

BEN MCKENZIE

y Jacob Silverman

DINERO FÁCIL

*Las criptomonedas,
el capitalismo de casino
y la era dorada del fraude*



EDICIONES OBELISCO

Si este libro le ha interesado y desea que le mantengamos informado de nuestras publicaciones, escribanos indicándonos qué temas son de su interés (Astrología, Autoayuda, Ciencias Ocultas, Artes Marciales, Naturismo, Espiritualidad, Tradición...) y gustosamente le complaceremos.

Puede consultar nuestro catálogo en www.edicionesobelisco.com

Colección Éxito

DINERO FÁCIL

Ben McKenzie y Jacob Silverman

1.^a edición: abril de 2024

Título original: *Easy Money*

Traducción: *David George*

Maquetación: *Isabel Also*

Corrección: *M.^a Jesús Rodríguez*

© 2023, Ben M. Schenkkan

Primera edición en inglés por Abrams Press,

sello editorial de Abrams, NY, USA

(Reservados todos los derechos)

© 2024, Ediciones Obelisco, S. L.

(Reservados los derechos para la presente edición)

Edita: Ediciones Obelisco, S. L.

Collita, 23-25. Pol. Ind. Molí de la Bastida

08191 Rubí - Barcelona - España

Tel. 93 309 85 25

E-mail: info@edicionesobelisco.com

ISBN: 978-84-1172-118-9

DL B 2830-2024

Impreso en SAGRAFIC

Passatge Carsí, 6 - 08025 Barcelona

Printed in Spain

Reservados todos los derechos. Ninguna parte de esta publicación, incluido el diseño de la cubierta, puede ser reproducida, almacenada, transmitida o utilizada en manera alguna por ningún medio, ya sea electrónico, químico, mecánico, óptico, de grabación o electrográfico, sin el previo consentimiento por escrito del editor. Diríjase a CEDRO (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

ÍNDICE

Capítulo 1: El dinero y las mentiras	11
Capítulo 2: ¿Qué podría salir mal?	41
Capítulo 3: La impresora de dinero va a toda máquina.	49
Capítulo 4: Comunidad.	71
Capítulo 5: SXSW, la CIA y los 1,5 billones de dólares que no estaban ahí.	99
Capítulo 6: El negocio del espectáculo	123
Capítulo 7: El dictador más genial del mundo	149
Capítulo 8: Ratas en un saco	165
Capítulo 9: El emperador va desnudo.	193
Capítulo 10: ¿Quién está al mando aquí?	229
Capítulo 11: Desquíbrate a ti mismo	253
Capítulo 12: Declaración de bancarrota	275
Capítulo 13: El padre del predicador	305
Epílogo.	323
Agradecimientos.	339
Apéndice	341
Índice analítico.	343

*A Morena, Julius, Frances y Arthur, mi equipo de casa,
y en recuerdo de Chris Huvane*

NOTA DEL AUTOR

Si actualmente posees o has poseído criptomonedas y has perdido dinero con esa inversión, ten por seguro que no estás solo. De hecho, te encuentras entre las filas de la gran mayoría de los cripto inversores, que sólo en Estados Unidos se cuentan por decenas de millones, llegando a los cientos de millones a nivel mundial. Este libro es para ti, te guste o no. Si quieres disponer de una ventana para ver cómo podrían haberte estafado, sigue leyendo.

Si te encuentras entre el 84% de los habitantes de Estados Unidos que no picaron, te felicito, pero no te pongas demasiado arrogante. La vida es una apuesta y nadie conoce las probabilidades.

Para que lo tengamos claro, la apuesta va en los dos sentidos. Lo que viene a continuación es mi opinión sobre los sucesos tal y como los percibí a lo largo de los casi dos años que pasé en la ratonera de las criptomonedas. A lo largo del libro empleo términos como «estafadores», «timadores», «defraudadores» y «tramposos» en referencia a los distintos actores en el sector de las criptomonedas. Estos calificativos no son más que un apunte taquigráfico de mi opinión. No quiero insinuar que una persona concreta haya quebrantado una ley o violado una normativa. De forma similar, no todos los que trabajan con criptomonedas tienen malas intenciones. Aunque puede que estemos en gran desacuerdo en cuanto a la utilidad de las criptomonedas, no han cometido ningún fraude. Espero que os unáis a mí para condenar a los que sí lo han hecho.

Que las fichas caigan donde tengan que caer.

CAPÍTULO 1

EL DINERO Y LAS MENTIRAS

Éste es un libro sobre las criptomonedas y el fraude: una parábola sobre el dinero y las mentiras, o más bien una parábola sobre el dinero falso y las mentiras por el dinero. En cuanto a la temática, tiene un sorprendente parecido con una leyenda popular. Al contrario de lo que sucede con esa fábula, esta historia es real.

Empezamos durante la salvaje fiebre especuladora de la era Trump. Fue la fugaz época de las acciones meme (acciones que se han popularizado debido a su presencia en las redes sociales), los NFT (tokens o vales no fungibles) y las ventas de terrenos en el metaverso. Aunque puede que el marketing fuese nuevo, los aspectos económicos eran familiares: estos planes especulativos para hacerse rico rápidamente no eran más que la última iteración del capitalismo de casino. La economista política Susan Strange¹ popularizó el término en la década de 1980, pero sus orígenes se remontan hasta por lo menos la década de 1930. En *Teoría general de la ocupación, el interés y el dinero*,² el economista John Maynard Keynes reprobó los ciclos de prosperidad y depresión de las acciones, en los que las apuestas con pocas probabilidades de ganar en los mercados no regulados (especialmente antes de la inven-

1. Strange, S.: *Casino capitalism*. Basil Blackwell, 1986.

2. Keynes, J. M.: *The general theory of employment, interest and money*. Palgrave Macmillan, 1936. (Trad. cast.: *Teoría general de la ocupación, el interés y el dinero*. Ciro, D.L.: Barcelona, 2011).

ción de las leyes de los mercados de valores) creó y destruyó fortunas de la noche al día. Casi un siglo después, el descriptor «casino» resulta ser todavía más adecuado: las criptomonedas y sus subproductos relacionados suelen ser considerados por los economistas como el mejor juego de suma cero. El beneficio de una persona es la pérdida para otra.

Puede que te hayas dado cuenta de algo sobre las criptomonedas: No *hacen* nada. Ciertamente, puedes negociar con ellas, apostando a que una subirá o bajará, pero no se usan para nada productivo. Las criptomonedas no están ligadas a nada de verdadero valor, al contrario que las acciones de una compañía o los futuros de una materia prima. Son código informático que no está relacionado con ningún activo real. Incluso los productos financieros más arcanos tienen algún tipo de relación con algo de utilidad en el mundo material. Como, de hecho, no generan ningún valor en sí mismas, invertir en criptomonedas se parece más a apostar: barajar activos entre los participantes en un juego de azar. Es el equivalente digital de jugar al póquer en un casino: puede que ganes, pero no se da un incremento en la utilidad general. No se ha generado nada de valor jugando. Los juegos de suma cero son estrictamente competitivos: para que tú ganes otro jugador debe perder. De forma muy parecida a lo que sucede en un casino normal, es necesario que los jugadores paguen una pequeña cantidad por cada mano para hacer que el juego siga adelante. En el caso de las criptomonedas, este dinero procede de las tasas que cobran los mercados, además de los costes relacionados con la validación de las transacciones. En Las Vegas, a esto se le llama *el rastrillo*: la cantidad que la casa se lleva de cada bote. Esto significa que, con el tiempo suficiente, el jugador medio perderá. Así es como los casinos siguen funcionando. Dado un período de tiempo lo suficientemente largo, la casa siempre gana: tiene que hacerlo.

Por afirmar lo obvio, las apuestas (el juego) no son realmente un caso válido que usar con respecto a las criptomonedas. Puedes apostar por literalmente cualquier cosa que no haya sucedido todavía. Podría, por ejemplo, apostar a que acabarás la frase que estás leyendo ahora (yo gano). Incluso las apuestas autorizadas no suponen un uso productivo del capital, y profundizaremos en sus numerosísimos inconvenientes a lo largo de este libro, pero por lo menos, cuando vayas

a Las Vegas conocerás las probabilidades. Hay una larga lista de reglas y normas que un casino debe seguir. La experiencia también tiene un valor de entretenimiento. Los jugadores pueden ganar o perder dinero en las mesas, pero por lo menos les regalan algunas bebidas y pueden disfrutar de una buena cena o del espectáculo. En ocasiones sospechaba que era incluso peor que eso.

Eso nos lleva a la *Época Dorada del Fraude*.³ Jim Chanos, el legendario vendedor al descubierto que acuñó la expresión, conoce bien el tema. Apostar contra compañías fraudulentas como Enron y la empresa alemana de pagos Wirecard le hizo ganar una fortuna. En la actualidad, Chanos ve fraudes (definidos como engaños para el beneficio personal, generalmente económico) en casi cada lugar en el que mira. Cuando empecé a prestar atención a los mercados financieros en otoño de 2020, llegué a una conclusión similar, con una sensación preocupante de que los trapicheos y la mentira habían invadido todos los aspectos de la economía, operando con impunidad política y legal. Eso me hizo querer gritar de rabia y hacer una apuesta propia.

En 2016, Estados Unidos eligió a un estafador como presidente. Millones de estadounidenses de toda condición social votaron por Donald Trump en lugar de por Hillary Clinton. Aunque Clinton ganó en términos de votos por millones de papeletas, no importó. Gracias al peculiar funcionamiento del sistema electoral, la mayor economía del mundo eligió a un hombre que miente sobre lo que sea. Donald Trump no fue el primer mentiroso en ocupar la Casa Blanca, pero puede que haya sido el primero en existir en un mundo que escapaba a la razón. Ayudó a crear una cultura política en la que la verdad (la realidad por consenso basada en los hechos) no importaba. Fue la época de los «hechos alternativos». El fraude y la corrupción podían operar sin miedo a las consecuencias.

El aumento simultáneo de la difusión de desinformación se ha documentado muy bien junto con una tendencia relacionada con ello: la erosión de la confianza entre los ciudadanos y su gobierno y también los unos con los otros. En una sociedad carente de confianza existe el

3. Agnew, H.: «Jim Chanos: “We are in the golden age of fraud”», *Financial Times*, 24 de julio, 2020.

riesgo de que los conflictos se vuelvan demasiado comunes, al tiempo que las sospechas y la mala fe dominen todas las interacciones. Cuando la confianza se desmorona masivamente, cuando la desinformación se extiende como un virus, cuando hay pocas instituciones que merezcan nuestra confianza o respeto, y cuando la gente considera que la única forma de ganar es hacer que alguien pierda, nos encontramos en terreno peligroso.

Dinero fácil es un trabajo de tipo reportaje, con una selección de entre cientos de entrevistas, con muchas noches de investigación mentalmente agotadora hasta altas horas y varias aventuras estrambóticas en el mundo del dinero digital falso. Mi colega Jacob Silverman y yo hemos hablado con gente de dentro y fuera del mundo de las criptomonedas, los titanes del sector y ciudadanos corrientes, creyentes, escépticos, víctimas, villanos y algunas personas escurridizas a las que fue difícil encontrar. Aunque el relato empieza conmigo, este libro tiene que ver con ellos. A lo largo de los siguientes trece capítulos, te llevaremos a un viaje que empieza en mi diminuta oficina en Brooklyn y se expande rápidamente para abarcar todo el mundo. Desde Texas a Florida, El Salvador a Washington D.C., e incluso las afueras de Manhattan, te proporcionaremos un vistazo al interior de uno de los mayores fraudes en la historia y que es mayor que el de Madoff por un orden de magnitud.

Como actor de televisión durante muchos años con un grado en económicas obtenido hace décadas, podría ser una opción improbable como autor de un libro sobre las criptomonedas; pero por raro que parezca, de hecho, mi formación me sitúa en un buen lugar para pinchar la burbuja alucinatoria alimentada por el dinero de mentira. En su esencia, éste es un relato sobre el dinero y la mentira. Lo que sé sobre el dinero lo aprendí en un aula hace más de veinte años (y ganando algo de dinero en Hollywood). Lo que sé sobre mentir lo aprendí gracias a pasar dos décadas en el mundo del espectáculo. La criptografía, las ciencias informáticas y las finanzas no son mi fuerte, pero puedo reconocer cuándo se están usando para conjurar (vender) una narrativa que puede que no sea verdad.

Yo también soy un cuentacuentos, así que permíteme que te cuente uno.



En otoño de 2020, el mercado de las llamadas criptomonedas (pedazos de código protegidos criptográficamente, las transacciones con los cuales suelen estar registradas en libros de contabilidad distribuidos conocidos como *blockchains* o cadenas de bloque) se dispararon. Unos pocos miles de criptomonedas⁴ en 2020 crecieron hasta ser 20 000 dos años después, y su presunto valor aumentó conjuntamente, desde unos 300 000 millones de dólares en el verano de 2020 hasta los tres billones de dólares en noviembre de 2021. Se estima que 40 millones de estadounidenses⁵ (en su enorme mayoría jóvenes y varones) se vieron arrastrados por ese frenesí especulativo. Vertieron miles de millones de dólares, euros, yuanes y otras divisas reales en tokens o vales digitales en las más de 500 criptomonedas que operaban a nivel mundial. La mayoría invirtió debido a una sencilla razón (querían ganar dinero) y se vieron inspirados por los relatos (y rumores en las redes sociales) de amigos y desconocidos que habían cosechado enormes beneficios invirtiendo en tokens digitales. Infectados por el miedo a quedarse fuera, ahora querían una parte de la acción.

A medida que más gente invirtió en ese bombo publicitario y vio cómo sus inversiones aumentaban de valor (por lo menos en la pantalla), se convirtieron en discípulos de facto de este sector incipiente, predicando el evangelio de las criptomonedas a todo aquel que quisiera escuchar. Los beneficios potenciales parecían ilimitados, y las barreras para la entrada eran pocas. Lo único necesario para poseer un pedazo de «dinero del futuro» era la voluntad de desprenderse de la versión real de él. Cuanta más gente invertía más subían los precios, lo que daba como resultado más miedo a quedarse fuera, lo que atraía a todavía más gente: una dinámica autorreforzante común a las burbujas económicas y los esquemas Ponzi. De forma sencilla, las criptomonedas se habían vuelto virales.

4. CoinMarketCap: «Today's cryptocurrency prices by market cap». <https://Coinmarketcap.com>

5. Centro de Investigaciones Pew, 11 de noviembre, 2021.

En su libro de 2019⁶ *Narrativas económicas: Cómo las fake news y las historias virales afectan la marcha de la economía*, el economista Robert Shiller, ganador del Premio Nobel, examinaba cómo las narrativas económicas se difundieron recurriendo a décadas de investigaciones en campos como la historia, la sociología, la antropología, la psicología, el marketing, la crítica literaria, y quizás y más apropiadamente para nuestros objetivos, la epidemiología. Definió una narrativa económica como «un relato contagioso que tiene el potencial de cambiar la forma en la que la gente toma decisiones económicas, como la decisión de... invertir en un activo especulativo volátil». ¿Su primer ejemplo?: El bitcoin.

Las historias que calan en el público no surgen de la nada: forman parte de la sociedad y de la cultura de las que surgen. De forma similar, las narrativas económicas se desarrollan como respuesta a los eventos económicos reales. La causalidad discurre en ambos sentidos: una narrativa económica que se desarrolle como reacción a un evento económico concreto puede precipitar uno futuro.

Imagina un pequeño banco en un pueblo. Un año una sequía da como resultado una mala cosecha, eliminando cualquier beneficio que los agricultores locales pudieran haber previsto. Empieza a extenderse el rumor de que los agricultores podrían no poder pagar sus préstamos. La posición económica del banco es, de hecho, sana y está asegurada frente a esa posibilidad, pero este rumor gana fuerza y se genera una narrativa económica de que el propio banco podría acabar siendo insolvente. A medida que cada vez más depositantes intentan sacar su dinero, se produce una estampida bancaria que da como resultado un colapso financiero. El suceso económico, una sequía, no produjo directamente la estampida bancaria, ya que el banco gozaba de buena salud. Fue la rápida difusión de una narrativa económica distorsionada la que dio lugar a su caída. *Narrativas económicas: Cómo las fake news y las historias virales afectan la marcha de la economía*, se publicó en 2019, antes de la actual difusión viral de las criptomonedas y de la pandemia

6. Shiller, R.: *Narrative Economics*. Princeton University Press, 2019. (Trad. cast.: *Narrativas económicas: Cómo las fake news y las historias virales afectan la marcha de la economía*. Ediciones Deusto, Barcelona, 2012).

de la COVID-19. Dada esta situación, es destacable observar cuán entrelazados se volverían estos dos virus en los siguientes años.

Para comprender los orígenes de las narrativas económicas en torno al bitcoin y otras criptomonedas, debemos remontarnos a los eventos que las inspiraron. Tanto las criptomonedas como las políticas del «dinero fácil» de las que este libro toma su título surgieron de las mismas raíces: la crisis financiera global (CFG), también conocida como la *crisis de las hipotecas subprime*.



En 2008, un terremoto económico sacudió los cimientos de la economía mundial. Sin saberlo los estadounidenses, la presión se había ido acumulando bajo la superficie del mercado de la vivienda durante años. Dos de sus mayores generadores fueron la desregulación financiera y los bajos tipos de interés: un empeño político de décadas de duración y bipartito para hacer crecer el sector financiero en combinación con una política dirigida a estimular la economía tras la primera burbuja de las compañías puntocom. Entre 2000 y 2003,⁷ la Reserva Federal (el banco central de Estados Unidos) redujo los tipos de interés del 6,5 % al 1 %. Miembros del Congreso de ambos partidos, además de la Administración de George W. Bush, potenciaron que el crédito fluyera en el mercado de la vivienda. La aspiración política expresada fue la de crear una «sociedad de propiedad» formada por dueños de viviendas.

Sin embargo, el efecto económico resultó ser menos noble. Los prestamistas concedieron hipotecas con desenfreno, frecuentemente a gente humilde o de clase trabajadora que tenían pocas posibilidades de amortizarlas. A muchos les fueron concedidas las llamadas hipotecas *subprime* (de alto riesgo). Como era más probable que el prestatario no lograra pagarlas que el receptor de una hipoteca de bajo riesgo, el préstamo tenía unos mayores tipos de interés (que frecuentemente eran variables). Los préstamos de baja calidad fueron entonces agrupados por los bancos en forma de valores respaldados por las hipotecas y de

7. FRED Economic Data/St. Louis Fed: «Interest rates, discount rate for United States». <https://fred.stlouisfed.org/series/INTDSRUSM193N>

obligaciones colateralizadas por impago (OCI). Esos paquetes de préstamos fueron, entonces, puestos en el mercado como de bajo riesgo y vendidos en grandes cantidades a inversores institucionales y a otros grandes clientes. Algunos de estos productos financieros basados en hipotecas se trocearon todavía más y fueron reconfigurados en forma de instrumentos financieros aún más complicados. Las agencias de *rating* (cuyo cometido era valorar el riesgo) otorgaron una alta calificación a productos financieros que prácticamente no tenían valor para complacer a sus clientes de Wall Street. Como resultado de ello, la rigidez, la complejidad y el apalancamiento se filtraron en el sistema financiero hasta un punto que, incluso, muchos profesionales del mundo de las finanzas no comprendieron.

Los economistas se centran en estructuras de incentivos, y con las hipotecas *subprime*, los incentivos se distorsionaron en sentido ascendente y descendente de la cadena. Desde el agente hipotecario que esperaba ganar una comisión hasta el ejecutivo que necesitaba mostrar unas cifras de ventas cada vez mejores a los consejos de administración, centrados en los beneficios, pocos tenían incentivos para dar un paso atrás y preguntar si algo de todo aquello era prudente. El pensamiento económico dominante de la época era que los precios de la vivienda no harían más que subir. La idea de que pudiera haber un gran descenso en el valor de la vivienda en Estados Unidos parecía improbable e incluso ridícula. ¿Cuándo había sucedido eso antes? Por supuesto, hubo señales de advertencia, y algunas personas ganaron mucho dinero apostando a un crac, tal y como mostró *La gran apuesta* en el libro y en la gran pantalla; pero la gente que manejaba el dinero y sus aliados en el poder pensaron que los buenos tiempos durarían siempre, por lo que promulgaron políticas egoístas e hicieron apuestas arriesgadas. Esta imprudencia es fácil que se dé cuando apuestas con el dinero de otras personas, hay pocas probabilidades de que se te haga responsable y puedes convencerte de que el mercado sólo avanza en una dirección.

Cuando el mercado inmobiliario siguió ahogándose a principios de 2008 y la economía mostró señales de entrar en una recesión, el gobierno federal intervino, intentando prevenir un mayor desastre. En enero, la Reserva Federal redujo los tipos de interés en tres cuartos de punto: el mayor recorte en veinticinco años. No fue suficiente: era necesaria una

acción más decidida para detener el colapso de la industria financiera y, por extensión, de toda la economía. En marzo, el gobierno empezó a rescatar a los agentes de bonos, las personas que habían creado los valores tóxicos respaldados por las hipotecas y las coberturas por riesgos crediticios. Fue la primera de una larga lista de actuaciones que, en esencia, garantizaban la deuda mala de la industria de las finanzas, pero que apenas hizo nada por ayudar a los propietarios de las viviendas y a los estadounidenses corrientes. Después de que Lehman Brothers se declarara en bancarrota en septiembre de 2008, los precios de las acciones y las materias primas se desplomaron y la economía mundial quedó al borde del colapso. Coordinándose con los bancos centrales de otros países, el gobierno estadounidense ofreció 700 000 millones de dólares⁸ en rescates financieros a bancos y billones de dólares en garantías de préstamos, logrando cortar lo peor del contagio. La expansión o flexibilización cuantitativa (EC o FC), por la cual un banco central adquiere productos financieros en el mercado libre para aportar garantías a los inversores, hizo el resto. Mediante la compra de fondos públicos a más largo plazo y de valores respaldados por las hipotecas, la Reserva Federal fomentó los préstamos y la inversión. Junto con el rescate financiero y las garantías a los préstamos, la EC borró billones de dólares de deuda corporativa de los libros de algunas de las mayores compañías (y hasta hace poco las más rentables) de Estados Unidos. Esa deuda fue absorbida por la hoja de balance del gobierno federal. Antes de la crisis, los activos de la Reserva Federal⁹ eran de 900 000 millones de dólares. A principios de 2010, eran de 2,3 billones de dólares.

Esto no acabó aquí. Estas políticas, que en su origen se planearon como una respuesta a corto plazo frente a una crisis inmediata, se arraigaron. Por razones tanto políticas como económicas, la Reserva Federal encontraría imposible deshacer su respaldo a la economía. De hecho, siguió aumentando. Hacia finales de 2014, lo que habían sido 2,3 bi-

8. Departamento del Tesoro de Estados Unidos: «Troubled Assets Relief Program (TARP)». <https://home.treasury.gov/data/troubled-assets-relief-program>

9. Consejo de Administración del Sistema de la Reserva Federal de Estados Unidos: «Credit and Liquidity Programs and the Balance Sheet». www.federalreserve.gov/monetarypolicy/bst_recenttrends.htm

lones de dólares en activos en los libros de contabilidad de la Reserva Federal habían crecido hasta los 4,4 billones de dólares: un nivel al que más o menos permanecería hasta marzo de 2020, cuando golpeó la COVID-19. Al mismo tiempo, los tipos de interés¹⁰ también permanecieron en niveles históricamente bajos: un 0% hasta 2016, y sólo subiendo por encima del 2% en 2019.

La respuesta del gobierno ante la crisis de las hipotecas *subprime* dio lugar a una era de dinero fácil que ha beneficiado a las corporaciones adineradas más que a nadie, pero eso no fue todo lo que ocasionó. Tras la desconfianza general nacida de la crisis, surgió una nueva mutación del sistema financiero: las criptomonedas.



El pueblo estadounidense había rescatado al sector empresarial de Estados Unidos, y no estaba contento con eso. Los ejecutivos financieros que se beneficiaron de la burbuja inmobiliaria quedaron impunes: sólo un tipo, un ejecutivo de Credit Suisse, acabó en la cárcel.¹¹ A millones de personas corrientes se les endosó una deuda insostenible, lo que contribuyó a un aumento del sinhogarismo, suicidios y depresión. Las pérdidas fueron, efectivamente, socializadas. Una poderosa narrativa desarrollada a partir de la tragedia de la gente corriente que había sido estafada por las élites. En el lado izquierdo, esto ayudó a inspirar el movimiento Ocupa Wall Street. En el lado derecho apareció el Tea Party. En Internet, a través de un autor (o autores) con pseudónimo, surgió otra historia.

La noche de Halloween de 2008, alguien o algunas personas que se hacía o hacían llamar Satoshi Nakamoto publicaron lo que se vendría a conocer como el libro blanco del bitcoin.¹² Todavía no sabemos quién era Satoshi, pero su libro blanco tendría un profundo impacto en la

10. FRED Economic Data / St. Louis Fed: «Federal Funds Effective Rate». <https://fred.stlouisfed.org/series/FEDFUNDS>

11. Wikipedia: «Kareem Serageldin», modificado por última vez el 5 de octubre, 2022. https://en.wikipedia.org/wiki/Kareem_Serageldin

12. Yakamoto, S.: «Bitcoin: A peer-to-peer electronic cash system». <https://bitcoin.org/bitcoin.pdf>

innovación financiera y en el futuro del dinero digital. Satoshi tenía una visión clara: «Una versión puramente entre iguales del dinero electrónico permitiría que los pagos *online* se enviaran directamente de una parte a la otra sin pasar por una institución financiera... La propia red requiere de una estructura mínima».

La propuesta de Satoshi era audaz, promocionada como un nuevo método que ayudaría a la gente a efectuar transacciones directamente entre sí, evitando a las instituciones financieras (de hecho, eso no es verdaderamente cierto. No se llevarían a cabo transacciones directamente, sino más bien a través de una base de datos compartida bajo un control común o colaborativo). Remplazar a una autoridad centralizada como un banco era algo más fácil de decir que de hacer, pero Satoshi ofreció una solución novedosa. Se basaba en combinar dos tecnologías desarrolladas anteriormente: la criptografía o cifrado de clave pública (o asimétrica) y la cadena de bloques o *blockchain*.

La criptografía de clave pública desempeña un papel vital en la vida moderna. Por ejemplo, todas las páginas web <https://> (casi todas las que usan las personas corrientes) emplean el cifrado asimétrico. Hace cosas como evitar que la información de las tarjetas de crédito sea robada al hacer compras *online*. La criptografía de clave pública posee dos propiedades útiles: cualquiera puede verificar la legitimidad de una transacción empleando información disponible públicamente (la clave pública), pero las personas/partes que llevan a cabo esas transacciones pueden mantener su identidad oculta (la clave privada).

Satoshi vinculó el sistema de cuentas (o direcciones) numeradas del bitcoin a claves públicas. Las transferencias de bitcoins entre cuentas son mensajes formados por la clave privada correspondiente a la dirección de origen autorizando la transferencia a la dirección o direcciones receptora(s). Las direcciones son, entonces, organizadas en forma de «carteras»: un *software* que gestiona la contabilidad y la traduce al equivalente de un único saldo bancario en lugar de docenas o cientos de direcciones distintas. De manera importante, el ser propietario de bitcoins es algo pseudónimo (pero no anónimo, como suele afirmarse erróneamente). Todos pueden ver qué direcciones están interactuando entre sí en un libro de contabilidad público, pero la gente no es consciente de quién es el propietario de cada dirección.

Este libro de contabilidad con un registro del horario y que sólo permite adjuntar datos es la cadena de bloques. En 1991, los ingenieros informáticos Stuart Haber y W. Scott Stornetta, basándose en el trabajo del criptógrafo David Chaum,¹³ dieron con una forma de registrar horariamente documentos, de forma que no pudieran amañarse. Cada «bloque» contiene el resumen criptográfico (un resumen computable breve de toda la información contenida en él) del bloque anterior, vinculando a los dos y generando un registro irreversible, un libro de contabilidad formado por bloques de datos que pueden añadirse a una cadena (*cadena de bloques*), pero de la que no pueden sustraerse datos.

Por ahora todo iba bien, pero seguía habiendo un problema: lo que se conoce como el *problema del doble gasto*. Si eliminas a una autoridad centralizada de la ecuación, ¿cómo te aseguras de que la gente no se la esté jugando al sistema gastando dinero que ya se ha enviado a algún otro lugar? ¿Cómo proteges a la red de la manipulación? «Satoshi» confiaba en lo que se llama *algoritmo de consenso*.

Un algoritmo de consenso es un proceso mediante el cual la gente con unos puntos de vista diferentes puede alcanzar un acuerdo limitado sobre un resultado con el paso del tiempo. La innovación del bitcoin consiste en hacer esto sin confiar en ningún reloj. Cada bloque del libro de contabilidad de los bitcoins debe cumplir las leyes del bitcoin. Por ejemplo, no puedes gastar un dinero que no tienes. Eso se puede comprobar muy rápidamente, pero ¿cómo sabes qué bloques se encuentran en el libro de contabilidad?

Cada bloque publicado remite al bloque anterior, cumple todas las normas y tiene un resumen criptográfico. Muchos, muchísimos bloques candidatos se calculan para encontrar el siguiente bloque, pero, una vez que se encuentra, toda la red coincide en que se trataba del siguiente bloque correcto.

Sin embargo, no pueden alcanzar este acuerdo a nivel mundial al instante, por lo que hay normas adicionales. Dichas normas tienen el efecto de incrementar la certeza del bloque actual correcto y de sus predecesores a lo largo del tiempo. La red se enfoca en un nuevo bloque

13. «Blind signatures for untraceable payments», Springer-Verlag, 1982. <https://chaum.com/wp-content/uploads/2022/01/Chaum-blind-signatures.pdf>

cada diez minutos, más o menos, adaptando dinámicamente el grado de dificultad necesario del bloque ganador. Cuantos más participantes, más difícil se vuelve el proceso y más energía es necesaria para adivinar el siguiente bloque de forma correcta. Ésta es la *prueba de trabajo* que hay tras el bitcoin: muchísimos ordenadores («mineros») llevando a cabo operaciones matemáticas relativamente sencillas una y otra vez, sin fin. El minero que tropieza con el bloque correcto es recompensado con un bitcoin por su esfuerzo. Al cabo de una hora, los participantes en la red están convencidos y, ya metidos en harina, con seis bloques: saben que es extremadamente improbable que nadie reescriba esa historia.

Como podría decirse, la visión de Satoshi es inmensamente inteligente, pero también engorrosa, hablando de forma práctica. A medida que más participantes se apuntan, el resumen criptográfico aumenta y se invierte más energía para ponerse de acuerdo sobre un bloque de datos que sigue siendo, más o menos, del mismo tamaño. Esto es lo que se llama una carrera de la Reina Roja, en referencia a *Alicia en el País de las Maravillas*, de Lewis Carroll, cuando la reina le dice a Alicia: «Pues bien, verás, aquí, *tienes que correr tanto como puedas para permanecer en el mismo lugar. ¡Si quieres desplazarte a otro, entonces, debes correr el doble de rápido!*».

Ése era el marco tecnológico y filosófico básico para el bitcoin, la criptomoneda original a partir de la cual surgió el resto. Ethereum, la segunda criptomoneda más importante en el momento de la redacción de este libro, se lanzó en 2015. Ofrecía una cadena de bloque alternativa y de código abierto y adquirió fama por ofrecer lo que se llaman *contratos inteligentes*: pequeños programas informáticos que ejecutan funciones automáticamente en la cadena de bloques de Ethereum. Un ejemplo sencillo puede consistir en usar contratos inteligentes para replicar el proceso de custodia por parte de una tercera persona. Podías programar una transacción que se llevaría a cabo si dos de las tres partes (como un comprador, un vendedor y un árbitro de confianza) dijeran que debería llevarse a cabo. Esto permitiría que el contrato actuara como algo parecido a un depositario, pero con una diferencia crítica: el depositario nunca debe, en realidad, poseer el dinero (de todos modos, ésa es la idea. En la práctica, estos «contratos» suelen encontrarse con problemas, tanto prácticos como legales).

Independientemente de ello, los contratos inteligentes se promocionaron como forma de automatizar los mercados financieros e introducir nuevos instrumentos financieros complicados. De ellos surgieron las DeFi, o finanzas descentralizadas: un vasto ecosistema no regulado de intercambios de criptomonedas, fondos comunes de préstamos, protocolos de negocios (en este contexto «protocolo» significa un conjunto de normas que permiten que se compartan datos entre ordenadores) y productos financieros complejos. Ethereum también llevó a la introducción de los NFT (tokens o vales no fungibles), que son básicamente enlaces de recibos de archivos JPEG almacenados en cadenas de bloque (chitón, no se lo digas a nadie que tenga uno). El número de criptomonedas se disparó en esta época, multiplicándose por diez en cinco años, pasando de menos de cien en 2013 a más de mil en 2017. Hoy se estima que hay 20 000 criptomonedas, la mayoría de ellas pequeñas e insignificantes, con su propiedad concentrada en las manos de unos pocos «peces gordos», y son muy parecidas a las acciones muy baratas de la bolsa (chicharros).

Si todo esto te parece complicado y confuso, no te preocupes, porque no estás solo. Me resulta confuso incluso a mí ahora. Si te hace sentir mejor, la mayoría de las personas que tienen bitcoins no pueden explicarlo con precisión (aunque jurarán que sí pueden). Aquí tenemos las buenas noticias: ahora eres libre de olvidar todo lo que acabo de decir. Los detalles operativos de la tecnología de la cadena de bloques no son importantes para comprender el ascenso de las criptomonedas en la cultura popular. Recuerda que la cadena de bloques tiene por lo menos treinta años y que apenas es usada por las empresas fuera de la industria de las criptomonedas. Desde por lo menos 2016, cientos de compañías han intentado incorporarla a su modelo de negocio, para después descartarla porque no funcionaba mejor que lo que ya estaban usando. Hazte una sencilla pregunta: Si la cadena de bloques es tan revolucionaria, después de treinta años, ¿por qué son las apuestas su único caso de uso? De forma bastante irónica, la tecnología más importante es la que le precede: la criptografía o cifrado de clave pública.

Lo que es importante comprender sobre las criptomonedas es la narrativa económica que se desarrolló a su alrededor: una constelación de relatos que a veces se superponen que se desarrollaron a lo largo de su

existencia. El relato original (que el bitcoin representa una respuesta ante los fracasos devastadores del sistema financiero tradicional) conserva una potencia importante porque todos estamos de acuerdo con su premisa: nuestro sistema financiero actual apesta. ¿Pero es el relato del bitcoin realmente cierto? ¿Hace lo que afirma hacer: crear una divisa entre iguales libre de intermediarios? ¿Era una moneda o divisa «sin confianza» (es decir, que no es necesario depositar toda la confianza en un solo ente, individuo o institución para que el sistema funcione) y que se basaba sólo en el código informático siquiera posible?

Para las primeras personas que adoptaron el bitcoin, esos debates seguían estando por venir. Habiéndose tropezado con un sistema monetario potencialmente nuevo, estaban centrados en una única pregunta: ¿podría volverse viral?



Puede que el bitcoin sea la divisa digital más popular, pero no fue la primera. En un artículo publicado en 1982, el criptógrafo David Chaum teorizó sobre el andamiaje intelectual de la cadena de bloques, sobre el que emergerían las criptomonedas alrededor de un cuarto de siglo más tarde. Chaum fundó DigiCash,¹⁴ su propia compañía de divisas digitales, a finales de la década de 1980. Aunque técnicamente no estaba basada en las cadenas de bloques, poseía características de privacidad criptográficas que tendrían un peso importante en iteraciones posteriores del dinero digital. DigiCash fue un proyecto legítimo, sin los conflictos de interés ni otras señales de alarma que rodean a otras empresas de criptomonedas. Lamentablemente, no logró despegar y a finales de la década de 1990 la compañía se declaró en bancarrota antes de ser vendida.

De forma similar, otros intentos con las monedas digitales no lograron alcanzar el éxito. Por ejemplo, eGold,¹⁵ fundado a finales de la dé-

14. Wikipedia: «DigiCash», modificado por última vez el 14 de marzo, 2022. <https://en.wikipedia.org/wiki/DigiCash>

15. Zetter, K.: «Bullion and bandits: The improbable rise and fall of E-Gold», *Wired*, 9 de junio, 2009. www.wired.com/2009/06/e-gold/

cada de 1990, permitía a sus clientes adquirir cantidades ínfimas de propiedades físicas de oro en el extranjero. Este proyecto se vio plagado de problemas: principalmente que los criminales empezaron a usarlo para blanquear dinero y otros fines ilícitos. Duró hasta mediados de la década de 2000, antes de ser cerrado por los agentes federales por violar las leyes de envío de dinero. Una historia similar implicó a Liberty Reserve,¹⁶ un servicio anónimo de envío de dinero dirigido desde Costa Rica. Los usuarios podían depositar dinero en una cuenta virtual en dólares mediante una transferencia bancaria electrónica o un abono y, luego, transferir esos fondos a otros clientes de Liberty. No había restricciones legales ni ningún esfuerzo por validar a los clientes o evitar el flujo de dinero ilícito, cosa que probablemente era el meollo del asunto. En 2013, en una operación que implicó a las autoridades de más de una docena de países, el FBI llevó a cabo una redada en Liberty por violar leyes de blanqueo de capitales, poniendo fin a este banco sin licencia en la sombra. Su fundador se declaró culpable y se le condenó a pasar veinte años en prisión.

El bitcoin tuvo otros precedentes importantes en áreas que iban desde las apuestas *online* hasta al intercambio de objetos en los juegos de rol multijugador *online*: cualquier lugar en el que se intercambiaran valores de forma digital. Tanto si se trataba de depositar dinero en casinos *online* como de pagarle a un elfo negro por su espada en el juego *EverQuest*, el asunto de cómo enviar dinero (o un equivalente digital) a alguien sin interferencias por parte de partes externas molestas seguía teniendo que resolverse adecuadamente. PayPal y otros servicios de pago ya existían, pero estaban sujetos a guardianes fastidiosos como la ley, las fronteras nacionales, los bancos y los acuerdos con las condiciones del servicio; y aunque algunos juegos, más destacablemente *Second Life*, con sus dólares linden, generaban economías *online* prósperas, seguían teniendo que captar al público en general.

16. Comunicado de prensa: «Founder of Liberty Reserve pleads guilty to laundering more than \$250 million through his digital currency business», Departamento de Justicia de Estados Unidos. www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundrying-more-250-million-through-his-digital