente porque ese precio, medido en euros, puede variar de forma notable en cuestión de semanas. Tampoco es una acción, porque no representa la propiedad de ninguna empresa, no da derecho a voto en ninguna junta, no reparte dividendos ni depende de los beneficios de un negocio: no existe una "empresa Bitcoin" detrás de la que estés comprando una parte, sino una red descentralizada sin dueño (siguiente pregunta).

Lo más preciso es describir a Bitcoin como una nueva categoría de activo, a menudo llamada activo digital o criptoactivo, que combina propiedades de varias categorías anteriores sin coincidir del todo con ninguna: comparte con el oro su oferta limitada y su función de reserva de valor (capítulo 29, comparativa con el oro), comparte con una moneda su uso, todavía minoritario, como medio de pago, y comparte con la tecnología de internet su naturaleza puramente digital y su capacidad de transferirse instantáneamente a cualquier parte del mundo. La mayoría de los organismos reguladores del mundo, incluida la Unión Europea a través del Reglamento MiCA (capítulo 24), han optado finalmente por tratarlo como una categoría jurídica propia -"criptoactivo"- en lugar de forzarlo dentro de las definiciones legales pensadas originalmente para el dinero o los valores financieros tradicionales.

¿En qué se diferencia Bitcoin del dinero que usamos a diario, como el euro?

La diferencia más importante es quién controla la oferta. El euro es una moneda fiduciaria (capítulo 1): el Banco Central Europeo puede aumentar la cantidad de euros en circulación cuando lo considera necesario para sus objetivos de política monetaria, como ocurrió a gran escala tras la crisis de 2008 y de nuevo durante la pandemia. Bitcoin, en cambio, tiene una oferta fijada matemáticamente en el propio protocolo: nunca existirán más de 21 millones de unidades, y el ritmo al que se crean nuevos bitcoins disminuye a la mitad cada

aproximadamente cuatro años mediante un mecanismo llamado "halving" (capítulo 13), sin que ninguna persona ni institución pueda acelerar ni frenar ese calendario.

La segunda gran diferencia es quién controla y verifica las transacciones. Cuando pagas con euros mediante una transferencia bancaria o una tarjeta, un banco o una red de pagos centralizada (como Visa o Mastercard) registra, aprueba y puede, en teoría, bloquear esa operación. Con Bitcoin, esa función la desempeña de forma colectiva una red de miles de ordenadores independientes repartidos por el mundo (capítulo 7), sin que ninguno de ellos, por sí solo, tenga capacidad de vetar la transacción de otro usuario legítimo. Esto tiene ventajas -nadie puede congelar tu cuenta de bitcoin por una decisión administrativa unilateral, como sí puede ocurrir con una cuenta bancaria- y también costes: si pierdes el acceso a tus propios bitcoins, no existe ningún banco al que llamar para recuperarlos (capítulo 19), mientras que un banco tradicional sí puede, en general, restituir el acceso a una cuenta con la documentación adecuada.

¿Por qué se dice que Bitcoin es descentralizado y qué significa eso en la práctica?

Que Bitcoin sea descentralizado significa que no existe una sede central, una empresa propietaria, un servidor principal ni una autoridad única capaz de decidir unilateralmente sus reglas de funcionamiento, tal como se detalla en el capítulo 7. En su lugar, la red está formada por miles de nodos -ordenadores que ejecutan el software de Bitcoin de forma voluntaria- repartidos por decenas de países, cada uno de los cuales mantiene una copia completa e independiente del historial de todas las transacciones jamás realizadas, y por mineros que compiten entre sí, en distintas partes del mundo, para procesar nuevos bloques de transacciones (capítulo 8).

En la práctica, esta descentralización se traduce en varias consecuencias muy concretas. Ningún gobierno puede "apagar" Bitcoin ordenando el cierre de una única oficina o servidor, porque no existe tal cosa: para detener la red por completo haría falta desconectar simultáneamente a decenas de miles de participantes independientes en todo el planeta, algo que ningún actor, ni siquiera una coalición de grandes gobiernos, ha conseguido hacer hasta la fecha, ni siquiera con prohibiciones tan drásticas como la china (capítulo 24). Cualquier cambio en las reglas fundamentales del protocolo requiere, además, un consenso amplio entre desarrolladores, mineros y usuarios, no la decisión de un consejo de administración: es lo que en el capítulo 22 llamamos el proceso de las "bifurcaciones" (forks), a menudo lento y conflictivo, precisamente porque nadie tiene autoridad para imponer un cambio al resto. Esta ausencia de un punto único de control o de fallo es, para muchos de sus defensores, la propiedad más valiosa de Bitcoin; para sus críticos, es también la fuente de buena parte de sus problemas prácticos, como la dificultad de revertir un error o de coordinar mejoras técnicas con rapidez, un debate que retomamos en el capítulo 26.

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", el documento técnico original que define Bitcoin, citado en detalle en el capítulo 5.
- Ammous, S. (2018). "The Bitcoin Standard: The Decentralized Alternative to Central Banking". Wiley. Análisis de Bitcoin desde la teoría monetaria clásica, citado también en el capítulo 1.

- Banco Central Europeo. Publicaciones divulgativas sobre las funciones clásicas del dinero (medio de intercambio, depósito de valor, unidad de cuenta) aplicadas al análisis de los criptoactivos.
- Reglamento (UE) 2023/1114, "Markets in Crypto-Assets" (MiCA), sobre la clasificación jurídica de los criptoactivos en la Unión Europea, citado también en los capítulos 24 y 29.

Capítulo 31. Uso y utilidad en la vida diaria

Resueltas las preguntas más básicas sobre qué es Bitcoin, este segundo bloque aborda una duda igual de habitual: hasta qué punto se puede usar realmente en el día a día, más allá de la teoría.

¿Se puede pagar el café, la compra del súper o la gasolina con Bitcoin hoy en día?

En términos generales, todavía no de forma directa y masiva, salvo excepciones concretas. La inmensa mayoría de los comercios de barrio, supermercados y gasolineras de España y de la mayor parte del mundo no aceptan bitcoin como forma de pago en su terminal de tarjeta, y no existe hoy ninguna obligación legal que los fuerce a hacerlo, a diferencia de lo que ocurrió brevemente en El Salvador (bloque de legalidad). Lo que sí existe, y ha crecido de forma notable, es un ecosistema de soluciones intermedias: tarjetas de débito emitidas por exchanges como Coinbase o Crypto.com (capítulo 29), que convierten tus bitcoins a euros de forma automática en el momento del pago, permitiéndote pagar en cualquier terminal que acepte tarjetas normales, aunque el comercio nunca llegue a "recibir" bitcoin directamente ni sea consciente de que lo has usado.

Donde sí es más habitual el pago directo en bitcoin es en un número creciente, aunque todavía reducido, de comercios online, en algunas plataformas de viajes y reservas, y en negocios concretos -cafeterías, tiendas, restaurantes- de ciudades o zonas con una comunidad cripto activa, a menudo mediante la red Lightning (capítulo 21), que permite pagos casi instantáneos y con comisiones mínimas, resolviendo buena parte de la lentitud y el coste que tenía pagar directamente en la cadena principal de Bitcoin. En la práctica, para la inmensa mayoría de la población, Bitcoin se usa hoy mucho más como un activo de inversión que como un medio de pago cotidiano, algo que sus propios defensores reconocen abiertamente y que no contradice su utilidad: muchas tecnologías -internet en sus primeros años, la tarjeta de crédito en sus inicios- tardaron años en pasar de un uso minoritario a uno generalizado.

¿En qué países o tiendas se acepta Bitcoin como forma de pago?

No existe ningún país, a fecha de 2026, en el que Bitcoin sea de aceptación obligatoria para todos los comercios: El Salvador, el único caso histórico de curso legal obligatorio, revirtió esa obligación en 2025 (bloque de legalidad), y la República Centroafricana, que también lo adoptó brevemente como moneda de curso legal en 2022, tampoco mantiene esa obligación en la práctica actual. Lo que sí existe es una aceptación voluntaria, cada vez más extendida, por parte de cadenas y comercios concretos: plataformas de viajes como Travala, empresas de tecnología, algunas franquicias de restauración en países concretos, y un número muy amplio de pequeños comercios independientes que se anuncian específicamente como "Bitcoin friendly", a menudo localizables mediante mapas colaborativos que mantiene la propia comunidad. Los casos de El Zonte y Lugano, que desarrollamos con más detalle en el capítulo 45, muestran cómo esa aceptación voluntaria puede llegar a concentrarse geográficamente hasta formar auténticas "economías circulares" locales.

En España, la aceptación directa de bitcoin en tiendas físicas sigue siendo minoritaria y depende de la iniciativa de cada negocio concreto, aunque ha crecido el número de comercios, especialmente en el sector tecnológico y en negocios de propietarios entusiastas

de las criptomonedas, que lo aceptan a través de procesadores de pago especializados que convierten automáticamente el bitcoin recibido a euros para el comerciante, eliminando para él el riesgo de la volatilidad. La tendencia general, más que la aceptación directa comercio a comercio, apunta hacia soluciones de conversión automática -tarjetas y procesadores de pago- que hacen invisible para el vendedor la naturaleza del activo con el que en realidad estás pagando.

¿Tiene sentido cobrar parte del sueldo en Bitcoin?

Es una posibilidad real en algunas empresas, especialmente en el sector tecnológico y entre negocios directamente vinculados al ecosistema cripto, pero conviene entenderla como lo que es: una decisión de inversión personal disfrazada de forma de cobro, no una alternativa neutral al salario en euros. Si tu empresa te ofrece la opción de recibir una parte de tu nómina en bitcoin, en la práctica estás decidiendo destinar ese porcentaje de tus ingresos a un activo con la volatilidad que describimos en el bloque de precio e inversión, en lugar de recibirlo en la moneda con la que probablemente pagas tu alquiler, tu hipoteca o tu compra semanal.

Los argumentos a favor -para quien ya tiene intención de invertir en bitcoin de todos modos- son la comodidad de acumular sin tener que comprar activamente cada mes, y en algunos casos el ahorro en comisiones de conversión. Los argumentos en contra son igual de sólidos: concentra tu principal fuente de ingresos y tu inversión en el mismo activo volátil, exactamente el tipo de concentración de riesgo que los asesores financieros suelen desaconsejar, y complica la gestión fiscal, porque en España cobrar en bitcoin no te exime de las obligaciones del IRPF y añade, además, la necesidad de valorar correctamente esa parte del salario en euros en el momento de recibirla. Como con cualquier decisión de este tipo, no existe una respuesta universal: depende de tu tolerancia al riesgo, de qué porcentaje de tu sueldo estarías dispuesto a destinar a ello, y de si ya tenías intención de invertir en bitcoin con ese mismo dinero.

¿Sirve Bitcoin como reserva de valor, como el oro, o solo para especular?

Ambas cosas son parcialmente ciertas, y no se excluyen entre sí. La etiqueta "oro digital", que exploramos en profundidad en el capítulo 29, refleja el argumento de fondo a favor de Bitcoin como reserva de valor: al igual que el oro, tiene una oferta limitada que nadie puede aumentar a voluntad, no depende de la política monetaria de ningún banco central, y es portable y divisible con una facilidad que el oro físico no tiene. Su historial de rentabilidad a largo plazo, pese a caídas muy pronunciadas por el camino, ha sido en la década transcurrida desde su creación superior al de la mayoría de los activos tradicionales, lo que ha convencido a un número creciente de inversores, incluidos algunos institucionales (bloque de futuro), de tratarlo como un componente legítimo de una cartera diversificada.

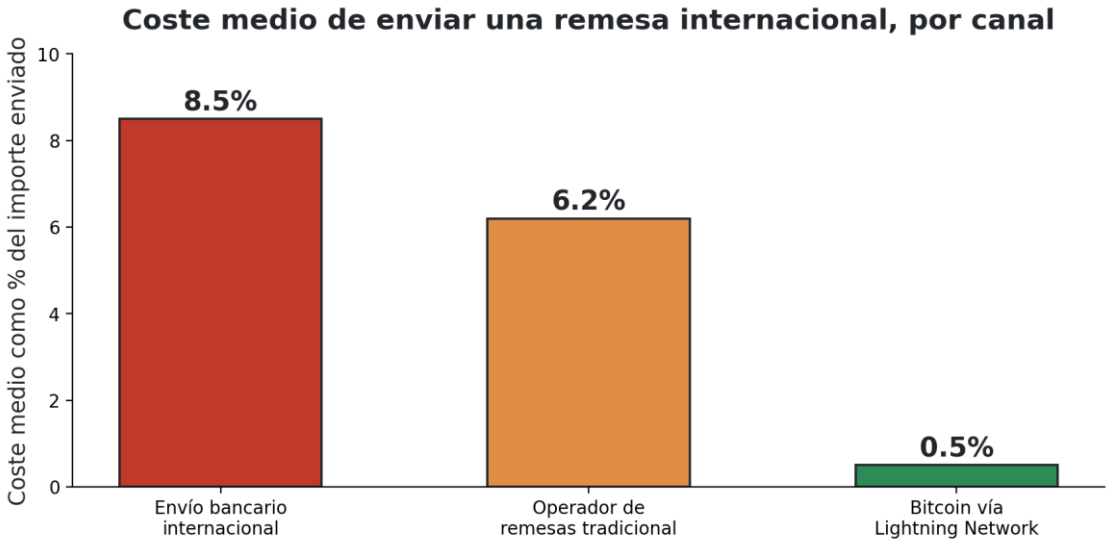
Al mismo tiempo, es innegable que una parte muy sustancial de la actividad diaria en el mercado de Bitcoin es puramente especulativa: comprar con la expectativa de vender más caro en un plazo corto, sin ninguna intención de usarlo como reserva de valor a largo plazo. Esta doble naturaleza no es exclusiva de Bitcoin -el oro también tiene un componente especulativo en su mercado de futuros, y las acciones de empresas sólidas también son objeto de especulación a corto plazo por parte de algunos inversores-, pero sí es más pronunciada en el caso de Bitcoin por su volatilidad y por lo reciente de su historia, que todavía

no ha tenido tiempo de asentar el mismo consenso social que el oro ha construido a lo largo de milenios.

¿Qué ventajas prácticas tiene usar Bitcoin frente a una transferencia bancaria normal?

La ventaja más citada es la velocidad y el alcance geográfico: una transferencia bancaria internacional tradicional puede tardar entre uno y varios días hábiles en completarse, pasar por varios bancos intermediarios que cobran comisiones adicionales en cada paso, y verse limitada por horarios bancarios y festivos locales. Una transacción de Bitcoin, en cambio, puede confirmarse en la red principal en cuestión de minutos, o de forma prácticamente instantánea si se usa la red Lightning (capítulo 21), a cualquier hora del día, cualquier día del año, y llegar directamente al destinatario en cualquier parte del mundo sin pasar por una cadena de bancos intermediarios.

Esto resulta especialmente valioso en dos contextos muy concretos: el envío de remesas internacionales -dinero que trabajadores migrantes envían a sus familias en su país de origen-, donde las comisiones de los servicios tradicionales pueden superar con facilidad el cinco o el diez por ciento del importe enviado, frente a comisiones de una pequeña fracción del uno por ciento cuando el envío se realiza mediante Bitcoin a través de la red Lightning, y el acceso a servicios financieros para las aproximadamente mil cuatrocientos millones de personas en el mundo que, según estimaciones del Banco Mundial, no tienen acceso a una cuenta bancaria tradicional pero sí, cada vez con más frecuencia, a un teléfono móvil con conexión a internet.



Cifras ilustrativas basadas en rangos típicos citados por el Banco Mundial y proveedores del sector.

El coste medio de enviar una remesa internacional varía mucho según el canal utilizado.

Frente a estas ventajas hay que sopesar también los costes: la volatilidad del activo mientras está en tránsito, la necesidad de un mínimo de conocimiento técnico para operar con seguridad (capítulo 19), y unas comisiones de la red principal de Bitcoin que, en momentos de mucha congestión, pueden llegar a ser más altas que las de una transferencia bancaria nacional ordinaria, aunque la red Lightning mitiga buena parte de este último problema.

Fuentes y estudios citados en este capítulo

- Banco Mundial. "Global Findex Database", estimaciones sobre población mundial sin acceso a servicios bancarios tradicionales (población "unbanked").
- Travala y otras plataformas de comercio electrónico, ejemplos citados de aceptación directa de pagos en bitcoin, y mapas colaborativos de comercios "Bitcoin friendly" mantenidos por la comunidad.
- Banco Mundial. "Remittance Prices Worldwide", informe sobre el coste medio de las remesas internacionales por los canales tradicionales.
- Agencia Tributaria, información general sobre la tributación en el IRPF de las retribuciones salariales percibidas en criptomonedas, citada también en el capítulo 29.

Capítulo 32. Precio, volatilidad e inversión

Este es, probablemente, el bloque de preguntas más buscado por quien se acerca a Bitcoin por primera vez: qué determina su precio, si es una burbuja, y cómo plantearse una inversión con cabeza.

¿Por qué el precio de Bitcoin sube y baja tanto?

La causa de fondo es sencilla: Bitcoin cotiza en un mercado abierto las veinticuatro horas del día, los siete días de la semana (a diferencia de la bolsa tradicional, que cierra por las noches y los fines de semana), con un tamaño de mercado todavía muy inferior al del oro o al de las principales bolsas de valores, como vimos en el capítulo 29. Un mercado de menor tamaño es, casi por definición, más sensible: la misma cantidad de dinero que apenas movería el precio de una acción de una gran empresa puede desplazar de forma notable el precio de Bitcoin, porque hay relativamente menos "profundidad" de compradores y vendedores dispuestos a absorber órdenes grandes sin que el precio se resienta.

A ese factor estructural se suman otros más coyunturales: la enorme influencia de las noticias regulatorias (una decisión de la SEC estadounidense, un cambio de postura de un gobierno importante, la salida de un exchange grande de un mercado como vimos con Binance en la Unión Europea), el efecto de los grandes flujos de entrada y salida de los fondos cotizados (ETF) que analizamos en el bloque de futuro, la actividad de traders que usan apalancamiento y cuyas posiciones se liquidan en cascada durante los movimientos bruscos, y un componente psicológico muy marcado -el ciclo de euforia y pánico que describimos en el capítulo 29 sobre el riesgo psicológico- que amplifica tanto las subidas como las bajadas más de lo que justificarían los fundamentos del activo.

¿Es Bitcoin una burbuja que tarde o temprano explotará?

Es una de las preguntas más recurrentes desde que Bitcoin superó por primera vez el dólar de valor, y la respuesta honesta es que depende de qué se entienda exactamente por "burbuja" y de a qué horizonte temporal te refieras. Bitcoin ha sufrido, a lo largo de su historia, varios desplomes que en su momento muchos analistas describieron como el pinchazo definitivo de una burbuja: caídas de más del ochenta por ciento en 2018 y de nuevo en 2022, tras las cuales, sin embargo, el precio no solo se recuperó sino que alcanzó nuevos máximos históricos en los años siguientes, un patrón que no encaja con la definición clásica de una burbuja financiera -como la de los tulipanes holandeses del siglo XVII o la de las puntocom en el año 2000-, en las que el precio del activo nunca volvió a recuperar sus máximos previos.

Los críticos más serios, como analizamos en detalle en el capítulo 26 a propósito de Warren Buffett y Charlie Munger, no suelen argumentar que Bitcoin sea una "burbuja" en el sentido de una estafa, sino que cuestionan si su valor puede sostenerse a largo plazo al no generar ningún flujo de caja ni beneficio empresarial que justifique objetivamente un precio concreto, a diferencia de una acción o un bono. Los defensores replican que el oro tampoco genera flujo de caja alguno y, sin embargo, nadie lo describe habitualmente como una burbuja, precisamente porque su valor como reserva de escasez verificable ha sido aceptado socialmente durante milenios; el argumento a favor de Bitcoin es que se encuentra en un proceso equivalente, todavía en construcción. Lo que sí es objetivamente cierto, y no depende de ninguna opinión, es que la volatilidad de Bitcoin seguirá siendo alta durante los próximos

años, y que cualquiera que invierta debe estar preparado, como mínimo, para caídas de esa magnitud sin que ello implique necesariamente que el proyecto haya fracasado.

¿Es buena idea invertir mis ahorros en Bitcoin?

Este libro no puede ni debe responder a esa pregunta por ti, porque la respuesta depende enteramente de tu situación financiera personal, tu tolerancia al riesgo y tu horizonte temporal, y porque, como se advierte en el capítulo 29, nada de lo escrito aquí constituye asesoramiento financiero personalizado. Lo que sí puede ofrecerte este libro son los elementos objetivos que cualquier asesor financiero responsable tendría en cuenta antes de darte una recomendación: Bitcoin es un activo de alta volatilidad, sin ningún tipo de garantía de rentabilidad ni de protección de capital, cuyo precio puede caer drásticamente en periodos cortos de tiempo, como detalla en profundidad el capítulo 29 sobre los riesgos de invertir en él.

La expresión "mis ahorros", en concreto, merece una precisión importante: la práctica totalidad de las guías de educación financiera, con independencia del activo del que hablen, distinguen entre el fondo de emergencia -el dinero que necesitas tener disponible y seguro para imprevistos, normalmente equivalente a varios meses de gastos- y el capital que puedes permitirte invertir en activos de riesgo a largo plazo. Destinar el fondo de emergencia a Bitcoin, o cualquier otro activo volátil, es una decisión que la mayoría de los profesionales financieros desaconsejaría, precisamente porque podrías verte obligado a vender en el peor momento posible, justo durante una caída de mercado, para cubrir un gasto imprevisto. Si tras cubrir ese colchón de seguridad decides destinar una parte de tu capital de inversión a largo plazo a Bitcoin, la decisión pasa a ser razonable siempre que sea coherente con tu perfil de riesgo, algo que solo tú -idealmente con el apoyo de un asesor financiero cualificado- puedes valorar.

¿Cuánto dinero mínimo necesito para comprar Bitcoin?

Prácticamente ninguno: a diferencia de comprar un lingote de oro entero o una acción cara de una empresa concreta, Bitcoin es divisible hasta ocho decimales (capítulo 13), y todas las plataformas reguladas que mencionamos en el capítulo 29 permiten comprar fracciones muy pequeñas, a menudo desde cantidades tan reducidas como uno o cinco euros. La unidad más pequeña de Bitcoin, un satoshi (la cienmillonésima parte de un bitcoin, en honor a su creador), ilustra bien esta divisibilidad: no hace falta comprar "un bitcoin entero" para empezar a invertir, del mismo modo que no hace falta comprar una hectárea entera de terreno para poseer una pequeña parcela de un fondo inmobiliario.

Lo que sí conviene tener en cuenta es que, cuanto más pequeño es el importe de cada operación, proporcionalmente más pesan las comisiones fijas que algunas plataformas cobran por transacción, lo que puede hacer que comprar cantidades muy reducidas de forma muy frecuente resulte menos eficiente que agrupar esas compras en importes algo mayores y con menor frecuencia, un equilibrio que conviene sopesar según la estructura de comisiones concreta de la plataforma que elijas (capítulo 29).

¿Es mejor comprar una pequeña cantidad de Bitcoin periódicamente o todo de golpe?

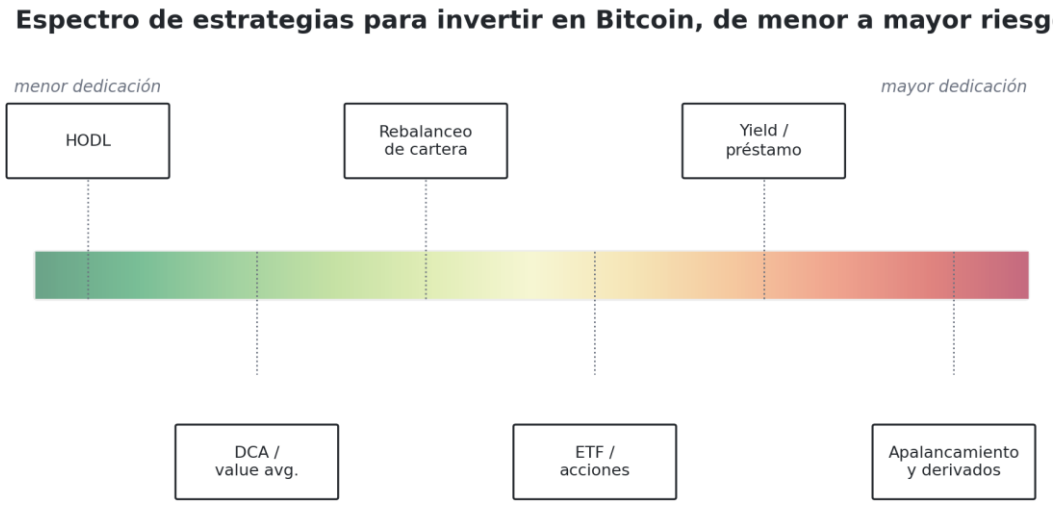
Como explicamos en el capítulo 29 al describir el primer paso práctico para invertir, existen fundamentalmente dos estrategias: invertir todo el capital disponible de una sola vez (lump

sum), o repartirlo en compras periódicas de importe fijo a lo largo del tiempo, una estrategia conocida como promediación del coste o dollar-cost averaging. Desde un punto de vista puramente matemático, si el precio de un activo tiende a subir a largo plazo, invertir todo de golpe cuanto antes suele producir, de media y en retrospectiva, un resultado ligeramente mejor que repartir la inversión, simplemente porque el capital pasa más tiempo expuesto a esa tendencia alcista.

Sin embargo, la promediación periódica tiene una ventaja que no es matemática sino psicológica y práctica, y que resulta especialmente relevante en un activo tan volátil como Bitcoin: reduce drásticamente el riesgo de invertir todo tu capital justo antes de una caída pronunciada -algo que, con la volatilidad descrita en las preguntas anteriores, es perfectamente posible- y, sobre todo, ayuda a evitar la parálisis o el arrepentimiento que muchos inversores primerizos sienten al intentar "acertar el momento perfecto" para entrar, algo que ni siquiera los profesionales consiguen de forma consistente. Para alguien que empieza sin experiencia previa, la mayoría de las guías de educación financiera recomiendan la promediación periódica precisamente por esa razón práctica, aunque matemáticamente pueda no ser la opción óptima en todos los escenarios posibles.

¿Qué diferentes estrategias existen para invertir en Bitcoin?

No existe una única forma "correcta" de invertir en Bitcoin: existen distintos enfoques, con perfiles de riesgo, dedicación y horizonte temporal muy diferentes entre sí, que además no son necesariamente excluyentes -es perfectamente posible combinar varios a la vez-. Repasamos a continuación los más relevantes, de menor a mayor riesgo y complejidad.



Las siete estrategias descritas en esta sección, ordenadas de menor a mayor riesgo y dedicación.

HODL: comprar y mantener a muy largo plazo

La estrategia más extendida entre los inversores particulares de Bitcoin es la conocida como HODL, un término nacido de una errata: en diciembre de 2013, un usuario de un foro de la comunidad escribió un mensaje titulado "I AM HODLING" (en lugar de "holding", manteniendo) en plena caída de precio, explicando que no pensaba vender pese al pánico generalizado; la expresión, con su error incluido, se quedó como término informal de la comunidad y hoy se usa también, de forma humorística, como acrónimo retroactivo de "Hold

On for Dear Life" ("aguanta con todas tus fuerzas"). En esencia, consiste en comprar bitcoin con la intención de mantenerlo durante años -a menudo una década o más- sin vender durante las caídas ni durante las subidas intermedias, apostando por la revalorización a muy largo plazo y aceptando de antemano, como parte del propio plan, las caídas del cincuenta o el setenta por ciento que describimos en el capítulo 29.

La lógica detrás de esta estrategia es tanto financiera como psicológica: financiera, porque como vimos en la pregunta anterior sobre lump sum frente a promediación, cuanto más tiempo permanece invertido un capital en un activo con tendencia alcista de fondo, mayor es estadísticamente la probabilidad de obtener un resultado positivo; psicológica, porque fijar de antemano la decisión de no vender pase lo que pase elimina la necesidad de tomar decisiones bajo presión emocional en plena caída de mercado, que es precisamente el escenario en el que, como detallamos en el riesgo psicológico del capítulo 29, la mayoría de los inversores particulares toma sus peores decisiones. El principal riesgo de esta estrategia es, precisamente, su rigidez: quien aplica un HODL estricto sin ningún tipo de revisión renuncia también a la posibilidad de reducir su exposición si su situación personal, sus objetivos financieros o su valoración del proyecto cambian sustancialmente con el tiempo.

Promediación del coste (dollar-cost averaging) y promediación por valor (value averaging)

Ya hemos descrito en la pregunta anterior la promediación del coste clásica: invertir un importe fijo a intervalos regulares, con independencia del precio de cada momento. Una variante menos conocida, pero usada por inversores algo más sofisticados, es la promediación por valor (value averaging): en lugar de invertir siempre el mismo importe, se fija un objetivo de crecimiento del valor total de la cartera para cada periodo, y se ajusta la aportación en consecuencia -invirtiendo más si el precio ha caído y la cartera vale menos de lo previsto, e invirtiendo menos, o incluso vendiendo una pequeña parte, si el precio ha subido y la cartera ya supera el objetivo-. Es, en la práctica, una forma más disciplinada y sistemática de "comprar más cuando está barato y menos cuando está caro", pero exige más cálculo y seguimiento que la promediación del coste simple, por lo que suele recomendarse solo a quien ya tiene cierta soltura llevando el control de su propia cartera.

Rebalanceo periódico de cartera

Otro enfoque intermedio, muy usado en la gestión de patrimonio tradicional y perfectamente aplicable a Bitcoin, consiste en fijar de antemano qué porcentaje del patrimonio total se quiere mantener en el activo -por ejemplo, un cinco o un diez por ciento- y revisar esa proporción de forma periódica, típicamente una o dos veces al año. Si Bitcoin ha subido mucho y pasa a representar, por ejemplo, un veinte por ciento de la cartera en lugar del diez por ciento previsto, se vende el exceso para volver al objetivo, materializando parte de la ganancia; si ha caído y su peso se ha reducido por debajo del objetivo, se compra algo más para recuperar la proporción fijada. Esta disciplina cumple una función doble: evita la sobreexposición involuntaria que se produce cuando un activo volátil sube mucho y termina pesando más de lo que su titular había decidido asumir originalmente, y evita también el abandono total del activo durante las caídas, al obligar, de forma sistemática y no emocional, a comprar precisamente en los momentos en que el precio está más deprimido.

Trading activo y especulación a corto plazo

En el extremo opuesto al HODL está el trading activo: comprar y vender con frecuencia, en ocasiones varias veces al día, intentando anticipar los movimientos de precio a corto plazo mediante análisis técnico, noticias o patrones de mercado. Es, con diferencia, la estrategia que exige más dedicación, más conocimiento técnico y más tolerancia al riesgo y al estrés, y los datos disponibles sobre el trading a corto plazo en cualquier mercado financiero -no solo en Bitcoin- son consistentes en un punto: la inmensa mayoría de los operadores particulares que practican esta estrategia obtiene, de media y a lo largo del tiempo, peores resultados que si simplemente hubiera mantenido una posición pasiva, debido a la combinación de comisiones acumuladas por operar con frecuencia, errores derivados de los sesgos psicológicos que describimos en el capítulo 29 (comprar en las subidas por FOMO, vender en pánico en las caídas) y la enorme dificultad objetiva de predecir con consistencia los movimientos de un mercado tan volátil. No es una estrategia que este libro recomiende para quien empieza sin experiencia; quien decide practicarla debe hacerlo, como mínimo, con capital que pueda permitirse perder por completo y con una formación específica muy superior a la que ofrece esta introducción general.

Inversión indirecta: ETF, acciones y vehículos corporativos

Para quien prefiere no gestionar directamente la compra y la custodia de bitcoin, existen vías de exposición indirecta a través del sistema financiero tradicional. La más directa son los ETF de Bitcoin al contado que mencionamos en el bloque de futuro, que cotizan en una bolsa de valores convencional y replican el precio del activo. Otra vía, más indirecta todavía, es comprar acciones de empresas que mantienen bitcoin en su balance como parte de su tesorería corporativa, como analizamos con detalle a propósito de Strategy y Michael Saylor en el capítulo 24: en ese caso no inviertes en bitcoin en sí, sino en una empresa cuyo valor de mercado está influido, entre otros factores, por el valor de sus reservas de bitcoin, lo que añade tanto el riesgo específico de esa empresa (su deuda, su gestión, sus otras líneas de negocio) como una volatilidad que, como vimos en el capítulo 24, puede llegar a ser todavía mayor que la del propio bitcoin en episodios de caída de mercado, precisamente por el efecto del apalancamiento financiero de estos vehículos.

Estrategias de rendimiento ("yield") y sus riesgos

Existen plataformas que ofrecen un interés periódico a cambio de depositar tu bitcoin y prestarlo a terceros, en un producto que se presenta al usuario de forma muy similar a un depósito bancario remunerado. Conviene abordar esta estrategia con una cautela mucho mayor que las anteriores: fue precisamente este tipo de producto el que provocó algunas de las mayores pérdidas de inversores particulares en la historia reciente del sector cripto. Las plataformas Celsius Network y BlockFi, ambas quebradas en 2022 tras prometer rendimientos de este tipo, resultaron incapaces de devolver los fondos depositados por cientos de miles de usuarios, en buena parte porque habían invertido esos depósitos en operaciones de riesgo mucho mayor del que comunicaban públicamente para poder sostener los intereses ofrecidos. Cualquier oferta de rentabilidad fija y aparentemente segura a cambio de depositar tus bitcoins en manos de un tercero debe analizarse con el mismo escepticismo que cualquier otra promesa de rentabilidad elevada que mencionamos en el capítulo 18, precisamente porque, al ceder la custodia, se reintroduce exactamente el riesgo de contraparte que la

autocustodia (capítulo 10) está pensada para eliminar: si la plataforma quiebra o gestiona mal esos fondos, tu bitcoin puede perderse igual que ocurrió con los clientes de Celsius y BlockFi, con independencia de lo sólida que pareciera la plataforma en el momento de depositar.

Productos apalancados y derivados: la estrategia de mayor riesgo

Por último, conviene mencionar la existencia de productos con apalancamiento (futuros, contratos por diferencia o CFD, y préstamos para comprar más bitcoin del que tu capital permitiría directamente), que multiplican tanto las ganancias como las pérdidas potenciales de cualquier movimiento de precio. Se trata, con diferencia, de la estrategia de mayor riesgo de todas las mencionadas en esta pregunta: en un activo ya de por sí tan volátil como Bitcoin, el apalancamiento puede provocar la pérdida de la totalidad del capital invertido -y en algunos productos, incluso una deuda adicional- en cuestión de horas ante un movimiento de precio que, sin apalancamiento, habría sido perfectamente asumible. La inmensa mayoría de las guías de educación financiera, con independencia del activo del que hablen, coinciden en que este tipo de productos son adecuados, como mucho, para operadores profesionales con una formación y una gestión del riesgo muy específicas, y no para un inversor particular que empieza, por lo que este libro se limita a señalar su existencia y su nivel de riesgo, sin entrar en más detalle sobre su funcionamiento.

Préstamos garantizados por bitcoin: obtener liquidez sin vender

Una estrategia distinta, cada vez más popular entre quienes ya tienen una posición consolidada en Bitcoin y desean obtener liquidez sin desprenderse de ella, consiste en pedir un préstamo en euros o dólares usando el propio bitcoin como garantía (colateral), en plataformas especializadas como Ledn, Strike o, en el ámbito bancario tradicional, entidades que ya ofrecen productos similares para otros activos. El mecanismo es sencillo: depositas una cantidad de bitcoin en la plataforma, que la retiene como garantía, y recibes a cambio un préstamo en moneda fiat por un porcentaje de su valor -normalmente entre el 30% y el 50%, lo que se conoce como ratio préstamo-valor o LTV-, con un interés anual que a mediados de 2026 se sitúa, según la plataforma y el importe, aproximadamente entre el 9% y el 14%. Si el precio de Bitcoin cae de forma pronunciada y el valor de la garantía se acerca demasiado al importe prestado, la plataforma puede exigir una garantía adicional o, en último término, liquidar parte del bitcoin depositado para cubrir el préstamo, un riesgo que conviene entender bien antes de contratar este tipo de producto.

La ventaja principal de esta estrategia, frente a simplemente vender una parte de tu bitcoin para obtener liquidez, es doble: por un lado, mantienes la exposición al precio de Bitcoin sobre la totalidad de tus tenencias, incluida la parte usada como garantía, de modo que si el precio sube durante la vida del préstamo sigues beneficiándote de esa subida igual que si no hubieras pedido el préstamo; por otro lado, y esto es lo que más ha impulsado el crecimiento de este mercado -que alcanzó unos 73.600 millones de dólares en préstamos garantizados con criptoactivos a finales de 2025, según datos de la industria-, pedir un préstamo no suele generar, a diferencia de una venta, un hecho fiscal inmediato en la mayoría de las jurisdicciones: no estás vendiendo el activo ni materializando una ganancia patrimonial, por lo que normalmente no tienes que tributar por él en el momento de recibir el préstamo, aunque conviene confirmar siempre el tratamiento fiscal exacto con un asesor, porque puede variar según el país y según si el préstamo termina en una liquidación forzosa. Conviene subrayar, de nuevo, que esta estrategia reintroduce un riesgo de contraparte -la plataforma que

gestiona el préstamo y custodia la garantía- similar al que describimos a propósito de las estrategias de rendimiento, por lo que la elección de una plataforma solvente y transparente sobre cómo gestiona los depósitos de sus clientes es una decisión al menos tan importante como las condiciones económicas del propio préstamo.

Resumen comparativo de las estrategias

La siguiente tabla reúne, a modo de resumen visual, el perfil de riesgo, la dedicación necesaria y el horizonte temporal habitual de cada una de las estrategias descritas en esta sección, para facilitar una comparación rápida entre ellas.

Estrategia	Nivel de riesgo	Dedicación requerida	Horizonte temporal típico	Genera hecho fiscal
HODL (comprar y mantener)	Moderado (volatilidad de mercado, sin apalancamiento)	Muy baja, una vez tomada la decisión inicial	Largo plazo (años)	Solo al vender
Promediación del coste (DCA)	Moderado, algo menor que la compra única por la diversificación temporal	Baja, requiere automatizar aportaciones periódicas	Largo plazo (años)	Solo al vender
Promediación por valor	Moderado	Media, exige cálculo y seguimiento periódico	Largo plazo (años)	Al vender la parte que exceda el objetivo
Rebalanceo periódico	Moderado, reduce la sobreexposición	Media, revisión una o dos veces al año	Largo plazo (años)	Sí, cada vez que se vende para rebalancear
Trading activo	Muy alto	Muy alta, seguimiento diario o intradía	Corto plazo (días u horas)	Sí, en cada operación con ganancia
Inversión indirecta (ETF, acciones)	Moderado a alto, según el vehículo	Muy baja	Variable, desde corto a largo plazo	Sí, según fiscalidad de productos financieros
Estrategias de rendimiento (yield)	Alto (riesgo de contraparte y de plataforma)	Baja	Corto a medio plazo	Sí, el interés percibido tributa como rendimiento
Productos apalancados y derivados	Muy alto (riesgo de pérdida total)	Alta, requiere gestión activa del riesgo	Muy corto plazo	Sí, en cada liquidación
Préstamos garantizados por bitcoin	Alto (riesgo de contraparte y de liquidación forzosa)	Baja una vez contratado	Corto a medio plazo (duración del préstamo)	Normalmente no, salvo liquidación

Como puede verse en la tabla, no hay ninguna estrategia sin riesgo, y el riesgo no siempre está donde parece a primera vista: incluso las estrategias más pasivas, como el HODL, están plenamente expuestas a la volatilidad de mercado descrita en este bloque, mientras que otras, como los préstamos garantizados, reducen el riesgo de mercado inmediato pero introducen un riesgo de contraparte y de liquidación que un simple HODL sin préstamo no

tiene. Elegir entre ellas, o combinar varias, depende por completo del perfil de riesgo, el horizonte temporal y los conocimientos de cada persona, tal y como recordábamos al principio de esta sección.

¿Qué ventajas tiene invertir en Bitcoin frente a tener el dinero en el banco?

La comparación más honesta no es tanto entre Bitcoin y "el banco" como institución -que sigue prestando servicios que Bitcoin no puede sustituir, como veremos al final de esta pregunta- sino entre Bitcoin y el efectivo o los depósitos bancarios como forma concreta de conservar el ahorro. Analizamos a continuación, una por una, las ventajas que con más frecuencia se citan a favor de Bitcoin en esta comparación.

Bitcoin en autocustodia frente a un depósito bancario tradicional

	DEPÓSITO BANCARIO	BITCOIN (AUTOCUSTODIA)
Protección frente a inflación	Depende del tipo de interés	Oferta fija de 21M (cap. 13)
Riesgo de contraparte	Sí, mitigado hasta 100.000€ (FGD)	Ninguno si hay autocustodia
Disponibilidad	Horario bancario, festivos	24/7, cualquier país
Bloqueo administrativo	Posible (embargo, orden judicial)	No hay intermediario que bloquear
Estabilidad de valor	Alta a corto plazo	Alta volatilidad (cap. 29)
Servicios asociados	Nóminas, tarjetas, préstamos	No ofrece estos servicios

Bitcoin en autocustodia frente a un depósito bancario tradicional, punto por punto.

Protección frente a la inflación y la pérdida de poder adquisitivo

El dinero depositado en una cuenta bancaria tradicional en euros pierde valor real cada año en la medida en que la inflación supera el interés que el banco paga por tenerlo allí, un fenómeno que ha sido la norma casi constante en la última década en la eurozona: los tipos de interés de las cuentas corrientes y de ahorro ordinarias han permanecido, la mayor parte del tiempo, muy por debajo de la inflación oficial, lo que significa que, en términos de lo que ese dinero puede comprar realmente, un ahorrador que mantuvo su capital solo en una cuenta corriente durante esos años perdió poder adquisitivo de forma silenciosa, aunque el número que veía en su saldo bancario nunca disminuyera. Este fenómeno, que los economistas llaman represión financiera cuando los tipos de interés se mantienen deliberadamente por debajo de la inflación durante periodos prolongados, es precisamente el tipo de erosión del ahorro que motivó, como vimos en el capítulo 4, buena parte del interés inicial por Bitcoin tras la crisis de 2008 y las políticas de expansión monetaria que la siguieron. Bitcoin, con la oferta fija de 21 millones de unidades que describimos en el capítulo 13, ofrece a quien lo posee una alternativa cuya oferta no puede diluirse por decisión de ningún banco central, un

argumento que sus defensores presentan como una forma de proteger el ahorro a largo plazo frente a ese fenómeno, aunque conviene recordar, una vez más, que esa protección no es automática ni está garantizada a corto plazo, precisamente por la volatilidad descrita a lo largo de todo este bloque.

Ausencia de riesgo de contraparte con autocustodia

El dinero de un depósito bancario no es, técnicamente, "tuyo" en el sentido estricto mientras está en el banco, sino un derecho de cobro frente a esa entidad: el banco presta y utiliza ese dinero en su propia operativa, y tu saldo es, en realidad, una deuda que el banco tiene contigo. En España y en el resto de la Unión Europea, ese derecho está protegido por el Fondo de Garantía de Depósitos hasta un máximo de 100.000 euros por titular y entidad; por encima de ese límite, o en el caso de que un banco entrase en un proceso de resolución, el ahorrador podría verse afectado. El precedente más citado en Europa es el rescate bancario de Chipre en 2013, en el que, por primera vez en la eurozona, una parte de los depósitos no garantizados de los principales bancos del país -por encima del límite protegido- fue directamente utilizada para recapitalizar esas mismas entidades, en lo que se conoció como un "corralito" o "bail-in" bancario, un mecanismo que desde entonces forma parte del marco legal ordinario de resolución bancaria en toda la Unión Europea. Un bitcoin guardado correctamente en una wallet propia mediante autocustodia (capítulo 10) no depende de la solvencia de ningún banco ni de ningún fondo de garantía con un límite máximo: sigue siendo tuyo con independencia de lo que le ocurra a cualquier entidad financiera, precisamente la propiedad que analizamos en el capítulo 27 a propósito de la libertad financiera individual. Esta ventaja, conviene subrayarlo, depende por completo de que el usuario practique realmente la autocustodia: mantener el bitcoin en la cuenta de un exchange reintroduce un riesgo de contraparte distinto, pero no menos real, como vimos con los casos de Mt. Gox y FTX en el capítulo 18.

Disponibilidad, portabilidad y acceso permanente

Una cuenta bancaria está sujeta a horarios de operativa, días festivos, límites diarios o mensuales de transferencia, y a la posibilidad, aunque excepcional en circunstancias normales, de que una cuenta sea bloqueada por una decisión administrativa o judicial, o de que un país imponga restricciones temporales a la salida de capitales en un episodio de crisis, como ocurrió en Grecia en 2015 con el llamado "corralito griego", que limitó durante meses la cantidad de dinero que los ciudadanos podían retirar de sus propias cuentas, o de forma mucho más prolongada en Argentina con el histórico "cepo cambiario" que ha restringido, en distintos periodos desde 2011, el acceso de los ciudadanos argentinos a divisas extranjeras. Bitcoin, como vimos en el bloque de uso diario, puede moverse a cualquier hora, cualquier día del año, a cualquier parte del mundo, sin necesidad de autorización de ningún intermediario y sin que ningún gobierno pueda imponer, de forma técnica, un límite a cuánto puedes mover de tu propia wallet, aunque sí pueda, como analizamos en el bloque de legalidad, restringir el acceso a las plataformas que facilitan convertirlo a moneda local.

Independencia frente a decisiones administrativas

Relacionado con el punto anterior, pero distinto de él, está la independencia frente a decisiones administrativas dirigidas específicamente contra una persona o una cuenta concreta, no contra el sistema financiero en su conjunto: un tribunal, una agencia

gubernamental o el propio banco pueden, en determinadas circunstancias legales, embargar o congelar una cuenta bancaria individual. Bitcoin guardado en autocustodia no puede congelarse de la misma manera, porque no existe ninguna entidad intermedia a la que una orden de este tipo pueda dirigirse: como explicamos en el capítulo 27, esta característica es, para muchos defensores de Bitcoin, una de sus propiedades más valiosas, aunque también es, para sus críticos, una de las razones por las que resulta más difícil de regular y más atractivo para quien busca evadir obligaciones legítimas, un debate que ya abordamos con más detalle en el capítulo 33 a propósito de la privacidad financiera.

Por qué el banco sigue siendo imprescindible: lo que Bitcoin no puede ofrecer

Frente a todas estas ventajas hay que sopesar, con la misma honestidad, lo que un banco ofrece y Bitcoin no. La estabilidad nominal de un depósito bancario no tiene parangón con la volatilidad de Bitcoin descrita a lo largo de todo este bloque: el dinero que necesitas disponible para tus gastos del mes que viene, o para tu fondo de emergencia (pregunta anterior sobre invertir los ahorros), debe estar en un instrumento estable y de acceso inmediato, no en un activo que puede valer un veinte por ciento menos la semana siguiente. El banco ofrece además servicios que Bitcoin no sustituye: domiciliación de recibos, nóminas, tarjetas aceptadas de forma universal en cualquier comercio físico, financiación mediante préstamos e hipotecas, y la garantía, hasta 100.000 euros, del Fondo de Garantía de Depósitos, una protección que, dentro de su límite, no tiene equivalente automático en la autocustodia de Bitcoin: si pierdes tu frase semilla (capítulo 19), no existe ningún fondo que te reembolse.

En definitiva: no es sustituir, es complementar

La conclusión más razonable, repetida ya varias veces a lo largo de este libro, no es sustituir una cosa por la otra, sino entender que el banco y Bitcoin cumplen funciones distintas y, para la mayoría de las personas, complementarias. El banco sigue siendo, y previsiblemente seguirá siendo durante mucho tiempo, la herramienta correcta para el dinero que necesitas disponible y estable a corto plazo, y para los servicios financieros cotidianos que Bitcoin no ofrece. Bitcoin, para quien decide destinarle una parte de su patrimonio con las precauciones descritas en el capítulo 29, se plantea como un complemento de ahorro a más largo plazo, con un perfil de riesgo, de independencia y de propiedades completamente distinto al de un depósito bancario, no como un sustituto integral de él.

¿Qué diferencia hay entre invertir en Bitcoin directamente y hacerlo a través de un ETF o producto financiero?

Un ETF de Bitcoin al contado (spot), como los que mencionamos en el bloque de futuro a propósito de BlackRock, es un producto financiero que cotiza en una bolsa de valores tradicional y que replica el precio de Bitcoin comprando y custodiando el activo real en nombre de los inversores del fondo. La diferencia clave frente a comprar Bitcoin directamente en un exchange es la custodia: al invertir en un ETF, no posees bitcoins que puedas retirar a tu propia wallet (capítulo 10), sino participaciones de un fondo que, a su vez, sí posee esos bitcoins; renuncias, por tanto, a la autocustodia que analizamos en el capítulo 29, a cambio de la comodidad de invertir a través de tu bróker o cuenta de valores habitual, con la misma sencillez operativa que comprarías una acción, y sujeto a la regulación de los mercados de valores tradicionales en lugar de a la regulación específica de criptoactivos.

Para muchos inversores institucionales y para quienes ya operan dentro del sistema financiero tradicional, esta comodidad y este marco regulatorio conocido son una ventaja decisiva, y explica buena parte del éxito de estos productos desde su aprobación. Para quienes dan más valor a los principios de autocustodia y descentralización que motivaron la creación de Bitcoin (capítulo 27), invertir a través de un ETF supone reintroducir precisamente el tipo de intermediario de confianza -el gestor del fondo, el custodio del activo subyacente- que Bitcoin fue diseñado para evitar, aunque sea un intermediario mucho más regulado y transparente que un banco tradicional.

¿Cómo se determina el valor de Bitcoin, quién decide el precio?

A diferencia de una moneda fiduciaria, cuyo valor puede verse influido por la política de un banco central, o de una acción, cuyo precio está ligado a los beneficios y las perspectivas de una empresa concreta, el precio de Bitcoin no lo decide ninguna persona ni institución: se determina exclusivamente por la oferta y la demanda en los mercados donde se negocia, minuto a minuto, en todo el mundo. Cuando hay más compradores dispuestos a pagar un precio que vendedores dispuestos a aceptarlo, el precio sube; cuando ocurre lo contrario, baja, exactamente el mismo mecanismo básico que determina el precio de cualquier materia prima cotizada en un mercado libre.

Lo que sí influye en esa oferta y demanda son múltiples factores que ya hemos ido mencionando: la escasez programada y decreciente de nuevas unidades (capítulo 13), las noticias regulatorias, los flujos de los grandes fondos institucionales, la percepción de Bitcoin como refugio en momentos de inestabilidad económica o, por el contrario, como activo de riesgo del que se huye en esos mismos momentos -su comportamiento no siempre es consistente en este sentido-, y el sentimiento general del mercado, que en un activo todavía joven y sin el consenso social del oro pesa proporcionalmente más que en activos más maduros.

¿Puede llegar un día en que Bitcoin valga cero?

No puede descartarse por completo, y cualquier análisis honesto debe reconocerlo: ningún activo financiero, por consolidado que esté, tiene una garantía absoluta de valor futuro, y Bitcoin, al ser relativamente joven y depender en última instancia de que un número suficiente de personas siga confiando en él y usándolo, no es una excepción. Los escenarios que con más frecuencia se citan como capaces de llevar su valor a cero -o cerca de cero- incluyen una prohibición coordinada y efectiva por parte de las principales economías del mundo (algo que ni siquiera China, con la prohibición más severa hasta la fecha, ha conseguido de forma global, como vimos en el capítulo 24), el descubrimiento de una vulnerabilidad crítica e irreparable en el propio protocolo (capítulo 20), o una pérdida generalizada y simultánea de confianza que llevara a la práctica totalidad de sus usuarios a abandonarlo a la vez.

Frente a esos escenarios, conviene señalar también los factores que juegan en sentido contrario: la descentralización de la red hace mucho más difícil una prohibición global efectiva que la de un producto o empresa centralizada; el protocolo lleva más de quince años funcionando sin haber sido comprometido con éxito (capítulo 15); y la base de usuarios, desarrolladores, empresas e inversores institucionales que sostienen a Bitcoin hoy es órdenes de magnitud mayor y más diversa que en sus primeros años, lo que reduce -sin eliminarlo del todo- el riesgo de un colapso repentino por falta de interés. Ninguna de estas

dos observaciones debe leerse como una predicción: la conclusión más honesta es que se trata de un riesgo real, aunque de probabilidad decreciente con el tiempo, y que cualquier decisión de inversión debe tenerlo en cuenta.

Fuentes y estudios citados en este capítulo

- Buffett, W. y Munger, C., declaraciones públicas y cartas a accionistas de Berkshire Hathaway sobre Bitcoin, citadas también en el capítulo 26.
- Datos históricos de precio y capitalización de mercado de Bitcoin, incluidas las caídas de 2018 y 2022 y su posterior recuperación, recogidos por observatorios de mercado como CoinMarketCap y CoinGecko.
- Estudios de finanzas conductuales (behavioral finance) sobre las estrategias de promediación del coste (dollar-cost averaging) frente a la inversión de una sola vez (lump sum investing).
- U.S. Securities and Exchange Commission (SEC). Documentación y comunicados sobre la aprobación de los ETF de Bitcoin al contado en Estados Unidos.
- Fondo de Garantía de Depósitos de Entidades de Crédito (FGD), España, sobre el límite de cobertura de 100.000 euros por titular y entidad.
- Cobertura periodística y documentación judicial sobre la quiebra de las plataformas de préstamo de criptoactivos Celsius Network y BlockFi en 2022.
- Estudios académicos y de la industria financiera sobre el rendimiento comparado del trading activo frente a la inversión pasiva a largo plazo en mercados de alta volatilidad.
- Eurogrupo y Banco Central Europeo, documentación oficial sobre el rescate bancario de Chipre de 2013 y el mecanismo de "bail-in" en la resolución bancaria europea.
- Banco de Grecia y cobertura periodística sobre los controles de capital impuestos en Grecia en 2015, y el "cepo cambiario" vigente de forma intermitente en Argentina desde 2011.
- Foro Bitcointalk, mensaje original "I AM HODLING" (diciembre de 2013), origen documentado del término HODL.
- Ledn, "Best Bitcoin-Backed Loan Rates" (2026); Strike, "Best Bitcoin-Backed Lenders in the US" (2026); Memeburn, "Bitcoin Lending Just Hit $67 Billion" (2026), sobre el mercado de préstamos garantizados con bitcoin y su tratamiento fiscal.

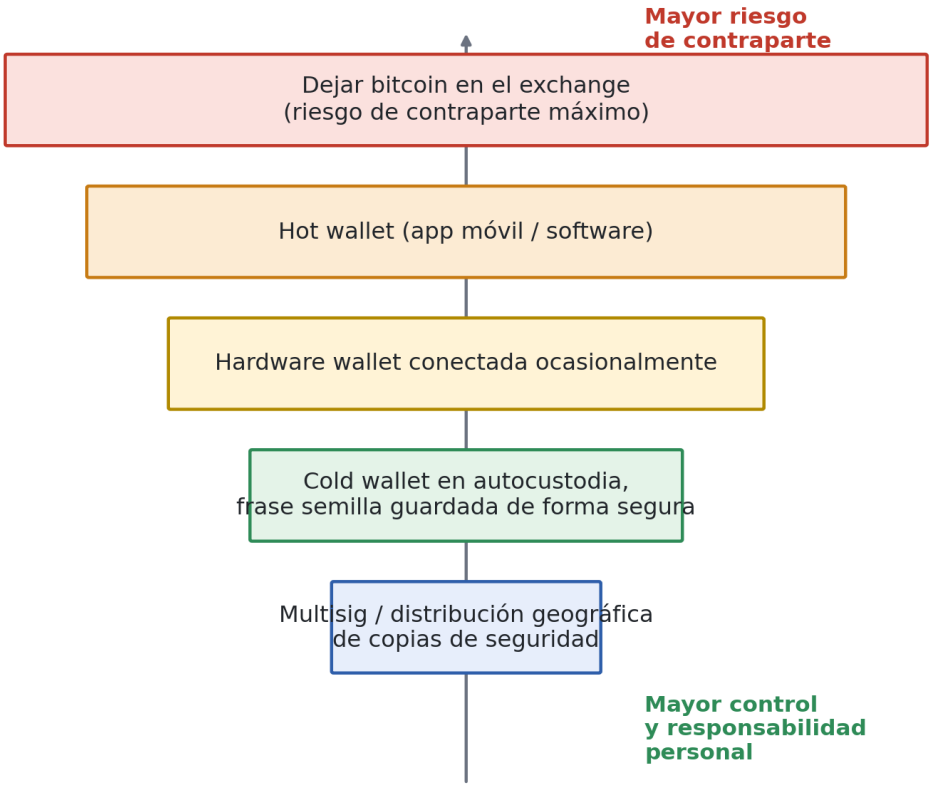
Capítulo 33. Seguridad y riesgos

Bitcoin tiene fama, en parte merecida y en parte exagerada, de ser un terreno peligroso para quien no sabe lo que hace. Este bloque repasa, en formato de preguntas concretas, los riesgos de seguridad más habituales que ya analizamos con detalle en capítulos anteriores.

¿Es seguro usar Bitcoin o me pueden robar fácilmente?

El protocolo de Bitcoin en sí mismo es extraordinariamente seguro: como explicamos en el capítulo 15, su mecanismo criptográfico no ha sido comprometido con éxito en más de quince años de funcionamiento, y forzar la red mediante un ataque directo requeriría una cantidad de potencia de cálculo que ningún actor conocido posee ni podría financiar de forma realista. Dicho esto, "usar Bitcoin de forma segura" no depende solo de la seguridad del protocolo, sino, sobre todo, de las decisiones del propio usuario, y es en ese terreno donde ocurre la inmensa mayoría de los robos y pérdidas que has podido leer en las noticias.

La gran mayoría de los robos de bitcoin no son ataques al protocolo, sino ataques a las personas o a las plataformas donde guardan sus fondos: el phishing (mensajes o webs falsas que imitan a un exchange real para robar tus credenciales), el malware que sustituye direcciones copiadas al portapapeles, la ingeniería social que convence a la víctima de entregar voluntariamente su frase semilla, o el hackeo de un exchange centralizado que gestiona mal su propia seguridad, como analizamos en detalle en el capítulo 18. Usar Bitcoin con las precauciones adecuadas -verificar siempre las direcciones, desconfiar de cualquier oferta que suene demasiado buena, usar autenticación de dos factores, y considerar la autocustodia en una wallet propia para cantidades significativas (capítulo 10)- reduce drásticamente ese riesgo, aunque, como con cualquier activo digital, nunca lo elimina del todo.



Pirámide de seguridad: del exchange a la autocustodia

Cuanto más autocustodiado y distribuido, mayor control personal pero también mayor responsabilidad.

¿Qué pasa si pierdo la contraseña o las "llaves" de mi billetera de Bitcoin?

Si pierdes el acceso a tu wallet -por ejemplo, olvidando la contraseña de un dispositivo o perdiendo el propio dispositivo- pero conservas tu frase semilla (las doce o veinticuatro palabras que se generan al crear la wallet, descritas en el capítulo 10), puedes recuperar el acceso completo a tus fondos instalando cualquier wallet compatible e introduciendo esa frase, sin perder ni un solo satoshi. La frase semilla es, precisamente, la copia de seguridad definitiva pensada para este escenario, y por eso todo el capítulo 25 del libro está dedicado a explicar cómo custodiarla correctamente.

El escenario verdaderamente irreversible es perder tanto el acceso a la wallet como la propia frase semilla: en ese caso, como detallamos en el capítulo 19, no existe ningún banco, empresa ni "servicio de atención al cliente" al que acudir para recuperar tus fondos, porque nadie más que tú -mediante esa frase- tiene la capacidad matemática de demostrar la propiedad de esos bitcoins. Se estima que varios millones de bitcoins, un porcentaje significativo del total que llegará a existir, están perdidos de forma permanente exactamente por este motivo, congelados para siempre en direcciones a las que nadie podrá volver a acceder. Es la razón por la que este libro insiste, en varios capítulos, en que proteger correctamente la frase semilla desde el primer día es, con diferencia, el paso de seguridad más importante de todos.

¿Me pueden hackear la cuenta y dejarme sin mis Bitcoins?

Depende, sobre todo, de dónde guardes tus fondos. Si los mantienes en la cuenta de un exchange, tu situación de seguridad depende en gran medida de las medidas que esa empresa haya implementado: un fallo en su infraestructura, un empleado malicioso o una vulnerabilidad no detectada podrían, en teoría, comprometer tus fondos igual que ocurrió en los casos históricos de Mt. Gox o FTX (capítulo 18), aunque las plataformas reguladas bajo MiCA que operan hoy en España (capítulo 29) están sujetas a exigencias de seguridad y de segregación de fondos de clientes considerablemente más estrictas que las que existían en aquellos casos.

Si mantienes tus fondos en una wallet propia, especialmente en un monedero hardware desconectado de internet (capítulo 10), el vector de ataque cambia por completo: ya no depende de la seguridad de una empresa externa, sino de que un atacante consiga acceso físico a tu dispositivo y, además, conozca o extraiga tu PIN o tu frase semilla, un escenario mucho más improbable para un usuario que sigue las prácticas de seguridad básicas que para quien deja sus claves en un archivo de texto sin cifrar en su ordenador, un error sorprendentemente común que analizamos en el capítulo 19. En resumen: sí, existe el riesgo de que te hackeen, pero ese riesgo depende en gran medida de decisiones que están bajo tu control, no de una fatalidad inherente al hecho de poseer bitcoin.

¿Qué riesgos principales tiene invertir o usar Bitcoin para alguien sin muchos conocimientos técnicos?

El capítulo 29 de este libro dedica una sección completa a enumerar en detalle los ocho grandes riesgos de invertir en Bitcoin -de mercado, regulatorio, de custodia, tecnológico, de liquidez, fiscal, de productos apalancados y psicológico-, y remitimos allí para una explicación exhaustiva de cada uno. Para alguien sin conocimientos técnicos previos, en concreto, los riesgos que con más frecuencia causan pérdidas reales no son los más sofisticados, sino los más básicos: comprar en una plataforma sin verificar que esté correctamente regulada, no entender que perder la frase semilla equivale a perder los fondos para siempre, caer en ofertas fraudulentas de rentabilidad garantizada (bloque siguiente), o invertir bajo la presión emocional de una subida rápida de precio sin haber definido antes cuánto se está dispuesto a arriesgar.

La buena noticia es que ninguno de estos riesgos requiere conocimientos técnicos avanzados para gestionarse correctamente: exige, sobre todo, informarse antes de actuar -algo que este propio libro pretende facilitar-, elegir plataformas reguladas, proteger la frase semilla con el mismo cuidado que las llaves de casa, y aplicar el sentido común financiero básico de no invertir más de lo que se puede permitir perder, un principio que vale exactamente igual para Bitcoin que para cualquier otro activo de riesgo.

¿Qué es una estafa tipo "pump and dump" y cómo me puede afectar en Bitcoin?

Un "pump and dump" (literalmente, "inflar y descargar") es un esquema en el que un grupo de personas, a menudo coordinadas en foros o canales privados, compra de forma simultánea una criptomoneda de bajo volumen y capitalización reducida para hacer subir artificialmente su precio de forma rápida y llamativa, atrayendo después a inversores externos que, viendo la subida, compran también por miedo a quedarse fuera (el FOMO que mencionamos en el capítulo 29). Una vez que el precio ha subido lo suficiente, los

organizadores originales venden de golpe sus posiciones ("dump"), provocando un desplome repentino que deja a los inversores que entraron tarde con pérdidas muy significativas, mientras los organizadores se embolsan la diferencia.

Este tipo de esquema es mucho más habitual, y mucho más dañino, en criptomonedas pequeñas y poco líquidas -con frecuencia proyectos sin ningún desarrollo real detrás, creados específicamente para este propósito- que en Bitcoin, cuya enorme capitalización de mercado y liquidez, descritas en el capítulo 29, hacen extraordinariamente difícil y costoso que un grupo de actores manipule su precio de esta manera de forma sostenida. Aun así, conviene conocer las señales de alarma: subidas de precio repentinas y sin ninguna noticia que las justifique, promoción agresiva en redes sociales por parte de cuentas con poco historial, y promesas de rentabilidad garantizada en un plazo muy corto, exactamente el mismo patrón que ya describimos, a mayor escala, en los casos de fraude reales analizados en el capítulo 26.

Un ejemplo instructivo de la escala que estos esquemas pueden alcanzar, incluso fuera del universo de las criptomonedas de nicho, es la fiebre de las "memecoins" que se disparó durante 2024 y 2025: tokens creados en cuestión de minutos, sin ningún propósito ni desarrollo tecnológico real detrás, cuyo único valor proviene de una broma, una referencia cultural viral o el simple efecto de "quedarse fuera" que ya mencionamos. Plataformas como Pump.fun, construidas específicamente para lanzar este tipo de tokens de forma instantánea sobre la red de otra criptomoneda (Solana), permitieron la creación de varios millones de tokens de este tipo en apenas un año, la inmensa mayoría de los cuales perdió la práctica totalidad de su valor en cuestión de horas o días tras un pico inicial de compras especulativas. Este fenómeno, aunque técnicamente distinto de Bitcoin en casi todos los aspectos relevantes -Bitcoin no permite crear tokens nuevos sobre su cadena principal con la misma facilidad, y no tiene un equipo ni una empresa central que pueda "lanzar" nada nuevo de la noche a la mañana-, contribuye de forma indirecta a la confusión pública que mencionamos al principio de este capítulo: muchos titulares de prensa y muchas conversaciones cotidianas no distinguen con precisión entre "Bitcoin", "las criptomonedas en general" y "las memecoins específicamente", lo que traslada a Bitcoin una parte de la reputación de volatilidad extrema y riesgo de estafa que, en realidad, corresponde de forma mucho más directa a este segmento concreto y mucho más especulativo del mercado.

¿Hasta qué punto las operaciones con Bitcoin son anónimas, me pueden rastrear?

Es una de las confusiones más extendidas sobre Bitcoin, y la respuesta técnica es que es pseudónimo, no anónimo, tal como explicamos en el capítulo 9. Cada transacción queda registrada de forma permanente y pública en la cadena de bloques, visible para cualquiera que quiera consultarla, pero identificada únicamente por una dirección alfanumérica, no por el nombre real del titular. Mientras nadie vincule esa dirección con tu identidad, tu actividad parece anónima; en el momento en que esa vinculación se produce -por ejemplo, al comprar bitcoin en un exchange regulado que exige verificación de identidad (KYC), como detallamos en el capítulo 29-, todo tu historial de transacciones asociado a esa dirección queda, en la práctica, tan trazable como el de una cuenta bancaria.

De hecho, existen empresas especializadas de análisis de cadena de bloques (chain analysis) que trabajan habitualmente con cuerpos policiales y agencias tributarias de todo el mundo, y

que han demostrado en numerosos casos judiciales su capacidad de rastrear el movimiento de fondos a través de la cadena de bloques con un nivel de detalle considerable, precisamente porque el registro es público y permanente, no se puede borrar. Quien busca un anonimato real, no simplemente pseudonimato, recurre a otras criptomonedas diseñadas específicamente para ello (como Monero) o a técnicas adicionales de ofuscación, pero conviene saber que el uso de esas técnicas para evadir obligaciones fiscales o legales es, en la mayoría de las jurisdicciones, ilegal, con independencia de la tecnología que se use para intentarlo.

¿Por qué importa la privacidad financiera, y por qué algunos negocios usan Bitcoin para no revelar cierta información?

La privacidad financiera -el derecho a que tus movimientos de dinero no sean visibles para cualquiera que quiera consultarlos- no es, en sí misma, una idea sospechosa: es el mismo principio por el que tu banco no publica tu saldo en internet, por el que una empresa no revela a sus competidores el importe exacto que paga a cada proveedor, o por el que la mayoría de la gente preferiría que su vecino no conociera su nómina. Como explicamos en el capítulo 27 a propósito de la vigilancia financiera y la libertad individual, para muchos defensores de Bitcoin esta privacidad no es un lujo, sino una condición básica de la libertad económica, en la línea de lo que ya en los años noventa defendía el movimiento cypherpunk que mencionamos en el capítulo 4: la idea de que la privacidad, incluida la financiera, es algo que hay que proteger activamente, no algo que se pierde automáticamente por el simple hecho de participar en la economía moderna.

En el terreno empresarial, existen razones legítimas y ampliamente reconocidas para que un negocio prefiera no exponer determinada información financiera de forma pública: proteger el importe de sus operaciones frente a competidores directos, evitar que proveedores o clientes conozcan las condiciones que ha negociado con otros, reducir el riesgo de ser objetivo de extorsión, secuestro o robo en contextos o países donde la ostentación de patrimonio conocido supone un riesgo real de seguridad física, o simplemente mantener la discreción habitual con la que cualquier empresa gestiona su información contable frente al público general, algo que ningún negocio tradicional considera una anomalía cuando lo hace mediante los mecanismos legales ordinarios (cuentas bancarias privadas, acuerdos de confidencialidad, sociedades no cotizadas). Bitcoin, con el pseudonimato descrito en la pregunta anterior, ofrece a estos negocios un grado de opacidad frente al público general -no frente a las autoridades- comparable, en cierto modo, al que ya ofrece una transferencia bancaria privada o un pago en efectivo de importe elevado.

Aquí conviene una distinción que este libro ha repetido en varios capítulos y que merece subrayarse una vez más: hay una diferencia legal y ética enorme entre no exponer tu información financiera al público -algo legítimo- y ocultarla de las autoridades fiscales o reguladoras para evadir tus obligaciones -algo ilegal, con independencia de si se hace con bitcoin, con efectivo, con sociedades opacas o con cualquier otro instrumento-. Como se detalla en la pregunta anterior y en el capítulo 34, cualquier plataforma regulada bajo MiCA exige verificación de identidad (KYC) y coopera con las autoridades tributarias, y las empresas de análisis de cadena de bloques han demostrado en numerosos casos judiciales que el uso de Bitcoin para lavado de dinero o evasión fiscal deja un rastro que, tarde o temprano, resulta localizable, como muestran los propios casos de fraude analizados en el capítulo 26. Los negocios legítimos que valoran su privacidad financiera operan, casi siempre,

dentro de plataformas reguladas y cumplen con sus obligaciones fiscales igual que lo harían con cualquier otro activo; quienes usan Bitcoin específicamente para ocultar actividad ilícita a las autoridades no están explotando una propiedad especial del protocolo, sino cometiendo el mismo delito que cometerían por cualquier otro medio, con el añadido de que la naturaleza pública y permanente de la cadena de bloques (capítulo 35) hace ese rastro, en muchos casos, más difícil de borrar que el de una transacción en efectivo.

Fuentes y estudios citados en este capítulo

- Chainalysis. "Crypto Crime Report", informes anuales sobre patrones de fraude, lavado de dinero y trazabilidad de fondos en cadenas de bloques públicas.
- Comisión Nacional del Mercado de Valores (CNMV) y otros reguladores europeos, advertencias públicas sobre esquemas de manipulación de precios ("pump and dump") en criptoactivos de baja capitalización.
- Estudios de recuperación de wallets y estimaciones sobre el volumen de bitcoins perdidos de forma permanente, citados también en el capítulo 19.
- Movimiento cypherpunk y su defensa histórica de la privacidad mediante criptografía, citado también en el capítulo 4.
- Reglamento (UE) 2023/1114 (MiCA) y normativa europea de prevención del blanqueo de capitales, sobre las obligaciones de verificación de identidad (KYC) de las plataformas reguladas, citados también en los capítulos 29 y 34.

Capítulo 34. Legalidad y regulación

La relación entre Bitcoin y los gobiernos es uno de los temas que más dudas genera, y también uno de los que más ha cambiado en los últimos años. Este bloque resume el estado actual, con las referencias a los capítulos donde se trata cada aspecto en detalle.

¿Es legal usar, comprar o vender Bitcoin en mi país?

En España y en la inmensa mayoría de los países del mundo, sí: comprar, poseer, vender y usar Bitcoin es legal, siempre que se cumplan las obligaciones fiscales y regulatorias correspondientes, que detallamos en la siguiente pregunta y en el capítulo 29. Desde el 1 de julio de 2026, además, el marco regulatorio en España y en el resto de la Unión Europea está definido con claridad por el Reglamento MiCA (Markets in Crypto-Assets), que exige a cualquier plataforma que ofrezca servicios de compraventa de criptoactivos contar con una autorización expresa de la Comisión Nacional del Mercado de Valores (CNMV), como explicamos en el capítulo 29.

La situación legal varía de forma notable según el país: mientras la Unión Europea ha optado por regular y supervisar el sector, China mantiene desde 2021 una prohibición prácticamente total de la minería y el comercio de criptomonedas (capítulo 24), y otros países han adoptado posturas intermedias, con restricciones parciales sobre determinadas actividades (como el acceso bancario a exchanges) sin llegar a prohibir la posesión individual. Antes de operar con Bitcoin en cualquier país, conviene comprobar la normativa vigente en ese momento y lugar concretos, precisamente porque, como muestra el caso de El Salvador o el de China, estas normas pueden cambiar de forma significativa en periodos relativamente cortos de tiempo.

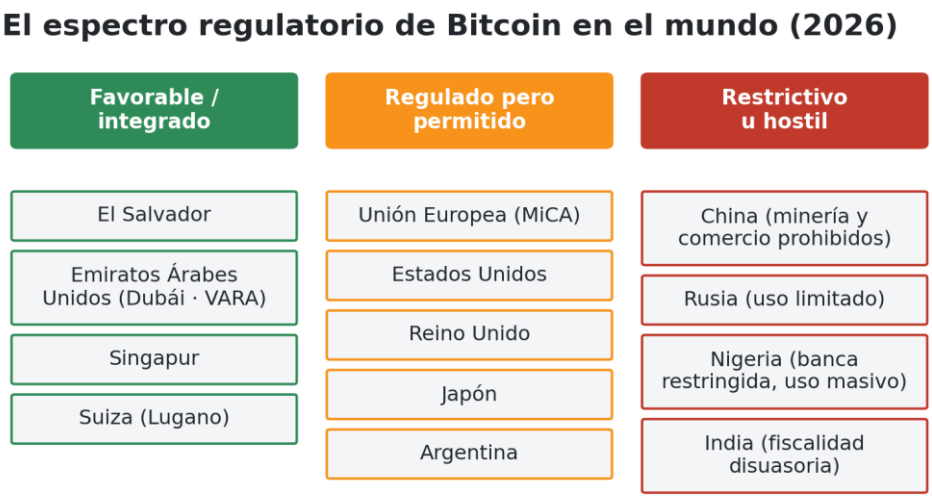
¿Cómo regula cada país a Bitcoin? Un vistazo comparado al panorama mundial en 2026

No existe un único "modelo" internacional para regular Bitcoin: cada país ha ido construyendo su propio marco a partir de su tradición jurídica, su relación con el sistema financiero internacional y su valoración política del fenómeno, lo que produce un mapa regulatorio muy heterogéneo y cambiante. A grandes rasgos pueden distinguirse cuatro posturas: la de plena regulación y supervisión (la Unión Europea con MiCA, Japón, Singapur), la de tolerancia con restricciones parciales (Reino Unido, Rusia, Nigeria), la de adopción entusiasta con incentivos fiscales (El Salvador, Emiratos Árabes Unidos) y la de prohibición o cuasi-prohibición (China). La siguiente tabla resume la situación de un grupo representativo de países a mediados de 2026, aunque conviene recordar que se trata de una fotografía de un panorama que cambia con frecuencia.

País o bloque	Postura regulatoria	Rasgos principales	Fiscalidad sobre ganancias
Unión Europea	Regulación armonizada	Reglamento MiCA en vigor desde 2024-2026, exige autorización de la autoridad nacional competente (en España, la CNMV) a toda plataforma que opere en el mercado único	Varía por Estado miembro; en España, IRPF entre el 19% y el 28% (capítulo 29)

País o bloque	Postura regulatoria	Rasgos principales	Fiscalidad sobre ganancias
Estados Unidos	Regulación fragmentada pero cada vez más favorable	Sin ley federal única; competencia repartida entre la SEC, la CFTC y reguladores estatales, con un giro hacia la claridad regulatoria y el fin de la "Operation Choke Point 2.0" en 2025	Impuesto federal sobre plusvalías, con tipos que dependen del tiempo de tenencia y el tramo de renta
Reino Unido	Regulación en desarrollo	Posesión, compraventa y uso son legales; los proveedores de servicios deben registrarse ante la FCA, que en 2026 está desplegando un régimen específico para stablecoins junto al Banco de Inglaterra	Impuesto sobre las plusvalías de capital (Capital Gains Tax)
Japón	Regulación pionera y consolidada	Bitcoin reconocido como medio de pago legal desde 2017 bajo la Ley de Servicios de Pago; los exchanges deben registrarse ante la Agencia de Servicios Financieros (FSA); reforma fiscal en curso en 2026 para reducir el tipo marginal desde cerca del 55% hacia el 20%	Hasta la reforma de 2026, tributación como renta general con tipos marginales muy elevados
Singapur	Regulación favorable a la innovación	La Autoridad Monetaria de Singapur (MAS) licencia a los exchanges bajo la Payment Services Act, con normas estrictas contra el blanqueo de capitales pero un entorno favorable a la tokenización y las finanzas institucionales	Sin impuesto sobre las plusvalías de capital para particulares en la mayoría de los casos
India	Tolerancia con fiscalidad punitiva	La posesión y el comercio son legales, pero el uso como medio de pago está prohibido de facto; un impuesto del 30% sobre las ganancias y una retención del 1% sobre cada transacción desincentivan la actividad	30% sobre las ganancias, más un 1% de retención en origen por operación
Rusia	Tolerancia parcial	Posesión y comercio legales como "propiedad", pero prohibido su uso como medio de pago dentro del país; desde 2024 se	Tributación como renta o ganancia patrimonial, con obligaciones de declaración específicas

País o bloque	Postura regulatoria	Rasgos principales	Fiscalidad sobre ganancias
		permite su uso en comercio internacional para eludir el aislamiento del sistema SWIFT	
Nigeria	Regulación reciente y en expansión	Ley de Valores e Inversiones de 2025 reconoce los criptoactivos como valores bajo supervisión de la SEC nigeriana; los bancos, antes obligados a bloquear cualquier relación con el sector, ya pueden operar con proveedores autorizados	En desarrollo, sin un régimen fiscal específico plenamente consolidado
Emiratos Árabes Unidos	Regulación favorable y ágil	La Autoridad Reguladora de Activos Virtuales de Dubái (VARA) ofrece licencias en semanas; entorno fiscal muy favorable, sin impuesto sobre la renta de las personas físicas	Sin impuesto sobre la renta personal ni sobre las plusvalías
Argentina	Regulación incipiente	Sin ley integral específica; el país está probando entornos regulatorios controlados ("sandboxes") de tokenización mientras desarrolla un marco definitivo	Impuesto sobre bienes personales y ganancias, con un tratamiento aún poco desarrollado para criptoactivos
El Salvador	Adopción como moneda de curso legal	Bitcoin es moneda de curso legal desde 2021 (capítulo 24), aunque una reforma de 2025 ligada a un acuerdo con el FMI eliminó la obligatoriedad de aceptarlo para los comercios	Sin impuesto sobre las plusvalías de Bitcoin para residentes
China	Prohibición	Minería y comercio prohibidos desde 2021; posesión individual tolerada de facto pero sin ningún reconocimiento legal ni acceso a plataformas reguladas dentro del país	No aplica; el uso comercial está fuera de la ley



Clasificación orientativa según el marco legal vigente a mediados de 2026; varios países combinan rasgos de más de una categoría según el uso (comercio, minería, pagos) — ver capítulo 34 para el detalle país por país.

El espectro regulatorio de Bitcoin en el mundo, de la adopción entusiasta a la prohibición.

Vista de este modo, la tabla anterior se agrupa con bastante claridad en tres grandes bloques de color: los países que compiten activamente por atraer capital y talento del sector con incentivos fiscales y licencias rápidas, los que han optado por una regulación estricta pero predecible que permite operar dentro de reglas claras, y una minoría que mantiene una postura restrictiva u hostil, ya sea por motivos de control de capitales, de estabilidad de su propia moneda o de recelo político hacia un activo que escapa, por diseño, al control directo del banco central. Conviene no confundir "restrictivo" con "irrelevante": Nigeria, pese a las restricciones bancarias que sufrió durante años, figura sistemáticamente entre los países con mayor adopción de base de Bitcoin del mundo (capítulo 45), lo que demuestra que la postura regulatoria de un gobierno y el comportamiento real de su población no siempre coinciden.

Más allá de las diferencias formales, el patrón que se repite en la mayoría de los países que han optado por regular en lugar de prohibir es el mismo que describimos a propósito de la Unión Europea: una vez que la demanda ciudadana e institucional alcanza un tamaño suficiente, a los gobiernos les resulta más práctico encauzarla dentro de un marco supervisado -con sus obligaciones de licencia, prevención de blanqueo de capitales y fiscalidad- que intentar prohibirla, una lección que China, con su prohibición de 2021 que no ha impedido que el país siga aportando en torno al 12% del hashrate mundial de minería según detallamos en el capítulo 35, ilustra a su manera: prohibir resulta mucho más fácil de anunciar que de aplicar con eficacia total.

¿Tengo que pagar impuestos si gano dinero con Bitcoin?

Sí, y de forma casi universal en los países con un sistema fiscal desarrollado. En España, como se detalla en el capítulo 29, las ganancias obtenidas al vender bitcoin, al canjearlo por otra criptomoneda o al usarlo para pagar tributan en el IRPF como ganancias patrimoniales dentro de la base imponible del ahorro, con tipos que en 2026 oscilan aproximadamente entre

el 19% y el 28% según el importe de la ganancia, sin ningún mínimo exento. Un matiz que sorprende a muchos principiantes es que cambiar una criptomoneda por otra -por ejemplo, bitcoin por ether- ya genera una obligación fiscal en el momento del canje, aunque el dinero nunca haya pasado por euros; el cálculo se realiza, con carácter general, mediante el método FIFO, que da por vendidas primero las unidades compradas primero.

Además del IRPF, existe una obligación informativa específica -el Modelo 721- para quien mantiene criptoactivos por un valor superior a 50.000 euros en plataformas situadas en el extranjero, que debe presentarse entre el 1 de enero y el 31 de marzo del año siguiente. No declarar estas ganancias no es una opción sin consecuencias: como explicamos en el capítulo 33 sobre la trazabilidad de las transacciones, la Agencia Tributaria tiene, cada vez con más frecuencia, acceso a la información de las plataformas reguladas que operan en España, y las sanciones por no declarar correctamente pueden superar con creces el ahorro fiscal que se pretendía obtener, además de que estas normas cambian con cierta frecuencia, por lo que conviene confirmarlas siempre con la Agencia Tributaria o un asesor fiscal antes de presentar cualquier declaración.

¿Los gobiernos pueden prohibir Bitcoin por completo?

Un gobierno puede, sin duda, prohibir el uso de Bitcoin dentro de su territorio, restringir el acceso bancario a las empresas que operan con él, o perseguir penalmente a quienes lo utilicen, como ha hecho China desde 2021 (capítulo 24). Lo que resulta extraordinariamente difícil, y hasta la fecha ningún gobierno lo ha conseguido de forma completa, es eliminar por completo la capacidad técnica de la red de seguir funcionando, precisamente por su naturaleza descentralizada (bloque de concepto básico): mientras exista, en cualquier parte del mundo, un número suficiente de nodos y mineros dispuestos a mantener la red activa, Bitcoin sigue funcionando técnicamente, aunque el acceso legal y práctico para los ciudadanos de un país concreto pueda quedar muy restringido.

El caso chino es ilustrativo: pese a contar con una de las prohibiciones más severas y mejor aplicadas del mundo, con el cierre forzoso de todas las operaciones mineras del país en 2021, la red de Bitcoin no dejó de funcionar en ningún momento a escala global, y buena parte de la potencia de minado que salió de China simplemente se trasladó a otros países, como analizamos en el capítulo 24. La conclusión práctica es que una prohibición nacional puede afectar mucho, y de forma muy real, a los ciudadanos y empresas de ese país concreto, pero no tiene capacidad de "apagar" Bitcoin a escala global salvo que fuera adoptada de forma simultánea y efectiva por la práctica totalidad de los países del mundo, un escenario de coordinación internacional que no se ha producido hasta la fecha.

¿Los bancos tradicionales ven Bitcoin como una amenaza o como una oportunidad?

La respuesta honesta es que ambas posturas conviven, a menudo dentro de la misma entidad. Durante buena parte de la última década, una parte significativa del sector bancario tradicional mantuvo una postura de cautela o abierta hostilidad hacia Bitcoin y el resto de criptoactivos, y en Estados Unidos esa tensión llegó a materializarse en la llamada "Operation Choke Point 2.0" (capítulo 28), una presión administrativa informal que dificultó el acceso bancario de numerosas empresas del sector cripto entre 2021 y 2025, hasta que una orden ejecutiva de agosto de 2025 puso fin oficialmente a esa práctica.

Al mismo tiempo, y de forma cada vez más visible, muchas de las mismas instituciones financieras tradicionales han pasado a ofrecer directamente servicios relacionados con Bitcoin: en España, bancos como Openbank, CaixaBank, Renta 4 o BBVA ya ofrecen a sus clientes la posibilidad de comprar y custodiar criptoactivos regulados bajo MiCA (capítulo 29), y a nivel internacional gestoras como BlackRock, que durante años mantuvieron una postura pública crítica frente a Bitcoin, lanzaron sus propios fondos cotizados (ETF) de Bitcoin al contado, que hoy gestionan decenas de miles de millones de dólares (bloque de futuro). Esta aparente contradicción refleja, en realidad, una evolución bastante lógica: cuanto mayor es la demanda de los clientes y más claro el marco regulatorio, menos sentido tiene para un banco quedarse fuera de un mercado que, aunque sigue siendo minoritario frente al conjunto del sistema financiero, ha dejado de ser ignorable.

Fuentes y estudios citados en este capítulo

- Comisión Nacional del Mercado de Valores (CNMV). Información sobre entidades autorizadas bajo el Reglamento MiCA en España, citada también en el capítulo 29.
- Agencia Tributaria. Información oficial sobre la tributación de las criptomonedas en el IRPF y el Modelo 721, citada también en el capítulo 29.
- Cobertura periodística y análisis regulatorio sobre la prohibición china de la minería y el comercio de criptomonedas desde 2021, citada también en el capítulo 24.
- House Financial Services Committee (Cámara de Representantes de EE. UU.). Investigación sobre la "Operation Choke Point 2.0", noviembre de 2025, citada también en el capítulo 28.
- Sumsub. "Crypto Regulation in 2026: What Changed and What's Ahead" (2026); Bitrue, "Global Crypto Regulation by Country for 2026" (2026), sobre el panorama regulatorio comparado por país.
- Financial Conduct Authority (Reino Unido), Financial Services Agency (Japón), Monetary Authority of Singapore, Investments and Securities Act (Nigeria, 2025) y Virtual Assets Regulatory Authority (Dubái, EAU). Fuentes oficiales de cada regulador nacional citado en la tabla comparativa.

Capítulo 35. Funcionamiento técnico (para no técnicos)

Este bloque retoma, en formato de preguntas directas y con analogías sencillas, los conceptos técnicos que ya explicamos con más extensión en la parte central del libro, pensado como repaso rápido para quien no necesita el detalle de ingeniería, solo entender la idea de fondo.

¿Qué es la "blockchain" y por qué es tan importante para Bitcoin?

La cadena de bloques o blockchain, explicada con detalle en el capítulo 7, es el libro de contabilidad público de Bitcoin: un registro que contiene, ordenada cronológicamente, la totalidad de las transacciones jamás realizadas en la red, agrupadas en bloques que se van encadenando unos con otros mediante técnicas criptográficas, de modo que alterar un bloque antiguo obligaría a recalcular también todos los bloques posteriores, algo computacionalmente inviable en la práctica. La analogía más útil es la de un libro de actas notariales que, en lugar de guardarse en el archivo de un único notario, se copia de forma idéntica y simultánea en miles de despachos distintos repartidos por todo el mundo: para falsificar una entrada tendrías que alterar, de forma coherente, la inmensa mayoría de esas copias a la vez, no solo una.

Es importante para Bitcoin porque resuelve el problema central que ningún sistema de dinero digital había resuelto antes de 2009: el del doble gasto, es decir, evitar que alguien pueda gastar la misma unidad de dinero digital dos veces, como sí podría hacer copiando un archivo informático corriente. Al mantener un único registro público, verificado de forma independiente por miles de participantes, la red puede comprobar en todo momento que cada bitcoin solo se gasta una vez, sin necesidad de que ningún banco central actúe como árbitro de confianza, que es precisamente la innovación que describimos en el capítulo 5 a propósito del documento original de Satoshi Nakamoto.

¿Qué significa que las transacciones de Bitcoin queden registradas para siempre en un "libro mayor público"?

Significa, en términos prácticos, que cualquier persona en el mundo, sin necesidad de permiso ni de ser parte de la transacción, puede consultar en cualquier momento el historial completo de todas las transacciones de Bitcoin realizadas desde el primer bloque en 2009, usando herramientas gratuitas llamadas exploradores de bloques. Esto contrasta radicalmente con un sistema bancario tradicional, donde el historial de tus movimientos solo lo conocen tu banco y las entidades a las que ese banco decide (o está obligado a) compartirlo, pero nunca es públicamente consultable por cualquiera.

Esta permanencia y transparencia tiene dos caras, ya apuntadas en el bloque de seguridad: por un lado, hace que el sistema sea extraordinariamente auditable -cualquiera puede verificar de forma independiente que la oferta total de Bitcoin nunca supera los 21 millones de unidades, sin tener que confiar en la palabra de nadie-, y por otro, implica que ninguna transacción, una vez confirmada, puede borrarse ni modificarse jamás, lo que exige mucho cuidado al operar, porque un error -como enviar fondos a la dirección equivocada- no se puede revertir del modo en que un banco podría, en algunos casos, revertir una transferencia errónea.

¿Qué es la minería de Bitcoin y por qué consume tanta energía?

La minería, explicada en profundidad en el capítulo 8, es el proceso mediante el cual ordenadores especializados de todo el mundo compiten entre sí para resolver un problema matemático extremadamente difícil de calcular pero fácil de verificar una vez resuelto; quien lo consigue primero obtiene el derecho a añadir el siguiente bloque de transacciones a la cadena y recibe, como recompensa, bitcoins de nueva creación más las comisiones de esas transacciones. Es, en esencia, una especie de lotería computacional continua en la que cada intento de resolver el problema consume electricidad, y cuantos más participantes compiten, más intentos por segundo se realizan en conjunto y más energía se consume en total.

Este consumo energético, que ha sido objeto de un intenso debate público y que analizamos con más detalle en el capítulo 28, no es un efecto secundario accidental, sino el mecanismo de seguridad central del sistema, llamado Prueba de Trabajo (Proof-of-Work), que abordamos en la siguiente pregunta: el coste energético real de intentar falsificar la cadena de bloques es precisamente lo que hace que hacerlo resulte económicamente inviable. Los defensores de Bitcoin señalan que buena parte de esa energía procede de fuentes renovables o de excedentes energéticos que de otro modo se desperdiciarían, mientras que sus críticos consideran que ese consumo, sea cual sea su origen, representa un coste medioambiental que otros sistemas de pago digitales no requieren; ambos argumentos, con sus matices, se desarrollan con las fuentes correspondientes en el capítulo 28.

¿Cuánto cuesta minar un bitcoin y quién gana realmente dinero con ello?

El coste de producir un bitcoin varía enormemente según la eficiencia del operador, y esa variación es precisamente lo que determina quién sobrevive en el sector y quién queda fuera del mercado en cada ciclo. Según los datos de mediados de 2026, los mineros industriales más eficientes -aquellos con acceso a electricidad muy barata y con el hardware más moderno- producen un bitcoin gastando entre 32.000 y 55.000 dólares en electricidad y alojamiento, mientras que el coste medio de producción del conjunto de la red ronda los 77.000 dólares, y algunos operadores con costes "todo incluido" (financiación del hardware, personal, refrigeración, mantenimiento) superan los 100.000 dólares por bitcoin producido.

Esta diferencia tan amplia explica un patrón que se repite en cada ciclo de mercado: cuando el precio de Bitcoin cae por debajo del coste de producción de los operadores menos eficientes, estos se ven obligados a apagar sus máquinas porque cada bitcoin minado les generaría pérdidas, mientras que los operadores más eficientes -con electricidad más barata, normalmente por debajo de 0,06 dólares por kilovatio-hora- pueden seguir minando con beneficio incluso en esas condiciones. La electricidad representa, de hecho, entre el 60% y el 80% del coste operativo total de una instalación minera, por lo que el acceso a energía barata es, con diferencia, la variable que más determina la rentabilidad de un minero, por encima incluso del hardware que utilice.

Quién gana dinero, por tanto, no es "el minero" en abstracto, sino específicamente el operador que combina electricidad barata, hardware eficiente y buena gestión operativa; el resto compite en un mercado donde los márgenes se estrechan de forma continua a medida que la dificultad de minado aumenta y la recompensa por bloque se reduce cada cuatro años en el halving (pregunta anterior), un proceso de selección natural que ha ido concentrando la

minería en manos de operadores cada vez más grandes y sofisticados, como veremos en la siguiente pregunta.

¿Qué son los "pools" de minería y por qué casi nadie mina en solitario?

Dado que la probabilidad de que un único minero individual resuelva el problema matemático de un bloque antes que el resto de la red combinada es hoy extraordinariamente baja -la potencia de cálculo total de la red equivale a cientos de millones de ordenadores potentes trabajando a la vez-, la inmensa mayoría de los mineros se agrupan en lo que se conoce como "pools" o grupos de minería: plataformas que combinan la potencia de cálculo de miles de participantes distintos, reparten entre todos ellos, de forma proporcional al esfuerzo aportado, cualquier recompensa que el grupo obtenga cuando alguno de sus miembros encuentra un bloque válido. De este modo, en lugar de una lotería en la que ganas todo o nada muy de vez en cuando, cada minero recibe un pago pequeño pero mucho más frecuente y predecible, similar a cambiar un billete de lotería único por muchas participaciones más pequeñas de un boleto compartido.

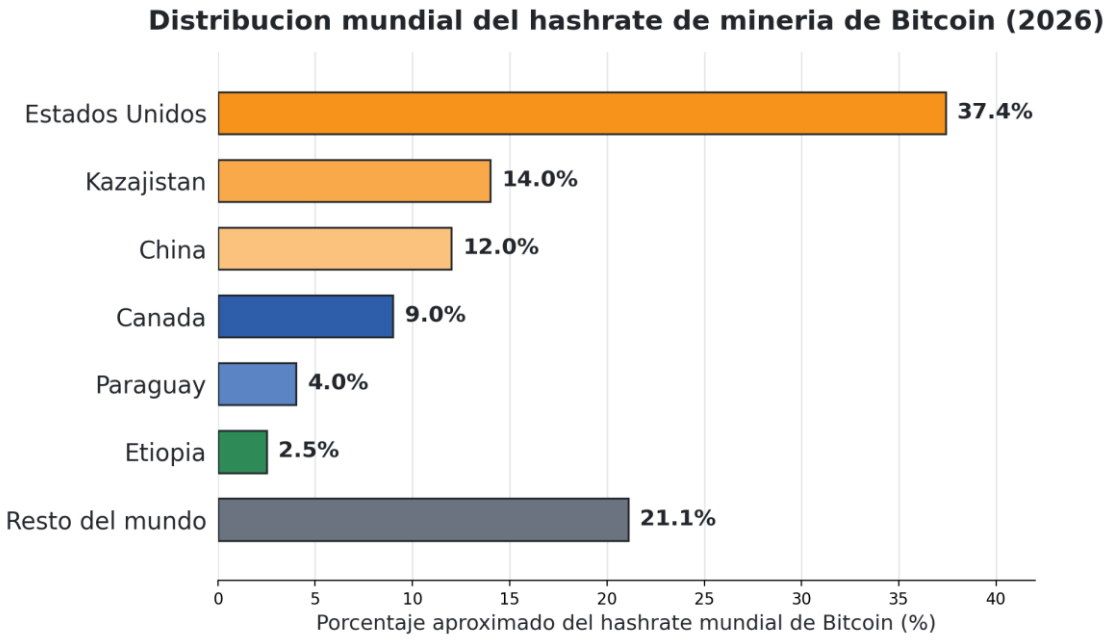
Este modelo, sin embargo, plantea una tensión estructural que analizamos con detalle en el capítulo 23 sobre la concentración de poder: si unos pocos pools llegan a controlar, entre todos, una parte demasiado grande de la potencia de cálculo total de la red, la seguridad teórica de Bitcoin -que depende de que ningún actor único controle más del 50% del hashrate- empieza a depender de la buena fe y la competencia entre un número reducido de operadores de pools, en lugar de depender de la competencia entre miles de mineros verdaderamente independientes. A mediados de la década de 2020, los mayores pools del mundo -entre ellos Foundry USA, AntPool, F2Pool y ViaBTC- concentran, entre los tres o cuatro primeros, bien más de la mitad del hashrate total de la red, lo que sigue siendo motivo de debate dentro de la comunidad, aunque conviene matizar que el control de un pool sobre la potencia de cálculo de sus miembros es limitado en la práctica: cualquier minero puede cambiar de pool en cuestión de minutos si sospecha de un comportamiento malicioso, lo que actúa como un freno disuasorio importante frente a un pool que intentase abusar de su posición.

¿En qué países se concentra la minería de Bitcoin y por qué ahí?

La geografía de la minería de Bitcoin ha cambiado radicalmente desde que China -que hasta 2021 albergaba la mayor parte del hashrate mundial- prohibió la actividad de forma oficial ese mismo año, obligando a una reubicación masiva de equipos hacia otros países. Según los datos de 2026, Estados Unidos se ha consolidado como el líder indiscutible, con aproximadamente el 37,4% del hashrate mundial (unos 375 EH/s), apoyado en mercados eléctricos muy desarrollados, capital institucional abundante y una regulación relativamente predecible en muchos estados; le siguen Kazajistán, con cerca del 14% gracias a su energía fósil barata (aunque su cuota lleva varios años en descenso por la presión regulatoria y las limitaciones de la red eléctrica local), y, de forma llamativa, China, que pese a mantener oficialmente prohibida la minería desde 2021 sigue aportando en torno al 12% del hashrate mundial a través de operaciones semitoleradas o directamente clandestinas, muchas de ellas aprovechando la energía hidroeléctrica estacional de provincias como Sichuan.

Otros países han encontrado un nicho específico basado en su matriz energética: Canadá lidera en sostenibilidad con cerca del 9% del hashrate mundial, mayoritariamente alimentado por energía hidroeléctrica; Paraguay atrae minería gracias al enorme excedente de energía

hidroeléctrica de la represa de Itaipú, una de las mayores del mundo, que le permite ofrecer algunos de los costes eléctricos marginales más bajos del planeta; y Etiopía ha entrado en el grupo de cabeza en los últimos años, apoyándose en nueva capacidad hidroeléctrica, hasta representar en torno al 2,5% del hashrate mundial. En conjunto, los tres primeros países por hashrate concentran aproximadamente el 78% de toda la minería mundial de Bitcoin, un grado de concentración geográfica que preocupa a parte de la comunidad por razones similares a las de la concentración en pools: cuanto más dependa la seguridad de la red de la estabilidad política y regulatoria de un puñado de jurisdicciones, más vulnerable es, en teoría, a decisiones políticas coordinadas o a eventos que afecten a esas regiones en concreto.



Distribución aproximada del hashrate mundial de Bitcoin por país (2026).

El denominador común de casi todos estos países ganadores es el mismo: acceso a electricidad barata y, cada vez más, a menudo procedente de fuentes renovables o de excedentes que de otro modo se desperdiciarían (hidroeléctrica en Canadá, Paraguay y Etiopía; geotérmica en proyectos como el salvadoreño que veremos en el capítulo 24), lo que ha ido desplazando gradualmente el argumento del "coste medioambiental" de la minería hacia un terreno más matizado del que existía hace unos años, aunque la disputa, como señalamos en el capítulo 28, sigue abierta y no plenamente resuelta.

¿Cómo ha evolucionado el hardware de minería y hacia dónde va?

Minar Bitcoin dejó de poder hacerse de forma rentable con un ordenador doméstico hace más de una década. Hoy la inmensa mayoría del hashrate mundial lo generan máquinas llamadas ASIC (circuitos integrados de aplicación específica), diseñadas desde cero con el único propósito de resolver, lo más rápido y con el menor consumo posible, el problema matemático concreto que exige el algoritmo de minería de Bitcoin (SHA-256), a diferencia de un ordenador de propósito general, que puede hacer muchas cosas distintas pero ninguna de ellas de forma tan optimizada.

La evolución de estas máquinas en términos de eficiencia energética ha sido extraordinaria: los primeros ASICs comerciales, de principios de la década de 2010, consumían del orden de 98 julios por cada terahash de potencia de cálculo (J/TH), mientras que los modelos más avanzados de 2026 operan ya en el rango de 15 a 20 J/TH, y algunos prototipos de última generación se acercan a los 10 J/TH, lo que supone, en conjunto, una mejora de eficiencia energética de aproximadamente siete veces en poco menos de una década. Esa mejora continua tiene un efecto económico directo sobre el sector descrito en la primera pregunta de este bloque: cada nueva generación de hardware deja fuera de mercado a las máquinas más antiguas, que dejan de ser rentables aunque la electricidad que consumen sea gratuita en términos comparativos, porque el coste de oportunidad de no sustituirlas por hardware más eficiente resulta demasiado alto frente a la competencia.

Este ritmo de mejora, sin embargo, se ha ido ralentizando de forma natural a medida que la tecnología de fabricación de semiconductores se acerca a límites físicos cada vez más difíciles de superar, algo similar a lo que ha ocurrido con los procesadores de los ordenadores convencionales en los últimos años; buena parte de la innovación actual en el sector se concentra ya no tanto en hacer el chip individual más eficiente, sino en optimizar el diseño de los centros de datos completos -refrigeración líquida o por inmersión, gestión inteligente de la carga en función del precio de la electricidad en cada momento, e incluso, como detallamos en el capítulo 38, el uso de inteligencia artificial para maximizar la eficiencia operativa de instalaciones que combinan minería de Bitcoin con computación para IA.

¿Qué es el ajuste de dificultad y por qué es tan importante?

Para que Bitcoin mantenga su ritmo de emisión previsible -un bloque nuevo cada diez minutos de media, tal y como diseñó Satoshi Nakamoto-, el protocolo necesita compensar automáticamente el hecho de que la potencia de cálculo total dedicada a la minería no es constante, sino que fluctúa de forma continua a medida que entran y salen mineros del mercado en función de su rentabilidad. Ese mecanismo de compensación se llama ajuste de dificultad, y consiste en que, cada 2.016 bloques (aproximadamente cada dos semanas), la red vuelve a calcular automáticamente lo difícil que debe ser el problema matemático que deben resolver los mineros: si en las dos semanas anteriores los bloques se han encontrado más rápido de lo previsto -señal de que ha entrado más potencia de cálculo a la red-, la dificultad sube; si se han encontrado más lento -señal de que algunos mineros han apagado sus máquinas, por ejemplo por una caída del precio-, la dificultad baja.

Este mecanismo es lo que permite que Bitcoin funcione con el mismo ritmo aproximado de emisión de nuevos bloques tanto si la red cuenta con unos pocos cientos de mineros aficionados, como ocurría en 2009, como si cuenta con cientos de miles de máquinas industriales especializadas repartidas por todo el planeta, como ocurre hoy: la dificultad se autorregula sola, sin que ninguna autoridad central tenga que intervenir para mantener el calendario de emisión, lo que refuerza el argumento, ya presentado en el capítulo 13, de que la política monetaria de Bitcoin no depende de decisiones humanas discrecionales sino de reglas matemáticas fijadas de antemano y aplicadas automáticamente por el propio protocolo.

¿Qué es eso de Proof-of-Work y qué papel juega en la seguridad de la red?

Prueba de Trabajo (Proof-of-Work) es el nombre técnico del mecanismo de minería que acabamos de describir, y su función esencial, detallada en el capítulo 8, es convertir la

seguridad de la red en un problema de coste económico real: para intentar reescribir el historial de transacciones de Bitcoin -por ejemplo, para gastar dos veces los mismos fondos-, un atacante tendría que controlar más de la mitad de toda la potencia de cálculo dedicada a la minería en todo el mundo (lo que se conoce como un "ataque del 51%"), y mantener ese control el tiempo suficiente para superar a todos los demás mineros honestos combinados, algo que a día de hoy requeriría una inversión en hardware y electricidad de miles de millones de dólares, sin ninguna garantía de éxito y con el efecto colateral casi seguro de hundir el propio valor de mercado del activo que se pretende manipular.

La analogía que usamos en el capítulo 8 es la de un examen extraordinariamente difícil de aprobar pero trivial de corregir: encontrar la solución correcta cuesta un esfuerzo computacional enorme, pero cualquier otro participante de la red puede verificar en una fracción de segundo si esa solución es válida. Ese desequilibrio deliberado -difícil de resolver, fácil de comprobar- es lo que permite que miles de participantes desconocidos entre sí, sin necesidad de confiar unos en otros, se pongan de acuerdo sobre cuál es la versión verdadera del historial de transacciones, sustituyendo la confianza en una institución central por la confianza en las matemáticas y en el coste económico de intentar hacer trampas.

¿Por qué solo puede haber 21 millones de Bitcoins y quién decidió ese número?

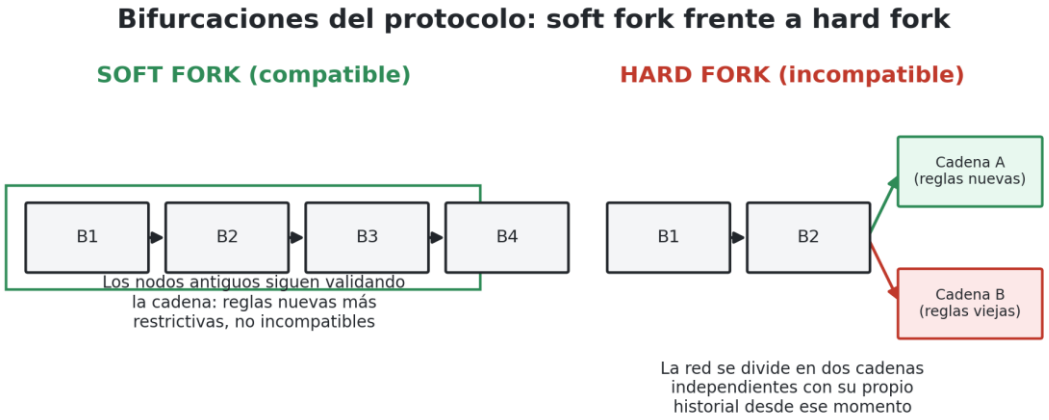
El límite de 21 millones de unidades fue una decisión de diseño incluida por Satoshi Nakamoto directamente en el código original del protocolo, descrita en el capítulo 13, y no responde a ninguna necesidad técnica inevitable, sino a una elección deliberada para garantizar una escasez matemática absoluta, a diferencia de las monedas fiduciarias, cuya oferta pueden ampliar los bancos centrales. Ese límite se alcanza de forma gradual y decreciente: cada aproximadamente cuatro años (cada 210.000 bloques minados), la recompensa que reciben los mineros por cada nuevo bloque se reduce a la mitad, en un evento conocido como "halving", hasta que, según las proyecciones actuales del protocolo, se mine el último satoshi hacia el año 2140.

Nadie puede cambiar ese número de forma unilateral: como explicamos en el bloque de concepto básico a propósito de la descentralización, alterar el límite de 21 millones exigiría el consenso de una parte abrumadora de los desarrolladores, mineros y usuarios de la red, y cualquier intento de imponerlo de forma unilateral por parte de un grupo minoritario resultaría, en la práctica, en la creación de una bifurcación (fork) distinta y separada de la Bitcoin original, no en un cambio real de la red existente, un fenómeno que ya se ha dado en la práctica -como analizamos en el capítulo 22- y que ilustra precisamente por qué ese límite se considera, a efectos prácticos, inmutable.

¿Se pueden crear más Bitcoins cambiando las reglas del sistema?

Técnicamente, cualquier grupo de desarrolladores podría publicar una versión modificada del software de Bitcoin que alterase el límite de 21 millones de unidades, pero esa modificación solo tendría efecto real si la aceptase voluntariamente una parte suficientemente amplia de la red -mineros, nodos y usuarios-, y hasta la fecha ningún intento de este tipo ha conseguido el respaldo necesario dentro de la cadena de Bitcoin original. Lo que sí ha ocurrido en varias ocasiones, como detallamos en el capítulo 22, es que grupos que discrepaban sobre otros aspectos del protocolo -no sobre el límite de emisión- se han separado para crear su propia

cadena alternativa con sus propias reglas, como Bitcoin Cash en 2017, pero esas bifurcaciones son, a todos los efectos prácticos y de mercado, proyectos distintos de Bitcoin, con su propio precio, su propia comunidad y su propio historial desde el momento de la separación, no una modificación de Bitcoin en sí.



Ejemplo real: la separación de Bitcoin Cash de Bitcoin en 2017 fue un hard fork.

Soft fork frente a hard fork: por qué unas bifurcaciones dividen la red y otras no.

La garantía real de que el límite de 21 millones se mantendrá no es, por tanto, una imposibilidad técnica absoluta, sino un incentivo económico extraordinariamente fuerte: la inmensa mayoría de los participantes de la red -mineros que han invertido en infraestructura, poseedores de bitcoin, empresas que dependen de su previsibilidad- tienen un interés directo en preservar precisamente la propiedad que hace valioso al activo, su escasez garantizada, por lo que cualquier intento de alterarla se enfrentaría a una resistencia coordinada y masiva por parte de quienes más tienen que perder si esa escasez desaparece.

¿Qué pasa técnicamente cuando envío Bitcoin de una persona a otra?

Cuando envías bitcoin, tu wallet crea un mensaje digital que especifica el origen de los fondos, la dirección de destino y el importe, y lo firma criptográficamente con tu clave privada (capítulo 9), un proceso matemático que demuestra que tienes autorización legítima para mover esos fondos sin necesidad de revelar la clave privada en sí misma, del mismo modo que puedes demostrar que conoces la combinación de una caja fuerte sin tener que decirla en voz alta. Esa transacción firmada se transmite a la red y llega a miles de nodos, que verifican de forma independiente que la firma es válida y que los fondos existen realmente y no han sido gastados previamente.

Una vez verificada, la transacción queda pendiente en una especie de sala de espera (el "mempool") hasta que un minero la incluye en el siguiente bloque que consigue resolver, un proceso que en la red principal de Bitcoin tarda de media unos diez minutos, aunque puede variar según la congestión de la red y la comisión pagada (capítulo 8). Una vez incluida en un bloque, la transacción se considera confirmada, y cuantos más bloques nuevos se añaden por encima de ese bloque, más irreversible se vuelve, hasta el punto de considerarse, tras un número suficiente de confirmaciones, prácticamente imposible de revertir. Para pagos que

requieren mayor rapidez, la red Lightning (capítulo 21) permite completar este mismo proceso de forma casi instantánea, liquidando el resultado neto en la cadena principal solo de vez en cuando.

Fuentes y estudios citados en este capítulo

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", citado también en los capítulos 5 y 30.
- Antonopoulos, A. (2017). "Mastering Bitcoin: Programming the Open Blockchain". O'Reilly Media. Referencia técnica estándar sobre el funcionamiento interno del protocolo, citada también en el capítulo 7.
- Cambridge Centre for Alternative Finance. "Cambridge Bitcoin Electricity Consumption Index", citado también en el capítulo 28 sobre el consumo energético de la minería.
- Hashrate Index. "Top 10 Bitcoin Mining Countries of 2026" (2026), sobre la distribución geográfica del hashrate mundial.
- Spark Research. "Bitcoin Mining Economics in 2026: Post-Halving Reality" (2026); Simple Mining Insights, "The Real Cost of Bitcoin Mining in 2026" (2026), sobre costes de producción y eficiencia de los ASIC.

Capítulo 36. Cómo empezar: compra, venta y custodia

El capítulo 29 ya ofrece una guía paso a paso completa para empezar a operar con Bitcoin; este bloque recoge, en formato de preguntas sueltas, las dudas prácticas más concretas que suelen surgir al dar esos primeros pasos.

¿Dónde se compra Bitcoin: en bancos, en apps, en páginas web especiales?

Hoy existen, en España, tres vías principales, todas ellas detalladas en el capítulo 29: los exchanges especializados (plataformas dedicadas exclusivamente a la compraventa de criptoactivos, como Coinbase, Kraken, Crypto.com o la española Bit2Me), las aplicaciones de bróker generalistas que han ido incorporando la compraventa de criptoactivos junto a acciones y fondos tradicionales, y, cada vez más, los propios bancos tradicionales, como Openbank, CaixaBank, Renta 4 o BBVA, que ya ofrecen este servicio integrado en su aplicación bancaria habitual. Las tres vías, si están correctamente autorizadas bajo el Reglamento MiCA vigente desde julio de 2026, ofrecen garantías regulatorias equivalentes, aunque difieren en comisiones, variedad de criptoactivos disponibles y comodidad de uso.

La elección entre unas y otras suele depender de la prioridad de cada persona: quien ya es cliente de un banco concreto y solo quiere una exposición sencilla a Bitcoin sin gestionar una cuenta nueva probablemente prefiera hacerlo directamente desde su banco; quien busca las comisiones más ajustadas o el acceso a un catálogo más amplio de criptoactivos suele decantarse por un exchange especializado. En cualquier caso, y como se insiste en el capítulo 29, conviene comprobar antes de registrarse que la plataforma elegida figura efectivamente en el listado de entidades autorizadas que publica la CNMV.

¿Qué diferencia hay entre comprar Bitcoin en un exchange y usar una app tipo broker?

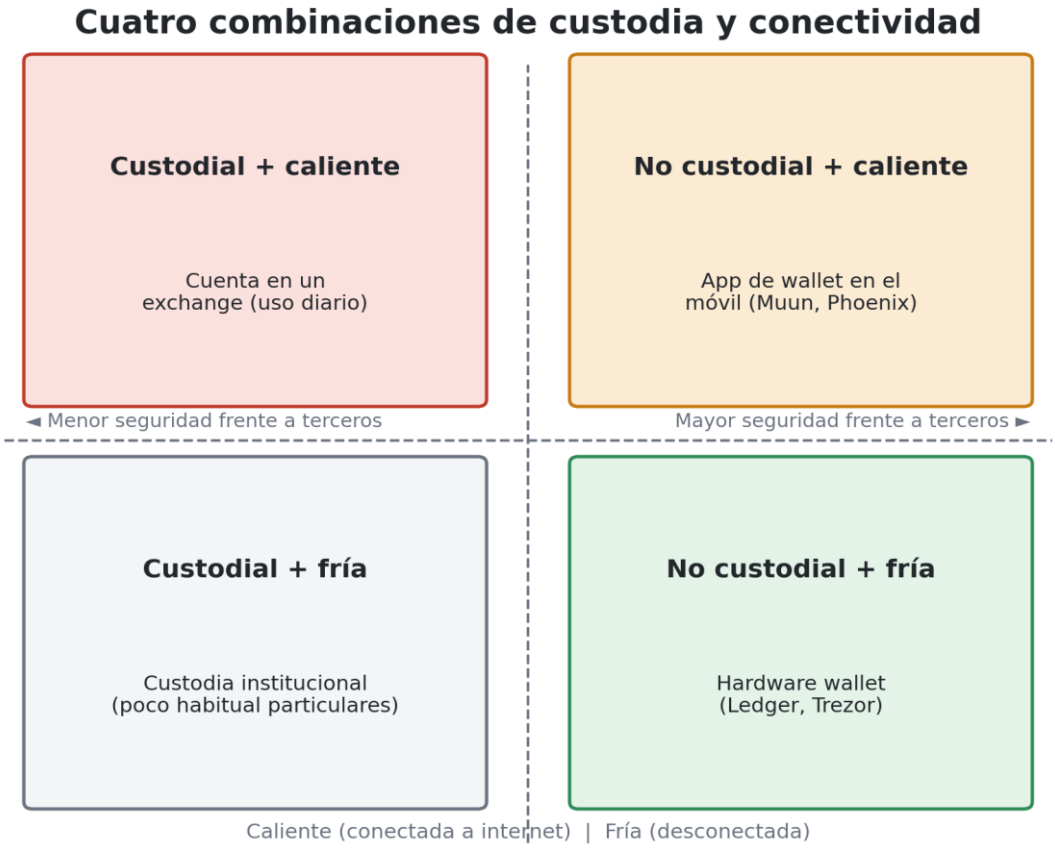
La diferencia principal no está tanto en el resultado de la compra -en ambos casos terminas siendo titular de una cantidad de bitcoin- como en la infraestructura y el objetivo con el que fueron diseñadas cada tipo de plataforma. Un exchange especializado está construido específicamente para el trading de criptoactivos: suele ofrecer un catálogo mucho más amplio de monedas, herramientas de análisis técnico más sofisticadas y, en muchos casos, la posibilidad más sencilla de retirar tus fondos a una wallet propia (capítulo 10), algo que resulta clave para quien quiere practicar la autocustodia.

Una app de bróker generalista, en cambio, suele integrar el criptoactivo como una clase de activo más dentro de una oferta que incluye acciones, fondos de inversión o ETF tradicionales, lo que resulta cómodo para quien quiere gestionar toda su cartera desde un único lugar, pero a menudo con limitaciones importantes: algunos brókeres no permiten retirar el bitcoin comprado a una wallet externa, ofreciendo solo una exposición al precio sin la posesión real del activo subyacente, una distinción fundamental que conviene verificar antes de elegir, especialmente para quien da valor a los principios de autocustodia que explicamos en el capítulo 27.

¿Qué es una billetera (wallet) de Bitcoin y qué tipos existen?

Una wallet, explicada en detalle en el capítulo 10, no es en realidad un lugar donde se "guardan" los bitcoins -como sugeriría el nombre en español, "billetera" o "monedero"-, sino una herramienta que almacena las claves criptográficas que demuestran tu propiedad sobre determinados bitcoins registrados en la cadena de bloques, y que te permite firmar las transacciones necesarias para moverlos. Existen dos grandes familias: las wallets de software (aplicaciones instaladas en tu móvil u ordenador, cómodas para el uso diario pero conectadas a internet y por tanto algo más expuestas) y las wallets hardware (dispositivos físicos dedicados que mantienen tus claves privadas completamente desconectadas de internet, ofreciendo el nivel de seguridad más alto disponible para un usuario particular).

Dentro de ambas categorías existe además la distinción entre wallets custodiales, en las que un tercero -como un exchange- guarda las claves en tu nombre, y wallets no custodiales, en las que solo tú tienes acceso real a las claves mediante tu frase semilla. Cruzando estas dos variables -custodial o no custodial, caliente o fría- se obtienen cuatro combinaciones posibles, cada una con un perfil de seguridad y de comodidad distinto, que conviene visualizar de una vez para entender dónde encaja cada opción habitual del mercado.



Cuatro combinaciones de custodia y conectividad, de la más cómoda a la más segura.

Como se insiste a lo largo de todo el libro, la máxima "not your keys, not your coins" ("si no tienes las claves, no tienes las monedas", capítulo 10) resume la diferencia práctica entre ambos modelos: en una wallet custodial dependes de que la empresa gestione bien tus fondos; en una no custodial, la responsabilidad -y el control total- recae enteramente en ti.

¿Es mejor guardar mis Bitcoins en un exchange o en una billetera propia (fría/caliente)?

La recomendación casi universal de la comunidad, explicada en el capítulo 29, es una regla de proporcionalidad más que una respuesta absoluta: para cantidades pequeñas que operas con frecuencia, mantenerlas en el exchange puede resultar razonable por comodidad; para cantidades significativas que no necesitas mover a corto plazo, la autocustodia en una wallet propia -idealmente una wallet fría (hardware, desconectada de internet) para el grueso de tus ahorros, y una wallet caliente (de software, conectada a internet) solo para el importe que uses de forma habitual- reduce el riesgo de contraparte que analizamos en el capítulo 18 a propósito de Mt. Gox y FTX.

Esta recomendación no está exenta de matices: la autocustodia elimina el riesgo de que la plataforma quiebre o sea hackeada, pero traslada por completo la responsabilidad de la seguridad a ti mismo, incluyendo el riesgo de perder la frase semilla (capítulo 19) o de sufrir un robo físico si no la proteges adecuadamente (capítulo 25). No existe una opción sin riesgo alguno; existe, en todo caso, una elección informada sobre qué tipo de riesgo -el de un tercero, o el propio- estás mejor preparado para gestionar en tu situación concreta.

¿Cuánto tarda en confirmarse una transacción de Bitcoin y por qué a veces se demora?

En la red principal de Bitcoin, cada bloque nuevo se mina, de media, cada diez minutos, y muchas plataformas y comercios consideran una transacción razonablemente segura tras una única confirmación, aunque para importes grandes es habitual esperar a varias confirmaciones adicionales -a menudo seis, es decir, aproximadamente una hora- para considerarla prácticamente irreversible, como explicamos en el capítulo 35 sobre el funcionamiento técnico de las transacciones. En condiciones normales de uso, este plazo resulta perfectamente asumible para la mayoría de los casos, aunque notablemente más lento que un pago con tarjeta.

La demora puede alargarse de forma notable en momentos de alta congestión de la red, cuando muchos usuarios intentan enviar transacciones a la vez y compiten por un espacio limitado en cada bloque, un fenómeno que suele coincidir con periodos de alta volatilidad de precio; en esos momentos, la comisión pagada determina en gran medida la prioridad con la que un minero incluye tu transacción, por lo que pagar una comisión más alta puede acelerar significativamente la confirmación. Para pagos que requieren rapidez incluso en momentos de congestión, la red Lightning (capítulo 21) resulta la alternativa más adecuada, al confirmar los pagos de forma prácticamente instantánea sin depender directamente del ritmo de los bloques de la cadena principal.

¿Qué comisiones se pagan al enviar o recibir Bitcoin?

Recibir bitcoin nunca tiene coste alguno para quien lo recibe: la comisión de red la paga siempre quien envía la transacción, como incentivo para que los mineros la incluyan en el siguiente bloque. Esa comisión no es un porcentaje fijo del importe enviado, como ocurre con muchas comisiones bancarias, sino que depende del tamaño en bytes de la transacción y de cuánta demanda de espacio haya en ese momento en la red: enviar una gran cantidad de

bitcoin puede llegar a costar la misma comisión de red que enviar una cantidad muy pequeña, siempre que el tamaño de los datos de la transacción sea similar.

Además de la comisión de la propia red de Bitcoin, hay que tener en cuenta las comisiones que cobra la plataforma que uses para comprar o vender: como detalla la comparativa del capítulo 29, estas oscilan aproximadamente entre el 0,16% y el 1,5% por operación según la plataforma elegida, a las que pueden sumarse comisiones adicionales por depósito con tarjeta o por retirar los fondos a una wallet externa. Sumando ambos conceptos -comisión de la plataforma y comisión de red-, comprar y mover cantidades pequeñas de forma muy frecuente puede resultar proporcionalmente más caro que agrupar esas operaciones, un factor a tener en cuenta al planificar tu estrategia de compra, como ya se apuntaba en el bloque de precio e inversión.

Fuentes y estudios citados en este capítulo

- Comisión Nacional del Mercado de Valores (CNMV). Listado de entidades autorizadas bajo MiCA para operar en España, citado también en el capítulo 29.
- Documentación técnica de wallets hardware (Ledger, Trezor) y de software sobre la gestión de claves privadas y frases semilla, citada también en el capítulo 10.
- Datos de comisiones medias de red de Bitcoin y tiempos de confirmación, recogidos por exploradores de bloques públicos como mempool.space.

Capítulo 37. Comparaciones con otras criptomonedas y tecnologías

Bitcoin fue la primera criptomoneda, pero está lejos de ser la única. Este bloque aclara en qué se diferencia de otros proyectos con los que a menudo se confunde o se compara, y profundiza en dos piezas centrales del resto del ecosistema que hasta ahora solo habíamos mencionado de pasada: los contratos inteligentes y los distintos tipos de criptoactivos que existen más allá de Bitcoin.

¿En qué se diferencia Bitcoin de otras criptomonedas como Ethereum o las stablecoins?

Bitcoin y Ethereum comparten la tecnología de base -una cadena de bloques pública y descentralizada-, pero persiguen objetivos bastante distintos, como apuntamos en el capítulo 21. Bitcoin fue diseñado, ante todo, como una forma de dinero digital escaso y resistente a la censura, con un protocolo deliberadamente simple y estable que apenas ha cambiado en sus reglas fundamentales desde su creación, precisamente para maximizar su previsibilidad y seguridad como reserva de valor. Ethereum, lanzado en 2015, fue diseñado como una plataforma mucho más amplia y programable, capaz de ejecutar aplicaciones descentralizadas complejas -desde préstamos automatizados hasta mercados de arte digital (NFT)- mediante los llamados "contratos inteligentes", a costa de una mayor complejidad técnica y de cambios de protocolo más frecuentes, incluyendo un cambio radical de su propio mecanismo de seguridad en 2022, pasando de una minería similar a la de Bitcoin a un sistema distinto llamado Proof-of-Stake.

Las stablecoins, por su parte, son una categoría completamente distinta: criptomonedas diseñadas para mantener un valor estable, normalmente vinculado uno a uno con una moneda fiduciaria como el dólar o el euro, mediante reservas de esa misma moneda o de activos equivalentes que respaldan cada unidad emitida. Mientras que el atractivo de Bitcoin reside precisamente en su escasez y su independencia de cualquier moneda fiduciaria, el atractivo de una stablecoin es justo el opuesto: ofrecer la rapidez y la programabilidad de una cadena de bloques sin la volatilidad de precio que caracteriza a Bitcoin, lo que las hace útiles sobre todo como herramienta de pago o de refugio temporal dentro del propio ecosistema cripto, no como una inversión con expectativa de revalorización. Las tres preguntas siguientes desarrollan estos dos conceptos -contratos inteligentes y stablecoins- con mucho más detalle del que hemos dado hasta ahora en el libro.

¿Qué son exactamente los contratos inteligentes (smart contracts)?

Un contrato inteligente es, en esencia, un programa informático que se ejecuta automáticamente sobre una cadena de bloques cuando se cumplen unas condiciones predefinidas en su propio código, sin necesidad de que ninguna de las partes confíe en la otra ni en un intermediario que verifique el cumplimiento del acuerdo. El nombre puede resultar algo engañoso: no es "inteligente" en el sentido de razonar o adaptarse, ni es un "contrato" en el sentido legal tradicional con el que estamos familiarizados, sino más bien una serie de instrucciones del tipo "si ocurre A, entonces ejecuta B" que la propia red garantiza que se cumplirán exactamente como fueron programadas, publicadas de forma pública y verificable para que cualquiera pueda auditar su código antes de interactuar con él.

El ejemplo más citado para entender la idea es el de una máquina expendedora: introduces la moneda correcta (la condición), y la máquina, sin que ningún vendedor intervenga, te entrega automáticamente el producto (la ejecución). Un contrato inteligente aplica esa misma lógica automática y sin intermediarios a operaciones financieras y digitales mucho más complejas: prestar dinero con garantías que se liquidan automáticamente si su valor cae por debajo de un umbral, repartir los ingresos de una obra digital entre varios creadores en el momento exacto de cada venta, o gestionar las reglas de votación de una organización sin ningún consejo de administración tradicional (lo que se conoce como una DAO, que detallamos más abajo). Ethereum, diseñado desde su origen en 2015 específicamente para ejecutar este tipo de programas de forma general y flexible, se convirtió en la plataforma de referencia para los contratos inteligentes, y hoy la inmensa mayoría de las aplicaciones que se agrupan bajo la etiqueta de "finanzas descentralizadas" o DeFi (siguiente pregunta) se ejecutan sobre Ethereum o sobre otras cadenas de bloques con capacidades similares.

¿Tiene Bitcoin contratos inteligentes de algún tipo?

Es una pregunta que genera bastante confusión, y la respuesta honesta es: de forma limitada y deliberada, sí, aunque no de la manera flexible y general en que los tiene Ethereum. El propio lenguaje de programación de Bitcoin, llamado Script, existe desde el primer día del protocolo (capítulo 5) y permite condiciones básicas de gasto -por ejemplo, exigir varias firmas distintas para autorizar una transacción, lo que llamamos multisig en el capítulo 10, o bloquear fondos hasta una fecha futura concreta-, pero fue diseñado de forma intencionadamente restringida, sin la capacidad de ejecutar bucles ni programas de complejidad arbitraria, precisamente para minimizar la superficie de posibles fallos de seguridad en una red cuyo objetivo principal es la máxima fiabilidad como dinero, no la máxima flexibilidad como plataforma de aplicaciones.

Sobre esa base limitada se han ido construyendo, con los años, capacidades más sofisticadas. La actualización Taproot de 2021, que ya mencionamos en el glosario, mejoró sustancialmente la eficiencia y la privacidad de las condiciones de gasto complejas. Los llamados Contratos de Registro Discreto (Discrete Log Contracts o DLC) permiten acuerdos financieros condicionados a un dato externo -por ejemplo, el precio de un activo en una fecha concreta, verificado por un tercero llamado oráculo- sin revelar los detalles del contrato en la cadena pública. El protocolo RGB, todavía en desarrollo activo, persigue un objetivo más ambicioso: permitir emitir activos y ejecutar lógica compleja apoyándose en la seguridad de Bitcoin pero manteniendo la mayor parte del cómputo fuera de la cadena principal. Y la propia red Lightning (capítulo 21), aunque no se piensa habitualmente en estos términos, es en el fondo una aplicación de contratos inteligentes muy sofisticada: cada canal de pago es, técnicamente, un contrato que ejecuta automáticamente las reglas acordadas entre las partes sin necesidad de confiar la una en la otra. La filosofía de fondo, coherente con todo lo que hemos visto sobre las prioridades de diseño de Bitcoin (capítulo 22), es añadir capacidad de programación de forma muy gradual y conservadora, capa por capa, en lugar de sacrificar la simplicidad y la seguridad del protocolo base por una flexibilidad que otras cadenas, como Ethereum, sí han priorizado desde su diseño original.

¿Qué son las stablecoins en profundidad y por qué son tan importantes en el ecosistema cripto?

Ya definimos las stablecoins de forma general al principio de este capítulo; profundicemos en su funcionamiento y en su peso real. Existen, fundamentalmente, tres modelos: las respaldadas por reservas fiduciarias, que mantienen en un banco o en activos equivalentes (como deuda pública a corto plazo) una cantidad de dólares o euros equivalente a las unidades emitidas, y que son sometidas, al menos en teoría, a auditorías periódicas que certifiquen esa correspondencia; las respaldadas por otros criptoactivos, sobreg-arantizadas para absorber la volatilidad del activo que las respalda; y las llamadas algorítmicas, que intentan mantener su valor mediante mecanismos puramente automáticos de oferta y demanda sin una reserva real detrás, un modelo que ha protagonizado algunos de los colapsos más sonados del sector, como el de TerraUSD en 2022, que perdió su vínculo con el dólar en cuestión de días y arrastró consigo decenas de miles de millones de dólares.

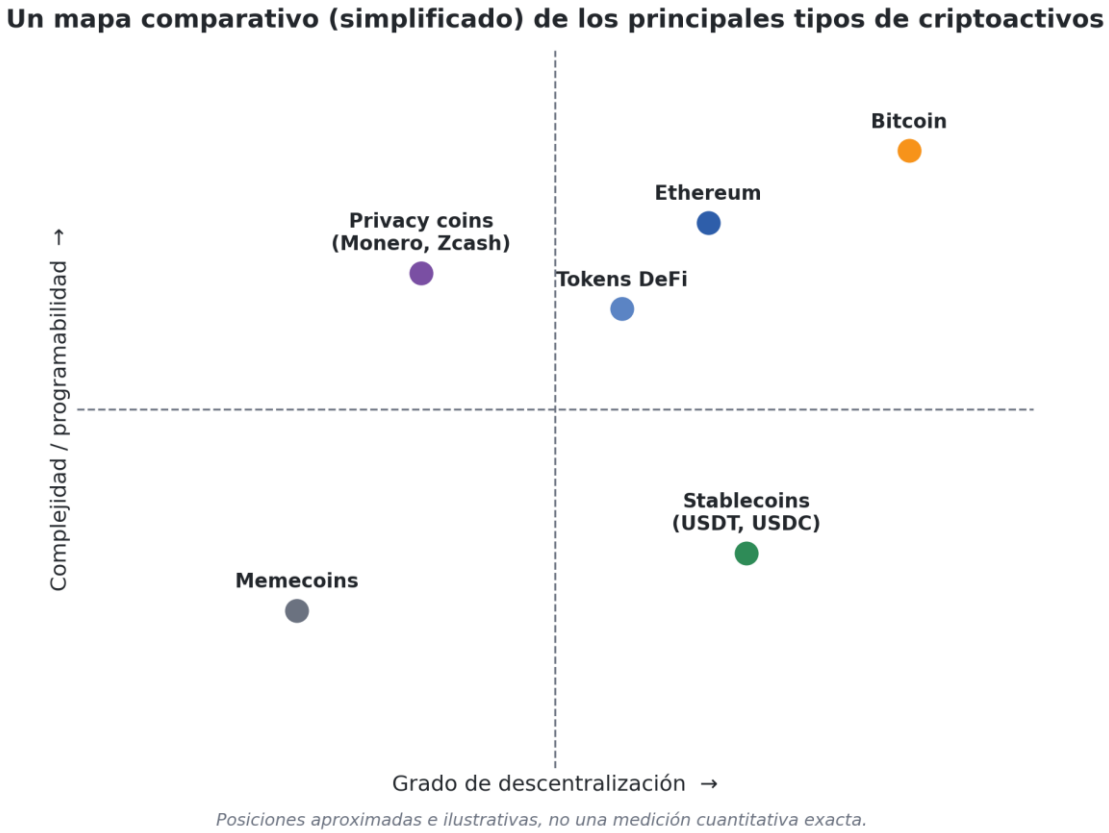
El peso de las stablecoins en el conjunto del ecosistema es, hoy, considerable: a mediados de 2026, su capitalización conjunta ronda los 300.000 millones de dólares, liderada con claridad por Tether (USDT), con en torno a 185.000-190.000 millones de dólares en circulación, y USD Coin (USDC), con unos 75.000 millones, que entre ambas concentran cerca del 90% de todo el mercado. Su función principal no es la especulación, sino servir de "puerto seguro" dentro del propio ecosistema cripto: un trader puede refugiarse en una stablecoin durante una caída de precio sin tener que salir por completo del ecosistema cripto de vuelta a su banco tradicional, y buena parte del volumen de negociación diario de Bitcoin y otros criptoactivos se produce, de hecho, contra stablecoins, no contra dólares o euros directamente. El Reglamento MiCA que hemos mencionado repetidamente a lo largo del libro (capítulos 24, 29 y 34) dedica un régimen específico y particularmente estricto a las stablecoins -llamadas allí "fichas referenciadas a activos" o "fichas de dinero electrónico"-, exigiendo reservas líquidas, auditorías y límites a su uso como medio de pago masivo dentro de la Unión Europea, precisamente por el riesgo sistémico que podría suponer un colapso de una stablecoin de gran tamaño para la estabilidad financiera general.

¿Qué son las DeFi y los DAO, y qué otros tipos de criptoactivos existen además de Bitcoin?

Las finanzas descentralizadas, o DeFi (decentralized finance), son el conjunto de aplicaciones construidas con contratos inteligentes que replican servicios financieros tradicionales -préstamos, intercambio de activos, seguros, mercados de derivados- sin bancos, brókers ni cámaras de compensación centralizadas: el contrato inteligente, publicado y auditable por cualquiera, sustituye a la institución financiera. Una DAO (organización autónoma descentralizada) aplica una lógica parecida a la gobernanza: en lugar de un consejo de administración tradicional, las decisiones -qué proyectos financiar, qué cambios aprobar- se someten a votación entre los poseedores de un token de gobernanza, y los resultados se ejecutan automáticamente mediante contratos inteligentes. Ambos conceptos son casi exclusivos del ecosistema de Ethereum y de plataformas similares, no de Bitcoin, precisamente por la limitación deliberada de programabilidad que describimos más arriba.

Más allá de Ethereum y las stablecoins, el resto del universo de criptoactivos -con más de veinte mil proyectos catalogados, como ya apuntamos en la siguiente pregunta- se agrupa en categorías bastante heterogéneas en cuanto a legitimidad y riesgo: las plataformas de contratos inteligentes alternativas a Ethereum (como Solana o Cardano, que compiten sobre todo en velocidad de transacción y coste); las soluciones de "capa 2", cadenas construidas encima de una principal para aumentar su capacidad sin comprometer su seguridad base, un

concepto que ya conoces de la red Lightning de Bitcoin; las monedas de privacidad, diseñadas para ofrecer un anonimato real que Bitcoin, como vimos en el capítulo 33, no proporciona por defecto; los tokens de gobernanza de proyectos DeFi concretos; y, en el extremo de mayor riesgo, las llamadas memecoins, criptoactivos creados a menudo como broma o fenómeno viral, sin ningún desarrollo tecnológico real detrás, cuyo valor depende casi por completo de la especulación y las modas de las redes sociales, y que concentran una parte muy desproporcionada de los esquemas de "pump and dump" que ya describimos en el capítulo 33. La regla general que se desprende de todo el libro aplica aquí con más fuerza que nunca: cuanto más se aleja un criptoactivo de la simplicidad, la transparencia y el historial de Bitcoin, mayor es, en términos estadísticos, el riesgo de que se trate de un proyecto especulativo, mal diseñado o directamente fraudulento.



Un mapa comparativo simplificado de los principales tipos de criptoactivos mencionados en este capítulo.

¿Por qué algunos dicen que Bitcoin es "oro digital"?

La etiqueta "oro digital", que exploramos en profundidad en el capítulo 29 al comparar Bitcoin con el oro físico, resume la tesis de que Bitcoin cumple, en el mundo digital, una función equivalente a la que el oro ha cumplido durante milenios en el mundo físico: una reserva de valor con oferta limitada y verificable, independiente de la voluntad de cualquier gobierno o banco central, capaz de proteger el patrimonio de quien lo posee frente a la devaluación de las monedas fiduciarias. A diferencia de la inmensa mayoría de las más de veinte mil criptomonedas que existen hoy, cuya oferta puede en muchos casos ampliarse o cuyo protocolo puede modificarse con relativa facilidad por parte de sus creadores, Bitcoin comparte con el oro esa propiedad de escasez verdaderamente rígida, que ningún otro criptoactivo replica con el mismo nivel de garantía ni de consenso social.

Conviene matizar, no obstante, que se trata de una etiqueta sobre las propiedades a largo plazo del activo, no una garantía de que su comportamiento de precio a corto plazo vaya a parecerse al del oro: como ilustramos con datos de 2026 en el capítulo 29, Bitcoin puede caer con mucha más fuerza que el oro incluso en periodos en los que este se mantiene estable, precisamente por su mercado todavía mucho más pequeño y su historia mucho más corta. "Oro digital" describe, por tanto, una aspiración y un argumento de fondo, no una equivalencia total y ya consolidada entre ambos activos.

¿Qué relación tiene Bitcoin con los NFT y otras aplicaciones de blockchain?

Los NFT (tokens no fungibles, por sus siglas en inglés) son certificados digitales de propiedad únicos, habitualmente asociados a obras de arte digital, coleccionables o activos virtuales, que se construyen casi siempre sobre la cadena de bloques de Ethereum o de otras plataformas con capacidad de ejecutar contratos inteligentes, no sobre la de Bitcoin, cuyo protocolo fue diseñado con un propósito mucho más limitado y específico: mover valor de forma segura, no gestionar activos digitales complejos y únicos. Existen, es cierto, algunas soluciones técnicas más recientes que permiten crear activos similares a los NFT directamente sobre la cadena de Bitcoin (como el protocolo Ordinals), pero se trata de desarrollos periféricos y controvertidos dentro de la propia comunidad de Bitcoin, no de una función central del protocolo.

Esta distinción es importante porque buena parte de la cobertura mediática de los últimos años ha tendido a mezclar, bajo la etiqueta genérica de "cripto", fenómenos muy distintos entre sí: la caída de precio de un proyecto de NFT concreto, el fraude de una aplicación descentralizada mal diseñada, o la quiebra de un exchange que operaba con múltiples criptoactivos, no dicen necesariamente nada sobre la solidez o el funcionamiento del protocolo de Bitcoin en sí mismo, del mismo modo que la quiebra de una empresa puntocom en el año 2000 no invalidaba el funcionamiento técnico de internet como tecnología.

¿Tiene sentido aprender primero Bitcoin antes de meterse en el resto de criptomonedas?

Desde un punto de vista puramente educativo, sí tiene bastante sentido, y es el enfoque que sigue este propio libro. Bitcoin fue la primera criptomoneda y sigue siendo, con diferencia, el proyecto con la comunidad más grande, la mayor capitalización de mercado, la infraestructura reguladora más desarrollada (capítulo 29) y la documentación técnica y académica más extensa; entender bien sus conceptos fundamentales -la cadena de bloques, la minería, las wallets, la escasez programada- te da una base sólida que se aplica, con matices, a la comprensión de la inmensa mayoría del resto del ecosistema cripto.

Desde un punto de vista de inversión, la cuestión es distinta y merece una precisión importante: el resto de criptomonedas (a menudo llamadas "altcoins", es decir, alternativas a Bitcoin) presentan, en conjunto, un perfil de riesgo considerablemente más alto que Bitcoin, con una volatilidad todavía mayor, una liquidez menor y, en un porcentaje muy significativo de los casos, sin ningún desarrollo tecnológico real detrás del proyecto ni intención duradera por parte de sus creadores. La recomendación implícita de la práctica totalidad de las guías de educación financiera sobre criptoactivos es clara en este sentido: si decides invertir, entender primero Bitcoin -el proyecto más establecido, más estudiado y con la infraestructura

regulatoria más madura- antes de aventurarse en proyectos más pequeños y especulativos reduce de forma significativa el riesgo de caer en los esquemas fraudulentos que analizamos en el capítulo 26.

Fuentes y estudios citados en este capítulo

- Buterin, V. (2014). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", documento técnico original de Ethereum.
- Documentación técnica sobre el cambio de Ethereum de Proof-of-Work a Proof-of-Stake ("The Merge", 2022), Ethereum Foundation.
- CoinMarketCap y CoinGecko, datos comparativos de capitalización de mercado entre Bitcoin y el resto de criptoactivos, citados también en capítulos anteriores.
- Banco Central Europeo. Informes sobre el funcionamiento y los riesgos de las stablecoins dentro del marco del Reglamento MiCA.
- DefiLlama y StableCoin.com, datos de capitalización agregada de stablecoins y cuota de mercado de USDT y USDC, julio de 2026.
- Documentación técnica de Discrete Log Contracts (DLC) y del protocolo RGB, comunidad de desarrollo de Bitcoin.
- Cobertura periodística y análisis técnico del colapso de TerraUSD y su token asociado LUNA, mayo de 2022, citado como ejemplo de stablecoin algorítmica fallida.

Capítulo 38. Futuro y contexto económico

Este último bloque de preguntas frecuentes cierra el recorrido mirando hacia adelante: qué papel podría jugar Bitcoin en el sistema económico global en las próximas décadas, retomando y sintetizando ideas ya desarrolladas en capítulos anteriores del libro.

¿Podría Bitcoin llegar a sustituir al dinero tradicional emitido por los bancos centrales?

Es uno de los debates más antiguos dentro de la propia comunidad de Bitcoin, y la respuesta mayoritaria entre los analistas serios, con independencia de su postura sobre el proyecto, es que una sustitución completa a corto o medio plazo resulta muy improbable, aunque no imposible a un plazo mucho más largo. Los obstáculos prácticos son considerables: la volatilidad de precio que describimos en el bloque de precio e inversión lo hace, hoy por hoy, poco funcional como unidad de cuenta estable para fijar salarios, precios o contratos a largo plazo; la capacidad de procesamiento de la red principal es limitada en comparación con los sistemas de pago centralizados actuales, aunque soluciones como la red Lightning (capítulo 21) mitigan buena parte de ese problema; y ningún gobierno importante ha mostrado, hasta la fecha, intención real de renunciar a su moneda nacional y a las herramientas de política monetaria que esta le proporciona.

Un escenario bastante más plausible, y que ya está ocurriendo de forma parcial, es el de la coexistencia: Bitcoin funcionando como un activo de reserva de valor complementario al sistema monetario tradicional -de forma similar al papel que hoy juega el oro en las reservas de muchos bancos centrales-, en lugar de sustituir por completo al dinero fiduciario en su función de medio de pago cotidiano. El propio caso de El Salvador, que probó la sustitución parcial mediante su ley de curso legal obligatorio en 2021 y terminó revirtiendo esa obligación en 2025 (bloque de legalidad) mientras mantenía su reserva estatal de bitcoin, ilustra bien esta distinción entre "sustituir el dinero del día a día" y "sostener parte del ahorro a largo plazo", que son dos preguntas económicas bastante distintas.

¿Qué impacto tiene Bitcoin en la inflación, las crisis financieras y el sistema económico actual?

El impacto directo de Bitcoin sobre la inflación general de una economía como la española o la europea es, hoy por hoy, marginal: su tamaño de mercado, aunque ha crecido enormemente, sigue siendo pequeño en comparación con la masa monetaria total de las principales economías del mundo, y no forma parte de los indicadores ni de las herramientas que utilizan los bancos centrales para fijar su política monetaria. El impacto que sí tiene, y que fue precisamente su motivación fundacional (capítulo 4), es de naturaleza distinta: ofrecer a quien lo desee una alternativa cuya oferta no puede ampliarse por decisión de un banco central, lo que sus defensores presentan como una protección personal frente a la pérdida de poder adquisitivo del ahorro en episodios de alta inflación o de políticas monetarias muy expansivas, como ocurrió tras la crisis de 2008 o durante la pandemia.

Sobre las crisis financieras, Bitcoin todavía no ha atravesado un ciclo económico completo de una gravedad comparable a la de 2008 con el tamaño de mercado y de adopción institucional que tiene hoy, por lo que su comportamiento en un escenario de ese tipo sigue siendo, en gran medida, una incógnita: en episodios de estrés de mercado más recientes se

ha comportado en ocasiones como un activo de refugio y en otras como un activo de riesgo del que los inversores huyen junto con otros activos volátiles, sin un patrón todavía plenamente consistente, algo que analizamos también en el capítulo 29 al hablar del riesgo de mercado.

¿Qué pasará con Bitcoin cuando se haya minado el último bloque y no queden Bitcoins nuevos por crear?

Según el calendario de emisión fijado en el protocolo (capítulo 13), se estima que el último satoshi se minará hacia el año 2140, un horizonte todavía muy lejano. A partir de ese momento, los mineros dejarán de recibir la recompensa de bitcoins de nueva creación que hoy constituye buena parte de su ingreso, y su actividad -y con ella, la seguridad de toda la red, sostenida por la Prueba de Trabajo (capítulo 35)- pasará a depender exclusivamente de las comisiones que paguen los usuarios por cada transacción incluida en un bloque.

Este es uno de los grandes interrogantes de largo plazo sobre la sostenibilidad económica de Bitcoin, y no existe un consenso absoluto sobre cómo se resolverá: los más optimistas argumentan que, para entonces, el volumen de transacciones y el valor de cada una serán lo suficientemente altos como para que las comisiones por sí solas sigan haciendo rentable la minería, especialmente si buena parte de las transacciones cotidianas se han trasladado a capas secundarias como la red Lightning y solo las operaciones de mayor valor se liquidan directamente en la cadena principal; los más escépticos señalan que se trata de una incógnita real sobre la que solo cabe especular, dado que faltan más de cien años para que el escenario se materialice y ninguna proyección económica a tan largo plazo puede considerarse fiable.

¿Cómo afecta que entren grandes fondos de inversión y empresas al mercado de Bitcoin?

La entrada de grandes gestoras de fondos como BlackRock, cuyo fondo cotizado de Bitcoin al contado (IBIT) gestionaba en 2026 activos por valor de más de cincuenta mil millones de dólares, en torno a la mitad de todo el mercado estadounidense de ETF de Bitcoin, ha tenido varios efectos observables. Por un lado, ha aportado una vía de acceso regulada y familiar para inversores institucionales y particulares que antes no estaban dispuestos a operar directamente en un exchange de criptoactivos, ampliando de forma considerable la base de capital que puede fluir hacia Bitcoin; por otro, ha aumentado la correlación entre el precio de Bitcoin y los flujos de entrada y salida de estos productos financieros tradicionales, hasta el punto de que, según estimaciones de mercado de 2026, los flujos de los ETF explican en torno a un 45% de los movimientos semanales de precio, un nivel de influencia que no existía antes de su aprobación.

Este proceso, que ya analizamos en detalle a propósito de Michael Saylor y Strategy en el capítulo 24, tiene también sus críticos: quienes valoran ante todo la descentralización y la independencia de Bitcoin frente al sistema financiero tradicional (capítulo 27) ven con cierta inquietud que una proporción creciente del activo termine concentrada en manos de un número relativamente reducido de grandes gestoras e instituciones, lo que en teoría podría reintroducir, de forma indirecta, parte de la concentración de poder financiero que Bitcoin fue diseñado para evitar, aunque la propiedad subyacente del bitcoin, a diferencia del oro en una cámara acorazada bancaria, sigue siendo verificable de forma pública e independiente por cualquiera en la cadena de bloques.

¿Cómo influye y va a influir la inteligencia artificial en Bitcoin?

Es una de las preguntas más recientes de este libro, y también una de las que más rápido está evolucionando: la relación entre la inteligencia artificial y Bitcoin se despliega, a día de hoy, en al menos cuatro frentes distintos y bastante independientes entre sí, que conviene separar con cuidado en lugar de tratarlos como un único fenómeno.

Cuatro frentes, en gran medida independientes, en los que confluyen hoy la inteligencia artificial y Bitcoin.

El primero, y quizá el más disruptivo a medio plazo, es el de los agentes de inteligencia artificial que pagan de forma autónoma. Hasta hace muy poco, cualquier pago requería, en algún punto de la cadena, la intervención de una persona: introducir una tarjeta, aprobar una transferencia, confirmar una suscripción. Los agentes de IA -programas capaces de actuar de forma autónoma para cumplir un objetivo, por ejemplo comprando datos, contratando capacidad de cómputo o accediendo a un servicio de pago por uso- necesitan una infraestructura de pago que no dependa de esa aprobación humana constante, que liquide de forma prácticamente instantánea y que funcione con importes tan pequeños que una comisión bancaria tradicional los haría inviables. En febrero de 2026, Lightning Labs, una de las empresas más importantes en el desarrollo de la red Lightning (capítulo 21), publicó en abierto un conjunto de herramientas que permite a agentes de IA operar de forma nativa sobre esa red: mantener saldo, recibir y enviar pagos, y contratar de forma autónoma acceso a APIs o a otros servicios digitales sin necesidad de una cuenta bancaria ni de una tarjeta de crédito asociada a una persona física. La combinación de las propiedades que ya conoces de Bitcoin y Lightning -pagos instantáneos, sin necesidad de autorización de un tercero, con comisiones mínimas incluso para importes muy pequeños (capítulo 36)- encaja de forma casi natural con las necesidades de lo que ya se empieza a llamar la "economía de las máquinas": dispositivos y programas que pagan, y cobran, entre sí sin intervención humana directa.

El segundo frente, muy distinto, es la creciente competencia -y en muchos casos colaboración- entre la minería de Bitcoin y los centros de datos dedicados a la inteligencia artificial por los mismos recursos: electricidad barata, terrenos con buena conectividad e infraestructura de refrigeración industrial. Desde finales de 2025, y de forma muy acelerada durante 2026, un número significativo de las mayores empresas mineras de Bitcoin ha reorientado una parte sustancial de su capacidad hacia el alquiler de infraestructura de computación de alto rendimiento (HPC) para entrenar e implementar modelos de inteligencia artificial, firmando contratos plurianuales por decenas de miles de millones de dólares combinados con empresas tecnológicas como Microsoft, CoreWeave o Google. La razón de fondo es puramente económica: el coste de producir un bitcoin ha llegado a superar, para buena parte de los mineros públicos, el propio precio de mercado del activo, mientras que alquilar esa misma infraestructura eléctrica e industrial a empresas de inteligencia artificial ofrece, en 2026, márgenes operativos sustancialmente más altos y contratos a largo plazo mucho más predecibles que la minería tradicional. Este giro plantea una pregunta legítima sobre la seguridad futura de la red: si una parte relevante de la capacidad industrial que hoy sostiene el hashrate de Bitcoin (capítulo 8) se reorienta de forma permanente hacia la IA, la seguridad de la red dependerá de que ese hashrate se redistribuya de forma suficientemente amplia entre otros operadores, en lugar de concentrarse todavía más, un matiz que conecta directamente con el riesgo del ataque del 51% que analizamos en el capítulo 9.

El tercer frente es el del propio mercado y el comportamiento de los precios. Los algoritmos de trading basados en inteligencia artificial, capaces de analizar noticias, redes sociales y patrones históricos de precio a una velocidad muy superior a la de cualquier operador humano, representan hoy una proporción creciente del volumen de negociación diario de Bitcoin, lo que según algunos analistas podría estar amplificando -no reduciendo- la velocidad y la intensidad de los movimientos de precio a corto plazo que describimos en el bloque de precio e inversión, precisamente porque muchos de estos sistemas tienden a reaccionar de forma parecida ante las mismas señales, generando movimientos en cascada. Al mismo tiempo, la propia inteligencia artificial se ha convertido en una herramienta habitual dentro de la propia industria de la minería, optimizando el diseño de nuevos chips ASIC (capítulo 11) y la gestión energética de las instalaciones industriales para maximizar su eficiencia.

El cuarto frente, más preocupante, es el de la seguridad: la inteligencia artificial generativa ha hecho mucho más sofisticados y más difíciles de detectar los fraudes que ya describimos en los capítulos 18 y 33 -deepfakes de figuras públicas o de conocidos que promocionan falsamente inversiones en Bitcoin, mensajes de phishing redactados sin ninguno de los errores que antes ayudaban a detectarlos, e ingeniería social automatizada a una escala que ningún equipo humano de estafadores podría alcanzar por sí solo-, lo que exige de cualquier usuario un nivel de escepticismo todavía mayor del que ya recomendábamos en aquellos capítulos ante cualquier oferta, mensaje o vídeo relacionado con Bitcoin que parezca demasiado convincente. A más largo plazo, y de forma todavía especulativa, algunos investigadores han empezado a vincular los avances en inteligencia artificial con la aceleración del riesgo de computación cuántica que ya mencionamos en el capítulo 20, en la medida en que la IA puede ayudar a optimizar los propios algoritmos cuánticos, aunque se trata, por ahora, de un riesgo compuesto y todavía lejano, no de una amenaza inminente.

En conjunto, ninguno de estos cuatro frentes sustituye ni transforma la naturaleza fundamental de Bitcoin como protocolo -sus reglas de emisión, su seguridad criptográfica y su descentralización, descritas a lo largo de todo este libro, no dependen de la inteligencia

artificial ni se ven alteradas por ella-, pero sí están cambiando, y previsiblemente seguirán cambiando con rapidez, quién y cómo interactúa con la red: menos personas pulsando botones, más programas autónomos moviendo valor por su cuenta; menos mineros compitiendo solo entre sí, más infraestructura compartida con la industria de la inteligencia artificial; y un entorno de fraude más sofisticado que exige, más que nunca, la misma prudencia que este libro ha repetido en cada capítulo dedicado a la seguridad.

¿Seguirá existiendo Bitcoin dentro de 20 o 30 años o puede ser reemplazado por otra tecnología?

Nadie puede responder con certeza a esta pregunta, y cualquiera que lo afirme con absoluta seguridad -en cualquiera de los dos sentidos- está haciendo una predicción, no una constatación de hechos. Lo que sí puede decirse, con base en la evolución histórica del propio proyecto, es que Bitcoin ha demostrado hasta la fecha una resiliencia considerable: ha sobrevivido a caídas de precio de más del ochenta por ciento, a la prohibición completa de su minería en China, a la quiebra de algunos de sus mayores intermediarios (Mt. Gox, FTX), y a innumerables predicciones de su desaparición inminente a lo largo de más de quince años, emergiendo cada vez con una base de usuarios, desarrolladores y capital institucional mayor que la anterior.

Los factores que jugarían a favor de su continuidad a largo plazo incluyen el llamado "efecto de red" -cuantas más personas, empresas e instituciones lo usan y lo aceptan, más valioso y más difícil de sustituir se vuelve, un fenómeno similar al que hace difícil desplazar a un estándar tecnológico ya establecido-, y la ventaja de ser el proyecto más antiguo, más probado y más ampliamente reconocido dentro de su categoría, algo comparable al papel de referencia dominante que sigue ocupando el oro entre los metales preciosos pese a la existencia de la plata o el platino. Los factores que jugarían en contra incluyen, como reconocemos a lo largo del libro, los riesgos tecnológicos de muy largo plazo como la computación cuántica (capítulo 20), la posibilidad de un desarrollo regulatorio global mucho más hostil del que existe hoy, o, simplemente, que dentro de varias décadas surja una tecnología capaz de ofrecer las mismas ventajas con menos inconvenientes. Con la información disponible en 2026, lo más honesto que puede decirse es que Bitcoin ha superado, hasta ahora, cada prueba de resistencia a la que se ha visto sometido, sin que eso constituya ninguna garantía sobre su próxima década, y mucho menos sobre las tres siguientes.

Fuentes y estudios citados en este capítulo

- BlackRock. Datos públicos de activos bajo gestión (AUM) del fondo iShares Bitcoin Trust (IBIT), 2026.
- Cobertura de mercado sobre los flujos de entrada y salida de los ETF de Bitcoin al contado y su correlación con el precio, 2026.
- Ley Bitcoin de El Salvador (2021) y su posterior reforma (2025), y acuerdo entre El Salvador y el Fondo Monetario Internacional (diciembre de 2024), citados también en el capítulo 34.
- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sobre el calendario de emisión y el límite de 21 millones de unidades, citado también en los capítulos 13 y 35.

- Lightning Labs. "lightning-agent-tools", herramientas de código abierto para pagos autónomos de agentes de IA sobre la red Lightning, publicadas en febrero de 2026.
- Cobertura periodística y financiera (CoinDesk, The Block, Bitcoin Magazine) sobre la reorientación de empresas mineras de Bitcoin hacia contratos de computación de alto rendimiento (HPC) para inteligencia artificial durante 2026, incluidos los casos de Core Scientific, TeraWulf, Hut 8, Cipher e IREN.
- Análisis de mercado sobre el peso del trading algorítmico y basado en inteligencia artificial en el volumen de negociación de criptoactivos, 2026.

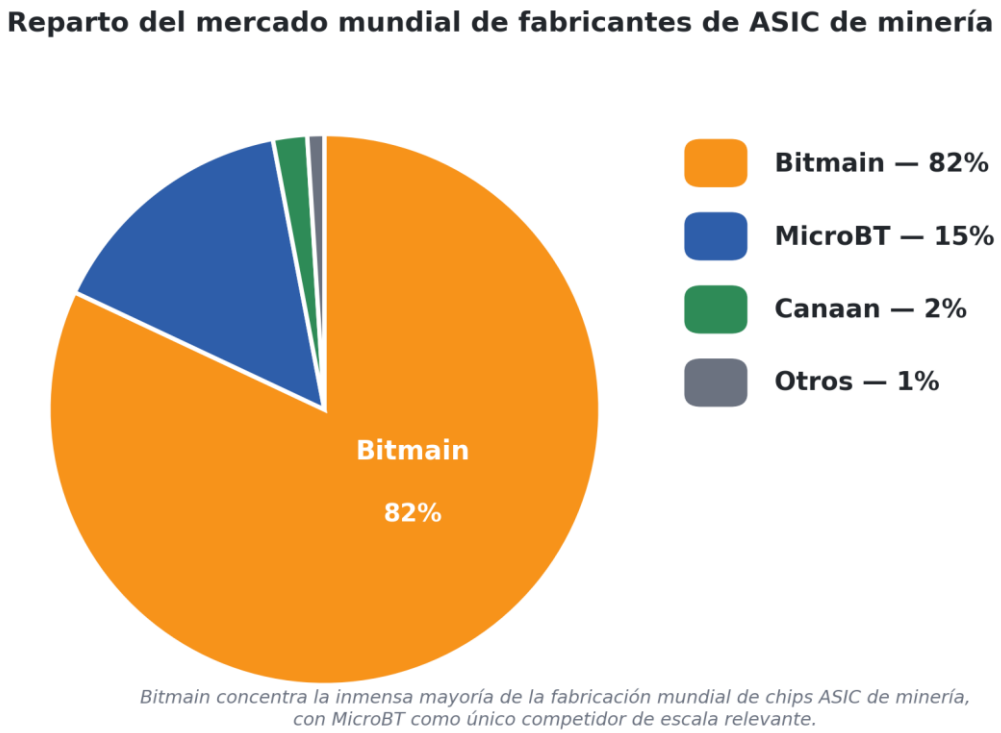
Capítulo 39. Minería de Bitcoin en profundidad

El capítulo 35 ya respondió las preguntas más básicas sobre la minería: qué es, cuánto cuesta, dónde se concentra geográficamente y cómo funcionan los pools. Este capítulo adicional profundiza en tres aspectos que merecen un espacio propio: quién fabrica el hardware que hace posible toda esa industria, de dónde sale realmente la energía que consume y qué ocurrirá con la seguridad de la red cuando, dentro de más de un siglo, deje de existir la recompensa de bloque tal y como la conocemos hoy.

¿Quién fabrica el hardware de minería y cómo funciona ese mercado?

El mercado de fabricación de ASIC para minería de Bitcoin es, en la práctica, un oligopolio muy concentrado: tres empresas -todas ellas de origen chino- controlan, entre las tres, más del 99% de la producción mundial. Bitmain, la mayor y más veterana, fabrica aproximadamente el 82% de todo el hardware de minería del mundo bajo su marca Antminer; MicroBT, su principal competidor, produce en torno al 15% con su línea Whatsminer; y Canaan, la tercera en discordia y una de las pocas cotizadas en bolsa de las tres, se queda con apenas un 2% del mercado. Esta concentración extrema no es casual: diseñar y fabricar un ASIC competitivo exige un acceso a procesos de fabricación de semiconductores de última generación -los mismos que usan los fabricantes de procesadores para móviles y ordenadores- y un volumen de pedidos que solo un puñado de empresas en el mundo puede permitirse negociar directamente con las grandes fundiciones de chips como TSMC.

Esta concentración geográfica e industrial ha generado, en los últimos años, una tensión comercial y política adicional: las tensiones arancelarias entre Estados Unidos y China han llevado a Bitmain y a otros fabricantes a anunciar, desde 2025, la apertura de plantas de ensamblaje en territorio estadounidense, en un intento de esquivar los aranceles que gravan la importación de hardware fabricado íntegramente en Asia y de acercarse a su mercado de clientes más importante, dado que Estados Unidos concentra, como vimos en el capítulo 35, más de un tercio del hashrate mundial. Este desplazamiento parcial de la fabricación no altera, de momento, la concentración del mercado en manos de las mismas tres empresas, pero sí ilustra hasta qué punto la geopolítica y el comercio internacional -no solo la tecnología- condicionan una industria que, en su día, se presentó como completamente descentralizada y ajena a las fronteras nacionales.



Reparto del mercado mundial de fabricación de ASIC de minería (2026).

Esta concentración en la fabricación plantea una pregunta legítima sobre la seguridad de la red que conviene distinguir con cuidado de la concentración en la minería propiamente dicha que vimos en el capítulo 35: un fabricante de hardware no controla, por el mero hecho de venderlo, la potencia de cálculo de las máquinas una vez compradas y operadas por miles de mineros independientes en todo el mundo, del mismo modo que un fabricante de coches no controla las decisiones de conducción de quienes los compran. Aun así, la comunidad de Bitcoin ha expresado en distintas ocasiones su incomodidad con la dependencia de un número tan reducido de fabricantes, y existen iniciativas de código abierto -como los proyectos de diseño de ASIC libres impulsados por organizaciones sin ánimo de lucro del ecosistema- que buscan, con un éxito todavía limitado, diversificar ese mercado a largo plazo.

¿De dónde sale la energía que usa la minería y qué tan "verde" es realmente?

El debate sobre el consumo energético de Bitcoin, que introdujimos en el capítulo 28, ha ido incorporando datos cada vez más precisos gracias al trabajo de instituciones académicas independientes, en particular el Centro de Cambridge para las Finanzas Alternativas (CCAF), cuyo informe de referencia de abril de 2025 -elaborado a partir de una encuesta directa a 49 empresas mineras en 16 jurisdicciones distintas, que en conjunto representan cerca del 48% del hashrate mundial- ofrece la fotografía más rigurosa disponible hasta la fecha. Según ese informe y sus actualizaciones de 2026, el consumo total de la red de Bitcoin se sitúa en torno a 138 teravatios-hora al año, una cifra comparable, según el punto de referencia que se use, al consumo eléctrico de un país de tamaño mediano.

Lo que ha cambiado de forma más notable en los últimos años es la composición de esa energía: en 2026, aproximadamente el 52,4% de la electricidad que consume la minería de

Bitcoin procede de fuentes de cero emisiones, frente a apenas el 37,6% en 2022, un incremento sustancial en un periodo relativamente corto. Ese 52,4% se reparte, a su vez, entre un 42,6% de fuentes renovables propiamente dichas -hidroeléctrica (23,4%, la mayor de todas, coherente con la concentración de minería en países como Canadá, Paraguay y Etiopía que vimos en el capítulo 35), eólica (15,4%) y solar (3,2%)- y un 9,8% de energía nuclear, que aunque no es renovable en sentido estricto, sí se considera de bajas emisiones de carbono.

Composición de la energía usada por la minería de Bitcoin (2026)

52,4% procede de fuentes de cero emisiones (renovables + nuclear), frente al 37,6% en 2022.
Fuente: Cambridge Centre for Alternative Finance (CCAF).

Composición de la energía usada por la minería de Bitcoin en 2026, según el CCAF.

Este dato matiza, sin resolverlo del todo, el debate que presentamos con las dos caras en el capítulo 28: los defensores de Bitcoin señalan esta tendencia ascendente como prueba de que la propia lógica económica de la minería -buscar la electricidad más barata posible, que suele coincidir con excedentes renovables o hidroeléctricos poco aprovechados- empuja al sector hacia fuentes cada vez más limpias sin necesidad de imponerlo por regulación; los críticos, por su parte, insisten en que incluso la energía de origen renovable tiene un coste de oportunidad, porque esa misma electricidad podría destinarse a otros usos -viviendas, industria, transporte eléctrico- en lugar de a una actividad cuyo valor social sigue siendo objeto de debate. Ambos argumentos, como ya señalamos en el capítulo 28, contienen elementos válidos y no se cancelan mutuamente.

¿Qué pasará con la minería cuando ya no haya recompensa de bloque?

Como explicamos en el capítulo 13 y de nuevo en el capítulo 35, la recompensa que reciben los mineros por cada bloque se reduce a la mitad cada aproximadamente cuatro años, hasta llegar, según las proyecciones actuales del protocolo, a un valor tan pequeño que hacia el año 2140 se considerará agotada la emisión de nuevos bitcoins. Esto plantea una pregunta legítima sobre el largo plazo, que los críticos de Bitcoin citan con cierta frecuencia: si los mineros dejan de recibir bitcoins nuevos como incentivo, ¿qué les seguirá motivando a dedicar electricidad y hardware a proteger la red mediante Proof-of-Work?

La respuesta que ofrece el propio diseño del protocolo es que las comisiones de transacción, que hoy representan una parte todavía minoritaria de los ingresos de un minero frente a la recompensa de bloque, están llamadas a convertirse en la fuente principal -y con el tiempo, única- de esos ingresos, sustituyendo gradualmente a la recompensa de nuevas unidades a medida que esta se reduce con cada halving sucesivo. Que ese mercado de comisiones sea suficiente, por sí solo, para mantener un nivel de seguridad de la red comparable al actual es, sin embargo, una cuestión abierta y objeto de debate entre economistas e investigadores del

protocolo: depende de que el volumen de transacciones y, sobre todo, la demanda de espacio en los bloques -limitada por diseño, como vimos en el capítulo 13- sea suficientemente alta como para generar comisiones que compensen económicamente a los mineros sin la ayuda de la emisión de nuevas unidades. Se trata de un escenario a más de un siglo vista, por lo que ningún analista serio presenta hoy una respuesta definitiva, pero conviene que el lector sepa que es una de las incertidumbres de largo plazo que la propia comunidad técnica de Bitcoin reconoce abiertamente, no un problema oculto o ignorado.

Fuentes y estudios citados en este capítulo

- Cambridge Centre for Alternative Finance (CCAF). "Digital Mining Industry Report" (abril de 2025) y actualizaciones de 2026, citado también en el capítulo 28 sobre el consumo energético de la minería.
- MEXC News, "Bitmain Statistics 2026: Trends That Matter Now" (2026); Coherent Market Insights, "Cryptocurrency Mining Equipment Market Size, Trends & Forecast, 2026-2033", sobre el reparto del mercado de fabricantes de ASIC.
- Cointelegraph, "Chinese Bitcoin ASIC makers to begin US production amid tariff pressure" (2025-2026), sobre el traslado parcial de la fabricación de hardware a Estados Unidos.
- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", sobre el diseño a largo plazo del mercado de comisiones, citado también en los capítulos 5, 13, 30 y 35.

Capítulo 40. Bitcoin City y las ciudades cripto en el mundo

El capítulo 24 introdujo Bitcoin City, el proyecto salvadoreño de ciudad libre de impuestos financiada con "bonos volcán". Este bloque amplía esa historia y la sitúa dentro de un fenómeno más amplio: el intento, por parte de distintos promotores privados y gobiernos, de construir ciudades o zonas económicas especiales diseñadas específicamente en torno a Bitcoin y a los principios de baja regulación y baja fiscalidad que sus impulsores asocian con él.

¿Qué es exactamente una "ciudad cripto" y por qué han proliferado estos proyectos?

Una ciudad cripto, en el sentido en que se usa habitualmente este término, no es simplemente una ciudad donde se puede pagar con Bitcoin -algo que, en mayor o menor medida, ya es posible en muchas ciudades del mundo-, sino un proyecto urbanístico y legal diseñado desde el principio para atraer a empresas y residentes relacionados con el sector cripto mediante una combinación específica de baja o nula fiscalidad, un marco regulatorio simplificado y, a menudo, cierto grado de autonomía legal respecto del país que las alberga. La lógica que comparten casi todos estos proyectos es la misma que ya vimos a propósito de los países con fiscalidad favorable en el capítulo 34: si un territorio ofrece condiciones sustancialmente mejores que las de su entorno, puede atraer capital, talento y actividad económica que de otro modo iría a otra parte, una estrategia de competencia fiscal entre jurisdicciones que no es exclusiva de Bitcoin -los paraísos fiscales tradicionales llevan aplicándola décadas- pero que el sector cripto ha adoptado con un entusiasmo particular, en parte por la afinidad ideológica entre buena parte de su comunidad fundadora y las ideas de menor intervención estatal que analizamos en el capítulo 27.

Bitcoin City (El Salvador): recapitulación y estado actual

Como detallamos en el capítulo 24, Bitcoin City es el proyecto más conocido de este tipo: una ciudad planificada junto al volcán de Conchagua, financiada en parte con los "bonos volcán" emitidos a finales de 2024, con el objetivo de convertirse en una zona económica especial sin impuestos directos salvo el IVA, alimentada por energía geotérmica volcánica. A mediados de 2026, el proyecto se encuentra en una fase de desarrollo de infraestructura básica -carreteras, red eléctrica, telecomunicaciones- más que en la construcción de la ciudad propiamente dicha, con un desfase notable entre los anuncios oficiales y lo que los reportajes sobre el terreno han podido verificar de forma independiente, un patrón que conviene tener presente al valorar cualquier proyecto de este tipo, incluidos los que se describen en las siguientes preguntas.

Próspera (Honduras): la ciudad chárter que adoptó Bitcoin como unidad de cuenta

Un proyecto distinto pero conceptualmente emparentado es Próspera, una ciudad chárter situada en la isla de Roatán, Honduras, que opera bajo un régimen legal especial conocido como ZEDE (Zona de Empleo y Desarrollo Económico), aprobado por Honduras en la década de 2010 para atraer inversión mediante un marco fiscal y regulatorio propio, con un grado de

autonomía respecto de las leyes hondureñas ordinarias notablemente mayor que el de Bitcoin City. Próspera adoptó Bitcoin como unidad de cuenta para buena parte de su actividad económica interna -incluidas, según sus promotores, las declaraciones fiscales de sus residentes y empresas-, y ofrece un régimen tributario muy reducido, con un impuesto sobre la renta corporativa del 1%, un impuesto sobre la renta personal del 5% y un impuesto sobre el valor de la tierra del 1%. Desde el inicio de su construcción en 2021, el proyecto ha atraído más de 200 empresas y más de 100 millones de dólares en inversión, según sus propios datos, y cuenta entre sus inversores con figuras destacadas del mundo tecnológico y libertario, entre ellas Peter Thiel y Marc Andreessen a través del fondo Pronomos Capital, y, desde enero de 2025, el brazo de capital riesgo de Coinbase.

Bitcoin City y Próspera: comparativa de dos proyectos de ciudad cripto (2026).

A diferencia de Bitcoin City, que es una iniciativa estatal impulsada por el propio gobierno salvadoreño, Próspera es un proyecto de iniciativa privada que opera dentro de un marco legal concedido por el Estado hondureño, lo que la ha hecho vulnerable a los cambios políticos internos del país: el proyecto ha atravesado, desde 2022, varios episodios de tensión legal con distintos gobiernos hondureños que han cuestionado la validez del régimen ZEDE que lo ampara, y a comienzos de 2026 Próspera seguía litigando para intentar recuperar la plenitud de su marco legal original, o en su defecto obtener una compensación económica por los perjuicios sufridos. La llegada a la presidencia de Honduras de un candidato con una postura más favorable a los negocios y con vínculos declarados con la administración estadounidense ha reavivado, según la cobertura periodística más reciente, las expectativas de que el proyecto pueda estabilizar su situación legal, aunque a la fecha de escribir este libro esa evolución seguía siendo incierta.

¿Qué riesgos comparten estos proyectos y qué lecciones ofrecen?

Tanto Bitcoin City como Próspera ilustran, cada una a su manera, la misma tensión estructural: la promesa de construir una ciudad entera en torno a un marco legal y fiscal excepcional depende, en última instancia, de la voluntad política del país anfitrión de

mantener ese marco en el tiempo, algo que ningún promotor privado ni ningún acuerdo internacional puede garantizar de forma absoluta frente a un cambio de gobierno o de mayoría legislativa. Esta es, en cierto modo, una versión concentrada geográficamente del mismo riesgo regulatorio que analizamos país por país en el capítulo 34: las normas pueden cambiar, y cuanto más dependa un proyecto de un régimen legal excepcional y no del marco jurídico ordinario de un país, más expuesto queda a esos cambios.

A esto se suma un segundo riesgo, más práctico, que las investigaciones periodísticas sobre Bitcoin City han puesto de relieve: la distancia frecuente entre el anuncio de un proyecto de esta ambición -con representaciones arquitectónicas atractivas y cifras de inversión prometedoras- y su ejecución material real, que suele ser mucho más lenta, costosa y sujeta a imprevistos de lo que los anuncios iniciales sugieren. Ninguna de estas dos observaciones implica que estos proyectos estén condenados al fracaso -Próspera, pese a sus dificultades legales, ha conseguido atraer inversión y actividad económica real de forma verificable-, pero sí aconsejan, como en tantos otros aspectos de este libro, una lectura escéptica de los anuncios más grandilocuentes hasta que se traducen en resultados comprobables sobre el terreno.

Fuentes y estudios citados en este capítulo

- Global Finance Magazine, "El Salvador: 'Volcano Bonds' Ready Eruption" (2025); AInvest, "Bitcoin City: El Salvador's Volcano Bond Dream Stalls" (2025), citados también en el capítulo 24.
- Wikipedia y Bitcoin Magazine, "The Free City Of Próspera: Can This Island City's Bitcoin Standard Pave The Way?" (2026), sobre el marco legal ZEDE y la adopción de Bitcoin como unidad de cuenta en Próspera.
- Colombia One, "Prospera: Honduras' Bitcoin City Project" (enero de 2026); GreekReporter, "Próspera, Honduras' Bitcoin City Project, Fights for Survival" (2024-2026), sobre la situación legal del proyecto y sus inversores.

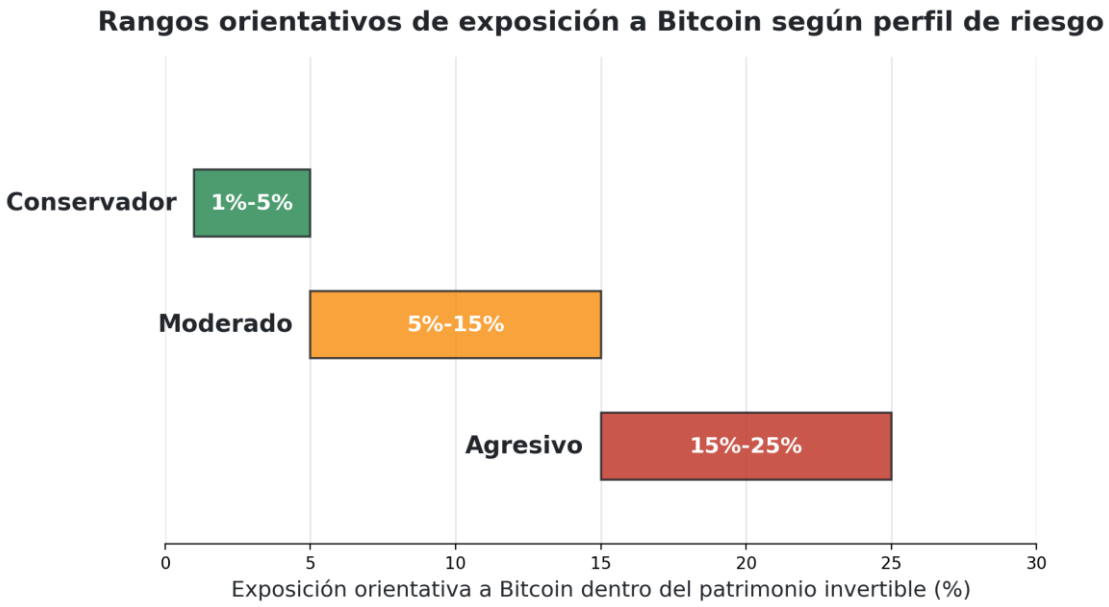
Capítulo 41. Cómo elegir tu propia estrategia según tu perfil de inversor

El capítulo 32 describió, una por una, las principales estrategias para invertir en Bitcoin -desde el HODL hasta los préstamos garantizados- y ofreció una tabla comparativa de riesgo, dedicación y horizonte temporal. Este capítulo da un paso más: en lugar de describir cada estrategia por separado, aborda la pregunta que en realidad se hace la mayoría de los lectores: "de todo esto, ¿qué encaja conmigo?". Como en el resto del libro, nada de lo que sigue constituye una recomendación personalizada de inversión; es, en cambio, un marco de referencia -el mismo tipo de marco que usaría cualquier asesor financiero responsable como punto de partida- para que cada persona lo aplique a su propia situación, idealmente con el apoyo de un profesional cualificado.

Los tres perfiles de riesgo clásicos, aplicados a Bitcoin

La educación financiera tradicional distingue, de forma muy asentada, entre tres perfiles de riesgo -conservador, moderado y agresivo-, definidos no por el activo en el que se invierte sino por la tolerancia psicológica y financiera del inversor a las pérdidas temporales. Aplicados a Bitcoin, un perfil conservador es el de quien prioriza, por encima de todo, no ver caer su patrimonio total de forma brusca, y que reaccionaría con angustia significativa ante una caída del 30% en una sola semana -algo, como vimos en el capítulo 32, perfectamente posible en Bitcoin-; para este perfil, la exposición razonable a Bitcoin dentro de una cartera diversificada suele situarse, según las guías de gestión patrimonial más conservadoras, en un rango que rara vez supera el 1%-5% del patrimonio invertible total, con una preferencia clara por el HODL simple o la promediación del coste (capítulo 32) frente a cualquier estrategia que exija seguimiento activo o apalancamiento.

Un perfil moderado acepta una volatilidad significativa en una parte de su cartera a cambio de una expectativa de mayor rentabilidad a largo plazo, siempre que el resto de su patrimonio -fondo de emergencia, vivienda, ahorro para la jubilación en instrumentos más estables- esté ya cubierto; para este perfil, una exposición de entre el 5% y el 15% del patrimonio invertible, gestionada mediante rebalanceo periódico (capítulo 32) para evitar que una subida fuerte de Bitcoin descompense el resto de la cartera, es la referencia que citan con más frecuencia las guías de asignación de activos que incorporan criptoactivos. Un perfil agresivo, por último, está dispuesto a asumir una volatilidad extrema en busca de una rentabilidad potencial mucho mayor, entendiendo y aceptando de antemano la posibilidad de pérdidas muy significativas; incluso dentro de este perfil, sin embargo, la práctica totalidad de las guías de educación financiera desaconsejan superar el entorno del 20%-25% del patrimonio invertible total en un único activo de la volatilidad de Bitcoin, precisamente por el principio de diversificación que se aplica a cualquier cartera de inversión, sea cual sea el activo concreto.



Rangos ilustrativos citados en guías de gestión patrimonial; no constituyen una recomendación personalizada.

Tres perfiles de riesgo y su exposición orientativa a Bitcoin dentro de una cartera diversificada.

La edad y el horizonte temporal como segunda variable

Además de la tolerancia psicológica al riesgo, la mayoría de los marcos de planificación financiera incorporan una segunda variable: cuánto tiempo falta hasta que ese capital vaya a necesitarse. Un inversor de veinticinco años que destina una pequeña parte de su ahorro a largo plazo a Bitcoin tiene, en términos puramente matemáticos, un horizonte temporal que le permite absorber varios ciclos completos de mercado -Bitcoin ya ha atravesado, como vimos en el capítulo 32, más de una caída superior al 70% seguida de una recuperación a nuevos máximos- antes de necesitar ese dinero, mientras que alguien a cinco años de la jubilación que destinara la misma proporción de su patrimonio se expone al riesgo, mucho más real para su situación concreta, de tener que vender precisamente durante una de esas caídas prolongadas para cubrir sus necesidades. Este principio no es exclusivo de Bitcoin -es el mismo que rige la reducción progresiva de exposición a renta variable a medida que se acerca la jubilación en cualquier plan de pensiones tradicional-, pero se vuelve más relevante cuanto mayor es la volatilidad del activo en cuestión, y pocos activos líquidos cotizados tienen una volatilidad mayor que Bitcoin.

Un ejercicio ilustrativo, no una recomendación

A modo puramente ilustrativo -y de nuevo, sin que esto constituya una recomendación personalizada-, una persona con un perfil moderado y un horizonte de inversión superior a ocho años podría plantearse, según el tipo de marco que aplicaría un asesor financiero, una combinación como la siguiente: cubrir primero el fondo de emergencia y las necesidades a corto plazo en instrumentos estables (capítulo 32); destinar la parte de su cartera de inversión a largo plazo mayoritariamente a instrumentos diversificados tradicionales (fondos indexados, renta fija, inmuebles); y reservar una porción minoritaria y acotada de antemano -por ejemplo, el extremo inferior del rango moderado que describimos más arriba- a Bitcoin, aportada mediante promediación del coste (capítulo 32) para suavizar el efecto de comprar en un mal momento, y revisada una o dos veces al año mediante rebalanceo para evitar que una

revalorización fuerte descompense el conjunto de la cartera. Este ejemplo no es una fórmula universal ni un objetivo a replicar; su único propósito es mostrar cómo se combinan, en la práctica, las variables de perfil de riesgo, horizonte temporal y estrategia concreta que hemos ido describiendo en este capítulo y en el capítulo 32.

Señales de que una estrategia no encaja con tu perfil real

Más allá de cualquier marco teórico, existen señales prácticas bastante fiables de que la estrategia elegida no encaja con la tolerancia al riesgo real de una persona, más allá de la que creía tener sobre el papel: revisar el precio de Bitcoin varias veces al día y que eso afecte al estado de ánimo o al sueño; sentir la tentación de vender en pánico durante una caída pese a haberse comprometido de antemano con un HODL a largo plazo; haber invertido dinero que, en realidad, se necesitaría a corto plazo para otros fines; o, en el extremo opuesto, sentir la tentación constante de aumentar la exposición mediante apalancamiento (capítulo 32) después de una subida fuerte de precio. Cualquiera de estas señales, según coinciden la práctica totalidad de las guías de finanzas conductuales citadas ya en el capítulo 32, es un indicio más fiable de que hay que reducir la exposición o cambiar de estrategia que cualquier cálculo teórico de perfil de riesgo hecho antes de invertir, precisamente porque la tolerancia al riesgo real de una persona solo se revela con certeza cuando el dinero está efectivamente en juego.

Fuentes y estudios citados en este capítulo

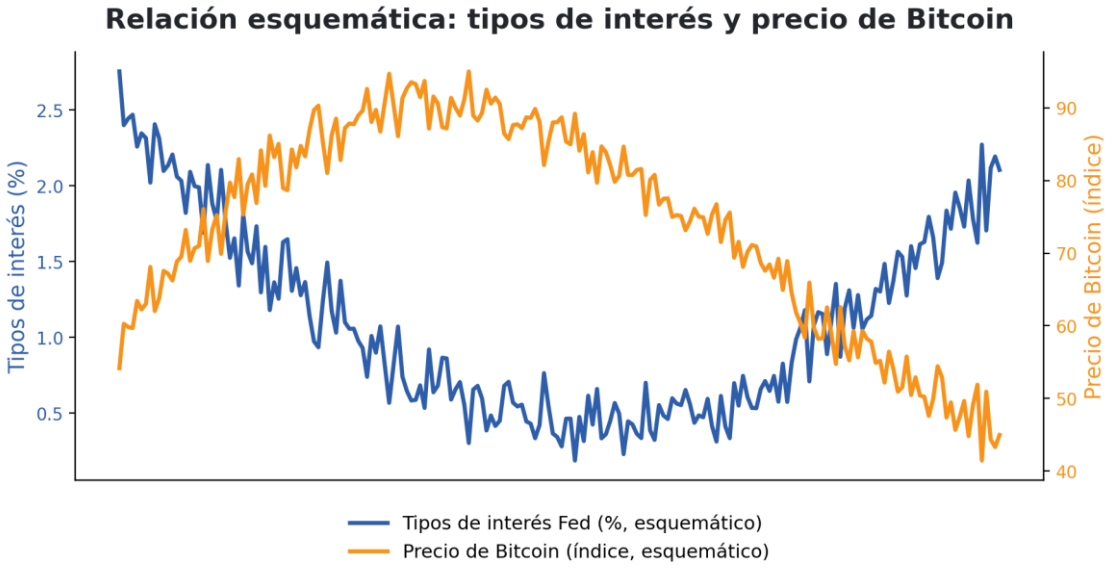
- Guías de asignación de activos y gestión patrimonial de entidades financieras internacionales sobre la incorporación de criptoactivos a carteras diversificadas, citadas también en el capítulo 32.
- Estudios de finanzas conductuales (behavioral finance) sobre la brecha entre la tolerancia al riesgo declarada y la tolerancia al riesgo real de los inversores particulares, citados también en el capítulo 29.
- Principios de planificación financiera por ciclo de vida (life-cycle investing) aplicados a la reducción progresiva de exposición a activos de riesgo según el horizonte temporal del inversor.

Capítulo 42. Bitcoin y la macroeconomía global

Los capítulos anteriores de este bloque han tratado Bitcoin sobre todo desde la perspectiva del usuario y del inversor individual. Este capítulo cierra la Parte VII mirando más allá: cómo se relaciona Bitcoin con las grandes variables macroeconómicas -los tipos de interés, el dólar, la inflación global- que determinan, en última instancia, el contexto en el que se mueve cualquier activo financiero, incluido Bitcoin.

¿Cómo afectan los tipos de interés de la Reserva Federal al precio de Bitcoin?

Bitcoin, pese a presentarse a menudo como un activo "desconectado" del sistema financiero tradicional, ha mostrado en la práctica una correlación notable con la política monetaria de los grandes bancos centrales, especialmente la Reserva Federal estadounidense. Cuando la Reserva Federal baja los tipos de interés o inyecta liquidez en el sistema -como ocurrió a gran escala tras 2008 y de nuevo en 2020, según describimos en el capítulo 4-, el dinero se vuelve más barato de tomar prestado y los inversores tienden a buscar activos de mayor riesgo y mayor rentabilidad potencial en busca de mejores retornos, un fenómeno que los economistas llaman "búsqueda de rendimiento" (search for yield); Bitcoin, como activo de alta volatilidad y alto potencial de revalorización, se ha beneficiado repetidamente de estos periodos de dinero barato. A la inversa, cuando la Reserva Federal sube los tipos de interés para combatir la inflación -como hizo de forma muy pronunciada entre 2022 y 2023-, el dinero se encarece, los activos considerados "seguros" (como la deuda pública a corto plazo) vuelven a ofrecer una rentabilidad atractiva sin apenas riesgo, y los inversores institucionales tienden a reducir su exposición a los activos más especulativos, Bitcoin incluido, un patrón que coincidió con algunas de las caídas de precio más pronunciadas de ese periodo.



Representación conceptual e ilustrativa de la correlación negativa observada entre tipos de interés y precio de Bitcoin en periodos recientes; no representa datos reales de ninguna serie temporal concreta — ver fuentes citadas en el capítulo 42.

Relación esquemática entre los tipos de interés de la Reserva Federal y el precio de Bitcoin.

Esta correlación, documentada de forma consistente por varios estudios de mercado, es uno de los argumentos que más debilitan la narrativa más extrema de "Bitcoin como activo totalmente descorrelacionado" que a veces circula entre sus defensores más entusiastas: en

la práctica, durante buena parte de su historia reciente, Bitcoin se ha comportado más como un activo de riesgo sensible a la liquidez global -de forma similar, aunque no idéntica, a las acciones tecnológicas de alto crecimiento- que como un refugio verdaderamente independiente del ciclo económico convencional, algo que sus defensores atribuyen a la todavía relativa juventud del activo y que esperan que se module con el tiempo a medida que su base de inversores madure y se diversifique.

¿Qué relación tiene Bitcoin con la fortaleza o debilidad del dólar estadounidense?

La relación entre Bitcoin y el dólar es más matizada de lo que sugiere el titular habitual de "Bitcoin sube cuando el dólar baja". Existe, en efecto, una correlación negativa moderada entre el índice del dólar (DXY, que mide su valor frente a una cesta de las principales divisas mundiales) y el precio de Bitcoin en períodos concretos, coherente con la idea de que Bitcoin actúa, para una parte de sus compradores, como una forma de diversificar la exposición al dólar como moneda de reserva mundial; esta lógica es especialmente visible entre inversores e instituciones de países con monedas históricamente inestables, para quienes acumular bitcoin cumple una función parecida a la que durante décadas cumplió acumular dólares físicos como reserva de valor frente a la propia divisa nacional.

Al mismo tiempo, conviene no exagerar esta relación: Bitcoin cotiza, se contabiliza y se negocia mayoritariamente en dólares en los mercados globales, lo que significa que buena parte de su "precio en dólares" está, en cierto sentido, atado a la propia unidad de referencia frente a la que se supone que ofrece una alternativa, una paradoja que los críticos señalan con frecuencia: mientras la infraestructura de mercado de Bitcoin -los pares de negociación más líquidos, la mayoría de los grandes exchanges, buena parte de las stablecoins que vimos en el capítulo 37- siga denominada mayoritariamente en dólares, la independencia de Bitcoin respecto al propio sistema que pretende complementar sigue siendo, en la práctica, parcial.

¿Qué papel juega Bitcoin frente a la inflación global y la desconfianza en las monedas fiduciarias?

El argumento más citado a favor de Bitcoin como cobertura frente a la inflación, que ya introdujimos en el capítulo 32 a propósito del ahorro personal, se traslada también a la escala macroeconómica: en países con episodios de hiperinflación severa -Argentina, Venezuela, Turquía o, más recientemente, algunas economías con controles de capital estrictos-, la adopción de Bitcoin entre la población general ha crecido de forma verificable, documentada por encuestas y por el volumen de operaciones en plataformas de intercambio entre particulares (peer-to-peer), precisamente en los periodos de mayor devaluación de la moneda local. Para estas poblaciones, la comparación relevante no es entre Bitcoin y un depósito bancario en dólares bien remunerado, sino entre Bitcoin y una moneda local que puede perder la mitad de su valor en cuestión de meses, un contexto en el que incluso un activo tan volátil como Bitcoin puede representar, en términos relativos, una opción menos mala que la alternativa disponible localmente.

A escala global y para las principales economías desarrolladas, sin embargo, la evidencia de que Bitcoin funcione como cobertura fiable frente a la inflación general es más débil y más disputada de lo que sugiere el argumento popular: como ya señalamos en el capítulo 32, Bitcoin ha mostrado episodios en los que cae con fuerza precisamente durante picos de

inflación o de incertidumbre económica, en lugar de subir para compensarla, lo que ha llevado a varios economistas a matizar la etiqueta de "cobertura frente a la inflación" y a preferir, en su lugar, hablar de un activo especulativo de largo plazo cuya tesis de valor depende más de la adopción futura y de la escasez programada que de una correlación mecánica y fiable con el índice de precios de cada trimestre.

Fuentes y estudios citados en este capítulo

- Estudios de correlación entre el índice del dólar (DXY), los tipos de interés de la Reserva Federal y el precio de Bitcoin, publicados por analistas de mercado y bancos de inversión, citados también en el capítulo 32.
- Reserva Federal de Estados Unidos, actas y comunicados sobre la política de tipos de interés en los ciclos de 2020-2021 y 2022-2023, citados también en el capítulo 4.
- Chainalysis. "Geography of Cryptocurrency Report", datos sobre adopción de criptoactivos por país y su correlación con episodios de inflación y controles de capital.
- Datos de volumen de negociación peer-to-peer de Bitcoin en Argentina, Venezuela, Turquía y Nigeria, recogidos por plataformas de análisis de mercado independientes.

Capítulo 43. Custodia avanzada: multisig, herencia y planificación patrimonial

Los capítulos 10 y 36 explicaron los fundamentos de la autocustodia: qué es una frase semilla, la diferencia entre monederos calientes y fríos, y los primeros pasos para comprar y guardar bitcoin de forma segura. Este capítulo se dirige a un lector algo más avanzado, que ya posee una cantidad de bitcoin que justifica invertir tiempo en una custodia más sofisticada, y aborda dos preguntas que surgen con mucha frecuencia una vez superada esa primera fase: cómo repartir el riesgo de la custodia entre varias claves, y qué ocurre con esos bitcoins si a su propietario le pasa algo.

¿Qué es exactamente una configuración multisig y cuándo tiene sentido usarla?

Ya definimos multisig (multifirma) en el glosario y lo mencionamos de pasada en el capítulo 10: una configuración de wallet que exige varias firmas independientes, cada una con su propia clave privada, para autorizar cualquier gasto de los fondos. La notación habitual es "M de N": una configuración 2 de 3, por ejemplo, genera tres claves privadas distintas -que pueden guardarse en tres dispositivos, tres ubicaciones físicas o incluso confiarse a tres personas de confianza distintas-, y basta con reunir dos cualesquiera de esas tres para autorizar una transacción, sin que ninguna de las tres claves por sí sola tenga poder para mover los fondos.

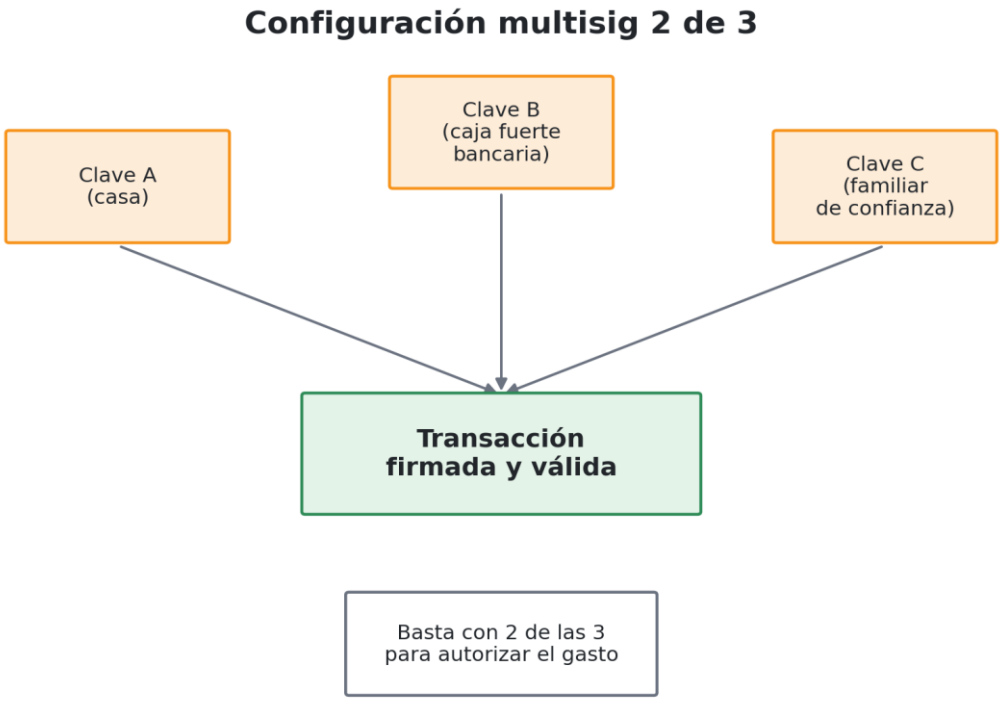
La ventaja frente a una wallet de una sola clave es doble: elimina el punto único de fallo que representa una sola frase semilla -si pierdes o te roban una de las tres claves de una configuración 2 de 3, tus fondos siguen a salvo y siguen siendo recuperables con las otras dos-, y protege frente a la coacción física que mencionamos en el capítulo 18 a propósito del "ataque de la llave inglesa de cinco dólares", porque un atacante que solo consigue acceso a una de las claves no puede, por sí solo, mover los fondos. El coste de esta seguridad adicional es la complejidad operativa: gestionar tres claves en lugar de una exige más disciplina, más dispositivos o ubicaciones que mantener, y un proceso de firma de transacciones algo más lento, por lo que la mayoría de las guías de seguridad recomiendan reservar el multisig para cantidades de bitcoin que justifiquen ese esfuerzo adicional -no hay un umbral universal, pero la práctica habitual del sector sitúa el punto de inflexión en torno a cantidades equivalentes a varios meses o años de ahorro, no en las primeras compras pequeñas de un usuario que empieza-.

¿Cómo se reparte físicamente una configuración multisig en la práctica?

Existen varios patrones habituales entre quienes usan multisig para proteger cantidades significativas. Un patrón común es la distribución geográfica: guardar cada una de las tres claves de una configuración 2 de 3 en una ubicación física distinta -por ejemplo, la vivienda habitual, una caja de seguridad bancaria y la casa de un familiar de confianza en otra ciudad-, de modo que ningún incendio, robo o catástrofe local pueda comprometer más de una clave a la vez. Otro patrón, más orientado a la seguridad frente a terceros que a la seguridad frente a desastres, combina distintos tipos de dispositivo para cada clave -un monedero hardware de un fabricante, un monedero hardware de un fabricante distinto, y una clave derivada y

guardada offline sin ningún dispositivo conectado-, de modo que una vulnerabilidad de seguridad descubierta en un fabricante concreto no comprometa la configuración completa.

Para quienes prefieren no gestionar personalmente toda la complejidad técnica, han surgido en los últimos años servicios especializados de "custodia colaborativa" (collaborative custody), en los que una empresa como Casa o Unchained Capital gestiona una de las claves de una configuración multisig -normalmente 2 de 3 o 3 de 5- mientras el cliente conserva el control de las restantes, de modo que la empresa nunca tiene, por sí sola, capacidad de mover los fondos, pero sí puede ayudar al cliente con la recuperación si pierde alguna de sus propias claves. Este modelo intenta situarse en un punto intermedio entre la autocustodia pura, con toda su responsabilidad personal, y la custodia total de un exchange, con todo el riesgo de contraparte que describimos en el capítulo 18.



Una configuración multisig 2 de 3: basta con dos de las tres claves para autorizar cualquier gasto.

¿Qué pasa con mis bitcoins si fallezco sin haber dejado instrucciones claras?

Es, probablemente, la pregunta de custodia avanzada más importante y más frecuentemente ignorada. A diferencia de una cuenta bancaria, donde un banco puede identificar al titular fallecido a través del DNI o el certificado de defunción y transferir los fondos a los herederos legales siguiendo el proceso de sucesión ordinario, unos bitcoins guardados en autocustodia no tienen ningún vínculo automático con la identidad de su propietario: quien conoce la frase semilla controla los fondos, sin que ningún juzgado, notario ni banco pueda intervenir para transferirlos a otra persona si esa frase semilla se pierde o si nadie más que el fallecido la conocía. En la práctica, esto significa que un patrimonio en bitcoin sin ningún plan de sucesión previsto corre un riesgo real de perderse para siempre en el momento del fallecimiento de su propietario, exactamente igual que si se hubiera perdido la frase semilla en vida, un escenario

que contribuye, según las estimaciones que citamos en el capítulo 33, a la cifra de bitcoins perdidos de forma permanente.

La planificación patrimonial de bitcoin exige resolver una tensión particular: hay que dejar instrucciones suficientes para que los herederos puedan acceder a los fondos tras el fallecimiento, pero sin exponer la frase semilla a un riesgo de robo mientras el propietario sigue con vida. Las soluciones más habituales incluyen repartir la información necesaria entre varios documentos o personas de confianza de modo que ninguno, por sí solo, tenga acceso completo -por ejemplo, combinando una configuración multisig con instrucciones notariales que solo revelan la ubicación de cada clave, no su contenido-; usar servicios especializados de herencia digital que activan el acceso a instrucciones cifradas solo tras la verificación de un certificado de defunción; o, en configuraciones más sencillas, dejar la frase semilla completa en un testamento notarial sellado, aceptando el riesgo, menor pero no nulo, de que el notario o alguien con acceso al testamento pueda conocer su contenido antes de tiempo.

¿Es aconsejable contárselo a mi familia si tengo bitcoin?

No existe una respuesta universal, y la propia pregunta ilustra la tensión de fondo entre seguridad y accesibilidad que atraviesa todo este capítulo: contárselo a la familia reduce el riesgo de que el patrimonio se pierda para siempre por desconocimiento tras un fallecimiento, pero aumenta el número de personas que conocen la existencia de esos fondos, con el riesgo asociado de coacción, robo o presión que ya mencionamos en capítulos anteriores. La práctica más recomendada por los especialistas en seguridad de criptoactivos no es un extremo ni otro, sino un término medio: informar a los herederos designados de la existencia del patrimonio en bitcoin y de dónde encontrar las instrucciones necesarias para acceder a él tras el fallecimiento, sin necesariamente compartir la frase semilla completa mientras el propietario sigue con vida, de modo que la información sensible solo se vuelve accesible en el momento en que realmente se necesita, no antes.

Fuentes y estudios citados en este capítulo

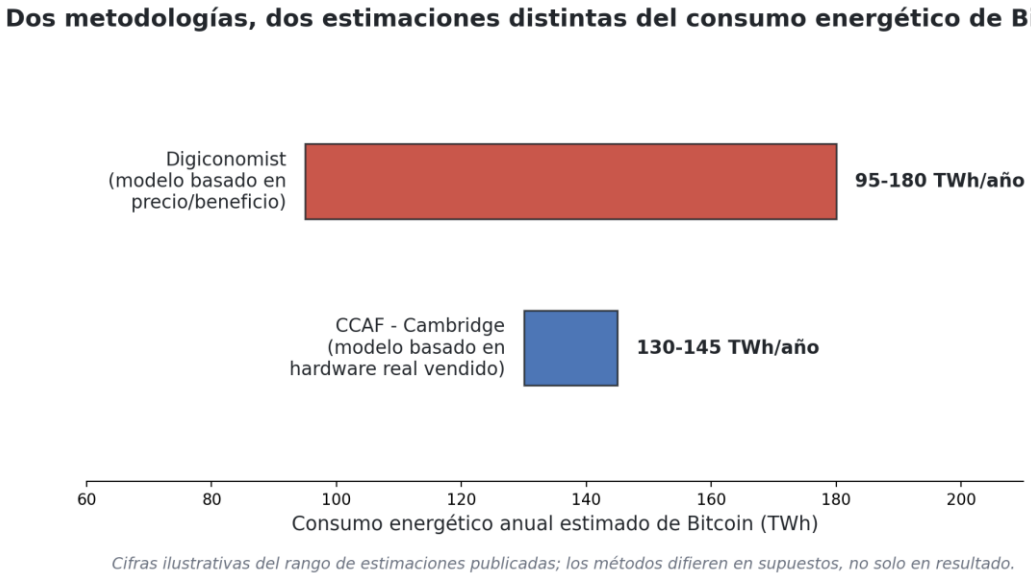
- Documentación técnica de configuraciones multisig (BIP-11, BIP-45 y estándares posteriores), especificaciones del protocolo Bitcoin.
- Casa y Unchained Capital, documentación pública sobre servicios de custodia colaborativa y planificación de herencia en bitcoin.
- Guías de seguridad del sector sobre distribución geográfica y por fabricante de configuraciones multisig, citadas también en el capítulo 10.
- Estudios sobre el volumen estimado de bitcoins perdidos de forma permanente por falta de planificación de sucesión, citados también en el capítulo 33.

Capítulo 44. Bitcoin y el medioambiente: el debate en profundidad

El consumo energético de la minería de Bitcoin apareció ya en los capítulos 28 y 35, y la composición de esa energía la detallamos con datos de 2026 en el capítulo 39. Este capítulo cierra el tema abordando una pregunta previa que rara vez se explica con el detalle que merece: por qué las cifras de consumo energético de Bitcoin que circulan en la prensa varían tanto de una fuente a otra, y qué otros factores medioambientales, más allá de la electricidad, entran en el debate.

¿Por qué las estimaciones de consumo energético de Bitcoin varían tanto según la fuente?

Quien busque "cuánta energía consume Bitcoin" encontrará cifras que pueden diferir en varias decenas de teravatios-hora según la fuente consultada, una discrepancia que no se debe a que unos estén "bien" y otros "mal", sino a que existen metodologías genuinamente distintas para estimar un dato que, a diferencia del consumo eléctrico de un país, no se puede medir de forma centralizada y directa. El índice de Digiconomist, uno de los más citados en la cobertura mediática, estima el consumo a partir de un modelo económico que infiere la cantidad de hardware de minería en funcionamiento a partir de la rentabilidad esperada de minar al precio de mercado del momento, un enfoque que tiende a producir estimaciones más altas y más sensibles a las variaciones de precio. El índice del Centro de Cambridge para las Finanzas Alternativas (CCAF), que ya citamos en el capítulo 39, parte en cambio de datos de ventas reales de hardware ASIC recabados directamente de los fabricantes y de encuestas a empresas mineras, un enfoque que sus autores consideran más fundamentado empíricamente pero que depende, a su vez, de la disposición de esas mismas empresas a compartir información precisa sobre su actividad.



Dos metodologías reconocidas, dos estimaciones distintas del mismo fenómeno.

Ninguna de las dos metodologías es una simple "estimación oficial" incontestable, y ambas han sido revisadas y corregidas por sus propios autores en varias ocasiones a medida que ha mejorado la información disponible; el lector que se encuentre con titulares que citan cifras

muy distintas entre sí no está necesariamente ante una contradicción o una manipulación, sino ante el reflejo honesto de que medir el consumo energético de una red descentralizada y global, sin ningún organismo central que reporte cifras oficiales verificadas, es un problema metodológicamente difícil que la comunidad académica todavía no ha resuelto de forma unánime.

Más allá de la electricidad: el debate sobre los residuos electrónicos (e-waste)

Un aspecto del debate medioambiental que recibe menos atención mediática que el consumo eléctrico, pero que algunos investigadores consideran igualmente relevante, es la generación de residuos electrónicos por la rápida obsolescencia del hardware de minería que describimos en el capítulo 39: dado que cada nueva generación de ASIC deja fuera de mercado a las máquinas más antiguas en cuestión de dos o tres años, y que esas máquinas, a diferencia de un ordenador de propósito general, no tienen prácticamente ninguna utilidad alternativa una vez dejan de ser rentables para minar, un estudio ampliamente citado de la Universidad de las Naciones Unidas y otros investigadores independientes ha estimado que la red de Bitcoin podría generar decenas de miles de toneladas de residuos electrónicos al año, una cifra comparable, según los términos de esa comparación, a la de países de tamaño medio en residuos electrónicos totales.

Los defensores de la industria minera matizan esta cifra señalando que una parte creciente del hardware retirado se revende para su uso en operaciones de minería en países con costes energéticos más bajos en lugar de desecharse directamente -alargando su vida útil real más allá de lo que sugiere el cálculo basado solo en la obsolescencia económica en el mercado principal-, y que algunos fabricantes han empezado a implementar programas de reciclaje de componentes, aunque la cobertura y la eficacia real de esos programas siguen siendo, según los propios críticos, limitadas y difíciles de auditar de forma independiente.

¿Cómo se compara el impacto medioambiental de Bitcoin con el de otros sectores?

Una parte del debate público se ha centrado, en los últimos años, en poner el consumo energético de Bitcoin en perspectiva frente a otras actividades económicas con un impacto medioambiental reconocido pero menos discutido. La minería de oro tradicional, por ejemplo, consume energía en la extracción, el transporte y el refinado, y genera un impacto medioambiental adicional -contaminación por mercurio y cianuro, alteración de ecosistemas, deforestación- que no tiene un equivalente directo en la minería de Bitcoin, aunque comparar ambas cifras de forma directa resulta metodológicamente complicado porque miden magnitudes distintas (energía frente a impacto ecológico combinado). El sistema bancario tradicional y las tarjetas de pago, por su parte, consumen energía en sucursales físicas, centros de datos, cajeros automáticos y la fabricación de tarjetas y terminales de pago, un consumo que, según algunos estudios comparativos citados por defensores de Bitcoin, podría ser de una magnitud similar o incluso superior por transacción en determinados escenarios, aunque estas comparaciones dependen mucho de qué se incluye exactamente en el cálculo de cada lado y son, por tanto, objeto de disputa activa entre analistas con conclusiones muy distintas según los supuestos de partida que utilicen.

La conclusión más honesta, coherente con el resto de este libro, es que no existe todavía un consenso metodológico sólido para responder de forma definitiva a la pregunta "¿es Bitcoin peor o mejor que X para el medioambiente?", y que cualquier cifra que se presente como una comparación simple y cerrada -en cualquiera de las dos direcciones- merece ser recibida con el mismo escepticismo informado que este libro ha aplicado a lo largo de todos sus capítulos a las afirmaciones categóricas sobre Bitcoin.

Fuentes y estudios citados en este capítulo

- Digiconomist. "Bitcoin Energy Consumption Index", metodología y estimaciones publicadas, citado también en el capítulo 28.
- Cambridge Centre for Alternative Finance (CCAF). "Cambridge Bitcoin Electricity Consumption Index" y "Digital Mining Industry Report", citados también en los capítulos 28 y 39.
- de Vries, A. y Stoll, C. Universidad de las Naciones Unidas y estudios independientes sobre la generación de residuos electrónicos (e-waste) de la minería de Bitcoin.
- Estudios comparativos sobre el consumo energético del sistema bancario tradicional y la minería de oro frente a la minería de Bitcoin, citados también en el capítulo 28.

Capítulo 45. Casos de estudio: comunidades que ya usan Bitcoin en su día a día

Más allá de la adopción estatal de El Salvador que analizamos en el capítulo 24, o de las cifras agregadas de adopción por país, existen comunidades concretas donde Bitcoin se usa, de forma verificable y cotidiana, para pagar la compra, la factura de la luz o el sueldo. Este capítulo cierra la Parte VII con un vistazo a algunos de esos casos, que ilustran cómo se ve la adopción de Bitcoin "sobre el terreno" más allá de los titulares sobre precio o regulación.

Tres comunidades, tres motivaciones de fondo muy distintas para adoptar Bitcoin.

El Zonte, El Salvador: "Bitcoin Beach", la comunidad que empezó antes que el propio país

Antes de que El Salvador adoptara Bitcoin como moneda de curso legal en 2021 (capítulo 24), ya existía un experimento comunitario que sirvió de inspiración directa para esa decisión: en 2019, un donante anónimo envió una cantidad significativa de bitcoin a la pequeña localidad costera de El Zonte, con una condición explícita: el dinero no podía cambiarse a dólares, sino que debía circular directamente en bitcoin dentro de la comunidad. La organización sin ánimo de lucro Bitcoin Beach, nacida de esa donación, trabajó con comerciantes locales, pescadores, vendedoras de pupusas y pequeños negocios para que empezaran a aceptar pagos en bitcoin a través de la red Lightning (capítulo 22), en una localidad donde buena parte de la población no tenía siquiera una cuenta bancaria tradicional y donde el teléfono móvil se convirtió, de la noche a la mañana, en la puerta de entrada a un sistema financiero al que antes no tenían acceso.

Más de seis años después, la iniciativa sigue activa: los vecinos de El Zonte pueden pagar facturas de electricidad, agua y teléfono, recibir atención médica o cortarse el pelo usando bitcoin a través de Lightning, y el propio proyecto ha financiado becas educativas, programas de surf para jóvenes locales y ayudas durante la pandemia, financiadas con las donaciones y con parte de la actividad económica generada. El caso de El Zonte se cita con frecuencia,

tanto por defensores como por analistas neutrales de la adopción de Bitcoin, como el ejemplo más citado de lo que en el sector se llama una "economía circular de Bitcoin": una comunidad en la que el bitcoin no solo se recibe, sino que también se gasta localmente en otros comercios de la misma zona, sin necesidad de convertirlo a moneda fiat en cada operación.

Lugano, Suiza: "Plan ₿", una ciudad europea que apuesta por Bitcoin

En un contexto completamente distinto -una ciudad suiza de renta alta, no una comunidad costera de un país en desarrollo-, el ayuntamiento de Lugano lanzó en 2022, en colaboración con la empresa Tether (emisora de la stablecoin USDT que ya presentamos en el capítulo 37), el proyecto "Plan ₿", con el objetivo declarado de convertir la ciudad en un referente europeo de adopción de Bitcoin. A mediados de 2026, más de 360 comercios de la ciudad aceptan pagos en bitcoin, USDT y en la moneda local complementaria LVGA, y el ayuntamiento acepta bitcoin y USDT como forma válida de pago para impuestos municipales, tasas y otros servicios públicos, una integración institucional bastante más profunda que la de la mayoría de las ciudades que han intentado experimentos similares.

El proyecto organiza además, desde 2023, un foro anual -el "Plan ₿ Forum"- que en su edición de octubre de 2025 reunió a más de cuatro mil participantes de sesenta y cuatro países, un aumento del 38% respecto al año anterior, consolidándose como uno de los mayores encuentros europeos dedicados a la adopción práctica de Bitcoin, más allá del debate puramente financiero o especulativo. El caso de Lugano ilustra un patrón de adopción distinto al de El Zonte: no nace de la necesidad de dar acceso financiero a una población desatendida por la banca tradicional, sino de una apuesta institucional deliberada por atraer inversión, turismo y visibilidad internacional en torno al ecosistema Bitcoin, un enfoque más cercano, en su lógica de fondo, al de Bitcoin City que describimos en el capítulo 40.

Nigeria: la adopción impulsada por la devaluación y el control de capitales

El caso nigeriano, que ya mencionamos en los capítulos 27 y 34 a propósito de la congelación de cuentas durante las protestas #EndSARS y del marco regulatorio de 2025, ilustra un tercer patrón de adopción, más extendido pero menos visible que los dos anteriores porque no depende de ningún proyecto institucional concreto, sino de millones de decisiones individuales. Según el Índice Global de Adopción Cripto de Chainalysis de 2026, Nigeria ocupa el segundo puesto mundial en adopción de criptoactivos, solo por detrás de India, impulsada en gran medida por el uso de bitcoin y, sobre todo, de stablecoins (capítulo 37) como cobertura frente a la devaluación acelerada de la naira y frente a las restricciones de acceso a divisas extranjeras que atraviesa el país; la adopción de stablecoins en el conjunto del África subsahariana creció un 180% en el último año analizado, con Nigeria a la cabeza y con Etiopía y Kenia apareciendo, por primera vez, entre los veinte primeros países del índice mundial.

Este patrón de adopción "desde abajo", basado en la necesidad práctica de proteger el poder adquisitivo cotidiano más que en ningún proyecto institucional, conecta directamente con el argumento que desarrollamos en el capítulo 42 a propósito de la relación entre Bitcoin, la inflación y las economías con monedas inestables: para buena parte de los usuarios nigerianos, la pregunta relevante no es si Bitcoin es más o menos volátil que el dólar, sino si es más o menos fiable que una naira cuyo valor se erosiona con rapidez, una comparación

que, en ese contexto concreto, favorece con frecuencia a los criptoactivos frente a la alternativa local disponible.

Qué tienen en común, y qué no, estos tres casos

Los tres casos descritos en este capítulo -una comunidad rural centroamericana, una ciudad europea de renta alta y un país africano con más de doscientos millones de habitantes- comparten un rasgo de fondo pese a sus enormes diferencias de escala y de contexto: en los tres, la adopción real de Bitcoin se ha sostenido más por una utilidad práctica percibida por sus usuarios -acceso financiero, atractivo institucional y turístico, o cobertura frente a la devaluación- que por la mera especulación sobre su precio futuro que domina buena parte de la cobertura mediática habitual sobre Bitcoin. Al mismo tiempo, difieren notablemente en su grado de consolidación y de riesgo: la economía circular de El Zonte y el proyecto de Lugano dependen, en última instancia, de la continuidad de organizaciones y acuerdos institucionales concretos, mientras que la adopción nigeriana, al estar repartida entre millones de decisiones individuales no coordinadas, resulta estructuralmente más difícil de revertir con una sola decisión política, aunque también más difícil de cuantificar con precisión, como ya señalamos a propósito de las limitaciones metodológicas del propio índice de Chainalysis.

Fuentes y estudios citados en este capítulo

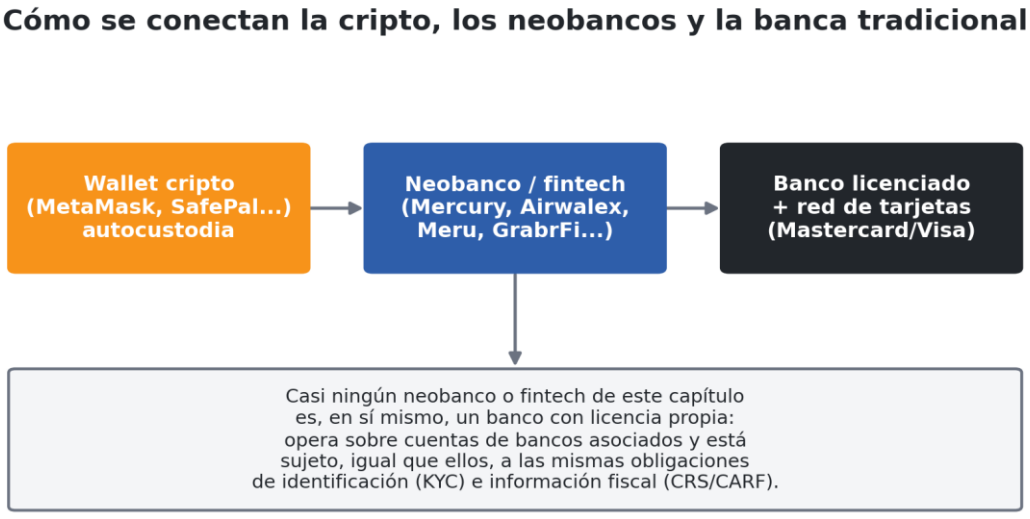
- Bitcoin Beach, documentación pública sobre el origen y la evolución del proyecto en El Zonte, El Salvador, desde 2019.
- Ayuntamiento de Lugano y Tether. "Plan ₿", documentación oficial sobre la integración de bitcoin y USDT en los pagos municipales y comerciales de la ciudad, y datos del Plan ₿ Forum de octubre de 2025.
- Chainalysis. "2026 Global Crypto Adoption Index", con los datos de adopción por país citados en este capítulo, incluida la clasificación de Nigeria y el crecimiento de la adopción de stablecoins en el África subsahariana.
- Human Rights Watch y cobertura periodística sobre las protestas #EndSARS de 2020 en Nigeria, citadas también en el capítulo 27.

Capítulo 46. Neobancos y fintechs: el puente entre las criptomonedas y la banca tradicional

Los capítulos anteriores han tratado, sobre todo, la relación directa entre una persona y su cripto: cómo comprarla, guardarla y usarla. Pero existe una capa intermedia, cada vez más relevante, que casi nunca se explica con claridad: la de los neobancos y las fintechs que conectan el mundo cripto con el sistema financiero tradicional, permitiendo cobrar, gastar y mover dinero entre ambos mundos con una fricción mucho menor que hace unos años. Este capítulo, y los tres que le siguen, exploran ese ecosistema con nombres y datos concretos: qué son, para qué sirven realmente, y también -algo igual de importante- qué no pueden hacer por ti.

Por qué existe este ecosistema: el problema de la "desbancarización"

Como vimos en el capítulo 28 a propósito de la "Operation Choke Point 2.0", y en el capítulo 26 al hablar de por qué Bitcoin genera resistencia institucional, durante años numerosas empresas y particulares con actividad relacionada con criptoactivos se encontraron con que los bancos tradicionales cerraban sus cuentas, rechazaban sus solicitudes o las sometían a un escrutinio desproporcionado, no por haber hecho nada ilegal, sino simplemente por el "riesgo reputacional" asociado al sector. Este fenómeno, real y bien documentado, generó un hueco de mercado que un conjunto de fintechs y neobancos ha ido llenando en los últimos años: empresas que, sin ser necesariamente bancos con licencia propia, ofrecen cuentas, tarjetas y servicios de pago diseñados específicamente para clientes -empresas web3, autónomos internacionales, exchanges, o simplemente personas que cobran o gastan en distintas divisas y con distinta frecuencia que un usuario bancario convencional- a los que la banca tradicional ha tendido a rechazar o a dificultar el acceso.



La mayoría de estos neobancos y fintechs operan sobre cuentas de bancos licenciados, no como bancos independientes.

Qué es, técnicamente, un "neobanco" o una fintech de pagos

Es importante entender un matiz técnico antes de seguir: la inmensa mayoría de las fintechs de este capítulo no son, en sí mismas, bancos con licencia bancaria plena propia (aunque esto está empezando a cambiar, como veremos con Mercury). En la práctica, operan como intermediarios tecnológicos que se asocian con uno o varios bancos licenciados -normalmente bancos pequeños o medianos dispuestos a aceptar el perfil de riesgo de estos clientes a cambio de una comisión-, y construyen sobre esa infraestructura bancaria una experiencia de usuario mucho más moderna, rápida y adaptada a necesidades internacionales: apertura de cuenta en minutos en lugar de semanas, múltiples divisas en una sola cuenta, tarjetas virtuales instantáneas, e integraciones directas con exchanges de criptoactivos que muchos bancos tradicionales siguen tratando con recelo. Esta estructura tiene una consecuencia importante que retomaremos con detalle en el capítulo 49: si el dinero de un neobanco descansa, en última instancia, sobre una cuenta de un banco licenciado, ese neobanco está sujeto, por transitividad, a exactamente las mismas obligaciones regulatorias de identificación de clientes (KYC) y de información fiscal que cualquier banco tradicional, aunque su interfaz y su marketing se sientan mucho más cercanos al mundo cripto que al de la banca de toda la vida.

Un vistazo rápido al panorama: quién es quién

Un mapa rápido de qué herramienta resuelve qué problema, antes de entrar en el detalle de cada una.

Antes de profundizar, uno por uno, en las plataformas concretas en los próximos dos capítulos, conviene tener un mapa general de qué tipo de servicio ofrece cada una, porque no todas resuelven el mismo problema:

- Mercury y Airwallex están pensadas, sobre todo, para empresas: startups, negocios con operaciones internacionales, y en el caso de Mercury específicamente, empresas del

sector cripto y web3 que necesitan una cuenta bancaria funcional que los bancos tradicionales les niegan.

- GrabrFi está pensada para particulares que necesitan una cuenta en dólares sin residir en Estados Unidos, típicamente autónomos y freelancers que facturan a clientes estadounidenses o que reciben pagos de plataformas internacionales.
- Meru combina una cuenta neobancaria con una wallet de stablecoins no custodial, dirigida sobre todo a usuarios de Latinoamérica que buscan una alternativa a sistemas bancarios locales inestables o restrictivos.
- MetaMask Card y SafePal, que veremos en el capítulo 48, no son neobancos en sentido estricto, sino wallets cripto que han añadido la capacidad de gastar directamente desde el saldo cripto mediante una tarjeta física o virtual, sin pasar primero por una cuenta bancaria tradicional gestionada por el usuario.

En el próximo capítulo entramos en detalle en las tres primeras: Mercury, Airwallex y GrabrFi, con sus condiciones, sus límites y su relación real -no la que sugiere su marketing- con el mundo cripto.

Fuentes y estudios citados en este capítulo

- Mercury. "Business Banking for Web3 Companies", documentación pública sobre los servicios ofrecidos a empresas de criptoactivos y las limitaciones existentes.
- Comité de Servicios Financieros de la Cámara de Representantes de Estados Unidos (2025), sobre la "Operation Choke Point 2.0", citada también en el capítulo 28.
- Cobertura periodística especializada (TechCrunch, Forbes Advisor, Sacra) sobre la financiación y expansión de Mercury y Airwallex durante 2026.

Capítulo 47. Mercury, Airwallex y GrabrFi: banca digital para empresas y particulares con actividad cripto

Este capítulo profundiza en tres plataformas concretas mencionadas en el capítulo anterior, con datos actualizados a 2026: qué ofrecen exactamente, a quién están dirigidas, y qué relación real tienen con las criptomonedas, que suele ser bastante más limitada de lo que muchos usuarios asumen.

Mercury: banca para empresas web3, sin custodiar cripto directamente

Mercury es, probablemente, el nombre más conocido entre las fintechs "cripto-friendly", pero conviene precisar desde el principio qué hace y qué no hace. Mercury ofrece cuentas bancarias en dólares para empresas -incluidas explícitamente empresas de blockchain, cripto, NFT y organizaciones descentralizadas (DAO)-, pero no permite mantener saldo en criptoactivos ni en stablecoins dentro de la propia cuenta: opera exclusivamente con moneda fiduciaria tradicional. Lo que sí ofrece es una vía fluida hacia el mundo cripto: transferencias sin comisión hacia exchanges importantes como Coinbase o Gemini, sin límites explícitos sobre el importe destinado a comprar criptoactivos, y una experiencia de apertura de cuenta pensada para startups que los bancos tradicionales suelen rechazar por no encajar en sus criterios de riesgo convencionales.

Un matiz importante: Mercury no da servicio a plataformas de intercambio (exchanges) ni a otras Empresas de Servicios Monetarios (Money Services Businesses), lo que excluye de su base de clientes, precisamente, a una parte del sector que más dificultades tiene para conseguir banca tradicional. Además, transferencias repetidas y de importe elevado hacia exchanges de criptoactivos pueden generar una revisión adicional por parte de sus equipos de cumplimiento normativo si no encajan con la actividad declarada de la empresa, un recordatorio de que "cripto-friendly" no equivale a "sin supervisión". En un desarrollo relevante de 2026, Mercury recibió la aprobación condicional de la Oficina del Interventor de la Moneda de Estados Unidos (OCC) para convertirse en un banco con licencia federal propia, lo que le permitiría, entre otras cosas, ofrecer préstamos directamente y depender menos de sus bancos asociados; la compañía alcanzó una valoración de 5.200 millones de dólares tras una ronda de financiación de 200 millones en 2026.

Mercury: de fintech asociada a un banco a aspirante a banco con licencia propia

Mientras no complete el proceso, Mercury sigue operando, como el resto de fintechs de este capítulo, sobre las cuentas de bancos licenciados asociados.

El camino de Mercury desde fintech asociada a bancos hasta aspirante a banco con licencia federal propia.

Airwallex: pagos globales para empresas, con un pie cada vez más metido en blockchain

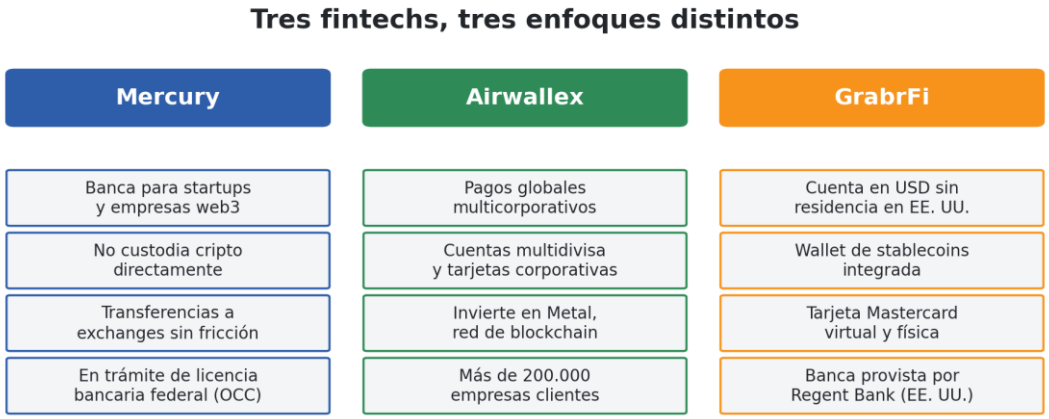
Airwallex tiene un enfoque distinto: en lugar de dirigirse específicamente a empresas cripto, ofrece infraestructura de pagos globales -cuentas multidivisa, tarjetas corporativas, tipos de cambio competitivos y APIs de pago- a empresas de cualquier sector con operaciones internacionales, entre clientes tan conocidos como SHEIN o McLaren. Su relación con el mundo cripto es más reciente e indirecta que la de Mercury: en junio de 2026, a través de su propio fondo de inversión (Capital49), Airwallex lideró una inversión en Metal, una red de liquidación basada en blockchain orientada a productos financieros tokenizados, convirtiéndose en su primer socio de diseño. La compañía cerró en 2026 una ronda de financiación de 320 millones de dólares que elevó su valoración a 11.000 millones, y superó los 200.000 negocios clientes y más de 266.000 millones de dólares en volumen de transacciones anualizado.

Para un usuario o una pequeña empresa con actividad cripto, Airwallex resulta útil sobre todo como capa de pagos internacionales -recibir y pagar en múltiples divisas con comisiones competitivas- más que como una puerta de entrada específica al mundo cripto, a diferencia de Mercury; su valor añadido está en la escala y en la sofisticación de su infraestructura de pagos globales, no en ninguna funcionalidad cripto nativa todavía disponible para el usuario medio.

GrabrFi: una cuenta en dólares sin necesidad de vivir en Estados Unidos

GrabrFi resuelve un problema distinto y muy concreto: permite a cualquier persona, sin importar su país de residencia, abrir una cuenta en dólares estadounidenses, con más de 250.000 usuarios en todo el mundo. Está pensada, sobre todo, para autónomos y freelancers que facturan a clientes o plataformas estadounidenses (Upwork, agencias, empresas de software) y que, de otro modo, tendrían que asumir comisiones de conversión de divisa elevadas o depender de intermediarios más caros y lentos. La banca subyacente la presta Regent Bank, una entidad bancaria estadounidense regulada, lo que sitúa a GrabrFi dentro del mismo esquema de "fintech sobre banco licenciado" que describimos en el capítulo anterior.

La parte relevante para este libro es su función de puente con las stablecoins: GrabrFi ofrece, junto a la cuenta corriente en dólares, una wallet de stablecoins integrada, que permite mantener saldo en USDC o USDT y transferirlo hacia fuera del sistema bancario tradicional -por ejemplo, para pagar a un contratista en otro país, o para retirarlo a un exchange- con una fricción mucho menor que una transferencia bancaria internacional convencional, además de una tarjeta Mastercard virtual y física con una comisión del 1,5% por operaciones fuera de Estados Unidos.



Ninguna de las tres ofrece anonimato: todas exigen verificación de identidad (KYC) y reportan información financiera conforme a la normativa de cada jurisdicción en la que operan.

Tres fintechs con enfoques distintos: banca empresarial cripto-friendly, pagos globales corporativos y cuentas en dólares sin residencia estadounidense.

El hilo común: ninguna de las tres sustituye a un banco central ni te libera de las normas

Pese a sus diferencias, las tres comparten un rasgo estructural que conviene subrayar antes de seguir: todas exigen un proceso de verificación de identidad (KYC) equivalente al de un banco tradicional, todas dependen en última instancia de bancos con licencia regulados por algún Estado, y ninguna ofrece ni promete ningún tipo de anonimato o de exención de las obligaciones fiscales del usuario o la empresa que las utiliza, un punto que desarrollaremos con el detalle que merece en el capítulo 49.

Fuentes y estudios citados en este capítulo

- Mercury. "Web3 Banking", documentación pública sobre servicios, límites y exclusiones para empresas de criptoactivos.
- CNBC (mayo de 2026). Cobertura de la ronda de financiación de Mercury y su valoración de 5.200 millones de dólares.
- Blockchain Council (2026). Análisis sobre la aprobación condicional de la licencia bancaria federal (OCC) de Mercury.
- Semafor y Yahoo Finance (2026). Cobertura de la expansión de Airwallex a Estados Unidos y su volumen de activos gestionados.
- TechCrunch (abril de 2026). "Airwallex is about to take on Stripe", sobre el lanzamiento de su terminal físico de pago y su inversión en Metal.
- GrabrFi. "US Account App", documentación pública sobre la cuenta en dólares, la wallet de stablecoins y la tarjeta Mastercard asociada, con banca provista por Regent Bank.

Capítulo 48. Meru, MetaMask Card y SafePal: cuando la wallet se convierte en cuenta bancaria

El capítulo anterior cubrió fintechs que parten de una cuenta bancaria y se acercan al mundo cripto. Este capítulo recorre el camino inverso: wallets y plataformas cripto-nativas que han añadido funciones bancarias -cuentas en dólares, tarjetas de débito, ingresos en moneda local- para que el usuario pueda operar sin salir nunca del todo del ecosistema cripto.

Meru: una wallet no custodial con alma de neobanco latinoamericano

Meru, fundada por R3mit Solutions Inc. y con sede en Orlando, combina dos cosas que rara vez van juntas: una wallet no custodial -es decir, donde el usuario mantiene el control de sus propias claves, como explicamos en el capítulo 10- y funciones típicamente bancarias, como una cuenta denominada en dólares y una tarjeta Visa asociada. Construida sobre la red Stellar, elegida por sus comisiones muy bajas y sus tiempos de confirmación rápidos, Meru permite a particulares y pequeñas empresas mantener saldo en stablecoins como USDC y USDT, recibir pagos desde plataformas como PayPal o Payoneer, generar rendimiento a través de protocolos DeFi, y retirar fondos a métodos de pago locales en varios países de Latinoamérica, incluida Bolivia, donde lanzó su wallet a finales de 2024.

El caso de uso central de Meru, según describe la propia compañía, es la "soberanía financiera" para usuarios que viven bajo sistemas bancarios locales inestables, con controles de capital estrictos o con acceso limitado a divisas fuertes -un problema real que ya documentamos en el capítulo 27 a propósito de Argentina y Venezuela-. A diferencia de Mercury o Airwallex, Meru no es una capa sobre la banca tradicional dirigida a empresas, sino una alternativa pensada explícitamente para el usuario particular que quiere reducir su dependencia del sistema bancario local sin necesidad de gestionar directamente una wallet técnica compleja.

MetaMask Card: gastar directamente desde tu wallet de autocustodia

MetaMask, la wallet de software para Ethereum y redes compatibles que ya presentamos en el capítulo 10, lanzó su propia tarjeta de débito vinculada directamente a la wallet del usuario, con una característica que la distingue de una tarjeta bancaria convencional: los fondos permanecen bajo autocustodia hasta el instante exacto en que se realiza el pago, en lugar de tener que transferirlos primero a una cuenta bancaria intermedia. La tarjeta, operada sobre la red Mastercard, permite pagar directamente con mUSD (la stablecoin propia del ecosistema MetaMask), wETH, EURe, GBPe, USDC o USDT, tanto de forma física como a través de Apple Pay y Google Pay.

Tras un año de prueba piloto en la Unión Europea, MetaMask expandió la tarjeta a Estados Unidos en febrero de 2026, y a mediados de 2026 estaba disponible en Argentina, Brasil, Canadá, Colombia, México, Suiza, el Reino Unido y varios países europeos. Existen dos modalidades: una tarjeta virtual gratuita con un 1% de devolución en mUSD, y una tarjeta física "Metal" con una cuota anual de 199 dólares que ofrece un 3% de devolución y sin comisiones por operaciones en el extranjero. Conviene señalar que, a mediados de 2026, las nuevas solicitudes de la tarjeta en Estados Unidos y los pedidos de la tarjeta física Metal estaban temporalmente pausados, un recordatorio de que la disponibilidad de estos

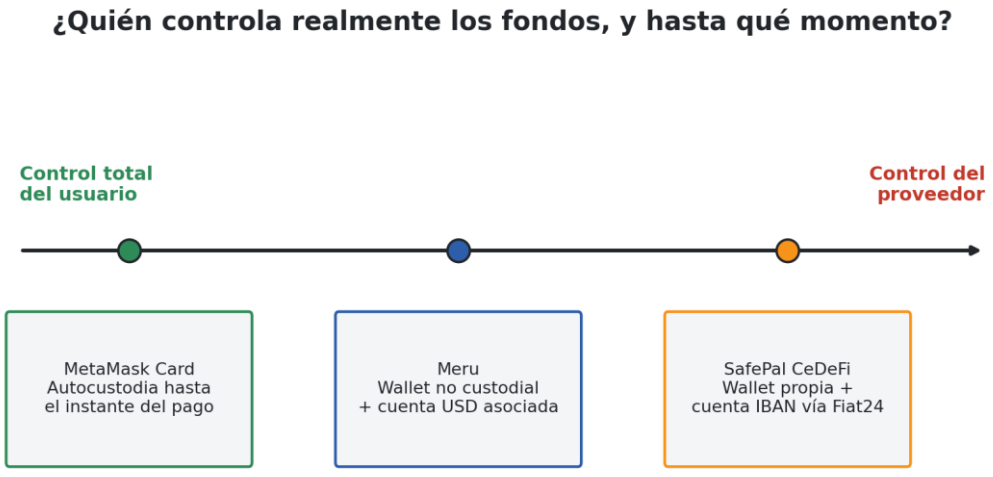
productos cambia con frecuencia y conviene verificarla directamente antes de planificar nada en torno a ellos.

SafePal: de monedero hardware a banca cripto-nativa con IBAN suizo

SafePal, la wallet hardware y software que mencionamos en el capítulo 36, ha ido añadiendo progresivamente funciones bancarias a su ecosistema. A través de su pasarela "CeDeFi Banking", operada en colaboración con Fiat24 y lanzada en marzo de 2024, los usuarios pueden abrir una cuenta bancaria individual con IBAN suizo, sin comisiones de gestión ni de depósito, directamente vinculada a su wallet SafePal. La compañía complementa este servicio con una tarjeta Mastercard -con ediciones especiales de diseño lanzadas periódicamente, como las ediciones limitadas de 2026- y con promociones de captación como la entrega de un monedero hardware SafePal X1 gratuito al abrir una cuenta.

Cada pago con una tarjeta cripto suele equivaler, a efectos fiscales, a vender ese cripto por su valor de mercado en ese instante: la comodidad del pago no elimina la obligación de declarar la ganancia o pérdida generada (capítulo 29).

Cada pago con una tarjeta vinculada a cripto implica, técnicamente, una venta de ese cripto: la comodidad no elimina el hecho fiscal.



Quién controla los fondos y hasta qué momento, en cada una de estas tres herramientas.

El patrón común: comodidad de gasto, no invisibilidad

Tanto MetaMask Card como SafePal ilustran un patrón que conviene entender bien antes de usar cualquiera de estas herramientas con regularidad: cada vez que pagas con una tarjeta vinculada directamente a un saldo cripto, la plataforma vende, en el instante del pago, la cantidad exacta de cripto necesaria para cubrir el importe en la moneda local del comercio. Desde el punto de vista de la experiencia de usuario, esto se siente exactamente igual que pagar con cualquier tarjeta de débito convencional; desde el punto de vista fiscal, sin embargo, cada uno de esos pagos constituye técnicamente una venta o disposición de un activo, con su correspondiente ganancia o pérdida patrimonial que, en España y en la mayoría de los países con un sistema fiscal desarrollado, debe declararse exactamente igual que si hubieras vendido esa cripto en un exchange, como detallamos en el capítulo 29. Comprar un café con una tarjeta cripto puede generar, en sentido estricto, una obligación de declarar esa microtransacción como una ganancia o pérdida patrimonial, algo que sorprende a muchos usuarios nuevos y que retomaremos, con toda la seriedad que merece, en el próximo capítulo.

Fuentes y estudios citados en este capítulo

- Meru / R3mit Solutions Inc. Documentación pública sobre la wallet no custodial, la integración con Stellar y el lanzamiento en Bolivia (2024).
- The Grid y Portal HQ (2026). Perfiles de empresa y casos de estudio sobre la expansión de Meru en Latinoamérica.
- MetaMask (2026). "Introducing MetaMask Card", documentación oficial sobre tokens soportados, modalidades de tarjeta y disponibilidad geográfica.
- CoinDesk (febrero de 2026). "MetaMask expands debit card nationwide across US after EU pilot".
- SafePal. Documentación pública sobre la pasarela CeDeFi Banking con Fiat24 y las cuentas IBAN suizas asociadas a la wallet.

Capítulo 49. Privacidad financiera, diversificación internacional y los límites legales: lo que la ley permite y lo que no

Los tres capítulos anteriores han descrito, con nombres y datos concretos, un ecosistema real de neobancos, fintechs y wallets con función bancaria que muchas personas usan, legítimamente, para acceder a servicios financieros que la banca tradicional les niega o les complica. Es habitual, sin embargo, que estas mismas herramientas se promocionen -o se busquen- también como una vía para "escapar" del control fiscal o regulatorio de un gobierno concreto. Este capítulo cierra el bloque abordando esa cuestión de frente, con el mismo rigor y la misma honestidad que este libro ha aplicado a cada debate abierto sobre Bitcoin: qué es legítimo, qué es ilegal, y por qué la diferencia importa mucho más de lo que sugiere el marketing de muchas de estas plataformas.

La motivación legítima, otra vez: recordemos de dónde viene

Como desarrollamos con detalle en el capítulo 27, la desconfianza hacia el control estatal sobre las finanzas personales no nace de la nada: los episodios de congelación de cuentas en Canadá durante 2022, el bloqueo de cuentas de manifestantes en Nigeria en 2020, y los controles de capital y la licuación inflacionaria del ahorro en países como Argentina o Venezuela son hechos verificables, no hipótesis conspirativas. En ese contexto, buscar herramientas que reduzcan la dependencia de un único banco, de un único país o de una única moneda -diversificar geográfica y tecnológicamente el propio patrimonio- es una respuesta racional y, en la inmensa mayoría de los casos, perfectamente legal a un riesgo real. Nada de lo que sigue en este capítulo pretende negar esa motivación legítima ni sugerir que quien la tiene actúa de mala fe.

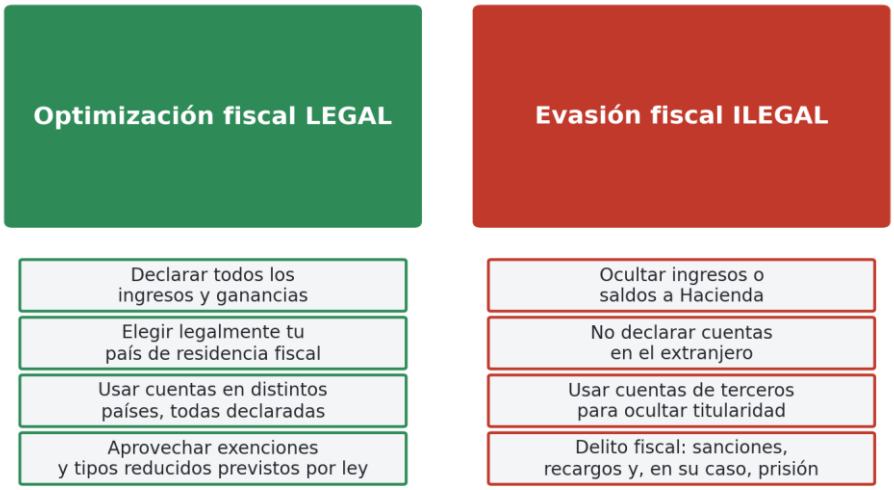
Lo que sí ha cambiado en 2026: el fin de la opacidad internacional

Donde este capítulo debe ser especialmente claro es en un punto técnico que muchos usuarios desconocen, y que cambia sustancialmente el cálculo de cualquiera que considere que abrir una cuenta en una fintech extranjera equivale a hacerla invisible para su administración tributaria de origen. Desde el 1 de enero de 2026 entró en vigor la versión ampliada del Estándar Común de Reporte de la OCDE (CRS 2.0), junto con el nuevo Marco de Reporte de Criptoactivos (CARF, Crypto-Asset Reporting Framework). Estos dos regímenes, complementarios entre sí, obligan a las entidades financieras -y, de forma explícita y por primera vez, a los exchanges y proveedores de servicios de criptoactivos- de las jurisdicciones participantes a identificar a sus titulares de cuenta y a reportar automáticamente esa información a la administración tributaria del país de residencia fiscal del titular, con el primer intercambio de datos correspondientes a 2026 previsto para 2027. El CARF, específicamente, rastrea las transacciones con criptoactivos, mientras que el CRS ampliado rastrea los saldos y las cuentas, incluyendo ahora explícitamente el dinero electrónico y las monedas digitales de banco central.

La implicación práctica es directa: Mercury, Airwallex, GrabrFi y, en la medida en que operan sobre infraestructura bancaria o de intercambio regulada, también Meru, SafePal y MetaMask Card en sus funciones de tarjeta, están constituidas o hacen negocios en jurisdicciones que participan en estos marcos de intercambio automático de información, precisamente porque

operan sobre bancos licenciados o sobre redes de tarjetas reguladas, como explicamos en el capítulo 46. Abrir una cuenta en cualquiera de estas plataformas no te saca del radar de tu administración tributaria de origen: en la inmensa mayoría de los casos, simplemente añade una fuente más de datos que esa administración recibirá, de forma automática y sin que tengas que hacer nada, al año siguiente.

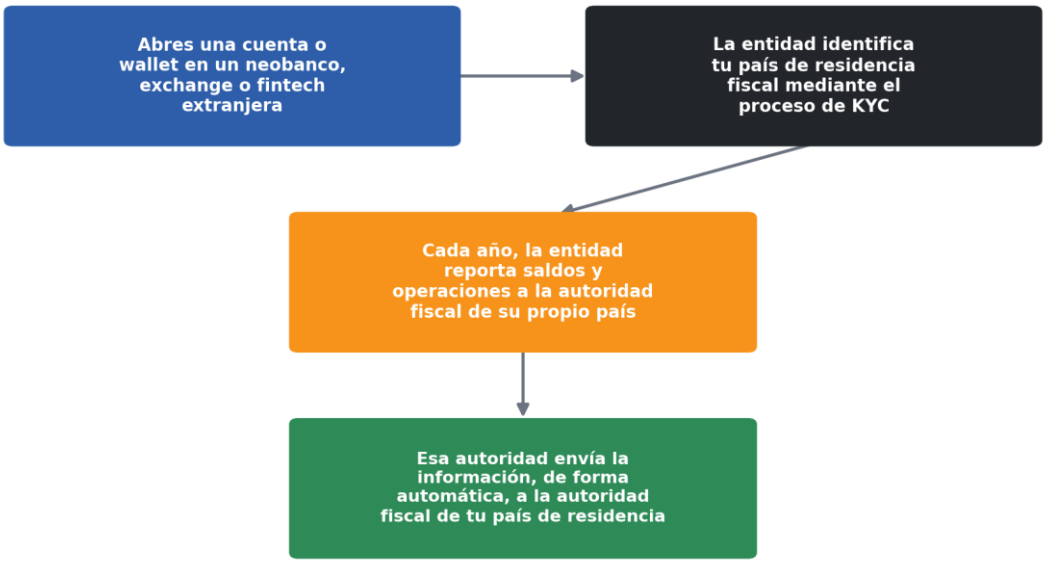
Dos cosas que se confunden a menudo, con consecuencias muy distintas



Ningún neobanco, wallet o tarjeta cripto mencionados en este capítulo cambia a cuál de las dos columnas pertenece una acción concreta: la diferencia la marca si se declara o no.

La diferencia entre optimizar tu fiscalidad dentro de la ley y evadirla no depende de qué herramienta uses, sino de si declaras.

Cómo funciona el intercambio automático de información (CRS 2.0 / CARF)



Así llega la información de tu cuenta o wallet extranjera a la autoridad fiscal de tu país de residencia.

Optimización fiscal legal frente a evasión fiscal ilegal: la distinción que de verdad importa

Es fundamental separar con toda claridad dos conceptos que el lenguaje coloquial mezcla constantemente, porque tienen consecuencias legales radicalmente distintas:

- La optimización o planificación fiscal legal consiste en estructurar tus finanzas dentro de las reglas que la ley permite: elegir de forma genuina tu residencia fiscal (lo que exige, casi siempre, vivir realmente en el país elegido, no solo abrir una cuenta allí), aprovechar exenciones, deducciones y regímenes especiales previstos expresamente por la normativa de cada país, o distribuir tu patrimonio entre distintas jurisdicciones y activos siempre que declares correctamente cada uno de ellos ante la administración que corresponda. Nada de esto es ilegal ni moralmente cuestionable: es, literalmente, usar la ley tal como está escrita.
- La evasión fiscal ilegal consiste en ocultar activos, ingresos o cuentas a la administración tributaria a la que legalmente debes declararlos, ya sea no reportando una cuenta en el extranjero, infravalorando deliberadamente ganancias patrimoniales, o usando la titularidad de terceros para esconder quién controla realmente un activo. En España, como recordamos del capítulo 34, esto puede constituir un delito fiscal si la cuota defraudada supera un umbral determinado, con sanciones que incluyen recargos económicos sustanciales y, en los casos más graves, penas de prisión, además de que ninguna de las plataformas descritas en este bloque ofrece de verdad el anonimato que haría posible ocultar esa información sin ser detectado, precisamente por el marco de intercambio automático que acabamos de describir.

Este libro no puede, ni pretende, ofrecer asesoramiento legal o fiscal personalizado: la fiscalidad de cada persona depende de su residencia, su nacionalidad, el origen de sus ingresos y decenas de variables específicas que solo un asesor fiscal cualificado, familiarizado con tu situación concreta, puede evaluar correctamente. Lo que sí puede decir, con la misma seguridad con la que ha tratado cualquier otro tema de este libro, es que ninguna de las herramientas descritas en los capítulos 46 a 48 -por sofisticada, internacional o "cripto-nativa" que parezca- convierte automáticamente una obligación fiscal existente en una obligación inexistente, y que tratarlas como si lo hicieran expone a quien lo intente a un riesgo legal real, no a una simple posibilidad remota.

Una nota final sobre el gasto cotidiano con tarjetas cripto

Vale la pena repetir, en este contexto, lo que ya señalamos en el capítulo 48: cada pago realizado con una tarjeta vinculada directamente a un saldo cripto -MetaMask Card, la tarjeta de SafePal, o cualquier equivalente- constituye, en la mayoría de los sistemas fiscales, una disposición del activo sujeta a declaración, exactamente igual que una venta en un exchange. La automatización y la comodidad de estas herramientas hacen que sea sorprendentemente fácil acumular, sin darse cuenta, un volumen considerable de operaciones sujetas a declaración simplemente por el uso cotidiano de una tarjeta, un detalle práctico que conviene tener presente antes de adoptar cualquiera de estas soluciones como método principal de gasto diario, y que refuerza, una vez más, una idea que recorre todo este libro: la tecnología puede cambiar radicalmente cómo se mueve el dinero, pero no deroga, por sí sola, ninguna obligación legal de quien lo mueve.

> *La libertad financiera que defendimos en el capítulo 27 -la capacidad de moverte, ahorrar y diversificarte sin depender de un único punto de control- es perfectamente compatible con cumplir tus obligaciones fiscales; de hecho, es precisamente esa combinación, y no su ausencia, la que hace sostenible a largo plazo cualquier estrategia financiera basada en estas herramientas.*

Con esto cerramos el bloque dedicado a neobancos y banca cripto. El siguiente y último capítulo del libro recoge, a modo de referencia rápida, el glosario de términos utilizados a lo largo de toda esta obra.

Fuentes y estudios citados en este capítulo

- OCDE. "Consolidated text of the Common Reporting Standard" (2025) y documentación sobre el Crypto-Asset Reporting Framework (CARF), en vigor desde el 1 de enero de 2026.
- Sovereign Group y EY Singapur (2026). Análisis técnico sobre CRS 2.0 y CARF y su impacto en la transparencia fiscal global de los criptoactivos.
- Gobierno de Jersey y otras administraciones participantes (2026). Documentación oficial sobre la implementación del CARF y la ampliación del CRS.
- Agencia Tributaria española. Régimen sancionador del delito fiscal y obligaciones de declaración de cuentas y criptoactivos en el extranjero (Modelo 721), citado también en el capítulo 34.
- Federal Court of Canada, Human Rights Watch y demás fuentes sobre los episodios de control financiero estatal citados en el capítulo 27, referenciadas aquí como contexto de la motivación legítima descrita al inicio de este capítulo.

PARTE VIII

REFERENCIA

Capítulo 50. Glosario de términos

Este glosario reúne, por orden alfabético, los términos técnicos más importantes introducidos a lo largo del libro, con una definición breve y el capítulo donde se explican con más profundidad, para que puedas usarlo como referencia rápida en el futuro.

A - D

- ASIC (capítulo 11): circuito integrado diseñado específicamente para calcular hashes SHA-256 de forma muy eficiente; el hardware dominante en la minería de Bitcoin actual.
- Bloque (capítulo 7): paquete de transacciones agrupadas y encadenadas criptográficamente al bloque anterior.
- Bloque génesis (capítulo 6): el primer bloque de la cadena de Bitcoin, minado por Satoshi Nakamoto el 3 de enero de 2009.
- Blockchain (capítulo 7): el registro público y compartido de todas las transacciones de Bitcoin, formado por bloques encadenados mediante hashes.
- Clave privada (capítulo 9): número secreto que otorga control total sobre los fondos asociados a él; nunca debe compartirse.
- Clave pública (capítulo 9): valor derivado matemáticamente de la clave privada, que se puede compartir sin riesgo y que permite verificar firmas.
- Coinbase (capítulo 11): la transacción especial que encabeza cada bloque y a través de la cual se crean los bitcoins nuevos.
- Cold wallet / monedero frío (capítulo 10): wallet cuyas claves privadas nunca han estado conectadas a internet.
- Confirmación (capítulo 7): cada bloque adicional minado sobre el bloque que contiene una transacción, que aumenta la seguridad frente a una posible reversión.
- Dificultad (capítulo 11): parámetro que regula cuán difícil debe ser encontrar un hash de bloque válido, ajustado automáticamente cada 2.016 bloques.

- Dirección (capítulo 9): identificador público, derivado de la clave pública, que se comparte para recibir pagos.
- Doble gasto (capítulo 2): el intento de gastar la misma unidad de dinero digital dos veces; el problema central que Bitcoin resuelve.

E - H

- Fork (capítulo 21): una bifurcación en las reglas del protocolo; puede ser "soft" (compatible hacia atrás) o "hard" (incompatible).
- Frase semilla / seed phrase (capítulo 9): secuencia de 12 o 24 palabras de la que se derivan todas las claves de una wallet.
- Hard fork (capítulo 21): cambio de reglas del protocolo incompatible con el software anterior, que puede dividir la red en dos cadenas.
- Hashrate (capítulo 16): la potencia de cómputo total dedicada a la minería en la red, medida en hashes por segundo.
- Halving (capítulo 13): la reducción a la mitad de la recompensa por bloque, que ocurre cada 210.000 bloques (aproximadamente cada cuatro años).
- Hot wallet / monedero caliente (capítulo 10): wallet cuyas claves privadas están, en algún momento, en un dispositivo conectado a internet.

L - N

- Lightning Network (capítulo 22): protocolo de segunda capa que permite pagos casi instantáneos y de bajo coste fuera de la cadena principal.
- Mempool (capítulo 11): el conjunto de transacciones válidas que están pendientes de ser incluidas en un bloque.
- Merkle root / raíz de Merkle (capítulo 7): hash único que resume de forma verificable todas las transacciones de un bloque.
- Minería (capítulo 11): el proceso de competir por encontrar un hash de bloque válido, que crea bitcoins nuevos y asegura la red.
- Multisig / multifirma (capítulo 10): configuración de wallet que exige varias firmas independientes para autorizar un gasto.
- Nodo (capítulo 12): ordenador que ejecuta el software de Bitcoin y valida de forma independiente bloques y transacciones.
- Nonce (capítulo 11): número que los mineros modifican repetidamente al intentar encontrar un hash de bloque válido.

P - S

- Prueba de trabajo / Proof of Work (capítulo 11): mecanismo que exige un coste computacional real, verificable en un instante, para proponer el siguiente bloque.
- SegWit (capítulo 21): mejora de 2017 que separa los datos de firma del resto de la transacción, aumentando la capacidad efectiva de los bloques.

- Sybil, ataque (capítulo 17): creación de múltiples identidades falsas por un mismo atacante para intentar ganar influencia desproporcionada.
- Satoshi (capítulo 13): la unidad más pequeña de bitcoin, equivalente a 0,00000001 BTC.
- Soft fork (capítulo 21): cambio de reglas del protocolo compatible con el software anterior (más restrictivo, no incompatible).

T - U

- Taproot (capítulo 21): mejora de 2021 que introduce firmas Schnorr y mejora la privacidad y eficiencia de los contratos complejos.
- UTXO (capítulo 8): "Unspent Transaction Output"; un fragmento de bitcoin creado como salida de una transacción y todavía no gastado.
- Whitepaper (capítulo 5): el documento técnico original de Bitcoin, publicado por Satoshi Nakamoto en octubre de 2008.