Market Talks
CENTRO DE EDUCACIÓN

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 3 DE 13

Antes de Bitcoin: los experimentos de dinero digital

Veinticinco años de intentos, casi aciertos y fracasos, y las piezas que cada uno dejó para Bitcoin

8 min de lectura 6 preguntas con sus respuestas

BLOCKCHAIN · PRINCIPIANTE · LECCIÓN 3 DE 13

Antes de Bitcoin: los experimentos de dinero digital

EN UNA FRASE

Bitcoin no surgió de la nada. Combinó ideas de proyectos anteriores de dinero digital y se diseñó para evitar la única debilidad que hizo caer a la mayoría de ellos.

Un sueño más antiguo que el navegador web

En las lecciones 1 y 2 vimos dos problemas: el dinero digital se puede copiar, y un sistema controlado por una sola parte puede ser congelado, cerrado o corrompido. Mucho antes de Bitcoin, criptógrafos y emprendedores ya intentaban resolver ambos.

Sus proyectos van de principios de los años ochenta a mediados de los dos mil. Algunos se convirtieron en negocios reales con clientes reales. Otros nunca salieron del papel. Ninguno triunfó del todo, pero casi todos aportaron algo que Bitcoin usaría después. Seguir su historia es la mejor manera de entender por qué Bitcoin está construido como está.



Figura 1. Más de 25 años de experimentos de dinero digital precedieron a Bitcoin. Cada uno dejó una pieza del diseño final.

DigiCash: privado, pero en manos de una empresa

En 1982, el criptógrafo David Chaum describió una técnica llamada **firma ciega**. Permite que un banco firme una moneda digital para confirmar que es válida sin ver qué moneda está firmando. El

resultado es dinero digital que se puede gastar de forma privada, casi como el efectivo, porque el banco no puede vincular un pago con la persona que retiró la moneda.

Chaum fundó DigiCash en 1989 para convertir la idea en un producto, y en 1995 el Mark Twain Bank de San Luis empezó a ofrecer su eCash a sus clientes. La tecnología funcionaba. El negocio no: se sumaron muy pocos bancos y comercios, y DigiCash se declaró en quiebra en 1998.

La debilidad de fondo era estructural. Cada moneda seguía teniendo que ser emitida por un banco o una empresa central, y esa misma parte central vigilaba el doble gasto. Cuando la empresa cayó, el dinero cayó con ella.

e-gold: respaldo real, un único punto de fallo

e-gold, lanzado en 1996, tomó otro camino. Cada unidad estaba respaldada por oro físico guardado en bóvedas, y los usuarios podían enviarse saldos respaldados en oro de un lado a otro del mundo en segundos. Creció rápido: en 2006 procesaba más de 2.000 millones de dólares en pagos al año.

Pero e-gold era una sola empresa, y eso la convertía en un solo blanco. La falta de verificación de identidad la hacía atractiva para delincuentes, y en 2007 las autoridades de EE. UU. acusaron a la empresa y a sus directivos. En 2008 se declararon culpables de conspiración para el lavado de dinero y de operar un negocio de transferencia de dinero sin licencia, y en 2009 se suspendieron las transferencias. Los titulares de cuentas esperaron años un proceso para recuperar sus fondos.

La enseñanza de la lección 2 se cumplió en la vida real: un único punto de control es también un único punto de fallo, ya sea por un hacker, una quiebra o una orden judicial.

Hashcash: encarecer las cosas a propósito

En 1997, el criptógrafo Adam Back propuso **Hashcash** como defensa contra el spam. Antes de enviar un mensaje, el ordenador del remitente tenía que resolver un pequeño acertijo, lo que exigía un momento de trabajo de cómputo. Para un solo correo, el coste es invisible. Para quien envía millones de mensajes de spam, se acumula muy rápido.

La clave está en la asimetría: el acertijo es lento de resolver pero instantáneo de comprobar. Cualquiera que reciba el correo puede confirmar que el trabajo se hizo sin repetirlo. Esta idea se llama **prueba de trabajo** (proof of work), y el whitepaper de Bitcoin cita Hashcash como influencia directa.

ANALOGÍA: LA PRUEBA DEL SUDOKU

Un sudoku difícil puede llevar una hora resolverlo, pero comprobar una cuadrícula terminada lleva un minuto. Si alguien te entrega un sudoku completo, sabes que se esforzó, aunque nunca lo viste hacerlo. La prueba de trabajo convierte esa idea en un sello digital de esfuerzo que cualquier ordenador puede verificar.

b-money, Bit Gold y RPOW: los planos

En 1998, dos propuestas se acercaron sorprendentemente a Bitcoin sobre el papel. El ingeniero informático Wei Dai describió **b-money**, en el que cada participante guarda una copia de quién posee qué, y el dinero nuevo se crea resolviendo problemas de cómputo. Por la misma época, el jurista e informático Nick Szabo propuso **Bit Gold**, que encadenaba soluciones de prueba de trabajo con marcas de tiempo para crear algo escaso y costoso de producir, una especie de oro digital.

Ninguno llegó a lanzarse. Ambos dejaron abierta una pregunta importante: si muchas personas independientes llevan los registros, ¿cómo se ponen de acuerdo sobre cuál es el correcto sin que nadie mande?

En 2004, el criptógrafo Hal Finney creó **RPOW** (pruebas de trabajo reutilizables), que permitía pasar fichas de prueba de trabajo de una persona a otra. Llegó a funcionar, pero para evitar el doble gasto dependía de un servidor de confianza que corría en un hardware seguro especial. Seguía habiendo una parte de confianza en el centro. Cinco años después, Finney recibiría el primer bitcoin enviado de una persona a otra.

La cadena de marcas de tiempo

Otra pieza llegó desde fuera del mundo del dinero. En 1991, los investigadores Stuart Haber y W. Scott Stornetta se preguntaron cómo demostrar cuándo se creó un documento digital y que no ha sido modificado desde entonces.

Su respuesta fue enlazar los registros en una cadena. Cada registro nuevo lleva una huella digital del anterior, así que cambiar cualquier registro antiguo rompería todos los eslabones siguientes. La historia se vuelve **a prueba de manipulaciones visibles**: aún puedes intentar reescribirla, pero todo el mundo verá que lo hiciste. El whitepaper de Bitcoin cita su trabajo tres veces, y la idea de enlazar registros así se convirtió en la «cadena» (chain) de blockchain. La lección 6 explica con detalle cómo funcionan estas huellas.

UN EJEMPLO REAL

Para que su cadena no se pudiera reescribir en silencio, la empresa de Haber y Stornetta empezó en 1995 a publicar una huella de sus registros más recientes en los anuncios clasificados de The New York Times. Cualquiera podía comparar un periódico impreso con la cadena, y nadie podía cambiar miles de ejemplares impresos a posteriori.

La pieza que faltaba

A mediados de los dos mil ya existían casi todas las piezas. Faltaba la más difícil:

Proyecto	Qué aportó	Qué seguía faltando
DigiCash (1989)	Pagos digitales privados	Dependía de un emisor central
Cadena de marcas de tiempo (1991)	Registros enlazados para que la historia no se pueda cambiar en silencio	No estaba pensada para el dinero
e-gold (1996)	Transferencias globales a gran escala	Una sola empresa que se podía cerrar
Hashcash (1997)	Prueba de trabajo: cara de crear, barata de verificar	No era dinero, solo un sello
b-money, Bit Gold (1998)	Registros compartidos y dinero creado mediante trabajo	Sin forma de acordar sin un líder; nunca se lanzaron
RPOW (2004)	Fichas de prueba de trabajo que se podían transferir	Dependía de un servidor de confianza

Cada intento dependía de alguien al mando o nunca resolvió cómo unos desconocidos podían acordar una sola historia sin él. En 2008, un autor anónimo juntó las piezas y añadió la que faltaba. Esa es la historia de la lección 4.

Por qué importa a los traders

- **Los emisores centrales fallan de formas conocidas.** DigiCash quebró y e-gold fue cerrado por la fiscalía. El mismo patrón volvió en 2013, cuando las autoridades de EE. UU. cerraron Liberty Reserve, otra moneda digital gestionada de forma centralizada. Cualquier activo que dependa de un solo emisor arrastra el riesgo empresarial y legal de ese emisor.
- **Las stablecoins de hoy recuerdan a e-gold.** Una stablecoin respaldada en dólares sigue un modelo parecido: una empresa mantiene reservas y emite tokens contra ellas. Por eso conviene entender las reservas, las licencias y la situación legal del emisor antes de confiar en una.
- **La narrativa del «oro digital» tiene raíces profundas.** La idea de Bit Gold de algo escaso porque es costoso de crear sigue influyendo en cómo muchos inversores comparan Bitcoin con el oro. Saber de dónde viene una narrativa te ayuda a juzgar cuánto peso merece cuando mueve el mercado.

Términos clave

Firma ciega	Forma en que un banco o emisor aprueba una moneda digital sin ver cuál aprueba, para que los pagos sigan siendo privados.
Prueba de trabajo	Evidencia de que un ordenador dedicó un esfuerzo real a resolver un acertijo. Lenta de producir, instantánea de comprobar.
Respaldado por activos	Dinero o tokens cuyo valor está sostenido por un activo real, como oro o dólares, en manos de un emisor.
Sellado de tiempo	Demostrar cuándo se creó un registro digital y que no se ha modificado desde entonces.
A prueba de manipulaciones visibles	Diseñado para que cualquier cambio en registros pasados sea visible para todos, aunque no se pueda impedir físicamente.
Escasez digital	Una oferta limitada de algo digital que no se puede simplemente copiar ni crear gratis.

Ideas clave

1. Los experimentos de dinero digital empezaron a principios de los años ochenta, más de 25 años antes de Bitcoin.
2. DigiCash aportó privacidad y e-gold escala global, pero ambos dependían de una sola empresa y cayeron con ella.
3. Hashcash introdujo la prueba de trabajo: un esfuerzo lento de producir pero instantáneo de verificar.
4. b-money, Bit Gold y RPOW esbozaron registros compartidos y dinero basado en trabajo, pero ninguno resolvió cómo unos desconocidos podían acordar sin una parte de confianza.
5. Las marcas de tiempo enlazadas mostraron cómo hacer que la historia sea a prueba de manipulaciones visibles. Bitcoin combinó estas piezas y añadió la que faltaba.

Ponte a prueba

Marca con un círculo una respuesta en cada pregunta. Las respuestas con su explicación están en la página siguiente. También puedes hacer este cuestionario en línea en markettalks.info y ver tu puntuación al instante.

1. ¿Cuál fue la innovación clave de DigiCash?

- A Oro guardado en bóvedas
- B Firmas ciegas que hacían privados los pagos digitales
- C Prueba de trabajo para frenar el spam
- D Un registro copiado por cada usuario

2. ¿Por qué terminó e-gold?

- A Por acciones legales contra la única empresa que lo gestionaba
- B Le robaron sus reservas de oro
- C Un fallo permitía a los usuarios copiar monedas
- D Sus usuarios se pasaron a Bitcoin

3. ¿Para qué se diseñó originalmente Hashcash?

A. Hacer privados los pagos en línea
B. Guardar saldos respaldados en oro
C. Encarecer el envío de spam por correo
D. Sellar en el tiempo documentos legales

4. ¿Qué propiedad hace útil la prueba de trabajo?

A. Cualquiera puede producirla al instante
B. Solo puede comprobarla un servidor central
C. Es fácil de copiar
D. Es lenta de producir pero instantánea de verificar

5. ¿Qué aportó el trabajo de Haber y Stornetta de 1991?

A. Dinero digital respaldado en oro
B. Enlazar registros en una cadena para que cambiar la historia sea visible
C. Correo electrónico anónimo
D. El primer exchange de criptomonedas

6. Antes de 2008, ¿qué pieza seguía faltando?

A. Conexiones a internet más rápidas
B. Una forma de hacer privados los pagos
C. Una forma de que desconocidos acordaran una sola historia compartida sin nadie al mando
D. Ordenadores lo bastante potentes para la prueba de trabajo

Respuestas

1 B

Firmas ciegas que hacían privados los pagos digitales

Las firmas ciegas de David Chaum permitían a un banco aprobar una moneda sin ver cuál era, así que los pagos podían ser privados, casi como el efectivo.

2 A

Por acciones legales contra la única empresa que lo gestionaba

e-gold lo gestionaba una sola empresa. Tras la acusación de la fiscalía, la empresa y sus directivos se declararon culpables en 2008 y las transferencias se suspendieron en 2009. Una empresa significaba un único punto de fallo.

3 C

Encarecer el envío de spam por correo

Adam Back propuso Hashcash para combatir el spam. Cada correo exigía un poco de trabajo de cómputo: nada para un mensaje, muy costoso para millones.

4 D

Es lenta de producir pero instantánea de verificar

Como un sudoku terminado, la prueba de trabajo cuesta esfuerzo crearla pero solo un momento comprobarla. Así cualquiera puede confirmar que el trabajo se hizo sin repetirlo.

5 B

Enlazar registros en una cadena para que cambiar la historia sea visible

Cada registro lleva una huella del anterior, así que cambiar un registro antiguo rompe todos los eslabones posteriores. Esta idea se convirtió en la «cadena» de blockchain.

6 C

Una forma de que desconocidos acordaran una sola historia compartida sin nadie al mando

Los sistemas anteriores dependían de una parte de confianza o nunca resolvieron cómo muchos participantes independientes podían acordar un solo registro. Bitcoin añadió esa pieza, como explica la lección 4.

FUENTES

- Departamento de Justicia de EE. UU., declaraciones de culpabilidad de e-gold (julio de 2008): https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- Wikipedia, DigiCash: https://en.wikipedia.org/wiki/DigiCash
- Wikipedia, e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute, Hal Finney: RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph, el coinventor de la blockchain explica por qué no es Satoshi Nakamoto: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

SIGUE APRENDIENDO

A continuación: Lección 4 2008 y el nacimiento de Bitcoin

Esta lección forma parte del curso gratuito de Blockchain del Centro de Educación de MARKET TALKS: lecciones de nivel principiante, intermedio y avanzado, cada una con un cuestionario y un PDF descargable.

Centro de Educación
Lecciones desde los principios básicos hasta temas avanzados

Análisis de Mercados
Análisis técnico y fundamental de los principales mercados

Informes
Bitcoin, Oro, Plata, SPX y más

markettalks.info

Telegram @MARKET_TALKS

Solo con fines educativos. Nada en este documento constituye asesoramiento financiero. © 2026 MARKET TALKS. Puedes compartir este PDF libremente sin modificarlo.